On algebraic curves with many automorphisms in characteristic $p$

Maria Montanucci$^1$

Received: 13 December 2021 / Accepted: 21 March 2022 / Published online: 19 May 2022
© The Author(s), under exclusive licence to Springer-Verlag GmbH Germany, part of Springer Nature 2022

Abstract
Let $\mathcal{X}$ be an irreducible, non-singular, algebraic curve defined over a field of odd characteristic $p$. Let $g$ and $\gamma$ be the genus and $p$-rank of $\mathcal{X}$, respectively. The influence of $g$ and $\gamma$ on the automorphism group $\text{Aut}(\mathcal{X})$ of $\mathcal{X}$ is well-known in the literature. If $g \geq 2$ then $\text{Aut}(\mathcal{X})$ is a finite group, and unless $\mathcal{X}$ is the so-called Hermitian curve, its order is upper bounded by a polynomial in $g$ of degree four (Stichtenoth). In 1978 Henn proposed a refinement of Stichtenoth’s bound of degree 3 in $g$ up to few exceptions, all having $p$-rank zero. In this paper a further refinement of Henn’s result is proposed. First, we prove that if an algebraic curve of genus $g \geq 2$ has more than $336g^2$ automorphisms then its automorphism group has exactly two short orbits, one tame and one non-tame, that is, the action of the group is completely known. Finally when $|\text{Aut}(\mathcal{X})| \geq 900g^2$ sufficient conditions for $\mathcal{X}$ to have $p$-rank zero are provided.

Keywords Algebraic curve · Automorphism group · $p$-rank · Genus

Mathematics Subject Classification 11G20 · 20B25

1 Introduction

Let $\mathcal{X}$ be a projective, geometrically irreducible, non-singular algebraic curve defined over an algebraically closed field $\mathbb{K}$ of positive characteristic $p$. Let $\mathbb{K}(\mathcal{X})$ be the field of rational functions on $\mathcal{X}$ (i.e. the function field of $\mathcal{X}$ over $\mathbb{K}$). The $\mathbb{K}$-automorphism group $\text{Aut}(\mathcal{X})$ of $\mathcal{X}$ is defined as the automorphism group of $\mathbb{K}(\mathcal{X})$ fixing $\mathbb{K}$ element-wise. The group $\text{Aut}(\mathcal{X})$ has a faithful action on the set of points of $\mathcal{X}$.

By a classical result, $\text{Aut}(\mathcal{X})$ is finite whenever the genus $g$ of $\mathcal{X}$ is at least two; see [16] and [7, Chapter 11; 22–24,31,33]. Furthermore it is known that every finite group occurs in
this way, since, for any ground field \( \mathbb{K} \) and any finite group \( G \), there exists an algebraic curve \( X \) defined over \( \mathbb{K} \) such that \( Aut(X) \cong G \); see [12, 13, 22].

This result raised a general problem for groups and curves, namely, that of determining the finite groups that can be realized as the \( \mathbb{K} \)-automorphism group of some curve with a given invariant. The most important such invariant is the *genus* \( g \) of the curve. In positive characteristic, another important invariant is the so-called *p-rank* of the curve, which is the integer \( 0 \leq \gamma \leq g \) such that the Jacobian of \( X \) has \( p^\gamma \) points of order \( p \).

Several results on the interaction between the automorphism group, the genus and the \( p \)-rank of a curve can be found in the literature. A remarkable example is the work of Nakajima [14] who showed that the value of the \( p \)-rank deeply influences the order of a \( p \)-group of automorphisms of \( X \). He also showed that curves for which the \( p \)-rank is the largest possible, namely \( \gamma = g \), have at most \( 84(g^2 - g) \) automorphisms.

In [8] Hurwitz showed that if \( X \) is defined over \( \mathbb{C} \) then \( |Aut(X)| \leq 84(g - 1) \), which is known as the *Hurwitz bound*. This bound is sharp, i.e., there exist algebraic curves over \( \mathbb{C} \) of arbitrarily high genus whose automorphism group has order exactly \( 84(g - 1) \). Well-known examples are the Klein quartic and the Fricke-Macbeath curve, see [11]. Roquette [15] showed that Hurwitz bound also holds in positive characteristic \( p \), if \( p \) does not divide \( |Aut(X)| \).

A general bound in positive characteristic is \( |Aut(X)| \leq 16g^4 \) with one exception: the so-called Hermitian curve. This result is due to Stichtenoth [20, 21].

The quartic bound \( |Aut(X)| \leq 16g^4 \) was improved by Henn in [6]. Henn’s result shows that if \( |Aut(X)| > 8g^3 \) then \( X \) is \( \mathbb{K} \)-isomorphic to one of the following four curves:

\[ \begin{align*}
&\text{the non-singular model of the plane curve } Y^2 + Y = X^{2k+1}, \text{ with } k > 1 \text{ and } p = 2; \\
&\text{the non-singular model of } Y^2 = X^n - X, \text{ where } n = p^h, h > 0 \text{ and } p > 2; \\
&\text{the Hermitian curve } \mathcal{H}_q : Y^{q+1} = X^q + X \text{ where } q = p^h \text{ and } h > 0; \\
&\text{the non-singular model of the Suzuki curve } S_q : X^{q_0}(X^q + X) = Y^q + Y, \text{ where } q_0 = 2^r, \\
&\phantom{S_q : } r \geq 1 \text{ and } q = 2q_0^2.
\end{align*} \]

All the above exceptions have \( p \)-rank zero. This observation raised the following problem.

**Open problem 1.1** *Is it possible to find a (optimal) function \( f(g) \) such that the existence of an automorphism group \( G \) of \( X \) with \( |G| \geq f(g) \) implies \( \gamma = 0 \)?*

Clearly from Henn’s result \( f(g) \leq 8g^3 \). Also \( f(g) \) cannot be asymptotically of order less than \( g^{3/2} \) as algebraic curves of positive \( p \)-rank with approximately \( g^{3/2} \) automorphisms are known; see for example [10].

Open Problem 1.1 was already studied in [3] where a positive answer is given under the additional hypothesis that \( g \) is even or that the automorphism group \( G \) is solvable.

**Theorem 1.2** [3, Theorem 1.1 and Theorem 1.2] Let \( \mathbb{K} \) be an algebraically closed field of odd characteristic \( p \) and let \( X \) be an algebraic curve defined over \( \mathbb{K} \). If \( X \) has even genus \( g \geq 2 \) and at least \( 900g^2 \) automorphisms then its \( p \)-rank \( \gamma \) is equal to zero. If \( X \) is of arbitrary genus \( g \geq 2 \) and it has a soluble automorphism group of order at least \( 84pg^2/(p - 2) \) then the \( p \)-rank of \( X \) is zero.

In this paper we analyze large automorphism groups of curves of arbitrary genus \( g \geq 2 \) giving a partial answer to Open Problem 1.1. The following theorem summarizes our main results.

**Theorem 1.3** *Let \( G \) be an automorphism group of an algebraic curve \( X \) defined over a field of odd characteristic \( p \). Denote with \( g \geq 2 \) and \( \gamma \) the genus and the \( p \)-rank of \( X \) respectively.*
On algebraic curves with many automorphisms in characteristic \( p \)

1. If \( |G| > 24g^2 \) then either \( G \) has a unique (non-tame) short orbit or it has exactly two short orbits, one tame and one non-tame.
2. If \( G \) has exactly one non-tame short orbit then \( |G| \leq 336g^2 \).
3. If \( |G| \geq 60g^2 \) and \( G \) has exactly one non-tame short orbit then \( \gamma \) is positive and congruent to zero modulo \( p \).
4. If \( |G| \geq 900g^2 \) then \( G \) has exactly one non-tame short orbit \( O_1 \) and one tame short orbit \( O_2 \). If \( \mathcal{X}/G_{p_1}^{(1)} \) is rational for \( P \in O_1 \) and the stabilizer \( G_{p,R} \) with \( R \in O_1 \setminus \{ P \} \) is either a \( p \)-group or a prime-to-\( p \) group then \( \gamma \) is zero.

Note that this theorem implies that whenever a quadratic bound like \( |Aut(\mathcal{X})| > 336g^2 \) holds, then the action of the group is completely known, having one tame and one non-tame short orbits.

The paper is organized as follows. In Sect. 2 some preliminary results on automorphism groups of algebraic curves in positive characteristic are recalled. In Sect. 3 Parts 1–3 of Theorem 1.3 are proven, while Part 4 is the main object of Sect. 4.

## 2 Preliminary results

In this paper, \( \mathcal{X} \) stands for a (projective, geometrically irreducible, non-singular) algebraic curve of genus \( g = g(\mathcal{X}) \geq 2 \) defined over an algebraically closed field \( \mathbb{K} \) of odd characteristic \( p \). Let \( Aut(\mathcal{X}) \) be the group of all automorphisms of \( \mathcal{X} \). The assumption \( g(\mathcal{X}) \geq 2 \) ensures that \( Aut(\mathcal{X}) \) is finite. However the classical Hurwitz bound \( |Aut(\mathcal{X})| \leq 84(g(\mathcal{X}) - 1) \) for complex curves fails in positive characteristic, and there exist four families of curves satisfying \( |Aut(\mathcal{X})| \geq 8g(\mathcal{X})^3 \); see [21], Henn [6], and also [7, Section 11.12].

For a subgroup \( G \) of \( Aut(\mathcal{X}) \), let \( \tilde{\mathcal{X}} \) denote a non-singular model of \( \mathbb{K}(\mathcal{X})^G \), that is, a (projective non-singular 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, \( \tilde{\mathcal{X}} \) 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 \( |G| \).

Let \( \Phi \) be the cover of \( \Phi : \mathcal{X} \to \tilde{\mathcal{X}} \) where \( \tilde{\mathcal{X}} = \mathcal{X}/G \). 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 \( \tilde{Q} \in \tilde{\mathcal{X}} \) is a branch point of \( G \) if there is a ramification point \( P \in \mathcal{X} \) such that \( \Phi(P) = \tilde{Q} \); 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 \( o = \{ R \mid R = g(P), \ g \in G \} \) of \( \mathcal{X} \), and it is long if \( |o| = |G| \), otherwise \( o \) is short. For a point \( \tilde{Q} \), the \( G \)-orbit \( o \) lying over \( \tilde{Q} \) consists of all points \( P \in \mathcal{X} \) such that \( \Phi(P) = \tilde{Q} \). If \( P \in o \) then \( |o| = |G|/|G_P| \) and hence \( \tilde{Q} \) 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 non-trivial element in \( G \) is fixed–point-free on \( \mathcal{X} \), that is, the cover \( \Phi \) 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

\[
G_{p}^{(i)} = \{ \alpha \in G_P \mid \text{ord}_P(\alpha(t) - t) \geq i + 1 \},
\]

where \( t \) is a uniformizing element (local parameter) at \( P \). Here \( G_{p}^{(0)} = G_P \).
Let \( \tilde{g} \) be the genus of the quotient curve \( \tilde{X} = X/G \). The Hurwitz genus formula [19, Theorem 3.4.13] gives the following equation

\[
2g - 2 = |G|(2\tilde{g} - 2) + \sum_{P \in \tilde{X}} d_P,
\]

where the different \( d_P \) at \( P \) is given by

\[
d_P = \sum_{i \geq 0} (|G|^{(i)} - 1),
\]

see [7, Theorem 11.70].

Let \( \gamma \) be the \( p \)-rank of \( X \), and let \( \tilde{\gamma} \) be the \( p \)-rank of the quotient curve \( \tilde{X} = X/G \). A formula relating \( \gamma \) and \( \tilde{\gamma} \) is known whenever \( G \) is a \( p \)-group. Indeed if \( G \) is a \( p \)-group, the Deuring-Shafarevich formula states that

\[
\gamma - 1 = |G|(\tilde{\gamma} - 1) + \sum_{i=0}^{k} (|G| - \ell_i),
\]

where \( \ell_1, \ldots, \ell_k \) are the sizes of the short orbits of \( G \); see [23] or [7, Theorem 11.62].

A subgroup of \( \text{Aut}(X) \) is a prime-to-\( p \) group (or a \( p' \)-subgroup) if its order is prime to \( p \). A subgroup \( G \) of \( \text{Aut}(X) \) is tame if the 1-point stabilizer of any point in \( G \) is \( p' \)-group. Otherwise, \( G \) is non-tame (or wild). By [7, Theorem 11.56], if \( |G| > 84(g(X) - 1) \) then \( G \) is non-tame.

An orbit \( o \) of \( G \) is tame if \( G_P \) is a \( p' \)-group for \( P \in o \). The following lemma gives a strong restriction to the action of the Sylow \( p' \)-subgroup of the stabilizer of a point \( P \in X \) when \( \gamma = \gamma(X) = 0 \).

**Result 2.1** [7, Lemma 11.129] If \( \gamma(X) = 0 \) then every element of order \( p \) in \( \text{Aut}(X) \) has exactly one fixed point on \( X \).

Bounds for the order of tame automorphism groups fixing a point are known; see [7, Theorem 11.60].

**Result 2.2** Let \( X \) be an irreducible curve of genus \( g > 0 \), and let \( G_P \) be a \( \mathbb{K} \)-automorphism group of \( X \) fixing a point \( P \). If the order \( n \) of \( G_P \) is prime to \( p \), then \( n \leq 4g + 2 \).

Strong restrictions for the short orbits structure of automorphism groups of algebraic curves are known when the Hurwitz bound \( 84(g(X) - 1) \) fails. In particular, the following theorem ensures that automorphism groups for which the Hurwitz bound is not satisfied have at most three short orbits.

**Theorem 2.3** [7, Theorem 11.56] Let \( X \) be an irreducible curve of genus \( g \geq 2 \) defined over a field \( \mathbb{K} \) of characteristic \( p \).

- If \( G \) is a \( \mathbb{K} \)-automorphism group of \( X \), then the Hurwitz’s upper bound \( |G| \leq 84(g-1) \) holds in general with exceptions occurring only if \( p > 0 \).
- If \( p > 0 \) then exceptions can only occur when the fixed field \( \mathbb{K}(X)^G \) is rational and \( G \) has at most three short orbits as follows:
  1. exactly three short orbits, two tame and one non-tame, with \( p \geq 3 \);
  2. exactly two short orbits, both non-tame;
  3. only one short orbit which is non-tame;
4. exactly two short orbits, one tame and one non-tame.

**Theorem 2.4** [7, Theorem 11.116 and Theorem 11.125] Let $\mathcal{X}$ be an algebraic curve of genus $g \geq 2$ defined over an algebraically closed field $K$ of positive characteristic $p$. If $G$ is an automorphism group of $\mathcal{X}$ with $|G| > 84(g - 1)$, then an upper bound for the order of $G$ in Cases 1,2 of Theorem 2.3 is given by:

1. $|G| < 24g^2$,
2. $|G| < 16g^2$,

respectively. If $G$ satisfies Case 3 of Theorem 2.3 then $|G| < 8g^3$. If $G$ satisfies Case 4 in Theorem 2.3 then $|G| < 8g^3$ unless one of the following cases occurs up to isomorphism over $K$:

- $p = 2$ and $\mathcal{X}$ is the non-singular model of the plane curve $Y^2 + Y = X^{2k+1}$, with $k > 1$;
- $p > 2$ and $\mathcal{X}$ is the non-singular model of $Y^2 = X^n - X$, where $n = ph$ and $h > 0$;
- $\mathcal{X}$ is the Hermitian curve $\mathcal{H}_q : Y^{q+1} = X^q + X$ where $q = ph$ and $h > 0$;
- $\mathcal{X}$ is the non-singular model of the Suzuki curve $\mathcal{S}_q : X^{q_0} (X^q + X) = Y^q + Y$, where $q_0 = 2^r, r \geq 1$ and $q = 2q_0^2$.

Furthermore, all the above algebraic curves have $p$-rank zero.

Theorem 2.4 shows in particular that a quadratic bound on $|G|$ in Case 4 of Theorem 2.3 is not possible. However nothing is known in Case 3 of Theorem 2.3. One of the first aims of this paper is to show that actually a quadratic bound with respect to the genus can be found also in this case.

**Remark 2.5** Examples of algebraic curves of genus $g$ with approximately $g^2$ automorphisms satisfying Case 4 in Theorem 2.3 are known. Given a prime power $q$, the GK curve $C$ is given by the affine model,

$$C : \begin{cases} y^{q+1} = x^q + x, \\ z^{q^2-q^2+1} = y^{q^2} - y, \end{cases}$$

see [4]. The curve $C$ has genus $g(C) = (q^3 - 2q^3 + q^2)/2$ and it is $F_{q^6}$-maximal. The automorphism group of $C$ is defined over $F_{q^6}$ and has order $q^3(q^3+1)(q^2-1)(q^2-q+1) \sim 4g(C)^2$. The set $C(F_{q^6})$ of the $F_{q^6}$-rational points of $C$ splits into two orbits under the action of $Aut(C)$: $O_1 = C(F_{q^2})$ and $O_2 = C(F_{q^6}) \setminus C(F_{q^2})$. The orbit $O_1$ is non-tame while $O_2$ is tame. Case 4 is indeed satisfied, see [4, Theorem 7].

Other two examples are the cyclic extensions of the Suzuki and Ree curves constructed in [18]. Again the order of the automorphism group of these curves is approximately $4g^2$ and it satisfies Case 4 in Theorem 2.3; see [5]. All the examples written in this remark have $p$-rank zero.

In order to give our partial answer to Open Problem 1.1 the following lemmas from [3] will be used.

**Lemma 2.6** [3, Lemma 4.1 and Remark 4.3] Let $\mathcal{X}$ be an algebraic curve of genus $g \geq 2$ defined over an algebraically closed field $K$ of odd characteristic $p$. Let $H$ be an automorphism group of $\mathcal{X}$ with a normal Sylow $d$-subgroup $Q$ of odd order. Suppose that a complement $U$ of $Q$ in $H$ is cyclic and that $N_H(U) \cap Q = \{1\}$. If

$$|H| \geq 30(g - 1),$$

then $d = p$ and $U$ is cyclic. Moreover, the quotient curve $\tilde{\mathcal{X}} = \mathcal{X}/Q$ is rational and either
1. \( \mathcal{X} \) has positive \( p \)-rank, \( Q \) has exactly two (non-tame) short orbits, and they are also the only short orbits of \( H \); or

2. \( \mathcal{X} \) has zero \( p \)-rank and \( H \) fixes a points.

If \( d = p \) is assumed then the hypothesis \( N_H(U) \cap Q = \{1\} \) is unnecessary.

**Lemma 2.7** [3, Lemma 4.8] Let \( G \) be an automorphism group of an algebraic curve \( \mathcal{X} \) of genus \( g \geq 2 \) defined over a field of odd characteristic \( p \). Suppose that

1. \( |G| \geq 16g^2 \);
2. any two distinct Sylow \( p \)-subgroups of \( G \) have trivial intersection;
3. \( G \) has a Sylow \( d \)-subgroup \( Q \) for which its normalizer \( N_G(Q) \) contains a subgroup \( H \) satisfying the hypotheses of Lemma 2.6;

then \( \mathcal{X} \) has zero \( p \)-rank.

The following result provides a list of known and useful properties of automorphism groups of algebraic curves in positive characteristic.

**Result 2.8** Let \( \mathcal{X} \) be an algebraic curve of genus \( g \geq 2 \) defined over a field of characteristic \( p \geq 3 \). Let \( G \) be an automorphism group of \( \mathcal{X} \).

1. \[14, Theorem 1\] If \( G \) is a \( p \)-group and \( \gamma(\mathcal{X}) > 0 \) then \( |G| \leq p(g - 1)/(p - 2) \). If \( \gamma(\mathcal{X}) = 0 \) then \( |G| \leq \max\{g, 4pg^2/(p - 1)^2\} \).
2. \[7, Theorem 11.60 and Theorem 11.79\] If \( G \) is abelian then \( |G| \leq 4g+4 \).
3. \[7, Theorem 11.78\] If \( P \in \mathcal{X} \) is such that the quotient curve \( \mathcal{X}/G_P^{(1)} \) is not rational then \( |G_P^{(1)}| \leq g \).
4. \[7, Lemma 11.44 (e)\] For \( P \in \mathcal{X} \), the stabilizer \( G_P \) of \( P \) in \( G \) is a semidirect product \( G_P = G_P^{(1)} \rtimes U \) where \( U \) is a cyclic \( p' \)-group and \( G_P^{(1)} \) is the Sylow \( p \)-subgroup of \( G_P \). In particular \( G_P \) is solvable.
5. \[7, Theorem 11.14\] If \( \mathcal{X} \) is rational and \( G \) is cyclic and tame then \( G \) has exactly two fixed points and no other short orbits on \( \mathcal{X} \).

An essential ingredient from group theory that we will use in the proof of Theorem 1.3 is the complete list of finite 2-transitive permutation groups, see [2, Tables 7.3 and 7.4].

A well known theorem of Burnside [2, Theorem 4.3] states that every finite 2-transitive group is either almost simple or affine. Finite affine 2-transitive groups are those having an elementary abelian regular normal socle, while almost simple 2-transitive groups are those having a simple socle \( N \).

Tables 1 and 2 list finite 2-transitive groups according to the two aforementioned categories. Recall that the degree of a 2-transitive permutation group is the cardinality of the set on which the group acts 2-transitively.

The list of finite 2-transitive permutation groups can be refined if the stabilizer of two points is cyclic.

**Theorem 2.9** [9, Theorem 1.1] Let \( G \) be a finite, 2-transitive permutation group on a set \( \mathcal{X} \). Suppose that the stabilizer \( G_P, Q \) of two distinct points \( P, Q \in \mathcal{X} \) is cyclic, and that \( G \) has no regular normal subgroups. Then \( G \) is one of the following groups in its usual 2-transitive permutation representation: \( PSL(2, q), PGL(2, q), Sz(q), PSU(3, q), PGU(3, q) \) or a group of Ree type.

**Theorem 2.10** [1, Theorem 1.7.6] Let \( G \) be a 2-transitive group on a set \( O \). If \( G \) has a regular normal subgroup \( N \), then \( N \) is an elementary abelian \( d \)-group where \( d \) is a prime and \( |O| = d^n \) for some \( n \geq 1 \).
Table 1  Affine 2-transitive groups

| Case | Degree | \( G_P \) | Condition |
|------|--------|------------|-----------|
| 1.  | \( q^d \) | \( SL(d, q) \leq G_P \leq \Gamma L(d, q) \) |           |
| 2.  | \( q^{2d} \) | \( Sp(d, q) \leq G_P \) | \( d \geq 2 \) |
| 3.  | \( q^6 \) | \( G_2(q) \leq G_P \) | \( q \) even |
| 4.  | \( q \) | \( (2^{1+2} \times 3) = SL(2, 3) \leq G_P \) | \( q = 5^2, 7^2, 11^2, 23^2 \) |
| 5.  | \( q \) | \( 2^{1+4} \leq G_P \) | \( q = 3^4 \) |
| 6.  | \( q \) | \( SL(2, 5) \leq G_P \) | \( q = 11^2, 19^2, 29^2, 59^2 \) |
| 7.  | \( 2^4 \) | \( A_6 \) |           |
| 8.  | \( 2^4 \) | \( A_7 \) |           |
| 9.  | \( 2^6 \) | \( PSU(3, 3) \) |           |
| 10. | \( 3^6 \) | \( SL(2, 12) \) |           |

Table 2  Almost Simple 2-transitive groups

| Case | Degree | Condition | \( N \) | \( \max|G/N| \) |
|------|--------|-----------|--------|---------------|
| 1.   | \( n \) | \( n \geq 5 \) | \( A_n \) | 2             |
| 2.   | \( (q^d - 1)/(q - 1) \) | \( d \geq 2, (d, q) \neq (2, 2), (2, 3) \) | \( PSL(d, q) \) | \( (d, q - 1) \) |
| 3.   | \( 2^{2d-1} + 2^{d-1} \) | \( d \geq 3 \) | \( Sp(2d, 2) \) | 1             |
| 4.   | \( 2^{2d-1} - 2^{d-1} \) | \( d \geq 3 \) | \( Sp(2d, 2) \) | 1             |
| 5.   | \( q^3 + 1 \) | \( q \geq 3 \) | \( PSU(3, q) \) | \( (3, q + 1) \) |
| 6.   | \( q^2 + 1 \) | \( q = 2^{2d+1} > 2 \) | \( Sz(q) \) | \( 2d + 1 \) |
| 7.   | \( q^3 + 1 \) | \( q = 3^{2d+1} > 3 \) | \( Ree(q) \) | \( 2d + 1 \) |
| 8.   | 11     |           | \( PSL(2, 11) \) | 1             |
| 9.   | 11     |           | \( M_{11} \) | 1             |
| 10.  | 12     |           | \( M_{11} \) | 1             |
| 11.  | 12     |           | \( M_{12} \) | 1             |
| 12.  | 15     |           | \( A_7 \) | 1             |
| 13.  | 22     |           | \( M_{22} \) | 2             |
| 14.  | 23     |           | \( M_{23} \) | 1             |
| 15.  | 24     |           | \( M_{24} \) | 1             |
| 16.  | 28     |           | \( PSL(2, 8) \) | 3             |
| 17.  | 176    |           | \( HS \) | 1             |
| 18.  | 276    |           | \( C_{o3} \) | 1             |

With all the ingredients introduced in Sect. 2 we can proceed with the proof of Theorem 1.3. Doing so, we can assume that \( G \) is an automorphism group of an algebraic curve \( \mathcal{X} \) of genus \( g = g(\mathcal{X}) \geq 2 \), \( p \)-rank \( \gamma = \gamma(\mathcal{X}) \), and such that \( |G| > 84(g - 1) \). By Theorems 2.3 and 2.4 unless \( |G| \leq 24g^2 \), \( G \) has either exactly one short orbit (Case 3 in Theorem 2.3) or exactly two short orbits, one tame and one non-tame (Case 4 in Theorem 2.4). We analyze these two cases separately in Sects. 3 and 4 respectively.
3 \hspace{1em} \text{\textit{G} satisfies Case 3 of Theorem 2.3}

In this section \( G \) stands for an automorphism group of an algebraic curve \( \mathcal{X} \) of genus \( g \geq 2 \) defined over a field \( \mathbb{K} \) of odd characteristic \( p \) satisfying Case 3 of Theorem 2.3. We denote by \( O \) the only short orbit of \( G \) on \( \mathcal{X} \).

We start with the following direct consequence of the Hurwitz genus formula.

**Lemma 3.1** If an automorphism group \( G \) of an algebraic curve \( \mathcal{X} \) of genus \( g \geq 2 \) has exactly one short orbit \( O \) then the size of \( O \) divides \( 2g - 2 \). In particular this holds true whenever \( G \) satisfies Case 3 in Theorem 2.3.

**Proof** Let \( \bar{g} \) be the genus of the quotient curve \( \mathcal{X}/G \). If the stabilizer \( G_P \) of a point \( P \in O \) is tame, then the Hurwitz genus formula (1) reads as follows

\[
2g - 2 = |G|(2\bar{g} - 2) + |G| - |O|.
\]

As from the Orbit stabilizer Theorem \( |G| = |G_P||O| \), the result follows.

In the non-tame case, in Equation (1) we have \( d_P = d_Q \) for \( P, Q \in O \) and \( d_R = 0 \) for \( R \neq O \). Hence \( |O| \) divides \( \sum_{P \in \mathcal{X}} d_P \), and the result follows as in the tame case from Equation (1).

We now move to the proof of Part 2 in Theorem 1.3.

**Theorem 3.2** If \( |G| \geq 60g^2 \) then \( \gamma \) is congruent to zero modulo \( p \).

**Proof** Let \( P \in O \) and let \( G_P \) be the stabilizer of \( P \) in \( G \). From Item 4 of Result 2.8, we can write \( G_P = G^{(1)}_P \times U \) where \( U \) is tame and cyclic. Denote by \( \mathcal{Y}_1 \) the quotient curve \( \mathcal{X}/G^{(1)}_P \).

We distinguish two cases.

- **Case 1:** \( O = \{P\} \). If \( \mathcal{Y}_1 \) is not rational then Item 3 of Result 2.8 and Result 2.2 imply that \( |G| = |G_P| \leq g(4g + 2) < 60g^2 \), a contradiction. Hence \( g(\mathcal{Y}_1) = 0 \). The factor group \( U_1 = G_P/G^{(1)}_P \cong U \) is a prime-to-\( p \) cyclic automorphism group of \( \mathcal{Y}_1 \) fixing the point \( P_1 \) lying below \( P \) in the cover \( \mathcal{X}/\mathcal{Y}_1 \). If \( |U| = 1 \) then a contradiction to \( |G| < 60g^2 \) is obtained from Result 2.8 part 1. Hence we can assume \( U_1 \) non-trivial. From Item 5 of Result 2.8 the group \( U_1 \) has another fixed point, say \( Q_1 \), on \( \mathcal{Y}_1 \). If \( Q \) denotes a point of \( \mathcal{X} \) lying above \( Q_1 \) in \( \mathcal{X}/\mathcal{Y}_1 \) then \( U \) acts on the \( G^{(1)}_P \)-orbit \( \Delta \) containing \( Q \) and since \( |U| \) is prime-to-\( p \) we get that \( U \) has at least another fixed point on \( \mathcal{X} \), say \( R \), which is also contained in \( \Delta \). This implies that the \( G \)-orbit containing \( R \) is short as the stabilizer of \( R \) in \( G \) is non-trivial. This is not possible since by hypothesis \( O = \{P\} \) is the only short orbit of \( G \).

- **Case 2:** \( O \supset \{P\} \). From the Orbit stabilizer Theorem \( |G| = |O||G_P| \). Also from Lemma 3.1 we can write \( 2g - 2 = k|O| \) for some \( k \geq 1 \). Then

\[
(2g - 2)^2 = k^2|O|^2 = k^2 \frac{|G|^2}{|G_P|^2},
\]

and hence since \( |G| \geq 60g^2 \),

\[
|G_P| = k^2 \frac{|G|^2}{(2g - 2)^2} = \frac{k^2|G|}{(2g - 2)^2} \cdot \frac{|G|}{|G_P|} > \frac{|G|}{|G_P|}.
\]

From \( |O| \leq 2g - 2 \) we have

\[
2g|G_P| > (2g - 2)|G_P| \geq |O||G_P| = |G| \geq 60g^2
\]

\( \square \) Springer
and hence $|G_P| \geq 30g > 30(g - 1)$. From Lemma 2.6 either $\gamma(\mathcal{X}) = 0$ or $\gamma(\mathcal{X}) > 0$ and in the latter case $G_P^{(1)}$ has exactly two (non-tame) short orbits which are also the only short orbits of $G_P$. Assume that $\gamma(\mathcal{X}) > 0$ and denote by $O_1 = \{P\}$ and $O_2$ the two short orbits of $G_P^{(1)}$ and $G_P$, with $|O_2| = p^i$ and $i \geq 0$.

If $i = 0$ we have that $G_P^{(1)}$ and $G_P$ fix exactly another point $R \in \mathcal{X} \setminus \{P\}$ and have no other short orbits. Since $O_1$ and $O_2$ are contained in $O$, we can write $|O| = 2 + h|G_P|$ for some $h \geq 0$. If $h = 0$ then $|O| = 2$ and hence from Item 1 of Result 2.8 and Result 2.2, $|G| = |G_P||O| = 2|G_P| \leq 2p(g - 1)(4g + 2)/(p - 2) \leq 30g^2$, a contradiction. If $h \geq 1$ then $|G_P| < |O| \leq 2g - 2$. Since $|G_P| \geq 30g$ we get a contradiction. This shows that necessarily $i \geq 1$. From the Deuring-Shafarevic formula (3) applied to $G_P^{(1)}$ one has

$$\gamma - 1 = |G_P^{(1)}|(0 - 1) + |G_P^{(1)}| - 1 + |G_P^{(1)}| - p^i,$$

and hence $\gamma$ is congruent to zero modulo $p$.

We now prove that actually the case $\gamma = 0$ in Theorem 3.2 cannot occur.

**Theorem 3.3** Let $\mathcal{X}$ be an irreducible curve of genus $g \geq 2$. If $G$ is an automorphism group of $\mathcal{X}$ satisfying Case 3 of Theorem 2.3 then either $|G| < 60g^2$ or $\gamma = \gamma(\mathcal{X})$ is positive and congruent to zero modulo $p$.

**Proof** Suppose that $G$ satisfies Case 3 in Theorem 2.3 and $|G| \geq 60g^2$. For $P \in O$ we can write $G_P = G_P^{(1)} \rtimes U$, where $U$ is tame and cyclic from Item 4 of Result 2.8. Then from Theorem 3.2 we have either $\gamma(\mathcal{X}) = 0$ or $\gamma(\mathcal{X})$ positive and congruent to zero modulo $p$.

Suppose by contradiction that $\gamma(\mathcal{X}) = 0$. Recall that $\mathcal{X}/G^{(1)}_P$ is rational from Lemma 2.6 as $|G_P| \geq 30g$.

Write $|G^{(1)}_P| = p^h$ with $h \geq 1$. By the Hurwitz genus formula applied with respect to $G^{(1)}_P$ one has,

$$2g - 2 = -2|G^{(1)}_P| + d_P = -2|G^{(1)}_P| + 2(|G^{(1)}_P| - 1) + \sum_{i \geq 2}(|G^{(i)}_P| - 1) = \sum_{i \geq 2}(|G^{(i)}_P| - 1) - 2,$$

since $G^{(1)}_P$ has exactly $\{P\}$ as its unique short orbit from Result 2.1. On the other hand, recalling that $\mathcal{X}/G$ is rational, the Hurwitz genus formula applied with respect to $G$ gives

$$2g - 2 = -2|G| + |O|(|G_P| - 1 + |G^{(1)}_P| - 1 + \sum_{i \geq 2}(|G^{(i)}_P| - 1))$$

and hence

$$2g - 2 = -|G| + |O||G^{(1)}_P| + 2g - 2).$$

Therefore,

$$|O||(|G_P| - |G^{(1)}_P|) = |O||G^{(1)}_P|(|U| - 1) = (|O| - 1)(2g - 2) < (2g - 2)|O|.$$ (4)

If $|U| = 1$ then $G_P = G_P^{(1)}$ and $|O||G^{(1)}_P|(|U| - 1) = (|O| - 1)(2g - 2)$ implies that $|O| = 1$ since $g \geq 2$. Hence $|G| = |G^{(1)}_P| \leq 4g^2$ from Item 1 of Result 2.8; a contradiction.
Since $|U| \geq 2$ we get from Equation (4), 

$$\frac{|G_P|}{2} \leq |G_P^{(1)}|(|U| - 1) < 2g - 2$$

and $|G| = |O||G_P| < (2g - 2)^2 < 4g^2$; a contradiction. □

This proves Item 2 in Theorem 1.3. Our next goal is to show that up to increasing the value of the constant $c = 60$ one can give a complete answer to Open Problem 1.1 when $G$ satisfies Case 3 in Theorem 2.3. This will prove Item 3 in Theorem 1.3 and show that curves with at least $336g^2$ automorphism have a very precise short orbits structure.

**Proposition 3.4** Let $\mathcal{X}$ be an irreducible curve of genus $g \geq 2$. If $G$ is an automorphism group of $\mathcal{X}$ satisfying Case 3 of Theorem 2.3. Then $|G| \leq 336g^2$.

**Proof** Assume by contradiction that there exists an algebraic curve $\mathcal{X}$ together with an automorphism group $G$ satisfying Case 3 in Theorem 2.3 with $|G| > 336g^2$. We choose $\mathcal{X}$ to be of minimal genus, that is, if $g' < g$ then an algebraic curve together with an automorphism group $G'$ satisfying Case 3 in Theorem 2.3 with $|G'| > 336g^2$ does not exist.

The first part of the proof is similar to the one of Theorem 3.2. Let $P \in O$, where $O$ denotes the only short orbit of $G$. Let $G_P^{(1)}$ be the Sylow $p$-subgroup of the stabilizer $G_P$ of $P$ in $G$ and denote by $\gamma_1$ the quotient curve $\mathcal{X}/G_P^{(1)}$. From Item 4 of Result 2.8, we can write $G_P = G_P^{(1)} \times U$ where $U$ is tame and cyclic. We distinguish two subcases.

- **Case 1:** $O = \{P\}$. If $\gamma_1$ is not rational then Item 3 of Result 2.8 and Result 2.2 imply that $|G| = |G_P| \leq g(4g + 2) < 336g^2$, a contradiction. Hence $g(\gamma_1) = 0$. The factor group $U_1 = G_P/G_P^{(1)} \cong U$ is a prime-to-$p$ cyclic automorphism group of $\gamma_1$ fixing the point $P_1$ lying below $P$ in the cover $\mathcal{X}/\gamma_1$. As before we can assume $|U| > 1$. From Item 5 of Result 2.8, the group $U_1$ has another fixed point, say $Q_1$, on $\gamma_1$. If $Q$ denotes a point of $\mathcal{X}$ lying above $Q_1$ in $\mathcal{X}/\gamma_1$ then $U$ acts on the $G_P^{(1)}$-orbit $\Delta$ containing $Q$ and since $|U|$ is prime-to-$p$ we get that $U$ has at least another fixed point, say $R$, on $\mathcal{X}$ which is contained in $\Delta$. This implies that the $G$-orbit containing $R$ is short as the stabilizer of $R$ in $G$ is non-trivial. This is not possible since by hypothesis $O = \{P\}$ is the only short orbit of $G$.

- **Case 2:** $O \supseteq \{P\}$. From the Orbit stabilizer Theorem $|G| = |O||G_P|$ and $|O|$ divides $2g - 2$ from Lemma 3.1. Write $2g - 2 = k|O|$ for some $k \geq 1$. Then

$$2g - 2 = k|O| = k^2 \frac{|G|^2}{|G_P|^2},$$

and hence since $|G| > 336g^2$,

$$|G_P| = k^2 \frac{|G|^2}{|G_P|(2g - 2)^2} = \frac{k^2|G|}{(2g - 2)^2} \cdot \frac{|G|}{|G_P|} = \frac{|G|}{|G_P|}.$$ 

From $|O| \leq 2g - 2$ we have

$$2g|G_P| > |G_P|(2g - 2) \geq |O||G_P| = |G| > 336g^2$$

and hence $|G_P| > 30(g - 1)$. From Lemma 2.6 either $\gamma(\mathcal{X}) = 0$ or $\gamma(\mathcal{X}) > 0$ and in the latter case $G_P^{(1)}$ has exactly two (non-tame) short orbits, and they are also the only short orbits of $G_P$. The claim follows by showing that the case $\gamma(\mathcal{X}) > 0$ cannot occur since Theorem 3.3 gives that the case $\gamma(\mathcal{X}) = 0$ cannot occur either.

Springer
Assume by contradiction that \( \gamma(\mathcal{X}) > 0 \) and denote by \( O_1 = \{ P \} \) and \( O_2 \), with \( |O_2| = p^i, i \geq 0 \) the two short orbits of \( G_p^{(1)} \) and \( G_p \). We have the following two possibilities.

- **Subcase 2.I**: \( O \neq O_1 \cup O_2 \). Let \( R \in O \setminus (O_1 \cup O_2) \). Then the orbit \( \Delta \) of \( G_p \) containing \( R \) is long and \( \Delta \subset O \). Hence \( |G_p| = |\Delta| < |O| \leq (2g - 2) \). This implies that \( |G| = |G_p||O| < (2g - 2)^2 < 4g^2 \), a contradiction.

- **Subcase 2.II**: \( O = O_1 \cup O_2 \). Denote by \( K \) the kernel of the permutation representation of \( G \) on \( O \). Since \( O = \{ P \} \cup O_2 \), \( G \) acts 2-transitively on \( O \). Then \( G/K \) is isomorphic to one of the finite 2-transitive permutation groups listed in Tables 1 and 2. The claim will follow with a case-by-case analysis.

- Suppose that \( \tilde{G} = G/K \) is one of the finite affine 2-transitive groups in Table 1. The first three cases cannot occur since \( \tilde{G} \) is solvable. This follows from the fact that \( G_p \) is solvable from Item 4 of Result 2.8 and hence every factor group of \( G_p \) is solvable as well. Cases 4, 5, 6 and 10 can be excluded as \( |O| \) must be even. In the remaining cases either \( |O| = 2^4 \) or \( |O| = 2^6 \). Since \( |O| - 1 \) must be a prime power both the cases can be excluded.

- Suppose that \( \tilde{G} = G/K \) is one of the finite almost simple 2-transitive groups in Table 2.

  Cases 8, 9, 12 and 14 can be excluded as \( |O| \) must be even, while Cases 13, 17 and 18 cannot occur since \( |O| - 1 \) is a prime power.

  Cases 10, 11, 15 and 16 can be excluded as follows. Note that \((|O|, p) = (12, 11), (24, 23), (28, 3)\). If \((|O|, p) = (12, 11)\) then \( |G_p^{(1)}| < (1, 1 \cdot (g - 1)) \) from Item 1 of Result 2.8, so that from Item 2 of Result 2.8, \( |G_p| < (1, 1 \cdot (g - 1)(4g + 4) < 5g^2 \). From the Orbit stabilizer Theorem \( |G| = 12|G_p| < 60g^2 \), a contradiction.

  If \((|O|, p) = (24, 23)\) then \( |G_p^{(1)}| < (1, 1 \cdot (g - 1)) \) from Item 1 of Result 2.8, so that from Item 2 of Result 2.8, \( |G_p| < (1, 1 \cdot (g - 1)(4g + 4) < 5g^2 \). From the Orbit stabilizer Theorem \( |G| = 24|G_p| < 120g^2 \), a contradiction.

  If \((|O|, p) = (28, 3)\) then \( |G_p^{(1)}| \leq 3(g - 1) \) from Item 1 of Result 2.8, so that from Item 2 of Result 2.8, \( |G_p| \leq (g - 1)(4g + 4) < 12g^2 \). From the Orbit stabilizer Theorem \( |G| = 28|G_p| < 336g^2 \), a contradiction.

  Since the stabilizer of a point in \( A_n \) with \( n \geq 5 \) is not solvable we get that Case 1 in Table 2 cannot occur from Item 4 of Result 2.8.

  Suppose that \( G \) satisfies one of the remaining cases in Table 2, that is, Cases 2-7. Let \( \mathcal{Y} \) be the quotient curve \( \mathcal{X}/K \). We claim that either \( K \) is trivial or \( \mathcal{X}/K \) is rational.

  Let \( K \) be trivial. Since \( |G| \geq 900g^2 \), \( |G_p| > 30(g - 1) \) and Sylow \( p \)-subgroups in \( G \) intersect trivially, we can apply Lemma 2.7 to get a contradiction.

  Hence \( K \) is not trivial. Suppose first that \( g(\mathcal{X}/K) \geq 2 \). The Hurwitz genus formula implies that \( 2g - 2 \geq |K|(2g(\mathcal{X}/K) - 2) \) so that

\[
\frac{|G|}{|K|} \geq \frac{|G|(2g(\mathcal{X}/K) - 2)}{2g - 2} > \frac{336g^2(g(\mathcal{X}/K) - 1)}{g-1} \geq 336g(\mathcal{X}/K)^2.
\]

We claim that the orbit \( \bar{O} \) of \( G/K \) lying below \( O \) in \( \mathcal{X}|\mathcal{X}/K \) is the only short orbit of \( G/K \) on \( \mathcal{X}/K \). Suppose by contradiction that \( G/K \) has another short orbit \( \bar{O}_n \). Then \( G \) acts on set of points lying above \( \bar{O}_n \), say \( O_n \). Since \( K \) has no other short orbits other than \( O \), we have that \( |O_n| = |K||\bar{O}_n| < |K||G_p||/|K| = |G| \) so that also \( O_n \) is a short orbit of \( G \); a contradiction. This shows that if \( g(\mathcal{X}/K) \geq 2 \) then \( \mathcal{X}/K \) has an automorphism group \( G/K \) or order at least \( 336g(\mathcal{X}/K)^2 \) with
exactly one short orbit on $\mathcal{X}/K$. Since $g(\mathcal{X}/K) < g$ this is not possible for the minimality of $g$.

Thus, $g(\mathcal{X}/K) \leq 1$. If $g(\mathcal{X}/K) = 1$ then, denoting with $\tilde{G}_p$ the stabilizer of the point $\tilde{P}$ with $P|\tilde{P}$ in $\mathcal{X}|\mathcal{X}/K$, $|\tilde{G}_p| \leq 12$ from [7, Theorem 11.94].

We observe that in Cases 2-7 in Table 2, $|\tilde{G}_p| \geq |O|$ so that also $|O| \leq 12$. We get $|G_p^{(1)}| \leq 3(g - 1)$ from Item 1 of Result 2.8, and from Item 2 of Result 2.8, $|G_p| \leq 3g - 1(4g + 4) \leq 12g^2$. From the Orbit stabilizer Theorem $|G| \leq 12|G_p| \leq 144g^2$, a contradiction. This shows that $\mathcal{X}/K$ is rational. Since Cases 3-7 cannot give rise to automorphism groups of the rational function field from [7, Theorem 11.14], only Case 2 can occur and so $\tilde{G} = G/K \cong PSL(2, q)$, $PGL(2, q)$.

We note that $(q^d - 1)/(q - 1) - 1 = (q^d - q)/(q - 1)$ cannot be a prime power unless $d = 2$ and $q \geq 5$.

Suppose first that $(|K|, p) = 1$. Then Sylow $p$-subgroups of $G$ correspond to Sylow $p$-subgroups of either $PSL(2, q)$ or $PGL(2, q)$ and hence in any case they intersect trivially. Since $|G| > 16g^2$ then claim follows from Lemma 2.7.

Hence $K$ contains $p$-elements. Let $Q_K$ be a Sylow $p$-subgroup of $K$. Then $Q_K$ is a normal subgroup of $G$ implying that $G$ has normal $p$-subgroups. Denote by $S$ the largest normal $p$-subgroup of $G$ and consider the quotient curve $\mathcal{X}/S$. From our choice of the subgroup $S$, the quotient group $G_S = G/S$ has no normal $p$-subgroups. We claim that $\mathcal{X}/S$ is rational.

Suppose first that $g(\mathcal{X}/S) \geq 2$. As before, the Hurwitz genus formula implies that $2g - 2 \geq |S|(2g(\mathcal{X}/S) - 2)$ so that

$$\frac{|G|}{|S|} \geq \frac{|G|(2g(\mathcal{X}/S) - 2)}{2g - 2} \geq \frac{336g^2(g(\mathcal{X}/S) - 1)}{g - 1} \geq 336g(\mathcal{X}/S)^2.$$  

We claim that the orbit $\tilde{O}$ of $G/S$ lying below $O$ in $\mathcal{X}|\mathcal{X}/S$ is the only short orbit of $G/S$ on $\mathcal{X}/S$. Suppose by contradiction that $G/S$ has another short orbit $\tilde{O}_n$. Then $G$ acts on set of points lying above $\tilde{O}_n$, say $O_n$. Since $K$ has no other short orbits other than $O$, we have that $|O_n| = |S||\tilde{O}_n| < |S||G|||S| = |G|$ so that also $O_n$ is a short orbit of $G$; a contradiction. This shows that if $g(\mathcal{X}/S) \geq 2$ then $\mathcal{X}/S$ has an automorphism group $G/S$ of order at least $336g(\mathcal{X}/S)^2$ with exactly one short orbit on $\mathcal{X}/S$. Since $g(\mathcal{X}/S) < g$ this is not possible for the minimality of $g$.

If $g(\mathcal{X}/S) = 1$ then the group $G_P S/S$ is a subgroup of $Aut(\mathcal{X}/S)$ fixing at least one point on $\mathcal{X}/S$ (the one lying below $P$ in $\mathcal{X}|\mathcal{X}/S$). Hence $|U| \leq |G_P||S_P|/|S| = |G_P S||S| = |G_P||G_P \cap S| \leq 12$ from [7, Theorem 11.94].

Recalling that $|O| = (2g - 2)$ and that $|G_p^{(1)}| \leq p(g - 1)/(p - 2)$ from Item 1 of Result 2.8, we get $|G| \leq 12(2g - 2)p(g - 1)/(p - 2) < 336g^2$; a contradiction. Hence $\mathcal{X}/S$ is rational and $G/S$ is a subgroup of $PGL(2, \mathbb{K})$ with no normal $p$-subgroups. From the classification of finite subgroups $PGL(2, \mathbb{K})$, see [24], $G/S$ is a prime to-p-subgroup which is either cyclic, or dihedral, or isomorphic to one of the the groups $A_4$, $S_4$. If $G/S \cong A_4$, $S_4$ then $|G| \leq 24|S||O| \leq 24(2g - 2)p(g - 1)/(p - 2) < 336g^2$ and hence we can discard these cases. Since $\gamma \equiv 0 \pmod{p}$, $S$ has exactly one fixed point (and possibly other non-trivial short orbits) on $\mathcal{X}$ from Equation (3). Using the fact that $S$ is normal in $G$ we get that the entire $G$ has a fixed point on $\mathcal{X}$ which is not possible as $|O| = q + 1$. □
Now Items 1–3 in Theorem 1.3 are proven. The next section will be devoted to the proof of Item 4 of Theorem 1.3.

4 $G$ satisfies Case 4 of Theorem 2.3

In order to prove the main theorem we assume that $\chi$ is an algebraic curve defined over an algebraically closed field of odd characteristic $p$ and genus $g$. Let $G$ be an automorphism group of $\chi$. We assume that $|G| \geq 900g^2$ and that $G$ satisfies Case 4 of Theorem 2.3, so that $G$ has two short orbits, one tame $O_2$ and one non-tame $O_1$. Furthermore, choosing a point $P$ in $O_1$, from Item 4 of Result 2.8, we write $G_P = G^{(1)}_P \rtimes U$ with $|U|$ prime-to-$p$ and cyclic. Let $\mathcal{Y}_1$ be the quotient curve $\chi/G^{(1)}_P$. To complete the proof of the main theorem we can also assume that $g(\mathcal{Y}_1) = 0$ and that $G_{P,R}$ is a $p$-group if it has a non-trivial Sylow $p$-subgroup. The following three cases are treated separately.

(iv.1) There is a point $R$ distinct from $P$ such that the stabilizer of $R$ in $G_P$ has order $p^t$ with $t \geq 1$.

(iv.2) No non-trivial element of $G^{(1)}_P$ fixes a place distinct from $P$, and there is a place $R$ distinct from $P$ but lying in the orbit of $P$ in $G$ such that the stabilizer of $R$ in $G_P$ is trivial.

(iv.3) No non-trivial element of $G^{(1)}_P$ fixes a place distinct from $P$, and, for every place $R$ distinct from $P$ but lying in the orbit of $P$ in $G$, the stabilizer of $R$ in $G_P$ is non-trivial.

4.1 $G$ satisfies Case (iv.1)

In this case, if $R$ is an arbitrary point on $\chi$ distinct from $P$ then the stabilizer of $R$ in $G_P$ is either trivial or a $p$-group of order $p^t$, $t \geq 1$. Since $\mathcal{Y}_1$ is rational, $\tilde{U} = G_P/G^{(1)}_P \cong U$ is cyclic it fixes two points on $\mathcal{Y}_1$ from Item 5 of Result 2.8, say $\tilde{P}$ (lying below $P$) and $\tilde{R}$. Denote by $O_{\tilde{R}}$ the orbit of $G^{(1)}_P$ lying above $\tilde{R}$. Then $|O_{\tilde{R}}| = p^t$ for some $t$ and $U$ acts on $O_{\tilde{R}}$. Since $(|U|, p) = 1$, $U$ has at least one fixed point on $O_{\tilde{R}}$, a contradiction. This shows that $|U| = 1$. Assume by contradiction that $g > 0$. From the Hurwitz genus formula applied to $G$ we have

$$2g - 2 = -2|G| + |O_1|d_P + |O_2|(|G_Q| - 1) = -|G| + \frac{|G|}{|G_P|}d_P - \frac{|G|}{|G_Q|},$$

so that

$$|G| = \frac{(2g - 2)|G^{(1)}_P||G_Q|}{-|G^{(1)}_P||G_Q| + d_P|G_Q| - |G^{(1)}_P|}.$$

If $|G_Q| \leq 3$ then from Item 1 of Result 2.8,

$$|G| \leq 6(g - 1)|G^{(1)}_P| \leq \frac{6p(g - 1)^2}{p - 2} \leq 18g^2,$$

a contradiction. So $|G_Q| > 3$. Since $d_P \geq 2|G^{(1)}_P| - 2$ and $|G^{(1)}_P| \geq 3$ we get

$$-|G^{(1)}_P||G_Q| + d_P|G_Q| - |G^{(1)}_P| \geq -|G^{(1)}_P||G_Q| + (2|G^{(1)}_P| - 2)|G_Q| - |G^{(1)}_P|$$

$$= |G^{(1)}_P||G_Q| - 2|G_Q| - |G^{(1)}_P| \geq |G_Q| - 3.$$
Thus, using again Item 1 of Result 2.8,

\[
|G| \leq \frac{(2g - 2)|G_P^{(1)}||G_Q|}{|G_Q| - 3} < 8g|G_P^{(1)}| \leq \frac{8pg(g - 1)}{p - 2} \leq 24g^2,
\]
a contradiction.

### 4.2 $G$ satisfies Case (iv.2)

In this case the orbit $\mathcal{o}(R)$ of $G_P$ containing $R$ is long. Let $o'(R)$ be the orbit of $R$ under $G$. Then from the Orbit Stabilizer Theorem $|o'(R)| \cdot |G_R| = |G|$. Moreover, as $R$ lies in the orbit of $P$ in $G$, also $o(R) \subseteq o'(R)$. Let $Q$ be a place contained in the unique tame short orbit of $G$. From Equation (1) applied to $G_P$,

\[
2(g - 1) = -2|G| + \frac{|G|}{|G_Q|}(|G_Q| - 1) + \frac{|G|}{|G_P|} d_P,
\]

where $d_P$ denotes the ramification at $P$ and $d_Q = e_Q - 1 = |G_Q| - 1$. Hence

\[
|G| = \frac{2(g - 1)}{|G_Q|}\frac{|G_P|}{|G_Q|(|d_P - |G_P||) - |G_P|}.
\] (5)

Combining Equation (5) and $|o(R)| = |G_P| \leq |o'(R)|$ yields $|G| = |G_P| |o'(R)| \geq |G_P|^2$, whence

\[
|G_P| \leq \frac{|G|}{|G_P|} = \frac{2(g - 1)}{|G_Q|(|d_P - |G_P||) - |G_P|} \leq 2(g - 1)|G_Q|.
\]

Thus,

\[
|G_Q|(|d_P - |G_P||) - |G_P| \geq d_P|G_Q| - |G_P||G_Q| - 2(g - 1)|G_Q|,
\]

and

\[
|G_Q|(|d_P - |G_P||) - |G_P| \geq |G_Q|(|d_P - |G_P|| - 2(g - 1)|G_Q|). \quad (6)
\]

From Equation (1) applied to $G_P$,

\[
2(g - 1) = -2|G_P| + (d_P + |G_P^{(1)}|(|U| - 1)) = d_P - |G_P| - |G_P^{(1)}|,
\]

and hence

\[
d_P - |G_P| - 2(g - 1) = |G_P^{(1)}|.
\]

From Equation (6) and Result 2.2,

\[
|G| \leq 2(g - 1)\frac{|G_P^{(1)}||U||G_Q|}{|G_P^{(1)}||G_Q|} \leq 2(g - 1)(4g + 2) < 8g^2.
\]

Since $|G| > 900g^2$, this case cannot occur.
4.3 $G$ satisfies Case (iv.4)

Let as before $P \in O_1$. If $O_1 = \{P\}$ then $G = G_P$. In particular $G$ is solvable and the claim follows from Theorem 1.2. Hence we can assume that $O \supseteq \{P\}$. We start with an intermediate lemma. We assume that $\mathcal{X}$ is a minimal counterexample with respect to the genus, that is, if $Y$ is an algebraic curve of genus $\tilde{g} < g$ together with an automorphism group $\tilde{G}$ satisfying Case 4 in Theorem 2.3 then $|	ilde{G}| < 900\tilde{g}^2$.

**Lemma 4.1** If $O_1 \subset \{P\}$ then $O_1$ has size $q + 1$ where $q = p^n$, $n \geq 1$ and $G$ acts 2-transitively on $O_1$. If $K$ denotes the Kernel of the permutation representation of $G$ over $O_1$, one of the following cases occurs.

- $G/K \cong PGL(2, q)$, $PSL(2, q)$,
- $G/K \cong PGU(3, q)$, $PSU(3, q)$,
- $G/K \cong Ree(q)$, when $p = 3$, $q = 3^{2r+1}$,
- $G/K$ has a regular normal soluble subgroup and the size of $O_1$ is a prime power.

Unless the last case occur, if $|G_P| \geq 30(g - 1)$ then $\mathcal{X}$ has zero $p$-rank.

**Proof** Let $o_0 = \{P\}, o_1, \ldots, o_k$ denote the orbits of $G_1^{(1)}$ contained in $O_1$, so that $O_1 = \bigcup_{i=0}^{k} o_i$. To prove that $G$ acts 2-transitively on $O_1$ we show that $k = 1$.

For any $i = 1, \ldots, k$ take $R_i \in o_i$. Since we are dealing with Case (iv.4), $R_i$ is fixed by an element $\alpha_i \in G_P$ of prime order $m \neq p$ dividing $|U|$. By Sylow’s Theorem there exist a subgroup $U_i$ conjugated to $U$ in $G_P$ containing $\alpha_i$ and $\alpha_i$ clearly preserves $o_i$. As previously noted, since $Y_1 = \mathcal{X}/G_1^{(1)}$ is rational, $\alpha_i$ fixes at most two $G_1^{(1)}$-orbits and hence $o_0$ and $o_i$ are the only fixed orbits of $\alpha_i$. Since $U^i$ is abelian and it fixes $o_0$, the orbits $o_0$ and $o_i$ are also the only $G_1^{(1)}$-orbits fixed by $U^i$. Since we can write $G_P = G_1^{(1)} \times U^i$ we get that the whole $G_P$ fixes $o_i$ for all $1 \leq i \leq k$. Thus, either $k = 1$ or $G_P$ fixes at least 3 $G_1^{(1)}$-orbits. The latter case cannot occur from Item 5 of Result 2.8 applied to $Y_1$ as automorphisms of a curve of genus zero have at most 2 fixed points.

This shows that $k = 1$ so that $G$ acts 2-transitively on $O_1$. Also $|O_1| = q + 1$ with $q = |G_1^{(1)}| = p^n$, $n \geq 1$ as we are dealing with Case (iv.4). Let $K$ denote the kernel of the action of $G$ on $O_1$ and let $\tilde{G} = G/K$ be the corresponding permutation group. Since the stabilizer of 2 points in $G$ (and hence $\tilde{G}$) is cyclic and $p$ is odd we get from Theorem 2.9 that $\tilde{G}$ is isomorphic to one of the groups listed. In the last case $O_1$ is a prime power and the regular normal subgroup an elementary abelian group from Theorem 2.10.

From $(|K|, p) = 1$, we have that Sylow $p$-subgroups of $G$ corresponds to Sylow $p$-subgroups of $\tilde{G}$. Since in all the cases but the last one Sylow $p$-subgroups of $\tilde{G}$ intersect trivially the same holds for $G$. If $|G_P| \geq 30(g - 1)$ the claim follows from Lemma 2.7. □

Assume the one of the first 3 cases listed in Lemma 4.1 occurs with $|G_P| < 30(g - 1)$. First of all we note that $K$ is not trivial. Suppose indeed by contradiction that $K$ is trivial so that $G \cong \tilde{G}$.

- $G \cong PSL(2, q)$, $PGL(2, q)$. Here $|G_P| = q(q - 1)/2$ or $|G_P| = q(q - 1)$ and in any case $|G_P|^2 > |G| = (q + 1)|G_P| \geq 900g^2$. Hence $|G_P| > 30(g - 1)$, a contradiction.
- $G \cong PSU(3, q)$, $PGU(2, q)$. In this case $|G_P| = q^3(q^2 - 1)/3$ or $|G_P| = q^3(q^2 - 1)$ and in any case $|G_P|^2 > |G| = (q^3 + 1)|G_P| \geq 900g^2$. Hence $|G_P| > 30(g - 1)$, a contradiction.
- $G \cong Ree(q)$. Now, $|G_P| = q^3(q - 1)$ and $|G_P|^2 > |G| = (q^3 + 1)|G_P| \geq 900g^2$. Hence $|G_P| > 30(g - 1)$, a contradiction.
Before analyzing the case in which $K$ is not trivial, we prove a trivial intersection condition for the stabilizers of points in distinct $G$-orbits.

**Lemma 4.2** If $Q \in O_2$ then $G_P \cap G_Q$ is trivial.

**Proof** Let $\alpha \in G_P \cap G_Q$ non-trivial. Then the order of $\alpha$ is not divisible by $p$. Hence $\alpha \in U$ up to conjugation. Since $|O_1| = q + 1$ from Lemma 4.1, $\alpha$ fixes at least another point $R \in O_1 \setminus \{P\}$. Since $P$, $Q$ and $R$ are in three distinct $G^{(1)}_P$-orbits the automorphism $\bar{\alpha}$ induced by $\alpha$ on $\mathcal{Y}_1$ has at least three fixed point on $\mathcal{Y}_1$. Since the order of $\alpha$ is the same as the order of $\bar{\alpha}$, from Item 5 of Result 2.8 we get that $\alpha$ has order 1, completing the proof. \(\Box\)

This proves that $K$ is not trivial and from Lemma 4.2 the only short orbits of $K$ are exactly the points in $O_1$.

We claim that $g(\mathcal{X}/K) = 0$. Assume first that $g(\mathcal{X}/K) \geq 2$. Then arguing as for the previous cases using the Hurwitz genus formula, $|G|/|K| \geq 900g(\mathcal{X}/K)^2$. Also the set of points $\bar{O}_1$ and $\bar{O}_2$ lying below $O_1$ and $O_2$ in $\mathcal{X}/\mathcal{Y}/K$ are respectively a short and a long orbit of $G/K$. If $G/K$ has not exactly one another tame short orbit on $\mathcal{X}/K$ then $|G|/|K| \leq 336g(\mathcal{X}/K)^2$ from Sect. 3 and Theorem 1.3 Item 1, a contradiction. Since now $G/K$ has exactly two short orbits (one tame and one non-tame) and $g(\mathcal{X}/2) < g$ from the minimality of $g$ we get a contradiction.

Suppose that $g(\mathcal{X}/K) = 1$. Then $|U| \leq 12$ from [7, Theorem 11.94]. Note that if $\gamma > 0$ then from Item 1 of Result 2.8, $|O_1| = 1 + |G^{(1)}_P| < 2|G^{(1)}_P| \leq 2(p(g - 1)/(p - 2) < 4g$. Hence

$$|G| < 4g|G^{(1)}_P||U| \leq 192g^2,$$

a contradiction. Thus $\mathcal{X}/K$ is rational and hence $G/K \cong PSL(2, q)$. $PGL(2, q)$ since the other groups do not occur as subgroups of automorphisms of curves of genus zero. From the Hurwitz genus formula

$$2g - 2 = -2|K| + (|K| - 1)(q + 1),$$

so that $g = (q - 1)(|K| - 1)/2$. In particular $|O||K| = (q + 1)|K| \leq 10g$. Hence

$$900g^2 \leq |G| = |O||G_P| < 10g|G_P|.$$  

So, $|G_P| > 30(g - 1)$. The claim now follows from Lemma 2.7.

We are left with the last case in Lemma 4.1, that is, a minimal normal subgroup of $G/K$ is soluble and the size of $O_1$ is a prime power. Since $q$ is odd, we get $q + 1 = 2t$ for some $t \geq 1$. From Mihăilescu Theorem either $q = p$ is a Marsenne prime or $q = 8$. Since $q$ is odd, $q = p$ is a Marsenne prime and $q = p = |G^{(1)}_P|$. Assume that $\gamma \neq 0$. If $|G_P| < 30(g - 1)$ we get from Item 1 of Result 2.8 that $|G| = |O||G_P| < 30(g - 1)(|G^{(1)}_P| + 1) < 900g^2$, a contradiction. Hence $|G_P| \geq 30(g - 1)$ and Lemma 2.7 gives the desired contradiction. Indeed Sylow $p$-subgroup of $G$ intersect trivially as they all fix exactly one point on $O_1$.

This proves Item 4 in Theorem 1.3 so that Theorem 1.3 is completely proven. We conclude this section with the following open problem.

**Open problem 4.3** Is the condition $|G| \geq 900g^2$ sufficient to imply $\gamma(\mathcal{X}) = 0$ also when $g(\mathcal{X}/G^{(1)}_P) \geq 1$ for $P \in O_1$, or $|G_{P,R}| = p^ih$ with $R \in O_1 \setminus \{P\}$, $i \geq 1$ and $h > 1$?

**Acknowledgements** The author would like to thank Prof. Massimo Giulietti and Dr. Pietro Speziali for the helpful discussions and comments on the topic.
On algebraic curves with many automorphisms in characteristic $p$

References

1. Biggs, N.L., White, A.T.: Permutation Groups and Combinatorial Structures, London Mathematical Society Lecture Note Series 33, p. 140. Cambridge University Press, Cambridge (1979)
2. Cameron, P. J.: Permutation Groups. London Mathematical Society Student Texts, 45. Cambridge University Press, Cambridge, x+220 (1999)
3. Giulietti, M., Korchmáros, G.: Algebraic curves with many automorphisms. Adv. Math. 349, 162–211 (2019)
4. Giulietti, M., Korchmáros, G.: A new family of maximal curves over a finite field. Math. Ann. 343, 229–245 (2009)
5. Giulietti, M., Montanucci, M., Quoos, L., Zini, G.: On some Galois covers of the Suzuki and Ree curves. J. Number Theory 189, 220–254 (2018)
6. Henn, H.W.: Funktionenkörper mit großer Automorphismengruppe. J. Reine Angew. Math. 302, 96–115 (1978)
7. Hirschfeld, J.W.P., Korchmáros, G., Torres, F.: Algebraic Curves over a Finite Field. Princeton Series in Applied Mathematics, Princeton (2008)
8. Hurwitz, A.: Über algebraische Gebilde mit eindeutigen Transformationen in sich. Math. Ann. 41, 403–442 (1893)
9. Kantor, W.M., O’Nan, M.E., Seitz, G.M.: 2-Transitive groups in which the stabilizer of two points is cyclic. J. Algebra 21, 17–50 (1972)
10. Korchmáros, G., Montanucci, M., Speziali, P.: Transcendence degree one function fields over a finite field with many automorphisms. J. Pure Appl. Algebra 222, 1810–1826 (2018)
11. Macbeath, A.M.: On a theorem of Hurwitz. Proc. Glasgow Math. Assoc. 5, 90–96 (1961)
12. Madan, M., Rosen, M.: The automorphism group of a function field. Proc. Am. Math. Soc. 115, 923–929 (1992)
13. Madden, D.J., Valenti, R.C.: The group of automorphisms of algebraic function fields. J. Reine Angew. Math. 343, 162–168 (1983)
14. Nakajima, S.: $p$-ranks and automorphism groups of algebraic curves. Trans. Am. Math. Soc. 303, 595–607 (1987)
15. Roquette, P.: Abschätzung der Automorphismenanzahl von Funktionenkörpern bei Primzahl charakteristik. Math. Z. 117, 157–163 (1970)
16. Schmid, H.L.: Über die Automorphismen eines algebraischen Funktionenkörpers von Primzahl charakteristik. J. Reine Angew. Math. 179, 5–15 (1938)
17. Serre, J.P.: Local Fields, Graduate Texts in Mathematics 67, Springer, New York, viii+241 pp (1979)
18. Skabelund, D.: New maximal curves as ray class fields over Deligne-Lusztig curves. Proc. Am. Math. Soc. 146, 525–540 (2017)
19. Stichtenoth, H.: Algebraic Function Fields and Codes. Graduate Texts in Mathematics, vol. 254. Springer, Berlin (2009)
20. Stichtenoth, H.: Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. I. Eine Abschätzung der Ordnung der Automorphismengruppe. Arch. Math. 24, 527–544 (1973)
21. Stichtenoth, H.: Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. II. Ein spezieller Typ von Funktionenkörpern. Arch. Math. 24, 615–631 (1973)
22. Stichtenoth, H.: Zur Realisierbarkeit endlicher Gruppen als Automorphismengruppen algebraischen Funktionenkörpers. Math. Z. 187, 221–225 (1984)
23. Sullivan, F.: $p$-torsion in the class group of curves with many automorphisms. Arch. Math. 26, 253–261 (1975)
24. Valenti, R.C., Madan, M.L.: A Hauptsatz of L.E. Dickson and Artin-Schreier extensions. J. Reine Angew. Math. 318, 156–177 (1980)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.