Available at: http://www.ictp.trieste.it/~pub_off IC/99/86

United Nations Educational Scientific and Cultural Organization
and
International Atomic Energy Agency
THE ABDUS SALAM INTERNATIONAL CENTRE FOR THEORETICAL PHYSICS

CURVES OF LARGE GENUS COVERED BY THE HERMITIAN CURVE

A. Cossidente[1] and G. Korchmáros[2]
Dipartimento di Matematica, Università della Basilicata, via N. Sauro 85, 85100 Potenza, Italy

and

F. Torres[3]
IMECC-UNICAMP, Cx. P. 6065, Campinas, 13083-970-SP, Brazil
and
The Abdus Salam International Centre for Theoretical Physics, Trieste, Italy.

Abstract

For the Hermitian curve $\mathcal{H}$ defined over the finite field $\mathbf{F}_{q^2}$, we give a complete classification of Galois coverings of $\mathcal{H}$ of prime degree. The corresponding quotient curves turn out to be special cases of wider families of curves $\mathbf{F}_{q^2}$-covered by $\mathcal{H}$ arising from subgroups of the special linear group $SL(2, \mathbf{F}_q)$ or from subgroups in the normaliser of the Singer group of the projective unitary group $PGU(3, \mathbf{F}_{q^2})$. Since curves $\mathbf{F}_{q^2}$-covered by $\mathcal{H}$ are maximal over $\mathbf{F}_{q^2}$, our results provide some classification and existence theorems for maximal curves having large genus, as well as several values for the spectrum of the genera of maximal curves. For every q^2, both the upper limit and the second largest genus in the spectrum are known, but the determination of the third largest value is still in progress. A discussion on the "third largest genus problem" including some new results and a detailed account of current work is given.

MIRAMARE – TRIESTE
July 1999

[1] E-mail: cossidente@unibas.it
[2] E-mail: korchmaros@unibas.it
[3] Regular Associate of the Abdus Salam ICTP. E-mail: ftorres@ime.unicamp.br

1. Introduction

In the current study of algebraic geometry in positive characteristic there is a growing interest to curves which are defined over a finite field $\mathbf{F}$ and have many $\mathbf{F}$-rational points. Such curves, especially $\mathbf{F}$-*maximal curves*, play indeed a very important role in Coding theory [16], Chapter 4, §7, [24], §8, [34], §VII.4, [38], §3.2.3, and some further motivation for their investigation also comes from Number Theory [28], [32] and Finite Geometry [20]. Here, maximality of a (projective geometrically irreducible non-singular algebraic) curve means that the number of its $\mathbf{F}$-rational points attains the Hasse-Weil upper bound

$$q^2 + 1 + 2qg\,,$$

with g being the genus of the curve and $\mathbf{F}$ the field $\mathbf{F}_{q^2}$ of order q^2. The majority of work has focused on determining the spectrum for the genera of maximal curves, and the relevant known results and open problems concern those maximal curves which have large genus g with respect to the order q^2 of the underlying field; see for example [2], [4], [7], [10], [11], [13], [14], and [15]. The precise upper bound limit is known to be $q(q-1)/2$ [23]. It seems plausible that only few maximal curves can have genus not too distant from the upper limit. However, the problem of finding and classifying such maximal curves is still open and appears to be rather difficult. For an up-dated discussion of the state of the art, see Section 5. The most well-known maximal curve is the so-called Hermitian curve $\mathcal{H}$ which is defined by the equation

$$Y^q Z + Y Z^q - X^{q+1} = 0\,. \tag{1.1}$$

In fact, $\mathcal{H}$ is the only $\mathbf{F}_{q^2}$-maximal curve, up to isomorphism, of genus $q(q-1)/2$ [29] and has a very large automorphism group (over $\mathbf{F}_{q^2}$), namely $\mathrm{Aut}(\mathcal{H}) \cong PGU(3, \mathbf{F}_{q^2})$. Moreover, all $\mathbf{F}_{q^2}$-quotient curves of $\mathcal{H}$ are also $\mathbf{F}_{q^2}$-maximal, see [26], Proposition 6. So, it would be of interest to solve the above mentioned open problem for quotient curves arising from automorphism groups of small order. The key to the solution is to classify all quotient curves of $\mathcal{H}$ arising from automorphisms of prime order; in other words to give a complete classification of Galois $\mathbf{F}_{q^2}$-coverings $\pi : \mathcal{H} \to \mathcal{X}$ of prime degree. This is actually the main goal in the present paper. Theorem 2.1 states that only five types of such coverings exist. It should be noted that almost all explicit examples of maximal curves in the literature are quotient curves of $\mathcal{H}$. This suggests that Theorem 2.1 might be an essential step toward the complete solution to the spectrum problem for maximal curves having large genus. For this reason, Theorem 2.1 also gives some further useful information, such as an explicit equation for a plane model of the covered curve. Actually, all these curves appear in previous work as special cases of wider families, see Remark 2.3. Some new information will be given in Sections 3 and 4, such as curves of types (I), (II), (III) and (IV) in Theorem 2.1 can be obtained from subgroups of prime order of $SL(2, \mathbf{F}_q)$ while those of class (V) from the Singer group S of $\mathcal{H}$. This gives a motivation for the study of quotient curves arising from subgroups of $SL(2, \mathbf{F}_q)$ or from subgroups of the normaliser in S. In Section 3, a variant of the classical Riemann-Hurwitz formula will be stated which allows a straightforward computation of the genus of all such but tame curves. However, the apparently difficult problem of determining an explicit (possibly singular) plane model for each of them remains open.

The present research is a continuation of [4] in which quotient curves arising from the subgroups of the Singer group of $\mathrm{Aut}(\mathcal{H})$ have been investigated. Computations concerning the genera of certain quotient curves covered by $\mathcal{H}$ are also given in [11]. However, their methods and results are quite different from ours, apart from a very few overlapping parts, see Remarks 2.3, 3.4, 4.3.

Throughout the paper we use the term of a *curve* to denote a projective geometrically irreducible non-singular algebraic curve defined over the algebraic closure $\bar{\mathbf{F}}_{q^2}$ of a finite field $\mathbf{F}_{q^2}$, of characteristic p, equipped with the Frobenius morphism over $\mathbf{F}_{q^2}$.

For basic facts on curves the reader is referred to [30] and [19], Chapter IV. The necessary background on finite groups and especially on subgroups of $PGU(3,\mathbf{F}_{q^2})$ can be found in [22], [20], and [21].

2. Classification of curves prime degree Galois covered by the Hermitian curve

Our purpose is to prove the following theorem.

Theorem 2.1. *Let $\mathcal{H}$ be the Hermitian curve defined over $\mathbf{F}_{q^2}$ and d a prime number. For a curve $\mathcal{X}$ of genus g such that $\pi : \mathcal{H} \to \mathcal{X}$ is a Galois $\mathbf{F}_{q^2}$-covering of degree d, we have either $d = 2 \neq p$ or $d = p$ or $d \geq 3$ and $(q^2-1)(q^2-q+1) \equiv 0 \pmod{d}$. Moreover, up to $\mathbf{F}_{q^2}$-isomorphism one the following cases occurs:*

(I) *$d = 2 \neq p$, $\mathcal{X}$ is the non-singular model of the plane curve*

$$y^q + y = x^{(q+1)/2}\,, \qquad \text{and} \quad g = \frac{(q-1)^2}{4}\,;$$

(II) *$d = p$ with $q = p^t$, $\mathcal{X}$ is the non-singular model of one of the following plane curves*

(1)

$$\sum_{i=1}^{t} y^{q/p^i} + \omega x^{q+1} = 0\,, \qquad \text{and} \quad g = \frac{q}{2}(\frac{q}{p} - 1)\,,$$

where ω is a fixed element of $\mathbf{F}_{q^2}$ such that $\omega^{q-1} = -1$;

(2)

$$y^q + y = (\sum_{i=1}^{t} x^{q/p^i})^2\,, \qquad \text{and} \quad g = \frac{q(q-1)}{2p}\,,$$

provided that $p \geq 3$;

(III) *$d \geq 3$ and $q \equiv 1 \pmod{d}$, $\mathcal{X}$ is the non-singular model of the plane curve*

$$y^q - yx^{2(q-1)/d} + \omega x^{(q-1)/d} = 0\,, \qquad \text{and} \quad g = \frac{q(q-1)}{2d}\,,$$

where ω is a fixed element in $\mathbf{F}_{q^2}$ such that $\omega^{q-1} = -1$;

(IV) *$d \geq 3$ and $q \equiv -1 \pmod{d}$, $\mathcal{X}$ is the non-singular model of one of the following plane curves*

(1)

$$y^q + y = x^{(q+1)/d}\,, \qquad \text{and} \quad g = \frac{q-1}{2}(\frac{q+1}{d} - 1)\,;$$

(2)

$$x^{(q+1)/d} + x^{2(q+1)/d} + y^{q+1} = 0\,, \qquad \text{and} \quad g = \frac{(q+1)(q-2)}{2d} + 1\,;$$

(V) *$d \geq 3$ and $(q^2-q+1) \equiv 0 \pmod{d}$, $\mathcal{X}$ is the non-singular model of the plane curve*

$$s(x^{q/d}, y^{1/d}, x^{1/d}y^{q/d}) = 0\,, \qquad \text{and} \qquad g = \frac{1}{2}(\frac{q^2-q+1}{d} - 1)\,; \tag{2.1}$$

where $s(X,Y,Z) := \prod(\beta X + \beta^q Y + Z)$, with β ranging over all d-th roots of unity.

Remark 2.2. The plane curve $\mathcal{C}$ given in (2.1) is actually a plane model of $\mathcal{X}$ over $\mathbb{F}_{q^3}$. To obtain a plane model over $\mathbf{F}_{q^2}$, one needs to replace $\mathcal{C}$ by $\kappa^{-1}(\mathcal{C})$, with κ as in (2.3). It turns out that a plane model of $\mathcal{X}$ over $\mathbf{F}_{q^2}$ is given by $cu(X,Y,Z) = 0$, where c is an appropriate element in $\mathbf{F}_{q^6}$ and

$$u(X,Y,Z) = s(aX + Y + a^{q^2+1}Z, a^{q^2+1}X + aY + Z, X + a^{q^2+1}Y + aZ) = 0\,, \tag{2.2}$$

$s(X,Y,Z)$ being the projectivization of (2.1).

Remark 2.3. Maximal curves over $\mathbf{F}_{q^2}$ with genera as in Theorem 2.1 are known to exist, see [10], Examples D, E, F, [13], Thm. 3.1, [14], Remark 5.2, [4], [11], Thm. 5.1, Corollary 4.5, Example 5.10, Example 6.3. However, the interesting question of determining all such maximal curves is still open, apart from case (I) for which uniqueness up to $\mathbf{F}_{q^2}$-isomorphism has been already proved [7], Thm. 3.1. In this context, Theorem 2.1 states the uniqueness for maximal curves prime degree Galois covered by the Hermitian curve, and it also provides a plane model for such curves by an explicit equation. For $d = 3$ (or, equivalently $q \equiv 2 \pmod 3$), Theorem 2.1(V) states that

$$\begin{aligned} s(X,Y,Z) &= (X+Y+Z)(\beta X + \beta^2 Y + Z)(\beta^2 X + \beta Y + Z) \\ &= X^3 + Y^3 + Z^3 - 3XYZ\,, \end{aligned}$$

so that

$$s(x^{q/3}, y^{1/3}, x^{1/3}y^{q/3}) = x^q + y + xy^q - 3(xy)^{(q+1)/3}\,,$$

defines a plane model over $\mathbb{F}_{q^3}$ of a $\mathbf{F}_{q^2}$-maximal curve of genus $(q+1)(q-2)/6$. As before, a plane model over $\mathbf{F}_{q^2}$ for such a curve is given by $cu(X,Y,Z) = 0$, where $u(X,Y,Z)$ is as in (2.2), $s(X,Y,Z) = X^qZ + YZ^q + XY^q - 3(XYZ)^{(q+1)/3}$ and c is an appropriate element in $\mathbf{F}_{q^6}$. It should be noticed that this was originally stated in [4], §6.

The proof of Theorem 2.1 uses the well-known isomorphism $\mathrm{Aut}(\mathcal{H}) \cong PGU(3, \mathbf{F}_{q^2})$ (see e.g. [27], [18], [21], [33]) and it depends on the classification of subgroups of $PGU(3, \mathbf{F}_{q^2})$ of prime order, see Proposition 2.4. We recall that $\mathrm{Aut}_{\mathbf{F}_{q^2}}(\mathcal{H}) = \mathrm{Aut}_{\bar{\mathbf{F}}_{q^2}}(\mathcal{H})$, [17], p. 101. To have an appropriate description of the actions of such subgroups on $\mathcal{H}$, we also need four more plane models of $\mathcal{H}$ different from (1.1), namely:

(M1) $X^{q+1} + Y^{q+1} + Z^{q+1} = 0$;
(M2) $Y^qZ - YZ^q + \omega X^{q+1} = 0$, where ω is a fixed element of $\mathbf{F}_{q^2}$ such that $\omega^{q-1} = -1$;
(M3) $XY^q - X^qY + \omega Z^{q+1} = 0$, where ω is a fixed element in $\mathbf{F}_{q^2}$ such that $\omega^{q-1} = -1$;
(M4) $XY^q + YZ^q + ZX^q = 0$.

Note that each of the models (M1), (M2) and (M3) is $\mathbf{F}_{q^2}$-isomorphic to (1.1). The model (M4) is $\mathbb{F}_{q^3}$-isomorphic to (M1), since for a suitable element $a \in \mathbf{F}_{q^6}$, the projective map

(2.3)

$$\kappa : \mathbf{P}^2(\bar{\mathbf{F}}_q) \to \mathbf{P}^2(\bar{\mathbf{F}}_q) \quad (x : y : x) \mapsto (ax + y + a^{q^2+1}z : a^{q^2+1}x + ay + z : x + a^{q^2+1}y + az)\,.$$

changes (M1) into (M4), cf. [4], Prop. 4.6.

Proposition 2.4. *Let $C_d = \langle T_d \rangle$ be a subgroup of $\mathrm{Aut}(\mathcal{H}) \cong PGU(3, \mathbf{F}_{q^2})$ of prime order d. Then d is as in Theorem 2.1 and up to conjugacy:*

(I) *If $d = 2 \neq p$ and $\mathcal{H}$ is defined by (1.1), then*

$$T_d : (X, Y, Z) \mapsto (-X, Y, Z)\,;$$

(II) *Let $d = p$.*

(1) If $\mathcal{H}$ is defined by (M2), then

$$T_d : (X, Y, Z) \mapsto (X, Y + Z, Z)\,;$$

(2) If $p \geq 3$ and $\mathcal{H}$ is defined by (1.1), then

$$T_d : (X, Y, Z) \mapsto (X + Z, X + Y + Z/2, Z)\,;$$

(III) *If $d \geq 3$ and $q \equiv 1 \pmod{d}$ and $\mathcal{H}$ is defined by (M3), then*

$$T_d : (X, Y, Z) \mapsto (\alpha X, \alpha^{-1} Y, Z)\,;$$

where α is a primitive d-th root of unity;

(IV) *If $d \geq 3$ and $q \equiv -1 \pmod{d}$ and $\mathcal{H}$ is defined by (M1), then we have two possibilities, either*

(1)

$$T_d : (X, Y, Z) \mapsto (\alpha X, Y, Z)\,, \quad \textit{or}$$

(2)

$$T_d : (X, Y, Z) \mapsto (\alpha X, \alpha^{-1} Y, Z)\,,$$

where α is a primitive d-th root of unity;

(V) *If $d \geq 3$ and $(q^2 - q + 1) \equiv 0 \pmod{d}$ and $\mathcal{H}$ is defined by (M4), then*

$$T_d : (X, Y, Z) \mapsto (\alpha X, \alpha^{q} Y, Z)\,,$$

where α is a primitive d-th root of unity.

Proof. An essential tool in the proof is the classification of all maximal subgroups of $PGU(3, \mathbf{F}_{q^2})$ given by Mitchell [27], q odd, and by Hartley [18], q even (see also [25], Ch. V, [21]). This group has order $q^3(q^3 + 1)(q^2 - 1)$. Hence there is a Sylow d-subgroup of $PGU(3, \mathbf{F}_{q^2})$ for each prime divisor d of q, $q + 1$, $q - 1$, and $(q^2 - q + 1)$. Since every subgroup of order d is contained in a Sylow d-subgroup and any two Sylow d-subgroups are conjugate, we may choose a Sylow d-subgroup R_d for each d, and only consider those subgroups C_d of order d that are contained in R_d.

(I) In $PGU(3, \mathbf{F}_{q^2})$, q odd, elements of order 2 are pairwise conjugate, and if $\mathcal{H}$ is given by (1.1), then T_d in (I) is an automorphism of order 2 in $\mathrm{Aut}(\mathcal{H})$.

(II) We first show that $G := \mathrm{Aut}(\mathcal{H}) \equiv PGU(3, \mathbf{F}_{q^2})$ has either one or two conjugacy classes of subgroups of order p, according as $p = 2$ or $p \geq 3$. Let $\mathcal{H}$ have equation 1.1. Then a Sylow p-subgroup R_p of G fixes the point $Q := (0 : 1 : 0)$ and consists of all automorphisms

$$(X, Y, Z) \to (X + aZ, Y + a^q X + bZ, Z)\,,$$

where $a, b \in \mathbf{F}_{q^2}$, and $b^q + b = 0$. Since no non-trivial element in R_p fixes a further point of $\mathcal{H}$, two elements of R_p are conjugate in G iff they are in the stabilizer G_Q of Q. By [22], §10.12, G_Q is the semidirect product of R_p with a group H of order $(q-1)$ comprising all automorphisms

$$(X, Y, Z) \to (uX, u^{q+1}Y, Z)\,, \qquad u \in \mathbf{F}_{q^2}^*\,.$$

Note that the center $Z(R_p)$ of R_p consists of all automorphisms

$$(X, Y, Z) \to (X, Y + b, Z)\,, \qquad b \in \mathbf{F}_q\,.$$

A direct computation shows that $Z(R_p)$ is a full conjugacy class of elements of order p in G_Q. For $p = 2$, each element of order p is in $Z(R_p)$. Hence we may assume that $p \geq 3$. Now let T_p be as in (II)(2). A straightforward computation shows that the centralizer of T_p in G_Q has order q^2, as it consists of all automorphisms

$$(*) \qquad (X, Y, Z) \to (X + aZ, Y + a^q X + bZ, Z)\,, \qquad a, b \in \mathbf{F}_q\,.$$

Hence, the conjugacy class of T_p comprises $q(q^2-1)$ elements of G_Q. Since $q^3 = q + q(q^2-1)$, this proves that each non-central element of R_p is conjugate to T_p under G_Q. Thus G has exactly two conjugacy classes of elements of order p, provided that $p \geq 3$. Now we are in a position to prove II(1).

For $p = 2$, the case $a = 0$ and $b = 1$ in $(*)$ gives T_2 in (II)(1). For $p \geq 3$, we see that T_p above is isomorphic to the automorphism in (II)(1) as follows. We change the model (1.1) into the model (M2) via the automorphism $(X, Y, Z) \to (\omega^{-1}X, \omega^{-1}Y, Z)$ with a fixed $\omega \in \mathbf{F}_{q^2}^2$ such that $\omega^{q-1} = -1$; then, the automorphism for $a = 0$ and $b = \omega^{q-1}$ in $(*)$ is turned into the automorphism in (II)(1).

(III) Let $d \geq 3$ and $q \equiv 1 \pmod{d}$, and denote by D the largest multiplicative subgroup of $\mathbf{F}_q$ of order a power of d. Then the automorphisms $(X, Y, Z) \to (uX, u^{-1}Y, Z)$ with u ranging in D, form a subgroup which turns out to be a Sylow d-subgroup R_d of $PGU(3, \mathbf{F}_{q^2})$. Since R_d is cyclic, it has only one subgroup of order d. On the other hand, R_d contains the automorphism T_d as given in this case and the result follows.

(IV) Let $d \geq 3$ and $q \equiv -1 \pmod{d}$. First we consider the case $d = 3$. Define j as the greatest power of 3 which divides $q + 1$. Then a Sylow 3-subgroup of $PGU(3, \mathbf{F}_{q^2})$ has order 3^{j+1}. To determine such a Sylow 3-subgroup R_3 explicitly, we adopt the plane model (M1) for $\mathcal{H}$. Let us introduce the following automorphisms of $\mathcal{H}$:

$$\phi_{u,v} : (X, Y, Z) \to (uX, vY, Z)\,,$$
$$\psi_{u,v} : (X, Y, Z) \to (Z, uX, vY)\,,$$
$$\tau_{u,v} : (X, Y, Z) \to (vY, uZ, X)\,.$$

where $u, v \in \mathbf{F}_{q^2}$. If both u and v only range in the subgroup M of order 3^j of $\mathbf{F}_{q^2}^*$, then the above automorphisms form a group of order 3^{j+1} which is a Sylow 3-subgroup R_3 of $PGU(3, \mathbf{F}_{q^2})$.

Note that R_3 is the semidirect product of $C_3 \times C'_{3^j}$ by C''_3, where $C_{3^j} = \langle \phi_{\epsilon,1} \rangle$, $C'_{3^j} = \langle \phi_{1,\epsilon} \rangle$, $C''_3 = \langle \psi_{1,1} \rangle$, and ϵ is a primitive third root of unity in $\mathbf{F}_{q^2}$. Moreover, the elements of order 3 in R_3 are $\phi_{u,v}$ with $u^3 = v^3 = 1$, $\psi_{u,v}$ and $\tau_{u,v}$, with $u, v \in M$. Now let ϕ be an element of order 3 in $C_{3^j} \times C'_{3^j}$. It is straightforward to check that ϕ is conjugate either to $\phi_{\epsilon,1}$ or to $\phi_{\epsilon,\epsilon^2}$ under a suitable element $\phi_{u,v}$, $u, v \in \mathbf{F}^*_{q^2}$. This shows that each subgroup of $C_{3^j} \times C'_{3^j}$ of order 3 is either (IV)(1) or (IV)(2), up to conjugacy. The next step is to check that $\langle \psi_{u,v} \rangle$, $u, v \in M$ and $(uv)^{3^{j-1}} = 1$, is conjugate to $\langle \phi_{\epsilon,\epsilon^2} \rangle$. Let w be an element in M such that $ws = (uv)^{-1}$. Then the points $(w : uw^2 : 1)$, $(\epsilon w : \epsilon^2 uw^2 : 1)$, $(\epsilon^2 w : \epsilon uw^2 : 1)$ defined over $\mathbf{F}_{q^2}$ are the fixed points of $\psi_{u,v}$. None of these points lies on $\mathcal{H}$, and they are the vertices of a triangle. According to [27] and [18], $PGU(3, \mathbf{F}_{q^2})$ contains an element that takes this triangle to the fundamental triangle. Then the conjugate of $\psi_{u,v}$ under the same element belongs to $C_{3^j} \times C'_{3^j}$, and thus $\langle \psi_{u,v} \rangle = \langle \phi_{\epsilon,\epsilon^2} \rangle$ up to conjugacy. For $(uv)^{3^{j-1}} \neq 1$, it turns out instead that the fixed points $(w : uw^2 : 1)$, $(\epsilon w : \epsilon^2 uw^2 : 1)$, $(\epsilon^2 w : \epsilon uw^2 : 1)$ of $\psi_{u,v}$ are not defined over $\mathbf{F}_{q^2}$, because $w^3 = (uv)^{-1}$ yields w to be in a cubic extension of $\mathbf{F}_{q^2}$. As a consequence of [27] and [18], we have then that $\psi_{u,v}$ is conjugate to an element of order 3 in a Singer subgroup of order $(q^2 - q + 1)$ of $PGU(3, \mathbf{F}_{q^2})$. Hence the subgroups $\langle \psi_{u,v} \rangle$ with $u, v \in M$ but $(uv)^{3^{j-1}} \neq 1$, are pairwise conjugate under $PGU(3, \mathbf{F}_{q^2})$, and thus each of them is conjugate to $\langle T_3 \rangle$ as given in (V). Now, by $\tau_{u^{-1},v^{-1}} = \phi^2_{u,v}$, all the above assertions hold true when $\psi_{u,v}$ is replaced by $\tau_{u,v}$, and this completes the proof for $d = 3$. In the case $d > 3$, a Sylow d-subgroup R_d of $PGU(3, \mathbf{F}_{q^2})$ is $C_d \times C'_d$, with $C_d = \langle \phi_{\alpha,1} \rangle$ and $C'_d = \langle \phi_{1,\alpha} \rangle$. Thus each subgroup of order d of R_d is either $\langle \phi_{\alpha,1} \rangle$ or $\langle \phi_{\alpha,\alpha^{-1}} \rangle$, up to conjugacy.

(V) Let $d \geq 3$ and $(q^2 - q + 1) \equiv 0 \pmod{d}$. Then a Sylow d-subgroup is a subgroup of a Singer subgroup of $PGU(3, \mathbf{F}_{q^2})$, and hence it is conjugate to $C_d = \langle T_d \rangle$ as given in (V), see [3]. □

Now we are in a position to prove Theorem 2.1.

Proof of Theorem 2.1. For each of the subgroups $C_d = \langle T_d \rangle$ listed in Proposition 2.4(I)-(IV) we will determine a $\mathbf{F}_{q^2}$-plane model for the quotient curve $\mathcal{H}/C_d$, or equivalently the subfield $\Sigma' := \mathbf{F}_{q^2}(\mathcal{H}/C_d) = \mathbf{F}_{q^2}(x', y')$ of the Hermitian function field over $\mathbf{F}_{q^2}$ $\Sigma := \mathbf{F}_{q^2}(\mathcal{H}) = \mathbf{F}_{q^2}(x, y)$. For the case (V) we will determine $\Sigma' = \mathbb{F}_{q^3}(\mathcal{H}/C_d)$. Afterwards we compute the genus of Σ'.

(I) According to Proposition 2.4(I), we define Σ by $y^q + y - x^{q+1} = 0$. By considering $x' := x^2$ and $y' := y$ we have that Σ' is the fixed field of C_d and that $(y')^q + y' = (x')^{(q+1)/2}$. For the value of g see [34], Prop. VI.4.1.

(II) (1) By Proposition 2.4(II.1), Σ is assumed to be $y^q - y + \omega x^{q+1} = 0$, with $\omega^{q-1} = -1$. Setting $x' := x$ and $y' := y^p - y$, we have that $[\Sigma : \Sigma'] = p$ and that Σ' is the fixed field of C_d. Moreover,

$$\mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_p}(y') := \sum_{i=1}^{t} (y')^{q/p^i} = y^q - y\,, \qquad q = p^t\,.$$

Hence $\mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_p}(y') + \omega(x')^{q+1} = 0$. As the polynomial $Tr_{\mathbf{F}_q/\mathbf{F}_p}(Y) + \omega(x')^{q+1}$ is irreducible, we obtain the claimed plane model for Σ'. For the value on g one proceeds as in [34], Prop. VI.4.1.

(2) Here, by Proposition 2.4(II.2), Σ is defined as in (I) above. Setting $x' := x^p - x$ and $y' := y - x^2/2$, then Σ' is the fixed field of C_d. An easy computation shows that

$$(y')^q + y' = -(\mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_p}(x'))^2/2\,,$$

and hence we obtain an equation defining Σ'. For the value of g see [34], Prop. VI.4.1.

(III) By Proposition 2.4(III), we define Σ by $xy^q - x^q y + \omega = 0$ with $\omega^{q-1} = -1$. Let $x' := x^d$, $y' := xy$ and

$$f(X,Y) := Y^q - YX^{2(q-1)/d} + \omega X^{(q-1)/d}\,.$$

Then $f(x',y') = 0$, and we claim that $f(X,Y)$ is irreducible in $\bar{\mathbf{F}}_q[X,Y]$. To prove the claim, assume on the contrary that $f(X,Y) = \prod_i f_i(X,Y)$, where $f_i(X,Y)$ are irreducible in $\bar{\mathbf{F}}_q[X,Y]$. From $\prod_i f_i(X^d, XY) = X^{q+1}(X^{q+1} + Y^{q+1} + 1)$ follows that one of the factors on the left hand, say $f_1(X^d, XY)$ is of type X^t, $(0 \le t \le q+1)$. Then $f_1(X,Y) = X^{t/d}$, and $t \equiv 0 \pmod d$. But $f(X,Y)$ has no factor of type X^k $(k > 1)$, and the claim is proved. Next we show that Σ' is the fixed field of C_d. Clearly, $\Sigma' \subseteq \mathrm{Fix}_{C_d}(\Sigma)$. Note that $\mathrm{ord}(C_d) = d$ yields $[\Sigma : \Sigma'] \le d$. In fact, each element of Σ turns out to be a linear combination of $1, x, \ldots, x^{d-1}$ over Σ'. To prove the latter claim, choose an element $h(x,y) \in \Sigma$. Then $h(x,y) = a_0(x) + \cdots + a_i(x)y^i + \cdots + a_n(x)y^n$, $a_i(x) \in \mathbf{F}_{q^2}(x)$. Clearly, $h(x,y) = b_0(x) + \cdots + b_i(x)y'^i + \cdots + b_n(x)y'^n$, where $b_i(x) = a_i(x)x^{-i}$. Thus $h(x,y) = b_0(x) + \cdots + b_i(x)y'^i + \cdots + b_b(x)y'^n$. It remains to show that $b_i(x)$ is a linear combination of $1, x, \ldots, x^{d-1}$ over Σ'. For $b_i(x) \in \mathbf{F}_{q^2}[x]$, then $b_i(x) = b_0 + \ldots b_i x^i + \cdots + b_s x^s$. Replacing $x' = x^{dj+k}$, $(0 \le k < d)$ by $x^k x'^j$, we see that $b_i(x)$ is a linear combination of $1, x, \ldots, x^{d-1}$ over Σ'. Finally, let $a(x) = a_0 + \cdots + a_{d-1}x^{d-1}$, $b(x) = b_0 + \ldots b_{d-1}x^{d-1}$, $a_i, b_i \in \Sigma'$. Then there exists $c(x) = c_0 + \cdots + c_{d-1}x^{d-1}$, $c_i \in \Sigma'/\mathbf{F}_{q^2}$ such that $a(x)/b(x) = c(x)$, and this completes the proof. Since T_d has two fixed points on $\mathcal{H}$, namely $(1:0:0)$ and $(0:1:0)$, from the Riemann-Hurwitz formula applied to $\mathcal{H} \to \mathcal{H}/C_d$, the genus is equal to $(q^2-q)/2d$.

Remark 2.5. Concerning the above Item (III), the referee pointed out a shorter proof of the absolute irreducibility which uses the polynomial $g(Y,Z) = y^q z - yz^q + \omega = 0$ with $\omega^{q-1} = -1$ instead of $f(X,Y)$. We sketch here the proof.

Let T_d be the automorphism of order d given in Proposition 2.4 (III); i.e., $T_d : (X,Y,Z) \mapsto (X, \alpha Y, \alpha^{-1}Z)$. We then have

$$\begin{array}{ccc}
\mathcal{H}' = \mathbf{F}_{q^2}(z',y') & \subseteq & \mathbf{F}_{q^2}(z,y) = \mathcal{H} \\
\cup\mid & & \cup\mid \quad \longleftarrow \boxed{\text{degree } q} \\
\mathbf{F}_{q^2}(z^d) & \subseteq & \mathbf{F}_{q^2}(z) \\
 & \uparrow & \\
 & \boxed{\text{degree } d} &
\end{array}$$

It can easily be seen that the extensions

$$\mathbf{F}_{q^2}(z^d) \subseteq \mathbf{F}_{q^2}(z) \subseteq \mathbf{F}_{q^2}(z,y)$$

are absolutely irreducible (i.e., the relative degrees of the fields involved do not change if one extends the base field from $\mathbf{F}_{q^2}$ to its algebraic closure). Also easily seen are:

$$\mathbf{F}_{q^2}(z',y') \subseteq \mathcal{H}^{\langle T_d \rangle} \quad \text{and} \quad \mathcal{H}'(z) = \mathcal{H}\,.$$

From this one concludes that $\mathbf{F}_{q^2}(z', y') = \mathcal{H}^{\langle T_d \rangle}$ and

$$[\mathbf{F}_{q^2}(z', y') : \mathbf{F}_{q^2}(z')] = q;$$

and, moreover, this degree does not change by going to the algebraic closure of $\mathbf{F}_{q^2}$. This means that the polynomial $g(Y, Z)$ is indeed absolutely irreducible.

(IV) Here Σ is defined by $x^{q+1} + y^{q+1} + 1 = 0$.

(1) Let $x' := x^d$ and $y' = y$. Then $[\Sigma : \Sigma'] = d$ and Σ' is the fixed field of C_d. There are exactly $q + 1$ totally ramified points in $\mathcal{H} \to \mathcal{H}/C_d$, namely $(0 : \eta : 1)$, with $\eta^{q+1} = -1$, and we obtain the claimed value for g.

(2) Let $x' = x^d$, $y' = xy$, and

$$f(X, Y) := X^{(q+1)/d} + X^{2(q+1)/d} + Y^{q+1}\,.$$

Then $f(x', y') = 0$, and we see that $f(X, Y)$ is $\bar{\mathbf{F}}_q$-irreducible arguing as in the proof of (III). Since T_d has no fixed point on $\mathcal{H}$, the Riemann-Hurwitz formula applied to $\mathcal{H} \to \mathcal{H}/C_d$ gives $g = (q^2 - q + 2d - 2)/2d$.

(V) By Remark 2.2 Σ can be defined over $\mathbb{F}_{q^3}$ by $xy^q + y + x^q = 0$.

Claim. *The following*

$$f(X, Y) := s(X^{q/d}, Y^{1/d}, X^{1/d}Y^{q/d})$$

belongs to $\mathbf{F}_q[X, Y]$ *and it is absolutely irreducible.*

Proof of the Claim. We only need to show that $d \,|\, i$ and $d \,|\, j$ for each term $c_{i,j}X_1^i X_2^{j-i} X_3^{d-j}$ in $s(X_1, X_2, X_3)$. Clearly, $s(\gamma X_1, \gamma^q X_2, X_3) = s(X_1, X_2, X_3)$ for each $\gamma^d = 1$, and $s(X_1, X_2, X_3) = s(X_2, X_3, X_1) = s(X_3, X_1, X_2)$. Polynomials satisfying both of the above properties have been investigated in [3]. In our case, $s(X_1, X_2, X_3)$ contains X_2^d. Thus [3], Lemma 6, yields $d - j \equiv (q^2 + 1)(-i) \pmod{d}$, whence $j \equiv qi \pmod{d}$ follows by $(q^2 - q + 1) \equiv 0 \pmod{d}$. Equivalently, there are integers u_{ij} and v_{ij} such that $qi - j = du_{ij}$ and $(q - 1)j + i = dv_{ij}$. Then

$$s(X^{q/d}, Y^{1/d}, X^{1/d}Y^{q/d}) = \sum c_{i,j} X^{qi+d-j} Y^{j-i+q(d-j)}\,,$$

and it follows that $f(X, Y) \in \mathbf{F}_{q^2}[X, Y]$. To show that it is absolutely irreducible, let $x' := x^d$, $y' := y^d$. Then

$$(*) \qquad f(x', y') = \prod_{\beta^d = 1} (\beta x^q + \beta^q y + xy^q) = (xy^q + y + x^q) \prod_{\beta^d = 1, \beta \neq 1} (\beta x^q + \beta^q y + xy^q)\,,$$

Since the product on the right side has d irreducible factors, the absolutely irreducibility of $f(X, Y)$ can be proved by arguing as in case (III). This completes the proof of the claim.

Now $(*)$ implies $f(x', y') = 0$ and then, $\Sigma' = \mathbb{F}_{q^3}(x', y')$ is the fixed of C_d over $\mathbb{F}_{q^3}$. To compute the genus, as T_d has exactly three fixed points which are the only (totally) ramified points, we use the Riemann-Hurwitz formula.

Remark 2.6. It seems plausible that one can prove the assertion that the polynomial $f(X, Y)$ written in the above claim, is absolutely irreducible using arguments to the ones in Remark 2.5.

3. The genus of maximal curves arising from tame subgroups of $SL(2, \mathbf{F}_q)$

We have already noticed that the group of automorphism $\mathrm{Aut}(\mathcal{H})$ of the Hermitian curve $\mathcal{H}$ is isomorphic to $PGU(3, \mathbf{F}_{q^2})$. From the classification of subgroups of $PSU(3, \mathbf{F}_{q^2})$ given in [27], [18] and [21] it follows that $\mathrm{Aut}(\mathcal{H})$ contains a subgroup Γ isomorphic to $SL(2, \mathbf{F}_q)$; moreover, any two such subgroups are conjugate in $\mathrm{Aut}(\mathcal{H})$. Geometrically, Γ is contained in the subgroup of $\mathrm{Aut}(\mathcal{H})$ that preserves a non-incident point-line pair (P_0, ℓ), where $P_0 \in \mathbf{P}^2(\mathbf{F}_{q^2}) \setminus \mathcal{H}$ and ℓ is its polar line with respect to the unitary polarity associated with $\mathcal{H}$. In particular, ℓ is a $\mathbf{F}_{q^2}$-rational line meeting $\mathcal{H}$ in $(q+1)$ pairwise distinct $\mathbf{F}_{q^2}$-rational points.

In this section our aim is to compute the genus of the quotient curve of $\mathcal{H}$ arising from each tame subgroup of Γ, see Proposition 3.3. Recall that an automorphism group is called tame if its order is prime to the characteristic of the base field. For this purpose, we need at first to give a suitable description of the action of subgroups of Γ on $\mathcal{H}$. We will use the plane model (M3) in §2.

We define the above point-line pair (P_0, ℓ) by choosing $P_0 = (0 : 0 : 1)$ and ℓ as the line at infinity: $Z = 0$. Then the subgroup of automorphisms of $\mathbf{P}^2(\bar{\mathbf{F}}_{q^2})$ preserving both (P_0, ℓ) and $\mathcal{H}$, consists of maps of type

$$(X, Y, Z) \to (aX + bY, cX + dY, Z)\,, \tag{3.1}$$

where

$$ac^q - a^q c = 0, \quad bd^q - b^q d = 0, \quad bc^q - a^q d = -1, \quad \text{and} \quad ad^q - b^q c = 1\,.$$

Those maps with $a, b, c, d \in \mathbf{F}_q$ and $ad - bc = 1$, form a subgroup isomorphic to $SL(2, \mathbf{F}_q)$. We choose this subgroup to represent Γ.

Let G be a subgroup of Γ. The following lemma shows that the action of G on the affine points of $\mathcal{H}$ is semi-regular, i.e. each point-orbit of affine points of $\mathcal{H}$ under G has length equal to the order of G.

Lemma 3.1. *Let $\tau \in \Gamma$ and $P \in \mathcal{H}$ an affine point such that $\tau(P) = P$. Then τ is the identity map.*

Proof. It follows from (3.1) and the fact that $\alpha^q = \alpha$ for each $\alpha \in \mathbf{F}_q$. □

From now on we assume that G is tame and investigate the action of G on the set $\mathcal{I} := \ell \cap \mathcal{H}$, consisting of all points $(1 : m : 0), m \in \mathbf{F}_q$, together with $(0 : 1 : 0)$. Since Γ acts on $\mathcal{I}$ as $PSL(2, \mathbf{F}_q)$ in its natural 2-transitive permutation representation on $\mathbf{P}^1(\mathbf{F}_q)$, we have actually to consider $\bar{G}$ instead of G, where $\bar{G}$ is the image of G under the canonical epimorphism

$$\phi : \Gamma \cong SL(2, \mathbf{F}_q) \to PSL(2, \mathbf{F}_q)\,.$$

Note that the kernel of ϕ is trivial for $p = 2$, otherwise it is the subgroup of order 2 generated by the automorphism

$$(X, Y, Z) \mapsto (-X, -Y, Z)\,.$$

Hence either $\mathrm{ord}(G) = 2\mathrm{ord}(\bar{G})$ or $\mathrm{ord}(G) = \mathrm{ord}(\bar{G})$, and in the later case $\mathrm{ord}(\bar{G})$ must be odd.

According to the classification of subgroups of $PSL(2,\mathbf{F}_q)$ [22], Hauptsatz 8.27, the tame subgroup $\bar{G}$ is one of the following groups:

(3.1) Cyclic of order d, where $d \mid (q+1)$ for $p=2$, or $d \mid (q+1)/2$ for $p \geq 3$;
(3.2) Dihedral of order $2d$, where $d \mid (q+1)/2$ for $p \geq 3$;
(3.3) Cyclic of order d where $d \mid (q-1)$ for $p=2$, or where $d \mid (q-1)/2$ id $p \geq 3$;
(3.4) Dihedral of order $2d$, where $d \mid (q-1)/2$ for $p \geq 3$;
(3.5) The group Sym_4 for $q^2 \equiv 1 \pmod{16}$, $\quad p \geq 5$;
(3.6) The group Alt_4 $\quad$ for $p \geq 5$;
(3.7) The group Alt_5 for $q^2 \equiv 1 \pmod{5}$, $\quad p \geq 7$.

We will use the symbols C_ℓ, D_ℓ to denote the cyclic group of order ℓ and the dihedral group of order 2ℓ, respectively. The possibilities for the action of $\bar{G}$ on $\mathcal{I}$ are listed in cases (3.1)-(3.7) below.

Case 3.1. Here $\bar{G}$ has $(q+1)/d$ orbits each of them having length d.

Case 3.2. If $q \equiv 3 \pmod 4$, then no involution fixes a point, and each orbit has length $2d$. If $q \equiv 1 \pmod 4$, then every involution has two fixed points. Hence just two orbits have length d and the remaining $(q+1)/2d-1$ orbits have length $2d$.

Case 3.3. Here $\bar{G}$ has two fixed points and the remaining $(q-1)/d$ orbits have length d.

Case 3.4. Here $\bar{G}$ has an orbit of length 2. If $q \equiv 3 \pmod 4$, then the remaining $(q-1)/2d$ orbits have length $2d$. If $q \equiv 1 \pmod 4$, then just 2 orbits have length d and the remaining $(q-1)/2d-1$ orbits have length $2d$.

Case 3.5. For $P \in \mathbf{P}^1(\mathbf{F}_q)$, let S be the stabilizer of P under Sym_4. We show first that S is either trivial, or isomorphic to any of the following cyclic groups: C_2, C_3, or C_4. If $S \ncong C_3$, then S contains an involution τ that fixes a point $Q \neq P$. Since $PSL(2,\mathbf{F}_q)$ is 2-transitive on $\mathbf{P}^1(\mathbf{F}_q)$, we may assume that P is the infinite point and Q is the origin. Then τ is given by the permutation $X' = -X, Y' = y, Z' = Z$, so τ is uniquely determined. This yields that S cannot be isomorphic to Alt_4, D_4 or D_2. From the classification of subgroups of Sym_4, it remains to show that S is not isomorphic to Sym_3. Let $\eta \in S$ be an element of order 3; then η is given by $X' = cX + d, Y' = Y, Z' = Z$, with $c, d \in \mathbf{F}_q$ and $c^3 = 1$. Then $c\eta c$ is the permutation $cX - d$ which is different from $c^{-1}X - c^{-1}d$. On the other hand, the latter permutation is η^{-1}. Hence $c\eta c \neq \eta^{-1}$, and this shows that $S \ncong Sym_3$.

Let $S \cong C_4$. Then $q \equiv 1 \pmod 4$ and S is generated by $X' = cX, Y' = Y, Z' = Z$, with $c^4 = 1$. Since Sym_4 contains exactly three elements of order 4, $\bar{G}$ has just one orbit of length 6.

Let $S \cong C_3$. Then $q \equiv 1 \pmod 3$ and S can be assumed to be generated by $X' = cX, Y' = Y, Z' = Z$, with $c^3 = 1$. Since Sym_4 contains exactly four subgroups of order 3, it turns out that $\bar{G}$ has exactly one orbit of length 8.

Let $S \cong C_2$. Then S can be assumed to be generated by the involution τ given by $X' = -X, Y' = Y, Z' = Z$. Note that $\tau \in PSL(2,\mathbf{F}_q)$ implies $q \equiv 1 \pmod 4$. Clearly, the orbit of P under $\bar{G}$ has length 12. In particular, the conjugacy class of τ has size 6. Hence τ is a non-central involution and $\bar{G}$ has only one orbit of length 12.

The above discussion proves the following results:

(I) For $q \equiv 1 \pmod 4$ and $q \equiv 1 \pmod 3$, $\bar{G}$ has one orbit of length 6, one orbit of length 8, one orbit of length 12 and each other orbit has length 24.

(II) For $q \equiv 1 \pmod 4$ and $q \equiv 2 \pmod 3$, $\bar{G}$ has one orbit of length 6, one orbit of length 12 and each other orbit has length 24.

(III) For $q \equiv 3 \pmod 4$ and $q \equiv 1 \pmod 3$, $\bar{G}$ has one orbit of length 8, and each other orbit has length 24.

(IV) For $q \equiv 3 \pmod 4$ and $q \equiv 2 \pmod 3$, each orbit under $\bar{G}$ has length 24.

Case 3.6. A repetition of the arguments used above shows that the following cases occur:

(I) For $q \equiv 1 \pmod 4$ and $q \equiv 1 \pmod 3$, $\bar{G}$ has two orbits of length 4, one orbit of length 6 and each other orbit has length 12.

(II) For $q \equiv 1 \pmod 4$ and $q \equiv 2 \pmod 3$, $\bar{G}$ has one orbit of length 6 and each other orbit has length 12.

(III) For $q \equiv 3 \pmod 4$ and $q \equiv 1 \pmod 3$, $\bar{G}$ has two orbits of length 4 and each other orbit has length 12.

(IV) For $q \equiv 3 \pmod 4$ and $q \equiv 2 \pmod{43}$, each orbit under $\bar{G}$ has length 12.

Case 3.7. Similar arguments can be used to prove the following.

(I) For $q \equiv 1 \pmod 5, q \equiv 1 \pmod 4$, and $q \equiv 1 \pmod 3$, $\bar{G}$ has one orbit of length 12, one orbit of length 20, one orbit of length 30 and the remaining orbits have length 60.

(II) For $q \equiv 1 \pmod 5, q \equiv 1 \pmod 4$, and $q \equiv 2 \pmod 3$, $\bar{G}$ has one orbit of length 12, one orbit of length 30 and the remaining orbits have length 60.

(III) For $q \equiv 1 \pmod 5, q \equiv 3 \pmod 4$, and $q \equiv 1 \pmod 3$, $\bar{G}$ has one orbit of length 12, one orbit of length 30 and the remaining orbits have length 60.

(IV) For $q \equiv 1 \pmod 5, q \equiv 3 \pmod 4$, and $q \equiv 2 \pmod 3$, $\bar{G}$ has one orbit of length 12, and the remaining orbits have length 60.

(V) For $q \equiv 4 \pmod 5, q \equiv 1 \pmod 4$, and $q \equiv 1 \pmod 3$, $\bar{G}$ has one orbit of length 20, one orbit of length 30 and the remaining orbits have length 60.

(VI) For $q \equiv 4 \pmod 5, q \equiv 1 \pmod 4$, and $q \equiv 2 \pmod 3$, $\bar{G}$ has one orbit of length 30 and the remaining orbits have length 60.

(VII) For $q \equiv 4 \pmod 5, q \equiv 3 \pmod 4$, and $q \equiv 1 \pmod 3$, $\bar{G}$ has one orbit of length 20, and the remaining orbits have length 60.

(VIII) For $q \equiv 4 \pmod 5, q \equiv 3 \pmod 4$, and $q \equiv 2 \pmod 3$, each orbit under $\bar{G}$ has length 60.

Now, the previous case by case analysis of the possible actions of $\bar{G}$ together with the Riemann-Hurwitz formula (see Lemma 3.2) allows us to compute the genus of the quotient curves associated to G, provided that G is tame. We stress that such curves are $\mathbf{F}_{q^2}$-maximal.

To state Lemma 3.2 let $\mathcal{X}$ denote a curve of genus g and H a subgroup of $\mathrm{Aut}(\mathcal{X})$. Let g' be the genus of the quotient curve $\mathcal{X}/H$ and suppose that the natural morphism $\pi : \mathcal{X} \to \mathcal{X}/H$ is

separable. Then the Riemann-Hurwitz formula applied to π states

$$2g-2 = n(2g'-2)+\delta\,,$$

where n is the order of H and δ is the degree of the ramification divisor D associated to π. For $P \in \mathcal{X}$ let

$$n_P := \#\{\tau \in H : \tau(P) = P\}\,.$$

Note that $\#\pi^{-1}(\pi(P)) = n/n_P$ and that $n_Q = n_P$ for each $Q \in \pi^{-1}(\pi(P))$. Now assume that H is tame, so that p does not divide n_P for each $P \in \mathcal{X}$, and the multiplicity of D at P is $(n_P - 1)$. As a matter of terminology, the orbit of P is said to be *small* if it consists of less than n elements.

Lemma 3.2. *If G is a tame subgroup of* $\mathrm{Aut}(\mathcal{X})$ *and* $\mathrm{ord}(G) = n$ *, then*

$$2g-2 = n(2g'-2)+\sum_{i=1}^{s}(n-\ell_i)\,,$$

where $\ell_1, \ldots, \ell_s$ are the lengths of the small orbits of G on $\mathcal{X}$.

We notice that the above computation generalizes Guerrero's approach [5], V.2.5, and it can be deduced from the proof of [5], V.1.3.

Proposition 3.3. *Let G denote a tame subgroup of $\Gamma \cong SL(2,\mathbf{F}_q)$, g the genus of the quotient curve $\mathcal{H}/G$. Then we obtain the following values for g, where $\bar{G}$ denotes the image of G under the canonical epimorphism $SL(2,\mathbf{F}_q) \to PSL(2,\mathbf{F}_q)$.*

1. *If $\bar{G} \cong C_d$, then*
$$g = \begin{cases} \frac{(q+1)(q-2)}{2d}+1 & \text{if } d \text{ is odd; } d \mid (q+1) \text{ for } p=2, \text{ or} \\ & d \mid (q+1)/2 \text{ for } p \geq 3\,, \\ \frac{(q+1)(q-3)}{4d}+1 & \text{if } d \mid (q+1)/2 \text{ and } p \geq 3\,. \end{cases}$$
2. *If $\bar{G} \cong D_d$, with $d \mid (q+1)/2$ and $p \geq 3$, then*
$$g = \begin{cases} \frac{(q+1)(q-3)}{8d}+1 & \text{for } q \equiv 3 \pmod 4\,, \\ \frac{(q+1)(q-3)+4d}{8d} & \text{for } q \equiv 1 \pmod 4\,. \end{cases}$$
3. *If $\bar{G} \cong C_d$, then*
$$g = \begin{cases} \frac{q(q-1)}{2d} & \text{if } d \text{ is odd; } d \mid (q-1) \text{ for } p=2, \text{ or} \\ & d \mid (q-1)/2 \text{ for } p \geq 3\,, \\ \frac{(q-1)^2}{4d} & \text{if } d \mid (q-1)/2 \text{ and } p \geq 3\,. \end{cases}$$
4. *If $\bar{G} \cong D_d$, with $d \mid (q-1)/2$ and $p \geq 3$, then*
$$g = \begin{cases} \frac{(q-1)^2+4d}{8d} & \text{for } q \equiv 3 \pmod 4\,, \\ \frac{(q-1)^2}{8d} & \text{for } q \equiv 1 \pmod 4\,. \end{cases}$$
5. *If $\bar{G} \cong Sym_4$, $q^2 \equiv 1 \pmod{16}$, $p \geq 5$, then*
$$g = \begin{cases} (q-1)^2/96 & \text{for } q \equiv 1 \pmod{24}\,, \\ (q^2-2q+33)/96 & \text{for } q \equiv -7 \pmod{24}\,, \\ (q^2-2q+61)/96 & \text{for } q \equiv 7 \pmod{24}\,, \\ (q^2-2q+93)/96 & \text{for } q \equiv -1 \pmod{24}. \end{cases}$$

6. *If* $\bar{G} \cong Alt_4$, $p \geq 5$, *then*

$$g = \begin{cases} (q-1)^2/48 & \text{for } q \equiv 1 \pmod{12}, \\ (q^2-2q+33)/48 & \text{for } q \equiv 5 \pmod{12}, \\ (q^2-2q+13)/48 & \text{for } q \equiv -5 \pmod{12}, \\ (q^2-2q+45)/48 & \text{for } q \equiv -1 \pmod{12}. \end{cases}$$

7. *If* $\bar{G} \cong Alt_5$ *and* $q^2 \equiv 1 \pmod 5$, $p \geq 7$, *then*

$$g = \begin{cases} (q-1)^2/240 & \text{for } q \equiv 1 \pmod{60}, \\ (q^2-2q+81)/240 & \text{for } q \equiv 41 \pmod{60}, \\ (q^2-2q+61)/240 & \text{for } q \equiv 31 \pmod{60}, \\ (q^2-2q+141)/240 & \text{for } q \equiv 11 \pmod{60}, \\ (q^2-2q+97)/240 & \text{for } q \equiv 49 \pmod{60}, \\ (q^2-2q+177)/240 & \text{for } q \equiv 29 \pmod{60}, \\ (q^2-2q+157)/240 & \text{for } q \equiv 19 \pmod{60}, \\ (q^2-2q+237)/240 & \text{for } q \equiv 59 \pmod{60}. \end{cases}$$

Remark 3.4. Comparison with results in [11] shows that the only overlapping concerns Proposition 3.3(1)(4). More precisely, case 1 and [11], Example 5.10, as well as case 4 and [11], Example 5.6, coincide. Furthermore, note that $SL(2, \mathbf{F}_q)$ is a subgroup of the group $\mathcal{F}$ introduced in [11], p.27; actually $\mathcal{F}$ is the central product of $SL(2, \mathbf{F}_q)$ with a cyclic group of order $(q+1)$. The results in the present section give an almost complete answer to the question posed in loc. cit.

4. The genus of maximal curves arising from weakly tame subgroups of the normaliser of a Singer subgroup in $PSU(3, \mathbf{F}_{q^2})$

The automorphism group $\mathrm{Aut}(\mathcal{H})$ of the Hermitian curve $\mathcal{H}$ contains cyclic groups of order (q^2-q+1); any two such groups are conjugate in $\mathrm{Aut}(\mathcal{H})$, [27], [18], [21]. These groups and their subgroups are the so-called *Singer subgroups* of $\mathrm{Aut}(\mathcal{H})$. Moreover, the normaliser $N = N(\Delta)$ of a Singer subgroup Δ of order (q^2-q+1) is a group of order $3(q^2-q+1)$ which is actually the semidirect product of Δ with a subgroup C_3 of order 3. Let $\mathcal{H}$ be given by (M4) (cf. §2). According to [3], §3, Δ can be chosen as the subgroup generated by

$$h : (X, Y, Z) \to (\alpha X, \alpha^q Y, Z)$$

with $\alpha \in \mathbf{F}_{q^6}$ a primitive (q^2-q+1)-th root of unity, while C_3 is generated by $(X, Y, Z) \to (Y, Z, X)$. By [31], Ch. 4, the subgroups of N up to conjugacy in N are as follows, where for $i = 0, 1, 2$, we let h_i denote the automorphism

$$(X, Y, Z) \to (\epsilon^i Y, \epsilon^{2i} Z, X)$$

of $\mathcal{H}$, ϵ being a primitive third root of unity.

Lemma 4.1. (I) *For every divisor* n *of* (q^2-q+1), *the cyclic subgroup* C_n *of order* n, *with* $C_n = \langle h^{(q^2-q+1)/n} \rangle$;

(II) *(1) Let* $q \equiv 2 \pmod 3$ *and* $n \equiv 0 \pmod 3$, *or* $q \equiv 1 \pmod 3$. *For every divisor* n *of* (q^2-q+1), *the subgroup of order* $3n$ *which is the semidirect product of* $C_n = \langle h^{(q^2-q+1)/n} \rangle$ *with* $\langle h_0 \rangle$.

(2) Let $q \equiv 2 \pmod 3$ and $n \not\equiv 0 \pmod 3$. For every divisor n of (q^2-q+1), the subgroup G_i $(i=0,1,2)$ of order $3n$ which is the semidirect product of $C_n = \langle h^{(q^2-q+1)/n} \rangle$ with $\langle h_i \rangle$.

The genera of the quotient curves arising from the above subgroups of $\mathrm{Aut}(\mathcal{H})$ are given in the following

Proposition 4.2. *Let $n \geq 3$ be an integer satisfying $(q^2-q+1) \equiv 0 \pmod n$. The genus of the quotient curve of the Hermitian curve over $\mathbf{F}_{q^2}$ arising from a tame subgroup in the normaliser of the Singer subgroup of $\mathrm{Aut}(\mathcal{H})$ is equal to either*

1. $g = ((q^2-q+1)/n - 1)/2$, *or*
2. $g = (q^2-q+1-n)/6n$ *for* $q \equiv 2 \pmod 3$ *and* $n \equiv 0 \pmod 3$ *or* $q \equiv 1 \pmod 3$, *or*
3. $g = (q^2-q+1-3n)/6n$ *for* $q \equiv 2 \pmod 3$ *and* $n \not\equiv 0 \pmod 3$.

Proof. In order to apply the Riemann-Hurwitz formula as stated in Lemma 3.2, we take a subgroup G from the list in Lemma 4.1, and determine its small orbits on $\mathcal{H}$. As (I) was investigated in previous work, see remark below, we limit ourselves to case (II). Then G has a short orbit $\mathcal{O}$ of length 3 consisting of the fixed points of h which are $(1:0:0)$, $(0:1:0)$ and $(0:0:1)$. For $q \equiv 1 \pmod 3$, h_0 has two fixed points $E_1 = (\epsilon : \epsilon^2 : 1)$ and $E_2 = (\epsilon^2 : \epsilon : 1)$ on $\mathcal{H}$. If they belonged to the same orbit under G, then C_n would contain an element that sends E_1 to E_2, and hence $\epsilon^n = 1$ would follow. On the other hand, $q^2-q+1 \equiv 0 \pmod 3$ together with $q \equiv 1 \pmod 3$ implies $n \not\equiv 0 \pmod 3$. This contradiction shows that G has a further two orbits, $\mathcal{O}' := \{(\beta\epsilon : \beta^q\epsilon^2 : 1) \mid \beta^n = 1\}$, and $\mathcal{O}'' = \{(\beta\epsilon^2 : \beta^q\epsilon : 1) \mid \beta^n = 1\}$. Now, from Lemma 3.2, $q^2-q-2 = 3n(2g-2) + 3n - 3 + 2(3n-n)$, and thus $g = (q^2-q-n+1)/6n$. For $q \equiv 2 \pmod 3$, the picture is richer. Let $n \equiv 0 \pmod 3$. Then G contains the linear transformation $(X,Y,Z) \to (\epsilon X, \epsilon^2 Y, Z)$, and therefore h_i, $(0 \leq i \leq 2)$, as defined in Lemma 4.1, belongs to G. A straightforward computation shows that each of these automorphisms has three fixed points, namely

$$\begin{aligned}
\mathrm{Fix}(h_0) &= \{(\epsilon : \epsilon^2 : 1), (1 : \epsilon : \epsilon^2), (\epsilon^2 : 1 : \epsilon)\}\,; \\
\mathrm{Fix}(h_1) &= \{(1 : \epsilon^2 : 1), (1 : 1 : \epsilon^2), (\epsilon^2 : 1 : 1)\}\,; \\
\mathrm{Fix}(h_2) &= \{(1 : \epsilon : 1), (1 : 1 : \epsilon), (\epsilon : 1 : 1)\}\,.
\end{aligned}$$

Note that $\mathrm{Fix}(h_0)$ is disjoint from $\mathcal{H}$, while both $\mathrm{Fix}(h_1)$ and $\mathrm{Fix}(h_2)$ lie on $\mathcal{H}$. Also, h_0 induces a 3-cycle on both $\mathrm{Fix}(h_1)$ and $\mathrm{Fix}(h_2)$. It turns out that G has two more short orbits, both of length n. As before, this gives $g = (q^2-q-n+1)/6n$. Finally, let $n \not\equiv 0 \pmod 3$. As $\mathrm{Fix}(h_0)$ is disjoint from $\mathcal{H}$, G_0 has just one short orbit, namely $\mathcal{O}$. Thus, Lemma 3.2 gives $g = (q^2-q+3n+1)/6n$. It remains to consider G_1 and G_2. Note that h_i $(0 \leq i \leq 2)$ does not belong to G_j for $i \neq j$. This shows that G_i, $(i = 1, 2)$ has exactly four short orbits, namely $\mathcal{O}$, $\mathcal{O}_i := \{(\beta\epsilon^{2i} : \beta^q, 1) : \beta^n = 1\}$, $\mathcal{O}_i' := \{(\beta : \beta^q\epsilon^{2i} : 1) : \beta^n = 1\}$, $\mathcal{O}_i'' = \{(\beta : \beta^q : \epsilon^{2i}) : \beta^n = 1\}$. From Lemma 3.2, $q^2-q-2 = 3n(2g-2)+3n-3+3(3n-n)$, and hence $g = (q^2-q-3n+1)/6n$. □

Remark 4.3. Proposition 4.2(1) has been previously stated in [4] and independently in [11], Thm. 5.1. Instead, Proposition 4.2(2)(3) provide new genera for $\mathbf{F}_{q^2}$-maximal curves.

5. On the third largest genus

The genus g of a $\mathbf{F}_{q^2}$-maximal curve $\mathcal{X}$ satisfies [23], [35], [8]

$$g \le g_2 := \lfloor \tfrac{(q-1)^2}{4} \rfloor \qquad \text{or} \qquad g = g_1 := q(q-1)/2\,.$$

As remarked in §1, the Hermitian curve $\mathcal{H}$ is the only $\mathbf{F}_{q^2}$-maximal curve (up to $\mathbf{F}_{q^2}$-isomorphism) with genus g_1 and hence $\mathcal{H}$ is the only maximal curve having genus as large as possible [29]. The curves defined by the non-singular models of the following plane curves

$$y^q + y = x^{(q+1)/2} \qquad q \text{ odd}\,, \qquad \text{and} \qquad \sum_{i=1}^{t} y^{q/2^i} = x^{q+1} \qquad q = 2^t\,,$$

have genus $(q-1)^2/4$ and $q(q-2)/4$, respectively. This shows that g_2 is the second largest genus for $\mathbf{F}_{q^2}$-maximal curves. For q odd, the above curve is the only $\mathbf{F}_{q^2}$-maximal curve (up to $\mathbf{F}_{q^2}$-isomorphism) of genus $(q-1)^2/4$ [7]. It seems plausible that uniqueness also holds true for q even but it has been so far proved under the additional Condition $(*)$ below (see [1]). Next we look for the third largest genus g_3 that $\mathcal{X}$ can have. Since the non-singular model of the curve

$$y^q + y = x^{(q+1)/3}\,, \qquad q \equiv 2 \pmod 3\,,$$

has genus $(q-1)(q-2)/6$, it is reasonable to search g_3 in the interval

$$\rceil \lceil \tfrac{(q-1)(q-2)}{6} \rceil, \lfloor \tfrac{(q-1)^2}{4} \rfloor \lceil\,. \tag{5.1}$$

In fact, according to [9], Prop. 2.5, for q odd we have

$$g_3 \le (q-1)(q-2)/4\,.$$

Since $\mathcal{X}$ is equipped with an $\mathbf{F}_{q^2}$-intrinsic linear series $\mathcal{D}_{\mathcal{X}}$ [7], §1, the approach due to Stöhr and Voloch [36] can be applied to investigate $\mathcal{D}_{\mathcal{X}}$. We have $\dim(\mathcal{D}_{\mathcal{X}}) \ge 2$, equality holding iff $\mathcal{X}$ is $\mathbf{F}_{q^2}$-isomorphic to the Hermitian curve [9], Thm. 2.4. Now if the genus belongs to (5.1), then $\dim(\mathcal{D}_{\mathcal{X}}) = 3$ [4], Lemma 3.1. So we look for g_3 among $\mathbf{F}_{q^2}$-maximal curves $\mathcal{X}$ such that $\dim(\mathcal{D}_{\mathcal{X}}) = 3$. In this case, the first three positive Weierstrass non-gaps at $P \in \mathcal{X}$ satisfy [7], Prop. 1.5(i),

$$m_1(P) < m_2(P) \le q < m_3(P)\,. \tag{5.2}$$

For $P \in \mathcal{X}(\mathbf{F}_{q^2})$, we have $m_2(P) = q$ and $m_1(P) \ge q/2$ by $2m_1(P) \ge m_2(P)$. At this point, we invoke Fuhrmann computations [6], Anhang §2, concerning the genus of certain semigroups of type $\langle m, q, q+1\rangle$. Notice that Fuhrmann's results were summarized in [4], Lemma 3.4. It follows that g (the genus of $\mathcal{X}$) satisfies

$$g \le \lfloor \tfrac{q^2-q+4}{6} \rfloor\,, \tag{5.3}$$

provided that

$$m_1(P) \notin \{\lfloor \tfrac{q+1}{2} \rfloor, q-1\}\,, \qquad P \in \mathcal{X}(\mathbf{F}_{q^2})\,. \tag{5.4}$$

This leads to investigate some consequences of the following implication

$$(*) \qquad \forall P \in \mathcal{X}(\mathbf{F}_{q^2}), \quad m_1(P) = q-1 \qquad \Rightarrow \qquad g < \lfloor \frac{q^2-q+4}{6} \rfloor\,.$$

Proposition 5.1. *If Condition* $(*)$ *is satisfied, then* $g_3 = \lfloor \tfrac{q^2-q+4}{6} \rfloor$.

Remark 5.2. If $q \equiv 2 \pmod 3$, the case $d = 3$ in Theorem 2.1(V) provides a $\mathbf{F}_{q^2}$-maximal curve of genus $(q^2 - q - 2)/6$. For this curve, $m_1(P) = q - 1$ for each $\mathbf{F}_{q^2}$-rational point P, see [4], Prop. 6.4. Therefore Condition $(*)$ above is not trivial.

Corollary 5.3. *If Condition $(*)$ is satisfied, then $(q^2 - q - 2)/6$ is the fourth larger genus that a maximal curve can have for $q \equiv 2 \pmod 3$.*

Proof. It follows from the theorem and the remark. □

Proof of Proposition 5.1. We first notice that $\mathbf{F}_{q^2}$-maximal curves having genus $\lfloor \frac{q^2-q+4}{6} \rfloor$ come from the case $d = 3$ in Theorem 2.1. Now let $\mathcal{X}$ be a $\mathbf{F}_{q^2}$-maximal curve of genus g such that $\dim(\mathcal{D}_{\mathcal{X}}) = 3$. Then (5.3), (5.4) together with the hypothesis allow us to assume $m_1(P) = \lfloor \frac{q+1}{2} \rfloor$. If q is odd, then $g = (q-1)^2/4$ [7], Thm. 2.3; otherwise $g = q(q-2)/4$ [1] and this completes the proof.

Remark 5.4. By Fuhrmann's results (op. cit.), a $\mathbf{F}_{q^2}$-maximal curve of genus $\lfloor \frac{q^2-q+4}{6} \rfloor$ must have at least a $\mathbf{F}_{q^2}$-rational point P such that $m_1(P) \in \{\lfloor \frac{2q+2}{3} \rfloor, q-2\}$. For $q \equiv 1 \pmod 3$, Proposition 5.6(5) shows that $(2q+1)/3$ occurs as a non-gap at certain $\mathbf{F}_{q^2}$-rational points.

Finally, we discuss necessary conditions for the existence of non-trivial separable $\mathbf{F}_{q^2}$-coverings

$$\pi : \mathcal{H} \to \mathcal{X}$$

from the Hermitian curve $\mathcal{H}$ to a ($\mathbf{F}_{q^2}$-maximal) curve $\mathcal{X}$.

Proposition 5.5. *Let g denote the genus of $\mathcal{X}$. If $g > \lfloor \frac{q^2-q+4}{3} \rfloor$, then $\deg(\pi) = 2$, $g = \lfloor \frac{(q-1)^2}{4} \rfloor$, and one of the following holds:*

1. *$\mathcal{X}$ is the non-singular model of $y^q + y = x^{(q+1)/2}$ provided that q odd*
2. *$\mathcal{X}$ is the non-singular model of $\sum_{i=1}^{t} y^{q/2^i} = x^{q+1}$ provided that $q = 2^t$.*

Proof. See [1]. □

Proposition 5.6. *Let g denote the genus of $\mathcal{X}$. If $g > \lfloor \frac{q^2-q+6}{8} \rfloor$ and $\deg(\pi) > 2$ then*

1. *$\deg(\pi) = 3$;*
2. *π is unramified iff $q \equiv 2 \pmod 3$ and $g = (q^2 - q + 4)/6$;*
3. *If π is ramified, then $g \leq (q^2 - q)/3$.*

Suppose now that π is ramified and that $g > \lfloor \frac{(q-1)(q-2)}{6} \rfloor$. Then

4. *If $q \equiv 2 \pmod 3$, $q \geq 5$, then $g = (q^2 - q - 2)/6$ and π is (totally) ramified at 3 points $P_1, P_2, P_3 \notin \mathbf{F}_{q^2}(\mathcal{H})$. Moreover for each i, $\pi(P_i) \notin \mathcal{X}(\mathbf{F}_{q^2})$ and the Weierstrass semigroup at $\pi(P_i)$ is given by*

$$\{h/3 : h \equiv 0 \pmod 3, h \in S\},$$

where

$$S := \cup_{j=1}^{q-2}[jq - (j-1), jq] \cup \{0, q^2 - 2q + 2, q^2 - 2q + 3, \dots\}.$$

In particular, $m_1(\pi(P_i)) = (2q-1)/3$ and $m_2(\pi(P_i)) = q$.

5. *If* $q \equiv 1 \pmod 3$, *then* $g = (q^2-q)/6$ *and* π *is (totally) ramified at 2 points* $P_1, P_2 \in \mathcal{H}(\mathbf{F}_{q^2})$. *The Weierstrass semigroup at* $\pi(P_i) \in \mathcal{X}(\mathbf{F}_{q^2})$ *is given by*
$$\langle (2q+1)/3, q, q+1 \rangle .$$
In particular, $m_1(\pi(P_i)) = (2q+1)/3$.
6. *If* $q \equiv 0 \pmod 3$ *and* $g = (q^2-q)/6$, *then* π *is (totally) ramified just at 1 point* $P_1 \in \mathcal{H}(\mathbf{F}_{q^2})$; *moreover* $m_1(\pi(P_1)) = 2q/3$.
7. *If* π *is normal, i.e. if* π *is Galois, then* $\mathcal{X}$ *is* $\mathbf{F}_{q^2}$*-isomorphic to one of the curves of case* $d = 3$ *in Theorem 2.1.*

Proof. The hypotheses on g and $\deg(\pi)$ together with the Riemann-Hurwitz formula yield $\deg(\pi) = 3$. Statement 2 also follows form the Riemann-Hurwitz formula. To see 3 we can assume that $p \neq 3$ and that π has just one (totally) ramified point. But then $(q^2 - q - 4) \equiv 0 \pmod 3$, contradicting 2.

Now let us assume that π is ramified at $P \in \mathcal{H}$ and let $Q := \pi(P)$. By the hypothesis on g, from [4], Lemma 3.1, [7], Prop. 1.5, we have

$$(**) \qquad m_1(Q) < m_2(Q) \leq q < m_3(Q) .$$

On the other hand, the only possibility for the Weierstrass semigroup $H(P)$ at P is the above semigroup S (whenever $P \notin \mathcal{H}(\mathbf{F}_{q^2})$), and $H(P) = \langle q, q+1 \rangle$ (whenever $P \in \mathcal{H}(\mathbf{F}_{q^2})$ [12], Thm. 2. Let us notice that if $h \in H(Q)$, then $3h \in H(P)$; the converse also holds for $p \neq 3$ (see e.g. [37], proof of Lemma 3.4).

Case $q \equiv 2 \pmod 3$**.** We claim that $P \notin \mathcal{H}(\mathbf{F}_{q^2})$ and $Q \notin \mathcal{X}(\mathbf{F}_{q^2})$. To see this we first suppose that $P \in \mathcal{H}(\mathbf{F}_{q^2})$. Then $m_3(Q) = q+1$ and we have 4 elements in $H(P)$ which are both congruent to zero modulo 3 and bounded by $3q+3$. This contradicts $(**)$. Now assume that $Q \in \mathcal{X}(\mathbf{F}_{q^2})$ so that $m_3(Q) = q+1$. We then have $3q+3 \in H(P)$ so that $3q+3 \geq 4q-3$, i.e. $q = 5$. In this case $H(Q) = \{0, 3, 5, 6, 7, 8 \dots\}$ so that $g = 3$. On the other hand $g = 4$ by [7], Thm. 2.3, $g = 4$. This contradiction completes the proof. Thus by [37], Lemma 3.4,

$$g = \#\{\ell \in \mathbf{N} \setminus S : \ell \equiv 0 \pmod 3\},$$

whence $g = (q^2 - q - 2)/6$ follows by an easy computation. Then the ramification number of π is 6 and so it ramifies at three points. The statement on Weierstrass semigroups comes from [37], proof of Lemma 3.4.

Case $q \equiv 1 \pmod 3$**.** We claim that $P \in \mathcal{H}(\mathbf{F}_{q^2})$. For $P \in \mathcal{H}(\mathbf{F}_{q^2})$, we have indeed just one element in $H(P)$ which is both congruent to zero modulo 3 and less than or equal to $3q$. This contradicts $(**)$. Now the proof can be done as in the previous case, except that

$$\{h/3 : h \equiv 0 \pmod 3, h \in \langle q, q+1 \rangle\} = \langle (2q+1)/3, q, q+1 \rangle$$

follows from [6], §A.2.

Case $q \equiv 0 \pmod 3$**.** Due to wild ramifications, the previous argument does not apply to compute the genus as before. For $g = (q^2 - q)/3$, the ramification number is 4, and hence π is ramified just at one point $P_1 \in \mathcal{H}$. The non-gaps at P_1 less than or equal to $3q$ turn out to be either $q, 2q-1, 2q, 3q-2, 3q-1, 3q$, or $q, q+1, 2q, 2q+1, 2q+2, 3q$. This yields $m_1(\pi(P_1)) = 2q/3$ and $m_2(\pi(P_1)) = q$. □

Remark 5.7. Let $\mathcal{X}$ be the curve in Theorem 2.1(II)(2) and P_0 the unique $\mathbf{F}_{q^2}$-rational point over $x = \infty$. Note that $\mathcal{D}_{\mathcal{X}} = |(q+1)P_0|$. Now, an easy computation shows that the first $(p+1)$ positive Weierstrass non-gaps are $2q/p, \ldots, pq/p, q+1$. This generalizes Proposition 5.6(6) and yields $\dim(\mathcal{D}_{\mathcal{X}}) = p$.

Remark 5.8. Our final remark concerns the open question of determining all $\mathbf{F}_{q^2}$-maximal curves $\mathcal{X}$ such that $\dim(\mathcal{D}_{\mathcal{X}}) = 3$. To the list of the known examples given in [4], §6, the non-singular model of the curve $x^{(q+1)/3} + x^{2(q+1)/3} + y^{q+1} = 0$, $q \equiv 2 \pmod 3$, (see Theorem 2.1(IV)(2)), has to be added.

Acknowledgements. The authors wish to thank James W.P. Hirschfeld for useful comments. This research was carried out with the support of the Italian Ministry for Research and Technology (project 40% "Strutture geometriche, combinatorie e loro applicazioni"). Part of this paper was written while F.T. was visiting the Abdus Salam ICTP (Trieste, Italy) supported by IMPA/Cnpq (Brazil) and ICTP. This work was done within the framework of the Associateship Scheme of the Abdus Salam International Centre for Theoretical Physics, Trieste, Italy.

References

[1] M. Abdón and F. Torres, *On maximal curves in characteristic two*, Manuscripta Math. **99**(1) (1999), 39–53.
[2] A. Cossidente, J.W.P. Hirschfeld, G. Korchmáros and F. Torres, *On plane maximal curves*, Compositio Math., to appear.
[3] A. Cossidente and G. Korchmáros, *The algebraic envelope associated to a complete arc*, Rend. Circ. Mat. Palermo Suppl. 51 Recent Progress in Geometry, E. Ballico, G. Korchmáros (Eds.), (1998), 9–24.
[4] A. Cossidente, G. Korchmáros and F. Torres, *On curves covered by the Hermitian curve*, J. Algebra **216**(1) (1999), 56–76.
[5] H. M. Farkas and I. Kra, *Riemann surfaces*, Grad. Text in Maths. Vol. 71, second edition, Springer-Verlag, 1992
[6] R. Fuhrmann, *Algebraische Funktionenkörper über endlichen Körpern mit maximaler Anzahl rationaler Stellen*, Ph.D. dissertation, Universität GH Essen, Germany, 1995.
[7] R. Fuhrmann, A. Garcia and F. Torres, *On maximal curves*, J. Number Theory **67**(1) (1997), 29–51.
[8] R. Fuhrmann and F. Torres, *The genus of curves over finite fields with many rational points*, Manuscripta Math. **89** (1996), 103–106.
[9] R. Fuhrmann and F. Torres, *On Weierstrass points and optimal curves*, Rend. Circ. Mat. Palermo Suppl. 51 Recent Progress in Geometry, E. Ballico, G. Korchmáros (Eds.), (1998), 25–46.
[10] A. Garcia, H. Stichtenoth, *Algebraic function fields over finite fields with many rational places*, IEEE Trans. Inf. Theory **41**(6), (1995), 1548–1563.
[11] A. Garcia, H. Stichtenoth and C.P. Xing, *On subfields of the Hermitian function field*, Compositio Math., to appear.
[12] A. Garcia and P. Viana, *Weierstrass points on certain non-classical curves*, Arch. Math. **46** (1986), 315–322.
[13] G. van der Geer and M. van der Vlugt, *How to construct curves over finite fields with many points*, Arithmetic Geometry, (Cortona 1994), F. Catanese Ed., Cambridge University Press, Cambridge, 169-189, 1997.
[14] G. van der Geer and M. van der Vlugt, *Generalized Reed-Muller codes and curves with many points*, Report W97-22, Mathematical Institute, University of Leiden, The Netherlands, (alg-geom/9710016).
[15] G. van der Geer and M. van der Vlugt, *Tables of curves with many points*, April 1998, http:// www.wins.uva.nl/geer.
[16] V.D. Goppa, *Geometry and Codes*, Mathematics and its applications, 24, Kluwer Academic Publishers, Dordrecht-Boston-London 1988.
[17] J.P. Hansen and J.P. Pedersen, *Automorphism groups of Ree type, Deligne-Lusztig curves and function fields*, J. Reine Angew. Math. **440** (1993), 99–109.
[18] R.W. Hartley, *Determination of the ternary collineation groups whose coefficients lie in the $GF(2^n)$*, Annals of Math. **27** (1926), 140–158.
[19] R. Hartshorne, *Algebraic Geometry*, Grad. Texts in Math., Vol. 52, Springer-Verlag, New York/Berlin, 1977.
[20] J.W.P. Hirschfeld, *Projective Geometries Over Finite Fields*, second edition, Oxford University Press, Oxford, 1998.
[21] A.R. Hoffer, *On unitary collineation groups*, J. Algebra **22** (1972), 211–218.

[22] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin-Heidelberg-New York, 1967.
[23] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Tokio **28** (1981), 721–724.
[24] J.H. van Lint and G. van der Geer, *Introduction to Coding Theory and Algebraic Geometry*, DMV Seminar Band 12, Birkhäuse Verlag, Besel, 1988.
[25] P.B Kleidman, *The maximal subgroups of the low- dimensional classical groups*, Ph.D. Thesis, Cambridge 1987.
[26] G. Lachaud, *Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis*, C.R. Acad. Sci. Paris **305**, Série I (1987), 729–732.
[27] H.H. Mitchell, *Determination of the ordinary and modular ternary linear groups*, Trans. Amer. Math. Soc. **12** (1911), 207–242.
[28] C.J. Moreno, *Algebraic Curves over Finite Fields*, Cambridge University Press, Vol. 97, 1991.
[29] H.G. Rück and H. Stichtenoth, *A characterization of Hermitian function fields over finite fields*, J. Reine Angew. Math. **457** (1994), 185–188.
[30] A. Seidenberg, Elements of the Theory of Algebraic Curves, Addison Wesley, Reading, Mass. 1969.
[31] M.W. Short, *The primitive soluble permutation groups of degree less then* 256, LNM 1519, Springer-Verlag, 1992.
[32] S.A. Stepanov, *Arithmetic of Algebraic Curves*, Consultants Bureau, New York and London, 1994.
[33] H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik*, Arch. Math. **24** (1973), 527–544 and 615–631.
[34] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag Berlin, 1993.
[35] H. Stichtenoth and C.P. Xing, *The genus of maximal function fields*, Manuscripta Math. **86** (1995), 217–224.
[36] K.O. Stöhr and J.F. Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. **52** (1986), 1–19.
[37] F. Torres, *On certain N–sheeted coverings of curves and numerical semigroups which cannot be realized as Weierstrass semigroups*, Comm. Algebra **23**(11) (1995), 4211–4228.
[38] M.A. Tsfasman and S.G. Vlăduţ, *Algebraic-Geometric Codes*, Kluwer Academic Publishers, Dordrecht-Boston-London 1991.