QUOTIENT CURVES OF THE DELIGNE-LUSZTIG CURVE OF SUZUKI TYPE

MASSIMO GIULIETTI, GÁBOR KORCHMÁROS, AND FERNANDO TORRES

ABSTRACT. Inspired by a recent paper of Garcia, Stichtenoth and Xing [2000, *Compositio Math.* **120**, 137–170], we investigate the quotient curves of the Deligne-Lusztig curve associated to the Suzuki group $\mathcal{S}z(q)$.

1. INTRODUCTION

The Deligne-Lusztig curve of Suzuki type (shortly DLS-curve) is the (projective geometrically irreducible, non-singular) algebraic curve defined to be the non-singular model over the finite field $\mathbb{F}_q$ of the (absolutely irreducible) plane curve $\mathcal{C}$ of equation $X^{q_0}(X^q+X)=Y^q+Y$, where $q_0=2^s$, $s\geq 1$ and $q=2q_0^2$. Several authors have studied the DLS-curve also in connection with coding theory, see [4], [5], [11], [12], [13], [14]. Here we only mention that the DLS-curve has genus $g=q_0(q-1)$ and that the number of its $\mathbb{F}_q$-rational points is q^2+1. Actually, the two latter properties characterize the DLS-curve, see [5]. The automorphism group of the DLS-curve is the Suzuki group $\mathcal{S}z(q)$. In this paper, we investigate the quotient curves of the DLS-curve arising from the subgroups of $\mathcal{S}z(q)$. For tame covering, that is for subgroups of odd order, we obtain an exhaustive list of such curves as given in the following theorem.

Theorem 1.1. *Let $\mathcal{X}$ be a tame quotient curve of the DLS-curve. Then one of the following holds.*

I) *r is any divisor of $q-1$, $\mathcal{X}$ has genus $g=\frac{q-1}{r}q_0$ and is a non-singular model over $\mathbb{F}_q$ of the plane curve of equation*

$$Y^{(q-1)/r}\Big(1+\sum_{i=0}^{s-1}X^{2^i(2q_0+1)-(q_0+1)}(1+X)^{2^i}\Big)=(X^{q_0}+1)(Y^{2(q-1)/r}+X^{q-1})\,,$$

MSC: Primary 11G20, Secondary 14G05, 20C20.

Keywords: quotient curve, finite field, rational point, Suzuki group.

This research was supported by Italian Ministry MIUR, project *Strutture Geometriche, Combinatoria e loro applicazioni*, PRIN 2001-2002, and by GNSAGA. The third author was supported by the Grant SB2000-0225 from the "Secretaria de Estado de Educación y Universidades del Ministerio de Educación, Cultura y Deportes de España".

II) *r is any divisor of $q+2q_0+1$, $\mathcal{X}$ has genus $g = \frac{q+2q_0+1}{r}(q_0-1)+1$ and is a non-singular model over $\mathbb{F}_{q^4}$ of the plane curve of equation*

$$Y^{(q+2q_0+1)/r}\left(1+\sum_{i=0}^{s-1} X^{2^i q_0}(1+X)^{2^i(q_0+1)-q_0} + X^{q/2}\right) = X^{q+2q_0+1} + Y^{2(q+2q_0+1)/r},$$

III) *r is any divisor of $q-2q_0+1$, $\mathcal{X}$ has genus $g = \frac{q-2q_0+1}{r}(q_0+1)-1$ and is a non-singular model over $\mathbb{F}_{q^4}$ of the plane curve of equation*

$$bY^{(q-2q_0+1)/r}\left(1+\sum_{i=0}^{s-1} X^{2^i(2q_0+1)-(q_0+1)}(1+X)^{2^i}\right) = (X^{q-2q_0+1}+Y^{2(q-2q_0+1)/r})(X^{q_0-1}+X^{2q_0-1}),$$

where $b = \lambda^{q_0}+\lambda^{q_0-1}+\lambda^{-q_0}+\lambda^{-q_0+1}$ and $\lambda \in \mathbb{F}_{q^4}$ is an element of order $q-2q_0+1$.

A similar complete list for non-tame coverings cannot be produced because the Suzuki group contains a huge number of pairwise non-isomorphic subgroups of even order. Our contribution consists in proving the existence of non-tame quotient curves of the DLS-curve of genus g as given in Theorem 1.2. For some of these curves we also provide a plane equation, see Theorem 1.3.

Theorem 1.2. *Let v, u, r be positive integers. For the following values of g the DLS-curve has a quotient curve $\mathcal{X}$ of genus g.*

i) $g = 2^{s-u+v}(2^{2s+1-v}-1)$, $v \le 2s+1$, $u \le v + \log_2(v+1)$,
ii) $g = \frac{1}{r}2^s(2^{2s+1-v}-1)$, $v \le 2s+1$, $r|(q-1)$, $r|(2^{2s+1-v}-1)$,
iii) $g = \frac{q_0(q-r-1)}{2r}$, $r|(q-1)$,
iv) $g = \frac{q_0(q-1)-1}{r} - (q_0-1)$, $r \mid (q+2q_0+1)$,
v) $g = \frac{q_0(q-1)-1}{r} - (q_0-1)$, $r \mid (q-2q_0+1)$,
vi) $g = \frac{1}{2}\left[\frac{q_0(q-1)-1}{r} - (q_0-1)\right]$, $r|(q+2q_0+1)$,
vii) $g = \frac{1}{2}\left[\frac{q_0(q-1)+1}{r} - (q_0+1)\right]$, $r|(q-2q_0+1)$,
viiii) $g = \frac{1}{4}\left[\frac{q_0(q-1)-1}{r} - (q_0-1)\right]$, $r|(q+2q_0+1)$,
ix) $g = \frac{1}{4}\left[\frac{q_0(q-1)+1}{r} - (q_0+1)\right]$, $r|(q-2q_0+1)$,
x) $g = \frac{q_0(q-1)-1+(\bar{q}^2+1)\bar{q}^2(\bar{q}-1)+\Delta}{(\bar{q}^2+1)\bar{q}^2(\bar{q}-1)}$, $\bar{q} = 2^{2\bar{s}+1}$, $\bar{s}|s$, $(2\bar{s}+1)|(2s+1)$, $\Delta := (\bar{q}^2+1)[(2q_0+2)(\bar{q}-1)+2\bar{q}(\bar{q}-1)] + \bar{q}^2(\bar{q}^2+1)(\bar{q}-2) + \bar{q}^2(\bar{q}+2\bar{q}_0+1)(\bar{q}-1)(\bar{q}-2\bar{q}_0)$,
xi) $g = 2^4(2^{9-v}-1)$, $3 \le v \le 2s+1$, *for* $q = 512$.

Theorem 1.3. i') *For $u = v$, $v|(2s+1)$ a non-singular model over $\mathbb{F}_q$ of the plane curve of equation*

$$X^{2q_0}(X^q+X) = b\sum_{i=0}^{(2s+1/v)-1} Y^{(2^v)^i}$$

is a quotient curve of the DLS-curve of genus g as in i).

ii') *For $u=2$, $v=1$ a non-singular model over $\mathbb{F}_q$ of the plane curve of equation*

$$\sum_{i=0}^{2s} X^{2^i} + \sum_{i=0}^{s} X^{2^i}\Big(\sum_{j=i}^{s} X^{2^j}\Big) + \sum_{i=s+1}^{2s} X^{2^i}\Big(\sum_{j=0}^{i-s-2} X^{2^j}\Big)^{2q_0} = \sum_{i=0}^{2s} Y^{2^i}$$

is a quotient curve of the DLS-curve of genus g as in i).

iii') *A non-singular model over $\mathbb{F}_q$ of the plane curve of equation*

$$1+\sum_{i=0}^{s-1} X^{2^i(2q_0+1)-(q_0+1)}(1+X)^{2^i} = \sum (-1)^{i+j}\frac{(i+j-1)!k}{i!j!}Y^i(X^{rj}(X^{q_0}+1)$$

where the summation is extended over all pairs (i,j) of non–negative integers with $i+2j=(q+2q_0+1)/r$, is a quotient curve of the DLS-curve of genus g as in iii).

iv') *A non-singular model over $\mathbb{F}_{q^4}$ of the plane curve of equation*

$$Y^{(q+2q_0+1)/r}\Big(1+\sum_{i=0}^{s-1} X^{2^i q_0}(1+X)^{2^i(q_0+1)-q_0}+X^{q/2}\Big) = X^{q+2q_0+1}+Y^{2(q+2q_0+1)/r}$$

is a quotient curve of the DLS-curve of genus g as in iv).

v') *Let b as in III). A non-singular model over $\mathbb{F}_{q^4}$ of the plane curve of equation*

$$bY^{\frac{q-2q_0+1}{r}}\Big(1+\sum_{i=0}^{s-1} X^{2^i(2q_0+1)-q_0-1)}(1+X)^{2^i}\Big) = (X^{q-2q_0+1}+Y^{\frac{2(q-2q_0+1)}{r}})(X^{q_0-1}+X^{2q_0-1})$$

is a quotient curve of the DLS-curve of genus g as in v).

vi') *A non-singular model over $\mathbb{F}_{q^4}$ of the plane curve of equation*

$$1+\sum_{i=0}^{s-1} X^{2^i q_0}(1+X)^{2^i(q_0+1)-q_0}+X^{q/2} = \sum (-1)^{i+j}\frac{(i+j-1)!}{i!j!}X^{ri}Y^j$$

is a quotient curve of the DLS-curve of genus g as in vi).

vii') *Let b be as in III). A non-singular model over $\mathbb{F}_{q^4}$ of the plane curve of equation*

$$b\Big(1+\sum_{i=0}^{s-1} X^{2^i(2q_0+1)-(q_0+1)}(1+X)^{2^i}\Big) = (X^{q_0-1}+X^{2q_0-1})\sum (-1)^{i+j}\frac{(i+j-1)!}{i!j!}X^{ri}Y^j$$

where the summation is extended over all pairs (i,j) of non–negative integers with $i+2j=(q+2q_0+1)/r$, is a quotient curve of the DLS-curve of genus g as in vii).

A motivation for the present work comes from the current interest in curves over finite fields with many rational points, see van der Geer's survey [7]. Indeed, the number of $\mathbb{F}_q$-rational points of a curve of genus g which is $\mathbb{F}_q$-covered by the DLS-curve is $N=1+q+2q_0g$ (see Proposition 3.1) and this value is in the interval from which the entries of the tables of curves with many rational points are taken for $g\le 50$, $q\le 128$ in [10]. Especially, both III) and v) for $q=32$, $r=5$ provide new entries, namely $g=10$, $N=113$, and $g=24$, $N=225$, and hence they imply $N_{32}(10)\ge 113$, $N_{32}(24)\ge 225$. Furthermore, the following table shows those values of (q,g) for which some of the curves in the above theorems attain the largest value of $\mathbb{F}_q$-rational points for which an $\mathbb{F}_q$-rational curve of genus g is previously known to exist.

(q,g)	N	Conditions	References
$(8,6)$	33	i) with $v=1$, $u=1$	[21]
$(32,12)$	129	i) with $v=3$, $u=4$	[8]
$(32,28)$	257	i) with $v=2$, $u=3$	[8]
$(32,30)$	273	i) with $v=1$, $u=2$	[8]
$(128,8)$	257	I) with $r=127$, or II) with $r=145$, or III) with $r=113$, or i) with $v=6$, $u=6$	[25]
$(128,14)$	353	i) with $v=4$, $u=6$, or iv) with $r=29$	[9]
$(128,24)$	513	i) with $v=5$, $u=5$	[8]
$(128,28)$	577	i) with $v=4$, $u=5$	[8]
$(128,30)$	609	i) with $v=3$, $u=5$	[9]

2. Preliminary results on the Suzuki group $\mathcal{S}z(q)$

The Suzuki group $\mathcal{S}z(q)$ has been the subject of numerous papers in finite geometry and permutation group theory. Here, we only summarise those results on the structure of $\mathcal{S}z(q)$ which play a role in the present work. For more details, the reader is referred to [16, Chapter XI.3], [19], and [24].

Result 2.1. *Let $q_0 = 2^s$, $s \geq 1$, and $q = 2q_0^2$. For $a, c \in \mathbb{F}_q$, let*

$$\widetilde{T}_{a,c} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ c & a^{2q_0} & 1 & 0 \\ ac + a^{2q_0+2} + c^{2q_0} & a^{2q_0+1} + c & a & 1 \end{pmatrix}.$$

The set $\widetilde{\mathbf{T}} = \{\widetilde{T}_{a,c} | a, c \in \mathbb{F}_q\}$ is a group of exponent 4, class 2 and order q^2. For any $b \in \mathbb{F}_q$ with $b \neq 0$, $\widetilde{\mathbf{T}}$ is isomorphic to the 2-dimensional linear group over $\mathbb{F}_q$ consisting of all linear transformation $(X,Y) \mapsto (X+a, b^{-1}a^{2q_0}X + Y + b^{-1}c)$ with a, c ranging over $\mathbb{F}_q$. In particular, the center $Z(\widetilde{\mathbf{T}})$ is an elementary abelian group of order 2^{2s+1} whose non–trivial elements are those of order 2 of $\widetilde{\mathbf{T}}$.

Result 2.2. *For $d \in \mathbb{F}_q$ and $d \neq 0$, let*

$$\widetilde{N}_d := \begin{pmatrix} d^{-q_0-1} & 0 & 0 & 0 \\ 0 & d^{-q_0} & 0 & 0 \\ 0 & 0 & d^{q_0} & 0 \\ 0 & 0 & 0 & d^{q_0+1} \end{pmatrix},$$

The set $\widetilde{\mathbf{N}} = \{\widetilde{N}_d | d \in \mathbb{F}_q, d \neq 0\}$ *is a group of order* $q-1$, *isomorphic to the multiplicative group of* $\mathbb{F}_q$. *Furthermore,* $\widetilde{\mathbf{N}}$ *normalises* $\widetilde{\mathbf{T}}$ *and induces a fixed point free automorphism on* $\widetilde{\mathbf{T}}$ *such that* $\widetilde{\mathbf{T}}\widetilde{\mathbf{N}}$ *is a Frobenius group with kernel* $\widetilde{\mathbf{T}}$.

Let

$$\widetilde{W} := \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

The Suzuki group $\mathcal{S}z(q)$ is defined as the 4-dimensional linear group generated by $\widetilde{\mathbf{T}}, \widetilde{\mathbf{N}}$ and $\widetilde{W}$, and the normaliser $N_{\mathcal{S}z(q)}(\widetilde{\mathbf{N}})$ is the dihedral group generated by $\widetilde{\mathbf{N}}$ together with $\widetilde{W}$. Since $\mathcal{S}z(q)$ is a simple group, $\mathcal{S}z(q)$ faithfully induces a linear collineation group of the 3-dimensional projective space $\mathbf{P}^3(\mathbb{F}_q)$. It turns out that $\mathcal{S}z(q)$ preserves the ovoid $\mathcal{O}_3$ of $\mathbf{P}^3(\mathbb{F}_q)$ consisting of the points $(0:0:0:1)$ and $(1:x:y:xy+x^{2q_0+1}+y^{2q_0})$ with x, y ranging over $\mathbb{F}_q$. More precisely, $\mathcal{S}z(q)$ is faithfully represented on $\mathcal{O}_3$ as a 2-transitive permutation group of Zassenhaus type of order $(q^2+1)q^2(q-1)$. The stabiliser of the point $(0:0:0:1)$ under $\mathcal{S}z(q)$ is the Frobenius group $\widetilde{\mathbf{T}}\widetilde{\mathbf{N}}$. Furthermore, $\mathcal{S}z(q)$ contains two conjugacy classes of subgroups of Singer type, one consisting of cyclic subgroups $\widetilde{\mathbf{D}}^+$ of order $q+2q_0+1$ and the other of cyclic subgroups $\widetilde{\mathbf{D}}^-$ of order $q-2q_0+1$. The normaliser $N_{\mathcal{S}z(q)}(\widetilde{\mathbf{D}}^+)$ has order $4(q+2q_0+1)$ and is the semidirect product of $\widetilde{\mathbf{D}}^+$ by a cyclic group of order 4. In particular, $N_{\mathcal{S}z(q)}(\widetilde{\mathbf{D}}^+)$ is a Frobenius group with Frobenius kernel $\widetilde{\mathbf{D}}^+$. All these results hold true for $\widetilde{\mathbf{D}}^-$.

Result 2.3. *The conjugates of the above subgroups, namely* $\widetilde{\mathbf{T}}, \widetilde{\mathbf{N}}, \widetilde{\mathbf{D}}^+$, *and* $\widetilde{\mathbf{D}}^-$, *form a partition of* $\mathcal{S}z(q)$. *If* $c(G)$ *denotes the number of conjugates of a subgroup* G, *then* $c(\widetilde{\mathbf{T}}) = q^2+1$, $c(\widetilde{\mathbf{N}}) = \frac{1}{2}q^2(q^2+1)$, $c(\widetilde{\mathbf{D}}^+) = \frac{1}{4}q^2(q-2q_0+1)(q-1)$ *and* $c(\widetilde{\mathbf{D}}^-) = \frac{1}{4}q^2(q+2q_0+1)(q-1)$.

In some cases, $\mathcal{S}z(q)$ contains subgroups isomorphic to the Suzuki group over a subfield $\mathbb{F}_{\bar{q}}$ of $\mathbb{F}_q$. This occurs if and only if $\bar{q} = 2^{2\bar{s}+1}$ with a divisor $\bar{s}$ of s such that $2\bar{s}+1$ divides $2s+1$. For such a $\bar{q}$, there is just one conjugacy class in $\mathcal{S}z(q)$.

Result 2.4. *Any subgroup of* $\mathcal{S}z(q)$ *is conjugate to either to* $\mathcal{S}z(\bar{q})$, *or to a subgroup of one of the following groups*: $\widetilde{\mathbf{T}}\widetilde{\mathbf{N}}$, $N_{\mathcal{S}z(q)}(\widetilde{\mathbf{N}})$, $N_{\mathcal{S}z(q)}(\widetilde{\mathbf{D}}^+)$, $N_{\mathcal{S}z(q)}(\widetilde{\mathbf{D}}^-)$.

In studying $\mathcal{S}z(q)$ as an automorphism group of the DLS-curve, we will need a suitable representation of $\mathcal{S}z(q)$ as a linear collineation group of $\mathbf{P}^4(\mathbb{F}_q)$.

Result 2.5. *For $a, c \in \mathbb{F}_q$, let*

$$T_{a,c} := \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ a & 1 & 0 & 0 & 0 \\ a^{q_0+1} + c^{q_0} & a^{q_0} & 1 & 0 & 0 \\ c & a^{2q_0} & 0 & 1 & 0 \\ ac + a^{2q_0+2} + c^{2q_0} & a^{2q_0+1} + c & 0 & a & 1 \end{pmatrix}.$$

For $d \in \mathbb{F}_q$ with $d \neq 0$, let

$$N_d := \begin{pmatrix} d^{-q_0-1} & 0 & 0 & 0 & 0 \\ 0 & d^{-q_0} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & d^{q_0} & 0 \\ 0 & 0 & 0 & 0 & d^{q_0+1} \end{pmatrix}, \qquad W := \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Let $[T_{a,c}]$, $[N_d]$, and $[W]$ be the linear collineations of $\mathbf{P}^4(\mathbb{F}_q)$ associated to $T_{a,c}$, N_d, and W, respectively. Then the group $[\mathcal{G}]$ generated by them is isomorphic to $\mathcal{S}z(q)$. Let

$$\mathcal{O}_4 = \{(1 : u : u^{q_0+1} + v^{q_0}y^{q_0} : bv : buv + u^{2q_0+2} + b^{2q_0}v^{2q_0}) | u, v \in \mathbb{F}_q\} \cup \{(0:0:0:0:1)\}.$$

Then $[\mathcal{G}]$ preserves $\mathcal{O}_4$ and acts on it as $\mathcal{S}z(q)$ in its unique 2-transitive permutation representation. The full collineation group of $\mathbf{P}^4(\mathbb{F}_q)$ preserving $\mathcal{O}_4$ is isomorphic to $\mathrm{Aut}(\mathcal{S}z(q))$ *and is the semidirect product of $[\mathcal{G}]$ by the non-linear group $[\mathcal{F}]$ of order $2s+1$ of $\mathbf{P}^4(\mathbb{F}_q)$ generated by the collineation $(X_0 : X_1 : X_2 : X_3 : X_4) \mapsto (X_0^2 : X_1^2 : X_2^2 : X_3^2 : X_4^2)$.*

Proof. Let $[\mathcal{G}]$ be the linear collineation group of $\mathbf{P}^4(\mathbb{F}_q)$ generated by $[T_{a,c}], [N_d]$ and $[W]$, with a, c, d ranging in f_q and $d \neq 0$. Then $[\mathcal{G}]$ preserves the set $\mathcal{O}_4$ consisting of the points $(1 : x : x^{q_0+1} + b^{q_0}y^{q_0} : by : bxy + x^{2q_0+2} + b^{2q_0}y^{2q_0})$ and $(0:0:0:0:1)$. Following the method used for the explicit construction of $\mathcal{S}z(q)$ in [19, Chapter IV] one can extend Tits' result to $[\mathcal{G}]$, see [19, Theorem 21.8]: $[\mathcal{G}]$ acts doubly transitively on $\mathcal{O}_4$; if $[G] \in [\mathcal{G}]$, then either $[G] = [N_d][T_{a,c}]$ for exactly one triple (d, a, c) with $d(\neq 0), a, c \in \mathbb{F}_q$, or $[G] = [N_d][T_{a,c}][W][T_{e,f}]$, for exactly one quintuple $(d, a, c, e, f) \in \mathbb{F}_q$, with $d(\neq 0), a, c, e, f \in \mathbb{F}_q$. Also, Theorem 21.11 and the Suzuki Tits Theorem 22.6 in [19] hold true: $[\mathcal{G}]$ is a simple group of order $q^2(q^2+1)(q-1)$. This implies that $[\mathcal{G}] \cong \mathcal{S}z(q)$. We remark that the image of $[G] \in [\mathcal{G}]$ under such an isomorphism can be easily obtained by deleting the third row and the third column of G. Since the non-linear collineation $F : (X_0 : X_1 : X_2 : X_3 : X_4) \mapsto (X_0^2 : X_1^2 : X_2^2 : X_3^2 : X_4^2)$ preserves $\mathcal{O}_4$, we have to prove that every collineation h of $\mathbf{P}^4(\mathbb{F}_q)$ preserving $\mathcal{O}_4$ is in $[\mathcal{H}][\mathcal{F}] \cong \mathrm{Aut}(\mathcal{S}z(q))$. If h fixes $\mathcal{O}_4$ pointwise, then h is the identity because $\mathcal{O}_4$ is not contained in any proper subspace of $\mathbf{P}^4(\mathbb{F}_q)$. Thus h acts on $\mathcal{O}_4$ faithfully. On the other hand, from the classification of finite 2-transitive permutation groups it follows that there are only three permutation groups of degree q^2+1 containing $\mathcal{S}z(q)$, namely $\mathrm{Aut}(\mathcal{S}z(q))$, Alt_{q^2+1} and Sym_{q^2+1}. It remains to show that the two latter cases cannot actually occur in our situation. Take six points on $\mathcal{O}_4$ no five of them linearly dependent in $\mathbf{P}^4(\mathbb{F}_q)$. By the fundamental theorem of projective geometry, the group generated by F is the collineation group of $\mathbf{P}^4(\mathbb{F}_q)$ fixing each of these six points. On the other hand, the stabilizer of six objects in Alt_n with $n \geq 10$ is not a cyclic group. This proves the assertion. $\square$

Remark 2.6. From now on we will use the term of Suzuki group and the symbol $\mathcal{S}z(q)$ to denote the four dimensional projective linear group introduced in Result 2.5. In particular, $\mathbf{T}, \mathbf{N}, \mathbf{D}^+, \mathbf{D}^-$ will stand for the corresponding subgroups $\widetilde{\mathbf{T}}, \widetilde{\mathbf{N}}, \widetilde{\mathbf{D}}^+, \widetilde{\mathbf{D}}^-$ under the isomorphism stated in Result 2.5.

3. Preliminary results on the DLS-curve

Throughout the present paper $\mathcal{X}$ will stand for the DLS-curve over $\mathbb{F}_q$. As we have mentioned in the Introduction $\mathcal{X}$ has genus $q_0(q-1)$ and contains exactly q^2+1 $\mathbb{F}_q$-rational points. By the Serre-Weil explicit formulae (see [20], [11]), the characteristic polynomial $h_{\mathcal{X}}(t)$ of the Frobenius morphism over $\mathbb{F}_q$ on the Jacobian variety of $\mathcal{X}$ is $(t^2+2q_0t+q)^{q_0(q-1)}$. Given a curve $\mathcal{Y}$ of genus g which is $\mathbb{F}_q$-covered by $\mathcal{X}$, Lachaud's theorem [18] implies that $h_{\mathcal{Y}}(t) = (t^2+2q_0t+q)^g$. By [22, V.1], the following proposition follows.

Proposition 3.1. *Let $\mathcal{Y}$ be a curve which is $\mathbb{F}_q$-covered by $\mathcal{X}$. Then the number of $\mathbb{F}_q$-rational points of $\mathcal{Y}$ is equal to $1+q+2gq_0$, where g is the genus of $\mathcal{Y}$.*

Remark 3.2. Let $\mathcal{Y}$ be a curve as in the previous proposition. One can show then that $\#\mathcal{Y}(\mathbb{F}_{q^2}) = 1+q^2, \#\mathcal{Y}(\mathbb{F}_{q^3}) = 1+q^3-2gq_0q$ and $\#\mathcal{Y}(\mathbb{F}_{q^4}) = 1+q^4+2gq^2$; i.e., $\mathcal{Y}$ is maximal over $\mathbb{F}_{q^4}$. As a matter of fact, the examples obtained so far in this paper give new insights toward the computation of the spectrum of genera of maximal curves over finite fields of characteristic two (compare with the examples in [6], [2], [3] and [1]).

The proposition below will be useful in the sequel.

Proposition 3.3. *For any $b \in \mathbb{F}_q$, $b \neq 0$, there are elements $x, y \in \mathbb{F}_q(\mathcal{X})$ such that*

$$\mathbb{F}_q(\mathcal{X}) = \mathbb{F}_q(x,y), \quad x^{2q_0}(x^q+x) = b(y^q+y).$$

Proof. We have $\mathbb{F}_q(\mathcal{X}) = \mathbb{F}_q(x,t)$ with $x^{q_0}(x^q+x) = t^q+t$. Let $y = b^{-1}(x^{2q_0+1}+t^{2q_0})$, that is $t^q = b^{q_0}y_0^q + x^{q+q_0}$. Then $\mathbb{F}_q(\mathcal{X}) = \mathbb{F}_q(x,y)$. Furthermore, $y^{q_0} = b^{-q_0}(x^{q+q_0}+t^q) = b^{-q_0}(x^{q_0+1}+t)$, and hence $y^q = b^{-1}(x^{q+q_0}+t^{2q_0})$. Now, since $y^q+y = b^{-1}(x^{q+q_0}+t^{2q_0}+x^{2q_0+1}+t^{2q_0}) = b^{-1}x^{2q_0}(x^q+x)$, the claim follows. $\square$

Let $\mathcal{C}_b$ be the plane curve of equation $X^{2q_0}(X^q+X) = b(Y^q+Y)$. $\mathcal{C}_b$ has only one singular point, namely the infinite point Y_∞ of the Y-axis which point is a q_0-fold point. We know from [13] that $\bar{\mathbb{F}}_q(\mathcal{X})$ has just one place centered at Y_∞. Let P_∞ denote the corresponding point of $\mathcal{X}$. From now on, we fix a projective frame $A_0A_1A_2A_3A_4U$ in

$\mathbf{P}^4(\bar{\mathbb{F}}_q)$ with fundamental vertices $A_0 := (1:0:0:0:0), \ldots, A_4 := (0:0:0:0:1)$, and $U := (1:1:1:1:1)$. With the notation of Proposition 3.3, let f be the morphism $f : \mathcal{X} \to \mathbf{P}^4(\bar{\mathbb{F}}_q)$ with coordinate functions

$$f := (f_0 : f_1 : f_2 : f_3 : f_4)\,,$$

such that $f_0 := 1$, $f_1 := x$, $f_2 := x^{q_0+1} + b^{q_0}y^{q_0}$, $f_3 := by$, $f_4 := bxy + x^{2q_0+2} + b^{2q_0}y^{2q_0}$. They are uniquely determined by f up to a proportionality factor in $\bar{\mathbb{F}}_q(\mathcal{X})$. For each point $P \in \mathcal{X}$, we have $f(P) = ((t^{-e_P}f_0)(P), \ldots, t^{-e_P}f_4)(P))$ where $e_P = -\min\{v_P(f_0), \ldots, v_P(f_4)\}$ for a local parameter t of $\mathcal{X}$ at P. It turns out that $f(\mathcal{X})$ is a parametrised curve not contained in any hyperplane of $\mathbf{P}^4(\bar{\mathbb{F}}_q)$. For a point $P \in f(\mathcal{X})$, the intersection multiplicity of $f(\mathcal{X})$ with a hyperplane H of equation $a_0X_0 + \ldots + a_4X_4 = 0$ is $v_P(a_0f_0 + \ldots + a_4f_4) + e_P$, and the intersection divisor $f^{-1}(H)$ cut out on $f(\mathcal{X})$ by H is defined to be $f^{-1}(H) = \operatorname{div}(a_0f_0 + \ldots + a_4f_4) + E$ with $E = \sum e_pP$. We have $v_{P_\infty}(f_1) = -q$, $v_{P_\infty}(f_3) = -2q_0 - q$, $v_{P_\infty}(f_2) = -q_0 - q$, $v_{P_\infty}(f_4) = -2q_0 - q - 1$, see Section 6 . Then $e_{P_\infty} = q + 2q_0 + 1$, and the representative $(f_0/f_4 : f_1/f_4 : f_2/f_4 : f_3/f_4 : 1)$ of f is defined on P_∞. Hence $f(P_\infty) = A_4$, and f_3/f_4 is a local parameter at P_∞. For a point $P \in \mathcal{X}$, an integer j is called a hermitian P-invariant (cf. [23]) if there exists a hyperplane intersecting $f(\mathcal{X})$ at $f(P)$ with multiplicity j. There are exactly five pairwise distinct hermitian P-invariants. Such integers arranged in increasing order define the order sequence of $\mathcal{X}$ at P. By [5], the order sequence of $\mathcal{X}$ at a point $P \in \mathcal{X}$ is either $(0, 1, q_0 + 1, 2q_0 + 1, q + 2q_0 + 1)$ or $(0, 1, q_0, 2q_0, q)$ according as $P \in \mathcal{X}(\mathbb{F}_q)$ or $P \notin \mathcal{X}(\mathbb{F}_q)$. The linear system

$$\{f^{-1}(H) \mid H \text{ hyperplane in } P^4(\bar{\mathbb{F}}_q)\}$$

is $|(q + 2q_0 + 1)P_0|$ for $P_0 \in \mathcal{X}(\mathbb{F}_q)$. Also, $(q + 2q_0 + 1)P \sim qP + 2q_0\mathbf{F}r(P) + \mathbf{F}r^2(P)$ for every $P \in \mathcal{X}$, where $\mathbf{F}r$ is the Frobenius morphism over $\mathbb{F}_q$; see [5].

Proposition 3.4. *$f(\mathcal{X})$ is a non-singular model defined over $\mathbb{F}_q$ of the DLS curve.*

Proof. We show that f is a closed embedding. By the above discussion, f is bijective and $f(\mathcal{X})$ has no singular point. □

According to Proposition 3.4, we will identify $f(\mathcal{X})$ with $\mathcal{X}$.

Proposition 3.5. *The automorphism group $\operatorname{Aut}(\mathcal{X})$ of $\mathcal{X}$ is isomorphic to $\mathcal{S}z(q)$ and acts on $\mathcal{X}(\mathbb{F}_q)$ as $\mathcal{S}z(q)$ in its unique 2-transitive permutation representation.*

Proof. For $a, c, d \in \mathbb{F}_q$ with $d \neq 0$, we define the following automorphisms of $\mathbb{F}_q(\mathcal{X})$:

$$\psi_{a,c} := \begin{cases} x \mapsto x + a, \\ y \mapsto b^{-1}a^{2q_0}x + y + b^{-1}c; \end{cases} \qquad \gamma_d := \begin{cases} x \mapsto dx, \\ y \mapsto d^{2q_0+1}y; \end{cases} \tag{3.1}$$

for $h := bxy + x^{2q_0+2} + b^{2q_0}y^{2q_0}$,

$$\varphi := \begin{cases} x \mapsto by/h, \\ y \mapsto bx/h. \end{cases} \tag{3.2}$$

Let Γ be the automorphism group of $\bar{\mathbb{F}}_q(\mathcal{X})$ generated by $\psi_{a,c}$, γ_d and φ. By straightforward computations, $[W]f = f\varphi$, $[N_d]f = f\gamma_d$ and $[T_{a,c}]f = f\psi_{a,c}$. This shows that there is a homomorphism $\Gamma \mapsto \mathcal{S}z(q)$. Actually, this homomorphism is an isomorphism because the identity is the only automorphism of $\bar{\mathbb{F}}_q(\mathcal{X})$ which acts as the identity map on the set of all places of $\bar{\mathbb{F}}_q(\mathcal{X})$, or, equivalently, on the set of all points of $\mathcal{X}$. Result 2.5 yields $\mathrm{Aut}_{\mathbb{F}_q}(\mathcal{X}) \cong \mathcal{S}z(q)$. Thus, $\Gamma = \mathrm{Aut}_{\mathbb{F}_q}(\mathcal{X})$. Finally, $\mathrm{Aut}_{\mathbb{F}_q}(\mathcal{X}) = \mathrm{Aut}(\mathcal{X})$ by [14]. □

Remark 3.6. For the rest of the paper, $\mathcal{X} = f(\mathcal{X})$ is chosen for a non-singular model over $\mathbb{F}_q$ of the DLS-curve. Then $\mathrm{Aut}(\mathcal{X}) \cong \mathcal{S}z(q)$, and $\mathrm{Aut}(\mathcal{X})$ acts on the set of places of $\bar{\mathbb{F}}_q(\mathcal{X})$ as $\mathcal{S}z(q)$ on the set of points of $\mathcal{X}$. In particular, $\psi_{a,c}$, γ_d, and φ correspond to $[T_{a,c}]$, $[N_d]$ and $[W]$ under such an isomorphism.

4. Quotient curves arising from subgroups of a cyclic subgroup of $\mathcal{S}z(q)$ of order $q-1$

For a divisor $r > 1$ of $q-1$, let $\mathcal{U}$ be a subgroup of $\mathcal{S}z(q)$ of order r. Up to conjugacy in $\mathcal{S}z(q)$, we have $\mathcal{U} = \{N_d | d^r = 1\}$. It is straightforward to check that $\mathcal{U}$ has exactly two fixed points on $\mathcal{X}$, namely A_0 and A_4. Let $\mathcal{X}_\mathcal{U}$ denote the quotient curve of $\mathcal{X}$ associated to $\mathcal{U}$, and let $g_\mathcal{U}$ be its genus. Since $\mathcal{U}$ is a tame subgroup, the Hurwitz genus formula gives $2q_0(q-1)-2 = r(2g_\mathcal{U}-2)+2(r-1)$, whence $g_\mathcal{U} = \frac{1}{r}q_0(q-1)$. To find an explicit equation of $\mathcal{X}_\mathcal{U}$ we first determine a plane (singular) model of $\mathcal{X}$ on which not only $\mathbf{N}$ but also $[W]$ acts linearly. For every non-zero element d in $\mathbb{F}_q$, both $[N_d]$ and $[W]$ preserve the line ℓ joining A_0 and A_4, as well as the plane α spanned by the other three fundamental points, namely A_1, A_2, and A_3. Now, project $\mathcal{X}$ from ℓ to α. The associated morphism $\mathcal{X} \to \mathbf{P}^2(\bar{\mathbb{F}}_q)$ is $\pi_\ell : (1 : x : x^{q_0+1} + b^{q_0}y^{q_0} : by : bxy + x^{2q_0+2} + b^{2q_0}y^{2q_0}) \mapsto (x : x^{q_0+1} + b^{q_0}y^{q_0} : by)$. In terms of linear systems, π_ℓ is associated to the 2-dimensional linear series cut out on $\mathcal{X}$ by hyperplanes through ℓ. We will need some computational results.

$$v_P(x) = \begin{cases} 1 & \text{for } P = (1 : 0 : (bc)^{q_0} : bc : (bc)^{2q_0}) \text{ with } c \in \mathbb{F}_q \setminus \{0\}, \\ 1 & \text{for } P = A_0, \\ -q & \text{for } P = A_4, \\ 0 & \text{otherwise.} \end{cases} \tag{4.1}$$

$$v_P(by) = \begin{cases} 1 & \text{for } P = (1 : a : a^{q_0+1} : 0 : a^{2q_0+2}) \text{ with } a \in \mathbb{F}_q \setminus \{0\}, \\ 2q_0+1 & \text{for } P = A_0, \\ -2q_0-q & \text{for } P = A_4, \\ 0 & \text{otherwise.} \end{cases} \tag{4.2}$$

(4.3)
$$v_P(x^{q_0+1}+(by)^{q_0}) = \begin{cases} 1 & \text{for } P=(1:a:0:a^{2q_0+1}:a^{2q_0+2}), a\in\mathbb{F}_q\setminus\{0\},\\ q_0+1 & \text{for } P=A_0,\\ -q_0-q & \text{for } \ P=A_4,\\ 0 & \text{otherwise.}\end{cases}$$

(4.4)
$$v_P(x+by) \ = \begin{cases} 1 & \text{for } P=(1:a:a^{q_0+1}+a^{q_0}:a:a^{2q_0+2}) \text{ with } a\in\mathbb{F}_q\setminus\{0,1\},\\ 2q_0+1 & \text{for } P=(1:1:0:1:1),\\ 1 & \text{for } P=A_0,\\ -2q_0-q & \text{for } P=A_4,\\ 0 & \text{otherwise.}\end{cases}$$

For $e'_P := -\min\{v_P(x), v_P(x^{q_0+1}+(by)^{q_0}), v_P(by)\}$,

$$e'_P \ = \begin{cases} -1 & \text{for } A_0,\\ q+2q_0 & \text{for } P=A_4,\\ 0 & \text{otherwise.}\end{cases} \tag{4.5}$$

Proof. Notice that $t := x$ is a local parameter at A_0. From $x^{2q_0}(x^q+x) = by^q+by$, we have $y = b^{-1}t^{2q_0+1}+b^{-1}t^{q+2q_0}+\ldots$, and hence $x+by = t+t^{2q_0+1}+\ldots$, and $x^{q_0+1}+(by)^{q_0} = t^{q_0+1}+t^{q+q_0}+\ldots$ whence the above results for A_0 follow. Also, $v_{A_0}(h) = q+2q_0+1$ where $h = bxy+x^{2q_0+2}+(by)^{2q_0}$. Since the involutory automorphism $[W]$ of $\mathcal{X}$ changes A_0 with A_4, and acts on $\bar{\mathbf{F}}_q(\mathcal{X})$ as (3.2), we have $v_{A_4}(x) = v_{A_0}(by/h) = -q$, $v_{A_4}(by) = v_{A_0}(bx/h) = -2q_0-q$, $v_{A_4}(x^{q_0+1}+(by)^{q_0}) = v_{A_0}((by/h)^{q_0+1}+(bx/h)^{q_0}) = -q_0-q$, and $v_{A_4}(x+by) = v_{A_0}(by/h+x/h) = v_{A_0}(x+by)-v_{A_0}(h) = -2q_0-q$.So, the above results for A_4 hold. Now, we assume $A_0\neq P\neq A_4$, that is $P = (1:a:a^{q_0+1}+(bc)^{q_0}:bc:abc+a^{2q_0+2}+(bc)^{2q_0})$ with $a^{2q_0+q}+a^{2q_0+1} = (bc)^q+bc$ and either $a\neq 0$, or $a=0$ and $c\in\mathbb{F}_q\setminus\{0\}$. In the latter case, $t := x$ is a local parameter and the local expansions of the coordinate functions of π_ℓ are

$$x=t,\quad x^{q_0+1}+b^{q_0}y^{q_0} = (bc)^{q_0}+t^{q_0+1}+\ldots,\quad by = bc+t^{2q_0+1}+\ldots.$$

Hence $v_P(x) = 1$, but $v_P(by) = 0$. Also, $v_P(x^{q_0+1}+(by)^{q_0}) = 0 = v_P(x+by)$. We have to investigate the case $a\neq 0$. Since $t := x+a$ is a local parameter, we have $x = a+t, y = c+\alpha t+\beta t^i+\ldots$ for some $i>1$ and $\beta\neq 0$. From $x^{2q_0}(x^q+x) = (by)^q+by$ we deduce that $\alpha\neq 0$ and that either $i = 2q_0+1$ or $i = 2q_0$ according as a belongs to $\mathbb{F}_q$ or does not. Hence the local expansions of the coordinate functions of π_ℓ are

$$x=a+t,\quad x^{q_0+1}+b^{q_0}y^{q_0} = a^{q_0+1}+(bc)^{q_0}+a^{q_0}t+\ldots,\quad by = bc+a^{2q_0}t+t^{2q_0+1}+\ldots$$

for $a\in\mathbb{F}_q\setminus\{0\}$, and

$$x=a+t,\quad x^{q_0+1}+b^{q_0}y^{q_0} = a^{q_0+1}+(bc)^{q_0}+a^{q_0}t+\ldots,\quad by = bc+a^{2q_0}t+(a^q+a)t^{2q_0}+\ldots$$

for $a \notin \mathbb{F}_q$. Thus $v_P(x) = 0$. Furthermore, $v_P(by) \neq 0$ if and only if $c = 0$. More precisely, this only occurs when $a \in \mathbb{F}_q \setminus \{0\}$, $P = (a : a^{q_0+1} : a^{q_0} : 0 : a^{2q_0+2})$, and $v_P(by) = 1$. Also, $v_P(x^{q_0+1} + y^{q_0}) \neq 0$ if and only if $a^{q_0+1} + (cb)^{q_0} = 0$. This condition is only satisfied by $a \in \mathbb{F}_q$. In fact, $a^{q_0+1} = (cb)^{q_0}$ together with $a^{2q_0}(a^q + a) = (cb)^q + cb$ implies $cb = a^{2q_0+1}$ and hence $a^q = a$. For $a \in \mathbb{F}_q \setminus \{0\}$, we have $P = (1 : a : 0 : a^{2q_0+1} : a^{2q_0+2})$ and $v_P(x^{q_0+1} + y^{q_0}) = 1$. Moreover, $v_P(x + by) \neq 0$ if and only if $a + bc = 0$, that is $a \in \mathbb{F}_q \setminus \{0\}$ and $P := (1 : a : a^{q_0+1} + a^{q_0} : a : a^{2q_0+2})$. More precisely, either $v_P(x + by) = 1$, or $v_P(x + by) = 2q_0 + 1$ according as $a \in \mathbb{F}_q \setminus \{0, 1\}$ or $a = 1$. Finally, the formula for e'_P follows from (4.1) and (4.2) together with (4.3). $\square$

The homogeneous coordinates $(X'_1 : X'_2 : X'_3)$ provide a natural projective frame in α with fundamental triangle $A_1A_2A_3$.

Lemma 4.1. *The plane curve $\pi_\ell(\mathcal{X})$ is birationally $\mathbb{F}_q$-isomorphic to $\mathcal{X}$ and it has degree $q + 2q_0 - 1$. The action of $[N_d]$ on $\pi_\ell(\mathcal{X})$ is induced by the linear automorphism $(X'_1 : X'_2 : X'_3) \mapsto (d^{-q_0}X'_1 : X'_2 : d^{q_0}X'_3)$, whereas the action of $[W]$ by $(X'_1 : X'_2 : X'_3) \mapsto (X'_3 : X'_2 : X'_1)$.*

Proof. Let $P := (1 : 1 : 1 : 0 : 1)$, $Q := (1 : u : u^{q_0+1} + b^{q_0}v^{q_0} : bv : buv + u^{2q_0+2} + b^{2q_0}v^{2q_0})$ be two points on $\mathcal{X}$ such that $\pi_\ell(Q) = \pi_\ell(P)$. A straightforward computation yields $Q = P$. Moreover, $by/(x^{q_0+1} + b^{q_0}y^{q_0})$ is a local parameter at P as $v_P(x) = 0$ and $v_P(y) = 1$. This implies that π_ℓ is birational. The second assertion follows from (4.5) by virtue of $\deg(\pi_\ell(\mathcal{X})) = \sum e'_P$. The third assertion is easily deduced from the matrix representations of $[N_d]$ and $[W]$. $\square$

To write an equation of $\pi_\ell(\mathcal{X})$ we will use in α the affine frame (X', Y') arising from the above projective frame $(X'_1 : X'_2 : X'_3)$ by $X' = X'_1/X'_2$, and $Y' = X'_3/X'_2$. Then $\pi_\ell(\mathcal{X})$ has equation $F(X', Y') = 0$ where $F(X', Y')$ is an absolutely irreducible polynomial with coefficients in $\mathbb{F}_q$ which satisfies $F(\xi, \eta) = 0$ where ξ, η are defined to be $\xi := x/(x^{q_0+1} + b^{q_0}y^{q_0}), \eta := by/(x^{q_0+1} + b^{q_0}y^{q_0})$.

Proposition 4.2. *The equation of $\pi_\ell(\mathcal{X})$ can be written in the form*

$$G_1(X'Y') = G_2(X'Y')(X'^{q-1} + Y'^{q-1}),$$

with $G_1(T), G_2(T) \in \mathbb{F}_q[T]$, $\deg(G_1(T)) = \frac{1}{2}q - 1$ and $\deg(G_2(T)) = q_0$.

Proof. Let $F(X', Y') = \sum a_{ij}X'^iY'^j$. Let r_∞ be the line of α with equation $X'_2 = 0$. By (4.3) and (4.5), the intersection divisor of r_∞ is given by $\pi_\ell^{-1}(r_\infty) = q_0A_0 + q_0A_4 + \sum P(1 : a : 0 : a^{2q_0+1} : a^{2q_0+2})$ with a ranging over $\mathbb{F}_q \setminus \{0\}$. In other words, for the intersection multiplicity of $\pi_\ell(\mathcal{X})$ with the line r_∞ we have

$$I(\pi_\ell(\mathcal{X}), r_\infty; \pi_\ell(P)) = \begin{cases} 1 & \textit{for } P = (1 : a : 0 : a^{2q_0+1} : a^{2q_0+2}) \textit{ with } a \in \mathbb{F}_q \setminus \{0\}, \\ q_0 & \textit{for } P = A_0 \textit{ and } P = A_4 , \\ 0 & \textit{otherwise.} \end{cases}$$

This implies that the monomials of degree $q+2q_0-1$ of $F(X',Y')$ are $Y'^{q_0}X'^{q+q_0-1}$ and $X'^{q_0}Y'^{q+q_0-1}$. By the last two claims in Lemma 4.1, there exist $e\,,e'\in\bar{\mathbb{F}}_q$ such that

$$\sum a_{ij}X'^iY'^j=e\sum a_{ij}\omega^{q_0(i-j)}X'^iY'^j\,,$$

$$\sum a_{ij}X'^iY'^j=e'\sum a_{ij}Y'^iX'^j\,,$$

where ω is a generator of the multiplicative group of $\mathbb{F}_q$. Then $a_{ij}=ea_{ij}\omega^{q_0(i-j)}$, $a_{ij}=e'a_{ji}$. For $i=q_0, j=q+q_0-1$, we have $a_{ij}=1$ and $\omega^{i-j}=1$, and the same holds for $i=q+q_0-1, j=q_0$. These equations yield $e=e'=1$. Hence $a_{ij}\omega^{q_0(i-j)}=a_{ij}=a_{ji}$. Suppose now that $a_{ij}\neq 0$. Then $\omega^{q_0(i-j)}=1$, and hence $i-j$ is divisible by $q-1$. Since $i+j<q+2q_0-1$, this only leaves three possibilities, namely $i=j$, $i=q-1+j$ and $j=q-1+i$. So, $F(X',Y')=G_1(X'Y')+\ldots a_{q-1+j,j}X'^{q-1+j}Y'^j+\ldots+a_{i,q-1+i}X'^iY'^{q-1+i}+\ldots$. As $a_{ij}=a_{ji}$, this gives

$$\begin{aligned}F(X',Y') &= G_1(X'Y')+\ldots a_{q-1+j,j}X'^{q-1+j}Y^j+a_{j,q-1+j}X'^jY'^{q-1+j}+\\ &\quad +\ldots+a_{i,q-1+i}X'^iY'^{q-1+i}+a_{q-1+i,i}X'^{q-1+i}Y^i+\ldots\\ &= G_1(X'Y')+(X'^{q-1}+Y'^{q-1})(a_{q-1+j,j}X'^jY'^j+a_{i,q-1+i}X'^iY'^i+\ldots)\\ &= G_1(X'Y')+G_2(X'Y')(X^{q-1}+Y^{q-1}).\end{aligned}$$

It remains to prove that $\deg(G_1)=\frac{1}{2}q-1$. Let r be the line of α with equation $X'+Y'=0$. From (4.4), the intersection divisor $\pi_\ell^{-1}(r)$ is $(2q_0+1)P(1:1:0:1:1)+\sum P(1:a:a^{q_0+1}+a^{q_0}:a:a^2+a^{2q_0}+a^{2q_0+2})$ with a ranging over $\mathbb{F}_q\setminus\{0,1\}$. Equivalently, for $I=(\pi_\ell(\mathcal{X}),r;\pi_\ell(P))$ we have

$$I=\begin{cases}1 & \textit{for } P=(1:a:a^{q_0+1}+a^{q_0}:a:a^2+a^{2q_0}+a^{2q_0+2}); a\in\mathbb{F}_q\setminus\{0,1\},\\ 2q_0+1 & \textit{for } P=(1:1:0:1:1),\\ 0 & \textit{otherwise.}\end{cases}$$

Since $\pi_\ell(1:1:0:1:1)$ is the infinite point of r but $\pi_\ell(1:a:a^{q_0+1}+a^{q_0}:a:a^2+a^{2q_0}:a^{2q_0+2})$ with $a\in\mathbb{F}_q\setminus\{0,1\}$ is a point at finite distance on r, we deduce from the equation of $\pi_\ell(\mathcal{X})$ that $\deg(G_1(T^2))=q-2$. More precisely, the roots of $G_1(T)$ are the elements of the set $\{(a_0^q(a+1))^{-1}\}\mid a\in\mathbb{F}_q\setminus\{0,1\}$. To obtain such a set in a simpler form, we note that $t\mapsto t^{2q_0-1}$ is a bijection of $\mathbb{F}_q$. Putting $u:=(a+1)^{-2q_0-1}$, we have $(a_0^q(a+1))^{-1}=(u+u^{q_0})^{2q_0-1}$. It turns out that the roots of $G_1(T)$ can be also written in the form $(u+u^{q_0})^{2q_0-1}$ with u ranging over $\mathbb{F}_q\setminus\{0,1\}$. □

To obtain an explicit expression for $G_1(T)$ and $G_2(T)$, we need the following result from finite field theory, see [15, Section 1.4]. *An element $a\in\mathbb{F}_q$ is of trace 0 or trace 1 according as the polynomial x^2+x+a is reducible or irreducible over $\mathbb{F}_q$.* Let Cl_0 and Cl_1 be the set of all elements of trace 0 and of trace 1 in $\mathbb{F}_q$, respectively. Equivalently, Cl_0 and Cl_1 consist of all roots of the polynomials

$$P_0(X):=X+X^2+X^4+\ldots+X^{q/2}\,,\qquad P_1(X)=1+X+X^2+X^4+\ldots+X^{q/2}\,,$$

respectively. Furthermore, Cl_0 is an additive subgroup of $\mathbb{F}_q$ of index 2 and its coset is Cl_1. Also, it is easily seen that $Cl_0 = \{c^{q_0} + c \mid c \in \mathbb{F}_q\}$. Define

$$G^-(T) := 1 + \sum_{i=0}^{s-1} T^{2^i(2q_0+1)-(q_0+1)}(1+T)^{2^i},$$

and

$$H(T) := TG^-(T).$$

Lemma 4.3. *$H(T)$ is the polynomial with the lowest degree (i.e. $\deg(H(T)) = \frac{1}{2}q$) whose roots are the $(2q_0-1)$-th powers of the elements in Cl_0.*

Proof. Since Cl_0 consists of $\frac{1}{2}q$ elements, and the map $x \to x^{2q_0-1}$ in $\mathbb{F}_q$ is bijective, we have to prove that if $a \in Cl_0$, then a^{2q_0-1} is a root of $H(T)$. Let $a \in Cl_0$, and put $t = a^{2q_0-1}$. Then $t^q = t$, $t^{q_0+1} = a^{q_0}$, $t^{2q_0+1} = a$, $t^{q/2+q_0} = a^{q/2}$. Now,

$$t^{q_0}H(t) = t^{q_0+1} + \sum_{i=0}^{s-1} t^{(2q_0+1)2^i} + \sum_{i=0}^{s-1} t^{(2q_0+2)2^i} =$$

$$= a^{q_0} + \sum_{i=0}^{s-1} a^{2^i} + \sum_{i=0}^{s-1} a^{(2q_0)2^i} =$$

$$= a^{q_0} + (a + a^2 + \ldots + a^{q_0/2}) + (a^{2q_0} + a^{4q_0} + \ldots + a^{q/2}) = P_0(a) = 0.$$

□

Lemma 4.4. *$G_1(T) = eG^-(T)$ with $e \in \mathbb{F}_q$.*

Proof. As we have seen in the final part of the proof of Proposition 4.2, $G_1(T)$ has degree $\frac{1}{2}q-1$ because its roots are $(u+u^{q_0})^{2q_0-1}$ with u ranging over $\mathbb{F}_q\setminus\{0,1\}$. In particular, every root of $G_1(T)$ is obtained exactly twice, as $(u+u^{q_0})^{2q_0-1} = (v+v^{q_0})^{2q_0-1}$ happens if and only if either $v = u$ or $v = u+1$. On the other hand, such elements are precisely the $2q_0-1$-powers of the non-zero elements in Cl_0. By Lemma 4.3, we obtain $TG_1(T) = eH(T))$ with $e \neq 0$, whence the claim follows. □

Lemma 4.5. *$G_2(T) = 1 + T^{q_0}$ and $e = 1$.*

Proof. As we have already noted, x is a local parameter at A_0, and the local expansions of by at A_0 is $by = x^{2q_0+1} + x^{q+2q_0} + \ldots$. Thus, by Equation (4.3)

$$\xi\eta = \frac{x^{2q_0+2} + x^{q+2q_0+1} + \ldots}{x^{2q_0+2} + \ldots} = 1 + x^{q-1} + \ldots.$$

Write $G_2(T) = a_0 + a_1T^m + \ldots$ where $m = 2^nk$, k odd, and $m \leq q_0$. Then $G_2(\xi\eta) = a_0 + a_1(1+x^{q-1}+\ldots)^m + \ldots = a_0 + a_1 + a_1x^{2^n(q-1)} + \ldots$, where $\ldots$ indicate terms of degree greater than $2^n(q-1)$. By Proposition 4.2 and Lemma 4.4, $G_1(\xi\eta) + G_2(\xi\eta)(\xi^{q-1}+\eta^{q-1}) = 0$, and $G_1(\xi\eta) = e(1+\ldots)$. Thus, $v_{A_0}(G_2(\xi\eta)(\xi^{q-1}+\eta^{q-1}) = v_{A_0}((a_0+a_1)x^{-q_0(q-1)} +$

$a_1x^{2^n(q-1)}x^{-q_0(q-1)}+\ldots)=0$. This yields $a_0=a_1$ and $2^n=q_0$. Hence $G_2(T)=a_0(1+T^{q_0})$. Moreover, $G_1(\xi\eta)+G_2(\xi\eta)(\xi^{q-1}+\eta^{q-1})$ becomes $e+a_0+\ldots$ where $\ldots$ indicate terms of positive degrees. Hence $e=a_0$. □

As a corollary to Proposition 4.2 and to the previous two lemmas, we have that an equation for $\pi_\ell(\mathcal{X})$ is

$$G^-(X'Y')=(X'^{q-1}+Y'^{q-1})((X'Y')^{q_0}+1).$$

So we have found the desired plane model on which both $\mathbf{N}$ and $[W]$ act linearly:

Theorem 4.6. *Let $G^-(T)\in\mathbb{F}_q[T]$ be defined to be*

$$G^-(T)=1+\sum_{i=0}^{s-1}T^{2^i(2q_0+1)-(q_0+1)}(1+T)^{2^i}.$$

Then $\mathcal{X}$ is birationally $\mathbb{F}_q$-isomorphic to the plane curve of equation

$$G^-(XY)=(X^{q-1}+Y^{q-1})((XY)^{q_0}+1). \tag{4.6}$$

We are in a position to give an explicit equation for the quotient curve $\mathcal{X}_{\mathcal{U}}$.

Theorem 4.7. *For every divisor r of $q-1$, the quotient curve of the DLS-curve associated to the cyclic subgroup $\mathcal{U}$ of $\mathcal{S}z(q)$ of order r has genus $g=g_{\mathcal{U}}=\frac{1}{r}q_0(q-1)$ and is $\mathbb{F}_q$-isomorphic to the non-singular model of the plane curve of equation*

$$Y^{(q-1)/r}\Big(1+\sum_{i=0}^{s-1}X^{2^i(2q_0+1)-(q_0+1)}(1+X)^{2^i}\Big)=(X^{q_0}+1)(Y^{2(q-1)/r}+X^{q-1}).$$

Proof. Let $\varphi_r:\pi_\ell(\mathcal{X})\mapsto\mathbf{P}^2(\bar{\mathbf{F}}_q)$ be the rational map $\varphi_r:=(1:X':Y')\mapsto(1:X'Y':Y'^r)$. Given a point $Q:=(1:u:v)\in\mathrm{Im}(\varphi_r)$ with $v\neq0$, let $P:=(1:u':v')\in\varphi_r^{-1}(Q)$. For $i=1,\ldots,r$, let $P_i:=(1:\tau^{-q_0i}u':\tau^{q_0i}v')$ with τ an element of order $(q-1)/r$ in the multiplicative group of $\mathbb{F}_q$. Then $P_i\in\varphi^{-1}(Q)$. On the other hand, the equation $v=Y'^r$ has precisely r solutions, namely $\tau^{q_0i}v'$ with $i=1,\ldots,r$. Hence φ_r has degree r, and $\varphi_r^{-1}(Q)=\{(1:\tau^{-q_0i}u/v':\tau^{q_0i}v')|i=1,\ldots,r\}$. This together with the third claim in Lemma 4.1 shows that a non–singular model of $\varphi_r(\pi_\ell(\mathcal{X}))$ is the quotient curve of $\mathcal{X}$ associated to the subgroup $\mathcal{U}$. Finally, Theorem 4.6 together with a direct computation gives the desired equation. □

5. Quotient curves arising from the Singer type subgroups

From the classification of the subgroups of $\mathcal{S}z(q)$, see Result 2.4 in Section 2, there exist two cyclic groups of Singer type up to conjugacy in $\mathrm{Aut}(\mathcal{X})\cong\mathcal{S}z(q)$, one of order $q+2q_0+1$, the long Singer subgroup $\mathbf{D}^+$, and one of order $q-2q_0+1$, the short Singer subgroup $\mathbf{D}^-$. We look for two (singular) plane curves $\mathcal{D}^+$ and $\mathcal{D}^-$, both birationally isomorphic to $\mathcal{X}$, such that $\mathbf{D}^+$ acts on $\mathcal{D}^+$ and $\mathbf{D}^-$ acts on $\mathcal{D}^-$ as a linear collineation group. We use the same approach as in Section 4. For this purpose, we choose a generator $\mathbf{g}$ of $\mathbf{D}^+$ (or $\mathbf{D}^-$)

represented by a 4×4-matrix B over $\mathbb{F}_q$, and check that $\mathbf{g}$ has exactly five fixed points: one, say B_0, is defined over $\mathbb{F}_q$ and the other four, say $B_1,\dots,B_4$ are defined over $\mathbb{F}_{q^4}$. We can arrange the indices in such a way that $B_2=\mathbf{F}(B_1),\ B_3=\mathbf{F}^2(B_1),\ B_4=\mathbf{F}^3(B_1)$, where $\mathbf{F}$ denotes the semilinear collineation $(X_0:X_1:X_2:X_3:X_4)\mapsto(X_0^q:X_1^q:X_2^q:X_3^q:X_4^q)$. The point B_0 is not on $\mathcal{X}$, while B_1 (and hence each of B_2,B_3,B_4) belongs to $\mathcal{X}$ or does not according as $\mathbf{g}$ generates $\mathbf{D}^+$ or $\mathbf{D}^-$. In both cases, the points B_i are linearly independent. Every element of order four in the normaliser of the Singer group generated by $\mathbf{g}$, fixes B_0 and preserves the set $\{B_1,B_2,B_3,B_4\}$. More precisely, it acts on $\{B_1,B_2,B_3,B_4\}$ as either $(B_1B_2B_3B_4)$, or $(B_1B_4B_3B_2)$. Each element of order two in the normaliser changes B_1 with B_3, and B_2 with B_4. At this point, we note that the line ℓ through B_2 and B_4 is defined over $\mathbb{F}_{q^2}$ as it is left invariant by $\mathbf{F}^2$. The linear system of all hyperplanes through ℓ cuts out on $\mathcal{X}$ a two-dimensional linear series g_2^n defined over $\mathbb{F}_{q^2}$. The degree n is either $q+2q_0+1$ or $q+2q_0-1$, according as $\mathbf{g}$ generates $\mathbf{D}^+$ or $\mathbf{D}^-$. The irreducible plane curve $\mathcal{D}$ associated with g_2^n is left invariant by the Singer group generated by $\mathbf{g}$ which acts on it as a linear collineation group. It turns out that $\mathcal{D}^+=\mathcal{D}$ for the long Singer subgroup $\mathbf{D}^+$ and $\mathcal{D}^-=\mathcal{D}$ for the short Singer subgroup $\mathbf{D}^-$ have the desired properties. To find an explicit equation for $\mathcal{D}$ we transform the above matrix B into its diagonal form Λ defined over $\mathbb{F}_{q^4}$. The eigenvalues are 1 and λ^{q^i}, $i=0,1,2,3$ for an element $\lambda\in\mathbb{F}_{q^4}$ whose order is either $q+2q_0+1$ or $q-2q_0+1$ according as $\mathbf{g}$ generates $\mathbf{D}^+$ or $\mathbf{D}^-$. Once we have chosen a new frame $(X_0':X_1':X_2':X_3':X_4')$ whose fundamental simplex is $B_0B_1B_2B_3B_4$, the plane curve $\mathcal{D}$ turns out to be the projection π_ℓ of $\mathcal{X}$ from the line ℓ viewed as the vertex, to the plane through $B_0B_1B_3$. In other terms, the projection is $\pi_\ell:(X_0':X_1':X_2':X_3':X_4')\mapsto(X_0':X_1':X_3')$. The equation of $\mathcal{D}$ is given in the following theorems.

Theorem 5.1. *Let $G^+(T)\in\mathbb{F}_q[T]$ be defined to be*

$$G^+(T)=1+\sum_{i=0}^{s-1}T^{2^iq_0}(1+T)^{2^i(q_0+1)-q_0}+T^{q/2}\,.$$

Then $\mathcal{X}$ is birationally $\mathbb{F}_{q^2}$-isomorphic to the plane curve $\mathcal{D}^+$ of equation

$$G^+(XY)=X^{q+2q_0+1}+Y^{q+2q_0+1}.$$

Theorem 5.2. *Let $G^-(T)\in\mathbb{F}_q[T]$ be defined to be*

$$G^-(T)=1+\sum_{i=0}^{s-1}T^{2^i(2q_0+1)-(q_0+1)}(1+T)^{2^i}\,.$$

Let $b:=\lambda^{q_0}+\lambda^{q_0-1}+\lambda^{-q_0}+\lambda^{-(q_0-1)}$ for an element $\lambda\in\mathbb{F}_q^4$ of order $q-2q_0+1$. Then $b\in\mathbb{F}_q$, and $\mathcal{X}$ is birationally $\mathbb{F}_{q^2}$-isomorphic to the plane curve $\mathcal{D}^-$ of equation

$$bG^-(XY)=(X^{q-2q_0+1}+Y^{q-2q_0+1})((XY)^{q_0-1}+(XY)^{2q_0-1}).$$

In carrying out the necessary computations for the proof, we will need to use some more notation. Fix an element λ in the multiplicative group of $\mathbb{F}^\star_{q^4}$ whose order is either $q+2q_0+1$ or $q-2q_0+1$; that is either $\lambda = w^{(q^2-1)(q-2q_0+1)}$, or $\lambda = w^{(q^2-1)(q+2q_0+1)}$, where w is a primitive element of $\mathbb{F}_{q^4}$. Also, let

$$b := \begin{cases} \lambda^{q_0} + \lambda^{q_0+1} + \lambda^{-q_0} + \lambda^{-(q_0+1)} & \text{for } \lambda^{q+2q_0+1} = 1, \\ \lambda^{q_0} + \lambda^{q_0-1} + \lambda^{-q_0} + \lambda^{-(q_0-1)} & \text{for } \lambda^{q-2q_0+1} = 1. \end{cases}$$

$$\mu := \frac{(1+\lambda)^2}{b\lambda}.$$

$$\rho := \frac{1}{b^{q_0}\mu}.$$

Furthermore, for $x, y \in \mathbb{F}_q(\mathcal{X})$ as in Proposition 3.3 let

$$h(x,y) := bxy + x^{2q_0+2} + b^{2q_0}y^{2q_0}\,,$$

and

$$k(x,y) := b^{q_0-1}x + b^{q_0}y + x^{q_0+1} + b^{q_0}y^{q_0}\,.$$

The following equalities are straightforward to check.

$$b^{2q_0} = (\lambda+\lambda^{-1})^q + (\lambda+\lambda^{-1})\,,$$

$$\lambda^4 + b^{2q_0}\lambda^3 + b^2\lambda^2 + b^{2q_0}\lambda + 1 = 0\,,$$

$$\lambda^2 = 1 + \lambda\mu b\,,$$

$$\mu^{q+1} = 1, \text{ and hence } \mu \in \mathbb{F}_{q^2},$$

$$h(x,y)^{q_0} = b^{q_0}x^{q_0}y^{q_0} + x^{2q_0+1} + by\,,$$

$$h(x,y)^q = bx^qy^q + x^{2q+2q_0} + b^{2q_0}y^{2q_0} = x^{q+2q_0+1} + bx^qy + b^{2q_0}y^{2q_0}\,,$$

$$(x^{q_0+1} + b^{q_0}y^{q_0})h(x,y)^{q_0} + b^{q_0+1}y^{q_0+1} + x^{q_0}h(x,y) = 0\,,$$

$$k(x,y+1) = k(x,y)\,,$$

$$h\Big(\frac{by}{h(x,y)}, \frac{x}{bh(x,y)}\Big) = h(x,y)^{-1}\,, \tag{5.1}$$

$$k\Big(\frac{by}{h(x,y)}, \frac{x}{bh(x,y)}\Big) = k(x,y)/h(x,y)\,. \tag{5.2}$$

We will also need a technical lemma. Let $P := (1 : u : u^{q_0+1} + b^{q_0}y^{q_0} : bv : buv + u^{2q_0+2} + b^{2q_0}y^{2q_0})$ be a point of $\mathcal{X}$. Then $t := x + u$ is a local parameter at P.

Lemma 5.3. *There exists $\bar{y} \in \bar{\mathbb{F}}_q(\mathcal{X})$ such that $v_P(\bar{y}) \geq q$ and*

$$by = bv + u^{2q_0}t + (u + v^q)t^{2q_0} + t^{2q_0+1} + \bar{y}\,. \tag{5.3}$$

Proof. From $x^{2q_0}(x^q+x)=by^q+by$ we have

$$by = by^q + (t+u)^{2q_0}(t^q+t+u^q+u)\,,$$

whence the claim follows for $\bar{y} := b(y-v)^q$. □

Let $B := WT_{o,b}$, that is

$$B := \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & b^{q_0} \\ 0 & 1 & 0 & 0 & b \\ 1 & 0 & 0 & b & b^{2q_0} \end{pmatrix}.$$

Let

$$M := \begin{pmatrix} 0 & b^{q_0-1} & 1 & b^{q_0-1} & 0 \\ \mu & 1 & 0 & \lambda & \lambda\mu \\ \mu^q & 1 & 0 & \lambda^q & \lambda^q\mu^q \\ \mu^{q^2} & 1 & 0 & \lambda^{q^2} & \lambda^{q^2}\mu^{q^2} \\ \mu^{q^3} & 1 & 0 & \lambda^{q^3} & \lambda^{q^3}\mu^{q^3} \end{pmatrix}, \quad \text{and} \quad \Lambda := \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 & 0 \\ 0 & 0 & \lambda^q & 0 & 0 \\ 0 & 0 & 0 & \lambda^{-1} & 0 \\ 0 & 0 & 0 & 0 & \lambda^{-q} \end{pmatrix}.$$

A straightforward computation shows that

$$MBM^{-1} = \Lambda. \tag{5.4}$$

Let $[M]$ be the collineation associated with M. Then $[M]$ is a morphism $\mathcal{X} \mapsto \mathbf{P}^4(\mathbb{F}_{q^4})$, and $[\Lambda]$ is a linear automorphism of $\mathcal{Y} := [M](\mathcal{X})$. The algebraic curve $\mathcal{Y}$ can be viewed as a parameterised curve associated to the morphism g with coordinate functions

$$g := (g_0 : g_1 : g_2 : g_3 : g_4)$$

where

$$g_0 := b^{q_0-1}f_1 + f_2 + b^{q_0-1}f_3 = k(x,y)\,,$$
$$g_1 := \mu f_0 + f_1 + \lambda f_3 + \lambda\mu f_4 = \mu + x + \lambda by + \mu\lambda h(x,y)\,,$$
$$g_2 := \mu^q f_0 + f_1 + \lambda^q f_3 + \lambda^q\mu^q f_4 = \mu^{-1} + x + \lambda^q by + \mu^{-1}\lambda^q h(x,y)\,,$$
$$g_3 := \mu^{q^2} f_0 + f_1 + \lambda^{q^2} f_3 + \lambda^{q^2}\mu^{q^2} f_4 = \mu + x + \lambda^{-1} by + \mu\lambda^{-1} h(x,y)\,,$$
$$g_4 := \mu^{q^3} f_0 + f_1 + \lambda^{q^3} f_3 + \lambda^{q^3}\mu^{q^3} f_4 = \mu^{-1} + x + \lambda^{-q} by + \mu^{-1}\lambda^{-q} h(x,y)\,.$$

Note that the fixed points of $[\Lambda]$ are $B_0 := (1:0:0:0:0)$, $B_1 := (0:1:0:0:0)$, $B_2 := (0:0:1:0:0)$, $B_3 := (0:0:0:1:0)$ and $B_4 := (0:0:0:0:1)$. The following lemma follows from Equation (5.3) together with a straightforward computation.

Lemma 5.4. *For a point $P := (1 : u : u^{q_0+1} + b^{q_0}y^{q_0} : bv : buv + u^{2q_0+2} + b^{2q_0}y^{2q_0}) \in \mathcal{X}$ the local expansion of the coordinate functions of g at P are*

$$\begin{aligned} g_0 = \; & g_0(P) + t(b^{q_0-1}(1+u^{2q_0}) + u^{q_0}) + t^{q_0}(u+u^q) \\ & + t^{q_0+1} + t^{2q_0}(b^{q_0-1}(u+u^q)) + t^{2q_0+1}b^{q_0-1} + \bar{g}_0\,, \end{aligned}$$

$$\begin{aligned} g_1 = \; & g_1(P) + t(1+\lambda(u^{2q_0}+\mu u^{2q_0+1}+\mu bv)) \\ & + t^{2q_0}\lambda(u+u^q)(1+\mu u^q) + t^{2q_0+1}\lambda(1+\mu u^q) + \bar{g}_1\,, \end{aligned}$$

$$\begin{aligned} g_2 = \; & g_2(P) + t(1+\lambda^q(u^{2q_0}+\mu^{-1} u^{2q_0+1}+\mu^{-1} bv)) \\ & + t^{2q_0}\lambda^q(u+u^q)(1+\mu u^q) + t^{2q_0+1}\lambda^q(1+\mu^{-1} u^q) + \bar{g}_2\,, \end{aligned}$$

$$\begin{aligned} g_3 = \; & g_3(P) + t(1+\lambda^{-1}(u^{2q_0}+\mu u^{2q_0+1}+\mu bv)) \\ & + t^{2q_0}\lambda^{-1}(u+u^q)(1+\mu u^q) + t^{2q_0+1}\lambda^{-1}(1+\mu u^q) + \bar{g}_3\,, \end{aligned}$$

$$\begin{aligned} g_4 = \; & g_4(P) + t(1+\lambda^{-q}(u^{2q_0}+\mu u^{2q_0+1}+\mu bv)) \\ & + t^{2q_0}\lambda^{-q}(u+u^q)(1+\mu u^q) + t^{2q_0+1}\lambda^{-q}(1+\mu u^q) + \bar{g}_4\,, \end{aligned}$$

with $v_P(\bar{g}_i) \geq q$ *for* $i = 0, \ldots, 4$.

We will also use a result on finite fields.

Lemma 5.5. *The system in* T

1) $b^{q_0}T^{q_0} + b^{q_0}T = b^{q_0-1}\mu + \mu^{q_0+1}$,
2) $b(T^q + T) = \mu^{2q_0}(\mu^q + \mu)$

is not solvable in $\bar{\mathbb{F}}_q$ *for* $\lambda^{q+2q_0+1} = 1$, *but it has exactly two solutions for* $\lambda^{q-2q_0+1} = 1$, *namely* $(\mu/b)\lambda^q$ *and* $(\mu/b)\lambda^q + 1$.

Proof. Assume that the above system is consistent, and let z denote a solution. We show that

3) $z^2 + z = (\mu/b)^2$.

From 1) it follows $bz^q + bz^{2q_0} + b^{1-2q_0}\mu^{2q_0} + \mu^{q+2q_0} = 0$. This together with 2) yield $b^{2q_0}(z^{2q_0}+z) + \mu^{2q_0} + b^{2q_0-1}\mu^{2q_0+1} = 0$. Adding it to the squared of 1) gives $b^{2q_0}z^2 + b^{2q_0}z = \mu^{2q_0+1}(\mu + 1/\mu + b^{2q_0-1}) + b^{2q_0-2}\mu^2 = 0$. Hence 3) follows form (1.1). Claim 3) implies that the system has at most two solutions, z and $z+1$. Actually, one of them is $(\mu/b)\lambda^q$. In fact, $(\mu/b)^2\lambda^{2q} + (\mu/b)\lambda^q + (\mu/b)^2 = 0$ holds if and only if $\lambda^{2q} + \lambda^q b^2\lambda/(1+\lambda^2) = 1$. This is true for $\lambda^{q^2+1} = 1$ and (1.1). It is straightforward to check that $(\mu/b)\lambda^q$ satisfies 1) and 2) if and only if $\lambda^{q-2q_0+1} = 1$. $\square$

Lemma 5.6. *For* $\lambda^{q+2q_0+1} = 1$, *we have* $B_1, B_3 \notin \mathcal{Y}$, *and* $\ell \cap \mathcal{Y} = \emptyset$.

Proof. Let $P := (1 : u : u^{q_0+1} + b^{q_0}y^{q_0} : bv : buv + u^{2q_0+2} + b^{2q_0}y^{2q_0})$ be a point of $\mathcal{X}$. If $g(P) \in \ell$, then the equation $\mu + u + \lambda bv + \mu\lambda buv + u^{2q_0+2} + (bv)^{2q_0} = \mu + u + \lambda^{-1}bv + \mu\lambda^{-1}buv + u^{2q_0+2} + (bv)^{2q_0} = 0$ yields $bv = \mu buv + u^{2q_0+2} + (bv)^{2q_0}$ and hence $u = \mu$. Now, suppose that $g(P) = B_i$, $i = 1, 3$. From $\mu^{-1} + u + \lambda^q v + \mu^{-1}\lambda^q buv + u^{2q_0+2} + (bv)^{2q_0} = \mu^{-1} + u + \lambda^{-q}v + \mu^{-1}\lambda^{-q}buv + u^{2q_0+2} + (bv)^{2q_0} = 0$ we have $v = \mu^{-1}buv + u^{2q_0+2} + (bv)^{2q_0}$ and $u = \mu^{-1}$. At this point, it is enough to show that if $u \in \{\mu, \mu^{-1}\}$, then (u, v) is not a point of the plane curve $\mathcal{C}'$ of equation $k(X,Y)=b^{q_0-1}X+b^{q_0}Y+X^{q_0+1}+(bY)^{q_0}=0$. Actually, this claim follows from Lemma 5.5 as both $\mathcal{C}_b$ and $\mathcal{C}'$ are defined over $\mathbb{F}_q$. $\square$

Let

$$\begin{aligned}P_1 &:= (1:1/\mu:(1/\mu)^{q_0+1}+(1/(\lambda\mu)+b)^{q_0}:1/(\lambda\mu)+b:\\ &\qquad (1/\mu)(1/(\lambda\mu)+b)+(1/\mu)^{2q_0+2}+(1/(\lambda\mu)+b)^{2q_0}),\\ P_2 &:= (1:\mu:(\mu)^{2q_0+1}+(\mu\lambda^q)^{q_0}:\mu\lambda^q:\mu^2\lambda^q+(\mu)^{2q_0+3}\lambda^q+(\mu\lambda^q)^{2q_0}),\\ P_3 &:= (1:1/\mu:(1/\mu)^{q_0+1}+1/(\lambda\mu)^{q_0}:1/(\lambda\mu):1/(\lambda\mu^2)+(1/\mu)^{2q_0+2}+1/(\lambda\mu)^{2q_0}),\\ P_4 &:= (1:\mu:\mu^{q_0+1}+(\mu\lambda^q+b)^{q_0}:\mu\lambda^q+b:\mu(\mu\lambda^q+b)+\mu^{2q_0+2}+(\mu\lambda^q+b)^{2q_0}).\end{aligned}$$

It is straightforward to check that $P_i\in\mathcal{X}$ for $i=1,\dots,4$.

Lemma 5.7. *For $\lambda^{q-2q_0+1}=1$, we have $g(P_i)=B_i$ for $i=1,\dots,4$. Furthermore, B_2 and B_4 are the common points of ℓ and $\mathcal{Y}$.*

Proof. A direct computation proves that $g(P_i)=B_i$, for $i=1,\dots,4$. Given a point $P:=(1:u:u^{q_0+1}+(bv)^{q_0}:bv:ubv+x^{2q_0+2}+(by)^{2q_0})\in\mathcal{X}$, suppose that $g(P)\in\ell$. Then $\mu+u+\lambda bv+\mu\lambda buv+u^{2q_0+2}+(bv)^{2q_0}=\mu+u+\lambda^{-1}bv+\mu\lambda^{-1}buv+u^{2q_0+2}+(bv)^{2q_0}=0$ yields $bv=\mu buv+u^{2q_0+2}+(bv)^{2q_0}$ and hence $u=\mu$. By Lemma 5.5 $P\in\{P_2,P_4\}$, whence $g(P)\in\{B_2,B_4\}$. $\square$

Lemma 5.8. *For $\lambda^{q-2q_0+1}=1$, we have*

$$\begin{array}{lll} v_{P_1}(g_0)=q_0, & v_{P_1}(g_1)=0, & v_{P_1}(g_3)=2q_0\,,\\ v_{P_2}(g_0)=q_0, & v_{P_2}(g_1)=q, & v_{P_2}(g_3)=1\,,\\ v_{P_3}(g_0)=q_0, & v_{P_3}(g_1)=2q_0, & v_{P_3}(g_3)=0\,,\\ v_{P_4}(g_0)=q_0, & v_{P_4}(g_1)=1, & v_{P_4}(g_3)=q\,.\end{array}$$

Proof. Since the order-sequence of $\mathcal{X}$ at any point $Q\in\mathcal{X}\setminus\mathcal{X}(\mathbb{F}_q)$ is $(0,1,q_0,2q_0,q)$, we have $v_{P_i}(g_j)\le q$ for $i=1,\dots,4$ and $j=0,1,3$. Then the lemma follows from Lemma 5.4 together with some computation. $\square$

Corollary 5.9. *For $\lambda^{q-2q_0+1}=1$, $\pi_\ell(B_2)=(0:0:1)$ and $\pi_\ell(B_4)=(0:1:0)$.*

Lemma 5.10. *For $\lambda^{q+2q_0+1}=1$, we have*

$$v_P(g_0)=\begin{cases}1 & \text{for } P=[B]^jA_0 \text{ with } j=0,\dots,q+2q_0,\ j\neq 1,\\ -q-2q_0 & \text{for } P=A_4,\\ 0 & \text{otherwise.}\end{cases}\tag{5.5}$$

Proof. The claim for A_0 and A_4 follows from Equations (4.1), (4.2) and (4.3). Note that A_4 is the only pole of g_0, hence $\mathrm{ord}(g_0)=q+2q_0$. By Equation (5.4), for any integer j the point $[B]^jA_0$ is a zero of g_0 apart from the case where $[B]^jA_0=A_4$. On the other hand, $[B]^jA_0=A_4$ only holds for $j\equiv 1 \pmod{q+2q_0+1}$, and this completes the proof. $\square$

Lemma 5.11. *For $\lambda^{q-2q_0+1}=1$, we have*

$$v_P(g_0) = \begin{cases} q_0 & \text{for } P \in \{P_1,P_2,P_3,P_4\} \\ 1 & \text{for } P=[B]^jA_0 \text{ with } j=0,\ldots,q-2q_0,\ j\neq 1, \\ -q-2q_0 & \text{for } P=P_\infty, \\ 0 & \text{otherwise.} \end{cases} \tag{5.6}$$

Proof. The assertion for P_i, $i=1,\ldots,4$ follows from Lemma 5.8. For the remaining cases, the proof is similar to that of Lemma 5.10. □

For $P\in\mathcal{X}$, let $e'_P := -\min\{v_P(g_0), v_P(g_1), v_P(g_3)\}$.

Lemma 5.12. *For $\lambda^{q+2q_0+1}=1$ we have*

$$e'_P = \begin{cases} q+2q_0+1 & \text{for } P=A_4 \\ 0 & \text{otherwise.} \end{cases} \tag{5.7}$$

Proof. $e'_{A_4}=q+2q_0+1$ can be easily checked once the valuations of the functions f_i, $i:=0,\ldots,4$ at $A_4=P_\infty$ are computed. Note that, because of the setup of the present paper, such computations are done in Section 6. For $P\neq A_4$, the claim follows from Lemma 5.6. □

Lemma 5.13. *For $\lambda^{q-2q_0+1}=1$ we have*

$$e'_P = \begin{cases} q+2q_0+1 & \text{for } P=A_4 \\ -1 & \text{for } P\in\{P_2,P_4\} \\ 0 & \text{otherwise.} \end{cases} \tag{5.8}$$

Proof. Similar to the previous one. For $P\neq A_4$, the claim follows from Lemmas 5.7 and 5.8. □

The homogenous coordinates $(X'_0 : X'_1 : X'_3)$ provide a natural projective frame in α with fundamental triangle $B_0B_1B_3$. To write an equation of $\mathcal{D}=\pi_\ell(\mathcal{Y})$ we will use in α the affine frame (X',Y') arising from the above projective frame by $X'=\rho\frac{X'_1}{X'_0}$, $Y'=\rho\frac{X'_3}{X'_0}$. Then $\mathcal{D}$ has equation $F(X',Y')=0$ where $F(X',Y')$ is an absolutely irreducible polynomial with coefficients in $\mathbb{F}_q$ which satisfies $F(\xi,\eta)=0$, where ξ,η are defined to be $\xi:=\rho\,\frac{\mu+x+\lambda by+\lambda\mu h(x,y)}{k(x,y)}$, $\eta:=\rho\,\frac{\mu+x+\lambda^{-1}by+\lambda^{-1}\mu h(x,y)}{k(x,y)}$.

Lemma 5.14. *The plane curve $\mathcal{D}$ is birationally $\mathbb{F}_{q^4}$-isomorphic to $\mathcal{X}$. The degree of $\mathcal{D}$ is $q+2q_0+1$ or $q+2q_0-1$ according as $\lambda^{q+2q_0+1}=1$ or $\lambda^{q-2q_0+1}=1$.*

Proof. We argue as in the proof of Lemma 4.1. Note that $\pi_\ell g(A_0)=(0:1:1)$. Take any point $Q:=(1:u:u^{q_0+1}+b^{q_0}v^{q_0}:bv:buv+u^{2q_0+2}+b^{2q_0}v^{2q_0})$ on $\mathcal{X}$ such that $\pi_\ell g(Q)=\pi_\ell g(P)$. Then $g(Q)$ lies on the hyperplane $X'_0=0$, and $g_1(Q)=g_3(Q)$. By Lemmas 5.10 and 5.11 together with straightforward computation it turns out that $P=Q$. Moreover, by Lemma 5.4 for $u=v=0$, $1/\xi$ is a local parameter at P. From these facts we deduce that π_ℓ is birational. Finally, Lemma 5.12 for $\lambda^{q+2q_0+1}=1$ and Lemma 5.13 for $\lambda^{q-2q_0+1}=1$ imply the assertion concerning the degree of $\mathcal{D}$. $\square$

The linear transformations $[\Lambda]$, $[MT_{o,b}M^{-1}]$ and $[MWM^{-1}]$ preserve the line ℓ. Hence, they act on the set of planes through ℓ, and give rise to linear automorphisms of $\mathcal{D}$. More precisely, the following lemmas hold.

Lemma 5.15. *The automorphism $[T_{0,b}]$ acts on $\mathcal{D}$ as the linear transformation $(\xi,\eta)\mapsto(\lambda^2\eta,\lambda^{-2}\xi)$.*

Proof. The lemma follows from the following two relations
$$\frac{x+\mu+\lambda(by+b)+\lambda\mu h(x,y+1)}{k(x,y+1)}=\lambda^2\;\frac{x+\mu+\lambda^{-1}by+\lambda^{-1}\mu h(x,y)}{k(x,y)},$$
$$\frac{x+\mu+\lambda^{-1}(by+b)+\lambda^{-1}\mu h(x,y+1)}{k(x,y+1)}=\lambda^{-2}\;\frac{x+\mu+\lambda by+\lambda\mu h(x,y)}{k(x,y)}.$$
$\square$

Lemma 5.16. *The automorphism $[W]$ acts on $\mathcal{D}$ as the linear transformation $(\xi,\eta)\mapsto(\lambda\eta,\lambda^{-1}\xi)$.*

Proof. The lemma follows from the following two relations, which are a consequence of Equations (5.1) and (5.2):
$$\frac{\mu+\frac{by}{h(x,y)}+\lambda(\frac{x}{h(x,y)}+\mu h(\frac{by}{h(x,y)},\frac{b^{-1}x}{h(x,y)}))}{k(\frac{by}{h(x,y)},\frac{b^{-1}x}{h(x,y)})}=\lambda\;\frac{x+\mu+\lambda^{-1}(y+\mu h(x,y))}{k(x,y)},$$
$$\frac{\mu+\frac{by}{h(x,y)}+\lambda^{-1}(\frac{x}{h(x,y)}+\mu h(\frac{by}{h(x,y)},\frac{b^{-1}x}{h(x,y)}))}{k(\frac{by}{h(x,y)},\frac{b^{-1}x}{h(x,y)})}=\lambda^{-1}\;\frac{x+\mu+\lambda(y+\mu h(x,y))}{k(x,y)}.$$
$\square$

The following corollaries are straightforward to check.

Corollary 5.17. *The automorphism $[B]$ acts on $\mathcal{D}$ as the linear transformation $(\xi,\eta)\mapsto(\lambda^{-1}\xi,\lambda\eta)$. In particular, such an automorphism has order either $q+2q_0+1$ or $q-2q_0+1$ according as $\lambda^{q+2q_0+1}=1$ or $\lambda^{q-2q_0+1}=1$.*

Corollary 5.18. *The automorphism $[BW]$ acts on $\mathcal{D}$ as the linear transformation $(\xi,\eta)\mapsto(\eta,\xi)$.*

Corollary 5.17 is the essential tool for the proof of the following result.

Proposition 5.19. *For $\lambda^{q+2q_0+1}=1$, the equation of $\mathcal{D}$ can be written in the form*

$$G(X'Y') = X'^{q+2q_0+1} + Y'^{q+2q_0+1},$$

with $G(T) \in \mathbb{F}_{q^4}[T]$.

Proof. We argue as in the proof of Proposition 4.2. Write the equation $F(X',Y')$ of $\mathcal{D}$ as $\sum a_{ij}X'Y'=0$. By Lemma 5.14 $F(X',Y')$ has degree $q+2q_0+1$. Let r_∞ be the line of α of equation $X'_0=0$. By Lemmas 5.10 and 5.12, the intersection divisor of r_∞ is $(\pi_\ell g)^{-1}(r_\infty)=\sum_{j=0}^{q+2q_0}[B]^jA_0=\sum_{j=0}^{q+2q_0}[M]^{-1}(0:\lambda^j\mu:\lambda^{qj}\mu^{-1}:\lambda^{-j}\mu:\lambda^{-qj}\mu^{-1})$. Then the intersection between $\mathcal{D}$ and r_∞ consists of the points $(0:\lambda^j:\lambda^{-j})$ where $j=0,\ldots,q+2q_0$. Taking $\lambda^{q+2q_0+1}=1$ into account, this yields that the monomials of degree $q+2q_0+1$ of $F(X',Y')$ are X'^{q+2q_0+1} and Y'^{q+2q_0+1}. Since by Corollary 5.17 the linear transformation $(\xi,\eta)\mapsto(\lambda^{-1}\xi,\lambda\eta)$ fixes $\mathcal{D}$, there exists $e\in\bar{\mathbb{F}}_q$ such that

$$\sum a_{ij}X'^iY'^j = e\sum a_{ij}\lambda^{i-j}X'^iY'^j\,,$$

that is $a_{ij}=ea_{ij}\lambda^{i-j}$. Letting $i=q+2q_0+1, j=0$ yields $e=1$. Furthermore, $a_{ij}\neq 0$ yields $\lambda^{i-j}=1$, that is $i-j$ is divisible by $q+2q_0+1$. Since $i+j\le q+2q_0+1$, this only leaves three cases, namely $i=j$; $i=0, j=q+2q_0+1$; $i=q+2q_0+1, j=0$. □

Proposition 5.20. *For $\lambda^{q-2q_0+1}=1$, the equation of $\mathcal{D}$ can be written in the form*

$$G_1(X'Y') = G_2(X'Y')(X'^{q-2q_0+1} + Y'^{q-2q_0+1})\,,$$

with $G_1(T), G_2(T) \in \mathbb{F}_{q^4}[T]$, and $\deg(G_2)=2q_0-1$.

Proof. Using the same notation as in the previous proof, from Lemmas 5.11 and 5.13 the intersection divisor of r_∞ is

$$(\pi_\ell g)^{-1}(r_\infty) = q_0(P_1+P_3)+(q_0-1)(P_2+P_4)+\sum_{j=0}^{q-2q_0}[B]^jA_0.$$

Then the intersection between $\mathcal{D}$ and r_∞ consists of $(0:0:1)$ and $(0:1:0)$, both counted $2q_0-1$ times, together with the points $\{(0:\lambda^j:\lambda^{-j})\mid j=0,\ldots,q-2q_0\}$, each counted just once. Since $j^{q-2q_0+1}=1$, this implies that the monomials of degree $q+2q_0-1$ of $F(X',Y')$ are $X'^{q-2q_0+1}(X'Y')^{2q_0-1}+Y'^{q-2q_0+1}(X'Y')^{2q_0-1}$. By Corollaries 5.17 and 5.18 both linear transformations $(\xi,\eta)\mapsto(\lambda^{-1}\xi,\lambda\eta)$ and $(\xi,\eta)\mapsto(\eta,\xi)$ fix $\mathcal{D}$. Hence there exist $e\,,e'\in\bar{\mathbb{F}}_q$ such that

$$\sum a_{ij}X'^iY'^j = e\sum a_{ij}\lambda^{i-j}X'^iY'^j\,,$$

$$\sum a_{ij}X'^iY'^j = e'\sum a_{ij}Y'^iX'^j\,,$$

that is $a_{ij}=ea_{ij}\lambda^{i-j}$, $a_{ij}=e'a_{ji}$. Letting $i=q$ and $j=2q_0-1$ yields $e=e'=1$. Apart from the cases $i=j$; $i=0, j=q-2q_0+1$; $i=q-2q_0+1, j=0$, some more possibilities also arise. In fact, $i\equiv j \pmod{q-2q_0+1}$ together with $i+j\le q+2q_0-1$

does not rule out either $j = q - 2_0 + 1 + i$ for $0 < i < 2q_0 - 1$ or $i = q - 2q_0 + 1 + j$ for $0 < j < 2q_0 - 1$. If such terms effectively exist, then they form a polynomial of type $G_3(X', Y') = \sum_{i<2q_0-1} a_{ij}(X'^i Y'^{q-2q_0+1+i} + X'^{q-2q_0+1+i} Y'^i)$. Note that $G_3(X', Y')$ can also be written as $G_4(X'Y')(X'^{q-2q_0+1} + Y'^{q-2q_0+1})$. Putting $G_2(T) = G_4(T) + T^{2q_0-1}$, we finally obtain the required equation of $\mathcal{D}$. $\square$

To determine explicitly the polynomials G, G_1, and G_2 in Propositions 5.19 and 5.20 some more computation is needed. Let $Z := \{z \in \mathbb{F}_{q^2} \mid b(z^q + z) = \mu^{2q_0}(\mu^q + \mu) = b^{2q_0-1}\mu^{2q_0}\}$. Let r be the line of equation $X' + \lambda^2 Y' = 0$. As $\xi + \lambda^2\eta = \frac{\rho(x+\mu)}{g_0}$, by Equation (4.1) and Lemmas 5.12, 5.13, the intersection divisor $(\pi_\ell g)^{-1}(r)$ is equal to

$$(\pi_\ell g)^{-1}(r) = \begin{cases} \sum_{z\in Z} P(z) + (2q_0+1)A_4 & \textit{for } \lambda^{q+2q_0+1} = 1, \\ \sum_{z\in Z,\, z\neq \frac{\mu\lambda^q}{b},\, z\neq \frac{b+\mu\lambda^q}{b}} P(z) + (2q_0+1)A_4 & \textit{for } \lambda^{q-2q_0+1} = 1, \end{cases}$$

where $P(z) := (1 : \mu : \mu^{q_0+1} + b^{q_0} z^{q_0} : bz : b\mu z + \mu^{2q_0+2} + b^{2q_0} z^{2q_0})$. For $P(z)$ in the support of $(\pi_\ell g)^{-1}(r)$, the X'-coordinate of $(\pi_\ell g)(P(z))$ is $\lambda A(z)/B(z)$, where $A(z) := z^{2q_0} + z + \frac{\mu^{2q_0+2}}{b^{2q_0}}$, $B(z) := z^{q_0} + z + \frac{\mu}{b} + \frac{\mu^{q_0+1}}{b^{q_0}}$. A straightforward computation yields $A(z) = B(z)^{2q_0}$. Hence the affine points of $\mathcal{D} \cap r$ are the points $(\lambda B(z)^{2q_0-1}, \lambda^{-1} B(z)^{2q_0-1})$, where z ranges over Z for $\lambda^{q+2q_0+1} = 1$, over $Z \setminus \{\frac{\mu\lambda^q}{b}, \frac{b+\mu\lambda^q}{b}\}$ for $\lambda^{q-2q_0+1} = 1$. Note that the number of elements in Z is q, but the pairwise distinct affine points in $\mathcal{D} \cap r$ are $\frac{1}{2}q$ for $\lambda^{q+2q_0+1} = 1$, $\frac{1}{2}q - 1$ for $\lambda^{q-2q_0+1} = 1$. More precisely, $P(z_1) = P(z_2)$ if and only if $B(z_1) = B(z_2)$ and this only happens when $(z_1 + z_2)^{q_0} = (z_1 + z_2)$, that is either $z_1 = z_2$ or $z_1 = z_2 + 1$ because of $g.c.d(2q_0 - 1, q - 1) = 1$. Notice also that for $\lambda^{q-2q_0+1} = 1$ and $z \in Z$, $B(z) = 0$ if and only if $z \in \{\frac{\mu\lambda^q}{b}, \frac{b+\mu\lambda^q}{b}\}$. Then the following lemma holds.

Lemma 5.21. *With the notation of Proposition 5.19, G is a polynomial of degree $\frac{1}{2}q$ whose roots are $\{B(z)^{4q_0-2} \mid z \in Z\}$, each of them counting once. With the notation of Proposition 5.20, G_3 is zero while G_1 is a polynomial of degree $\frac{1}{2}q - 1$ whose roots are $\{B(z)^{4q_0-2} \mid z \in Z, B(z) \neq 0\}$, each of them counting once.*

The proposition below is the key to find the polynomials G and G_1.

Proposition 5.22. *The set $\Sigma(\lambda) := \{B(z) \mid z \in Z\}$ coincides with Cl_0 or Cl_1 according as $\lambda^{q-2q_0+1} = 1$ or $\lambda^{q+2q_0+1} = 1$.*

Proof. Given any $z_1 \in Z$, each other element in Z is written in the form $z = z_1 + c$ with c ranging over $\mathbb{F}_q$. Then $\Sigma(\lambda) = \{B(z_1) + c^{q_0} + c \mid c \in \mathbb{F}_q\}$. Hence, either $\Sigma(\lambda) = Cl_0$ or $\Sigma(\lambda) = Cl_1$ according as $B(z_1) \in Cl_0$ or $B(z_1) \in Cl_1$. Assume at first that $\Sigma(\lambda) = Cl_0$. Then z_1 can be chosen in such a way that $B(z_1) = 0$. This implies $z_1^{q_0} + z_1 = b^{-1}\mu + b^{-q_0}\mu^{q_0+1}$. Then z_1 is a solution of the system in Lemma 5.5. Therefore, $\lambda^{q^2-2q_0+1} = 1$. Viceversa, for $\lambda^{q^2-2q_0+1} = 1$, the system in Lemma 5.5 is consistent, and taking $(b\mu\lambda)^{-1}$ as z_1 $\Sigma(\lambda) = Cl_0$ follows. Since $Cl_1 = \mathbb{F}_q \setminus Cl_0$, the proposition is proved. $\square$

Let $G^+(T) \in \mathbb{F}_q[T]$ be defined to be

$$G^+(T) = 1 + \sum_{i=0}^{s-1} T^{2^i q_0}(1+T)^{2^i(q_0+1)-q_0} + T^{q/2}\,.$$

Proposition 5.23. *With the notation of Proposition 5.19, $G(T) = eG^+(T)$, with $e \in \mathbb{F}_{q^4}$.*

Proof. By Proposition 5.22 $B(z)$ coincides with Cl_1. Hence, by Lemma 5.21, we need to show that $G^+(a^{4q_0-2}) = 0$ for any $a \in Cl_1$. Notice that $G^+(a^{4q_0-2}) = 0$ if and only if $G^+(a^{2q_0-1}) = 0$, as G^+ is defined over $\mathbb{F}_2$. Put $t = a^{2q_0-1}$. Then $t^q = t$, $t^{q_0+1} = a^{q_0}$, $t^{2q_0+1} = a$, $t^{q/2+q_0} = a^{q/2}$. Now,

$$(1+t)^{q_0}G^+(t) = (1+t)^{q_0}(1+t)^{q/2} + \sum_{i=0}^{s-1}(t^{q_0}(t+1)^{q_0+1})^{2i} =$$

$$1 + t^{q_0} + t^{q/2} + t^{q/2+q_0} + \sum_{i=0}^{s-1}(t^{2q_0+1})^{2^i} + \sum_{i=0}^{s-1}(t^{q_0+1})^{2^i} + \sum_{i=0}^{s-1}((t^{q_0})^{2^i} + (t^{2q_0})^{2^i}) =$$

$$1 + t^{q_0} + t^{q/2} + t^{q/2+q_0} + \sum_{i=0}^{s-1}(t^{2q_0+1})^{2^i} + \sum_{i=0}^{s-1}(t^{q_0+1})^{2^i} + (t^{q_0} + t^{q/2}) =$$

$$1 + a^{q/2} + \sum_{i=0}^{s-1} a^{2^i} + \sum_{i=0}^{s-1}(a^{q_0})^{2^i} = 1 + a + a^2 + a^4 + \ldots + a^{q/2} = 0.$$

Hence the claim follows. □

Proof of Theorem 5.1 From Propositions 5.19 and 5.23 we deduce that an equation of $\mathcal{D}$ is given by $eG^+(X'Y') = X'^{q+2q_0+1} + Y'^{q+2q_0+1}$, with $e \in \mathbb{F}_{q^4}$. Furthermore, $P := (0, \lambda^{-1})$ is a point of $\mathcal{D}$. In fact, $P = (\pi_\ell g)(1 : \mu^{-1} : \mu^{-q_0-1} + (\lambda\mu^{-1})^{q_0} : \lambda\mu^{-1} : \lambda\mu^{-2} + \mu^{-2q_0-2} + (\lambda\mu^{-1})^{2q_0})$. Hence, $e = 1$ and the proof is complete.

Throughout the rest of the present section we assume $\lambda^{q-2q_0+1} = 1$, and keep up the notation introduced in Proposition 5.20. Furthermore, as in Section 4, we define

$$G^-(T) = 1 + \sum_{i=0}^{s-1} T^{2^i(2q_0+1)-(q_0+1)}(1+T)^{2^i}\,, \quad \text{and} \quad H(T) = TG^-(T)\,.$$

Lemma 5.24. *The roots of H are the $(4q_0 - 2)$-th powers of the elements in $\Sigma(\lambda)$.*

Proof. Notice that as H is defined over $\mathbb{F}_2$ the map $a \mapsto a^2$ is a permutation of the roots of H. Then the claim follows from Proposition 5.22 and Lemma 4.3. □

Proposition 5.25. *There exists $e \in \mathbb{F}_{q^4}$ such that $G_1(T) = eG^-(T)$.*

Proof. The claim follows from Lemmas 5.21 and 5.24. □

Lemma 5.26. *The multiplicity of* 0 *as a root of* G_2 *is* $q_0 - 1$.

Proof. By Lemma 5.8, $v_{P_2}(\xi) = q - q_0$, $v_{P_2}(\eta) = 1 - q_0$, $v_{P_2}(\xi\eta) = q - 2q_0 + 1$. Then, from

$$v_{P_2}(G_1(\xi\eta)) = v_{P_2}(G_2(\xi\eta)) + v_{P_2}(\xi^{q-2q_0+1} + \eta^{q-2q_0+1})$$

it follows that $v_{P_2}(G_2(\xi\eta)) = (q - 2q_0 + 1)(q_0 - 1)$, whence the claim. □

Proposition 5.27. *There exists* $e' \in \mathbb{F}_{q^4}$ *such that* $G_2(T) = e'(T^{q_0-1} + T^{2q_0-1})$.

Proof. For $\alpha \in \bar{\mathbb{F}}_q$ root of G_2, let $\mathcal{C}_\alpha$ be the conic of equation $X'Y' = \alpha$. If $\mathcal{C}_\alpha$ meets $\mathcal{D}$ in a point at finite distance, say (x', y'), then $G_1(x'y') = G_1(\alpha) = 0$, that is $\mathcal{C}_\alpha$ is a component of $\mathcal{D}$, but this is impossible. Hence $\mathcal{C}_\alpha \cap \mathcal{D}$ contains no point at finite distance. This means that $v_{P_i}(\xi\eta - \alpha) > 0$ for some $i \in \{1, 2, 3, 4\}$. Lemma 5.4 together with a straightforward computation shows that $\alpha \in \{0, 1\}$. Then the proposition follows from Lemma 5.26. □

Proof of Theorem 5.2 By Proposition 5.20 and Lemma 5.21, an equation of $\mathcal{D}$ is

$$cG^-(X'Y') = (X'^{q-2q_0+1} + Y'^{q-2q_0+1})((X'Y')^{q_0-1} + (X'Y')^{2q_0-1}), \tag{5.9}$$

where $c \in \mathbb{F}_{q^4}$. We prove that $c = b$. From Lemma 5.4 we have for $u = v = 0$:

$$g_0 = b^{q_0-1}t + t^{q_0+1} + \dots; \quad g_1 = \mu + t + \lambda t^{2q_0+1} + \dots; \quad g_3 = \mu + t + \lambda^{-1}t^{2q_0+1} + \dots;$$

whence

$$\rho g_1/g_0 = (1/b^{2q_0-1})t^{-1}(1 + \dots); \qquad \rho g_3/g_0 = (1/b^{2q_0-1})t^{-1}(1 + \dots).$$

Since

$$cH(\rho^2 g_1 g_3/g_0^2) = \rho^{q-2q_0+1}[(g_1^{q-2q_0+1} + g_2^{q-2q_0+1})/g_0^{q-2q_0+1}](\rho^2 g_1 g_3/g_0^2)^{q_0}[1 + (\rho^2 g_1 g_3/g_0^2)^{q_0}]$$

and

$$cH(\rho^2 g_1 g_3/g_0^2) = c[(1/b^{2q_0-1})^2 t^{-2}(1 + \dots)]^{q/2} + \dots = c(1/b^{2q_0-1})t^{-q}(1 + \dots),$$

$$\rho^{q-2q_0+1}(g_1^{q-2q_0+1} + g_2^{q-2q_0+1})/g_0^{q-2q_0+1} =$$

$$\rho^{q-2q_0+1}[\mu^{q-2q_0}(\lambda + \lambda^{-1})t^{2q_0+1}(1 + \dots)]/[(t^{q-2q_0+1})b^{(q_0-1)(q-2q_0+1)}(1 + \dots)] =$$

$$\rho^{q-2q_0+1}[\mu^{q-2q_0}(\lambda + \lambda^{-1})/b^{(q_0-1)(q-2q_0+1)}]t^{-q+4q_0}(1 + \dots) =$$

$$b^{6-6q_0}t^{-q+4q_0}(1 + \dots),$$

$$(\rho^2 g_1 g_3/g_0^2)^{q_0} = [(1/b^{2q_0-1})^2 t^{-2}(1 + \dots)]^{q_0} = b^{2q_0-2}t^{-2q_0}(1 + \dots),$$

$$(1 + \rho^2 g_1 g_3/g_0^2)^{q_0} = b^{2q_0-2}t^{-2q_0}(1 + \dots),$$

it follows that $c = b$, and the proof is complete.

5.1. Quotient curves arising from $\mathbf{D}^+$.

Theorem 5.28. *Let r be any divisor of $q+2q_0+1$. The quotient curve associated to the (cyclic) subgroup of order r of $\mathbf{D}^+$ has genus $\frac{q_0(q-1)-1}{r}-(q_0-1)$ and is the non–singular model of the plane $\mathcal{D}_r^+$ curve of equation*

$$Y^{(q+2q_0+1)/r}\Big(1+\sum_{i=0}^{s-1}X^{2^iq_0}(1+X)^{2^i(q_0+1)-q_0}+X^{q/2}\Big)=X^{q+2q_0+1}+Y^{2(q+2q_0+1)/r}.$$

Proof. Let $\tau=\lambda^{(q+2q_0+1)/r}$. Then $\tau^r=1$. Let $\varphi_r:\mathcal{D}^+\mapsto \mathbf{P}^2(\bar{\mathbf{F}}_q)$ be the rational map $\varphi_r:=(1:X':Y')\mapsto(1:X'Y':Y'^r)$. Given a point $Q:=(1:u:v)\in \mathrm{Im}(\varphi_r)$ with $v\neq 0$, let $P:=(1:x_0:y_0)\in\varphi_r^{-1}(Q)$. For $i=1,\ldots,r$, let $P_i:=(1:\tau^{-i}x_0:\tau^iy_0)$. Then $P_i\in\varphi^{-1}(Q)$. On the other hand, the equation $v=Y'^r$ has exactly r solutions, namely τ^iy_0 with $i=1,\ldots,r$. This shows that $\varphi_r^{-1}(Q)=\{(1:\tau^{-i}u/y_0:\tau y_0)|i=1,\ldots,r\}$. In particular, φ_r has degree r. By Corollary 5.17, it turns out that the non–singular model of $\varphi_r(\mathcal{D}^+)$ is the quotient curve of $\mathcal{X}$ with respect to the automorphism $[B]^{(q+2q_0+1)/r}$ of $\mathcal{X}$. A straightforward computation gives the desired equation. ∎

5.2. Quotient curves arising from $\mathbf{D}^-$.

Theorem 5.29. *Let r be any divisor of $q-2q_0+1$. The quotient curve associated to the (cyclic) subgroup of order r of $\mathbf{D}^-$ has genus $\frac{q_0(q-1)+1}{r}-(q_0+1)$ and is the non–singular model of the plane $\mathcal{D}_r^-$ curve of equation*

(5.10)
$$bY^{\frac{q-2q_0+1}{r}}\Big(1+\sum_{i=0}^{s-1}X^{2^i(2q_0+1)-q_0-1)}(1+X)^{2^i}\Big)=(X^{q-2q_0+1}+Y^{\frac{2(q-2q_0+1)}{r}})(X^{q_0-1}+X^{2q_0-1}).$$

Proof. The proof is similar to the proof of Theorem 5.28. ∎

6. Quotient curves arising from non-tame subgroups

In the following sections we will investigate the quotient curves of the DLS-curve arising from its automorphism groups of even order. We will give a method for computing the genera of such curves, and in several cases we will also provide an equation for them. Our approach is similar to that employed in [6] and [1] where the function field point of view was used to investigate the analogous problem for the Hermitian curve. In that context, $\mathbb{F}_q$-automorphisms are viewed as elements of the automorphism group of the function field. In our case, $\mathbb{F}_q(\mathcal{X})=\mathbb{F}_q(x,y)$ with $x^{2q_0}(x^q+x)=by^q+by$, and $\mathrm{Aut}(\mathcal{X})\cong\mathcal{S}z(q)$, see Remark 3.6. The extension $\mathbb{F}_q(\mathcal{X})|\mathbb{F}_q(x)$ is Galois of degree q, and x has a unique pole in $\mathbb{F}_q(\mathcal{X})$ that we denote by $\mathcal{P}_\infty$. Such a place is totally ramified in $\mathbb{F}_q(\mathcal{X})$, while all other rational places of $\mathbb{F}_q(x)$ split completely in $\mathbb{F}_q(\mathcal{X})|\mathbb{F}_q(x)$. The Galois group of $\mathbb{F}_q(\mathcal{X})|\mathbb{F}_q(x)$ is $\bar{\mathbf{T}}_0:=\{\psi_{0,c}\mid c\in\mathbb{F}_q\}$ with $\psi_{a,c}$ as in Section 3. Note that $\bar{\mathbf{T}}_0$ comprises the identity and the elements of order 2 of the Sylow 2-subgroup $\bar{\mathbf{T}} = \{\psi_{a,c} \mid a, c \in \mathbb{F}_q\}$ of $\mathrm{Aut}(\mathcal{X})$. Let $\mathcal{X}_\mathcal{U}$ be the quotient curve of $\mathcal{X}$ associated to a subgroup $\mathcal{U}$ of $\mathrm{Aut}(\mathcal{X})$ of even order. In computing the genus $g_\mathcal{U}$ of $\mathcal{X}_\mathcal{U}$ by means of the Hurwitz genus formula, the essential problem is to compute $\deg(\mathrm{Diff}(\mathbb{F}_q(\mathcal{X})|\mathbb{F}_q(\mathcal{X}_\mathcal{U}))$. Since $\mathbb{F}_q(\mathcal{X})|\mathbb{F}_q(\mathcal{X}_\mathcal{U})$ is a non-tame extension, knowing the order of $\mathcal{U}$ and its action on places of $\mathbb{F}_q(\mathcal{X})$ is not sufficient to compute $\deg(\mathrm{Diff}(\mathbb{F}_q(\mathcal{X})|\mathbb{F}_q(\mathcal{X}_\mathcal{U}))$. However as in [6], the Hilbert different's formula see [22, Prop.III.5.12, Theor. III.8.8] allows us to overcome this difficulty. Let $\mathbb{P}$ denote the set of all places of $\mathbb{F}_q(\mathcal{X})$. For $\mathcal{P} \in \mathbb{P}$, the Hilbert different's formula states that the different exponent $d(\mathcal{P})$ of $\mathcal{P}$ with respect to the extension $\mathbb{F}_q(\mathcal{X})|\mathbb{F}_q(\mathcal{X}_\mathcal{U})$ is

$$d(\mathcal{P}) = \sum_{\sigma \in \mathcal{U}\setminus\{1\}, \sigma(\mathcal{P}) = \mathcal{P}} i_\mathcal{P}(\sigma),$$

where $i_\mathcal{P}(\sigma) = v_P(\sigma(t) - t)$, t being a local parameter at $\mathcal{P}$. Hence,

$$\deg(\mathrm{Diff}(\mathbb{F}_q(\mathcal{X})|\mathbb{F}_q(\mathcal{X}_\mathcal{U})) = \sum_{1 \neq \sigma \in \mathcal{U}} \Big(\sum_{\mathcal{P} \in \mathbb{P}, \sigma(\mathcal{P}) = \mathcal{P}} i_\mathcal{P}(\sigma) \Big).$$

Proposition 6.1. *For $1 \neq \psi_{a,c} \in \bar{\mathbf{T}}$,*

$$i_{\mathcal{P}_\infty}(\psi_{a,c}) = \begin{cases} 2q_0 + 2 & \text{for } a = 0\,, \\ 2 & \text{for } a \neq 0\,. \end{cases} \tag{6.1}$$

Proof. Let $t := f_3/f_4$. Then t is a local parameter at $\mathcal{P}_\infty$. By straightforward computation

$$\psi_{a,c}(t) = \frac{a^{2q_0}x + by + c}{f_4 + \alpha},$$

where $\alpha = a^{2q_0+1}x + cx + aby + a^{2q_0+2} + ac + c^{2q_0}$. Hence

$$\psi_{a,d}(t) - t = \frac{xf_4a^{2q_0} + cf_4 + by\alpha}{f_4(f_4 + \alpha)}\,.$$

Then the assertion follows from the following computation. Let $f_1 := x$, $f_2 := x^{q_0+1} + b^{q_0}y^{q_0}$, $f_3 := by$, $f_4 := bxy + x^{2q_0+2} + b^{2q_0}y^{2q_0}$. Then

1. $v_{\mathcal{P}_\infty}(f_1) = -q$,
2. $v_{\mathcal{P}_\infty}(f_3) = -2q_0 - q$,
3. $v_{\mathcal{P}_\infty}(f_2) = -q_0 - q$,
4. $v_{\mathcal{P}_\infty}(f_4) = -2q_0 - q - 1$.

In fact, we have

1. $\mathcal{P}_\infty$ is the only pole of x and $[\mathbb{F}_q(\mathcal{X}) : \mathbb{F}_q(x)] = q$.
2. $\mathcal{P}_\infty$ is the only pole of by and $[\mathbb{F}_q(\mathcal{X}) : \mathbb{F}_q(by)] = 2q_0 + q$.
3. $f_2^{2q_0} = by^q + x^{q+2q_0} = by + x^{2q_0+1}$ and $v_{\mathcal{P}_\infty}(by + x^{2q_0+1}) = -q(2q_0 + 1)$.
4. $f_4^{q_0} = b^{q_0}x^{q_0}y^{q_0} + x^{q+2q_0} + by^q = b^{q_0}x^{q_0}(y^{q_0} + x^{q_0+1}) + by$ whence $q_0v_{\mathcal{P}_\infty}(f_4) = -(qq_0 + q + q_0)$.

□

Corollary 6.2 (Hilbert different's formula for the DLS-curve)**.** *For a subgroup $\mathcal{U}$ of* $\mathrm{Aut}(\mathcal{X})$ *let N_i denote the number of elements of $\mathcal{U}$ of order i with $i > 1$. Then*

$$\deg(\mathrm{Diff}(\mathbb{F}_q(\mathcal{X})|\mathbb{F}_q(\mathcal{X}_{\mathcal{U}})) = \sum_{i>1} k_i N_i$$

where

$$k_i = \begin{cases} 2q_0+2 & \text{for } \ i=2\ , \\ 2 & \text{for } \ i=4 \ \text{ and } \ \text{for } \ i \mid q-1\ , \\ 4 & \text{for } \ i \mid q-2q_0+1\ , \\ 0 & \text{otherwise.} \end{cases} \tag{6.2}$$

Proof. A full set of conjugacy class representatives of non trivial elements in $\mathcal{S}z(q)$ is $\{[T_{0,1}],[T_{1,1}],[N_d],(\mathbf{g}^+)^j,(\mathbf{g}^-)^j\}$ where d ranges over $\mathbb{F}_q\setminus\{0\}$, $\mathbf{g}^{\pm}$ generates $\mathbf{D}^{\pm}$ and $j = 1,\ldots q\pm 2q_0$. For the corresponding automorphisms in $\mathrm{Aut}(\mathcal{X})$, (6.2) for $i = 2,4$ comes from (6.1), while (6.2) for odd i follows from the fact that the number of fixed points on $\mathcal{X}$ of $[N_d]$, $(\mathbf{g}^+)^j$, and $(\mathbf{g}^-)^j$ is equal to $2,0$ and 4, respectively. Finally, (6.2) holds true for any non-trivial element of $\mathrm{Aut}(\mathcal{X})$ since elements in $\mathcal{S}z(q)$ (and hence in $\mathrm{Aut}(\mathcal{X})$) of the same order are pairwise conjugate. □

7. Quotient curves of $\mathcal{X}$ associated to 2 subgroups

Throughout this section we use the following notation:

- $\mathcal{U}$ is a subgroup of $\bar{\mathbf{T}}$;
- $\mathcal{U}_2$ is the subgroup of $\mathcal{U}$ consisting of all elements of order 2 together with the identity;
- $\mathcal{X}_{\mathcal{U}}$ is the quotient curve of $\mathcal{X}$ arising from $\mathcal{U}$;
- $g_{\mathcal{U}}$ is the genus of $\mathcal{X}_{\mathcal{U}}$.

We begin by giving a formula for computing the genus.

Proposition 7.1. *Let $\mathcal{U}$ have order 2^u. If $\mathcal{U}_2$ has order 2^v, then*

$$g_{\mathcal{U}} = 2^{s-u+v}(2^{2s+1-v}-1).$$

Proof. By Corollary 6.2

$$d(\mathcal{P}_\infty) = 2(2^u-2^v)+(2q_0+2)(2^v-1)\,.$$

Then the Hurwitz genus formula yields

$$2q_0(q-1)-2 = 2^u(2g_{\mathcal{U}}-2)+2(2^u-2^v)+(2q_0+2)(2^v-1)\,,$$

that is

$$g_{\mathcal{U}} = q_0(q-2^v)/2^u = 2^{s-u+v}(2^{2s+1-v}-1)\,.$$

□

Proposition 7.1 rises the problem of classifying the subgroups of $\bar{\mathbf{T}}$ in terms of the number of their elements of order 2. Such a general problem is computationally beyond our possibility, because $\bar{\mathbf{T}}$ contains a huge number of pairwise non-conjugate subgroups. What we do here is to prove some results which are useful to investigate special cases. The following proposition states some numerical conditions on u and v.

Proposition 7.2. *Let $\mathcal{U}$ have order 2^u. If $\mathcal{U}_2$ has order 2^v then*

I) $u \leq 2v$;
II) *for every integer u' with $v \leq u' \leq u$ there is a subgroup of $\mathcal{U}$ of order $2^{u'}$;*
III) *for $2^v < q$ we have $u - v \leq s$.*

Proof. The map $\Phi : \bar{\mathbf{T}} \to \mathbb{F}_q$ given by $\Phi(\psi_{a,c}) = a$ is a homomorphism from $\bar{\mathbf{T}}$ onto the additive subgroup of $\mathbb{F}_q$. The restriction of Φ to $\mathcal{U}$ is the homomorphism $\Phi_{|\mathcal{U}}$ with kernel $\mathrm{Ker}(\Phi_{|\mathcal{U}}) = \{\psi_{0,c} | c \in \mathbb{F}_q\}$ isomorphic to $\mathcal{U}_2$. Both $\mathrm{Im}(\Phi_{|\mathcal{U}})$ and $\mathrm{Ker}(\Phi_{|\mathcal{U}})$ are linear subspaces of $\mathbb{F}_q$ regarded as a vector space over $\mathbb{F}_2$. This yields $u = v+w$ where 2^w denotes the order of $\mathrm{Im}(\Phi_{|\mathcal{U}})$ viewed as an additive subgroup of $\mathbb{F}_q$. Now, since $\psi_{a,c}^2 = \psi_{0,a^{2q_0+1}}$ holds, we have that $\mathrm{Im}(\Phi_{|\mathcal{U}})^{2q_0+1} := \{a^{2q_0+1} | a \in \mathrm{Im}(\Phi_{|\mathcal{U}})\}$ is a subset of $\mathrm{Ker}(\Phi_{|\mathcal{U}})$. As $a \mapsto a^{2q_0+1}$ is one-to-one map of $\mathbb{F}_q$, we have $w \leq v$, whence assertion I) follows. We note that the factor–group $\mathcal{U}/\mathcal{U}_2$ is an elementary abelian of order 2^w because $\mathcal{U}_2$ contains all elements of $\mathcal{U}$ of order 2. Assertion II) follows from the well known fact that the converse of the Lagrange theorem holds for any elementary abelian group. Proposition 7.1 together with the fact that $g_{\mathcal{U}}$ must be an integer gives assertion III). □

In the case where $\mathcal{U} = \bar{\mathbf{T}}$ and $\mathcal{U}_2 = Z(\bar{\mathbf{T}})$, assertion II) in Proposition 7.2 has the following corollary.

Lemma 7.3. *For every integer u with $s \leq u \leq 2s+1$, there is a subgroup $\mathcal{U}$ of $\bar{\mathbf{T}}$ of order 2^u containing all elements of $\bar{\mathbf{T}}$ of order 2.*

The existence of a subgroup of $\bar{\mathbf{T}}$ with a given number of elements of order 2 is ensured by the following lemmas.

Lemma 7.4. *Let $\mathcal{H}$ be an elementary abelian subgroup of $\bar{\mathbf{T}}$ of order 2^v. Then there is a subgroup $\mathcal{U}$ of order 2^{v+1} such that $\mathcal{U}_2$ coincides $\mathcal{H}$.*

Proof. Since the normaliser of the Sylow 2-subgroup $\mathbf{T}$ of $\mathcal{S}z(q)$ acts transitively on the set of elements of order 2 in $\mathbf{T}$, we may assume $\psi_{0,1} \in \mathcal{H}$. Then the group generated by $\mathcal{H}$ and $\psi_{1,0}$ has the required property. □

Lemma 7.5. *Let $\mathcal{B}$ be an additive subgroup of $\mathbb{F}_q$ of order 2^v with $0 \leq v \leq 2s+1$. If there exists an additive subgroups $\mathcal{A}$ of $\mathbb{F}_q$ of order 2^{u-v} such that $\mathcal{A}^{2q_0+1} \subseteq \mathcal{B}$, then there is a subgroup $\mathcal{U}$ of $\bar{\mathbf{T}}$ of order 2^u such that $\mathrm{Ker}(\Phi_{|\mathcal{U}}) = \mathcal{B}$ and $\mathrm{Im}(\Phi_{|\mathcal{U}}) = \mathcal{A}$.*

Proof. We keep the notation introduced in the proof of Proposition 7.2. The proof of Lemma 7.5 is by induction on u. First we consider the case $u = v$. We have $\mathcal{A} = \{0\}$, and hence $\mathcal{A}^{2q_0+1} = \{0\}$. Let $\mathcal{U} = \{\psi_{0,c} | c \in \mathcal{B}\}$. Then $\mathcal{U}$ has the required properties. Suppose now that $u > v$. As $\mathcal{A}$ is an elementary abelian group, it contains a subgroup $\mathcal{A}_0$ of index 2, that is of order 2^{u-1-v}. Since $\mathcal{A}_0^{2q_0+1} \subseteq \mathcal{A}^{2q_0+1}$, there is by induction a subgroup $\mathcal{U}_0$ in $\bar{\mathbf{T}}$ with $\mathrm{Ker}(\Phi_{|\mathcal{U}_0}) = \mathcal{B}$ and $\mathrm{Im}(\Phi_{|\mathcal{U}_0}) = \mathcal{A}_0$. For a fixed $\beta = \psi_{a,c} \in \bar{\mathbf{T}}$ with $a \in \mathcal{A} \setminus \mathcal{A}_0$, let $\mathcal{U}$ be the subgroup of $\bar{\mathbf{T}}$ generated by $\mathcal{U}_0$ together with β. We show that $\mathcal{U}$ has order 2^{u-v}, that is $\mathcal{U} = \beta U_0 \cup U_0$. To do this, it is enough to check that $\beta U_0 = U_0 \beta$. For every element $\gamma := \psi_{a_0,c_0}$ of $\mathcal{U}_0$, we have $(\beta\gamma)^2 = \psi_{0,(a+a_0)^{2q_0+1}}$. Since $a + a_0 \in \mathcal{A}$, we have $(a + a_0)^{2q_0+1} \in \mathcal{B}$. As $\mathrm{Ker}(\Phi_{|\mathcal{U}_0}) = \mathcal{B}$, we obtain indeed $(\beta\gamma)^2 \in \mathcal{U}_0$. Using this fact together with two more properties, namely that $\mathbf{T}$ has exponent 4 and that every involutory element in $\mathbf{T}$ is in the center $Z(\mathbf{T})$, we have

$$\beta\gamma = \beta\gamma(\beta\gamma^4\beta^3) = (\beta\gamma)^2\gamma^3\beta^3 = \gamma^3(\beta\gamma)^2\beta^2\beta \in \mathcal{U}_0\mathcal{U}_0\mathcal{U}_0\beta = \mathcal{U}_0\beta.$$

Finally, $\Phi(\beta\gamma) = \Phi(\beta) + \Phi(\gamma) = a + a_0$ implies not only that $\mathrm{Im}(\Phi_{|\mathcal{U}}) = \mathcal{A}$ but also that no element in $\beta\mathcal{U}_0$ is in $\mathrm{Ker}(\Phi_{|\mathcal{U}})$, whence $\mathrm{Ker}(\Phi_{|\mathcal{U}}) = \mathrm{Ker}(\Phi_{|\mathcal{U}_0}) = \mathcal{B}$ follows. □

Lemma 7.6. *For two positive integers u, v with $u \geq v$, there is a subgroup $\mathcal{U}$ of order 2^u such that $\mathcal{U}_2$ has order 2^v, provided that one of the following holds:*

- $v \leq 2s + 1$ *and* $u \leq v + \log_2(v + 1)$,
- $(u - v)|(2s + 1)$ *and* $v \geq u - v$.

Proof. For any additive subgroup $\mathcal{A}$ of $\mathbb{F}_q$ of order 2^{u-v}, the additive subgroup $\mathcal{B}'$ of $\mathbb{F}_q$ generated by all elements in $\mathcal{A}^{2q_0+1}$ has order at most $2^{2^{u-v}-1}$. In fact, $\mathbb{F}_q$ can be viewed as a vector space over its subfield $\mathbb{F}_2$, and the subspace generated by $\mathcal{A}^{2q_0+1}$ has dimension at most $2^{u-v} - 1$. Suppose at first that both $v \leq 2s + 1$ and $u \leq v + \log_2(v + 1)$ hold. Then there exists an additive subgroup $\mathcal{B}$ of $\mathbb{F}_q$ of order 2^v containing $\mathcal{B}'$, and the first claim follows from Lemma 7.5. Now suppose that $v \geq u - v \geq 0$, $(u - v)|(2s + 1)$. Then there exists a subfield of $\mathbb{F}_m$ of $\mathbb{F}_q$ of order $m = 2^{u-v}$. Let $\mathcal{B}$ be any additive subgroup of order 2^v containing the additive group $\mathcal{A}$ of $\mathbb{F}_m$. Again Lemma 7.5 proves the claim. □

Remark 7.7. Lemma 7.4 does not hold true for subgroups $\mathcal{U}$ of order $2^{v+\ell}$ with $\ell > 1$, as the following example shows. Fix an element $e \in \mathbb{F}_q \setminus \mathbb{F}_2$. The set $\mathcal{U}_2 = \{\psi_{0,0}, \psi_{0,1}, \psi_{0,e}, \psi_{0,e+1}\}$ is an elementary abelian group of order 2^v with $v = 2$. Assume that there is a subgroup $\mathcal{U}$ of $\bar{\mathbf{T}}$ of order 2^4 whose elements of order 2 are those of $\mathcal{U}_2$. Then there are three pairwise distinct non-zero elements $a_1 = 1, a_2, a_3 \in \mathbb{F}_q$ and three elements $c_1, c_2, c_3 \in \mathbb{F}_q$ such that ψ_{a_i,c_i}, $i = 1, 2, 3$ together with $\psi_{0,0}$ form a complete set of representatives of the cosets of $\mathcal{U}/\mathcal{U}_2$. Furthermore, $\mathrm{Im}(\Phi) = \{0, 1, a_2, a_3\}$. Hence $a_3 = 1 + a_2$. On the other hand, $\{a_2^{2q_0+1}, a_3^{2q_0+1}\} = \{e, e + 1\}$ by the proof of Lemma 7.4. Thus $a_3^{2q_0+1} = 1 + a_2^{2q_0+1}$. From these results, $(1 + a_2)^{2q_0+1} = 1 + a_2^{2q_0+1}$. Hence $a_2^{2q_0-1} = 1$. But this is impossible as $a_2 \neq 1$ and $2q_0 - 1$ is coprime to $q - 1$.

In some cases we are able to provide an equation for the quotient curve $\mathcal{X}_{\mathcal{U}}$.

Theorem 7.8. *For a subfield $\mathbb{F}_{q'}$ of $\mathbb{F}_q$, let $\mathcal{U}$ be the elementary abelian subgroup of $\bar{\mathbf{T}}$ consisting of all automorphisms $\psi_{0,c}$ with $b^{-1}c \in \mathbb{F}_{q'}$. Then the quotient curve $\mathcal{X}_{\mathcal{U}}$ has genus $g_{\mathcal{U}} = q_0(q/q'-1)$ and is a non-singular model over $\mathbb{F}_q$ of the irreducible plane curve of equation*

$$X^{2q_0}(X^q+X) = b\sum_{i=0}^{n-1} Y^{(q')^i} \tag{7.1}$$

where $q = (q')^n$.

Proof. Let $\Phi : \mathcal{C}_b \to \mathbf{P}^2(\bar{\mathbb{F}}_q)$ be the rational map $\Phi : (1 : X : Y) \mapsto (1 : X : Y^{q'} + Y)$. Given a point $Q := (1 : u : v) \in \mathrm{Im}(\Phi)$, let $P := (1 : x_0 : y_0) \in \Phi^{-1}(Q)$. For $\omega \in \{b^{-1}c \in \mathbb{F}_q \mid \psi_{0,c} \in \mathcal{U}\} = \mathbb{F}_{q'}$, let $P_i := (1 : x_0 : y_0 + \omega)$. Then $P_i \in \Phi^{-1}(Q)$. On the other hand, the equation $\eta = Y^{q'} + Y$ has exactly q' solutions, namely $\{y_0 + \omega \mid \omega \in \mathbb{F}_{q'}\}$. This shows that $\Phi^{-1}(Q) = \{(1 : x_0 : y_0 + b^{-1}c) \mid \psi_{0,c} \in \mathcal{U}\}$. Hence, the non-singular model of $\Phi(\mathcal{C}_b)$ is the quotient curve of $\mathcal{X}$ with respect to $\mathcal{U}$. Then a straightforward computation showing that

$$y^q + y = (y^{q'} + y) + (y^{q'} + y)^{q'} + \ldots (y^{q'} + y)^{(q')^{n-1}}$$

completes the proof. □

Theorem 7.9. *For a cyclic subgroup $\mathcal{U}$ of order 4 of $\mathrm{Aut}(\mathcal{X})$, the quotient curve $\mathcal{X}_{\mathcal{U}}$ of $\mathcal{X}$ associated to $\mathcal{U}$ has genus $g_{\mathcal{U}} = \frac{1}{4}q_0(q-2)$ and it is a non-singular model over $\mathbb{F}_q$ of the irreducible plane curve of equation*

$$\sum_{i=0}^{2s} X^{2^i} + \sum_{i=0}^{s} X^{2^i}\Big(\sum_{j=i}^{s} X^{2^j}\Big) + \sum_{i=s+1}^{2s} X^{2^i}\Big(\sum_{j=0}^{i-s-2} X^{2^j}\Big)^{2q_0} = \sum_{i=0}^{2s} Y^{2^i}. \tag{7.2}$$

Proof. Since the cyclic subgroups of $\mathcal{S}z(q)$ of order 4 are pairwise conjugate under $\mathcal{S}z(q)$, we may assume $\mathcal{U}$ to be generated by $\psi_{1,0}$. Let $\Phi : \mathcal{C}_b \to \mathbf{P}^2(\bar{\mathbb{F}}_q)$ be the rational map $\Phi : (1 : X : Y) \mapsto (1 : X^2 + X : b^2Y^2 + bY + X^3 + X)$. Given a point $Q := (1 : u : v) \in \mathrm{Im}(\Phi)$, let $P := (1 : x_0 : y_0) \in \Phi^{-1}(Q)$. Then it is easily seen that $\Phi^{-1}(Q) = \{\psi_{1,0}^i(P) \mid i = 1, \ldots, 4\}$. Hence a non-singular model of $\Phi(\mathcal{C}_b)$ is the quotient curve of $\mathcal{X}$ arising from $\mathcal{U}$. Now, since

$$\sum_{i=0}^{2s}(b^2Y^2 + bY + X + X^3)^{2^i} = b(Y^q + Y) + \sum_{i=0}^{2s}(X + X^3)^{2^i},$$

we only have to show that

$$\sum_{i=0}^{2s}(X + X^3)^{2^i} + X^{2q_0}(X^q + X) =$$

$$\sum_{i=0}^{2s}(X+X^2)^{2^i}+\sum_{i=0}^{s}(X+X^2)^{2^i}\Big(\sum_{j=i}^{s}(X+X^2)^{2^j}\Big)+\sum_{i=1}^{s-1}\Big((X+X^2)^{2^i}(\sum_{j=0}^{i-1}(X+X^2)^{2^j})\Big)^{2q_0}.$$

This follows from the following two equations:

$$\sum_{i=0}^{2s}(X+X^3)^{2^i}+X^{2q_0}(X^q+X)=\sum_{i=0}^{2s}(X+X^2)^{2^i}+\sum_{i=0}^{2s}(X(X+X^2))^{2^i}+X^{2q_0}\sum_{i=0}^{2s}(X+X^2)^{2^i}$$

$$=\sum_{i=0}^{2s}(X+X^2)^{2^i}+\sum_{i=0}^{2s}(X^{2^i}+X^{2q_0})(X+X^2)^{2^i}\,,$$

$$X^{2^i}+X^{2q_0}=\begin{cases}\sum_{j=i}^{s}(X+X^2)^{2^j} & \text{if} \quad i<s+1\ ,\\ 0 & \text{if} \quad i=s+1\ ,\\ (\sum_{j=0}^{i-s-2}(X+X^2)^{2^j})^{2q_0} & \text{if} \quad i>s+1\ .\end{cases}$$

□

8. Quotient curves arising from subgroups of order $2^u r$ fixing a place; $u>1$ and $r>1$ is a divisor of $q-1$

We keep the notation introduced in Section 7. In addition, let $\bar{\mathbf{N}}=\{\gamma_d \mid d\in\mathbb{F}_q\}$ with γ_d as in (3.1). Then $\bar{\mathbf{T}}\bar{\mathbf{N}}$ is the normaliser of $\bar{\mathbf{T}}$. Assume that $\bar{\mathbf{T}}\bar{\mathbf{N}}$ contains a subgroup $\mathcal{U}$ of order $2^u r$ with $r\mid q-1$. Every subgroup of order $2^u r$ is conjugate to $\mathcal{U}$ under $\mathrm{Aut}(\mathcal{X})$. Note that $\bar{\mathbf{T}}\bar{\mathbf{N}}$ viewed as a permutation group on the set of all $\mathbb{F}_q$-rational places different from $\mathcal{P}_\infty$, is a Frobenius group with kernel $\bar{\mathbf{T}}$ and nucleus $\bar{\mathbf{N}}$. Thus, the order of a non-trivial element $\sigma\in\bar{\mathbf{T}}\bar{\mathbf{N}}$ is either a 2-power or a divisor of $q-1$ according as σ belongs to $\bar{\mathbf{T}}$ or does not. This together with Corollary 6.2 gives the following result.

Theorem 8.1. *For a subgroup $\mathcal{U}$ of $\bar{\mathbf{T}}\bar{\mathbf{N}}$ of order $2^u r$, let the subgroup $\mathcal{U}_2$ of $\mathcal{U}$ consist of all elements of order 2 together with the identity. If $\mathcal{U}_2$ has order 2^v, then*

$$g_{\mathcal{U}}=\frac{1}{r}[2^{s-u+v}(2^{2s+1-v}-1)]\,.$$

Proof. By the Hurwitz genus formula,

$$2q_0(q-1)-2=r2^u(2g_{\mathcal{U}}-2)+2(2^u-2^v)+(2q_0+2)(2^v-1)+2(r2^u-2^u)$$

□

9. Quotient curves arising from dihedral subgroups of order $2r$ with a divisor $r > 1$ of $q - 1$

The normaliser $N_{\mathrm{Aut}(\mathcal{X})}(\bar{\mathbf{N}})$ of $\bar{\mathbf{N}}$ in is the dihedral group of order $2(q-1)$ which comprises $\bar{\mathbf{N}}$ together with a coset consisting entirely of elements of order 2. Let $\mathcal{U}$ be a subgroup of $\mathrm{Aut}(\mathcal{X})$ of order $2r$ with a divisor $r > 1$ of $q - 1$. Up to conjugacy, $\mathcal{U}$ is a subgroup of $N_{\mathrm{Aut}(\mathcal{X})}(\bar{\mathbf{N}})$. Hence $\mathcal{U}$ has $r - 1$ non-trivial elements of odd order and each of the remaining r elements in $\mathcal{U}$ have order 2. The argument in Section 8 depending on the Hurwitz genus and the Hilbert different formulas, enable us to compute the genus of the quotient curve $\mathcal{X}_{\mathcal{U}}$ of $\mathcal{X}$ arising from $\mathcal{U}$. To find an equation for $\mathcal{X}_{\mathcal{U}}$ we also need the Waring formula in two indeterminates, say U and V, see [17, Theorem 1.76]:

Result 9.1.

$$U^k + V^k = \sum (-1)^{i+j} \frac{(i+j-1)!k}{i!j!} (U+V)^i (UV)^j \tag{9.1}$$

where the summation is extended over all pairs (i, j) of non–negative integers for which $i + 2j = k$ holds.

Theorem 9.2. *Let $\mathcal{U}$ be a subgroup of $\mathrm{Aut}(\mathcal{X})$ of order $2r$ with $r \mid q - 1$, and $r > 1$. Then the quotient curve $\mathcal{X}_{\mathcal{U}}$ has genus $g_{\mathcal{U}} = q_0(q - r - 1)/2r$ and it is a non–singular model over $\mathbb{F}_q$ of the irreducible plane curve of equation is*

$$1 + \sum_{i=0}^{s-1} X^{2^i(2q_0+1)-(q_0+1)}(1+X)^{2^i} = \sum (-1)^{i+j} \frac{(i+j-1)!k}{i!j!} Y^i (X^{rj}(X^{q_0}+1),$$

where the summation is extended over all pairs (i, j) of non–negative integers with $i+2j = (q + 2q_0 + 1)/r$.

Proof. With the notation introduced in Section 4, let $\phi_r : \pi_\ell(\mathcal{X}) \mapsto \mathbf{P}^2(\bar{\mathbb{F}}_q)$ be the rational map defined as $\phi_r : (1 : X' : Y') \mapsto (1 : X'Y' : X'^r + Y'^r)$. We argue as in the proof of Theorem 4.7. Given a point $Q := (1 : u : v) \in \mathrm{Im}(\phi_r)$ with $u, v \neq 0$, let $P := (1 : x_0 : y_0) \in \phi_r^{-1}(Q)$, For $i = 1, \ldots, r$, let $P_i := (1 : \tau^{-q_0 i}x_0 : \tau^{q_0 i}y_0), P_i' := (1 : \tau^{q_0 i}y_0 : \tau^{-q_0 i}x_0)$ with an element τ of order $(q - 1)/r$ in the multiplicative group of $\mathbb{F}_q$. Then both P_i and P_i' are in $\phi^{-1}(Q)$. On the other hand, the equation $Y'^{2r} + vY'^r + u^r = 0$ has $2r$ pairwise distinct solutions. Hence, ϕ_r has degree $2r$. So, the quotient curve $\mathcal{U}_{\mathcal{X}}$ of $\mathcal{X}$ associated to $\mathcal{U}$ is the non singular model over $\mathbb{F}_q$ of the irreducible plane curve $\phi_r\pi_\ell(\mathcal{X})$. The equation of the latter curve derives from (4.6) taking into account Result 9.1 applied to $U = X^r$, $V = Y^r$ and $k = (q - 1)/r$. ∎

10. Quotient curves arising from subgroups of order $2r$ with a divisor $r>1$ of $q \pm 2q_0 + 1$

The long as well as the short Singer subgroup of $\mathcal{S}z(q)$ is the maximal cyclic subgroup of a dihedral group of $\mathcal{S}z(q)$. Up to conjugacy under $\mathcal{S}z(q)$, such a dihedral group $\mathcal{U}$ comprises the Singer subgroup $\mathbf{D}$ generated by $[B]^{(q\pm 2q_0+1)/r}$ together with the coset $[W]\mathbf{D}$ of elements of order 2. The statements in Section 9 hold true if $q-1$ is replaced by $q+2q_0+1$ for the long Singer subgroup and by $q-2q_0+1$ for the short Singer subgroup.

Theorem 10.1. *Let $r>1$ be a divisor of $q+2q_0+1$. The quotient curve $\mathcal{X}_\mathcal{U}$ of $\mathcal{X}$ associated to a subgroup $\mathcal{U}$ of order $2r$ has genus*

$$g_\mathcal{U} = \frac{1}{2}\left[\frac{q_0(q-1)-1}{r} - (q_0-1)\right].$$

Furthermore, $\mathcal{X}_\mathcal{U}$ is the non–singular model over $\mathbb{F}_{q^4}$ of the irreducible plane curve of equation

$$1 + \sum_{i=0}^{s-1} X^{2^i q_0}(1+X)^{2^i(q_0+1)-q_0} + X^{q/2} = \sum (-1)^{i+j}\frac{(i+j-1)!}{i!j!}X^{ri}Y^j, \tag{10.1}$$

where the summation is extended over all pairs (i,j) of non–negative integers with $i+2j=(q+2q_0+1)/r$.

Proof. To find the equation we will argue as in the proof of Theorem 9.2. Let $\psi_r : \mathcal{D}^+ \mapsto \mathbf{P}^2(\bar{\mathbf{F}}_q)$ be the rational map $\psi_r := (1:X:Y) \mapsto (1:XY:X^r+Y^r)$. Given a point $Q := (1:u:v) \in \mathrm{Im}(\psi_r)$ with $u \neq 0, v \neq 0$, let $P := (1:x_0:y_0) \in \psi_r^{-1}(Q)$. For $i=1,\ldots,r$, let $P_i := (1:\tau^{-i}x_0:\tau^i y_0), R_i := (1:\tau^i y_0:\tau^{-i}x_0)$, with τ an element of order $(q-1)/r$ in the multiplicative group of $\mathbb{F}_q$. Then both P_i and R_i are in $\psi_r(Q)^{-1}$. On the other hand, if $P := (1,u',v') \in \psi_r(Q)^{-1}$, then $v' = u(u')^{-1}$, and hence $(u')^{2r} + v(u')^r + u = 0$. Since the latter equation has $2r$ pairwise distinct solutions in $u' \in \bar{\mathbb{F}}_q$, we obtain that $\psi_r(Q)^{-1} = \{P_i | i=1,\ldots,r\} \cup \{R_i | i=1,\ldots,r\}$. This shows that ψ_r has degree $2r$. By Corollaries 5.17 and 5.18, the non–singular model of $\psi_r(\mathcal{D}^+)$ is the quotient curve $\mathcal{X}_\mathcal{U}$ of $\mathcal{X}$ arising from $\mathcal{U}$. The computation for the equation of $\psi_r(\mathcal{D}^+)$ can be carried out as before, by applying (9.1) for $U=X^r, V=Y^r$, and $k=(q+2q_0+1)/r$. $\square$

Theorem 10.2. *Let $r>1$ be a divisor of $q-2q_0+1$. The quotient curve $\mathcal{X}_\mathcal{U}$ associated to a subgroup $\mathcal{U}$ of order $2r$ has genus*

$$g_\mathcal{U} = \frac{1}{2}\left[\frac{q_0(q-1)+1}{r} - (q_0+1)\right].$$

Furthermore, $\mathcal{X}_\mathcal{U}$ is the non–singular model over $\mathbb{F}_{q^4}$ of the irreducible plane curve of equation

$$b\Big(1 + \sum_{i=0}^{s-1} X^{2^i(2q_0+1)-(q_0+1)}(1+X)^{2^i}\Big) = (X^{q_0-1}+X^{2q_0-1})\sum (-1)^{i+j}\frac{(i+j-1)!}{i!j!}X^{ri}Y^j,$$

where the summation is extended over all pairs (i,j) of non–negative integers with $i+2j=(q+2q_0+1)/r$.

Proof. Let $\psi_r : \mathcal{D}^+ \mapsto \mathbf{P}^2(\bar{\mathbf{F}}_q)$ be the rational map $\psi_r := (1:X:Y) \mapsto (1:XY:X^r+Y^r)$. Arguing as in the proof of Theorem 10.2, it turns out that a non-singular model of $\psi_r(\mathcal{D}^+)$ is the quotient curve of $\mathcal{X}$ arising from $\mathcal{U}$. Again, the computation for the equation of $\psi_r(\mathcal{D}^-)$ can be carried out as before, by applying (9.1) for $U=X^r, V=Y^r$, and $k=(q-2q_0+1)/r$. □

11. Quotient curves arising from subgroups of order $4r$ with a divisor $r>1$ of $q\pm 2q_0+1$

The normaliser $N_{\mathcal{S}z(q)}(\mathbf{D}^+)$ of the long Singer subgroup $\mathbf{D}^+$ of $\mathcal{S}z(q)$ is a Frobenius group of order $4(q+2q_0+1)$ with kernel $\mathbf{D}^+$ and complement C_4 where C_4 is the cyclic group generated by the linear collineation associated to the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Let $\mathcal{U}$ be a subgroup of order $4r$ such that $r>1$ divides $q+2q_0+1$. Up to conjugacy under $\mathcal{S}z(q)$, $\mathcal{U}$ is a subgroup of $N_{\mathcal{S}z(q)}(\mathbf{D}^+)$, hence $\mathcal{U}$ comprises r elements of odd order, the same number of elements of order 2 and $2r$ elements of order 4. As before, Corollary 6.2 allows us to compute $g_{\mathcal{U}}$ by means of the Hurwitz genus formula. The case of $q-2q_0+1$ can be treated in a similar way. Therefore, we have the following results.

Proposition 11.1. *Let $\mathcal{U}$ be a subgroup of order $4r$, with a divisor $r>1$ of $q\pm 2q_0+1$. Then the quotient curve $\mathcal{X}_{\mathcal{U}}$ of $\mathcal{X}$ associated to $\mathcal{U}$ has genus*

$$g_{\mathcal{U}} = \begin{cases} \frac{1}{4}[\frac{q_0(q-1)-1}{r}-(q_0-1)] & \text{for } r \mid q+2q_0+1, \\ \frac{1}{4}[\frac{q_0(q-1)+1}{r}-(q_0+1)] & \text{for } r \mid q-2q_0+1. \end{cases}$$

12. Quotient curves arising from subgroups isomorphic to $\mathcal{S}z(\bar{q})$

In this section we assume that $\bar{q}:=2^{2\bar{s}+1}$, with $\bar{s}$ divisor of s such that $2\bar{s}+1$ divides $2s+1$. This is the arithmetical condition in order that $\mathcal{S}z(q)$ contains a subgroup isomorphic to $\mathcal{S}z(\bar{q})$. Hence there exists a subgroup $\mathcal{U}$ of $\mathrm{Aut}(\bar{\mathbb{F}}_q(\mathcal{X}))$ isomorphic to $\mathcal{S}z(\bar{q})$.

Theorem 12.1. *Let $\bar{q}:=2^{2\bar{s}+1}$, with $\bar{s}$ divisor of s such that $2\bar{s}+1$ divides $2s+1$. The quotient curve $\mathcal{X}_{\mathcal{U}}$ of $\mathcal{X}$ associated to a subgroup $\mathcal{U}$ isomorphic to $\mathcal{S}z(\bar{q})$ has genus*

$$g_{\mathcal{U}} = \frac{q_0(q-1)-1+(\bar{q}^2+1)\bar{q}^2(\bar{q}-1)+\Delta}{(\bar{q}^2+1)\bar{q}^2(\bar{q}-1)}$$

where

$$\Delta := (\bar{q}^2+1)[(2q_0+2)(\bar{q}-1)+2\bar{q}(\bar{q}-1)]+\bar{q}^2(\bar{q}^2+1)(\bar{q}-2)+\bar{q}^2(\bar{q}+2\bar{q}_0+1)(\bar{q}-1)(\bar{q}-2\bar{q}_0).$$

Proof. The group $\mathcal{U}$ has $(\bar{q}^2+1)(\bar{q}-1)$ elements of order 2, and $(\bar{q}^2+1)(\bar{q}^2-\bar{q})$ elements of order 4. Furthermore, $\mathcal{U}$ has $\frac{1}{2}\bar{q}^2(\bar{q}^2+1)$ subgroups of order $\bar{q}-1$. Also, $\mathcal{U}$ has $\frac{1}{4}\bar{q}^2(\bar{q}+2\bar{q}_0+1)(\bar{q}-1)$ subgroups of order $\bar{q}-2\bar{q}_0+1$, Finally, $\mathcal{U}$ has $\frac{1}{4}\bar{q}^2(\bar{q}-2\bar{q}_0+1)(q-1)$ subgroups of order $\bar{q}+2\bar{q}_0+1$ By Corollary 6.2, $\deg(\mathrm{Diff}(\mathcal{X}|\mathcal{X}_{\mathcal{U}}))$ equals

$$(\bar{q}^2+1)[(2q_0+2)(\bar{q}-1)+2\bar{q}(\bar{q}-1)]+\bar{q}^2(\bar{q}^2+1)(\bar{q}-2)+\bar{q}^2(\bar{q}+2\bar{q}_0+1)(\bar{q}-1)(\bar{q}-2\bar{q}_0),$$

whence the assertion follows by the Hurwitz genus formula. □

References

[1] M. Abdón and L. Quoos, *On the genera of subfields of the Hermitian function field*, preprint.

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

[3] A. Cossidente, G. Korchmáros and F. Torres, *Curves of large genus covered by the Hermitian curve*, Comm. Algebra **28**(10) (2000), 47007–4728.

[4] P. Deligne and G. Lusztig, *Representations of reductive groups over finite fields*, Ann. of Math. **103** (1976), 103–161.

[5] R. Fuhrmann and F. Torres, *On Weierstrass points and optimal curves*, Rend. Circ. Mat. Palermo. Suppl. **51** (Recent Progress in Geometry, E. Ballico and G. Korchmáros Eds.) (1998), 25–46.

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

[7] G. van der Geer, *Error–correcting codes and curves over finite fields*, "Mathematics Unlimited–2001 and Beyond", B. Engquist; W. Schmid Eds., 1115–1138, Springer-Verlag, 2001.

[8] G. van der Geer and M. van der Vlugt, *Curves over finite fields of characteristic* 2 *with many rational points*, C.R. Acad. Sci. Paris **317**, Série I (1993), 593–597.

[9] G. van der Geer and M. van der Vlugt, *Quadratic forms, generalized Hamming weights of codes and curves with many points*, J. Number Theory, **59** (1996), 20–36.

[10] G. van der Geer and M. van der Vlugt, *Tables of curves with many points*, January 2002, http:// www.wins.uva.nl/ geer.

[11] J.P. Hansen, *Deligne-Lusztig varieties and group codes*, Lect. Notes Math. **1518** (1992), 63–81.

[12] J.P. Hansen and J.P. Pedersen, *Automorphism group of Ree type, Deligne-Lusztig curves and function fields*, J. Reine Angew. Math. **440** (1993), 99–109.

[13] J.P. Hansen and H. Stichtenoth, *Group codes on certain algebraic curves with many rational points*, AAECC **1** (1990), 67–77.

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

[15] J.W.P. Hirschfeld, "Projective Geometries Over Finite Fields", second edition, Oxford University Press, Oxford, 1998.

[16] B. Huppert and N. Blackburn, "Finite Groups III", Springer Verlag 1982.

[17] R. Lidl and H. Niederreiter, "Finite Fields", Cambridge University Press, 1987.

[18] 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.

[19] H. Lüneburg, "Translation Planes", Springer-Verlag, 1980.

[20] J.P. Serre, *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini*, C.R. Acad. Sci. Paris **296** Série I, (1983), 397–402.
[21] H. Stichtenoth, "Algebraic-geometric codes associated to Artin-Schreier extensions of $\mathbb{F}_q(z)$". In: *Proc. 2nd Int. Workshop on Alg. and Comb. Coding Theory*, Leningrad (1990), 203–206.
[22] H. Stichtenoth, "Algebraic function fields and codes", Springer-Verlag Berlin, 1993.
[23] K.O. Stöhr and J.F. Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. (3) **52** (1986), 1–19.
[24] J. Tits, *Ovoïdes et groupes de Suzuki*, Arch. Math. **13** (1962), 187–198.
[25] M. Wirtx, *Konstruktion und Tabellen linearer Codes*, Westfälische Wilhelms-Universität Münster, 1991.

Dipartimento di Matematica e Informatica, Università di Perugia, 06123 Perugia, Italy

E-mail address: giuliet@dipmat.unipg.it

Dipartimento di Matematica, Università della Basilicata, Campus Universitario Contrada Macchia Romana, 85100, Potenza, Italy

E-mail address: korchmaros@unibas.it

IMECC-UNICAMP, Cx.P. 6065, Campinas, 13083-970, SP-Brazil

E-mail address: ftorres@ime.unicamp.br

Current Address: Dpto. Algebra, Geometría y Topología. Fac. Ciencias - Universidad de Valladolid, c/ Prado de la Magdalena s/n 47005, Valladolid, Castilla, Spain

E-mail address: ftorres@agt.uva.es