On large automorphism groups of algebraic curves in positive characteristic

M. Giulietti * and G. Korchmáros *

February 23, 2013

Abstract

In his investigation on large K-automorphism groups of an algebraic curve, Stichtenoth obtained an upper bound on the order of the first ramification group of an algebraic curve $\mathcal{X}$ defined over an algebraically closed field of characteristic p. Stichtenoth's bound has raised the problem of classifying all $\mathbb{K}$-automorphism groups G of $\mathcal{X}$ with the following property: There is a point $P \in \mathcal{X}$ for which

$$|G_P^{(1)}| > \frac{p}{p-1} g. \tag{1}$$

Such a classification is obtained here by proving Theorem 1.3

1 Introduction

Let $\mathbb{K}$ be an algebraically closed field of characteristic $p \geq 0$. Let $\mathrm{Aut}(\mathcal{X})$ be the $\mathbb{K}$-automorphism group of a (projective, non-singular, geometrically irreducible, algebraic) curve $\mathcal{X}$ embedded in an r-dimensional projective space $\mathrm{PG}(r, \mathbb{K})$. If $\mathcal{X}$ has genus $g \geq 2$, then $\mathrm{Aut}(\mathcal{X})$ is finite, but this does not hold for either rational or elliptic function fields. Over $\mathbb{C}$, more generally in zero characteristic, the classical Hurwitz bound for curves of genus $g \geq 2$ is

$$|\mathrm{Aut}(\mathcal{X})| \leq 84(g-1). \tag{2}$$

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

In positive characteristic, $\mathcal{X}$ with $g \geq 2$ may happen to have larger automorphism group. Nevertheless, from previous work by Roquette [18], Stichtenoth [19, 20], Henn [10], Hansen and Petersen [9], Garcia, Stichtenoth and Xing [4], Çakçak and Özbudak,[2], Giulietti, Korchmáros and Torres [6], Lehr and Matignon [16], curves with very large automorphism groups comparing with their genera are somewhat rare.

The Hermitian curve is the unique curve with $|\mathrm{Aut}(\mathcal{X})| \geq 16g^4$, see [19]. If $p > g$ then (2) holds with only one exception, namely the hyperelliptic curve $\mathbf{v}(Y^p - Y - X^2)$ with $g = \frac{1}{2}(p+1)$ and $|G| = 2p(p^2-1)$, see [18]. Curves with $|\mathrm{Aut}(\mathcal{X})| \geq 8g^3$ were classified in [10]:

Theorem 1.1 (Henn). *Let $\mathcal{X}$ be a projective, geometrically irreducible non-singular curve of genus $g \geq 2$. If a subgroup G of $|\mathrm{Aut}(\mathcal{X})|$ has order at least $8g^3$, then $\mathcal{X}$ is birationally equivalent to one of the following plane curves:*

(I) *The hyperelliptic curve $\mathbf{v}(Y^2 + Y + X^{2^k+1})$ with $p = 2$ and $g = 2^{k-1}$; $|\mathrm{Aut}(\mathcal{X})| = 2^{2k+1}(2^k+1)$ and $\mathrm{Aut}(\mathcal{X})$ fixes a point $P \in \mathcal{X}$.*

(II) *The hyperelliptic curve $\mathbf{v}(Y^2 - (X^q - X))$ with $p > 2$ and $g = \frac{1}{2}(n-1)$; either $G/M \cong \mathrm{PSL}(2,n)$ or $G/M \cong \mathrm{PGL}(2,n)$, where n is a power of p and M is a central subgroup of G of order 2.*

(III) *The Hermitian curve $\mathbf{v}(Y^n + Y - X^{n+1})$ with $p \geq 2$, and $g = \frac{1}{2}(n^2 - n)$; either $G \cong \mathrm{PSU}(3,n)$ or $G \cong \mathrm{PGU}(3,n)$ with n a power of p.*

(IV) *The* DLS *curve (the Delign-Lusztig curve arising from the Suzuki group) $\mathbf{v}(X^{n_0}(X^n + X) - (Y^n + Y))$ with $p = 2$, $n_0 = 2^r, r \geq 1, n = 2n_0^2$, and $g = n_0(n-1)$; $G \cong \mathrm{Sz}(n)$ where $\mathrm{Sz}(n)$ is the Suzuki group.*

Another relevant example in this direction is the following.

(V) *The* DLR *curve (the Delign-Lusztig curve arising from the Ree group) $\mathbf{v}(X^{n_0}(X^n + X) - (Y^n + Y))$ with $p = 3$, $n_0 = 3^r$, $n \geq 0$, $n = 3n_0^2$, and $g = n_0(n-1)$; $G \cong \mathrm{Ree}(n)$ where $\mathrm{Ree}(n)$ is the Ree group.*

An important ingredient in the proof of Theorem 1.1, as well as in other investigations on curves with a large automorphism group G, is Stichtenoth's upper bound on the order of the Sylow p-subgroup in the stabiliser G_P of a point $P \in \mathcal{X}$. In terms of ramification groups, such a Sylow p-subgroup is the first ramification group $G_P^{(1)}$, and the bound depends on the ramification pattern of the Galois covering $\mathcal{X} \to \mathcal{Y}$ where $\mathcal{Y}$ is a non-singular model of the quotient curve $\mathcal{X}/G_P^{(1)}$.

Theorem 1.2 (Stichtenoth)**.** *Let $\mathcal{X}$ be a projective, geometrically irreducible, non-singular curve of genus $g \geq 2$. If $P \in \mathcal{X}$, then*

$$|G_P^{(1)}| \leq \frac{4p}{p-1} g^2.$$

More precisely, if $\mathcal{X}_i$ is the quotient curve $\mathcal{X}/G_P^{(i)}$, then one of the following cases occurs:

(i) *$\mathcal{X}_1$ is not rational, and $|G_P^{(1)}| \leq g$;*

(ii) *$\mathcal{X}_1$ is rational, the covering $\mathcal{X} \to \mathcal{X}_1$ ramifies not only at P but at some other point of $\mathcal{X}$, and*

$$|G_P^{(1)}| \leq \frac{p}{p-1} g; \tag{3}$$

(iii) *$\mathcal{X}_1$ and $\mathcal{X}_2$ are rational, the covering $\mathcal{X} \to \mathcal{X}_1$ ramifies only at P, and*

$$|G_P^{(1)}| \leq \frac{4|G_P^{(2)}|}{(|G_P^{(2)}|-1)^2} g^2 \leq \frac{4p}{(p-1)^2} g^2. \tag{4}$$

Stichtenoth's bound raises the problem of classifying all automorphism groups G with the following property: There is a point $P \in \mathcal{X}$ such that

$$|G_P^{(1)}| > \frac{p}{p-1} g. \tag{5}$$

In this paper, we obtain such a classification by proving the following result.

Theorem 1.3. *If* (1) *holds, then either G fixes P or one of the four cases* (II),. . .,(V) *in Theorem 1.1 occurs.*

2 Background and some preliminary results

Let $\mathcal{X}$ be a projective, non-singular, geometrically irreducible, algebraic curve of genus $g \geq 2$ embedded in the r-dimensional projective space $\mathrm{PG}(r, \mathbb{K})$ over an algebraically closed field $\mathbb{K}$ of positive characteristic $p > 0$. Let Σ be the function field of $\mathcal{X}$ which is an algebraic function field of transcendency degree one over $\mathbb{K}$. The automorphism group $\mathrm{Aut}(\mathcal{X})$ of $\mathcal{X}$ is defined to be the automorphism group of Σ fixing every element of $\mathbb{K}$. It has a faithful permutation representation on the set of all points $\mathcal{X}$ (equivalently on the set of all places of Σ). The orbit

$$o(P) = \{Q \mid Q = P^\alpha,\, \alpha \in G\}$$

is *long* if $|o(P)| = |G|$, otherwise $o(P)$ is *short* and G_P is non-trivial.

If G is a finite subgroup of $\mathrm{Aut}(\mathcal{X})$, the subfield Σ^G consisting of all elements of Σ fixed by every element in G, also has transcendency degree one. Let $\mathcal{Y}$ be a non-singular model of Σ^G, that is, a projective, non-singular, geometrically irreducible, algebraic curve with function field Σ^G. Sometimes, $\mathcal{Y}$ is called the quotient curve of $\mathcal{X}$ by G and denoted by $\mathcal{X}/G$. The covering $\mathcal{X} \mapsto \mathcal{Y}$ has degree $|G|$ and the field extension Σ/Σ^G is of Galois type.

If P is a point of $\mathcal{X}$, the stabiliser G_P of P in G is the subgroup of G consisting of all elements fixing P. For $i = 0, 1, \ldots$, the i-th ramification group $G_P^{(i)}$ of $\mathcal{X}$ at P is

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

where t is a uniformizing element (local parameter) at P. Here $G_P^{(0)} = G_P$ and $G_P^{(1)}$ is the unique Sylow p-subgroup of G_P. Therefore, $G_P^{(1)}$ has a cyclic complement H in G_P, that is, $G_P = G_P^{(1)} \rtimes H$ with a cyclic group H of order prime to p. Furthermore, for $i \geq 1$, $G_P^{(i)}$ is a normal subgroup of G and the factor group $G_P^{(i)}/G_P^{(i+1)}$ is an elementary abelian p-group. For i big enough, $G_P^{(i)}$ is trivial.

For any point Q of $\mathcal{X}$, let $e_Q = |G_Q|$ and

$$d_Q = \sum_{i \geq 0} (|G_Q^{(i)}| - 1).$$

Then $d_Q \geq e_Q - 1$ and equality holds if and only if $\gcd(p, |G_Q|) = 1$.

Let g' be the genus of the quotient curve $\mathcal{X}/G$. The Hurwitz genus formula together with the Hilbert different formula give the following equation

$$2g - 2 = |G|(2g' - 2) + \sum_{Q \in \mathcal{X}} d_Q. \tag{6}$$

If G is tame, that is $p \nmid |G|$, or more generally for G with $p \nmid e_Q$ for every $Q \in \mathcal{X}$, Equation (6) is simpler and may be written as

$$2g - 2 = |G|(2g' - 2) + \sum_{i=1}^{k} (|G| - |\ell_i|) \tag{7}$$

where $\ell_1,\ldots,\ell_k$ are the short orbits of G on $\mathcal{X}$.

Let $G_P = G_P^{(1)} \rtimes H$. The following upper bound on $|H|$ depending on g is due to Stichtenoth [19]:

$$|H| \le 4g+2.$$

For any abelian subgroup G of $\mathrm{Aut}(\mathcal{X})$, Nakajima [17] proved that

$$|G| \le \begin{cases} 4g+4 & \text{for} \quad p\ne 2, \\ 4g+2 & \text{for} \quad p=2. \end{cases}$$

Let $\mathcal{L}$ be the projective line over $\mathbb{K}$. Then $\mathrm{Aut}(\mathcal{L}) \cong \mathrm{PGL}(2,\mathbb{K})$, and $\mathrm{Aut}(\mathcal{L})$ acts on the set of all points of $\mathcal{L}$ as $\mathrm{PGL}(2,\mathbb{K})$ naturally on $\mathrm{PG}(2,\mathbb{K})$. In particular, the identity of $\mathrm{Aut}(\mathcal{L})$ is the only automorphism in $\mathrm{Aut}(\mathcal{L})$ fixing at least three points of $\mathcal{L}$. Every automorphism $\alpha\in\mathrm{Aut}(\mathcal{L})$ fixes a point; more precisely, α fixes either one or two points according as its order is p or relatively prime to p. Also, $G_P^{(1)}$ is an infinite elementary abelian p-group. For a classification of subgroups of $\mathrm{PGL}(2,\mathbb{K})$, see [24].

Let $\mathcal{E}$ be an elliptic curve. Then $\mathrm{Aut}(\mathcal{E})$ is infinite; however for any point $P\in\mathcal{E}$ the stabiliser of P is rather small, namely

$$|\mathrm{Aut}(\mathcal{E})_P| = \begin{cases} 2,4,6 & \text{when } p\ne 2,3, \\ 2,4,6,12 & \text{when } p=3, \\ 2,4,6,8,12,24 & \text{when } p=2. \end{cases}$$

Let $\mathcal{F}$ be a (hyperelliptic) curve of genus 2. For any solvable subgroup G of $\mathrm{Aut}(\mathcal{F})$, Nakajima's bound together with some elementary facts on finite permutation groups, yield $|G|\le 48$.

In the rest of this Section, $\mathcal{X}$ stands for a non–hyperelliptic curve of genus $g\ge 3$, and it is assumed to be the canonical curve of $\mathbb{K}(\mathcal{X})$. So, $\mathcal{X}$ is a non-singular curve of degree $2g-2$ embedded in $\mathrm{PG}(g-1,\mathbb{K})$, and the canonical series of $\mathbb{K}(\mathcal{X})$ is cut out on $\mathcal{X}$ by hyperplanes. Let $1,x_1,\ldots,x_{g-1}$ denote the coordinate functions of this embedding with respect to a homogeneous coordinate frame $(X_0,X_1,\ldots,X_{g-1})$ in $\mathrm{PG}(g-1,\mathbb{K})$.

For a point $P\in\mathcal{X}$, the order sequence of $\mathcal{X}$ at P is the strictly increasing sequence

$$j_0(P)=0<j_1(P)=1<j_2(P)<\ldots<j_{g-1}(P) \tag{8}$$

such that each $j_i(P)$ is the intersection number $I(P,\mathcal{X}\cap H_i)$ of $\mathcal{X}$ and some hyperplane H_i at P, see [21]. For $i=g-1$, such a hyperplane H_{g-1} is uniquely determined being the osculating hyperplane to $\mathcal{X}$ at P. Another characterisation of the integers $j_i(P)$, called P-orders or Hermitian P-invariants, appearing in (8) is that j is a P-order if and only if $j+1$ is a Weierstrass gap, that is, no element in $\mathbb{K}(\mathcal{X})$ regular outside P has a pole of order $j+1$. Now, assume that $j_{g-1}(P) = 2g-2$, that is, P is the unique common point of H_{g-1} with $\mathcal{X}$. Then the hyperplanes of $\mathrm{PG}(g-1,\mathbb{K})$ whose intersection number with $\mathcal{X}$ at P is at least $j_{g-2}(P)$ cut out on $\mathcal{X}$ a linear series g_n^1 of degree $n = 2g-2-j_{g-2}(P)$ and projective dimension 1. Let ℓ be the projective line over $\mathbb{K}$. Then g_n^1 gives rise to a covering $\mathcal{X} \to \ell$ of degree n which completely ramifies at P. If it also ramifies at the points $P_1, \ldots, P_k$ of $\mathcal{X}$ other than P, that is $e_{P_i} > 1$ for $i = 1, \ldots, k$, then (6) yields

$$2g-2 = -2n + d_P + \sum_{i=1}^{k} d_{P_i} \geq -(n+1) + \sum_{i=1}^{k} d_{P_i}. \tag{9}$$

Note that n must be at least 3 as $\mathcal{X}$ is neither rational, nor elliptic and nor hyperelliptic.

From finite group theory, the following results and permutation representations play a role in the proofs.

Huppert's classification theorem, see [14, Chapter XII]: Let G be a solvable 2-transitive permutation group of even degree n. Then n is a power of 2, and G is a subgroup of the affine semi-linear group $\mathrm{A}\Gamma L(1,n)$.

The Kantor-O'Nan-Seitz theorem, see [15]: Let G be a finite 2-transitive permutation group whose 2-point stabiliser is cyclic. Then G has either a regular normal subgroup, or G is one of the following groups in their natural 2-transitive permutation representations:

$$\mathrm{PSL}(2,n),\ \mathrm{PGL}(2,n),\ \mathrm{PSU}(3,n),\ \mathrm{PGU}(3,n), \mathrm{Sz}(n),\ \mathrm{Ree}(n).$$

The natural 2-transitive permutation representations of the above linear groups:

(i) $G = \mathrm{PGL}(2,n)$, is the automorphism group of $\mathrm{PG}(1,n)$; equivalently, G acts on the set Ω of all $\mathbb{F}_n$-rational points of the projective line defined over $\mathbb{F}_n$. The natural 2-transitive representation of $\mathrm{PSL}(2,n)$ is obtained when $\mathrm{PSL}(2,n)$ is viewed as a subgroup of $\mathrm{PGL}(2,n)$,

(ii) $G = \mathrm{PGU}(3,n)$ is the linear collineation group preserving the classical unital in the projective plane $\mathrm{PG}(2,n^2)$, see [12]; equivalently

G is the automorphism group of the Hermitian curve regarded as a plane non-singular curve defined over the finite field $\mathbb{F}_n$ acting on the set Ω of all $\mathbb{F}_{n^2}$-rational points. $\mathrm{PSU}(3,n)$ can be viewed as a subgroup of $\mathrm{PGU}(3,n)$ and this is the natural 2-transitive representation of $\mathrm{PSU}(3,n)$.

(iii) $G = \mathrm{Sz}(n)$ with $n = 2n_0^2$, $n_0 = 2^r$ and $r \geq 1$, is the linear collineation group of $\mathrm{PG}(3,n)$ preserving the Tits ovoid, see [22, 23, 11]; equivalently G is the automorphism group of the DLS curve regarded as a non-singular curve defined over the finite field $\mathbb{F}_n$ acting on the set Ω of all $\mathbb{F}_n$-rational points.

(iv) $G = \mathrm{Ree}(n)$ with $n = 3n_0^2$, $n_0 = 3^r$ and $r \geq 0$, is the linear collineation group of $PG(7,n)$ preserving the Ree ovoid, see [22]; equivalently, G is the automorphism group of the DLS curve regarded as a non-singular curve defined over the finite field $\mathbb{F}_n$ acting on the set Ω of all $\mathbb{F}_n$-rational points.

For each of the above linear groups, the structure of the 1-point stabilizer and its action in the natural 2-transitive permutation representation, as well as its automorphism group, are explicitly given in the papers quoted.

Cyclic fix-point-free subgroups of some 2-transitive groups. The following technical lemma is a corollary of the classification of subgroups of $\mathrm{PSU}(3,n)$ and $\mathrm{Ree}(n)$.

Lemma 2.1. *Let G be a 2-transitive permutation group of degree n. Let U be a cyclic subgroup of G which contains no non-trivial element fixing a point.*

(i) If $G = \mathrm{PSU}(3,n)$ in its natural 2-transitive permutation representation, then $|U|$ divides either $n+1$ or n^2-n+1.

(ii) If $G = \mathrm{Sz}(n)$ in its natural 2-transitive permutation representation, then $|U|$ divides either $n+1$, or $n-2n_0+1$, or $n+2n_0+1$.

(iii) If $G = \mathrm{Ree}(n)$ in its natural 2-transitive permutation representation, then $|U|$ divides either $n+1$, or $n-3n_0+1$, or $n+3n_0+1$.

Schur multiplier of some simple groups. For a finite group G, a group Γ is said to be a covering of G if Γ has a central subgroup U, i.e. $U \subseteq Z(\Gamma)$, such that $G \cong \Gamma/U$. If, in addition, Γ is perfect, that is Γ coincides with its commutator subgroup, then the covering is called proper. For a simple group G, a perfect covering is also called a semisimple group. From Schur's work, see [1] and [13, V.23,24,25], if G is a simple group, then it possesses a "universal" proper covering group $\bar{\Gamma}$ with the property that every proper covering group of G is a homomorphic image of $\bar{\Gamma}$. The center $Z(\bar{\Gamma})$ is called the Schur multiplier of G. The Schur multipliers of simple groups are known, see Griess [7, 8, 5]. In particular, the Schur multiplier of $\mathrm{PSL}(2,q)$ with $q \geq 5$ odd, has order 2; $\mathrm{PSU}(3,q)$ with $q \geq 3$ has non-trivial Schur multiplier only for $3|(q+1)$, and if this occurs the Schur multiplier has order 3; $\mathrm{Ree}(n)$ with $n > 3$ has trivial Schur multiplier. Therefore, the following result holds.

Lemma 2.2. *Let G be a simple group isomorphic to either $\mathrm{PSU}(3,n)$ with $n \geq 3$, or $\mathrm{Ree}(n)$ with $n > 3$. If the center $Z(\Gamma)$ of a group Γ has order 2 and $G \cong \Gamma/Z(\Gamma)$ then Γ has a subgroup isomorphic to G and $\Gamma = Z(G) \times G$.*

3 Large p-subgroups of $\mathrm{Aut}(\mathcal{X})$ fixing a point

In this section, Theorem 1.3 is proven.

We assume that case (iii) of Theorem 1.2 with $G \neq G_P$ occurs. In terms of the action of G_P on $\mathcal{X}$, Theorem 1.2 (iii) implies that

(*) *no non-trivial p-element in G_P fixes a point distinct from P.*

Let Ω be the set of all points $R \in \mathcal{X}$ with non-trivial first ramification group $G_R^{(1)}$. So, Ω consists of all points $R \in \mathcal{X}$ which are fixed by some element of G of order p. Since $P \in \Omega$ and $G \neq G_P$, Ω contains at least two points. It may be noted that the 2-point stabilizer of G is tame and hence cyclic.

Choose a non-trivial element z from the centre of a Sylow p-subgroup S_p of G containing $G_P^{(1)}$. Then z commutes with a non-trivial element of $G_P^{(1)}$. This together with (*) imply that z fixes P. Therefore, $z \in G_P^{(1)}$. In particular, z fixes no point of $\mathcal{X}$ distinct from P. Let $g \in S_p$. Then $zg = gz$ implies that
$$(P^g)^z = P^{gz} = P^{zg} = (P^z)^g = P^g$$
whence $P^g = P$. This shows that every element of S_p must fix P, and hence $S_p = G_P^{(1)}$. Since the Sylow p-subgroups of G are conjugate under G, every p-element fixes exactly one point of $\mathcal{X}$. From Gleason's Lemma, see [3, Theorem 4.14], Ω is a G-orbit, and hence the unique non-tame G-orbit.

By (iii) of Theorem 1.2, the quotient curve $\mathcal{X}_1 = \mathcal{X}/G_P^{(1)}$ is rational. This implies that $\mathcal{Y} = \mathcal{X}/G$ is also rational.

If there are at least two more short G-orbits, say Ω_1 and Ω_2, from (7),

$$\begin{aligned} 2g-2 \;\; &\geq \;\; -2|G| + (|G_P| + |G_P^{(1)}| + |G_P^{(2)}| - 3)\,|\Omega| \\ &\qquad\qquad + (|G_{Q_1}| - 1)\,|\Omega_1| + (|G_{Q_2}| - 1)\,|\Omega_2|, \end{aligned}$$

where $Q_i \in \Omega_i$ for $i = 1, 2$. Note that

$$(|G_{Q_1}| - 1)|\Omega_1| + (|G_{Q_2}| - 1)|\Omega_2| \geq |G|$$

since $|G_{Q_i}| - 1 \geq \frac{1}{2}|G_{Q_i}|$, and $|G| = |G_{Q_i}|\,|\Omega_i|$. Also, $|G| = |G_P|\,|\Omega|$, and $|G_P^{(2)}| > 1$ by (iii) of Theorem 1.2. Therefore,

$$2g - 2 \geq (|G_P^{(1)}| - 1)\,|\Omega|.$$

Since $|\Omega| \geq 2$, this implies that $g \geq |G_P^{(1)}|$, a contradiction.

Therefore, one of the following cases occurs:

(i) Ω is the unique short orbit of G;

(ii) G has two short orbits, namely Ω and a tame G-orbit. Furthermore, either

  (iia) there is a point $R \in \Omega$ such that the stabiliser of R in G_P is trivial;

  (iib) no point $R \in \Omega$ with the property as in (iia) exists.

Before investigating the above three cases separately, a useful equation is established.

Since $\mathcal{X}_1$ is rational, from (*)

$$2g - 2 + 2|G_P^{(1)}| = 2|G_P^{(1)}| - 2 + |G_P^{(2)}| - 1 + \ldots = d_P - |G_P| + |G_P^{(1)}|. \quad (10)$$

Therefore,

$$d_P = 2g - 2 + |G_P^{(1)}| + |G_P|. \quad (11)$$

3.1 Case (i)

We prove that only one example occurs, namely the DLR curve for $n = 3$.

From (*) it follows that $|\Omega| \geq |G_P^{(1)}| + 1$ whence $|\Omega| > g - 1$ by (1). On the other hand, (6) gives

$$2g - 2 = -2|G| + \deg D(\mathcal{X}/G) = |\Omega|(d_P - 2|G_P|). \tag{12}$$

whence $|\Omega|$ is a divisor of $2g-2$. Therefore, $|\Omega| = 2g-2$ and $d_P = 2|G_P|+1$. This and (11) give

$$2g - 2 + |G_P^{(1)}| - |G_P| = 1. \tag{13}$$

Since $G_P = G_P^{(1)} \rtimes H$, it follows that $2g - 2 = (|H| - 1)|G_P^{(1)}| + 1$. This and (1) imply that $|H| = 2$.

Therefore, $p \neq 2$ and $|G_P^{(1)}| = 2g-3$. Since $|\Omega| = 2g-2$ and G_P only fixes P, this implies that $G_P^{(1)}$ acts on $\Omega \setminus \{P\}$ as a transitive permutation group. Hence, $|\Omega| = q + 1$ with $q = |G_P^{(1)}|$. Since Ω is a G-orbit, it follows that G induces on Ω a 2-transitive permutation group $\bar{G}$ whose one-point stabiliser has order either q or $2q$ according as $|G| = 2|\bar{G}|$ or $G = \bar{G}$.

If $|G| = 2|\bar{G}|$, the subgroup H is the kernel of the permutation representation of G on Ω; that is, H fixes every point in Ω. In particular, H is a normal subgroup of G. Therefore, $\bar{G}$ can be viewed as a $\mathbb{K}$–automorphism group of the quotient curve $\mathcal{Z} = \mathcal{X}/G$. Let P' be the point of $\mathcal{Z}$ lying under P. Since $2 \nmid |G_P^{(1)}|$ it follows that $G_P^{(1)} \cong \bar{G}_{P'}^{(1)}$. Also, the points of $\mathcal{Z}$ lying under the points in Ω form the unique short $\bar{G}$-orbit. Therefore, case (i) occurs for $\mathcal{Z}$ and $\bar{G}$. From what was shown before, this implies that $\bar{G}_{P'} = \bar{G}_{P'}^{(1)} \rtimes \bar{H}$ with $|\bar{H}| = 2$ But this is impossible as the stabiliser $\bar{G}_{P'}$ has order q.

If $G = \bar{G}$, two cases are distinguished according as G is solvable or not. In the former case, Huppert's classification theorem implies that $q+1 = d^k$ with d prime. Since $|\Omega| = 2g - 2$ is even, so $d = 2$. From Huppert's classification for $d = 2$ it also follows that G_P is a subgroup of the 1-point stabiliser of $\mathrm{A\Gamma L}(1, q+1)$, and hence $|G_P|$ divides kq. On the other hand, $q+1 = 2^k$ can only occur when k and q are both primes. Since $|G_P| = 2q$, this implies that $k = 2$. Hence $q = g = 3$; that is, $p = 3$ and $|G_P^{(1)}| = g = 3$ which contradicts (1).

Suppose that G is not solvable. If G has a regular normal subgroup M, then G/M is not solvable. On the other hand, $|G_P| = 2q$ and $|M| = |\Omega|$. From $|G| = |G_P||\Omega|$, it follows that $|G/M| = 2q$. But this is not possible for a non-solvable group, as q is a prime power.

If G does not have a regular normal subgroup, then we apply Kantor-O'Nan-Seitz theorem. Since $|G| = 2q$, this shows that either $|\Omega| = 6$ and $G \cong \mathrm{PSL}(2,5)$, or $|\Omega| = 28$ and $G \cong \mathrm{Ree}(3)$. In the former case, $|G_P^{(1)}| = 5$ and $g = 4$; hence (1) does not hold. In the latter case, $|G_P^{(1)}| = 27$ and $g = 15$. This is consistent with (1), and $\mathcal{X}$ is the smallest DLR curve. Therefore (V) holds for $q = n^3$ with $n = 3$.

3.2 Case (iia)

We prove that no example occurs. Let Δ denote the unique tame orbit of G. Choose a point P from Ω and a point Q from Δ. Let

$$N = |G_Q|(d_P - |G_P|) - |G_P|.$$

Then

$$|G| = 2(g-1)\frac{|G_P^{(1)}||H||G_Q|}{N}, \tag{14}$$

where $G_P = G_P^{(1)} \rtimes H$.

By hypothesis, there exists a point $R \in \Omega$ such that the the orbit $o(R)$ of R under G_P is long. Let $o'(R)$ denote the orbit of R under G. Then $|o'(R)| \cdot |G_R| = |G|$. Since P and R lie in the same orbit Ω of G, so $G_R \cong G_P$. Also, $o(R)$ is contained in $o'(R)$. Therefore,

$$|G_P| \le \frac{|G|}{|G_P|} = 2(g-1) \cdot \frac{|G_Q|}{N} \le 2(g-1)|G_Q|. \tag{15}$$

Now, a lower bound on N is given. As

$$N \ge d_P|G_Q| - |G_P||G_Q| - 2(g-1)|G_Q|,$$

so

$$N \ge |G_Q|(d_P - |G_P| - 2(g-1)). \tag{16}$$

This and (11) imply that $N \ge |G_P^{(1)}||G_Q|$. From (15),

$$N \le 2(g-1)|G_Q|/|G_P|.$$

Hence $|G_P||G_P^{(1)}| \le 2(g-1)$. Since $|G_P| > 1$, this contradicts (1).

3.3 Case (iib)

We prove that $\mathcal{X}$ is one of the examples (II),(III),(IV) and (V) with $q > 3$ in (V). Let Δ denote the unique tame orbit of G. Choose a point P from Ω and a point Q from Δ.

First the possible structure of G and its action on Ω are investigated.

Lemma 3.1. *G acts on Ω as a 2-transitive permutation group. In particular, $|\Omega| = q + 1$ with $q = p^t$, and the possibilities for the permutation group $\bar{G}$ induced by G on Ω are as follows:*

(1) $\bar{G} \cong \mathrm{PSL}(2, q)$ *or* $\mathrm{PGL}(2, q)$;

(2) $\bar{G} \cong \mathrm{PSU}(3, n)$ *or* $\mathrm{PGU}(3, n)$, *with* $q = n^3$;

(3) $\bar{G} \cong \mathrm{Sz}(n)$, *with* $p = 2,\ n = 2n_0^2,\ n_0 = 2^k$, *with k odd, and* $q = n^2$;

(4) $\bar{G} \cong \mathrm{Ree}(n)$ *with* $p = 3,\ n = 3n_0^2,\ n_0 = 3^k$, *and* $q = n^3$;

(5) *a minimal normal subgroup of $\bar{G}$ is solvable, and the size of Ω is a prime power.*

Proof. For a point $P \in \Omega$, let $\Omega_0 = \{P\}, \Omega_1, \ldots \Omega_k$ with $k \geq 1$ denote the orbits of $G_P^{(1)}$ contained in Ω. Then, $\Omega = \bigcup_{i=0}^{k} \Omega_i$. To prove that G acts 2-transitively on Ω, it suffices to show that $k = 1$.

For any i with $1 \leq i \leq k$, take a point $R \in \Omega_i$. By hypothesis, R is fixed by an element $\alpha \in G_P$ whose order m is a prime different from p. Since $|G_P| = |G_P^{(1)}||H|$ and m divides $|G_P|$, this implies that m must divide $|H|$. By the Sylow theorem, there is a subgroup H' conjugate to H in G_P which contains α; here, α preserves Ω_i.

Since the quotient curve $\mathcal{X}_1 = \mathcal{X}/G_P^{(1)}$ is rational, α fixes at most two orbits of $G_P^{(1)}$. Therefore, Ω_0 and Ω_i are the orbits preserved by α. As H' is abelian and $\alpha \in H'$, this yields that H' either preserves both Ω_0 and Ω_i or interchanges them. The latter case cannot actually occur as H' preserves Ω_0. So, the orbits Ω_0 and Ω_i are also the only orbits of $G_P^{(1)}$ which are fixed by H'. Since $G_P = G_P^{(1)} \rtimes H'$, this implies that the whole group G_P fixes Ω_i. As i can be any integer between 1 and k, it follows that G_P fixes each of the orbits $\Omega_0, \Omega_1, \ldots, \Omega_k$. Hence, either $k = 1$ or G_P preserves at least three orbits of $G_P^{(1)}$. The latter case cannot actually occur, as the quotient curve $\mathcal{X}_1 = \mathcal{X}/G_P^{(1)}$ is rational.

Therefore $k = 1$. Also, the size of Ω is of the form $q+1$ with $q = |G_P^{(1)}|$; in particular, q is a power of p.

Let $\bar{G}$ denote the 2-transitive permutation group induced by G on Ω. We apply the Kantor-O'Nan-Seitz theorem to $\bar{G}$. Up to isomorphism, $\bar{G}$ is one of the groups on the list, with $\bar{G}$ acting in each of the first four cases in its natural 2-transitive permutation representation. $\square$

We also need the following consequence of Lemma 3.1.

Lemma 3.2. *The subgroups G_P and G_Q have trivial intersection, and G_Q is a cyclic group whose order divides $q+1$. Also,*

$$2g - 2 = \frac{|G|\,(|G_P| - |G_P^{(1)}|\,|G_Q|)}{|G_Q|(|G| - |G_P|)} \tag{17}$$

Proof. Let $\alpha \in G_P \cap G_Q$ be non-trivial. Then $p \nmid \operatorname{ord}\alpha$, and hence $\alpha \in H$. This shows that α fixes not only P but another point in Ω, say R. Since $Q \notin \Omega$, this shows that α has at least three fixed points. These points are in three different orbits of $G_P^{(1)}$. Since the quotient curve $\mathcal{X}_1 = \mathcal{X}/G_P^{(1)}$ is rational, this implies that α fixes every orbit of $G_P^{(1)}$, a contradiction. Hence $|G_P \cap G_Q| = 1$. Therefore, no non-trivial element of G_Q fixes a point in Ω. Since $|\Omega| = q+1$, the second assertion follows. Substituting d_P from (11) into (14) gives (17). $\square$

First the case when the action of G is faithful on Ω is considered.

If $G \cong \mathrm{PGL}(2,q)$, then

$$|G| = q^3 - q,\ |G_P| = q^2 - q,\ |G_P^{(1)}| = q.$$

From Theorem 1.2(iii), the second ramification group $G_P^{(2)}$ is non-trivial. As $G \cong \mathrm{PGL}(2,q)$, G_P has a unique conjugacy class of elements of order p. Since $G_P^{(i)}$ is a normal subgroup of G_P, if $g \in G_P^{(i)}$ with $i \geq 1$ then every conjugate of g in G also belongs to $G_P^{(i)}$. Therefore,

$$G_P^{(1)} = G_P^{(2)} = \ldots = G_P^{(k)},\ |G_P^{(k+1)}| = 1.$$

Since the quotient curve $\mathcal{X}_1 = \mathcal{X}/G_P^{(1)}$ is rational, from (6),

$$2g = (q-1)(k-1).$$

By (1), this is only possible for $k = 2$. Therefore $g = \frac{1}{2}(q-1)$ with $q \geq 5$ odd, and $|G_Q| = \frac{1}{2}(q+1)$.

Let $q \equiv 1 \pmod 4$. Then $2g-2 \equiv 2 \pmod 4$, and an involutory element in $\mathrm{PGL}(2,q) \setminus \mathrm{PSL}(2,q)$ has a no fixed point on Ω. Since G_Q has odd order, such an involutory element in $\mathrm{PGL}(2,q) \setminus \mathrm{PSL}(2,q)$ has no fixed point in Δ, either. Therefore, an involutory element in $\mathrm{PGL}(2,q) \setminus \mathrm{PSL}(2,q)$ fixes no point of $\mathcal{X}$. From (7) applied to such an involutory element $2g-2 \equiv 0 \pmod 4$, a contradiction.

Let $q \equiv 3 \pmod 4$, then $2g-2 \equiv 0 \pmod 4$ and an involutory element in $\mathrm{PGL}(2,q) \setminus \mathrm{PSL}(2,q)$ has exactly two fixed points in Ω. As before, $2 \nmid |G_Q|$ implies that such an involutory element has no fixed point in Δ. Therefore, an involutory element in $\mathrm{PGL}(2,q) \setminus \mathrm{PSL}(2,q)$ fixes exactly two points of $\mathcal{X}$. From (7) applied to such an involutory element $2g-2 \equiv 2 \pmod 4$, a contradiction. Therefore, the case $G \cong \mathrm{PGL}(2,q)$ does not occur.

If $G \cong \mathrm{PSL}(2,q)$ with q odd, then

$$|G| = \tfrac{1}{2}(q^3-q),\ |G_P| = \tfrac{1}{2}(q^2-q),\ |G_P^{(1)}| = q.$$

The previous argument depending on the higher ramification groups at P still works as G_P has two conjugacy classes of elements of order p, and each of them generates $G_P^{(1)}$. Therefore, $k = 2$ and hence $g = \frac{1}{2}(q-1)$. But to show that this case cannot actually occur, more is needed.

The $\mathbb{K}$–automorphism group of a hyperelliptic curve in odd characteristic contains a central involution, say α. Since α commutes with every p-element of G, from (*) it follows that α must fix Ω pointwise. If $P \in \Omega$, then $|G_P|$ is even. But then the automorphism group generated by G_P together with α is not cyclic although it fixes P; a contradiction.

Therefore, $\mathcal{X}$ is not hyperelliptic. So, $\mathcal{X}$ may be assumed to be the canonical curve of $\mathbb{K}(\mathcal{X})$ embedded in $\mathrm{PG}(g-1,\mathbb{K})$. Then G is isomorphic to a linear collineation group Γ of $\mathrm{PG}(g-1,\mathbb{K})$ preserving $\mathcal{X}$ such that the restriction of the action of Γ on $\mathcal{X}$ is G. To simplify notation, the symbol G is used to indicate Γ, too.

Lemma 3.3. *Let $G \cong \mathrm{PSL}(2,q)$ with q odd. Then*

(1) $j_{g-1}(P) = 2g-2$;

(2) Let H_{g-2} be a hyperplane of $\mathrm{PG}(g-1,\mathbb{K})$ such that

$$I(P, \mathcal{X} \cap H_{g-2}) = j_{g-2}(P).$$

If H_{g-2} contains a point $R \in \Omega$ distinct from P, then

$$I(R, \mathcal{X} \cap H_{g-2}) = 2g - 2 - j_{g-2}(P)$$

and hence P and R are the only common points of $\mathcal{X}$ and H_{g-2}.

Proof. To show (1) assume on the contrary that the osculating hyperplane H_{g-1} to $\mathcal{X}$ at P contains a point $S \in \mathcal{X}$ distinct from P. Since $G_P^{(1)}$ preserves H_{g-1}, the $G_P^{(1)}$-orbit of S lies in H_{g-1}. Since such a $G_P^{(1)}$-orbit is long, this implies that H_{g-1} contains from $\mathcal{X}$ at least q points other than P. Hence, $\deg\mathcal{X} \geq j_{g-1}(P) + q$. On the other hand, $j_{g-1}(P) \geq g - 1$. Therefore,

$$\deg\mathcal{X} \geq g - 1 + q > g - 1 + pg/(p-1) > 2g - 2,$$

contradicting $\deg\mathcal{X} = 2g - 2$.

Similar argument may be used to show (2). Again, assume on the contrary that H_{g-2} contains a point $T \in \mathcal{X}$ other than P and R. As H_{g-1} does not contain R, H_{g-2} is the unique hyperplane through R whose intersection number with $\mathcal{X}$ at P is $j_{g-2}(P)$. In particular, the stabiliser H of R in G_P preserves H_{g-2}. Since the H-orbit of T is long, H_{g-2} contains from $\mathcal{X}$ at least $\frac{1}{2}(q-1)$ points other than P and R. On other hand $j_{g-2}(P) \geq g - 2$. Therefore,

$$2g - 2 = \deg\mathcal{X} \geq g - 2 + 1 + \tfrac{1}{2}(q-1),$$

whence $g \geq \frac{1}{2}(q+1)$, a contradiction. $\square$

Since Ω is a $G_P^{(1)}$-orbit, Lemma 3.3(2) shows that for every $R \in \Omega \setminus \{P\}$ there exists a hyperplane $H_{g-2}(R)$ such that

$$I(P, \mathcal{X} \cap H_{g-2}(R)) = j_{g-2}(P), \qquad I(R, \mathcal{X} \cap H_{g-2}(R)) = n = 2g - 2 - j_{g-2}(P).$$

Since such hyperplanes are distinct for distinct points R, from (9) it follows that $2g - 2 \geq -(n+1) + q(n-1)$ with $n \geq 3$. As $g = \frac{1}{2}(q-1)$, this leaves just one possibility, namely $q = 5$, $g = 2$, $n = 3$. But then $\mathcal{X}$ would be hyperelliptic, a contradiction. Therefore the case $G \cong \mathrm{PSL}(2, q)$ does not occur.

If $G \cong \mathrm{PSU}(3, n)$ with $q = n^3$ then

$$|G| = (n^3 + 1)n^3(n^2 - 1)/\mu,\ |G_P| = n^3(n^2 - 1)/\mu,\ |G_P^{(1)}| = n^3,$$

where $\mu = \gcd(3, n+1)$. By (17),

$$2g = \frac{(n^3+1)(n^2-1)}{\mu|G_Q|} - (n^3+1).$$

Since (1) is assumed, Lemma 2.1 (i) together with the first two assertions in Lemma 3.2 ensure the existence of a divisor $t \geq 1$ of $(n^2-n+1)/\mu$ such that $|G_Q| = (n^2-n+1)/(t\mu)$. Hence

$$2g = (n-1)(t(n+1)^2 - (n^2+n+1)). \tag{18}$$

Since t is odd, this and (1) imply that $t = 1$. Then $g = \frac{1}{2}n(n-1)$. Therefore, (III) holds. Since $\mathrm{PSU}(3, n)$ is a subgroup of $\mathrm{PGU}(3, n)$ of index μ, the above argument works for $G \cong \mathrm{PGU}(3, n)$.

If $G \cong \mathrm{Sz}(n)$ with $q = n^2$ and $n = 2n_0^2$ for a power $n_0 \geq 2$ of 2, then

$$|G| = (n^2+1)n^2(n-1),\ |G_P| = n^2(n-1),\ |G_P^{(1)}| = n^2.$$

By (17),

$$2g = \frac{(n+2n_0+1)(n-2n_0+1)(n-1)}{|G_Q|} - (n^2-1).$$

From the preceding argument depending on (1) and Lemmas 2.1 and 3.2, there is an odd integer t such that either (A) or (B) holds, where

$$\begin{array}{llll}
\text{(A)} & 2g = (t-1)(n^2-1) - 2tn_0(n-1), & |G_Q| = (n+2n_0+1)/t; \\
\text{(B)} & 2g = (t-1)(n^2-1) + 2tn_0(n-1), & |G_Q| = (n-2n_0+1)/t.
\end{array}$$

In case (A), t must be at least 3. But then (1) does not hold except for $n_0 = 2$. In the latter case, however, t does not divide $n + n_0 + 1 = 11$. In case (B), (1) implies that $t = 1$. Then $g = n_0(n-1)$. Therefore, (IV) holds.

If $G \cong \mathrm{Ree}(n)$ with $q = n^3$ and $n = 3n_0^2$ for a power $n_0 \geq 0$ of 3, then

$$|G| = (n^3+1)n^3(n-1), \quad |G_P| = n^3(n-1), \quad |G_P^{(1)}| = n^3.$$

By (17),

$$2g = (n-1)\left(\frac{(n+3n_0+1)(n-3n_0+1)(n+1)}{|G_Q|} - (n^2+n+1)\right).$$

Again the previous argument based on (1) and Lemmas 2.1 and 3.2 works showing this time the existence of an integer $t \geq 1$ such that either (A) or (B), or (C) holds, where

$$\begin{array}{ll}\text{(A)} & 2g = (n-1)[(t-1)(n^2+1)-(t+1)n],\ |G_Q| = (n+1)/t;\\ \text{(B)} & 2g = (n-1)[t(n^2-1)-3tnn_0+n(2t-1)-3tn_0+t-1],\\ & \qquad |G_Q| = (n+3n_0+1)/t;\\ \text{(C)} & 2g = n-1)[t(n^2-1)+3tnn_0+n(2t-1)+3tn_0+t-1],\\ & \qquad |G_Q| = (n-3n_0+1)/t.\end{array}$$

In case (A), hypothesis (1) yields that $t = 2$. Then $|G_Q| = \frac{1}{2}(n+1)$, hence $|G_Q|$ is even. But this is impossible as every involution in $\mathrm{Ree}(n)$ has a fixed point.

If case (B) occurs, then $t \geq 2$. Since t is odd and $t \neq 3$, t must be at least 5. But then (1) does not hold.

If case (C) holds with $t = 1$, this (C) reads $2g = 3n_0(n-1)(n+n_0+1)$, and (V) for $n > 3$ follows. Otherwise, $t \geq 5$ contradicting (1).

It remains to investigate the possibility of the permutation representation $\bar{G}$ of G on Ω having non-trivial kernel. Such a kernel M is a cyclic normal subgroup of G whose order is relatively prime to p. By Lemma 3.2 no point outside Ω is fixed by a non-trivial element in M. Let $\tilde{g}$ be the genus of the quotient curve $\mathcal{Y} = \mathcal{X}/M$. From (7) applied to M,

$$2g - 2 = |M|(2\tilde{g} - 2) + (|M| - 1)(q + 1).$$

By (1), this implies that either $|M| = 2$, or $|M| = 3$ and $\tilde{g} = 0$.

Suppose first that $|M| = 2$, $\tilde{g} = 0$. Then, $g = \frac{1}{2}(q-1)$ and $\mathcal{Y}$ is rational. So, $\mathcal{Y}$ may be assumed to be the projective line ℓ over $\mathbb{K}$. Let Ω' be the set of all points of ℓ which lie under the points of Ω. Then $|\Omega'| = |\Omega|$ and $\bar{G}$ acts on Ω' and Ω in the same way. So, $\bar{G}$ may be viewed as a subgroup of $\mathrm{PGL}(1, \mathbb{K})$ acting on a subset Ω' of ℓ. This shows that no non-trivial element of $\bar{G}$ fixes three distinct points.

Assume that $\bar{G}$ has a regular normal subgroup. Arguing as in Case (i), this yields $q + 1 = 2^k$ with both q and k primes. In particular, $q = p$ with $p - 1 > g = \frac{1}{2}(p-1)$. From Roquette's theorem [18], $|G| < 84(g-1) = 42(p-3)$. On the other hand

$$|G| \geq 2(p+1)p,$$

as $\bar{G}$ is doubly transitive on Ω. This together with $p+1=2^k$ leaves only one possibility, namely $p=7$, $k=3$, $g=3$, $|G|=112$ and $\bar{G}$ is sharply 2-transitive on Ω. In particular, $|G_P|=14$, $|G_P^{(1)}|=7$. But then (17) yields that $|G_Q|=1$, a contradiction.

If $\bar{G}$ has no regular normal subgroup, from the classification of Zassenhaus groups either $\bar{G}$ is a sharply 3-transitive group on Ω, or $\bar{G}$ is $\mathrm{PSL}(2,q)$, Therefore, $|G|=2q(q-1)(q+1)$ in the former case, and $|G|=q(q-1)(q+1)$ in the latter case. In both cases, $|G|>8(\frac{1}{2}(q-1)^3)=8g^3$. By Theorem 1.1, (II) holds.

Suppose next that $|M|=2$, $\tilde{g}=1$. Since $G_P^{(1)}$ may be viewed as a subgroup of $\mathrm{Aut}(\mathcal{Y})$ of the elliptic curve $\mathcal{Y}=\mathcal{X}/M$, the order of $G_P^{(1)}$ does not exceed 24. Thus, q is one of the integers $2,3,4,8$. This leaves just one case, namely $q=p=g=3$, but then (1) fails.

Suppose now that $|M|=2$, $\tilde{g}\geq 2$. Then (1) holds for $\mathcal{Y}=\mathcal{X}/M$ with $\bar{G}$ acting faithfully on $\bar{\Omega}$. From what proven before, either $\bar{G}$ contains a subgroup $\bar{G}'\cong \mathrm{PGU}(3,n)$ of index $\gcd(3,n+1)$, or $\bar{G}\cong \mathrm{Ree}(n)$ with $n>3$.

In the former case, let G' be the subgroup of G for which $G'/M=\bar{G}'$. Since $|M|=2$ and hence $M\subset Z(G)$, Lemma 2.2 implies that $G'=M\times U$ with $U\cong \mathrm{PSU}(3,n)$. Also, U acts on Ω as $\mathrm{PSU}(3,n)$ in its natural 2-transitive permutation representation. Since the one-point stabiliser U_P of U with $P\in\Omega$ contains a cyclic subgroup V of even order, it turns out that the the subgroup of G generated V and M is a not cyclic, although it fixes P; a contradiction.

In the latter case, the same argument works for $G=G'=\mathrm{Ree}(n)$.

Finally, suppose that $|M|=3$, $\tilde{g}=0$. Then $g=q-1$. This together with (1) imply that $p>g+1=q$, a contradiction.

References

[1] M. Aschbacher, Finite group theory, Corrected reprint of the 1986 original. Cambridge Studies in Advanced Mathematics, 10. Cambridge University Press, Cambridge, 1993. x+274 pp.

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

[3] P. Dembowski, *Finite geometries*. Reprint of the 1968 original. Classics in Mathematics. Springer-Verlag, Berlin, 1997. xii+375 pp.

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

[5] D. Gorenstein, Finite simple groups, The Uinversity Series in Mathematics, Plenum Press, New York, 1982 x+333 pp.

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

[7] R. Griess, Schur multipliers of the known finite simple groups. *Bull. Amer. Math. Soc.* **78** 1972 68–71.

[8] R. Griess, Schur multipliers of the known finite simple groups. II. *The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979),* pp. 279–282, Proc. Sympos. Pure Math., **37**, Amer. Math. Soc., Providence, R.I., 1980.

[9] 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.

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

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

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

[13] B. Huppert, *Endliche Gruppen. I*, Grundlehren der Mathematischen Wissenschaften **134**, Springer, Berlin, 1967, xii+793 pp.

[14] B. Huppert and B.N. Blackburn, *Finite groups. III*, Grundlehren der Mathematischen Wissenschaften **243**, Springer, Berlin, 1982, ix+454 pp.

[15] W.M. Kantor, M. O'Nan and G.M. Seitz, 2-transitive groups in which the stabilizer of two points is cyclic, *J. Algebra* **21** (1972), 17–50.

[16] C. Lehr and M. Matignon, Automorphism groups for p-cyclic covers of the affine line, *Compositio Math.* **141** (2005), 1213–1237.

[17] S. Nakajima, On abelian automorphism groups of algebraic curves, *J. London Math. Soc.* **36** (1987), 23–32.

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

[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] J. Tits, Les groupes simples de Suzuki et de Ree, *Séminaire Bourbaki* **6**, Soc. Math. France, Paris, 1995, 65–82.

[23] J. Tits, Ovoides et groupes de Suzuki, *Arch. Math.* **13** (1962), 187–198.

[24] R.C. Valentini and M.L. Madan, A Hauptsatz of L.E. Dickson and Artin–Schreier extensions, *J. Reine Angew. Math.* **318** (1980), 156–177.