On the Dickson-Guralnick-Zieve curve

Massimo Giulietti* Gábor Korchmáros, † Marco Timpanella ‡

Keywords: Algebraic curves, Finite fields, Automorphism groups.
Mathematics Subject Classifications: 11G20, 14H37, 14H05.

Abstract

The Dickson-Guralnick-Zieve curve, briefly DGZ curve, defined over the finite field $\mathbb{F}_q$ arises naturally from the classical Dickson invariant of the projective linear group $PGL(3, \mathbb{F}_q)$. The DGZ curve is an (absolutely irreducible, singular) plane curve of degree $q^3 - q^2$ and genus $\frac{1}{2}q(q-1)(q^3-2q-2)+1$. In this paper we show that the DGZ curve has several remarkable features, those appearing most interesting are: the DGZ curve has a large automorphism group compared to its genus albeit its Hasse-Witt invariant is positive; the Fermat curve of degree $q-1$ is a quotient curve of the DGZ curve; among the plane curves with the same degree and genus of the DGZ curve and defined over $\mathbb{F}_{q^3}$, the DGZ curve is optimal with respect the number of its $\mathbb{F}_{q^3}$-rational points.

1 Introduction

The classical Dickson invariant of the projective linear group $PGL(3, \mathbb{F}_q)$ with $q = p^h$, p prime, is the (absolutely irreducible) homogeneous polynomial $F(x, y, z) \in \mathbb{F}_q(x, y, z)$ given by $F(x, y, z) = D_1(x, y, z)/D_2(x, y, z)$ where

$$D_1(x,y,z) = \begin{vmatrix} x & x^q & x^{q^3} \\ y & y^q & y^{q^3} \\ z & z^q & z^{q^3} \end{vmatrix}, \quad D_2(x,y,z) = \begin{vmatrix} x & x^q & x^{q^2} \\ y & y^q & y^{q^2} \\ z & z^q & z^{q^2} \end{vmatrix};$$

see [5]. In geometric terms, the plane curve $\mathcal{C}$ of projective equation $F(x, y, z) = 0$ has an automorphism group $G \cong PGL(3, \mathbb{F}_q)$. In the early 2000s, Guralnick

*Massimo Giulietti: massimo.giulietti@unipg.it Dipartimento di Matematica ed Informatica,- Università di Perugia- Via Vanvitelli - 60123 Perugia (Italy).

†Gábor Korchmáros: gabor.korchmaros@unibas.it Dipartimento di Matematica, Informatica ed Economia - Università degli Studi della Basilicata - Viale dell'Ateneo Lucano 10 - 85100 Potenza (Italy)

‡Marco Timpanella: marco.timpanella@unibas.it Dipartimento di Matematica, Informatica ed Economia - Università degli Studi della Basilicata - Viale dell'Ateneo Lucano 10 - 85100 Potenza (Italy)

and Zieve pointed out that G is quite large compared to the genus $\mathfrak{g}$; more precisely $|G| \approx c\mathfrak{g}^{8/5}$, that is, $8/5$ is the amplitude of $|G|$ (with respect to $\mathfrak{g}$); see [7, 13]. Among the curves with positive Hasse-Witt invariant, $\mathcal{C}$ is still the unique known example with an automorphism group whose amplitude is as high as (or higher than) $8/5$. For $q = p$, $\mathcal{C}$ is ordinary and in this case the amplitude appears exceptionally high, as $8/5$ is far away from the maximum amplitude $3/2$ that a solvable automorphism group of an ordinary curve may have; see [12].

In this paper we call $\mathcal{C}$ the Dickson-Guralnick-Zieve curve, briefly DGZ curve, and show several properties concerning its automorphisms, quotient curves, and the number of its points. In the smallest case $q = 2$, the DGZ curve is isomorphic over $\mathbb{F}_8$ to the well known Klein quartic; see Remark 1. From now we assume $q \geq 3$.

In Section 4 we show that $\mathcal{C}$ is an absolutely irreducible plane curve of degree $d = q^3 - q^2$. We prove that the singular points of $\mathcal{C}$ are exactly the points of $PG(2, \mathbb{F}_{q^2}) \setminus PG(2, \mathbb{F}_q)$. Each of them is a $(q-1)$-fold point and it is the center of a unique branch of $\mathcal{C}$. This shows that there is a one-to-one correspondence between the points of $\mathcal{C}$ and those of a nonsingular model $\mathcal{X}$ of $\mathcal{C}$. In particular, for any $i \geq 1$, the number of points of $\mathcal{C}$ in $P(2, \mathbb{F}_{q^i})$ equals $|\mathcal{X}(\mathbb{F}_{q^i})|$ where $\mathcal{X}(\mathbb{F}_{q^i})$ is the set of all $\mathbb{F}_{q^i}$-rational points of $\mathcal{X}$. We also find the exact value of $|\mathcal{X}(\mathbb{F}_{q^i})|$ for $i = 1, 2, 3$, which are $0, q^4 - q, q^6 - q^5 - q^4 + q^3$, but it remains open the problem to compute $|\mathcal{X}(\mathbb{F}_{q^i})|$ for $i \geq 4$, and more general, the L-polynomial of the DGZ curve.

In Section 5, we look inside the action and the ramification groups of a Sylow p-subgroup of G. The results collected are used in Section 6 to find the genus of $\mathcal{C}$ which is $\mathfrak{g} = \frac{1}{2}q(q-1)(q^3 - 2q - 2) + 1$, and show that the quotient curve of $\mathcal{C}$ arising from a Sylow p-subgroup of G is isomorphic to the Fermat curve $\mathcal{F}_{q-1}$ of equation $x^{q-1} + y^{q-1} + z^{q-1} = 0$.

In Section 7 we prove that G is the full automorphism group of the DGZ-curve. Our proof does not depend on deeper results from Group theory, as it only uses the Hurwitz genus formula and the classification of maximal subgroups of $PSL(3, q)$ due to Mitchell [15] for odd q, and to Hartley [8] for even q.

In Section 8 we work out the geometry of the DGZ curve. We show that $\mathcal{C}$ is non-classical in the sense that each nonsingular point of $\mathcal{C}$ is a flex. We also show that $\mathcal{C}$ is $\mathbb{F}_q$-Frobenius non-classical, that is, the tangent at any nonsingular point of $\mathcal{C}$ contains the image of the point by the $\mathbb{F}_q$-Frobenius map Φ_q which takes the point $P = (a : b : c)$ to $P^q = (a^q : b^q : c^q)$. Frobenius non-classicality of $\mathcal{C}$ remains valid when q is replaced by q^3. Furthermore, we compute the orders $v_P(R)$ and $v_P(S)$ of every $P \in \mathcal{C}$, for both the ramification divisor R and the Stöhr-Voloch divisor S. This allows us to answer positively the natural question whether $\mathcal{C}$ has many $\mathbb{F}_{q^3}$-rational points compared to other plane curves defined over $\mathbb{F}_{q^3}$ with the same degree and genus of $\mathcal{C}$. For this purpose, the term of $(d, \mathfrak{g}, i)$-optimal curve is useful for curves whose number of $\mathbb{F}_{q^i}$-rational points is big as possible, in the family of all (absolutely irreducible) plane curves of degree d and genus $\mathfrak{g}$ defined over $\mathbb{F}_{q^i}$. With this terminology, the affirmative answer is given by Corollary 8.10 which states that DGZ-curve is indeed $(q^3 - q^2, \frac{1}{2}q(q-1)(q^3 - 2q - 2) + 1, 3)$-optimal. The above question also has a combinatorial analog where one takes all $\mathbb{F}_{q^i}$-points of the curve, that is, the (possibly singular) points of the curve lying in $PG(2, \mathbb{F}_{q^i})$. Here again, the DGZ-curve is $(q^3 - q^2, \frac{1}{2}q(q-1)(q^3-2q-2)+1, 3)$-optimal.

2 Background on automorphisms of curves

In this section, $\mathcal{X}$ stands for a (projective, nonsingular, geometrically irreducible, algebraic) curve defined over an algebraically closed field $\mathbb{K}$ of positive characteristic p. Since we work with plane curves, we consider $\mathcal{X}$ as a nonsingular model of an absolutely irreducible plane curve $\mathcal{C}$ defined over $\mathbb{K}$. Doing so, we set $\mathfrak{g}(\mathcal{C}) = \mathfrak{g}(\mathcal{X})$ for the genus of $\mathcal{X}$, $\mathbb{K}(\mathcal{X}) = \mathbb{K}(\mathcal{C})$ for the function field of $\mathcal{X}$, and $\mathrm{Aut}(\mathcal{X}) = \mathrm{Aut}(\mathcal{C})$ for the automorphism group of $\mathcal{X}$ which fixes $\mathbb{K}$ element-wise.

By a result due to Schmid, $\mathrm{Aut}(\mathcal{X})$ is finite; see [11, Theorem 11.50]. For a subgroup G of $\mathrm{Aut}(\mathcal{X})$, let $\bar{\mathcal{X}}$ denote a nonsingular model of $\mathbb{K}(\mathcal{X})^G$, that is, a projective nonsingular geometrically irreducible algebraic curve with function field $\mathbb{K}(\mathcal{X})^G$, where $\mathbb{K}(\mathcal{X})^G$ consists of all elements of $\mathbb{K}(\mathcal{X})$ fixed by every element in G. Usually, $\bar{\mathcal{X}}$ is called the quotient curve of $\mathcal{X}$ by G and denoted by $\mathcal{X}/G$. The field extension $\mathbb{K}(\mathcal{X})|\mathbb{K}(\mathcal{X})^G$ is Galois of degree $|G|$.

Since our approach is mostly group theoretical, we give interpretation of concepts from Function field theory in terms of Group theory.

Let Φ be the cover of $\mathcal{X} \mapsto \bar{\mathcal{X}}$ where $\bar{\mathcal{X}} = \mathcal{X}/G$ is a quotient curve of $\mathcal{X}$ with respect to G. A point $P \in \mathcal{X}$ is a ramification point of G if the stabilizer G_P of P in G is nontrivial; the ramification index e_P is $|G_P|$. A point $\bar{Q} \in \bar{\mathcal{X}}$ is a branch point of G if there is a ramification point $P \in \mathcal{X}$ such that $\Phi(P) = \bar{Q}$; the ramification (branch) locus of G is the set of all ramification (branch) points. The G-orbit of $P \in \mathcal{X}$ is the subset of $\mathcal{X}$ $o = \{R \mid R = g(P), g \in G\}$, and it is *long* if $|o| = |G|$, otherwise $o(P)$ is *short*. For a point $\bar{Q}$, the G-orbit o lying over $\bar{Q}$ consists of all points $P \in \mathcal{X}$ such that $\Phi(P) = \bar{Q}$. If $P \in o$ then $|o| = |G|/|G_P|$ and hence $\bar{Q}$ is a branch point if and only if o is a short G-orbit. It may be that G has no short orbits. This is the case if and only if every nontrivial element in G is fixed–point-free on $\mathcal{X}$, that is, the cover Φ is unramified. On the other hand, G has a finite number of short orbits. For a non-negative integer i, the i-th ramification group of $\mathcal{X}$ at P is denoted by $G_P^{(i)}$ (or $G_i(P)$ as in [17, Chapter IV]) and defined to be

$$G_P^{(i)} = \{g \mid \mathrm{ord}_P(g(t) - t) \geq i + 1, g \in G_P\},$$

where t is a uniformizing element (local parameter) at P. Here $G_P^{(0)} = G_P$. The structure of G_P is well known; see for instance [17, Chapter IV, Corollary 4] or [11, Theorem 11.49].

Result 1. *The stabilizer G_P of a point $P \in \mathcal{X}$ in G has the following properties.*

(i) $G_P^{(1)}$ *is the unique normal p-subgroup of G_P;*

(ii) *For* $i \geq 1$, $G_P^{(i)}$ *is a normal subgroup of* G_P *and the quotient group* $G_P^{(i)}/G_P^{(i+1)}$ *is an elementary abelian* p*-group.*

(iii) $G_P = G_P^{(1)} \rtimes U$ *where the complement* U *is a cyclic whose order is prime to* p.

Result 2. *Let* G *be a subgroup of* $\mathrm{Aut}(\mathcal{X})$. *For* $P \in \mathcal{X}$ *put* $e = |G_P/G_P^{(1)}|$ *and* $d = |G_P^{(1)}/G_P^{(2)}|$. *Then* e *divides* $d-1$.

Let $\bar{\mathfrak{g}}$ be the genus of the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/G$. The Hurwitz genus formula gives the following equation

$$2\mathfrak{g} - 2 = |G|(2\bar{\mathfrak{g}} - 2) + \sum_{P \in \mathcal{X}} d_P. \tag{1}$$

where

$$d_P = \sum_{i \geq 0} (|G_P^{(i)}| - 1). \tag{2}$$

Here $D(\mathcal{X}|\bar{\mathcal{X}}) = \sum_{P \in \mathcal{X}} d_P$ is the *different*. For a tame subgroup G of $\mathrm{Aut}(\mathcal{X})$, that is for $p \nmid |G_P|$,

$$\sum_{P \in \mathcal{X}} d_P = \sum_{i=1}^{m} (|G| - \ell_i)$$

where $\ell_1, \ldots, \ell_m$ are the sizes of the short orbits of G.

A subgroup of $\mathrm{Aut}(\mathcal{X})$ is a p'-group (or a prime to p) group if its order is prime to p. A subgroup G of $\mathrm{Aut}(\mathcal{X})$ is *tame* if the 1-point stabilizer of any point in G is p'-group. Otherwise, G is *non-tame* (or *wild*). Obviously, every p'-subgroup of $\mathrm{Aut}(\mathcal{X})$ is tame, but the converse is not always true. From the classical Hurwitz's bound, if $|G| > 84(\mathfrak{g}(\mathcal{X}) - 1)$ then G is non-tame; see [20] or [11, Theorems 11.56]: An orbit o of G is *tame* if G_P is a p'-group for $P \in o$, otherwise o is a *non-tame orbit* of G.

Stichtenoth's result [20] on the number of short orbits of large automorphism groups; see [11, Theorems 11.56, 11.116]:

Result 3. *Let* G *be a subgroup of* $\mathrm{Aut}(\mathcal{X})$ *whose order exceeds* $84(\mathfrak{g}(\mathcal{X}) - 1)$. *Then* G *has at most three short orbits, as follows:*

(a) *exactly three short orbits, two tame and one non-tame, and* $|G| < 24\mathfrak{g}(\mathcal{X})^2$;

(b) *exactly two short orbits, both non-tame, and* $|G| < 16\mathfrak{g}(\mathcal{X})^2$;

(c) *only one short orbit which is non-tame*;

(d) *exactly two short orbits, one tame and one non-tame.*

Nakajima's bound [16]; see also [11, Theorem 11.54]:

Result 4. *If* $\mathcal{X}$ *has positive* p*-rank and* S *is a* p*-subgroup of* $\mathrm{Aut}(\mathcal{X})$ *then*

$$|S| \leq \begin{cases} \frac{p}{p-2}\,(\mathfrak{g}(\mathcal{X}) - 1) & \text{for} \quad \gamma(\mathcal{X}) > 1, \\ \mathfrak{g}(\mathcal{X}) - 1 & \text{for} \quad \gamma(\mathcal{X}) = 1. \end{cases} \tag{3}$$

The following corollary to the Deuring Shafarevic formula; see [11, Theorem 11.129]:

Result 5. *If $\mathcal{X}$ has zero p-rank then any element of order p has exactly one fixed point P.*

The results from Group theory which play a role in the paper are quoted below. Here G stands for any finite group. We use standard notation and terminology; see [14].

The orbit theorem [14, Theorem 3.2]:

Result 6. *Let $G \leq \mathrm{Aut}(\mathcal{X})$ and $P \in \mathcal{X}$. Then*

$$|G| = |G_P||P^G|.$$

Result 7. *Let G be a p-group, and H a proper subgroup of G. Then H is properly contained in its normalizer.*

The maximal subgroups of $PGL(3, q)$ were classified by Mitchell [15] and [8]; see also [11, Theorem A.10]. In this paper we only need the following corollaries of that classification; see [15, Theorem 29], [8, pg. 157].

Result 8. *For $q = p^m$, the following is a complete list of subgroups of the group $PGL(2, q)$ up to conjugacy:*

(i) *the cyclic group of order n with $n \mid (p^m \pm 1)$;*

(ii) *the elementary abelian p-group of order p^f with $f \leq m$;*

(iii) *the dihedral group of order $2n$ with $n \mid (q \pm 1)$;*

(iv) *the alternating group of degree 4 for $p > 2$, or $p = 2$ and m even;*

(v) *the symmetric group of degree 4 for $p > 2$;*

(vi) *the alternating group of degree 5 for $5 \mid (q^2 - 1)$;*

(vii) *the semidirect product of an elementary abelian p-group of order p^h by a cyclic group of order n with $h \leq m$ and $n \mid (q - 1)$;*

(viii) *$PSL(2, p^f)$ for $f \mid m$;*

(ix) *$PGL(2, p^f)$ for $f \mid m$.*

Result 9. *For $q = p^k$, the following is a complete list of subgroups of the group $PSL(3, q)$ up to conjugacy:*

(i) *groups of order $q^3(q - 1)^2(q + 1)/\mu$;*

(ii) *groups of order $6(q - 1)^2/\mu$;*

(iii) *groups of order $3(q^2 + q + 1)/\mu$;*

(iv) *groups of order* $q(q+1)(q-1)$*;*

(v) $PSL(3,p^m)$*, where* m *is a factor of* k*;*

(vi) *groups containing* $PSL(3,p^m)$ *as self-conjugate subgroups of index* 3 *if* p^m-1 *is divisible by* 3 *and* k/m *is divisible by* 3*;*

(vii) *the group* $PSU(3,p^{2m})$*, where* $2m$ *is a factor of* k*;*

(viii) *groups containing* $PSU(3,p^{2m})$ *as self-conjugate subgroups of index* 3 *if* p^m+1 *is divisible by* 3 *and* $k/2m$ *is divisible by* 3*;*

(ix) *The Hessian groups of order* 216 *if* $q-1$ *is divisible by* 9*,* 72 *and* 36 *if* $q-1$ *is divisible by* 3*.*

(x) *Groups of order* 168*, which exist if* $\sqrt{-7}$ *exists in* $\mathbb{F}_q$*.*

(xi) *Groups of order* 360*, which exist if both* $\sqrt{5}$ *and a cube root of unity exist in* $\mathbb{F}_q$*;*

(xii) *Groups of order* 720 *containing the groups of order* 360 *as self-conjugate subgroups. These exist only for* $p=5$ *and* k *even;*

(xiii) *Groups of order* 2520*, each isomorphic with the alternating group of degree* 7*. These exist only for* $p=5$ *and* k *even.*

Result 10. *Let* Ω *be a set of smallest size on which* $PSL(3,q)$ *has a nontrivial action. Then* $|\Omega| \geq q^2+q+1$*.*

3 Background on non-classical plane curves

An irreducible (not necessarily nonsingular) plane curve $\mathcal{C}$ defined over $\mathbb{K}$ is called *non-classical* if its Hessian curve vanishes; see [21] and [11, Section 7.8]. If $\mathcal{C}$ is given by a homogeneous equation $F(x,y,z)=0$, a necessary and sufficient condition for $\mathcal{C}$ to be non-classical is the existence of homogeneous polynomials $G_0(x,y,z), G_1(x,y,z), G_2(x,y,z)$ of the same degree together with a homogeneous polynomial $H(x,y,z)$ such that

$$HF = G_1^{p^m}x + G_2^{p^m}y + G_0^{p^m}z \tag{4}$$

for some $m \geq 1$. Let $\mathcal{L}$ be the (not necessary complete) linear series cut out by lines. For a point $P \in \mathcal{C}$, the $(\mathcal{L},P)$-order sequence is (j_0,j_1,j_2) with $j_0 = 0 < j_1 < j_2$ where $j_i = I(P,\mathcal{C}\cap r)$ is the intersection number of $\mathcal{C}$ with a line r through P and $i=1$ or 2 according as r is a non-tangent line or the tangent to $\mathcal{C}$ at P. The $\mathcal{L}$-order sequence of $\mathcal{C}$ is $(\varepsilon_0,\varepsilon_1,\varepsilon_2)$ if $(\varepsilon_0,\varepsilon_1,\varepsilon_2)=(j_0,j_1,j_2)$ for all but a finite number of points of $\mathcal{C}$. Let x be a separable variable of $\mathcal{C}$, and let $D^{(i)}(t)$ be the i-th Hasse derivative of $t \in \mathbb{K}(\mathcal{C})$ relative to x. If $\mathcal{C}$ is non-classical and (4) holds then its order sequence is $(0,1,p^m)$ and the Wronskian of $\mathcal{C}$ with respect to $\mathcal{L}$ is the determinant

$$W_R = \begin{vmatrix} x & y & 1 \\ D(x) & D(y) & 0 \\ D^{(p^m)}(x) & D^{(p^m)}(y) & 0 \end{vmatrix} = D^{(p^m)}(y).$$

If V is the intersection divisor of $\mathcal{C}$ with a line of $PG(2,\mathbb{K})$, the ramification divisor of $\mathcal{L}$ is

$$R = \mathrm{div}(W_R) + (p^m+1)\mathrm{div}(dx) + 3V,$$

and $\deg(R) = (1+p^m)(2\mathfrak{g}(\mathcal{X})-2) + 3\deg(\mathcal{C})$. Let $v_P(R) = \mathrm{ord}_P(W)$. Then $R = \sum v_P(R)P$.

If the irreducible plane curve $\mathcal{C}$ is defined over a finite field $\mathbb{F}_q$ (and $\mathbb{K} = \overline{\mathbb{F}}_q$), another concept of non-classicality is defined, namely that arising from the action of the q-Frobenius map Φ on the nonsingular points of $\mathcal{C}$ defined by $\Phi(P) = P^q$ where $P = (x:y:z)$ and $P^q = (x^q:y^q:z^q)$; see [21] and [11, Section 8.6]. More precisely, $\mathcal{C}$ is called $\mathbb{F}_q$-*Frobenius non-classical* if the tangent at any nonsingular point $P \in \mathcal{C}$ contains P^q. A necessary and sufficient condition for a non-classical curve $\mathcal{C}$ with $1 < p^m \le q$ to be $\mathbb{F}_q$-Frobenius non-classical is the existence of a homogeneous polynomial $T(x,y,z)$ such that

$$TF = G_1x^{q/p^m} + G_2y^{q/p^m} + G_0z^{q/p^m} \tag{5}$$

with G_0, G_1, G_2 as given in (4); see [11, Theorem 8.72]. Frobenius non-classical curves are somewhat rare; see [3, 21]. In some cases, they have many points over $\mathbb{F}_q$; see [1, 4, 10, 21]. Also, they are closely related to univariate polynomials with minimal values sets, see [2]. Since $\mathcal{L}$ is defined over $\mathbb{F}_q$, $\mathcal{C}$ also has its $\mathbb{F}_q$-Frobenius order sequence (ν_0, ν_1); see [11, Definition 8.46]. If (5) holds then $\nu_0 = 0$ and $\nu_1 = p^m$ by [11, Proposition 8.42]. Let

$$W_S = \begin{vmatrix} x^q & y^q & 1 \\ x & y & 1 \\ D^{(p^m)}(x) & D^{(p^m)}(y) & 0 \end{vmatrix} = (x - x^q)D^{(p^m)}(y).$$

If V is the intersection divisor of $\mathcal{C}$ with a line of $PG(2,\mathbb{F}_q)$, the Stöhr-Voloch divisor of $\mathcal{L}$ over $\mathbb{F}_q$ is

$$S = \mathrm{div}(W_S) + p^m\mathrm{div}(dx) + (q+2)V,$$

and $\deg(S) = p^m(2\mathfrak{g}(\mathcal{C})-2) + (q+2)\deg(\mathcal{C})$; see [11, Definition 8.45].

4 The DGZ-curve and its singular points

A straightforward computation shows that both $D_1(x,y,z)$ and $D_2(x,y,z)$ are $GL(3,\mathbb{F}_q)$ invariant up to a constant. In other words, the following result dating back to Dickson holds.

Lemma 4.1 (Dickson)**.** *Let* $A \in GL(3, \mathbb{F}_q)$*, and* $[x, y, z]^t = A[\bar{x}, \bar{y}, \bar{z}]^t$*. Then* $D_1(x, y, z) = \det(A) D_1(\bar{x}, \bar{y}, \bar{z})$*, and* $D_2(x, y, z) = \det(A) D_2(\bar{x}, \bar{y}, \bar{z})$*.*

As a corollary of Lemma 4.1, the rational function

$$F(x, y, z) = \frac{D_1(x, y, z)}{D_2(x, y, z)} \tag{6}$$

is $GL(3, \mathbb{F}_q)$ invariant.

Lemma 4.2. *$F(x, y, z)$ is a homogeneous polynomial of degree $q^3 - q^2$ defined over $\mathbb{F}_q$.*

Proof. From Lemma 4.1, the algebraic plane curve $\mathcal{D}_1$ with homogeneous equation $D_1(x, y, z) = 0$ is left invariant by $PGL(3, \mathbb{F}_q)$, and the same holds for the algebraic plane curve $\mathcal{D}_2$ with homogeneous equation $D_2(x, y, z) = 0$. Obviously, the line ℓ of equation $x = 0$ is a component of $\mathcal{D}_2$. Since $PGL(3, \mathbb{F}_q)$ acts on the set of all lines of the projective plane $PG(2, \mathbb{F}_q)$ as transitive permutation group, this yields that each such line is a component of $\mathcal{D}_2$. On the other hand, deg $D_2(x, y, z) = q^2 + q + 1$ and $PG(2, \mathbb{F}_q)$ has as many as $q^2 + q + 1$ lines. Therefore, $\mathcal{D}_2$ splits into $q^2 + q + 1$ lines each counted with multiplicity 1. The same argument applies to $\mathcal{D}_1$ showing that each line of $PG(2, \mathbb{F}_q)$ is a component of $\mathcal{D}_1$. Therefore $D_2(x, y, z)$ divides $D_1(x, y, z)$. □

From now on $\mathcal{C}$ stands for the algebraic plane curve with homogenous equation $F(x, y, z) = 0$. According to Introduction, $\mathcal{C}$ is the DGZ curve.

Remark 1. Let $q = 2$. A straightforward computation shows that

$$F(x, y, z) = x^4 + x^2y^2 + x^2yz + x^2z^2 + xy^2z + xyz^2 + y^4 + y^2z^2 + z^4 \tag{7}$$

This curve already mentioned in Serre's lecture notes [18] was investigated by Top [23]. Actually $\mathcal{C}$ is isomorphic over $\mathbb{F}_8$ to the well known Klein curve of equation $x^3y + y^3z + z^3x = 0$. This implies that $\mathrm{Aut}(\mathcal{C}) \cong PGL(3, 2)$.

Proposition 4.3. *The DGZ curve has no $\mathbb{F}_q$-rational points.*

Proof. Since $PGL(3, \mathbb{F}_q)$ acts on the set of all points of $PG(2, \mathbb{F}_q)$ as a transitive permutation group, it is sufficient to show the result for the origin $O = (0 : 0 : 1)$. Since $D_1(x, y, 1) = xy^q - yx^q + g_1(x, y)$ with $\deg g_1(x, y) > q + 1$ and $D_2(x, y, 1) = xy^q - x^qy + g_2(x, y)$ with $\deg g_2(x, y) > q + 1$, the origin is a $(q + 1)$-fold point for both curves $\mathcal{D}_1$ and $\mathcal{D}_2$. From this the result follows. □

Proposition 4.4. *Each point lying in $PG(2, \mathbb{F}_{q^2}) \setminus PG(2, \mathbb{F}_q)$ is a $(q - 1)$-fold point of $\mathcal{C}$.*

Proof. Since $PGL(3, \mathbb{F}_q)$ acts on the set of all points of $PG(2, \mathbb{F}_{q^2}) \setminus PG(2, \mathbb{F}_q)$ as a transitive permutation group, it suffices to perform the proof for a point $P = (\alpha : 0 : 1)$ with $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. In the affine plane $AG(2, \mathbb{F}_{q^2})$ with line at infinity $z = 0$, the translation $\tau : (x, y) \mapsto (x - \alpha, y)$ taking P to the origin $O = (0, 0)$, maps $\mathcal{D}_1$ and $\mathcal{D}_2$ to the curves $\mathcal{Y}_1$ and $\mathcal{Y}_2$ with affine equations

$$H_1(x, y) = \begin{vmatrix} (x+\alpha) & (x+\alpha)^q & (x+\alpha)^{q^3} \\ y & y^q & y^{q^3} \\ 1 & 1 & 1 \end{vmatrix}$$

and

$$H_2(x, y) = \begin{vmatrix} (x+\alpha) & (x+\alpha)^q & (x+\alpha)^{q^2} \\ y & y^q & y^{q^2} \\ 1 & 1 & 1 \end{vmatrix}$$

respectively. Expanding along the first row yields $H_1(x, y) = (\alpha - \alpha^q)y^q + g_1(x, y)$ and $H_2(x, y) = (\alpha - \alpha^q)y + g_2(x, y)$, where $\deg g_1(x, y) > q$ and $\deg g_2(x, y) > 1$. The translation τ maps $\mathcal{C}$ to a curve $\mathcal{Z}$ with affine equation $G(x, y)$. Then

$$G(x, y) = \frac{H_1(x, y)}{H_2(x, y)} = y^{q-1} + G_1(x, y), \tag{8}$$

with $\deg G_1(x, y) > q - 1$. This shows that P is a $(q - 1)$-fold point of $\mathcal{C}$. □

Lemma 4.5. *The singular points of the DGZ curve are those which lie in* $PG(2, \mathbb{F}_{q^2}) \setminus PG(2, \mathbb{F}_q)$.

Proof. Let P be a singular point of $\mathcal{C}$. Since $D_1(x, y, z) = D_2(x, y, z)F(x, y, z)$, P is a singular point of $\mathcal{D}_1$, as well. On the other hand, a straightforward computation yields

$$\frac{\partial D_1}{\partial x} = y^q - y^{q^3}, \quad \frac{\partial D_1}{\partial y} = x^{q^3} - x^q.$$

Therefore $\mathcal{D}_1$, and hence $\mathcal{C}$, can only have singularities at points lying in $PG(2, \mathbb{F}_{q^2})$. Now, the assertion follows from Proposition 4.4. □

Lemma 4.6. *Each point of the DGZ curve lying in $PG(2, \mathbb{F}_{q^2}) \setminus PG(2, \mathbb{F}_q)$ is the center of a unique branch. Furthermore, such a branch has order $q - 1$, and its intersection number with its tangent is q.*

Proof. Let $P \in PG(2, \mathbb{F}_{q^2}) \setminus PG(2, \mathbb{F}_q)$ be a point of $\mathcal{C}$. W.l.o.g. $P = (\alpha : 0 : 1)$. With the notation used in the proof of Proposition 4.4, take a branch γ of $\mathcal{Z}$ centred in $(0, 0)$. From the proof of that proposition, γ has a primitive representation $(x(t), y(t))$ with $x(t), y(t) \in \overline{\mathbb{F}}_q[[t]]$ where

$$\begin{cases} x(t) = c_1 t^u + \ldots \\ y(t) = d_1 t^v + \ldots \end{cases}$$

with $c_1 \neq 0$, $d_1 \neq 0$, and, by (8), $v > u$ and $u \leq (q - 1)$. By direct computation $H_1(x(t), y(t)) = (\alpha - \alpha^q)d_1^q t^{vq} + d_1 c_1^q t^{v+qu} + g(t)$, where all the terms in $g(t)$ have higher degree than $(v + qu)$. On the other hand $G(x(t), y(t)) = 0$. Therefore

$vq = v + qu$ whence $u = q-1$ and $v = q$. From [11, Theorem 4.36], γ is the unique branch of $\mathcal{Z}$ centred at O, and its order equals $q-1$. Going back to $\mathcal{C}$, there is unique branch of $\mathcal{C}$ centred at P and

$$\gamma = \begin{cases} x(t) = \alpha + c_1 t^{q-1} + \dots \\ y(t) = d_1 t^q + \dots \end{cases} . \tag{9}$$

is a primitive representation for it. Since the tangent at γ is the line $y=0$, $I(P, \mathcal{C} \cap \{y=0\}) = I(P, \gamma \cap \{y=0\}) = q$. □

Proposition 4.7. *The DGZ curve is absolutely irreducible.*

Proof. First we show that $\mathcal{C}$ does not have two different absolutely irreducible components. Assume on the contrary that $\mathcal{G}$ and $\mathcal{H}$ are two such components. Let $P \in \mathcal{G} \cap \mathcal{H}$, and take a branch γ of $\mathcal{G}$ and a branch δ of $\mathcal{H}$ both centred at P. Then P is a singular point of $\mathcal{C}$ with at least two branches centred at P. From Lemma 4.5, $P \in PG(2,\mathbb{F}_{q^2}) \setminus PG(2,\mathbb{F}_q)$, but this contradicts Lemma 4.6. Therefore, $\mathcal{C}$ has a unique absolutely irreducible component $\mathcal{G}$ with multiplicity $\mu \geq 1$. On the other hand, Lemma 4.5 yields that $\mathcal{C}$ has only a finite number of singular points. Therefore, $\mu = 1$. □

As a corollary we have the following result.

Corollary 4.8. *At every point of the DGZ curve, there is only one branch of $\mathcal{C}$ centred at that point.*

By Corollary 4.8, there is a bijection between the points of $\mathcal{X}$ and those of $\mathcal{C}$. This shows that $\mathcal{C}(\mathbb{F}_{q^n}) = \mathcal{X}(\mathbb{F}_{q^n})$ for every $n \geq 1$. The point-set of $PG(2,\mathbb{F}_{q^3})$ is partitioned in three subsets, Λ_1, Λ_2 and Λ_3 where Λ_1 is the set of all points in $PG(2,\mathbb{F}_q)$, Λ_2 consists of all points of $PG(2,\mathbb{F}_{q^3}) \setminus PG(2,\mathbb{F}_q)$ covered by the lines of $PG(2,\mathbb{F}_q)$, and Λ_3 is the set of remaining points in $PG(2,\mathbb{F}_{q^3})$. Obviously, $|\Lambda_1| = q^2+q+1$. A direct computation shows that $|\Lambda_2| = (q^2+q+1)(q^3-q)$. Hence

$$|\Lambda_3| = q^6 - q^5 - q^4 + q^3. \tag{10}$$

Lemma 4.9. $\mathcal{C}(\mathbb{F}_{q^3}) = \Lambda_3$.

Proof. From Proposition 4.3, $\mathcal{C}(\mathbb{F}_{q^3}) \cap \Lambda_1 = \emptyset$. Furthermore, if L is a line of $PG(2,\mathbb{F}_q)$ then $L \cap \mathcal{C} \subseteq \mathcal{C}(\mathbb{F}_{q^2})$ as a consequence of Proposition 4.4 and of the Bézout's theorem. Therefore, $\mathcal{C}(\mathbb{F}_{q^3}) \cap \Lambda_2 = \emptyset$ also. Let $P \in \Lambda_3$, with $P = (\alpha : \beta : \gamma)$. Then

$$D_1(P) = \begin{vmatrix} \alpha & \alpha^q & \alpha^{q^3} \\ \beta & \beta^q & \beta^{q^3} \\ \gamma & \gamma^q & \gamma^{q^3} \end{vmatrix} = \begin{vmatrix} \alpha & \alpha^q & \alpha \\ \beta & \beta^q & \beta \\ \gamma & \gamma^q & \gamma \end{vmatrix} = 0.$$

On the other hand $D_2(P) \neq 0$, hence $F(P) = 0$ and the assertion follows. □

Theorem 4.10. *The DGZ curve has genus $\mathfrak{g} = \frac{1}{2}q(q-1)(q^3-2q-2)+1$.*

Proof. From Equation (6),

$$\frac{\partial F}{\partial y} = \left(\frac{\partial D_1}{\partial y} D_2 - D_1 \frac{\partial D_1}{\partial y}\right) \frac{1}{D_2^2}.$$

In affine coordinates, $f_y(x,y) =$

$$\frac{(x^{q^3+q} - x^{q^3+1})(y^{q^2} - y^q) + (x^{q^2+q} - x^{q^2+1})(y^q - y^{q^3}) + (x^{2q} - x^{q+1})(y^{q^3} - y^{q^2})}{D_2(x,y,1)^2}.$$

This shows that f_y does not vanish on the generic points of $\mathcal{C}$. Hence, x is a separating variable of $\mathbb{K}(\mathcal{C})$. Thus $\mathrm{div}(dx) \neq 0$ and $\deg(\mathrm{div}(dx)) = 2\mathfrak{g}(\mathcal{X}) - 2$; see [11, Theorem 5.50]. Let P be a point of $\mathcal{C}$. Four cases are distinguished according as

(a) $P = (a : b : 1)$ and $a \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$;

(b) $P = (a : b : 1)$ and $a \in \mathbb{F}_q$;

(c) $P = (a : b : 1)$ and $a \notin \mathbb{F}_{q^2}$;

(d) $P = (a : b : 0)$.

In Case (a), Proposition 4.6 shows that the (unique) branch γ centred at P has a primitive representation

$$\begin{cases} x(t) = a + c_1 t^{q-1} \\ y(t) = b + d_1 t^q + \ldots \end{cases}.$$

In particular, $\mathrm{ord}_\gamma(dx) = (q-2)$.

In Case (b) some more efforts are needed. In this case, the (unique) branch centered at P has a primitive representation

$$\begin{cases} x(t) = a + c_1 t^q \\ y(t) = b + d_1 t^{q-1} + \ldots \end{cases}.$$

Since $D_1(x,y,z) = D_2(x,y,z)F(x,y,z)$, we have that $D_1(x(t), y(t), 1) = 0$ in $\mathbb{K}[[t]]$. Thus $dD_1(x(t), y(t), 1)/dt = 0$ in $\mathbb{K}[[t]]$. From this, by a direct computation,

$$x'(t) = \frac{x(t)^q y'(t) - x(t)^{q^3} y'(t)}{y(t)^q - y(t)^{q^3}} = \frac{t^{(q+2)(q-1)} g_1(t)}{t^{q(q-1)} g_2(t)} = t^{2q-2} g(t).$$

Therefore $\mathrm{ord}_\gamma(dx) = 2q - 2$.

In Case (c), P is a simple point of $\mathcal{C}$. Again, let γ be the unique branch of $\mathcal{C}$ centered at P. Therefore, $\mathrm{ord}_\gamma(dx) = 0$ unless the tangent line of $\mathcal{C}$ at P is vertical. That line has equation $x = a$. This yields that the univariate polynomial

$$D(y) = D_1(a, y, 1) = \begin{vmatrix} a & a^q & a^{q^3} \\ y & y^q & y^{q^3} \\ 1 & 1 & 1 \end{vmatrix}$$

has a multiple root. Since $D'(y) = (a - a^{q^2})^q$, this gives $a \in \mathbb{F}_{q^2}$, a contradiction.

In Case (d),

$$d\left(\frac{1}{x(t)}\right) = \frac{1}{x(t)^2}\frac{dx(t)}{dt} = t^{-2}.$$

Hence $\mathrm{ord}_\gamma(dx) = -2$.

Summing up this gives $\deg(dx) = (q-2)q^2(q^2-q) + (2q-2)(q^2-q)q - 2(q^2-q) = 2\mathfrak{g}(\mathcal{C}) - 2$ whence the formula for $\mathfrak{g}(\mathcal{C})$ follows. □

5 Action of a Sylow p-subgroup of G and its normalizer on the DGZ-curve

As we have pointed out after Lemma 4.1, $F(x,y,z)$ is a $GL(3,q)$-invariant homogeneous polynomial. Therefore, $PGL(3,q)$ is a subgroup of $\mathrm{Aut}(\mathcal{C})$. In terms of the function field $\mathbb{K}(x,y)$ of $\mathcal{C}$, this shows that the map $\varphi_{\alpha,\beta}$ defined by

$$\varphi_{\alpha,\beta} = \begin{cases} x' = x + \alpha \\ y' = y + \beta \end{cases} \qquad \alpha, \beta \in \mathbb{F}_q,$$

is an automorphism of $\mathbb{K}(x,y)$. These automorphisms form the translation group T of $\mathrm{Aut}(\mathcal{C})$, and the fixed points of T are precisely the $q^2 - q$ points of $\mathcal{C}(\mathbb{F}_{q^2}) \cap \ell_\infty$, where ℓ_∞ is the line $z = 0$.

Let Q be the Sylow p-subgroup of $PGL(3,q)$ whose elements have matrix representation

$$\begin{pmatrix} 1 & 0 & \alpha \\ \gamma & 1 & \beta \\ 0 & 0 & 1 \end{pmatrix}$$

with α, β, γ in $\mathbb{F}_q$. A straightforward computation shows that the elements of Q fix the point $Y_\infty = (0:1:0)$, and those with $\gamma \neq 0$ have no further fixed point in $PG(2,\mathbb{K})$.

Now look at Q as a subgroup of $\mathrm{Aut}(\mathcal{C})$. Then Q contains T and the subgroup Φ consisting of all maps

$$\phi_\gamma = \begin{cases} x' = x \\ y' = \gamma x + y \end{cases} \quad ,$$

with $\gamma \in \mathbb{F}_q$. More precisely, $Q = T \rtimes \Phi$ where $|Q| = q^3, |T| = q^2$ and $|\Phi| = q$. Also, the quotient group $\bar{Q} = Q/T$ is an elementary abelian group of order q.

Since $Y_\infty \notin \mathcal{C}$, it turns out that no element in $Q \setminus T$ fixes a point in $\mathcal{C}$.

Furthermore, the maps

$$\psi_{\lambda,\mu} = \begin{cases} x' = \lambda x \\ y' = \mu y \end{cases} \quad ,$$

where $\lambda, \mu \in \mathbb{F}_q \setminus \{0\}$ are automorphisms of $\mathcal{C}$ and they form an abelian subgroup Ψ of $\mathrm{Aut}(\mathcal{C})$ of order $(q-1)^2$. When $\lambda = \mu$, the $q-1$ maps $\psi_{\lambda,\lambda}$ form the dilatation group D of $\mathrm{Aut}(\mathcal{C})$, and the fixed points of D are the q^2-q points of $\mathcal{C}(\mathbb{F}_{q^2})\cap\ell_\infty$. Also, the quotient group Ψ/D is a cyclic group of order $q-1$.

A straightforward computation shows that Ψ is contained in the normalizer of Q. Therefore, the group generated by them is the semidirect product $Q\rtimes\Psi$. Furthermore, Ψ is also contained in the normalizer of T. Hence the quotient group $(Q\rtimes\Psi)/T$ is isomorphic to the semidirect product $\bar{Q}\rtimes\bar{\Psi}$ where $\bar{\Psi}=(\Psi T)/T$. Observe that $\bar{Q}\rtimes\bar{\Psi}$ can be regarded as an automorphism group of the projective line ℓ_∞. Doing so, if $\ell_\infty=\{(1:m:0)|m\in\mathbb{K}\}\cup\{(0:1:0)\}$ then $\bar{Q}\rtimes\bar{\Psi}$ consists of all maps such that $(1:m:0)\mapsto(1:am+b:0)$ with a,b ranging over $\mathbb{K}$ and $a\neq 0$. Under the action of $\bar{Q}\rtimes\bar{\Psi}$, $\mathcal{C}(\mathbb{F}_{q^2})\cap\ell_\infty$ splits into $q-1$ orbits $\Delta_1,\ldots,\Delta_{q-1}$ each of size q.

Remark 2. Let S_p be a Sylow p-subgroup of $\mathrm{Aut}(\mathcal{C})$ containing Q. Assume that S_p is larger than Q. From Result 7, there exists a subgroup $U\leq S_p$ such that $Q\trianglelefteq U$ and that $[U:Q]=p^r$ for some $r\geq 1$. We show that $T\trianglelefteq U$. For any $u\in U$ and $t\in T$, the conjugate $t'=utu^{-1}$ of t by u has q^2-q fixed points. On the other hand, no element in $Q\setminus T$ has a fixed point in $\mathcal{C}$. Therefore, $t'\in T$, and hence $T\trianglelefteq U$. It turns out that U leaves $\mathcal{C}(\mathbb{F}_{q^2})\cap\ell_\infty$ invariant. Let $\hat{U}=U/T$, $\hat{Q}=Q/T$ and $\bar{U}=U/Q$. Then $\hat{U}$ is the permutation group induced by U on $\mathcal{C}(\mathbb{F}_{q^2})\cap\ell_\infty$. From $\hat{Q}\trianglelefteq\hat{U}$, the Q-orbit partition $\{\Delta_1,\ldots,\Delta_{q-1}\}$ is left invariant by $\hat{U}$. Since this partition has as many as $q-1$ members while p divides $|\hat{U}|$, this yields that $\hat{U}$ must fixes at least two members. In other words, $\bar{U}$ fixes at least two points of the quotient curve $\mathcal{Z}=\mathcal{C}/Q$ that will be investigated in Section 6.

6 Some quotient curves of the DGZ-curve

Let $\mathcal{Y}=\mathcal{C}/T$ be the quotient curve of the DGZ curve with respect to the group of translations T.

Proposition 6.1. *Let $\xi=x^q-x$ and $\eta=y^q-y$. Then the function field of $\mathcal{Y}$ is $\mathbb{K}(\xi,\eta)$ with $H(\xi,\eta)=0$ where $H(X,Y)\in\mathbb{F}_q[X,Y]$ is the absolutely irreducible polynomial such that*

$$H(X,Y)=\frac{X^{q^2-1}-Y^{q^2-1}}{X^{q-1}-Y^{q-1}}+1. \tag{11}$$

Proof. Since $\varphi_{\alpha,\beta}(\xi)=\varphi_{\alpha,\beta}(x^q)-\varphi_{\alpha,\beta}(x)=x^q+\alpha^q-(x+\alpha)=x^q-x=\xi$, $\mathbb{K}(\mathcal{Y})$ contains ξ. Similarly, $\eta\in\mathbb{K}(\mathcal{Y})$. Therefore, $\mathbb{K}(\xi,\eta)$ is a subfield of $\mathbb{K}(\mathcal{Y})$. On the other hand $[\mathbb{K}(\mathcal{C}):\mathbb{K}(\mathcal{Y})]=q^2$. As $[\mathbb{K}(\mathcal{C}):\mathbb{K}(\xi,y)]=q$ and $[\mathbb{K}(\xi,y):\mathbb{K}(\xi,\eta)]=q$, this shows that $[\mathbb{K}(\mathcal{C}):\mathbb{K}(\xi,\eta)]=q^2$, whence $\mathbb{K}(\xi,\eta)=\mathbb{K}(\mathcal{Y})$ follows. Since $q-1$ divides q^2-1, $H(X,Y)$ is a polynomial whose degree equals q^2-q. Furthermore,

$$F(x,y,1)=\frac{D_1(x,y,1)}{D_2(x,y,1)}=\frac{(\xi^{q^2}+\xi^q+\xi)(\eta^{q^2}+\eta^q)-(\eta^{q^2}+\eta^q+\eta)(\xi^{q^2}+\xi^q)}{(\xi^q+\xi)\eta^q-(\eta^q+\eta)\xi^q}.$$

Observe that right hand side can also be written as

$$\frac{\xi^{q^2-1} - \eta^{q^2-1} + \xi^{q-1} - \eta^{q-1}}{\xi^{q-1} - \eta^{q-1}}.$$

As $F(x, y, 1) = 0$, this yields $H(\xi, \eta) = 0$. Take an absolutely irreducible factor $L(X, Y)$ of $H(X, Y)$ so that $L(\xi, \eta) = 0$. Then the polynomial $M(X, Y) = L(X^q - X, Y^q - Y)$ has degree at most $q^3 - q^2$, and $M(x, y) = 0$. As $F(x, y) = 0$ this yields that $\deg F(X, Y) \leq \deg M(X, Y)$ whence $\deg M(X, Y) = q^3 - q^2$ follows. Hence, $\deg H(X, Y) = \deg L(X, Y)$ showing that $H(X, Y)$ is absolutely irreducible. □

Proposition 6.2. *Let P be a point of $\mathcal{X}$ where the cover $\mathcal{X}|\mathcal{Y}$ ramifies. Then the second ramification group at P is trivial.*

Proof. In terms of $\mathcal{C}$, the ramification points of the cover $\mathcal{X}|\mathcal{Y}$ are the fixed points of T. They are exactly the points of $\mathcal{C}$ lying on the line $z = 0$ at infinity. Therefore, $P = (1 : b : 0)$ with $b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. As in the proof of Proposition 4.4, P is taken to a point $R = (0 : b : 1)$ by the linear map σ with matrix representation

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

The image $\sigma(\mathcal{C})$ is an algebraic plane curve $\mathcal{D}$ isomorphic to $\mathcal{C}$. Furthermore, $\varphi_{\alpha,\beta}$, regarded as a linear map preserving $\mathcal{C}$, has matrix representation

$$\Lambda = \begin{pmatrix} 1 & 0 & \alpha \\ 0 & 1 & \beta \\ 0 & 0 & 1 \end{pmatrix}.$$

Since

$$\Sigma^{-1}\Lambda\Sigma = \begin{pmatrix} 1 & 0 & 0 \\ \beta & 1 & 0 \\ \alpha & 0 & 1 \end{pmatrix},$$

the map

$$\tilde{\varphi}_{\alpha,\beta} : (x, y) \mapsto \left(\frac{x}{\alpha x + 1}, \frac{y + \beta x}{\alpha x + 1} \right)$$

is an automorphism of $\mathcal{D}$. Therefore, R is a point of the algebraic plane curve $\mathcal{D} = \sigma(\mathcal{C})$, and the maps $\tilde{\varphi}_{\alpha,\beta}$ with $\alpha, \beta \in \mathbb{F}_q$ form a subgroup $\tilde{T}$ of $\mathrm{Aut}(\mathcal{D})$. We have to determine the second ramification group of $\tilde{T}$ at R. For this purpose, take $\bar{t} = \frac{x}{y-b}$ for a local parameter at R, and compute $v_R(\tilde{\varphi}_{\alpha,\beta}(\bar{t}) - \bar{t})$. A direct computation yields

$$\tilde{\varphi}_{\alpha,\beta}(\bar{t}) - \bar{t} = \tilde{\varphi}_{\alpha,\beta}\left(\frac{x}{y-b}\right) - \frac{x}{y-b} = \frac{x}{\alpha x + 1} \cdot \frac{\alpha x + 1}{\beta x + y - b(\alpha x + 1)} - \frac{x}{y-b} =$$

$$= x^2 \cdot \frac{(b\alpha - \beta)}{(x(\beta - b\alpha) + y - b)(y - b)}.$$

From (9) and Corollary 4.8, $\mathcal{D}$ has a unique branch $\bar{\gamma}$ centred at R with primitive representation

$$\begin{cases} x(t) = c_2 t^q \\ y(t) = b + d_2 t^{q-1} + \dots \end{cases},$$

then

$$\tilde{\varphi}_{\alpha,\beta}(\bar{t}) - \bar{t} = \frac{c_2 t^{2q}(b\alpha - \beta)}{(c_2 t^q(\beta - b\alpha) + d_2 t^{q-1})t^{q-1} + \dots} = t^2 + h(t)$$

with $\mathrm{ord}(h) > 2$. So $v_R(\tilde{\varphi}_{\alpha,\beta}(\bar{t}) - \bar{t}) = 2$ and the assertion follows. □

Proposition 6.3. *The curve $\mathcal{Y}$ has genus $\mathfrak{g}(\mathcal{Y}) = \frac{1}{2}(q-1)(q^2-2q-2)+1$.*

Proof. From the proof of Proposition 6.2, the cover $\mathcal{X}|\mathcal{Y}$ ramifies at the points of $\mathcal{C}$ on the line ℓ_∞. This, together with Proposition 6.2, gives

$$\sum_{P\in\ell_\infty} d_P = \sum_{P\in\ell_\infty} (|G_P^{(i)}|-1) = \sum_{P\in\ell_\infty} ((|G_P^{(0)}|-1)+(|G_P^{(1)}|-1)) = 2(q^2-1)(q^2-q).$$

Now, from the Hurwitz genus formula, the assertion follows. □

Since the normalizer of T is larger than T, some more quotient curves of $\mathcal{Y}$ (and hence of $\mathcal{X}$) arise.

As pointed out in Section 5, a subgroup of $\mathrm{Aut}(\mathcal{Y})$ of order q is $\Phi := \{\phi_\gamma \mid \gamma \in \mathbb{F}_q\}$, where

$$\phi_\gamma : (\xi, \eta) \mapsto (\xi, \gamma\xi + \eta).$$

Let $\mathcal{Z} = \mathcal{Y}/\Phi$ be the quotient curve of $\mathcal{Y}$ with respect to Φ. To find an equation for $\mathcal{Z}$ it is useful to represent $\mathbb{K}(\mathcal{Y})$ in the form $\mathbb{K}(v, w)$ with $v = \eta\xi^{-1}$ and $w = \xi^{-1}$, equivalently, $\xi = w^{-1}$ and $\eta = vw^{-1}$. From $H(\xi, \eta) = 0$, we have $M(v, w) = 0$ where $M(X, Y)$ is the absolutely irreducible polynomial defined by

$$M(X,Y) = \frac{X - X^{q^2}}{X - X^q} + Y^{q^2-q} = 1 + X^{q-1} - X^{q(q-1)} + Y^{q(q-1)}. \qquad (12)$$

This shows that $\mathbb{K}(\mathcal{Y}) = \mathbb{K}(v, w)$ with $M(v, w) = 0$. With this notation,

$$\phi_\gamma : (v, w) \mapsto (v + \gamma, w).$$

Proposition 6.4. *Let $\theta := v - v^q$ and $\sigma := w$. Then the function field of $\mathcal{Z}$ coincides with the function field $\mathbb{K}(\theta, \sigma)$ defined by*

$$1 + \theta^{q-1} + \sigma^{q(q-1)} = 0, \qquad (13)$$

that is $\mathcal{Z}$ has equation $R(X, Y) = 1 + X^{q-1} + Y^{q(q-1)} = 0$.

Proof. As in the proof of Proposition 6.1, $\phi_\gamma(\theta)=\theta$ and $\phi_\gamma(\sigma)=\sigma$ shows that $\mathbb{K}(\theta,\sigma)$ is a subfield of $\mathbb{K}(\mathcal{Z})$. On the other hand $[\mathbb{K}(\mathcal{Y}):\mathbb{K}(\mathcal{Z})]=q$. Since $[\mathbb{K}(\mathcal{Y}):\mathbb{K}(\theta,w)]=q$ and $\mathbb{K}(\theta,w)=\mathbb{K}(\theta,\sigma)$, then $[\mathbb{K}(\mathcal{Y}):\mathbb{K}(\theta,\sigma)]=q$, whence $\mathbb{K}(\theta,\sigma)=\mathbb{K}(\mathcal{Z})$ follows. On the other hand,

$$R(\theta,\sigma)=1+\theta^{q-1}+\sigma^{q(q-1)}=1+v^{q-1}-v^{q(q-1)}+w^{q(q-1)}=M(v,w)=0.$$

□

Proposition 6.5. *The curve $\mathcal{Z}$ is isomorphic to the Fermat curve of degree $q-1$.*

Proof. Let $\mathbb{K}(\mathcal{F}_{q-1})=\mathbb{K}(s,t)$ with $s^{q-1}+t^{q-1}+1=0$ be the function field of the Fermat curve $\mathcal{F}_{q-1}$ of degree $q-1$. Then the map

$$\begin{array}{c}\mathbb{K}(\mathcal{F}_{q-1})\to\mathbb{K}(\mathcal{Z})\\ (s,t)\to(s^q,t)\end{array}$$

is an isomorphism from $\mathcal{F}_{q-1}$ to $\mathcal{Z}$, since $R(s^q,t)=1+(s^q)^{q-1}+t^{q(q-1)}=(1+s^{q-1}+t^{q-1})^q=0$. □

Remark 3. Proposition 6.5 shows that $\mathcal{Z}$ is a line for $q=2$ while it is an irreducible conic for $q=3$.

Remark 4. Let $\gamma(\mathcal{F}_{q-1})$ denote the p-rank of $\mathcal{F}_{q-1}$. Since Q leaves ℓ_∞ invariant and T is the subgroup of Q fixing ℓ_∞ pointwise, each of the q^2-q common points of $\mathcal{C}$ with ℓ_∞ is fixed by exactly q^2 elements of Q. Furthermore, each point on a line of $PG(2,\mathbb{F}_q)$ through P_∞ is fixed by exactly q elements of Q, and hence each of the $q(q^2-q)$ common points of $\mathcal{C}$ with such lines is fixed by exactly q elements of Q. No more point of $\mathcal{C}$ is fixed by some nontrivial element of Q. From Proposition 6.5 and Deuring Shafarevic formula applied to Q,

$$\gamma(\mathcal{C})=q^3(\gamma(\mathcal{F}_{q-1})-1)+(q^2-q)(q^2-1)+q(q^2-q)(q-1)+1.$$

This shows that $\gamma(\mathcal{F}_{q-1})$ determines $\gamma(\mathcal{C})$ and viceversa. Unfortunately, $\gamma(\mathcal{F}_{q-1})$ is only known for $q=p$ in which case $\mathcal{F}_{p-1}$ is ordinary and hence $\gamma(\mathcal{F}_{p-1})=\frac{1}{2}(p-2)(p-3)$; see [24]. In this case $\gamma(\mathcal{C})=\frac{1}{2}p(p-1)(p^3-2p-2)+1$ which shows that $\mathcal{C}$ is ordinary, as well. For $q>p$, $\mathcal{F}_{q-1}$ and hence $\mathcal{C}$ are not ordinary although both have positive p-rank; see [24].

7 The full automorphism group of the DGZ curve

This section is devoted to a deeper investigation of the automorphism group of $\mathcal{C}$. By Lemma 4.1, $\mathrm{Aut}(\mathcal{C})$ contains a subgroup $G\cong PGL(3,\mathbb{F}_q)$. Our goal is to prove that $\mathrm{Aut}(\mathcal{C})=G$. This result is true for $q=2$; see Remark 1.

Proposition 7.1. *Q is a Sylow p-subgroup of* $\mathrm{Aut}(\mathcal{C})$.

Proof. We adopt notation and hypotheses from Remark 2.

From Proposition 6.5, $\bar{U}$ can be regarded as a p-subgroup of $\mathrm{Aut}(\mathcal{F}_{q-1})$. As $|\mathrm{Aut}(\mathcal{F}_{q-1})| = 6(q-1)^2$, this is only possible for $p \le 3$.

Let $p = 3$. Then a Sylow p-subgroup of $\mathrm{Aut}(\mathcal{F}_{q-1})$ has order 3 and its nontrivial elements are σ and σ^2 where $\sigma(x, y, z) = (y, z, x)$. Since $p = 3$, σ (and also σ^2) viewed as an automorphism of $PG(2, \mathbb{K})$ has a unique fixed point, namely $(1 : 1 : 1)$ which is not a point of $\mathcal{F}_{q-1}$. Actually, this holds true for $\bar{U}$ as $\bar{U}$ is also a Sylow p-subgroup of $\mathrm{Aut}(\mathcal{F}_{q-1})$. On the other hand, from Remark 2, $\bar{U}$ has a fixed point in $\mathcal{F}_{q-1}$. This contradiction rules out the case $p = 3$.

Let $p = 2$. This time a Sylow p-subgroup of $\mathrm{Aut}(\mathcal{F}_{q-1})$ has order 2 and its nontrivial element is $\sigma(x, y, z) = (y, x, z)$. In particular, σ viewed as an automorphism of $PG(2, \mathbb{K})$ fixes the line $x = y$ pointwise but no further point. Just one fixed point of σ, namely $(1, 1, 0)$ is in $\mathcal{F}_{q-1}$. This remains true for $\bar{U}$ as $\bar{U}$ is also a Sylow p-subgroup $\mathrm{Aut}(\mathcal{F}_{q-1})$. On the other hand, from Remark 2, $\bar{U}$ has at least two fixed points in $\mathcal{F}_{q-1}$. This contradiction rules out the case $p = 2$. □

Proposition 7.2. $\mathrm{Aut}(\mathcal{C})$ *has exactly two short orbits* Ω *and* Δ *where* Ω *is non-tame and* Δ *is tame.*

Proof. From the proof of Proposition 4.4, the set of $q^4 - q$ points lying in $PG(2, \mathbb{F}_{q^2}) \setminus PG(2, \mathbb{F}_q)$ is an orbit under the action of $PGL(3, q)$ and the stabiliser in $PGL(3, q)$ of any such point has order $q^2(q^2 - 1)$ by Result 6. Therefore $\mathcal{C}$ has a non-tame short orbit Ω under the action of $\mathrm{Aut}(\mathcal{C})$.

We show that $\mathrm{Aut}(\mathcal{C})$ has a short tame orbit Δ, as well. From Lemma 4.9, $\mathcal{C}(\mathbb{F}_{q^3})$ consists of all points in Λ_3. Take $P \in \mathcal{C}(\mathbb{F}_{q^3})$ and assume by contradiction that there exists a group $D \le \mathrm{Aut}(\mathcal{C})_P$ such that $|D| = p^l$ for some $l \ge 1$. Let S_p a Sylow p-subgroup of $\mathrm{Aut}(\mathcal{C})$ containing D. Then S_p and Q are conjugate in $\mathrm{Aut}(\mathcal{C})$, that is, $Q = \gamma S_p \gamma^{-1}$ for some $\gamma \in \mathrm{Aut}(\mathcal{C})$. Let $U = \gamma D \gamma^{-1}$ and $P' = \gamma(P)$. Then $U(P') = P'$. As no element in $Q \setminus T$ fixes a point in $\mathcal{C}$, U is a subgroup of T and $P' \in \mathcal{C}(\mathbb{F}_{q^2})$. Also, the set of all fixed points of T in $\mathcal{C}(\mathbb{F}_{q^2})$ has size $q^2 - q$. Let $M = \gamma^{-1} T \gamma$. Then M also has exactly $q^2 - q$ fixed points, and the stabiliser of P in S_p coincides with M. Let C_{q^2+q+1} be the Singer subgroup of $\mathrm{Aut}(\mathcal{C})$ fixing P. Then C_{q^2+q+1} fixes exactly two other points in $PG(2, \mathbb{F}_{q^3})$ and no non-trivial element of C_{q^2+q+1} fixes a further point. From Result 1, C_{q^2+q+1} normalizes M. Therefore, the set of fixed points of M is left invariant by C_{q^2+q+1}. Since $q^2 + q + 1 > q^2 - q > 3$, this yields that some nontrivial element in C_{q^2+q+1} has more than three fixed points, a contradiction.

Therefore, Ω and Δ are short orbits of $\mathrm{Aut}(\mathcal{C})$. From Result 3, either they are the only short orbits of $\mathrm{Aut}(\mathcal{C})$, or there exists just one further tame short orbit of $\mathrm{Aut}(\mathcal{C})$. The latter possibility may be investigated as in the proof of Result 3. From (III) in that proof, this possibility may only occur when $p > 2$ and $|\mathrm{Aut}(\mathcal{C})_P| = 2$ for the stabiliser of each point P in the tame orbits. But in our case, if $P \in \mathcal{C}(\mathbb{F}_{q^3})$, the Singer subgroup of $\mathrm{Aut}(\mathcal{C})$ fixing P has order $q^2 + q + 1 > 2$; a contradiction. □

Theorem 7.3. $\mathrm{Aut}(\mathcal{C}) \cong PGL(3, q)$.

Proof. Take a point $P \in \Omega$ and a point $R \in \Delta$. Proposition 7.2 together with the Hurwitz genus formula applied to $\Gamma = \mathrm{Aut}(\mathcal{C})$ give

$$2\mathfrak{g}(\mathcal{C}) - 2 = |\Gamma|(2\bar{\mathfrak{g}} - 2) + |\Omega| d_P + |\Delta| d_R \tag{14}$$

where $\bar{\mathfrak{g}} = \mathfrak{g}(\mathcal{X}/\Gamma)$. Since $|\Gamma| > 84(\mathfrak{g}(\mathcal{C}) - 1)$ for $q > 2$, Result 3 yields $\bar{\mathfrak{g}} = 0$. Furthermore, $|\Gamma_P| \geq q^2(q^2-1)$ and $|\Gamma_P^{(1)}| = q^2$. Actually, $|\Gamma_P| = q^2(q^2-1)$ and $\Gamma_P^{(2)}$ is trivial by Result 2. Then (14) reads

$$2\mathfrak{g}(\mathcal{C}) - 2 = -2|\Gamma| + \frac{|\Gamma|}{|\Gamma_P|}(|\Gamma_P| - 1 + |\Gamma_P^{(1)}| - 1) + \frac{|\Gamma|}{|\Gamma_R|} d_R \tag{15}$$

As Γ_R does not contain p-elements, $d_R = (|\Gamma_R| - 1)$ and (15) reads

$$2\mathfrak{g}(\mathcal{C}) - 2 = \frac{|\Gamma|}{|\Gamma_P|}\left(q^2\left(1 - \frac{q^2-1}{|\Gamma_R|}\right) - 2\right).$$

Furthermore, $|\Gamma_R| = \lambda(q^2+q+1)$ with $\lambda \geq 1$ as R is a fixed point of a Singer subgroup of $PGL(3,q)$. Therefore,

$$1 - \frac{q^2-1}{|\Gamma_R|} = \frac{(\lambda-1)q^2 + \lambda q + \lambda + 1}{\lambda(q^2+q+1)} > \frac{\lambda - 1}{\lambda}.$$

Suppose $\lambda > 1$. From (15),

$$2\mathfrak{g}(\mathcal{C}) - 2 = \frac{|\Gamma|}{|\Gamma_P|}\left(q^2\left(1 - \frac{q^2-1}{|\Gamma_R|}\right) - 2\right) > \frac{|\Gamma|}{|\Gamma_P|}\left(\frac{q^2}{2} - 2\right),$$

that is impossible since $|\Gamma| \geq q^3(q^3-1)(q^2-1)$. Hence $\lambda = 1$ and $|\Gamma_R| = q^2+q+1$. Finally, (15) yields

$$|\Gamma| = q^3(q^3-1)(q^2-1) = |PGL(3,q)|.$$

□

8 The Geometry of the DGZ-curve

We show that $\mathcal{C}$ has exceptional geometric properties, as well.

Proposition 8.1. *The DGZ curve is non-classical and $\mathbb{F}_q$-Frobenius non-classical.*

Proof. Let

$$G_1(x,y,z) = yz^{q^2} - y^{q^2}z,\ G_2(x,y,z) = x^{q^2}z - xz^{q^2},\ G_0(x,y,z) = xy^{q^2} - x^{q^2}y.$$

A straightforward computation shows that Equation (6) can also be written as $D_2F = G_1^q x + G_2^q y + G_0^q z$. By (4) with $H = D_2$ and $q = p^m$, $\mathcal{C}$ is non-classical. Furthermore, $G_1x + G_2y + G_0z$ is the zero polynomial. This shows that $\mathcal{C}$ is q-Frobenius non-classical. □

Obviously, $\mathcal{C}$ may be regarded as a curve defined over $\mathbb{F}_{q^i}$ with $i \geq 1$. For $q = 2$, $\mathcal{C}$ has equation (7). Then [23, Section 3] yields that $\mathcal{C}$ is $\mathbb{F}_8$-Frobenius non-classical. We prove that Top's result holds for any q.

Proposition 8.2. *The DGZ curve is $\mathbb{F}_{q^3}$-Frobenius non-classical.*

Proof. From Proposition 8.1, $\mathcal{C}$ is non-classical. A straightforward computation shows that $G_1x^{q^2}+G_2y^{q^2}+G_0z^{q^2}$ is the zero polynomial so the assertion follows from equation (5). □

Let ℓ be a line of $PG(2,\mathbb{F}_q)$. From Lemma 4.6, the intersection divisor of $\mathcal{C}$ cut out by ℓ is

$$V = \sum_{i=1}^{q^2-q} qP_i$$

where $P_1,\ldots,P_{q^2-q}$ are the common points of $\mathcal{C}$ and ℓ. Therefore, the ramification divisor of $\mathcal{L}$ is

$$R = \mathrm{div}(W_R) + (q+1)\mathrm{div}(dx) + 3V,$$

and $\deg(R) = (q+1)(2\mathfrak{g}(\mathcal{C})-2) + 3(q^3-q^2) = q(q-1)(q^4+q^3-2q^2-q-2)$. Furthermore, Proposition 8.1 yields $(\varepsilon_0,\varepsilon_1,\varepsilon_2) = (0,1,q)$.

In terms of $(\mathcal{L},P)$-orders, Lemma 4.6 is stated in the following lemma.

Lemma 8.3. *For $P \in \mathcal{C}(\mathbb{F}_{q^2})$, the $(\mathcal{L},P)$-order sequence is $(0,q-1,q)$, and $v_P(R) = q-2$.*

Proof. Let $P \in \mathcal{C}(\mathbb{F}_{q^2})$. Then the $(\mathcal{L},P)$-order sequence is $(0,q-1,q)$ as a consequence of Lemma 4.6. Furthermore, observe that the matrix $\left(\binom{j_i}{\varepsilon_k}\right)$ has determinant $q-1 \not\equiv 0 \pmod p$. Therefore $v_P(R) = q-2$ from [11, Theorem 7.55]. □

Lemma 8.4. *For a point $P \notin \mathcal{C}(\mathbb{F}_{q^2}) \cup \mathcal{C}(\mathbb{F}_{q^3})$, the $(\mathcal{L},P)$-order sequence is $(0,1,q)$, and $v_P(R) = 0$.*

Proof. Assume on the contrary that $v_P(R) = m > 0$ for some point $P \in \Gamma$ with $\Gamma = \mathcal{C} \setminus (\mathcal{C}(\mathbb{F}_{q^2}) \cup \mathcal{C}(\mathbb{F}_{q^3}))$. Since $\mathcal{C}(\mathbb{F}_q) = \emptyset$ by Proposition 4.3, the orbit of P in $\mathrm{Aut}(\mathcal{C})$ is long by Proposition 7.2. Therefore

$$\sum_{P\in\Gamma} v_P(R) = m|PGL(3,q)| = mq^3(q^3-1)(q^2-1).$$

But this contradicts $\deg(R) = q(q-1)(q^4+q^3-2q^2-q-2)$. Then $v_P(R) = 0$ for any point $P \notin \mathcal{C}(\mathbb{F}_{q^2}) \cup \mathcal{C}(\mathbb{F}_{q^3})$ and the $(\mathcal{L},P)$-order sequence is $(0,1,q)$. □

Lemma 8.5. *For $P \in \mathcal{C}(\mathbb{F}_{q^3})$, the $(\mathcal{L},P)$-order sequence is $(0,1,q+1)$, and $v_P(R) = 1$.*

Proof. Let $v_P(R) = m$ for a point $P \in \mathcal{C}(\mathbb{F}_{q^3})$. Since $\mathcal{C}(\mathbb{F}_{q^3})$ is an orbit of $\mathrm{Aut}(\mathcal{C})$, we have $v_P(R) = m$ for every $P \in \mathcal{C}(\mathbb{F}_{q^3})$. From Lemmas 8.3 and 8.4, $q(q-1)(q^4+q^3-2q^2-q-2) = \deg(R) = (q-2)(q^4-q) + m(q^6-q^5-q^4+q^3)$, whence $m = 1$. In particular, $j_2 \geq q+1$. On the other hand, if $j_2 > q+1$ then $v_P(R) \geq \sum_{i=0}^{2}(j_i - \varepsilon_i) > 1$ by [11, Theorem 7.55]. Therefore, $j_2 = q+1$. □

As a corollary we have the following result.

Proposition 8.6.

$$v_P(R) = \begin{cases} q-2, & \text{for } P \in \mathcal{C}(\mathbb{F}_{q^2}), \\ 1, & \text{for } P \in \mathcal{C}(\mathbb{F}_{q^3}), \\ 0, & \text{otherwise} . \end{cases}$$

Since $\mathcal{L}$ is defined over $\mathbb{F}_q$, $\mathcal{C}$ also has its $\mathbb{F}_q$-Frobenius order sequence (ν_0, ν_1). In our case $\nu_0 = 0$ and $\nu_1 = q$ by Proposition 8.1, and the Stöhr-Voloch divisor of $\mathcal{L}$ over $\mathbb{F}_q$ is

$$S = \mathrm{div}(W_S) + q\mathrm{div}(dx) + (q+2)V.$$

Thus $\deg(S) = q(2\mathfrak{g}(\mathcal{C}) - 2) + (q+2)(q^3-q^2) = q^6 - q^5 - q^4 + q^3$.

Proposition 8.7.

$$v_P(S) = \begin{cases} 1, & \text{for } P \in \mathcal{C}(\mathbb{F}_{q^3}), \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Replacing R with S in the proof of Lemma 8.4 we see that $v_P(S) = 0$ for $P \in \mathcal{C} \setminus (\mathcal{C}(\mathbb{F}_{q^2}) \cup \mathcal{C}(\mathbb{F}_{q^3}))$. Let $m_1 = v_P(S)$ for $P \in \mathcal{C}(\mathbb{F}_{q^3})$ and $m_2 = v_P(S)$ for $P \in \mathcal{C}(\mathbb{F}_{q^2})$. Then $q^6-q^5-q^4+q^3 = \deg(S) = m_1(q^6-q^5-q^4+q^3)+m_2(q^4-q)$, whence $m_1 = 1$ and $m_2 = 0$ follow. □

Lemma 8.8. *Let $\mathcal{D}$ be a plane absolutely irreducible curve defined over $\mathbb{F}_{q^3}$ which is non-classical with order sequence $(0, 1, p^\alpha q)$, $\alpha \geq 0$. Then $\alpha = 0$ if $\mathcal{D}$ has the following properties:*

(i) $\deg(\mathcal{D}) = \deg(\mathcal{C}) = q^3 - q^2$,

(ii) $|\mathbb{F}_{q^3}(\mathcal{U})| \geq |\mathbb{F}_{q^3}(\mathcal{C})| = q^6 - q^5 - q^4 + q^3$, *where $\mathcal{U}$ is a nonsingular model of $\mathcal{D}$ defined over $\mathbb{F}_{q^3}$.*

Proof. Let Ω denote the set of all branches of $\mathcal{D}$ which correspond to the $\mathbb{F}_{q^3}$-rational points of $\mathcal{U}$. Each branch $\gamma \in \Omega$ is centered at a point in $PG(2, \mathbb{F}_{q^3})$. For any line ℓ of $PG(2, \mathbb{F}_{q^3})$, a pair (γ, ℓ) is called *incident* if the center of γ lies on ℓ.

Obviously, we have as many as $|\Omega|(q^3+1)$ incident branch-line pairs (γ, ℓ). On the other hand, for any line ℓ of $PG(2, \mathbb{F}_{q^3})$, let $\lambda(\ell)$ denote the number of branches in Ω whose center lies on ℓ. The double counting of such incident branch-line pairs gives

$$|\Omega|(q^3+1) = \sum_{\ell \in PG(2,\mathbb{F}_{q^3})} \lambda(\ell). \tag{16}$$

It is useful to divide the lines of $PG(2,\mathbb{F}_{q^3})$ into two families: Σ_1 comprises all lines ℓ which are tangent to some branches in Ω, while Σ_2 consists of the remaining lines. For a line $\ell \in \Sigma_1$ which is tangent to $\gamma \in \Omega$, the intersection number $I(\gamma, \mathcal{D} \cap \ell) \geq qp^\alpha$. Therefore, if $\gamma_1, \ldots, \gamma_{r_\ell} \in \Omega$ are the branches in Ω tangent to ℓ then Bézout's theorem yields

$$\lambda(\ell) = |\mathcal{D} \cap \ell| \leq (q^3 - q^2) - r_\ell q p^\alpha, \text{ for } \ell \in \Sigma_1.$$

Since each γ has a unique tangent, we have $\sum_{\ell \in \Sigma_1} r_\ell = |\Omega|$. Furthermore, if $\ell \in \Sigma_2$ then the obvious upper bound on $\lambda(\ell)$ is $q^3 - q^2$. From (16),

$$|\Omega|(q^3 + 1) + |\Omega| p^\alpha q \leq (q^6 + q^3 + 1)(q^3 - q^2).$$

This together with (ii) give

$$(q^6 - q^5 - q^4 + q^3)(q^3 + 1 + p^\alpha q) \leq (q^6 + q^3 + 1)(q^3 - q^2),$$

whence $\alpha = 0$ follows. □

Proposition 8.9. *Let $\mathcal{D}$ be a plane absolutely irreducible curve defined over $\mathbb{F}_{q^3}$ such that*

(I) $\deg(\mathcal{D}) = \deg(\mathcal{C}) = q^3 - q^2$,

(II) $\mathfrak{g}(\mathcal{D}) = \mathfrak{g}(\mathcal{C}) = \frac{1}{2}q(q-1)(q^3 - 2q - 2) + 1$,

Then $|\mathbb{F}_{q^3}(\mathcal{U})| \leq |\mathbb{F}_{q^3}(\mathcal{C})|$, where $\mathcal{U}$ is a nonsingular model of $\mathcal{D}$ defined over $\mathbb{F}_{q^3}$.

Proof. Let $\mathcal{L}'$ be the 2-dimensional linear series cut out on $\mathcal{D}$ by lines. Then the Stöhr-Voloch divisor S' of $\mathcal{L}$ over $\mathbb{F}_{q^3}$ has degree

$$\deg(S') = \nu'(2\mathfrak{g}(\mathcal{D}) - 2) + (q^3 + 2)(q^3 - q^2)$$

where ν' is the $\mathbb{F}_{q^3}$-Frobenius order of $\mathcal{D}$. Assume that $|\mathbb{F}_{q^3}(\mathcal{U})| \geq |\mathbb{F}_{q^3}(\mathcal{C})|$. Then either $\mathcal{D}$ is $\mathbb{F}_{q^3}$-Frobenius classical, or Lemma 8.8 yields $\nu' \leq q$. In both cases $1 \leq \nu' \leq q$. This together with (I) and (II) yield $\deg(S') \leq \deg(S)$. Therefore,

$$\sum_{P' \in \mathbb{F}_{q^3}(\mathcal{U})} v_P(S') \leq \sum_{P \in \mathbb{F}_{q^3}(\mathcal{C})} v_P(S). \tag{17}$$

Since $v_{P'}(S') \geq 1$ for any $P' \in \mathbb{F}_{q^3}(\mathcal{U})$ while $v_P(S) = 1$ for any $P \in \mathbb{F}_{q^3}(\mathcal{C})$ by Proposition 8.7, (17) yields $|\mathbb{F}_{q^3}(\mathcal{U})| = |\mathbb{F}_{q^3}(\mathcal{C})|$. □

Proposition 8.9 has the following corollary.

Corollary 8.10. *The DGZ curve is a $(q^3 - q^2, \frac{1}{2}q(q-1)(q^3 - 2q - 2) + 1, 3)$ optimal curve over $\mathbb{F}_{q^3}$.*

Remark 5. Proposition 8.9 remains valid if $\mathbb{F}_{q^3}(\mathcal{U})$ is replaced by the set $\mathbb{F}_{q^3}(\mathcal{D})$ of all points of $\mathcal{D}$ lying on $PG(2, \mathbb{F}_{q^3})$. In fact, the proof of Proposition 8.9 still works whenever Ω stands for $\mathbb{F}_{q^3}(\mathcal{D})$ and $\sum_{\ell \in \Sigma_1} r_\ell = |\Omega|$ is replaced by $\sum_{\ell \in \Sigma_1} r_\ell \geq |\Omega|$.

Finally we point out a combinatorial property of $\mathcal{C}(\mathbb{F}_{q^3})$. For this purpose, recall that a (k, n)-arc $\mathcal{K}$ in the projective plane Π consists of k points in Π such that some line in Π meets $\mathcal{K}$ in exactly n pairwise distinct points but no line in Π meets $\mathcal{K}$ in more than $n+1$ points. Furthermore, $\mathcal{K}$ is called complete, that is, it is maximal, if no point $P \in \Pi$ other than those in $\mathcal{K}$ exists such that $\mathcal{K} \cup \{P\}$ is a $(k+1, n)$-arc. Complete (k, n)-arcs, especially $(k, 2)$-arcs, have intensively been investigated in Finite geometry, and they have relevant applications in Coding theory; see [9] and [11, Chapter 13]. In that context, an interesting problem is to find plane curves $\mathcal{D}$ defined over a finite field $\mathbb{F}$ whose set of points in $PG(2, \mathbb{F})$ is a complete (k, n)-arc. It seems plausible that only a few curves with such combinatorial property may exist, see [6]. Our contribution in this direction is the following result.

Proposition 8.11. *The set* $\mathcal{C}(\mathbb{F}_{q^3})$ *is a complete* $(q^6 - q^5 - q^4 + q^3, q^3 - q^2)$*-arc.*

Proof. From a combinatorial point of view, $\mathcal{C}(\mathbb{F}_{q^3})$ consists of all points in $PG(2, \mathbb{F}_{q^3})$ which are uncovered by lines defined over $\mathbb{F}_q$. Through a point P in $PG(2, \mathbb{F}_q)$, there are as many as $q^3 + 1$ lines defined over $\mathbb{F}_{q^3}$. Those of them which are also defined over $\mathbb{F}_q$ are $q+1$, whereas the remaining $q^3 - q$ lines defined over $\mathbb{F}_{q^3}$ meet $PG(2, \mathbb{F}_q)$ only in P. Choose one of these $q^3 - q$ lines, say ℓ. Then ℓ meets a line r defined over $\mathbb{F}_q$ in a point distinct from P if and only if $P \notin r$. Furthermore, any two lines r and s both defined over $\mathbb{F}_q$ meet ℓ in two different points whenever $P \notin r$ and $P \notin s$. Since the number of lines defined over $\mathbb{F}_q$ equals $q^2 + q + 1$ and $q + 1$ of them contain P, a counting argument shows that $\ell \cap \mathcal{C}(\mathbb{F}_{q^3}) = q^3 - q^2$. On the other hand, since $\deg(\mathcal{C}) = q^3 - q^2$, no line meets $\mathcal{C}(\mathbb{F}_{q^3})$ in more than $q^3 - q^2$ points. Therefore, $\mathcal{C}(\mathbb{F}_{q^3})$ is a (k, n)-arc in $PG(2, \mathbb{F}_{q^3})$ with $k = q^6 - q^5 - q^4 + q^3$ and $n = q^3 - q^2$. To show that such a (k, n)-arc is complete, take any point $Q \in PG(2, \mathbb{F}_{q^3}) \setminus \mathcal{C}(\mathbb{F}_{q^3})$. Choose a point in $P \in PG(2, \mathbb{F}_q)$ not lying on the unique line through Q which is defined over $\mathbb{F}_q$. Then the line ℓ through P and Q is one of the $q^3 - q$ lines defined over $\mathbb{F}_{q^3}$ which meet $PG(2, \mathbb{F}_q)$ only in P. As we have seen, ℓ meets $\mathcal{C}(\mathbb{F}_{q^3})$ in exactly $n = q^3 - q^2$ points. Since ℓ also contains Q, this yields that Q cannot be added to $\mathcal{C}(\mathbb{F}_{q^3})$ in such a way that the resulting point-set $\mathcal{C}(\mathbb{F}_{q^3}) \cup \{Q\}$ is a $(k+1, n)$-arc. In other words, $\mathcal{C}(\mathbb{F}_{q^3})$ is complete. □

References

[1] N. Arakelian and H. Borges, Frobenius nonclassicality with respect to linear systems of curves of arbitrary degree. *Acta Arith.* **167** (2015), 43-66.

[2] H. Borges, Frobenius nonclassical components of curves with separated variables, *J. Number Theory* **159** (2016), 402-425.

[3] H. Borges and R. Conceição, A new family of Castle and Frobenius nonclassical curves, *J. Pure Appl. Algebra* **222** (2018), 994-1002.

[4] H. Borges and M. Homma, Points on singular Frobenius nonclassical curves, *Bull. Braz. Math. Soc. (N.S.)* **48** (2017), 93-101.

[5] L. E. Dickson, A fundamental system of invariants of the general modular linear group with a solution of the form problem, *Trans. Am. Math. Soc.* **12** (1911), 75-98.

[6] M. Giulietti, F. Pambianco, F. Torres, E. Ughi, On complete arcs arising from plane curves, *Des. Codes Cryptogr.* **25** (2002), 237-246 .

[7] R.M. Guralnick and M.E. Zieve, Work on Automorphisms of Ordinary Curves, in preparation (Talk in Leiden, Workshop on Automorphism of Curves, 18-08-2004).

[8] R.W. Hartley, The ternary collineation groups whose coefficients lie in the $GF(2^n)$, *Annals of Mathematics*, **27** (1925), 140-158.

[9] J. W. P. Hirschfeld, *Projective geometries over finite fields*, Second edition. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1998.

[10] J.W.P. Hirschfeld and G. Korchmáros, Arcs and curves over a finite field, *Finite Fields Appl.* **5** (1999), 393–408.

[11] J.W.P. Hirschfeld, G. Korchmáros and F. Torres, *Algebraic curves over a finite field*, Princeton Univ. Press, 2008.

[12] G. Korchmáros and M. Montanucci, Ordinary algebraic curves with many automorphisms in positive characteristic, arXiv:1701.02186 [math.AG].

[13] A. Kontogeorgis and V. Rotger, On abelian automorphism groups of Mumford curves, *Bull. London Math. Soc.* **40** (2008), 353-362.

[14] A. Machí, *Groups, An introduction to ideas and methods of the theory of groups*, Unitext, **58**, Springer, Milan, 2012.

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

[16] S. Nakajima, p-ranks and automorphism groups of algebraic curves, *Trans. Amer. Math. Soc.* **303** (1987), 595607.

[17] J.P. Serre, *Local Fields*, Graduate Texts in Mathematics **67**, Springer, New York, 1979. viii+241 pp.

[18] J.P. Serre, Rational points on curves over finite fields, Lectures given at Harvard University, 1985. Notes by F. Q. Gouvea.

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

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

[21] K.O. Stöhr and J.F Voloch, Weierstrass points and curves over finite fields, *Proc. London Math. Soc.* **52** (1986), 1-19.

[22] F. Sullivan, p-torsion in the class group of curves with many automorphisms, *Arch. Math.* **26** (1975), 253–261.

[23] J. Top, Curves of genus 3 over small finite fields *Indag. Mathem., N.S.,* **14** (2003), 275-283.

[24] Noriko, Yui, On the Jacobian variety of the Fermat curve, *J. Algebra* **65** (1980), 1-35.