A new family of maximal curves over a finite field

M. Giulietti * and G. Korchmáros *

February 22, 2013

Abstract

A new family of $\mathbb{F}_{q^2}$-maximal curves is presented and some of their properties are investigated.

1 Introduction

Let q be a power of a prime number p. A maximal curve defined over a finite field $\mathbb{F}_{q^2}$ with q^2 elements, briefly an $\mathbb{F}_{q^2}$-maximal curve, is a projective, geometrically irreducible, non-singular algebraic curve defined over $\mathbb{F}_{q^2}$ whose number of $\mathbb{F}_{q^2}$-rational points attains the famous Hasse-Weil upper bound $q^2+1+2gq$ where g is the genus of the curve. Maximal curves have also been investigated for their applications in Coding theory. Surveys on maximal curves are found in [11, 14, 12, 13, 36, 37], see also [10, 9, 31, 35].

By a result of Serre, see Lachaud [27, Proposition 6], any non-singular curve which is $\mathbb{F}_{q^2}$-covered by an $\mathbb{F}_{q^2}$-maximal curve is also $\mathbb{F}_{q^2}$-maximal. Apparently, the known maximal curves are all Galois $\mathbb{F}_{q^2}$-covered by one of the curves below, see [1, 2, 3, 4, 5, 6, 7, 8, 15, 16, 17, 18, 19, 20, 21, 22, 28, 29].

(A) for every q, the Hermitian curve over $\mathbb{F}_{q^2}$;

(B) for every $q=2q_0^2$ with $q_0=2^h$, $h\geq 1$, the DLS curve (the Deligne-Lusztig curve associated with the Suzuki group) over $\mathbb{F}_{q^4}$;

*Research supported by the Italian Ministry MURST, Strutture geometriche, combinatoria e loro applicazioni, PRIN 2006-2007

(C) for every $q = 3q_0^2$ with $q_0 = 3^h$, $h \geq 1$, the DLR curve (the Deligne-Lusztig curve associated with the Ree group) over $\mathbb{F}_{q^6}$;

(D) for every $q = p^{3h}$, the GS-curve (the Garcia-Stichtenoth curve) over $\mathbb{F}_{q^2}$.

It seems plausibile that each of the known $\mathbb{F}_{q^2}$-maximal curve is Galois $\mathbb{F}_{q^2}$-covered by exactly one of the above curves, apart from a very few possible exceptions for small q's. This has been investigated so far in three special cases: The smallest GS-curve, $q = 8$, is Galois $\mathbb{F}_{q^2}$-covered by the Hermitian curve over $\mathbb{F}_{64}$, but this does not hold for $q = 27$, see [16], while an unpublished result by Rains and Zieve states that the smallest DLR-curve, q=3, is not Galois $\mathbb{F}_{3^6}$-covered by the Hermitian curve over $\mathbb{F}_{3^6}$.

In this preliminary report, a new $\mathbb{F}_{q^2}$-maximal curve $\mathcal{X}$ is constructed for every $q = n^3$. For $q > 8$, the relevant property of $\mathcal{X}$ is not being $\mathbb{F}_{q^2}$-covered by any of the four curves (A),(B),(C),(D); we stress that this even holds for non Galois $\mathbb{F}_{q^2}$-coverings. The case $q = 8$ remains open.

The automorphism group $\mathrm{Aut}(\mathcal{X})$ of $\mathcal{X}$ is also determined; its size turns out to be large compared to the genus $\mathcal{X}$. For curves with large automorphism groups, see [23, 30, 33].

2 Construction

Throughout this paper, p is a prime, $n = p^h$ and $q = n^3$ with $h \geq 1$.

We will need some identities in $\mathbb{F}_{n^2}[X]$ concerning the polynomial

$$h(X) = \sum_{i=0}^{n} (-1)^{i+1} X^{i(n-1)}. \tag{1}$$

Lemma 2.1.

$$X^{n^2} - X = (X^n + X)h(X), \tag{2}$$

and

$$X^{n^3} + X - (X^n + X)^{n^2-n+1} = (X^n + X)h(X)^{n+1}, \tag{3}$$

Proof. A straightforward computation shows (2). Also,

$$(X^n - X)^n (X^{n^3} - X + (X^n - X)^{n^2-n+1}) = (X^{n^2} - X)^{n+1}. \tag{4}$$

Now, choose $\rho \in \mathbb{F}_{q^2}$ with $\rho^n = -\rho$ and replace X by ρX. From (4),

$$[(\rho X)^n - \rho X]^n[(\rho X)^{n^3} - \rho X + ((\rho X)^n - \rho X)^{n^2-n+1}] = [(\rho X)^{n^2} - (\rho X)]^{n+1}.$$

Since $\rho^{n^2} = \rho$ and $\rho^{n^3} = -\rho$, the assertion (3) follows. □

In the three–dimensional projective space $\mathrm{PG}(3, q^2)$ over $\mathbb{F}_{q^2}$, consider the algebraic curve $\mathcal{X}$ defined to be the complete intersection of the surface Σ with affine equation

$$Z^{n^2-n+1} = Yh(X), \tag{5}$$

and the Hermitian cone $\mathcal{C}$ with affine equation

$$X^n + X = Y^{n+1}. \tag{6}$$

Note that $\mathcal{X}$ is defined over $\mathbb{F}_{q^2}$ but it is viewed as a curve over the algebraic closure $\mathbb{K}$ of $\mathbb{F}_{q^2}$. Moreover, $\mathcal{X}$ has degree $n^3 + 1$ and possesses a unique infinite point, namely the infinite point X_∞ of the X-axis.

A treatise on Hermitian surfaces over a finite field is found in [24, 32].

Our aim is to prove the following theorem.

Theorem 2.2. *$\mathcal{X}$ is an $\mathbb{F}_{q^2}$-maximal curve.*

To do this, it is enough to show the following two lemmas, see [26].

Lemma 2.3. *The curve $\mathcal{X}$ lies on the Hermitian surface $\mathcal{H}$ with affine equation*

$$X^{n^3} + X = Y^{n^3+1} + Z^{n^3+1}. \tag{7}$$

Proof. Clearly, $X_\infty \in \mathcal{H}$. Let $P = (x, y, z)$ be any affine point of $\mathcal{X}$. From (5), $z^{n^3+1} = y^{n+1}h(x)^{n+1}$. On the other hand, (3) together with (6) imply that $y^{n+1}h(x)^{n+1} = x^{n^3} + x - y^{n^3+1}$. This proves the assertion. □

Lemma 2.4. *The curve $\mathcal{X}$ is irreducible over $\mathbb{K}$.*

Proof. Let $\mathcal{Y}$ be an irreducible component of $\mathcal{X}$ defined over $\mathbb{K}$. Let $\mathbb{K}(\mathcal{Y})$ be the function field of $\mathcal{Y}$. Let $x, y, z, t \in \mathbb{K}(\mathcal{Y})$ be the coordinate functions of the embedding of $\mathcal{Y}$ in $\mathrm{PG}(3, \mathbb{K})$. Since $\mathcal{Y}$ lies on $\mathcal{H}$,

$$x^{n^3} + x - y^{n^3+1} - z^{n^3+1} = 0. \tag{8}$$

Take a non-singular affine point $P = (x_P, y_P, z_P)$ on $\mathcal{Y}$, and let $\xi = x - x_P$, $\eta = y - y_P$, $\zeta = z - z_P$. From (7),

$$\xi - \eta y_P^{n^3} - \zeta z_P^{n^3} = -\xi^{n^3} + \eta^{n^3} y_P + \eta^{n^3+1} + \zeta^{n^3} z_P + \zeta^{n^3+1},$$

whence

$$v_P(\xi - \eta y_P^{n^3} - \zeta z_P^{n^3}) \geq n^3,$$

where, as usual, $v_P(u)$ with $u \in K(\mathcal{X}) \setminus 0$ stands for the valuation of u at P.

Since the tangent plane π_P to $\mathcal{H}$ at P has equation

$$X - x_P - y_P^{n^3}(Y - y_p) - z_P^{n^3}(Z - z_P) = 0,$$

the intersection number $I(P, \mathcal{Y} \cap \pi_P)$ is at least n^3. Therefore, if $\mathcal{X} \neq \mathcal{Y}$, then either $\deg \mathcal{Y} = n^3$ or $\mathcal{Y}$ lies on π. Since the equation of π_P may also be written as

$$X - y_P^{n^3} Y - z_P^{n^3} Z + x_P^{n^3} = 0, \tag{9}$$

and

$$x_P^{n^3} + x_P - y_P^{n^3+1} - z_P^{n^3+1} = 0$$

implies that

$$x_P^{n^6} + x_P^{n^3} - y_P^{n^6+n^3} - z_P^{n^6+n^3} = 0,$$

we see that the point, the so-called Frobenius image of P,

$$\varphi(P) = (x_P^{q^2}, y_P^{q^2}, z_P^{q^2})$$

also lies on π_P.

Now, in the former case, $\mathcal{X}$ splits into $\mathcal{Y}$ and a line. In particular, $\mathcal{Y}$ is defined over $\mathbb{F}_{q^2}$. Now, if the above point is not defined over $\mathbb{F}_{q^2}$, that is $P \in \mathcal{Y}$ but $P \in \mathrm{PG}(3, \mathbb{K}) \setminus \mathrm{PG}(3, \mathbb{F}_{q^2})$, then the point $\varphi(P)$ of $\mathcal{Y}$ is distinct from P. Also, π_P contains $\varphi(P)$. From this, the intersection divisor of $\mathcal{Y}$ cut out by π has degree bigger than n^3; a contradiction with $\deg \mathcal{Y} = n^3$.

It remains to consider the case where $\mathcal{Y}$ lies on π for every non-singular affine point P. Since the tangent planes to $\mathcal{H}$ at distinct points of $\mathcal{X}$ are distinct, $\mathcal{Y}$ must be a line lying on $\mathcal{H}$. But this contradicts the fact that the lines of $\mathcal{C}$ contain the vertex of $\mathcal{C}$ which is a point outside $\mathcal{H}$. □

From [26] and Theorem 2.2, $\mathcal{X}$ is a non-singular curve, and the linear series $|qP + \varphi(P)|$ with $P \in \mathcal{X}$ is cut out by the planes of $\mathrm{PG}(3, \mathbb{K})$.

Theorem 2.5. *$\mathcal{X}$ has genus $g = \frac{1}{2}(n^3+1)(n^2-2)+1$.*

Proof. Every linear collineation $(X,Y,Z) \to (X,Y,\lambda Z)$ with $\lambda^{n^2-n+1} = 1$ preserves both Σ and $\mathcal{C}$. For $\lambda \neq 1$, the fixed points of such a collineation g_λ are exactly the points of the plane π_0 with equation $Z = 0$. Since π_0 contains no tangent to $\mathcal{X}$, the number of fixed points of g_λ with $\lambda \neq 1$ is independent from λ and equal to n^3+1.

The above collineation g_λ defines an automorphism of $\mathcal{X}$. Let Λ be the group consisting of all these automorphisms. Since $p \nmid |\Lambda|$, the Hurwitz genus formula gives

$$2g-2 = (n^2-n+1)(2\bar{g}-2) + (n^3+1)(n^2-n),$$

where $\bar{g}$ is the genus of the quotient curve $\mathcal{Y} = \mathcal{X}/\Lambda$. From the definition of $\mathcal{X}$ and Λ, this quotient curve $\mathcal{Y}$ is the complete intersection of $\mathcal{C}$ and the rational surface of equation $Z = Y g(X)$. This shows that $\mathcal{Y}$ is birationally equivalent to the Hermitian curve of equation $X^n + X = Y^{n+1}$. Since the latter curve has genus $\frac{1}{2}(n^2-n)$, we find that $\bar{g} = \frac{1}{2}(n^2-n)$. Now, from the above equation, $2g-2 = (n^3+1)(n^2-2)$ whence the assertion follows. $\square$

3 $\mathbb{F}_{q^2}$-coverings of the Hermitian curves

We show that if $q > 8$ then $\mathcal{X}$ is not $\mathbb{F}_{q^2}$-covered by any of the curves (A),(B),(C),(D). Actually, this holds trivially for (B),(C),(D), as the genus of each of the latter three curves is smaller than the genus of $\mathcal{X}$. Therefore, we only need to prove the following result.

Proposition 3.1. *If $q > 8$, then $\mathcal{X}$ is not $\mathbb{F}_{q^2}$-covered by the Hermitian curve defined over $\mathbb{F}_{q^2}$.*

Proof. Assume on the contrary that $\mathcal{X}$ is $\mathbb{F}_{q^2}$-covered by the Hermitian curve $\mathcal{H}_q$ over $\mathbb{F}_{q^2}$. Let m denote the degree of such a covering φ. Since $\mathcal{H}_q$ has genus $\frac{1}{2}q(q-1) = \frac{1}{2}n^3(n^3-1)$, the Hurwitz genus formula applied to φ gives:

$$n^6 - n^3 - 2 \geq m(n^3+1)(n^2-2).$$

This yields that $m \leq n$ for $n > 2$.

On the other hand, each of the $q^3+1 = n^9+1$ $\mathbb{F}_{q^2}$-rational point of $\mathcal{H}_q$ lies over an $\mathbb{F}_{q^2}$-rational point of $\mathcal{X}$ and the number of $\mathbb{F}_{q^2}$-rational points of

$\mathcal{H}_q$ lying over a given $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}$ is at most m. Since $\mathcal{X}$ has exactly $n^8 - n^6 + n^3 + 1$ $\mathbb{F}_{q^2}$-rational points, this gives:

$$n^9 + 1 \leq m(n^8 - n^6 + n^5 + 1).$$

For this $m > n$, a contradiction. $\square$

4 Automorphism group over $\mathbb{F}_{q^2}$

Let $\mathrm{Aut}(\mathcal{X})$ be the $\mathbb{F}_{q^2}$-automorphism group of $\mathcal{X}$. In terms of the associated function field, $\mathrm{Aut}(\mathcal{X})$ is the group of all automorphisms of $\mathbb{K}(\mathcal{X})$ which fixes every element in the subfield $\mathbb{F}_{q^2}$ of $\mathbb{K}$.

First we point out that $\mathrm{Aut}(\mathcal{X})$ contains a subgroup isomorphic to the special unitary group $\mathrm{SU}(3, n)$. This requires to lift $\mathrm{SU}(3, n)$ to a collineation group of $\mathrm{PG}(3, q^2)$.

If the non-degenerate Hermitian form in the three dimensional vector space $V(3, n^2)$ over $\mathbb{F}_{n^2}$ is given by $X^nT + XT^n - Y^{n+1}$ then $\mathrm{SU}(3, n)$ is represented by the matrix group of order $(n^3+1)n^3(n^2-1)$ generated by the following matrices:

For $a, b \in \mathbb{F}_{n^2}$ such that $a^n + a - b^{n+1} = 0$, and for $k \in \mathbb{F}_{n^2}$, $k \neq 0$,

$$Q_{(a,b)} = \begin{pmatrix} 1 & b^n & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}, \; H_k = \begin{pmatrix} k^{-n} & 0 & 0 \\ 0 & k^{n-1} & 0 \\ 0 & 0 & k \end{pmatrix}, \; W = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

The subgroup of $\mathrm{SU}(3, n)$ consisting of its scalar matrices λI, with $\lambda \in \mathbb{F}_{n^2}$ is either trivial or has order 3 according as $\gcd(3, n+1)$ is either 1 or 3.

From each of the above matrices a 4×4-matrix arises by adding $0, 0, 1, 0$ as a third row and as a third column. If $\tilde{Q}_{(a,b)}$, $\tilde{H}_k, \tilde{W}$ are the 4×4 matrices obtained in this way, the matrix group T generated by them is isomorphic to $\mathrm{SU}(3, n)$.

By the same lifting procedure, each 3×3 diagonal matrix λI defines a 4×4 diagonal matrix $\tilde{D}_\lambda$ with diagonal $[\lambda, \lambda, 1, \lambda]$. If λ ranges over the set of all (n^2-n+1)–st roots of unity, the matrices $\tilde{D}_\lambda$ form a cyclic group C_{n^2-n+1}. Obviously, $\tilde{D}_\lambda$ commutes with every matrix in T, and hence the group M generated by T and C_{n^2-n+1} is TC_{n^2-n+1}. Here, $T \cap C_{n^2-n+1}$ is either trivial or a subgroup of order 3, according as $\gcd(3, n+1) = 1$ or $\gcd(3, n+1) = 3$. In the latter case, let $C_{(n^2-n+1)/3}$ be the subgroup of C_{n^2-n+1} of index 3. Note that if $\gcd(3, n+1) = 3$ then $9 \nmid (n^2 - n + 1)$. Therefore, M can be written as a direct product, namely

$$M = \begin{cases} T \times C_{n^2-n+1} & \text{when} \quad \gcd(3, n+1) = 1; \\ T \times C_{(n^2-n+1)/3} & \text{when} \quad \gcd(3, n+1) = 3. \end{cases}$$

In $\mathrm{PG}(3, q^2)$ equipped with homogeneous coordinates (X, Y, Z, T), every regular 4×4 matrix defines a linear collineation, and two such matrices define the same linear collineation if and only if one is a multiple of the other. Since both third row and column in each of the above matrices is $0, 0, 1, 0$, the group M can be viewed as a collineation group of $\mathrm{PG}(3, q^2)$. Our aim is to prove that M preserves $\mathcal{X}$. This will be done in two steps.

Lemma 4.1. *The group T preserves $\mathcal{X}$.*

Proof. Let $P = (x, y, z, 1) \in \mathcal{X}$. The image of P under $\tilde{Q}_{(a,b)}$ is $(x_1, y_1, z, 1)$ with $x_1 = x + b^n y + a$, $y_1 = y + b$. From (6),

$$x_1^n + x_1 = y_1^{n+1}. \tag{10}$$

Furthermore, if $x^n + x \neq 0$, then by (2)

$$yh(x) = y\,\frac{x^{n^2} - x}{x^n + x} = y\,\frac{(x^n + x)^n - (x^n + x)}{x^n + x} = y\,\frac{y^{(n+1)n} - y^{n+1}}{y^{n+1}} = -y + y^{n^2}.$$

Since $b \in \mathbb{F}_{n^2}$, this implies that $yh(x) = y_1(y_1^{n^2-1} - 1)$. On the other hand, from (10),

$$y_1^{n^2-1} = (x_1^n + x_1)^{n-1}.$$

Therefore, if $x_1^n + x_1 \neq 0$, then

$$yh(x) = y_1((x_1^n + x_1)^{n-1} - 1) = y_1\left(\frac{(x_1^n + x_1)^n}{x_1^n + x_1} - 1\right) = y_1 h(x_1).$$

Since $x^n + x = 0$ only holds for finitely many of points of $\mathcal{X}$, and the same holds for $x_1^n + x_1 = 0$, this implies that $\tilde{Q}_{(a,b)} \in \mathrm{Aut}(\mathcal{X})$.

Similar calculation works for $\tilde{H}_k$ showing that $\tilde{H}_k \in \mathrm{Aut}(\mathcal{X})$.

To deal with $\tilde{W}$, homogeneous coordinates are needed. Note that (6) reads $X^nT + XT^n = Y^{n+1}$ in homogeneous coordinates. Let $P = (x, y, z, t)$ be a point of $\mathcal{X}$. Then the image of P is the point $P' = (t, -y, z, x)$. Since

$x^n t + xt^n = t^n x + tx^n$ and $x^n t + xt^n - y^{n+1} = 0$, we have that $P' \in \mathcal{C}$. Further, if $x^n + xt^{n-1} \neq 0$ and $t \neq 0$, then

$$yh(x) = y\,\frac{x^{n^2} - xt^{n^2-1}}{x^n + xt^{n-1}} = -y\,\frac{t^{n^2} - tx^{n^2-1}}{t^n + tx^{n-1}} = -yh(t).$$

From this $\tilde{W} \in \mathrm{Aut}(\mathcal{X})$, as $x^n + xt^{n-1} = 0$ and $t = 0$ only hold for finitely many points of $\mathcal{X}$. □

Lemma 4.2. *The group C_{n^2-n+1} preserves $\mathcal{X}$.*

Proof. A straightforward computation shows the assertion. □

Lemmas 4.1 and 4.2 have the following corollary.

Theorem 4.3. $\mathrm{Aut}(\mathcal{X})$ *contains a subgroup M such that*

$$M \cong \begin{cases} \mathrm{SU}(3,n) \times C_{n^2-n+1} & \textit{when} \quad \gcd(3,n+1) = 1; \\ \mathrm{SU}(3,n) \times C_{(n^2-n+1)/3} & \textit{when} \quad \gcd(3,n+1) = 3. \end{cases}$$

Actually, $\mathrm{Aut}(\mathcal{X}) = M$ when $\gcd(3,n+1) = 1$, but $\mathrm{Aut}(\mathcal{X})$ is a bit larger when $\gcd(3,n+1) = 3$. To show this, the following bound on $|\mathrm{Aut}(\mathcal{X})|$ will be useful.

Lemma 4.4. $|\mathrm{Aut}(\mathcal{X})| \leq (n^3+1)n^3(n^2-1)(n^2-n+1)$.

Proof. From the remark before Theorem 2.5, $\mathrm{Aut}(\mathcal{X})$ is linear, that is, it consists of all linear collineations of $\mathrm{PG}(3,\mathbb{K})$ preserving $\mathcal{X}$. Obviously, $\mathrm{Aut}(\mathcal{X})$ fixes Z_∞, the vertex of $\mathcal{C}$. Further, $\mathrm{Aut}(\mathcal{X})$ preserves $\mathcal{H}$ as $\mathcal{X}$ lies on $\mathcal{H}$, and $\mathrm{Aut}(\mathcal{X})$ is a subgroup of $\mathrm{PGU}(4,q^2)$, see [26, Theorem 3.7]. Also, $\mathrm{Aut}(\mathcal{X})$ must preserve the plane π_0 of equation $Z = 0$, as π_0 is the polar plane of Z_∞ under the unitary polarity arising from $\mathcal{H}$. Therefore, $\mathrm{Aut}(\mathcal{X})$ induces a collineation group S of π_0 preserving the Hermitian curve of π_0 of equation (6). Hence, S is isomorphic to a subgroup of $\mathrm{PGU}(3,n)$. In particular, $|S| \leq (n^3+1)n^3(n^2-1)$. The subgroup U of $\mathrm{Aut}(\mathcal{X})$ fixing π_0 pointwise preserves every line through Z_∞. From (5), all, but finitely many, lines through Z_∞ meeting $\mathcal{X}$ contain each exactly n^2-n+1 pairwise distinct common points from $\mathcal{X}$. Therefore, $|U| \leq n^2-n+1$. Since $|\mathrm{Aut}(\mathcal{X})| = |S||U|$, the assertion follows. □

For $\gcd(3,n+1) = 1$, Theorem 4.3 together with Lemma 4.4 determine $\mathrm{Aut}(\mathcal{X})$.

Theorem 4.5. *If* $\gcd(3, n+1) = 1$, *then* $\mathrm{Aut}(\mathcal{X}) \cong \mathrm{SU}(3, n) \times C_{n^2-n+1}$. *In particular,* $|\mathrm{Aut}(\mathcal{X})| = n^3(n^3+1)(n^2-1)(n^2-n+1)$. *Furthermore,* $\mathrm{Aut}(\mathcal{X})$ *is defined over* $\mathbb{F}_{q^2}$ *but it contains a subgroup isomorphic to* $\mathrm{SU}(3, n)$ *defined over* $\mathbb{F}_{n^2}$.

For $\gcd(3, n+1) = 3$, we exhibit one more linear collineation preserving $\mathcal{X}$. To do this choose a primitive n^3+1 roots of unity in $\mathbb{F}_{q^2}$, say ρ, and define $\tilde{E}$ to be the diagonal matrix

$$[\rho^{-1}, \rho^{n^2-n}, 1, \rho^{-1}].$$

It is straightforward to check that the associated linear collineation of $\mathrm{PG}(3, q^2)$ preserves $\mathcal{X}$, and that it induces on π_0 the collineation α associated to the diagonal matrix $[1, \rho^{n^2-n+1}, 1]$. In π_0, the Hermitian curve $\mathcal{H}_0$ of equation (6) is preserved by α which also fixes every common point point of $\mathcal{H}_0$ and the line of equation $Y = 0$. Since α has order $n+1$ but the stabiliser of three collinear points of $\mathcal{H}_0$ has order $(n+1)/3$ when $\gcd(3, n+1) = 3$, it turns out that $\alpha \in \mathrm{PGU}(3, n) \setminus \mathrm{PSU}(3, n)$. Therefore, the group generated by M together with $\tilde{E}$ is larger than M and, when viewed as a collineation group of $\mathrm{PG}(3, q^2)$, it preserves $\mathcal{X}$. This together with Theorem 4.3 and Lemma 4.4 give the following result.

Theorem 4.6. *Let* $\gcd(3, n+1) = 3$. *Then* $\mathrm{Aut}(\mathcal{X})$ *has a normal subgroup* C_{n^2-n+1} *such that* $\mathrm{Aut}(\mathcal{X})/C_{n^2-n+1} \cong \mathrm{PGU}(3, n)$. *In particular,* $|\mathrm{Aut}(\mathcal{X})| = n^3(n^3+1)(n^2-1)(n^2-n+1)$. *Also,* $\mathrm{Aut}(\mathcal{X})$ *is defined over* $\mathbb{F}_{q^2}$ *but it contains a subgroup isomorphic to* $\mathrm{SU}(3, n)$ *defined over* $\mathbb{F}_{n^2}$. *Furthermore,* $\mathrm{Aut}(\mathcal{X})$ *has a subgroup* M *index* 3 *such that* $M \cong \mathrm{SU}(3, n) \times C_{(n^2-n+1)/3}$.

5 Some quotient curves with very large automorphism group

Since $\mathrm{Aut}(\mathcal{X})$ is large, $\mathcal{X}$ produces plenty of quotient curves. Here we limit ourselves to point out that some of these curves $\mathcal{X}_1$ have very large automorphism groups, that is, $|\mathrm{Aut}(\mathcal{X}_1)| > 24g_1^2$ where g_1 is the genus of $\mathcal{X}_1$.

For a divisor d of n^2-n+1, the group C_{n^2-n+1} contains a subgroup C_d of order d. Let $\mathcal{X}_1 = \mathcal{X}/C_d$ the quotient curve of $\mathcal{X}$ with respect to C_d. Since C_d fixes exactly n^3+1 points of $\mathcal{X}$, and C_d is tame, the Hurwitz genus formula gives

$$(n^3+1)(n^2-2) = 2g-2 = d(2g_1-2) + (d-1)(n^3+1),$$

whence

$$g_1 = \frac{1}{2}\left(\frac{(n^3+1)(n^2-d-1)}{d} + 2\right).$$

Furthermore, since C_d is a normal subgroup of $\mathrm{Aut}(\mathcal{X})$, see Theorems 4.5 and 4.6, $\mathrm{Aut}(\mathcal{X})/C_d$ is a subgroup G_1 of $\mathrm{Aut}(\mathcal{X}_1)$ such that

$$|G_1| = \frac{n^3(n^3+1)(n^2-1)(n^2-n+1)}{d}.$$

Comparing $|G_1|$ to g_1 shows that if $d \geq 7$ then $|G_1| > 24g_1^2$.

6 The Weierstrass semigroup at an $\mathbb{F}_{q^2}$-rational place

As we observed in Section 2, $X_\infty = (1,0,0,0)$ is the unique infinite point of $\mathcal{X}$. Our aim is to compute the Weierstrass semigroup $H(X_\infty)$ of $\mathcal{X}$ at X_∞. For this purpose, certain divisors on $\mathcal{X}$ are to consider. From Section 2, the function field $\mathbb{K}(\mathcal{X})$ of $\mathcal{X}$ is $\mathbb{K}(x,y,z)$ with $z^{n^2-n+1} = yL(x)$, $x^n + x = y^{n+1}$. Let (ξ) denote the principal divisor of $\xi \in \mathbb{K}(\mathcal{X})$, $\xi \neq 0$. Note that

$$(x)_\infty = (n^3+1)X_\infty,\ (y)_\infty = (n^3-n^2+n)X_\infty,\ (yh(x))_\infty = (n^3(n^2-n+1))X_\infty,$$

whence $(z)_\infty = n^3X_\infty$.

A useful tool for the study of $H(X_\infty)$ is the concept of a telescopic semigroup, see [25, Section 5.4]. Let $(a_1,\ldots,a_k)$ be a sequence of positive integers with greatest common divisor 1. Define

$$d_i = gcd(a_1,\ldots,a_i) \qquad \text{and} \qquad A_i = \{a_1/d_i,\ldots,a_i/d_i\}$$

for $i = 1,\ldots,k$. Let $d_0 = 0$. If a_i/d_i belongs to the semigroup generated by A_{i-1} for $i = 2,\ldots,k$, then the sequence $(a_1,\ldots,a_k)$ is said to be *telescopic*. A semigroup is called telescopic if it is generated by a telescopic sequence. Recall that the genus of a numerical semigroup Λ is defined as the size of

$\mathbb{N}_0 \setminus \Lambda$. By Proposition 5.35 in [25], the genus of a semigroup Λ generated by a telescopic sequence $(a_1, \dots, a_k)$ is

$$g(\Lambda) = \frac{1}{2}\left(1 + \sum_{i=1}^{k}\left(\frac{d_{i-1}}{d_i} - 1\right) a_i\right) \tag{11}$$

Lemma 6.1. *The genus of the numerical semigroup generated by the three integers $n^3 - n^2 + n, n^3, n^3 + 1$ is*

$$\frac{(n^3+1)(n^2-2)}{2} + 1$$

Proof. The sequence $(n^3 - n^2 + n, n^3, n^3 + 1)$ is telescopic. Then (11) applies, and the claim follows from straightforward computation. □

Proposition 6.2. *The Weierstrass semigroup of F at X_∞ is the subgroup generated by $n^3 - n^2 + n, n^3, n^3 + 1$.*

Proof. The numerical semigroup Λ generated by $n^3 - n^2 + n, n^3, n^3 + 1$ is clearly contained in $H(X_\infty)$. As $g(H(X_\infty)) = g(\Lambda)$, the claim follows. □

As a corollary, we have the following result.

Proposition 6.3. *The order sequence of $\mathcal{X}$ at X_∞ is $(0, 1, n^2-n+1, n^3+1)$.*

Lemma 5.34 in [25] enables us to compute a basis of the linear space $L(mX_\infty)$ for every positive integer m.

Lemma 6.4 (Lemma 5.34 in [25])**.** *If $(a_1, \dots, a_k)$ is telescopic, then for every m in the semigroup generated by $a_1, \dots, a_k$ there exist uniquely determined non-negative integers $j_1, \dots, j_k$ such that $0 \le j_i < \frac{d_{i-1}}{d_i}$ for $i = 2, \dots, k$ and*

$$m = \sum_{i=1}^{k} j_i a_i.$$

Proposition 6.5. *For a positive integer m, a basis of the linear space $L(mX_\infty)$ is*

$$\{y^{j_1} z^{j_2} x^{j_3} \mid j_1(n^3-n^2+n)+j_2 n^3+j_3(n^3+1) \le m, j_i \ge 0, j_2 \le n^2-n, j_3 \le n-1\}.$$

Proof. The result is an immediate consequence of Lemma 6.4. □

References

[1] M. Abdón and A. Garcia, On a characterization of certain maximal curves, *Finite Fields Appl.* **10** (2004), 133–158.

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

[3] M. Abdón and F. Torres, On maximal curves in characteristic two, *Manuscripta Math.* **99** (1999), 39–53.

[4] M. Abdón and F. Torres, On F_{q^2}-maximal curves of genus $\frac{1}{6}(q-3)q$, *Beiträge Algebra Geom.* **46** (2005), 241–260.

[5] E. Çakçak and F. Özbudak, Subfields of the function field of the Deligne–Lusztig curve of Ree type, *Acta Arith.* **115** (2004), 133–180.

[6] E. Çakçak and F. Özbudak, Number of rational places of subfields of the function field of the Deligne–Lusztig curve of Ree type, *Acta Arith.* **120** (2005), 79–106.

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

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

[9] R. Fuhrmann, A. Garcia and F. Torres, On maximal curves, *J. Number Theory* **67**(1) (1997), 29–51.

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

[11] 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.

[12] A. Garcia, Curves over finite fields attaining the Hasse–Weil upper bound, *European Congress of Mathematics*, *Vol. II* (Barcelona, 2000), Progr. Math. **202**, Birkhäuser, Basel, 2001, 199–205.

[13] A. Garcia, On curves with many rational points over finite fields, *Finite Fields with Applications to Coding Theory, Cryptography and Related Areas*, Springer, Berlin, 2002, 152–163.

[14] A. Garcia and H. Stichtenoth, Algebraic function fields over finite fields with many rational places, *IEEE Trans. Inform. Theory* **41** (1995), 1548–1563.

[15] A. Garcia and H. Stichtenoth, On Chebyshev polynomials and maximal curves, *Acta Arith.* **90** (1999), 301–311.

[16] A. Garcia and H. Stichtenoth, A maximal curve which is not a Galois subcover of the Hermitian curve, *Bull. Braz. Math. Soc. (N.S.)* **37** (2006), 139–152.

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

[18] M. Giulietti, J.W.P. Hirschfeld, G. Korchmáros and F. Torres, Curves covered by the Hermitian curve, *Finite Fields Appl.* **12** (2006), 539–564.

[19] M. Giulietti, J.W.P. Hirschfeld, G. Korchmáros and F. Torres, Families of curves covered by the Hermitian curve, *Sémin. Cong.*, to appear.

[20] M. Giulietti, G. Korchmáros and F. Torres, Quotient curves of the Deligne–Lusztig curve of Suzuki type, *Acta Arith.*, **122** (2006), 245–274.

[21] J.P. Hansen, Deligne–Lusztig varieties and group codes, Lecture Notes in Math. **1518**, Springer, Berlin, 1992, 63–81.

[22] J.P. Hansen and H. Stichtenoth, Group codes on certain algebraic curves with many rational points, *Appl. Algebra Eng. Comm. Comput.* **1** (1990), 67–77.

[23] H.-W. Henn, Funktionenkörper mit grosser Automorphismengruppe, *J. Reine Angew. Math.* **302** (1978), 96–115.

[24] J.W.P. Hirschfeld, *Finite Projective Spaces of Three Dimensions*, Oxford Univ. Press, Oxford, 1985, x+316 pp.

[25] T. Høholdt, J. Van Lint, R. Pellikaan, Algebraic geometry codes, in: V.S. Pless, W.C. Huffman (Eds.), *Handbook of Coding Theory*, North-Holland, 1998, pp. 871-961.

[26] G. Korchmáros and F. Torres, Embedding of a maximal curve in a Hermitian variety, *Compositio Math.* **128** (2001), 95–113.

[27] 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.

[28] F. Pasticci, On quotient curves of the Suzuki curve, *Ars Comb.*, to appear.

[29] J.P. Pedersen, A function field related to the Ree group, *Coding Theory and Algebraic Geometry*, Lecture Notes in Math. **1518**, Springer, Berlin, 1992, 122–132.

[30] P. Roquette, Abschätzung der Automorphismenanzahl von Funktionenkörpern bei Primzahlcharakteristik, *Math. Z.* **117** (1970), 157–163.

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

[32] B. Segre, Forme e geometrie hermitiane, con particolare riguardo al caso finito, *Ann. Mat. Pura Appl.* **70** (1965), 1–201.

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

[34] H. Stichtenoth, Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. II. Ein spezieller Typ von Funktionenkörpern, *Arch. Math.* **24** (1973), 615–631.

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

[36] G. van der Geer, Curves over finite fields and codes, *European Congress of Mathematics*, *Vol. II* (Barcelona, 2000), Progr. Math. **202**, Birkhäuser, Basel, 2001, 225–238.

[37] G. van der Geer, Coding theory and algebraic curves over finite fields: a survey and questions, *Applications of Algebraic Geometry to Coding Theory, Physics and Computation*, NATO Sci. Ser. II Math. Phys. Chem. **36**, Kluwer, Dordrecht, 2001, 139–159.