ORDINARY ALGEBRAIC CURVES WITH MANY AUTOMORPHISMS IN POSITIVE CHARACTERISTIC

GÁBOR KORCHMÁROS AND MARIA MONTANUCCI

Keywords: Algebraic curves, algebraic function fields, positive characteristic, automorphism groups.

Subject classifications: 14H37, 14H05.

Abstract. Let $X$ be an ordinary (projective, geometrically irreducible, nonsingular) algebraic curve of genus $g(X) \geq 2$ defined over an algebraically closed field $K$ of odd characteristic $p$. Let $\text{Aut}(X)$ be the group of all automorphisms of $X$ which fix $K$ element-wise. For any solvable subgroup $G$ of $\text{Aut}(X)$ we prove that $|G| \leq 34(g(X) + 1)^{3/2}$. There are known curves attaining this bound up to the constant 34. For $p$ odd, our result improves the classical Nakajima bound $|G| \leq 84(g(X) - 1)g(X)$, see [8], and, for solvable groups $G$, the Gunby-Smith-Yuan bound $|G| \leq 6(g(X)^2 + 12\sqrt{21}g(X)^{3/2})$ where $g(X) > cp^2$ for some positive constant $c$; see [2].

1. Introduction

In this paper, $X$ stands for a (projective, geometrically irreducible, nonsingular) algebraic curve of genus $g(X) \geq 2$ defined over an algebraically closed field $K$ of odd characteristic $p$. Let $\text{Aut}(X)$ be the group of all automorphisms of $X$ which fix $K$ element-wise. The assumption $g(X) \geq 2$ ensures that $\text{Aut}(X)$ is finite. However the classical Hurwitz bound $|\text{Aut}(X)| \leq 84(g(X) - 1)$ for complex curves fails in positive characteristic, and there exist four families of curves satisfying $|\text{Aut}(X)| \geq 8g^3(X)$; see [11], Henn [4], and also [3, Section 11.12]. Each of them has has $p$-rank $\gamma(X)$ (equivalently, its Hasse-Witt invariant) equal to zero; see for instance [1]. On the other hand, if $X$ is ordinary, i.e. $g(X) = \gamma(X)$, Guralnik and Zieve announced in 2004, as reported in [2, 5], that for odd $p$ there exists a sharper bound, namely $|\text{Aut}(X)| \leq c_p g(X)^{8/5}$ with some constant $c_p$ depending on $p$. It should be noticed that no proof of this sharper bound is available in the literature. In this paper, we concern with solvable automorphism groups $G$ of an ordinary curve $X$, and for odd $p$ we prove the even sharper bound:

**Theorem 1.1.** Let $X$ be an algebraic curve of genus $g(X) \geq 2$ defined over an algebraically closed field $K$ of odd characteristic $p$. If $X$ is ordinary and $G$ is a solvable subgroup of $\text{Aut}(X)$ then

$$|G| \leq 34(g(X) + 1)^{3/2}. \tag{1}$$

For odd $p$, our result provides an improvement on the classical Nakajima bound $|G| \leq 84(g(X) - 1)g(X)$, see [8], and, for solvable groups, on the recent Gunby-Smith-Yuan bound $|G| \leq 6(g(X)^2 + 12\sqrt{21}g(X)^{3/2})$ proven in [2] under the hypothesis that $g(X) > cp^2$ for some positive constant $c$.

The following example is due to Stichtenoth and it shows that (1) is the best possible bound apart from the constant $c$. Let $\mathbb{F}_q$ be a finite field of order $q = p^b$ and let $\overline{\mathbb{F}}_q$ denote its algebraic closure. For a positive integer $m$ prime to $p$, let $Y$ be the irreducible curve with affine equation

$$y^q + y = x^m + \frac{1}{x^m}. \tag{2}$$
and $F = \mathbb{K}(\mathcal{Y})$ its function field. Let $t = x^{m(q-1)}$. The extension $F|\mathbb{K}(t)$ is a non-Galois extension as the Galois closure of $F$ with respect to $H$ is the function field $\mathbb{K}(x, y, z)$ where $x, y, z$ are linked by \eqref{2} and $z^q + z = x^m$. Furthermore, $\mathfrak{g}(\mathcal{Y}) = (q-1)(qm-1)$, $\gamma(\mathcal{Y}) = (q-1)^2$ and $\text{Aut}(\mathcal{Y})$ contains a subgroup $Q \rtimes U$ of index 2 where $Q$ is an elementary abelian normal subgroup of order $q^2$ and the complement $U$ is a cyclic group of order $m(q-1)$. If $m = 1$ then $\mathcal{Y}$ is an ordinary curve, and in this case $2\mathfrak{g}(\mathcal{Y})^{3/2} = 2(q-1)^3 < 2q^2(q-1)$ which shows indeed that \eqref{1} is sharp up to the constant $c$.

2. Background and Preliminary Results

For a subgroup $G$ of $\text{Aut}(\mathcal{X})$, let $\bar{\mathcal{X}}$ 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, $\bar{\mathcal{X}}$ is called the quotient curve of $\mathcal{X}$ by $G$ and denoted by $\mathcal{X}/G$. The field extension $\mathbb{K}(\mathcal{X})|\mathbb{K}(\mathcal{X})^G$ is Galois of degree $|G|$.

Since our approach is mostly group theoretical, we prefer to use notation and terminology from Group theory rather than from Function field theory.

Let $\Phi$ be the cover of $\mathcal{X}|\bar{\mathcal{X}}$ where $\bar{\mathcal{X}} = \mathcal{X}/G$. 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 $\bar{Q} \in \bar{\mathcal{X}}$ is a branch point of $G$ if there is a ramification point $P \in \mathcal{X}$ such that $\Phi(P) = \bar{Q}$, the ramification (branch) locus of $G$ is the set of all ramification (branch) points. The $G$-orbit of $P \in \mathcal{X}$ is the subset $o = \{ R \mid R = g(P), g \in G \}$ of $\mathcal{X}$, and it is long if $|o| = |G|$, otherwise $o$ is short. For a point $\bar{Q}$, the $G$-orbit $o$ lying over $\bar{Q}$ consists of all points $P \in \mathcal{X}$ such that $\Phi(P) = \bar{Q}$. If $P \in o$ then $|o| = |G|/|G_P|$ and hence $\bar{Q}$ is a branch point if and only if $o$ is a short $G$-orbit. It may be that $G$ has no short orbits. This is the case if and only if every 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 \cite{10} Chapter IV]) and defined to be

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

where $t$ is a uniformizing element (local parameter) at $P$. Here $G_P^{(0)} = G_P$.

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

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

where the different $d_P$ at $P$ is given by

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

Let $\gamma$ be the $p$-rank of $\mathcal{X}$, and let $\bar{\gamma}$ be the $p$-rank of the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/S$. The Deuring-Shafarevich formula, see \cite{12} or \cite{3} Theorem 11.62], states that

$$\gamma - 1 = |G|(|\bar{\gamma} - 1| + \sum_{i=1}^k (|G| - \ell_i))$$

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

A subgroup of $\text{Aut}(\mathcal{X})$ is a prime to $p$ group (or a $p'$-subgroup) if its order is prime to $p$. A subgroup $G$ of $\text{Aut}(\mathcal{X})$ is tame if the 1-point stabilizer of any point in $G$ is $p'$-group. Otherwise, $G$ is non-tame (or wild). Obviously, every $p'$-subgroup of $\text{Aut}(\mathcal{X})$ is tame, but the converse is not always true. By a theorem of Stichtenoth, see \cite{3} Theorem 11.56, if $|G| > 84(q(\mathcal{X})-1)$ then $G$ is non-tame. An orbit $o$ of $G$ is tame if $G_P$ is a $p'$-group for $P \in o$. The stabilizer $G_P$ of a point $P \in \mathcal{X}$ in $G$ is a semidirect product $G_P = Q_P \rtimes U$ where the normal subgroup $Q_P$ is a $p$-group while the complement $U$ is a cyclic prime to $p$ group; see \cite{3}
Theorem 11.49). By a theorem of Serre, if $X$ is an ordinary curve then $Q_P$ is elementary abelian and no nontrivial element of $U$ commutes with a nontrivial element of $Q_P$; see \[3, \text{Lemma 11.75}\]. In particular, $|U|$ divides $|Q_P| - 1$, see \[3, \text{Proposition 1}\], and $G_P$ is not abelian when either $Q_P$ or $U$ is nontrivial.

The following two lemmas of independent interest play a role in our proof of Theorem 1.1.

**Lemma 2.1.** Let $X$ be an ordinary algebraic curve of genus $g(X) \geq 2$ defined over an algebraically closed field $\mathbb{K}$ of odd characteristic $p$. Let $H$ be a solvable automorphism group of $\text{Aut}(X)$ containing a normal $p$-subgroup $Q$ such that $|Q|$ and $|H : Q|$ are coprime. Suppose that a complement $U$ of $Q$ in $H$ is abelian and that

$$|H| > \begin{cases} 18(g - 1) & \text{for } |U| = 3, \\ 12(g - 1) & \text{otherwise.} \end{cases}$$

Then $U$ is cyclic, and the quotient curve $\overline{X} = X/Q$ is rational. Furthermore, $Q$ has exactly two (non-tame) short orbits, say $\Omega_1, \Omega_2$. They are also the only short orbits of $H$, and $g(X) = |Q| + (|\Omega_1| + |\Omega_2|) + 1$.

**Proof.** From the Schur-Zassenhaus theorem \[\mathbb{Z} \text{ Corollary 7.5}\], $H = Q \times U$. Set $|Q| = p^k$, $|U| = u$. Then $p \nparallel u$. Furthermore, if $u = 2$ then $|H| = 2|Q| > 9g(X)$ whence $|Q| > 4.5g(X)$. From Nakajima’s bound $X$, see \[3, \text{Theorem 11.84}\], has zero $p$-rank. Therefore $u \geq 3$.

Three cases are treated separately according as the quotient curve $\overline{X} = X/Q$ has genus $\tilde{g}$ at least 2, or $\overline{X}$ is elliptic, or rational.

If $g(X) \geq 2$, then $\text{Aut}(X)$ has a subgroup isomorphic to $U$, and \[3, \text{Theorem 11.79}\] yields $4g(X) + 4 \geq |U|$. Furthermore, from the Hurwitz genus formula applied to $Q$, $g - 1 \geq |Q|(g(X) - 1)$. Therefore, if $c = 12$ or $c = 18$, according as $|U| > 3$ or $|U| = 3$,

$$(4g(X) + 4)|Q| \geq |U||Q| = |H| > c(g - 1) = 12|Q|(g(X) - 1),$$

whence

$$c < 4 \frac{g(X) + 1}{g(X) - 1} \leq 12,$$

a contradiction.

If $X$ is elliptic, then the cover $X|\overline{X}$ ramifies, otherwise $X$ itself would be elliptic. Thus, $Q$ has some short orbits. Take one of them together with its images $o_1, \ldots, o_{|U|}$ under the action of $H$. Since $Q$ is a normal subgroup of $H$, $o = o_1 \cup \ldots \cup o_{|U|}$ is a $H$-orbit of size $u_1p^v$ where $p^v = |o_1| = \ldots |o_{|U|}|$. Equivalently, the stabilizer of a point $P \in o$ has order $p^{k-v}u/u_1$, and it is the semidirect product $Q_1 \rtimes U_1$ where $|Q_1| = p^{k-v}$ and $|U_1| = u/u_1$ for a subgroup $Q_1$ of $Q$ and $U_1$ of $U$ respectively. The point $\overline{P}$ lying under $P$ in the cover $X|\overline{X}$ is fixed by the factor group $U_1 = U_1Q/Q$. Since $\overline{X}$ is elliptic, \[3, \text{Theorem 11.94}\] implies $|U_1| \leq 12$ for $p = 3$ and $|U_1| \leq 6$ for $p > 3$. As $U_1 \cong U_1$, this yields the same bound for $|U_1|$, that is, $u \leq 4u_1$ for $p = 3$ and $u \leq 6u_1$ for $p > 3$. Furthermore, $d_P \geq 2(p^{k-v} - 1) \geq \frac{2}{3}p^{k-v}$. From the Hurwitz genus formula applied to $Q$, if $p = 3$ then

$$2g - 2 \geq 3^v u_1 d_P \geq 3^v u_1 (\frac{2}{3}p^{k-v}) \geq \frac{4}{3}3^k u_1 \geq \frac{1}{3}p^k u = \frac{1}{3}|Q||U| = \frac{1}{3}|H|,$$

while for $p > 3$,

$$2g - 2 \geq p^v u_1 d_P \geq p^v u_1 (\frac{2}{3}p^{k-v}) \geq \frac{4}{3}p^k u_1 \geq \frac{2}{3}p^k u = \frac{2}{3}|Q||U| = \frac{2}{3}|H|,$$

But this contradicts (6).

If $\overline{X}$ is rational, then $Q$ has at least one short orbit. Furthermore, $\overline{U} = UQ/Q$ is isomorphic to a subgroup of $\text{PGL}(2, \mathbb{K}) \cong \text{Aut}(\overline{X})$. Since $U \cong \overline{U}$, the classification of finite subgroups of $\text{PGL}(2, \mathbb{K})$, see \[14\], shows that $U$ is cyclic, $\overline{U}$ fixes two points $P_0$ and $\overline{P}_\infty$ but no nontrivial element in $\overline{U}$ fixes a point other than $P_0$ and $\overline{P}_\infty$. Let $o_\infty$ and $o_0$ be the $Q$-orbits lying over $P_0$ and $\overline{P}_\infty$, respectively. Obviously, $o_\infty$ and $o_0$ are short orbits of $H$. We show that $Q$ has at most two short orbits, the candidates being $o_\infty$ and $o_0$. By absurd, there is a $Q$-orbit $o$ of size $p^m$ with $m < k$ which lies over a point $P \in \overline{X}$ different from both $P_0$ and $\overline{P}_\infty$. 
Since the orbit of $\bar{P}$ in $\bar{U}$ has length $u$, then the $H$-orbit of a point $P \in o$ has length $up^n$. If $u > 3$, the Hurwitz genus formula applied to $Q$ gives

$$2g - 2 \geq -2p^k + up^n(p^{k-m} - 1) \geq -2p^k + up^n \cdot \frac{2}{3}p^{k-m} \geq -2p^k + \frac{2}{3}up^k \geq \frac{2}{3}(u - 3)p^k \geq \frac{1}{3}up^k = \frac{1}{3}|H|,$$

a contradiction with $|H| > 12(g - 1)$. If $u = 3$ then $p > 3$, and hence

$$2g - 2 \geq -2p^k + 3p^m(p^{k-m} - 1) = p^k - 3p^m > \frac{1}{3}p^k,$$

whence $|H| = 3p^k < 18(g - 1)$, a contradiction with $\mathfrak{R}$. This proves that $H$ has exactly two short orbits. Assume that $Q$ has two short orbits. They are $o_\infty$ and $o_0$. If their lengths are $p^a$ and $p^b$ with $a, b < k$, the Deuring-Shafarevich formula applied to $Q$ gives

$$g(\mathcal{X}) - 1 = g(\mathcal{Y}) - 1 = -p^k + (p^k - p^a) + p^k - p^b$$

whence $g(\mathcal{X}) = p^k - (p^a + p^b) + 1 > 0$. The same argument shows that if $Q$ has just one short orbit, then $g(\mathcal{X}) = 0$, a contradiction. \hfill \square

**Lemma 2.2.** Let $N$ be an automorphism group of an algebraic curve of even genus such that $|N|$ is even. Then any 2-subgroup of $N$ has a cyclic subgroup of index 2.

**Proof.** Let $U$ be a subgroup of $\text{Aut}(\mathcal{X})$ of order $d = 2^n \geq 2$, and $\bar{X} = \mathcal{X}/N$ the arising quotient curve. From the Hurwitz genus formula applied to $U$,

$$2g(\mathcal{X}) - 2 = 2(p - 2)p^{n-1} = 2^n(2p\bar{X} - 2) + \sum_{i=1}^{m} (2\ell_i - \ell_i)$$

where $\ell_1, \ldots, \ell_m$ are the short orbits of $U$ on $\mathcal{X}$. Since $2(p - 2)p^{n-1} \equiv 2 \pmod{4}$ while $2^n(2p\bar{X} - 2) \equiv 0 \pmod{4}$, some $\ell_i$ ($1 \leq i \leq m$) must be either 1 or 2. Therefore, $U$ or a subgroup of $U$ of index 2 fixes a point of $\mathcal{X}$ and hence is cyclic. \hfill \square

### 3. The proof of Theorem 1.1

The assertion holds for $g(\mathcal{X}) = 2$, as $|G| \leq 48$ for any solvable automorphism group $G$ of a genus two curve; see \cite[Proposition 11.99]{[R]}]. For $g(\mathcal{X}) > 2$, $\mathcal{X}$ is taken by absurd for a minimal counterexample with respect the genera so that for any solvable subgroup of $\text{Aut}(\mathcal{X})$ of an ordinary curve $\bar{\mathcal{X}}$ of genus $g(\bar{\mathcal{X}}) \geq 2$ we have $|\bar{G}| \leq 34(\bar{g} + 1)^{3/2}$. Two cases are treated separately.

#### 3.1. Case I: $G$ contains a minimal normal $p$-subgroup.

**Proposition 3.1.** Let $\mathcal{X}$ be an ordinary algebraic curve of genus $g$ defined over an algebraically closed field $\mathbb{K}$ of odd characteristic $p > 0$. If $G$ is a solvable subgroup of $\text{Aut}(\mathcal{X})$ containing a minimal normal $p$-subgroup $N$, then $|G| \leq 34(g + 1)^{3/2}$.

**Proof.** Take the largest normal $p$-subgroup $Q$ of $G$. Let $\bar{X}$ be the quotient curve of $X$ with respect to $Q$ and let $\bar{G} = G/Q$. The quotient group $\bar{G}$ is a subgroup of $\text{Aut}(\bar{X})$ and it has no normal $p$-subgroup, otherwise $G$ would have a normal $p$-subgroup properly containing $Q$. For $\bar{g} = g(\bar{X})$ three cases may occur, namely $\bar{g} \geq 2$, $\bar{g} = 1$ or $\bar{g} = 0$. If $\bar{g} \geq 2$, from the Hurwitz genus formula,

$$2\bar{g} - 2 \geq |Q|(2\bar{g} - 2) = \frac{|G|}{|\bar{G}|}(2\bar{g} - 2)$$

whence $|\bar{G}| > 34(\bar{g} + 1)^{3/2}$. Since $\bar{X}$ is still ordinary, this contradicts our choice of $\mathcal{X}$ to be a minimal counterexample. If $\bar{g} = 1$ then the cover $\mathbb{K}(\mathcal{X})/\mathbb{K}(\bar{X})$ ramifies. Take short orbit $\Delta$ of $Q$. Let $\Gamma$ be the non-tame short orbit of $G$ that contains $\Delta$. Since $Q$ is normal in $G$, the orbit $\Gamma$ partitions into short orbits...
of $Q$ whose components have the same length which is equal to $|\Delta|$. Let $k$ be the number of the $Q$-orbits contained in $\Gamma$. Then,
\[ |G_P| = \frac{|G|}{k|\Delta|}, \]
holds for every $P \in \Gamma$. Moreover, the quotient group $G_PQ/Q$ fixes a place on $\tilde{X}$. Now, from [3, Theorem 11.94 (ii)],
\[ \frac{|G_PQ|}{|Q|} = \frac{|G_P|}{|G_P \cap Q|} = \frac{|G_P|}{|Q_P|} \leq 12. \]
From this together with the Hurwitz genus formula and [3, Theorem 2 (i)],
\[ 2g - 2 \geq 2k|\Delta|(|Q_P| - 1) \geq 2k|\Delta|\frac{|Q_P|}{2} \geq \frac{k|\Delta||G_P|}{12} = \frac{|G|}{12}, \]
which contradicts our hypothesis $|G| > 34(g + 1)^{3/2}$.

It turns out that $\tilde{X}$ is rational. Therefore $\tilde{G}$ is isomorphic to a subgroup of $PGL(2, \mathbb{K})$ which contains no normal $p$-subgroup. From the classification of finite subgroups of $PGL(2, \mathbb{K})$, see [13], $\tilde{G}$ is a prime to $p$ subgroup which is either cyclic, or dihedral, or isomorphic to one of the the groups $Alt_4$, $Sym_4$. In all cases, $\tilde{G}$ has a cyclic subgroup $U$ of index at most 6 and of order distinct from 3. We may dismiss all cases but the cyclic one assuming that $G = Q \times U$ with $|G| \geq \frac{2}{3}(g(X) + 1)^{3/2}$. Then $|G| > 12(g - 1)$. Therefore, Lemma 2.1 applies to $G$. Thus, $Q$ has exactly two (non-tame) orbits, say $\Omega_1$ and $\Omega_2$, and they are also the only short orbits of $G$. More precisely,
\[ \gamma - 1 = |Q| - (|\Omega_1| + |\Omega_2|). \]
We may also observe that $G_p$ with $P \in \Omega_1$ contains a subgroup $V$ isomorphic to $U$. In fact, $|Q||U| = |G| = \frac{|G_p||\Omega_1|}{|Q_p \times V||\Omega_1|} = \frac{|V||Q_P||\Omega_1|}{|V||Q_P||\Omega_1|}$ with a prime to $p$ subgroup $V$ fixing $P$, whence $|U| = |V|$. Since $V$ is cyclic the claims follows.

We go on with the case where both $\Omega_1$ and $\Omega_2$ are nontrivial, that is, their lengths are at least 2.

Assume that $Q$ is non-abelian and look at the action of its center $Z(Q)$ on $X$. Since $Z(Q)$ is a nontrivial normal subgroup of $G$, arguing as before we get that the factor group $X/Z(Q)$ is rational, and hence the Galois cover $X/(X/Z(Q))$ ramifies at some points. In other words, there is a point $P \in \Omega_1$ (or $R \in \Omega_2$) such that some nontrivial subgroup $T$ of $Z(Q)$ fixes $P$ (or $Q$). Suppose that the former case occurs. Since $\Omega_1$ is a $P$-orbit, $T$ fixes $\Omega_1$ pointwise.

The group $G$ induces a permutation group on $\Omega_1$ and let $M_1$ be the kernel of this permutation representation. Obviously, $T$ is a nontrivial $p$-subgroup of $M_1$. Therefore $M$ contains some but not all elements from $Q$. Since both $M_1$ and $Q$ are normal subgroups of $G$, $N = M_1 \cap Q$ is a nontrivial normal $p$-subgroup of $G$. From (ii), the quotient curve $X = X/N$ is rational, and hence the factor group $\tilde{G} = G/N$ is isomorphic to a subgroup of $PGL(2, \mathbb{K})$. Since $1 \leq N \leq Q$, the order of $\tilde{G}$ is divisible by $p$. From the classification of subgroups of $PGL(2, \mathbb{K})$, see [13], $\tilde{G} = \tilde{Q} \times \tilde{U}$ where $\tilde{Q}$ is an elementary abelian $p$-group of order $q$ and $\tilde{U} \cong U/N \cong U$ with $|\tilde{U}| = |U|$ is a divisor of $q - 1$.

This shows that $Q$ acts on $\Omega_1$ as an abelian transitive permutation group. Obviously this holds true when $Q$ is abelian. Therefore, the action of $Q$ on $\Omega_1$ is sharply transitive. In terms of 1-point stabilizers of $Q$ on $\Omega_1$, we have $Q_{P} = Q_{P'}$ for any $P, P' \in \Omega_1$. Moreover, $Q_{P} = N$, and hence $Q_{P}$ is a normal subgroup of $G$.

Furthermore, since $X$ is an ordinary curve, $Q_{P}$ is an elementary abelian group by [3, Theorem 2 (i)] and [3 Theorem 11.74 (iii)].

The quotient curve $X/Q_{P}$ is rational and its automorphism group contains the factor group $Q/Q_{P}$. Hence, exactly one of the $Q_{P}$-orbits is preserved by $Q$. Since $\Omega_1$ is a $Q$-orbit consisting of fixed points of $Q_{P}$, $\Omega_2$ must be a $Q_{P}$-orbit. Similarly, if $Z(Q) \neq Q_{P}$, the factor group $Z(Q)Q_{P}/Q_{P}$ is an automorphism group of $X/Q_{P}$ and hence exactly one of the $Q_{P}$-orbits is preserved by $Z(Q)$. Either $Z(Q)$ fixes a point in $\Omega_1$ but then $Z(Q) = Q_{P}$, or $\Omega_2$ is a $Z(Q)$-orbit. This shows that either $Z(Q) = Q_{P}$ or $Z(G)$ acts transitively on $\Omega_2$.\"
Two cases arise according as $Q_P$ is sharply transitive and faithful on $\Omega_2$ or some nontrivial element in $Q_P$ fixes $\Omega_2$ pointwise.

If some nontrivial element in $Q_P$ fixes $\Omega_2$ pointwise then the kernel $M_2$ of the permutation representation of $H$ on $\Omega_2$ contains a nontrivial $p$-subgroup. Hence the above results extends from $\Omega_1$ to $\Omega_2$, and $Q_R$ is a normal subgroup of $Q$.

If $Q_P$ is (sharply) transitive on $\Omega_2$ then the abelian group $Z(Q)Q_P$ acts on $\Omega_2$ as a sharply transitive permutation group, as well. Hence either $Z(Q) = Q_P$, or as before $M_2$ contains a nontrivial $p$-subgroup, and $Q_R$ is a normal subgroup of $Q$. In the former case, $Q = Q_PQ_R$ and $Q_R \cap Q_P = \{1\}$, and $Z(Q) = Q_P$ yields that

$$Q = Q_P \times Q_R.$$ 

This shows that $Q$ is abelian, and hence $|Q| \leq 4g + 4$. Also, either $|Q_P|$ (or $|Q_R|$) is at most $\sqrt{4g + 4}$. Since $\mathcal{X}$ is an ordinary curve, the second ramification group $G^{(2)}_P$ at $P \in \Omega_1$ is trivial. For $G_P = Q_P \times V$, Lemma 11.81 gives $|U| = |V| \leq |Q_P| - 1$. Hence $|U| < |Q_P| \leq \sqrt{|Q|} \leq \sqrt{4g + 4}$ whence

$$|G| = |U||Q| \leq 8(g + 1)^3/2.$$ 

If $Q_R$ is a normal subgroup, take a point $R$ from $\Omega_2$, and look at the subgroup $Q_P \cap Q_R$ of $Q_P$ fixing $R$. Actually, we prove that both $Q_P \cap Q_R = Q_P$ or $Q_P \cap Q_R$ is trivial. Suppose that $Q_P \cap Q_R \neq \{1\}$. Since $Q_P \cap Q_R = Q_P \cap Q_R$ and both $Q_P$ and $Q_R$ are normal subgroups of $G$, then same holds for $Q_P \cap Q_R$. By (ii), the quotient curve $\mathcal{X}/Q_P \cap Q_R$ is rational and hence its automorphism group $Q/Q_P \cap Q_R$ fixes exactly one point. Furthermore, each point in $\Omega_1$ is totally ramified. Therefore, $Q_R = Q_P \cap Q_R$, otherwise $Q_R/Q_P \cap Q_R$ would fix any point lying under a point in $\Omega_1$ in the cover $\mathcal{X}/Q_P \cap Q_R$.

It turns out that either $Q_P = Q_R$ or $Q_P \cap Q_R = \{1\}$, whenever $P \in \Omega_1$ and $R \in \Omega_2$.

In the former case, from the Deuring-Shafarevič formula applied to $Q_P$, the stabilizer $Q_P$ of $Q_P$ of $Q_P$ is abelian, since $Q_P$ is the image of $Q_P$ in $G_P$, and hence $G_P$ has a permutation representation on $\Omega_2$ with kernel $K$. As $\Omega_2$ is a short orbit of $Q$, the stabilizer $Q_R$ of $R \in \Omega_2$ in $Q$ is nontrivial. Since $Q$ is abelian, this yields that $K$ is nontrivial, and hence it is a nontrivial elementary abelian normal subgroup of $G$. In other words, $Q$ is an $r$-dimensional vector space $V(r, p)$ over a finite field $\mathbb{F}_p$ with $|Q| = p^r$, the action of each nontrivial element of $U$ by conjugacy is a nontrivial automorphism of $V(r, p)$, and $K$ is a $K$-invariant subspace. By Maschke’s theorem, see for instance [7 Theorem 6.1], $K$ has a complementary $U$-invariant subspace. Therefore, $Q$ has a subgroup $M$ such that $Q = K \times M$, and $M$ is a normal subgroup of $G$. Since $K \cap M = \{1\}$, and $\Omega_2$ is an orbit of $Q$, this yields $|M| = |\Omega_2|$. The factor group $G/M$ is an automorphism group of the quotient curve $\mathcal{X}/M$, and $Q/M$ is a nontrivial $p$-subgroup of $G/M$ whereas $G/M$ fixes two points on $\mathcal{X}/M$. Therefore the quotient curve $\mathcal{X}/M$ is not rational since the 2-point stabilizer in the representation of $\text{PGL}(2, \mathbb{K})$ as an automorphism group of the rational function field is a prime to $p$ (cyclic) group. We show that $\mathcal{X}/M$ is neither elliptic. From the Deuring-Shafarevič formula, $g(\mathcal{X}) - 1 = g(\mathcal{X}/M) - 1 = |\Omega| + 1 + |\Omega_2|$, and so $g(X)$ is even. Since $M$ is a normal subgroup of odd order, $g(X) \equiv 0 \pmod{2}$ yields that $g(X/M) \equiv 0 \pmod{2}$. In particular, $g(\mathcal{X}/M) \neq 1$. Therefore, $g(\mathcal{X}/M) \geq 2$. At this point we may repeat our previous argument and prove $|G/M| > 34g(\mathcal{X}/M) + 1)^{3/2}$. Again, a contradiction to our choice of $X$ to be a minimal counterexample, which ends the proof in the case where just one of $\Omega_1$ and $\Omega_2$ is trivial.
We are left with the case where both short orbits of \( Q \) are trivial. Our goal is to prove a much stronger bound for this case, namely \(|U| \leq 2\) whence

\begin{equation}
|G| \leq 2(g(\mathcal{X}) + 1).
\end{equation}

We also show that if equality holds then \( \mathcal{X} \) is a hyperelliptic curve with equation

\begin{equation}
f(U) = aT^2 + b + cT^{-1}, \quad a, b, c \in \mathbb{K}^*.
\end{equation}

where \( f(U) \in \mathbb{K}[U] \) is an additive polynomial of degree \(|Q|\).

Let \( \Omega_1 = \{P_1\} \) and \( \Omega_2 = \{P_2\} \). Then \( Q \) has two fixed points \( P_1 \) and \( P_2 \) but no nontrivial element in \( Q \) fixes a point of \( \mathcal{X} \) other than \( P_1 \) and \( P_2 \). From the Deuring-Shafarevič formula

\begin{equation}
g(\mathcal{X}) + 1 = \gamma(\mathcal{X}) + 1 = |Q|.
\end{equation}

Therefore, \(|U| \leq g(\mathcal{X})\). Actually, for our purpose, we need a stronger estimate, namely \(|U| \leq 2\). To prove the latter bound, we use some ideas from Nakajima’s paper [8], regarding the Riemann-Roch spaces \( \mathcal{L}(D) \) of certain divisors \( D \) of \( \mathbb{K}(\mathcal{X}) \). Our first step is to show

(i) \( \text{dim}_K \mathcal{L}((Q) - 1)P_1) = 1 \),

(ii) \( \text{dim}_K \mathcal{L}((Q) - 1)P_1 + P_2 \geq 2 \).

Let \( \ell \geq 1 \) be the smallest integer such that \( \text{dim}_K \mathcal{L}(\ell P_1) = 2 \), and take \( x \in \mathcal{L}(\ell P_1) \) with \( v_{P_1}(x) = -\ell \). As \( Q = Q_{P_1} \), the Riemann-Roch space \( \mathcal{L}(\ell P_1) \) contains all \( c_x = \sigma(x) - x \) with \( \sigma \in \mathbb{C} \). This yields \( c_x \in \mathbb{K} \) by \( v_{P_1}(c_x) \geq -\ell + 1 \) and our choice of \( \ell \) to be minimal. Also, \( Q = Q_{P_2} \) together with \( v_{P_2}(c_x) \geq 1 \) show \( v_{P_2}(c_x) \geq 1 \). Therefore \( c_x = 0 \) for all \( \sigma \in \mathbb{C} \), that is, \( x \) is fixed by \( Q \). From \( \ell = [\mathbb{K}(\mathcal{X}) : \mathbb{K}(x)] = [\mathbb{K} : \mathbb{K}(\mathcal{X})^Q][\mathbb{K}(\mathcal{X})^Q : \mathbb{K}(x)] \) and \( |Q| = [\mathbb{K} : \mathbb{K}(\mathcal{X})^Q] \), it turns out that \( \ell \) is a multiple of \(|Q|\). Thus \( \ell > |Q| - 1 \) whence (i) follows. From the Riemann-Roch theorem, \( \text{dim}_K \mathcal{L}((Q) - 1)P_1 + P_2 \geq |Q| - g + 1 = 2 \) which proves (ii).

Let \( d \geq 1 \) be the smallest integer such that \( \text{dim}_K \mathcal{L}(dP_1 + P_2) = 2 \). From (ii)

\begin{equation}
d \leq |Q| - 1.
\end{equation}

Let \( \alpha \) be a generator of the cyclic group \( U \). Since \( \alpha \) fixes both points \( P_1 \) and \( P_2 \), it acts on \( \mathcal{L}(dP_1 + P_2) \) as a \( \mathbb{K} \)-vector space automorphism \( \bar{\alpha} \). If \( \bar{\alpha} \) is trivial then \( \alpha(u) = u \) for all \( u \in \mathcal{L}(dP_1 + P_2) \). Suppose that \( \bar{\alpha} \) is nontrivial. Since \( U \) is a prime to \( p \) cyclic group, \( \bar{\alpha} \) has two distinct eigenspaces, so that \( \mathcal{L}(dP_1 + P_2) = \mathbb{K} \oplus \mathbb{K} u \) where \( u \in \mathcal{L}(dP_1 + P_2) \) is an eigenvector of \( \bar{\alpha} \) with eigenvalue \( \xi \in \mathbb{K}^\times \) so that \( \bar{\alpha}(u) = \xi u \). Therefore there is \( u \in \mathcal{L}(dP_1 + P_2) \) with \( u \neq 0 \) such that \( \alpha(u) = \xi u \) with \( \xi^{[U]} = 1 \). The pole divisor of \( u \) is

\begin{equation}
div(u)_{\infty} = dP_1 + P_2.
\end{equation}

Since \( Q = Q_{P_1} = Q_{P_2} \), the Riemann-Roch space \( \mathcal{L}(dP_1 + P_2) \) contains \( \sigma(u) \) and hence it contains all

\begin{equation}
\theta_{\sigma} = \sigma(u) - u, \quad \sigma \in Q.
\end{equation}

By our choice of \( d \) to be minimal, this yields \( \theta_{\sigma} \in \mathbb{K} \), and then defines the map \( \theta \), from \( \mathbb{C} \) into \( \mathbb{K} \) that takes \( \sigma \) to \( \theta_{\sigma} \). More precisely, \( \theta \) is a homomorphism from \( \mathbb{C} \) into the additive group \( (\mathbb{K}, +) \) of \( \mathbb{K} \) as the following computation shows:

\begin{equation}
\theta_{\sigma_1 \circ \sigma_2} = (\sigma_1 \circ \sigma_2)(u) - u = \sigma_1(\sigma_2(u) - u + u) - u = \sigma_1(\theta_{\sigma_2}) + \sigma_1(u) - u = \theta_{\sigma_2} + \theta_{\sigma_1} = \theta_{\sigma_1 + \theta_{\sigma_2}}.
\end{equation}

Also, \( \theta \) is injective. In fact, if \( \theta_{\sigma_0} = 0 \) for some \( \sigma_0 \in \mathbb{C} \setminus \{1\} \), then \( u \) is in the fixed field of \( \sigma_0 \), which is impossible since \( v_{P_2}(u) = -1 \) whereas \( P_2 \) is totally ramified in the cover \( \mathcal{X}/(\mathcal{X}/(\sigma P)) \). The image \( \theta(Q) \) of \( \theta \) is an additive subgroup of \( \mathbb{K} \) of order \(|Q|\). The smallest subfield of \( \mathbb{K} \) containing \( \theta(Q) \) is a finite field \( \mathbb{F}_{p^n} \) and hence \( \theta(Q) \) can be viewed as a linear subspace of \( \mathbb{F}_{p^n} \) considered as a vector space over \( \mathbb{F}_p \). Therefore the polynomial

\begin{equation}
f(U) = \prod_{\sigma \in Q} (U - \theta_{\sigma})
\end{equation}
is a linearized polynomial over $\mathbb{F}_p$; see [4] Section 4, Theorem 3.52. In particular, $f(U)$ is an additive polynomial of degree $|Q|$; see also [11] Chapter V, § 5. Also, $f(U)$ is separable as $\theta$ is injective. From (15), the pole divisor of $f(u) \in \mathbb{K}(\mathcal{X})$ is
\[
(16) \quad \text{div}(f(u)) = |Q|(dP_1 + P_2).
\]
For every $\sigma_0 \in Q$,
\[
\sigma_0(f(u)) = \prod_{\sigma \in Q} (\sigma(u) - \theta) = \prod_{\sigma \in Q} (u + \theta - \sigma) = \prod_{\sigma \in Q} (u - \theta - \sigma) = f(u).
\]
Thus $f(u) \in \mathbb{K}(\mathcal{X})^Q$. Furthermore, from $\alpha \in N_{G}(Q)$, for every $\sigma \in Q$ there is $\sigma' \in Q$ such that $\alpha \sigma = \sigma' \alpha$. Therefore
\[
\alpha(f(u)) = \prod_{\sigma \in Q} (\alpha(u) - \sigma) = \prod_{\sigma \in Q} (\alpha(\sigma(u)) - \xi u) = \prod_{\sigma \in Q} (\sigma'(\sigma(u)) - \xi u) = \prod_{\sigma \in Q} (\sigma' u - \xi u) = \xi f(u).
\]
This shows that if $R \in \mathcal{X}$ is a zero of $f(u)$ then $\text{Supp}(\text{div}(f(u)_0))$ contains the $U$-orbit of $R$ of length $|U|$. Actually, since $\sigma(f(u)) = f(u)$ for $\sigma \in Q$, $\text{Supp}(\text{div}(f(u)_0))$ contains the $G$-orbit of $R$ of length $|G| = |Q||U|$. This together with (16) give
\[
(17) \quad |U| = (d + 1).
\]
On the other hand, $\mathbb{K}(\mathcal{X})^Q$ is rational. Let $P_1$ and $P_2$ the points lying under $P_1$ and $P_2$, respectively, and let $R_1, R_2, \ldots, R_k$ with $k = (d + 1)/|U|$ be the points lying under the zeros of $f(u)$ in the cover $\mathcal{X}/(\mathcal{X}/Q)$. We may represent $\mathbb{K}(\mathcal{X})^Q$ as the projective line $\mathbb{K} \cup \{\infty\}$ over $\mathbb{K}$ so that $P_1 = \infty$, $P_1 = 0$ and $R_i = t_i$ for $1 \leq i \leq k$. Let $g(t) = t^d + t^{-1} + h(t)$ where $h(t) \in \mathbb{K}[t]$ is a polynomial of degree $k = (d + 1)/|U|$ whose roots are $r_1, \ldots, r_k$. It turns out that $f(u), g(t) \in \mathbb{K}(\mathcal{X})$ have the same pole and zero divisors, and hence
\[
(18) \quad c f(u) = t^d + t^{-1} + h(t), \quad c \in \mathbb{K}^*.
\]
We prove that $\mathbb{K}(\mathcal{X}) = \mathbb{K}(u, t)$. From [12], see also [3] Remark 12.12, the polynomial $ctf(x) - T^{d+1} - 1 - h(T)T$ is irreducible, and the plane curve $C$ has genus $g(C) = \frac{1}{2}(q - 1)(d + 1)$. Comparison with (12) shows $\mathbb{K}(\mathcal{X}) = C$ and $d = 1$ whence $|U| \leq 2$. If equality holds then $\deg h(T) = 1$ and $\mathcal{X}$ is a hyperelliptic curve with equation (14).

3.2. Case II: $G$ contains no minimal normal $p$-subgroup.

Proposition 3.2. Let $\mathcal{X}$ be an ordinary algebraic curve of genus $g$ defined over a field $\mathbb{K}$ of odd characteristic $p > 0$. If $G$ is a solvable subgroup of $\text{Aut}(\mathcal{X})$ with a minimal normal subgroup $N$ satisfying Case II, then $|G| \leq 34(g(\mathcal{X})) + 1)^{3/2}$.

Proof. From Proposition 3.1 $G$ contains no nontrivial normal $p$-subgroup. The factor group $\tilde{G} = G/N$ is a subgroup of $\text{Aut}(\mathcal{X})$ where $\mathcal{X} = \mathcal{X}/N$. Furthermore, $|N| \leq 4g(\mathcal{X}) + 4$ as $N$ is abelian; see [3] Theorem 11.79. Arguing as in Section 3.1 we see that $\mathcal{X}$ is either rational or elliptic, that is, $g(\mathcal{X}) \geq 2$ is impossible.

A detailed description of the arguments is given below. Assume that $\mathcal{X}$ is a minimal counterexample with respect to the genus. Since $\mathcal{X}$ is ordinary, any $p$-subgroup $S$ of $G$ is an elementary abelian group and it has a trivial second ramification group at any point $\mathcal{X}$. The latter property remains true when $\mathcal{X}$ is replaced by $\mathcal{Y}$. To show this claim, take $P \in \mathcal{X}$ and let $S_P$ the subgroup of the factor group $S = SN/N$ fixing $P$. Since $p \not| |N|$ there is a point $P \in \mathcal{X}$ lying over $P$ which is fixed by $S$. Hence the stabilizer $S_P$ of $P$ in $S$ is a nontrivial normal subgroup of $G_P$. Since $N$ is a normal subgroup in $G$, so is $N_P$ in $G_P$. This yields that the product $N_P S_P$ is actually a direct product. Therefore $N_P$ is trivial, otherwise the second ramification group of $S$ in $P$ is nontrivial by a result of Serre; see [3] Theorem 11.75. Actually, $N$ may be assumed to be the largest normal subgroup $N_1$ of $G$ whose order is prime to $p$. If the quotient curve $\mathcal{X}_1 = \mathcal{X}/N_1$ is neither rational, nor elliptic then its $\mathbb{K}$-automorphism group $G_1 = G/N_1$ has order bigger than $34(g(\mathcal{X}_1)) + 1)^{3/2}$, by the Hurwitz genus formula applied to $N_1$. Since $G$ and hence $G_1$ is solvable, $G_1$ has a minimal normal $d$-subgroup where $d$ must
be equal to $p$ by the choice of $N_1$ to be the largest normal, prime to $p$ subgroup of $G$. Take the largest normal $p$-subgroup $N_2$ of $G_1$. Observe that $N_2 \subseteq G_1$, otherwise $G_1$ is an (elementary) abelian group of order bigger than $34(g(X_1) + 1)^{3/2}$ contradicting the bound $4(g(X_1) + 4)$; see [3 Theorem 11.79]. Now, define $X_2$ to be the quotient curve $X_1/N_2$. Since the second ramification group of $N_1$ at any point of $X_1$ is trivial, the Hurwitz genus formula together with the Deuring-Shafarevich formula give $g(X_1) - \gamma(X_1) = |N_2|(g(X_2) - \gamma(X_2))$. In particular, $X_2$ is neither ordinary or rational by the choice of $p$.

Theorem 11.127]. Also, the factor group $g$ cyclic prime to $p$.

This and (19) yield a contradiction.

First we investigate the elliptic case. Since $g(X) \geq 2$, the Hurwitz genus formula applied to $X$ ensures that $N$ has a short orbit. Let $\Gamma$ be a short orbit of $G$ containing a short orbit of $N$. Since $N$ is a normal subgroup of $G$, $\Gamma$ is partitioned into short-orbits $\Sigma_1, \ldots, \Sigma_k$ of $N$ each of length $|\Sigma|$.

Take a point $R_i$ from $\Sigma_i$ for $i = 1, 2, \ldots, k$, and set $\Sigma = \Sigma_1$ and $S = S_1$. With this notation, $|G| = |G_S||\Gamma| = |G_S||\Sigma|$, and the Hurwitz genus formula gives

\[ 2g(X) - 2 \geq \sum_{i=1}^{k} |\Sigma_i||N_{S_i}| - 1 = k|\Sigma||N_S| - 1) \geq \frac{1}{2}k|\Sigma||N_S| = \frac{1}{2}|G||N_S|/|G_S|. \]

Also, the factor group $G_S/N$ is a subgroup of $\text{Aut}(X)$ fixing the point of $X$ lying under $S$ in the cover $X|\mathcal{X}$. From [3 Theorem 11.94 (ii)],

\[ \frac{|G_S N|}{|N|} = \frac{|G_S|}{|G_S \cap N|} = \frac{|G_S|}{|N_S|} \leq 12. \]

This and (19) yield $|G| \leq 48(g(X) - 1)$, a contradiction with our hypothesis $34(g(X) + 1)^{3/2}$.

Therefore, $X$ is rational. Thus $G$ is isomorphic to a subgroup of $PGL(2, \mathbb{C})$. Since $p$ divides $|G|$ but $|N|$, $G$ contains a nontrivial $p$-subgroup. From the classification of the finite subgroups of $PGL(2, \mathbb{C})$, see [13], either $p = 3$ and $G \cong \text{Alt}_4$, $\text{Sym}_4$, or $G = \bar{Q} \times \tilde{C}$ where $\bar{Q}$ is a normal $p$-subgroup and its complement $\tilde{C}$ is a cyclic prime to $p$ subgroup and $|\tilde{C}|$ divides $|Q| - 1$.

If $G \cong \text{Alt}_4, \text{Sym}_4$ then $|G| \leq 24$ whence $|G| \leq 24|N| \leq 96(g(X) + 1)$ as $N$ is abelian. Comparison with our hypothesis $|G| \geq 34(g(X) + 1)^{3/2}$ shows that $g(X) \leq 6$. For small we need a little more. If $|N|$ is prime then $|N| \leq 2g(X) + 1$; see [3 Theorem 11.108], and hence $|G| \leq 48(g(X) + 1)$ which is inconsistent with $|G| \geq 34(g(X) + 1)^{3/2}$. Otherwise, since $p = 3$ and $|N|$ has order a power of prime distinct from $p$, the bound $|N| \leq 4(g(X) + 1)$ with $g(X) \leq 6$ is only possible for $g(X)$, $|N| \in \{3, 16\}$.

Comparison of $|G| \leq 24|N|$ with $|G| \geq 34(g(X) + 1)^{3/2}$ rule out the latter three cases. Furthermore, since $N$ is an elementary abelian group of order 16, $g(X)$ must be odd by Lemma 2.2. Finally, $g(X) = 3, |N| = 16$, $G/N \cong \text{Sym}_4$ is impossible as Henn’s bound $|G| \geq 8g(X)^3$ implies that $X$ has zero $p$-rank, see [3 Theorem 11.127].

Therefore, the case $G = \bar{Q} \times \tilde{C}$ occurs. Also, $\tilde{G}$ fixes a unique place $\tilde{P} \in X$. Let $\Delta$ be the $N$-orbits in $X$ lying over $\tilde{P}$ in the cover $X|\mathcal{X}$. We prove that $\Delta$ is a long orbit of $N$. By absurd, the permutation
representation of $G$ on $\Delta$ has a nontrivial 1-point stabilizer containing a nontrivial subgroup $M$ of $N$. Since $N$ is abelian, $M$ is in the kernel. In particular, $M$ is a normal subgroup of $G$ contradicting our choice of $N$ to be minimal.

Take a Sylow $p$-subgroup $Q$ of $G$ of order $|Q| = p^h$ with $h \geq 1$, and look at the action of $Q$ on $\Delta$. Since $|\Delta| = |N|$ is prime to $p$, $Q$ fixes a point $P \in \Delta$, that is, $Q = Q_P$. Since $\mathcal{X}$ is an ordinary curve, $Q_P$ and hence $Q$ is elementary abelian; see [8, Theorem 2 (i)] or [3, Theorem 11.74 (iii)]. Therefore, $G_P = Q \rtimes U$ where $U$ is a prime to $p$ cyclic group. Thus

\begin{equation}
|\bar{Q}||C||N| = |\bar{G}||N| = |G| = |G_P||\Delta| = |Q||U||\Delta| = |Q||U||N|,
\end{equation}

whence $|Q| = |\bar{Q}|$ and $|U| = |\bar{C}|$. Consider the subgroup $H$ of $G$ generated by $G_P$ and $N$. Since $\Delta$ is a long $N$-orbit, $G_P \cap N = \{1\}$. As $N$ is normal in $H$ this implies that $H = N \rtimes G_P = N \rtimes (Q \rtimes U)$ and hence $|H| = |N||Q||U|$ which proves $G = H = N \rtimes (Q \rtimes U)$.

Since $\mathcal{X}$ is rational and $\bar{P}$ is the unique fixed point of nontrivial elements of $\bar{Q}$, each $\bar{Q}$-orbit other than $\{\bar{P}\}$ is long. Furthermore, $\bar{C}$ fixes a point $\bar{R}$ other than $\bar{P}$ and no nontrivial element of $\bar{C}$ is fixed point distinct from $\bar{P}$ and $\bar{R}$. This shows that the $G$-orbit $\Omega_1$ of $\bar{R}$ has length $|Q|$. In terms of the action of $G$ on $\mathcal{X}$, there exist as many as $|Q|$ orbits of $N$, say $\Delta_1, \ldots, \Delta_{|Q|}$, whose union $\Lambda$ is a short $G$-orbit lying over $\Omega_1$ in the cover $\mathcal{X}|\mathcal{X}$. Obviously, if at least one of $\Delta_i$ is a short $N$-orbit then so all are.

We show that this actually occur. Since the cover $\mathcal{X}|\mathcal{X}$ ramifies, $N$ has some short orbits, and by absurd there exists a short $N$-orbit $\Sigma$ not contained in $\Lambda$. Then $\Sigma$ and $\Lambda$ are disjoint. Let $\Gamma$ denote the (short) $G$-orbit containing $\Sigma$. Since $N$ is a normal subgroup of $G$, $\Gamma$ is partitioned into $N$-orbits, say $\Sigma = \Sigma_1, \ldots, \Sigma_k$, each of them of the same length $|\Sigma|$. Here $k = |Q||U|$ since the set of points of $\bar{X}$ lying under these $k$ short $N$-orbits is a long $G$-orbit. Also, $|N| = |\Sigma_i||N_{R_i}|$ for $i \leq k$ and $R_i \in \Sigma_i$. In particular, $|\Sigma_1| = |\Sigma|$ and $|N_{R_1}| = |B_{R_1}|$. From the Hurwitz genus formula,

\begin{equation}
2g(\mathcal{X}) - 2 \geq -2|N| + \sum_{i=1}^{k} |\Sigma_i|(|N_{R_i}| - 1) = -2|N| + |Q||U||\Sigma_1|(|N_{R_1}| - 1).
\end{equation}

Since $N_{R_i}$ is nontrivial, $|N_{R_i}| - 1 \geq \frac{1}{2}|N_{R_i}|$. Therefore,

\begin{equation}
2g(\mathcal{X}) - 2 \geq -2|N| + \frac{1}{2}|Q||U||\Sigma_1|(|N_{R_1}| - 1) = -2|N| + \frac{1}{2}|Q||U||N| = |N|\left(\frac{1}{2}|Q||U| - 2\right) = \frac{1}{2}|N||\bar{Q}||U| - 4).
\end{equation}

As $|Q||U| - 4 \geq \frac{1}{2}|Q||U|$ by $|Q||U| \geq 4$, this gives

\begin{equation}
2g(\mathcal{X}) - 2 \geq \frac{1}{4}|N||\bar{Q}||Q| = \frac{1}{4}|G|.
\end{equation}

But this contradicts our hypothesis $|G| > 34(g(\mathcal{X}) + 1)^{3/2}$.

Therefore, the short orbits of $N$ are exactly $\Delta_1, \ldots, \Delta_{|Q|}$. Take a point $S_i$ from $\Delta_i$ for $i = 1, \ldots, |Q|$. Then $N_{S_i}$ and $N_{S_i}$ are conjugate in $G$, and hence $|N_{S_i}| = |N_{S_i}|$. From the Hurwitz genus formula applied to $N$,

\begin{equation}
2g(\mathcal{X}) - 2 \geq -2|N| + \sum_{i=1}^{|Q|} |\Delta_i|(|N_{S_i}| - 1)) = -2|N| + |Q||\Delta_1|(|N_{S_1}| - 1) \geq -2|N| + \frac{1}{2}|Q||\Delta_1||N_{S_1}|.
\end{equation}

Since $|N| = |\Delta_1||N_{S_1}|$, this gives $2g(\mathcal{X}) - 2 \geq \frac{1}{2}|N||Q| - 4|Q|$ whence $2g(\mathcal{X}) - 2 \geq \frac{1}{4}|N||Q|$ provided that $|Q| \geq 5$. The missing case, $|Q| = 3$, cannot actually occur since in this case $|\bar{C}| = |U| \leq |Q| - 1 = 2$, whence $|Q| = |Q||U||N| \leq 6|N| \leq 24(g(\mathcal{X}) + 1)$, a contradiction with $|G| > 34(g(\mathcal{X}) + 1)^{3/2}$. Thus

\begin{equation}
|N||Q| \leq 8(g(\mathcal{X}) - 1).
\end{equation}

Since $|N||U| < |N||Q|$, this also shows

\begin{equation}
|N||U| < 8g(\mathcal{X}) - 1).
\end{equation}

Therefore,

\begin{equation}
|G||N| = |N|^2|U||Q| < 64(g(\mathcal{X}) - 1)^2.
\end{equation}
Equations (21) and (22) together with our hypothesis \(|G| > 34(g(X) + 1)^{3/2}\) yield

\[
|N| < \frac{64}{34} \sqrt{g(X) - 1}.
\]

From (23) and \(|G| = |N||Q||U| \geq 34(g(X) + 1)^{3/2}\) we obtain

\[
|Q||U| > \frac{34^2}{64}(g(X) - 1) > 18(g(X) - 1)
\]

which shows that Lemma 2.1 applies to the subgroup \(Q \times U\) of \(\text{Aut}(X)\). With the notation in Lemma 2.1, this gives that \(Q \times U\) and \(Q\) have the same two short orbits, \(\Omega_1 = \{P\}\) and \(\Omega_2\). In the cover \(X/\overline{X}\), the point \(\overline{P} \in \overline{X}\) lying under \(P\) is fixed by \(Q\). We prove that \(\Omega_2\) is a subset of the \(N\)-orbit \(\Delta\) containing \(P\). For this purpose, it suffices to show that for any point \(R \in \Omega_2\), the point \(\overline{R} \in \overline{X}\) lying under \(R\) in the cover \(X/\overline{X}\) coincides with \(\overline{P}\). Since \(\Omega_2\) is a \(Q\)-short orbit, the stabilizer \(Q_R\) is nontrivial, and hence \(Q\) fixes \(\overline{R}\). Since \(\overline{X}\) is rational, this yields \(\overline{P} = \overline{R}\). Therefore, \(\Omega_2 \cup \{P\}\) is contained in \(\Delta\), and either \(\Delta = \Omega_2 \cup \{P\}\) or \(\Delta\) contains a long \(Q\)-orbit. In the latter case, \(|U| < |Q| < |N|\), and hence

\[
|G| = |N||Q||U|/|Q||U| < |N||Q||U||U|/|N|^2 \leq \frac{64^2}{34}(g(X) - 1)^3
\]

whence \(|G| < 34(g(X) + 1)^{3/2}\), a contradiction with our hypothesis. Otherwise \(|N| = |\Delta| = 1 + |\Omega_2|\). In particular, \(|N|\) is even, and hence it is a power of 2. Also, from the Deuring-Shafarevič Formula, \(g(X) - 1 = \gamma(X) - 1 = -|Q| + 1 + |\Omega_2|\) where \(|\Omega_2| \geq 1\) is a power of \(p\). This implies that \(g(X)\) is also even. Since \(N\) is an elementary abelian 2-group, Lemma 2.2 yields that either \(|N| = 2\) or \(|N| = 4\).

If \(|N| = 2\) then \(\Omega_2\) consists of a unique point \(P\) and \(Q \times U\) fixes both points \(P\) and \(R\). Since \(\Delta = \{P, R\}\), and \(\Delta\) is a \(G\)-orbit, the stabilizer \(G_{P,R}\) is an index 2 (normal) subgroup of \(G\). On the other hand, \(G_{P,R} = Q \times U\) and hence \(Q\) is the unique Sylow \(p\)-subgroup of \(Q \times U\). Thus \(Q\) is a characteristic subgroup of the normal subgroup \(G_{P,R}\) of \(G\). But then \(Q\) is a normal subgroup of \(G\), a contradiction with our hypothesis.

If \(|N| = 4\) then \(|\Delta| = 4\) and \(p = 3\). The permutation representation of \(G\) of degree 4 on \(\Delta\) contains a 4-cycle induced by \(N\) but also a 3-cycle induced by \(Q\). Hence if \(K = \ker\) then \(G/K \cong \text{Sym}_4\). On the other hand, since both \(N\) and \(\ker\) are normal subgroups of \(G\), their product \(NK\) is normal, as well. Hence \(NK/K\) is a normal subgroup of \(G/K\), but this contradicts \(G/K \cong \text{Sym}_4\). \(\Box\)

References

[1] M. Giulietti and G. Korchmáros, Garden of curves with many automorphisms, in Algebraic curves and finite fields, 93–120, Radon Ser. Comput. Appl. Math., 16, De Gruyter, Berlin, 2014.
[2] G.B. Gunby, A. Smith and A. Yuan, Irreducible canonical representations in positive characteristic, Research in Number Theory (2015) 1:3, 1-25.
[3] J.W.P. Hirschfeld, G. Korchmáros, and F. Torres, Algebraic Curves over a Finite Field, Princeton Series in Applied Mathematics, Princeton (2008).
[4] H.W. Henn, Funktionenkörper mit großem Automorphismengruppe, J. Reine Angew. Math. 302 (1978), 96–115.
[5] A. Kontogeorgis and V. Rotger, On abelian automorphism groups of Mumford curves, Bull. London Math. Soc. 40 (2008), 353-362.
[6] R. Lidl and H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and its Applications 20, Cambridge Univ. Press, Cambridge, 1997, xiv+755 pp.
[7] A. Machì, Groups, An introduction to ideas and methods of the theory of groups, Unitext, 58, Springer, Milan, 2012. xiv+371 pp.
[8] S. Nakajima, \(p\)-ranks and automorphism groups of algebraic curves, Trans. Amer. Math. Soc. 303 (1987), 595-607.
[9] J.P. Serre, Corps locaux, Hermann, Paris, (1968).
[10] J.-P. Serre, Local Fields, Graduate Texts in Mathematics 67, Springer, New York, (1979). viii+241 pp.
[11] H. Stichtenoth, Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahl- charakteristik. II. Ein spezieller Typ von Funktionenkörpern, Arch. Math. 24 (1973), 615–631.
[12] F. Sullivan, \(p\)-torsion in the class group of curves with many automorphisms, Arch. Math. 26 (1975), 253–261.
[13] R.C. Valenti and M.L. Madan, A Hauptsatz of L.E. Dickson and Artin–Schreier extensions, J. Reine Angew. Math. 318 (1980), 156–177.
Authors’ addresses:
Gábor KORCHMÁROS and Maria MONTANUCCI
Dipartimento di Matematica, Informatica ed Economia
Università degli Studi della Basilicata
Contrada Macchia Romana
85100 Potenza (Italy).
E-mail: gabor.korchmaros@unibas.it and maria.montanucci@unibas.it