Journal of Algebra 427 (2015) 264–294

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Large 2-groups of automorphisms of algebraic curves over a field of characteristic 2 ☆

Massimo Giulietti [a,*], Gábor Korchmáros [b]

[a] *Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Via Vanvitelli, 1-06123 Perugia, Italy*
[b] *Dipartimento di Matematica, Università della Basilicata, Contrada Macchia Romana, 85100 Potenza, Italy*

ARTICLE INFO

Article history:
Received 1 May 2014
Available online xxxx
Communicated by Michel Broué

MSC:
14H37

Keywords:
Algebraic curves
Positive characteristic
Automorphism groups

ABSTRACT

Let S be a 2-subgroup of the $\mathbb{K}$-automorphism group $\mathrm{Aut}(\mathcal{X})$ of an algebraic curve $\mathcal{X}$ of genus $\mathfrak{g}(\mathcal{X})$ defined over an algebraically closed field $\mathbb{K}$ of characteristic 2. It is known that S may be quite large compared to the classical Hurwitz bound $84(\mathfrak{g}(\mathcal{X})-1)$. However, if S fixes no point, then the size of S is smaller than or equal to $4(\mathfrak{g}(\mathcal{X})-1)$. In this paper, we investigate algebraic curves $\mathcal{X}$ with a 2-subgroup S of $\mathrm{Aut}(\mathcal{X})$ having the following properties:

(I) $|S| \geq 8$ and $|S| > 2(\mathfrak{g}(\mathcal{X})-1)$,
(II) S fixes no point on $\mathcal{X}$.

Theorem 1.2 shows that $\mathcal{X}$ is a general curve and that either $|S| = 4(\mathfrak{g}(\mathcal{X})-1)$, or $|S| = 2\mathfrak{g}(\mathcal{X})+2$, or, for every involution $u \in Z(S)$, the quotient curve $\mathcal{X}/\langle u\rangle$ inherits the above properties, that is, it has genus ≥ 2, and its automorphism group $S/\langle u\rangle$ still has properties (I) and (II). In the first two cases, S is completely determined. We also give examples illustrating our results. In particular, for every $\mathfrak{g} = 2^h+1 \geq 9$, we exhibit a (general bielliptic) curve $\mathcal{X}$ of genus $\mathfrak{g}$ whose

☆ Research supported by the Italian Ministry MIUR, PRIN project 2012XZE22K Strutture Geometriche, Combinatoria e loro Applicazioni, and by INdAM.
* Corresponding author.
E-mail addresses: giuliet@dmi.unipg.it (M. Giulietti), gabor.korchmaros@unibas.it (G. Korchmáros).

http://dx.doi.org/10.1016/j.jalgebra.2014.12.019

$\mathbb{K}$-automorphism group has a dihedral 2-subgroup S of order $4(\mathfrak{g}-1)$ that fixes no point in $\mathcal{X}$.

1. Introduction

In the present paper, $\mathbb{K}$ is an algebraically closed field of characteristic 2, $\mathcal{X}$ is a (projective, non-singular, geometrically irreducible, algebraic) curve of genus $\mathfrak{g} \geq 2$, $\mathrm{Aut}(\mathcal{X})$ is the $\mathbb{K}$-automorphism group of $\mathcal{X}$, and S is a (non-trivial) subgroup of $\mathrm{Aut}(\mathcal{X})$ whose order is a power of 2.

From previous work of Nakajima [13], the size of S is related to the 2-rank γ of $\mathcal{X}$ which is defined to be the rank of the (elementary abelian) group of the 2-torsion points in the Jacobian variety of $\mathcal{X}$; see [8, Section 6.7]. It is known that $\gamma \leq \mathfrak{g}$. If equality holds then $\mathcal{X}$ is a *general* curve, see [8, Theorem 6.96] and [3]. Nakajima [13, Theorem 1] showed that $|S| \leq 4(\gamma-1)$ for $\gamma > 1$, whereas $|S| \leq 4(\mathfrak{g}-1)$ for $\gamma = 1$. Moreover, [7, Theorem 3.4] states that if $\gamma = 0$, then S has a unique fixed point on $\mathcal{X}$, see also [8, Theorem 11.333]. In the latter case, $|S| \leq 8\mathfrak{g}^2$ by an earlier result of Stichtenoth [17] who also pointed out that this bound is attained by the non-singular model $\mathcal{X}$ of the hyperelliptic curve of genus 2^{k-1} and equation $Y^2 + Y + X^{2^k+1} = 0$.

The above results have given a motivation to investigate the possibilities for $\mathcal{X}$, $\mathfrak{g}$ and S when either $|S|$ is close to $8\mathfrak{g}^2$ (and S fixes a point of $\mathcal{X}$), or $|S|$ is close to $4(\mathfrak{g}-1)$ but S fixes no point of $\mathcal{X}$.

The first possibilities have recently been investigated by Lehr, Matignon and Rocher, see [11,12,15,16]. In [11], it is shown that $|S| \geq 4\mathfrak{g}^2$ only occurs when $\mathcal{X}$ is the non-singular model of the Artin–Schreier curve of equation $Y^q + Y + f(X) = 0$ with $f(X) = XP(X) + cX$ where $P(X)$ is an additive polynomial of $\mathbb{K}[X]$ and q is a power of 2.

To investigate the second possibility the hypotheses below are assumed:

(I) $|S| \geq 8$ and $|S| > 2(\mathfrak{g}-1)$,
(II) S fixes no point on $\mathcal{X}$.

Before stating our results on S we point out the prominent role of central involutions in this context. Let u be a central involution in S, that is an involution $u \in Z(S)$, and consider the associated quotient curve $\bar{\mathcal{X}} = \mathcal{X}/U$ where $U = \langle u \rangle$. The factor group $\bar{S} = S/U$ has order $\frac{1}{2}|S|$ and it is a $\mathbb{K}$-automorphism group of $\bar{\mathcal{X}}$. Also, $\mathfrak{g} - 1 \geq 2(\bar{\mathfrak{g}} - 1)$ where $\bar{\mathfrak{g}}$ is the genus of $\bar{\mathcal{X}}$. Therefore, either

(A) $\bar{\mathfrak{g}} \leq 1$; or
(B) $\bar{\mathfrak{g}} = 2$ and $|\bar{S}| = 4$; or
(C) $\bar{\mathfrak{g}} \geq 2$, and hypothesis (I) is inherited by $\bar{S}$, viewed as a subgroup of $\mathrm{Aut}(\bar{\mathcal{X}})$, but $\bar{S}$ fixes a point on $\bar{\mathcal{X}}$; or

(D) $\bar{\mathfrak{g}} \geq 2$ and both hypotheses (I) and (II) are inherited by $\bar{S}$, viewed as a subgroup of $\mathrm{Aut}(\bar{\mathcal{X}})$.

If case (D) occurs then u is called an *inductive* central involution of S. Note that, if $|S| \geq 16$ and no non-trivial element in S fixes a point of $\mathcal{X}$ then every central involution is inductive. It may happen that $\bar{S}$ also has an inductive central involution, say $\bar{u}$. In this case the quotient curve $\bar{\bar{\mathcal{X}}} = \bar{\mathcal{X}}/\langle \bar{u} \rangle$ with its inherited $\mathbb{K}$-automorphism group $\bar{\bar{S}} = \bar{S}/\langle \bar{u} \rangle$ satisfies both (I) and (II), as well. Therefore, an inductive argument can be used to go on as far as the resulting curve has an inductive central involution. Since the order of the inherited group halves at each step, after a finite number of steps a curve free from inductive central involutions is obtained. Such a finite sequence of curves is called an *inductive sequence*. It may be noted that an inductive sequence gives rise to an upper central series and that its length is at most $h - 3$, where $|S| = 2^h$. Actually, this bound can be attained, see the examples in Subsection 6.5 that also illustrate some features of inductive sequences of curves.

Now, our results are stated.

Theorem 1.1. *Let $\mathcal{X}$ be a curve of genus $\mathfrak{g} \geq 2$ defined over an algebraically closed field $\mathbb{K}$ of characteristic 2. Let γ be the 2-rank of $\mathcal{X}$. Assume that $\mathrm{Aut}(\mathcal{X})$ has a subgroup S of order a power of 2 such that both (I) and (II) hold. If S contains no inductive central involution then $\mathfrak{g} = \gamma$, and one of the following two cases occurs.*

(1) *$|S| = 4(\mathfrak{g} - 1)$, $\mathcal{X}$ is a bielliptic curve, and S is a dihedral group.*
(2) *$|S| = 2\mathfrak{g} + 2$, and $S = D \rtimes E$, the semidirect product of an elementary abelian group D of index 2 by a group E of order 2. If S is abelian, then it is an elementary abelian group and $\mathcal{X}$ is a hyperelliptic curve.*

Theorem 1.1 is a corollary of the following result proven in Section 4.

Theorem 1.2. *Let $\mathcal{X}$ be a curve of genus $\mathfrak{g} \geq 2$ defined over an algebraically closed field $\mathbb{K}$ of characteristic 2. Let γ be the 2-rank of $\mathcal{X}$. Assume that $\mathrm{Aut}(\mathcal{X})$ has a subgroup S of order a power of 2 such that both (I) and (II) hold. Then one of the following cases occurs:*

(i) *$|S| = 4(\mathfrak{g} - 1)$, $\gamma = \mathfrak{g}$ and $\mathcal{X}$ is a bielliptic curve. Furthermore, either*
  (ia) *S is dihedral and has no inductive central involution; or*
  (ib) *$S = (E \times \langle u \rangle) \rtimes \langle w \rangle$ where E is a cyclic group of order $\mathfrak{g} - 1$ and u and w are involutions. The factor group $S/\langle u \rangle$ is a dihedral group, and the two involutions of $E \times \langle u \rangle$ are the unique two central inductive involutions of S.*
(ii) *$\gamma = \mathfrak{g}$, and (2) in Theorem 1.1 holds.*
(iii) *Every central involution of S is inductive.*

It is worth observing that all curves in Theorem 1.1 are general curves. In fact, automorphism groups of general curves have specific properties. In particular, in characteristic 2, every 2-element fixing a point is an involution, see corollary to Theorem 2 in [13]. For non-general curves with $\gamma \geq 2$, Nakajima's bound $|S| \leq 4(\gamma - 1)$ is better than $|S| < 4(\mathfrak{g} - 1)$. For $\gamma = 1$, Nakajima's bound can be improved to $|S| \leq \mathfrak{g} - 1$, provided that $|S| \geq 8$ and S is neither dihedral nor semi-dihedral, see the remark after Lemma 3.1. For $\gamma = 0$, as noted before, S must fix a point, and hence condition (II) is not satisfied.

In the literature, there has been known, so far, only one infinite family of curves related to Theorem 1.1, namely the family described in Section 6.3 which provides an example of type (2). The existence problem for an infinite family of curves of type (1) in Theorem 1.1 is solved positively in Section 5. In fact, for every $\mathfrak{g} = 2^h + 1 \geq 9$, we construct a general bielliptic curve $\mathcal{X}$ whose $\mathbb{K}$-automorphism group has a dihedral 2-subgroup S of order $4(\mathfrak{g} - 1)$ that fixes no point in $\mathcal{X}$. For this purpose, cyclic extensions of elliptic curves over a finite field are considered. The idea is to show that some of such extensions have a dihedral automorphism group attaining Nakajima's bound. This requires explicit computations in elliptic function fields with finite constant field, which appear to be of independent interest. Our construction of such curves also suggests the existence of curves of genus $\mathfrak{g}$ with a semi-dihedral $\mathbb{K}$-automorphism group of order $2(\mathfrak{g} - 1)$. An example with $\mathfrak{g} = 17$, $\gamma = 9$ and $|S| = 32$ is exhibited in Subsection 6.6. This shows that if the first hypothesis in (I) is relaxed to $|S| \geq 2\mathfrak{g} - 2$, then more groups and non-general curves enter in play when an analog of Theorem 1.1 is considered. Finally, an infinite family of curves of type (iii) in Theorem 1.2 is given in Subsection 6.4.

Our proof of Theorem 1.2 combines function fields with permutation groups. The ingredients from function field theory are the Deuring–Shafarevich, the Hurwitz genus and the Hilbert differential formulaes. The basic idea is to interpret the Deuring–Shafarevich formula as a combinatorial result regarding the orbits of S and then use it as an extra-tool in the study of the action of S on $\mathcal{X}$. With this approach, the other two formulaes also play a role in the arguments, although of minor importance. The first essential step in the proof is to prove that S has only two short orbits on $\mathcal{X}$, one of length $\ell_1 = \frac{1}{2}|S|$ the other of size $\ell_2 = \frac{1}{2}|S| - \gamma + 1$. This shows that γ heavily influences not only the size of S but also its action on $\mathcal{X}$. The second step is to prove that if $|\ell_2| = 2$ then case (ii) occurs; in particular, when S is abelian, then $\mathcal{X}$ is a hyperelliptic curve and S is an elementary abelian group. For $|\ell_2| > 2$, the picture appears to be much richer, see the examples in Section 6. However, if S has a non-inductive central involution, then $|\ell_2| = \frac{1}{4}|S|$ and $\mathcal{X}$ is a general bielliptic curve. In the final step we determine the abstract structure of S. Our arguments only require the existence of a central involution in S fixing a point of $\mathcal{X}$ that may be or not a non-inductive central involution. The result is stated in Theorem 4.3, and the proof relies on Suzuki's classification of 2-groups containing an involution whose centralizer has order 4.

One may ask whether analogous results for p-groups of automorphisms S may hold in characteristic $p > 2$. The answer is negative for $p > 3$. In fact, if $p > 2$ then $|S| \leq \frac{p}{p-2}(\gamma - 1)$ for $\gamma \geq 2$ and $|S| \leq \mathfrak{g} - 1$ for $\gamma = 1$, see [13], while $|S| \leq \frac{4p}{(p-1)^2} g^2$ for $\gamma = 0$

(and S fixes a point), see [17]. Comparing these results with conditions (I) and (II) shows indeed that only the case $p = 3$ is possible. Therefore, let $p = 3$ and assume that $\mathcal{X}$ is a genus $\mathfrak{g} \geq 2$ curve equipped with a 3-subgroup S of $\mathrm{Aut}(\mathcal{X})$ satisfying both conditions (I) and (II). Our approach and arguments can be adapted to prove that $\mathcal{X}$ is a general curve with $|S| = 3(\mathfrak{g} - 1)$, and that S is abelian only for $\mathfrak{g} = 4$. However, there is major difference with respect to the case $p = 2$, since the action of S on $\mathcal{X}$ has two orbits of equal length $|S|/3$, and some index 3 subgroup M of S acts on $\mathcal{X}$ semi-regularly so that the quotient curve $\bar{\mathcal{X}}/M$ is a genus 2 curve with a subgroup of $\mathrm{Aut}(\bar{\mathcal{X}})$ of order 3. The latter property means that the field extension $\mathbb{K}(\mathcal{X})/\mathbb{K}(\bar{\mathcal{X}})$ is unramified. Therefore, to pursuit the investigation, the pro-p fundamental group of $\bar{\mathcal{X}}$ is useful, see [14], and different tools from Group theory, such as the classification of 3-groups of maximal nilpotency class, are needed. This has been done in a separate work, a preliminary version being [5].

2. Preliminaries to the proof of Theorem 1.2

In this section, S is a 2-subgroup of $\mathrm{Aut}(\mathcal{X})$, that is, a $\mathbb{K}$-automorphism group of $\mathcal{X}$ whose order is a power of 2.

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

Let $\bar{P}_1, \ldots, \bar{P}_k$ be the points of the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/S$ where the cover $\mathcal{X}/\bar{\mathcal{X}}$ ramifies. For $1 \leq i \leq k$, let L_i denote the set of points of $\mathcal{X}$ which lie over $\bar{P}_i$. In other words, $L_1, \ldots, L_k$ are the short orbits of S on its faithful action on $\mathcal{X}$. Here the orbit of $P \in \mathcal{X}$

$$o(P) = \{Q \mid Q = P^g, g \in S\}$$

is *long* if $|o(P)| = |S|$, otherwise $o(P)$ is *short*. It may be that S has no short orbits. This is the case if and only if every non-trivial element in S is fixed-point-free on $\mathcal{X}$. On the other side, S has a finite number of short orbits.

If P is a point of $\mathcal{X}$, the stabilizer S_P of P in S is the subgroup of S consisting of all elements fixing P. For a non-negative integer i, the i-th ramification group of $\mathcal{X}$ at P is denoted by $S_P^{(i)}$ (or $S_i(P)$ as in [18, Chapter IV]) and defined to be

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

where t is a uniformizing element (local parameter) at P. Here $S_P^{(0)} = S_P^{(1)} = S_P$. Furthermore, for $i \geq 1$, $S_P^{(i)}$ is a normal subgroup of S_P and the factor group $S_P^{(i)}/S_P^{(i+1)}$ is an elementary abelian p-group. For i big enough, $S_P^{(i)}$ is trivial.

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

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

where

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

Let γ be the 2-rank of $\mathcal{X}$, and let $\bar{\gamma}$ be the 2-rank of the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/S$. The Deuring–Shafarevich formulas, see [20] or [8, Theorem 11.62], states that

$$\gamma - 1 = |S|(\bar{\gamma} - 1) + \sum_{i=1}^{k} \left(|S| - \ell_i \right) \tag{3}$$

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

Besides the Hurwitz and the Deuring–Shafarevich formulas which are our main tools from Algebraic geometry, we also need some technical results.

Proposition 2.1. *Assume that S fixes the point $P \in \mathcal{X}$. Let $i \geq 2$ be the smallest integer for which the ith ramification group $S_P^{(i)}$ of S at P is trivial. If S has order 2, then i is even.*

Proof. Since S has order two, $\mathcal{X}$ is a double cover of the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/S$. Hence, $\mathbb{K}(\mathcal{X})$ is an Artin–Schreier extension of $\mathbb{K}(\mathcal{X})^S = \mathbb{K}(\bar{\mathcal{X}})$. By (c) of Lemma 3.7.8 in [19], the different exponent d_P is even. Then the claim follows from (2). □

Proposition 2.2. *If $\gamma = 0$, then S has a (unique) fixed point.*

For a proof, see [6]; see also [8, Section 11.15] and [7].

Proposition 2.3 *(Nakajima's bound). If $\gamma = 1$, then $|S| \leq 4(\mathfrak{g} - 1)$ and if $\gamma \geq 2$ then $|S| \leq 4(\gamma - 1)$.*

For a proof, see [13]; see also [8, Theorem 11.84].

Our main tool from Group theory is Suzuki's characterization of dihedral and semi-dihedral 2-groups, see [21, Lemma 4]. We stress that the dihedral group $\mathbf{D}_n$ of order $2n = 2^{m+1}$ with $m \geq 3$, as well as the semi-dihedral group $\mathbf{SD}_n$ group of the same order, are generated by an element g of order 2^m together with an involution h. But the relation linking g and h is $hgh = g^{-1}$ in $\mathbf{D}_n$, while it is $hgh = g^{2^{m-1}-1}$ in $\mathbf{SD}_n$. Another difference between $\mathbf{D}_n$ and $\mathbf{DS}_n$ is that $\mathbf{D}_n$ contains exactly $n + 1$ involutions, namely $g^{2^{m-1}}$ and all $g^i h$, while $\mathbf{SD}_n$ does only $2^{m-1} + 1$, namely $g^{2^{m-1}}$ and $g^i h$ with even i.

Proposition 2.4 *(Suzuki's classification). A 2-group H which contains an involution whose centralizer has order 4 is either dihedral, or semi-dihedral, or it has order 4.*

We also need a few technical lemmas on finite 2-groups.

Lemma 2.5. *(See [9, Satz 14.9].) Up to isomorphisms, there exist exactly four non-abelian groups H of order $2^{m+1} \geq 16$ containing a cyclic subgroup of index 2, namely the dihedral group, the semi-dihedral group, the generalized quaternion group, and the group generated by an element g of order 2^{m-1} together with an involution h such that $hgh = g^{1+2^{m-2}}$. The number of involutions of H is equal to $2^m + 1, 2^{m-1} + 1, 1, 3$ respectively.*

Lemma 2.6. *Let H be a transitive permutation group on a set Δ whose 1-point stabilizer of H has order two. Let Δ_w be the set of all fixed points of an involution w of H. Then $|C_H(w)| = 2|\Delta_w|$.*

Proof. It is enough to observe that $g \in H$ leaves Δ_w invariant if and only $g \in C_H(w)$. □

Lemma 2.7. *Let u be a central involution of a 2-group H of order at least 16. Assume that $\bar{H} = H/\langle u \rangle$ is a dihedral group. Let $\bar{C}$ be a maximal cyclic subgroup of $\bar{H}$. Then the counter-image C of $\bar{C}$ under the natural epimorphism $\tau : H \to \bar{H}$ is either a cyclic subgroup of H, or it is a direct product $E \times \langle u \rangle$ with a cyclic subgroup E.*

Proof. Take an element $c \in H$ such that $\bar{c} = \tau(c)$ is a generator of $\bar{C}$. Then, either $\langle c \rangle = C$ and C is cyclic, or $E = \langle c \rangle$ is a cyclic subgroup of C of index 2. In the latter case, $u \notin E$ and hence $C = E \times \langle u \rangle$. □

Lemma 2.8. *(See [9, Satz 14.10].) Up to isomorphisms, there are five groups of order 8. Two of them are non-abelian, namely the dihedral and the quaternion groups.*

3. Central involutions in $\mathbf{Aut}(\mathcal{X})$

We begin with a number of results valid for curves $\mathcal{X}$ of genus $\mathfrak{g} \geq 2$ which satisfy both hypotheses (I) and (II).

Lemma 3.1. *The 2-rank γ of $\mathcal{X}$ is at least 2.*

Proof. From Proposition 2.2, $\gamma \geq 1$. To prove the assertion by absurd, assume that $\gamma = 1$.

Assume first that there is an involution $u \in Z(S)$ that fixes a point on $\mathcal{X}$. From (3) applied to $U = \langle u \rangle$, the 2-rank of the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/U$ is equal to 0, and u fixes precisely two points on $\mathcal{X}$, say P_1 and P_2. As $u \in Z(S)$, the set $\{P_1, P_2\}$ is preserved by S. Therefore, the stabilizer S_{P_1} of P_1 in S has index two in S, and it fixes P_2 as well. Let $\bar{P}_1$ and $\bar{P}_2$ be the points of $\bar{\mathcal{X}}$ lying under P_1 and P_2, respectively. Obviously, $\bar{P}_1 \neq \bar{P}_2$. Furthermore, the factor group S_{P_1}/U is a subgroup of $\mathrm{Aut}(\bar{\mathcal{X}})$, and it fixes both $\bar{P}_1$ and $\bar{P}_2$. Since $\bar{\mathcal{X}}$ has zero 2-rank, Proposition 2.2 implies that S_{P_1}/U is trivial. Therefore, $S_{P_1} = U$ and hence $|S| = 4$; a contradiction with (I).

Thus, we may assume by (I), together with (1), that some non-central involution v in S has a fixed point on $\mathcal{X}$. The above argument applied to $C_S(v)$ shows that $|C_S(v)| = 4$. By Proposition 2.4, then S contains a cyclic group S_1 of index 2. From (I), the unique involution u in S_1 fixes a point on $\mathcal{X}$. On the other hand, $u \in Z(S)$. As we have seen before, this is impossible. □

The proof of Lemma 3.1 also shows that if $\gamma = 1$ and $|S| > \mathfrak{g} - 1$, with $|S| \geq 8$, then S is either dihedral or semi-dihedral.

Lemma 3.2. *S has exactly two short orbits on $\mathcal{X}$, the larger one of size $\ell_1 = \frac{1}{2}|S|$ and the shorter one of size $2 \leq \ell_2 \leq \frac{1}{4}|S|$.*

Proof. Let $\bar{\gamma}$ be the 2-rank of the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/S$. From (3),

$$\gamma - 1 = \bar{\gamma}|S| - |S| + \sum_{i=1}^{k}\big(|S| - \ell_i\big) = (\bar{\gamma} + k - 1)|S| - \sum_{i=1}^{k}\ell_i \geq \left(\bar{\gamma} + \frac{k}{2} - 1\right)|S|,$$

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

If no such short orbits exist, then $\gamma - 1 = |S|(\bar{\gamma} - 1)$ holds, whence $\bar{\gamma} > 1$ follows by $\gamma \geq 2$. For $\bar{\gamma} > 1$, this equation yields that $|S| \leq (\gamma - 1) \leq (\mathfrak{g} - 1)$ contradicting (I).

Therefore, $k \geq 1$, and if $\bar{\gamma} \geq 1$ then the above equation implies that $|S| \leq 2(\gamma - 1) \leq 2(\mathfrak{g} - 1)$, a contradiction with (I).

So, $\bar{\gamma} = 0$ and $1 \leq k \leq 2$. Actually, k must be 2, $\gamma \geq 2$ being inconsistent with $k = 1$ and $\bar{\gamma} = 0$ in the above equation.

Therefore, S has precisely two short orbits say Ω_1 and Ω_2, and

$$\gamma - 1 = |S| - (\ell_1 + \ell_2)$$

with $|\Omega_1| = \ell_1$ and $|\Omega_2| = \ell_2$.

Assume without loss of generality that $\ell_1 \geq \ell_2$. Obviously, $\ell_2 < \frac{1}{2}|S|$, as otherwise we would have $\gamma = 1$ contradicting Lemma 3.1. Also, $\ell_1 > \frac{1}{4}|S|$, since $\gamma - 1 \geq |S|(1 - \frac{1}{4} - \frac{1}{4})$ is inconsistent with (I). Then,

$$\ell_1 = \frac{1}{2}|S|, \tag{4}$$

and

$$\gamma - 1 = \frac{1}{2}|S| - \ell_2, \tag{5}$$

with $\ell_2 \leq \frac{1}{4}|S|$. □

We keep up the notation introduced in the preceding proof. So, Ω_1 and Ω_2 stand for the two short orbits of S on $\mathcal{X}$. Here $\ell_1 = |\Omega_1| = \frac{1}{2}|S|$ while $2 \le \ell_2 = |\Omega_2| \le \frac{1}{4}|S|$. To investigate the smallest case $\ell_2 = 2$ some technical lemmas are needed.

Lemma 3.3. *If $P \in \Omega_1$ then $|S_P| = 2$. If $Q \in \Omega_2$ then*

$$2\mathfrak{g} - 2 \ge |S| + \ell_2\left(\left|S_Q^{(2)}\right| + \left|S_Q^{(3)}\right| - 4 + \sum_{i\ge 4}\left|S_Q^{(i)}\right| - 1\right), \tag{6}$$

and equality holds if and only if the genus of the quotient curve $\mathcal{X}/S$ is equal to zero.

Proof. The first assertion clearly follows from $\ell_1 = \frac{1}{2}|S|$. Let $\bar{\mathfrak{g}}$ be the genus of the quotient curve $\mathcal{X}/S$. From (1) applied to S,

$$\begin{aligned} 2\mathfrak{g} - 2 = (2\bar{\mathfrak{g}} - 2)|S| + \frac{1}{2}|S|\big(2\big(|S_P| - 1\big) + \big|S_P^{(2)}\big| - 1 + \ldots\big) \\ + \ell_2\big(2\big(|S_Q| - 1\big) + \big|S_Q^{(2)}\big| - 1 + \ldots\big). \end{aligned}$$

This together with $|S_P| = 2$ give

$$2\mathfrak{g} - 2 = (2\bar{\mathfrak{g}} + 1)|S| + \frac{1}{2}|S|\big(\big|S_P^{(2)}\big| - 1 + \big|S_P^{(3)}\big| - 1 + \ldots\big) + \ell_2\big(-2 + \big|S_Q^{(2)}\big| - 1 + \ldots\big).$$

If $|S_P^{(2)}| = 2$, then by Proposition 2.1 $|S_P^{(3)}| = 2$, which contraditcs (I).

Therefore, $|S_P^{(2)}| = 1$ and hence (6) holds. □

Lemma 3.4. *If u is a central involution of S which fixes a point of Ω_2, then u fixes Ω_2 pointwise but fixes no point outside Ω_2.*

Proof. Since Ω_2 is an orbit of S and $u \in Z(S)$, u fixes Ω_2 pointwise. Assume on the contrary that u also fixes a point on Ω_1. Then u must fix Ω_1 pointwise. From (3) applied to $U = \langle u \rangle$,

$$\gamma - 1 = 2\big(\gamma' - 1\big) + \frac{1}{2}|S| + \ell_2,$$

where γ' stands for the 2-rank of the quotient curve $\mathcal{X}' = \mathcal{X}/U$. Since $\ell_2 \ge 2$, this yields that $\mathfrak{g} - 1 \ge \gamma - 1 \ge \frac{1}{2}|S|$ contradicting (I). □

Lemma 3.5. *If a central involution u of S fixes a point of Ω_1 then u fixes Ω_1 pointwise, $\ell_2 = 2$ and $\mathcal{X}$ is a hyperelliptic curve.*

Proof. From Lemma 3.4, S fixes no point outside Ω_1. The argument in the proof of that lemma applied to Ω_1 proves the first assertion and gives the equation

$$\gamma - 1 = 2(\gamma' - 1) + \frac{1}{2}|S|,$$

where γ' stands for the 2-rank of the quotient curve $\mathcal{X}' = \mathcal{X}/U$, with $U = \langle u \rangle$. This and (5) imply that $\gamma' = 0$ and $\ell_2 = 2$. In particular, $\mathcal{X}$ is a hyperelliptic curve. □

Lemma 3.6. *If $\ell_2 > 2$ then every non-inductive central involution of S fixes a point on $\mathcal{X}$.*

Proof. Let u be a non-inductive central involution of S and assume on the contrary that u fixes no point on $\mathcal{X}$. From (1) applied to $U = \langle u \rangle$,

$$2\mathfrak{g} - 2 = 2(2\bar{\mathfrak{g}} - 2),$$

where $\bar{\mathfrak{g}}$ is the genus of the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/U$. Therefore, $\bar{\mathfrak{g}} \geq 2$ and

$$|\bar{S}| = \frac{1}{2}|S| > \mathfrak{g} - 1 = 2(\bar{\mathfrak{g}} - 1).$$

Furthermore, $\ell_2 > 2$ yields that $|S| \geq 16$, whence $|\bar{S}| \geq 8$. Since u is non-inductive, $\bar{S}$ must have a fixed point on $\bar{\mathcal{X}}$. If $\bar{R} \in \bar{\mathcal{X}}$ is such a point, and $R_1, R_2 \in \mathcal{X}$ are the points lying over $\bar{R}$, then S leaves the pair $\{R_1, R_2\}$ invariant. Hence, Ω_2 consists of the points R_1 and R_2. But then $\ell_2 = 2$, a contradiction. □

Lemma 3.7. *If S has a non-inductive central involution then either $\ell_2 = 2$, or $\ell_2 = \frac{1}{4}|S| \geq 4$. In the latter case, $\mathcal{X}$ is a general, bielliptic curve with $|S| = 4(\mathfrak{g} - 1)$.*

Proof. Suppose that $\ell_2 > 2$ and take a non-inductive central involution u of S. By Lemmas 3.6, 3.4 and 3.5, the set of fixed points of u is Ω_2. From (3) applied to $U = \langle u \rangle$,

$$\gamma - 1 = 2(\bar{\gamma} - 1) + \ell_2, \tag{7}$$

where $\bar{\gamma}$ is the 2-rank of the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/U$. Comparing this with (5) shows that $\bar{\gamma} = 0$ is inconsistent with $\ell_2 \leq \frac{1}{4}|S|$. So, the case $\bar{\gamma} = 0$ does not actually occur.

If $\bar{\gamma} = 1$ then (7) and (5) give $\ell_2 = \frac{1}{4}|S|$. In this case, $\bar{\mathfrak{g}} \geq \bar{\gamma} = 1$. From (1) applied to $U = \langle u \rangle$,

$$2\mathfrak{g} - 2 = 2(2\bar{\mathfrak{g}} - 2) + \frac{1}{4}|S|d_P$$

where P is any point in Ω_2. From Proposition 2.1, either $d_P = 2$ or $d_P \geq 4$. The latter cannot actually occur by (I). Since the central involution u is non-inductive, one of the cases (A), (B) and (C) in Introduction occurs. Since $\frac{1}{4}|S| \geq 4$, that is, $|\bar{S}| = \frac{1}{2}|S| \geq 8$, case (B) is ruled out. If case (C) occurred then S would have an orbit of length 2, contradicting the hypothesis $\ell_2 > 2$. Therefore, case (A) holds. As $\bar{\mathfrak{g}} \geq \bar{\gamma} = 1$, we have that $\bar{\mathfrak{g}} = 1$. This implies that $|S| = 4(\mathfrak{g} - 1) = 4(\gamma - 1)$ and hence $\mathcal{X}$ is a general curve. Therefore, $\mathcal{X}$ is bielliptic as u is an involution and $\mathcal{X}/U$ is an elliptic curve.

Let $\bar{\gamma} \geq 2$. This time, (7) and (5) give

$$\ell_2 = \frac{1}{4}|S| - (\bar{\gamma} - 1). \tag{8}$$

From this, $|S| \geq 16$ and hence $|\bar{S}| \geq 8$. Also, $|\bar{S}| = \frac{1}{2}|S| > \mathfrak{g} - 1 > 2(\bar{\mathfrak{g}} - 1)$. Since u is a non-inductive central involution, $\bar{S}$ has a fixed point on $\bar{\mathcal{X}}$. But this implies that $\ell_2 = 2$ as in the final part of the proof of Lemma 3.6. □

4. Proof of Theorem 1.2

We prove two theorems. They together with Lemmas 3.6 and 3.7 provide a proof of Theorem 1.2.

Theorem 4.1. *Let $\mathcal{X}$ be a curve of genus $\mathfrak{g} \geq 2$ defined over an algebraically closed field $\mathbb{K}$ of characteristic 2. Assume that $\mathrm{Aut}(\mathcal{X})$ has a subgroup S of order a power of 2 satisfying both hypotheses* (I) *and* (II). *If $\ell_2 = 2$ then case* (ii) *of Theorem 1.2 holds.*

Proof. Hypothesis (I) together with (5) yield

$$|S| > 2(\mathfrak{g} - 1) \geq 2(\gamma - 1) = |S| - 4.$$

Since $|S|$ is a power of 2 bigger than four, two possibilities arise only. Either

(a) $|S| = 2\mathfrak{g}$ and $\mathfrak{g} = \gamma + 1$, or
(b) $|S| = 2\mathfrak{g} + 2$ and $\mathfrak{g} = \gamma$.

In both case, from (1) applied to S we deduce that the genus of the quotient curve $\mathcal{X}/S$ is equal to 0.

To rule out case (a), suppose on the contrary that $\mathfrak{g} = \frac{1}{2}|S|$. Lemma 3.3 for $\mathfrak{g} = \frac{1}{2}|S|$ implies that $|S_Q^{(2)}| = 2$ but $|S_Q^{(3)}| = 1$, which contradicts Proposition 2.1.

In case (b), Lemma 3.3 implies that the second ramification group $S_R^{(2)}$ is trivial at every $R \in \Omega_1 \cup \Omega_2$ and hence at every point in $\mathcal{X}$. Also, since $\ell_2 = 2$, the stabilizer D of $Q \in \Omega_2$ in S is an elementary abelian group D of order $\frac{1}{2}|S|$. From (3) applied to D,

$$\gamma - 1 = |D|(\tilde{\gamma} - 1) + |D| - 2 + \sum_{i=1}^{k} \big(|D| - l_i\big)$$

where $l_1, \ldots, l_k$ are sizes of the short orbits $\Lambda_1, \ldots, \Lambda_k$ of D disjoint from Ω_2. This together with (5) yield that either $\bar{\gamma} = 0$, $k = 2$ and $l_1 = l_2 = \frac{1}{2}|D|$, or no non-trivial element of D fixes a point of $\mathcal{X}$ outside Ω_2.

We show that the former case cannot actually occur. The factor group $\bar{S} = S/D$ is a $\mathbb{K}$-automorphism group of the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/D$. Set $\Omega_2 = \{P_1, P_2\}$. Let $\bar{P}_1$ and

$\bar{P}_2$ be the points of $\bar{\mathcal{X}}$ lying under P_1 and P_2, respectively. Since D fixes both P_1 and P_2 while S interchanges them, $\bar{S}$ interchanges $\bar{P}_1$ with $\bar{P}_2$. In particular, these points of $\bar{\mathcal{X}}$ are not fixed by $\bar{S}$. Assume that $l_1 = l_2 = \frac{1}{2}|D|$. Let $\bar{\Lambda}_1, \bar{\Lambda}_2$ be the points of $\bar{\mathcal{X}}$ under the D-orbits Λ_1 and Λ_2. Since $\Omega_1 = \Lambda_1 \cup \Lambda_2$ and S acts transitively on Ω_1, $\bar{S}$ interchanges $\bar{\Lambda}_1$ with $\bar{\Lambda}_2$. Since Ω_1 and Ω_2 are the only short orbits of S, it turns out that $\bar{S}$ has no fixed point on $\bar{\mathcal{X}}$. On the other hand, Proposition 2.2 shows that $\bar{S}$ must have a fixed point on $\bar{\mathcal{X}}$, a contradiction.

For a point $P \in \Omega_1$, let $u \in S$ be the unique non-trivial element in S_P. Then u is an involution not contained in D. Let $U = \langle u \rangle$. Then $S = \langle D, U \rangle$. More precisely, since D and U have trivial intersection, $S = D \rtimes U$. If S is abelian, then u is a central involution, and hence $\mathcal{X}$ is hyperelliptic by Lemma 3.5. This completes the proof. □

Remark 4.2. If $|S| = 8$, then $\ell_2 = 2$ and Lemma 2.8 yields that S is either elementary abelian, or dihedral.

Theorem 4.3. *Let $\mathcal{X}$ be a curve of genus $\mathfrak{g} \geq 2$ defined over an algebraically closed field $\mathbb{K}$ of characteristic 2. Assume that $\mathrm{Aut}(\mathcal{X})$ has a subgroup S of order a power of 2 satisfying both hypotheses* (I) *and* (II). *If $\ell_2 = \frac{1}{4}|S| > 2$ and some central involution of S fixes a point, then case* (i) *of Theorem 1.2 holds.*

Proof. From Lemmas 3.4 and 3.5, there exists an involution $u \in Z(S)$ which fixes Ω_2 pointwise but no point from Ω_1. Furthermore, $|S| \geq 16$.

Let $W \in \Omega_1$. By (4) the stabilizer S_W of W in S has order two. Hence S_W consists of an involution w together with the identity. Note that $w \neq u$ by Lemma 3.5. Let Ω_w be the set of all fixed points of w. Since both Ω_1 and Ω_2 have even size, Ω_w also has even size.

If $|\Omega_w| = 2$ then $|C_S(w)| = 4$ by Lemma 2.6, and Proposition 2.4 yields that S is either dihedral, or semi-dihedral. The former case gives (ia). We must show that the latter case cannot actually occur.

Suppose on the contrary that $S \cong \mathbf{SD}_m$ with $m = |S|$. Since $|\Omega_w| = 2$, the conjugacy class of w in S consists of $\frac{1}{4}|S|$ involutions. Since u is a further involution of S, Lemma 2.5 yields that these $\frac{1}{4}|S|+1$ involutions are all the involutions in S. Therefore, the stabilizer S_Q of any point $Q \in \Omega_2$ has a unique involution, namely u. From (1) applied to S_Q,

$$2\mathfrak{g} - 2 \geq |S_Q|(2\tilde{\mathfrak{g}} - 2) + \sum_{P \in \Omega_2} d_P. \tag{9}$$

Here S_Q is a cyclic group of order 4. Now, $|S_Q| = |S_Q^{(1)}| = 4$ and since the factor group $S_Q^{(1)}/S_Q^{(2)}$ is elementary abelian, either $S_Q^{(2)} = S_Q$ or $S_Q^{(2)} = \langle u \rangle$. From Proposition 2.1, in the latter case $S_Q^{(3)} = S_Q^{(2)}$ holds. Therefore, $d_Q \geq 8$. Since Ω_2 has even size, S_Q fixes at least one more point $Q' \in \Omega_2$. By the previous argument, $d_{Q'} \geq 8$. For every other point $P \in \Omega_2$, we have $d_P \geq 4$. From (9), $2\mathfrak{g} - 2 \geq |S|$, a contradiction.

Assume now that $|\Omega_w| \geq 4$. Then $|C_S(w)| \geq 8$, see Lemma 2.6.

Let $d = |\Omega_w \cap \Omega_2|$. Consider the subgroup M of S of order 4 generated by u and w. Let γ_w be the 2-rank of the quotient curve $\mathcal{X}/M$. From (3) applied to M,

$$\begin{aligned}\gamma - 1 &\geq 4(\gamma_w - 1) + \big(|\Omega_w| - d\big) + 3d + \left(\frac{1}{4}|S| - d\right) \\ &= 4(\gamma_w - 1) + |\Omega_w| + d + \frac{1}{4}|S|. \end{aligned} \tag{10}$$

By (5), $d = 0$, $|\Omega_w| = 4$, $\gamma_w = 0$, and equality holds in (10). Therefore, the following assertions hold.

(a) M has exactly $\frac{1}{8}|S| + 2$ short orbits, each of size two; namely two orbits of $\langle u \rangle$ in Ω_w and each of the orbits of $\langle w \rangle$ in Ω_2.
(b) uw has no fixed point on Ω_1.
(c) $\Omega_w \subseteq \Omega_1$ with

$$|\Omega_w| = 4. \tag{11}$$

Since $|S| \geq 16$, from (11) it follows that $|\Omega_w| < \frac{1}{2}|S| = |\Omega_1|$. This together with (b) imply that S has at least five involutions.

By Lemma 2.6,

$$\big|C_S(w)\big| = 8. \tag{12}$$

Since $|S| \geq 16$, this yields that S is not abelian.

Let τ be the natural group homomorphism from $S \to \bar{S}$ where $\bar{S}$ is the factor group $S/\langle u \rangle$. Note that $\bar{S}$ is a $\mathbb{K}$-automorphism group of the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/S$ of order at least eight, and we are going to show that $\bar{S}$ is either a dihedral or a semi-dihedral group.

By Lemma 3.4, u fixes no point on Ω_1. Therefore, $|\bar{\Omega}_1| = \frac{1}{2}|\Omega_1|$ where the set $\bar{\Omega}_1$ consists of all points of $\bar{\mathcal{X}}$ lying under the points of Ω_1 with respect to the covering $\mathcal{X} \to \bar{\mathcal{X}}$. Also, $\bar{S}$ is a transitive permutation group on $\bar{\Omega}_1$. Take two points, $P, R \in \Omega_w$ such that $R \neq u(P)$. Then

$$\Omega_w = \big\{P, u(P), R, u(R)\big\}. \tag{13}$$

Let $\bar{P}$ and $\bar{R}$ be the points of $\bar{\mathcal{X}}$ lying under P and R, respectively. Then $\bar{P}, \bar{R}$ are the only fixed points of $\bar{w} = \tau(w)$ on $\bar{\Omega}_1$. From Lemma 2.6, $|C_{\bar{S}}(\bar{w})| = 4$. Proposition 2.4 yields that $\bar{S}$ is either dihedral, or semi-dihedral. These two possibilities are investigated separately.

Assume that $\bar{S}$ is dihedral. Let $\bar{C}$ be a (maximal) cyclic subgroup of $\bar{S}$ of order $\frac{1}{4}|S|$. Set $C = \tau^{-1}(\bar{C})$. From Lemma 2.7, either C itself cyclic, or $C = E \times \langle u \rangle$ with a cyclic subgroup E.

If $w \in C$, then $u \in C$ implies that C has at least two involutions. Hence $C = E \times \langle u \rangle$. Furthermore, the only involution in E is either w or uw. From Lemma 3.5 and assertion (b), neither u nor uw has a fixed point on Ω_1. Suppose that S has an involution w', $w' \neq w$, with a fixed point in Ω_1. Since S is transitive on Ω_1 and the 1-point stabilizer of S on Ω_1 has order two, we have that w and w' are conjugate under S. Since C is a (normal) subgroup of S of index 2 and $w \in C$, this implies that w' is also in C. But then we would have either $w' = u$ or $w' = uw$, a contradiction. Therefore, every point in Ω_1 must be fixed by w. Hence $\Omega_w = \Omega_1$. From (11), $|\Omega_1| = 4$ and hence $|S| = 8$, a contradiction.

If $w \notin C$, then no non-trivial element in C fixes a point in Ω_1, and hence C is sharply transitive on Ω_1. Bearing (13) in mind, take $h \in C$ such that $h(P) = R$. Then $h \neq u$ and $hwh^{-1}(R) = R$. Since the stabilizer of R in S is generated by w, this yields that $h \in C_S(w)$ with $h \neq w$. Moreover, $h \in Z(S)$ as S is generated by an abelian group C containing h together with w. As $h \neq u$, the center $Z(S)$ contains at least two non-trivial elements, whence S can be neither dihedral or semi-dihedral. By Lemma 2.5, C is not cyclic, and therefore $C = E \times \langle u \rangle$ holds. Since $h \in Z(S)$, h preserves Ω_w, and

$$h\big(u(P)\big) = (hu)(P) = (uh)(P) = u(R).$$

Therefore, the permutation induced by h on Ω_w is either the product of the transpositions (PR) and $(u(P)u(R))$, or it is the 4-cycle $(PRu(P)u(R))$. In the latter case, $h^2 = u$ as C is sharply transitive on Ω_1. Actually this is impossible, because the square of every element of $E \times \langle u \rangle$ of order ≥ 4 is in E, and hence distinct from u. Therefore, h is an involution distinct from u. Suppose that h fixes a point on $\mathcal{X}$. Since $h \in Z(S)$ and h does not fix P, h has no fixed point on Ω_1. Therefore, h fixes a point in Ω_2, and hence every point in Ω_2 is fixed by h. Let $L = \langle h, u \rangle$. If $\tilde{\gamma}$ is the 2-rank of the quotient curve $\tilde{\mathcal{X}} = \mathcal{X}/L$, from (5) and (3) applied to L,

$$\frac{1}{4}|S| = \gamma - 1 \geq 4(\tilde{\gamma} - 1) + \frac{3}{4}|S|,$$

whence $|S| \leq 8$, a contradiction. Therefore h is fixed-point-free on $\mathcal{X}$. From Lemma 3.6, h is an inductive central involution of S.

Note that u, h and uh are the only three involutions in C, and each such involution is central in S. As $\bar{S}$ is dihedral, any other involution in S is not central. We show that uh is fixed-point-free on $\mathcal{X}$, as well. Suppose on the contrary that $P \in \Omega_2$ is fixed by uh. Since $uh \in Z(C)$, the orbit Δ of P under C is pointwise fixed by uh. We have that $|C_P| \leq 4$, as C_P is a subgroup of S_P and $|S_P| = 4$. Actually, $|C_P| = 4$ since $u, uh \in C_P$ and $uh \neq u$. Hence, $C_P = \{1, u, h, uh\}$, and $|\Delta| = \frac{1}{8}|S|$. Now, choose $Q \in \mathcal{X}$ from $\Omega_2 \setminus \Delta$, and $s \in S$ such that s takes P to Q. Then $suhs^{-1}$ fixes Q. Since $uh \in C$ and C is a normal subgroup of S, this implies that $suhs^{-1} \in C$. Hence, either $suhs^{-1} = h$ or $suhs^{-1} = uh$. In both cases, $C_P = C_Q$. From (3) applied to C_P,

$$\frac{1}{4}|S| = \gamma - 1 = 4(\widehat{\gamma} - 1) + \frac{3}{8}|S| + \frac{3}{8}|S|,$$

where $\widehat{\gamma}$ is the 2-rank of the quotient curve $\widehat{\mathcal{X}} = \mathcal{X}/C_P$. But this is only possible for $|S| = 8$, a contradiction.

From Lemma 3.6, not only h but also uh is an inductive central involution. On the other hand, u, the third central involution of S, is not inductive. In fact, from (1) applied to $U = \langle u \rangle$ it follows that the genus of the quotient curve $\mathcal{X}/U$ is equal to 1. This gives case (ib).

To rule out the case that $\bar{S}$ is semi-dihedral, we give a lower bound for the number n_4 of subgroups of S of order 4 which contains u.

By (4) and (11), S has $\frac{1}{8}|S|$ pairwise distinct subgroups $M = \{1, w, u, uw\}$ when w ranges over the involutions in S fixing a point of Ω_1.

Since $\ell_2 = \frac{1}{4}|S|$ and u fixes Ω_2 pointwise, the stabilizer S_Q with $Q \in \Omega_2$ contains u and has order 4. Let r be the number of fixed points of S_Q in Ω_2. Obviously $r \geq 1$. Let $\tilde{\gamma}$ be the 2-rank of the quotient curve $\tilde{\mathcal{X}} = \mathcal{X}/S_Q$. From (3) applied to S_Q,

$$\gamma - 1 \geq 4(\tilde{\gamma} - 1) + 3r + \left(\frac{1}{4}|S| - r\right) = 4(\tilde{\gamma} - 1) + \frac{1}{4}|S| + 2r.$$

Since (I) holds, (5) and $r \geq 1$ yield that $r = 2$ and $\tilde{\gamma} = 0$.

Since $|S| \geq 16$, this shows that there is point $R \in \Omega_2$ such that $S_Q \neq S_R$. Therefore,

$$n_4 \geq \frac{1}{8}|S| + 2.$$

As a consequence, $\bar{S}$ more than $\frac{1}{8}|S| + 1 = \frac{1}{4}|\bar{S}| + 1$ pairwise distinct involutions. By Proposition 2.5, $\bar{S}$ is not a semi-dihedral group. □

5. Bielliptic curves with a large dihedral automorphism group of order a power of 2

Cyclic extensions of order a power of the characteristic of $\mathbb{K}$ are well known from the classical literature on function field theory, see [1,2,10,22,23]. Here we briefly outline the construction technique for such extensions when it is applied to an elliptic function field. Then we show that in some cases the resulting cyclic function field has a dihedral automorphism group with the properties described in case (1) of Theorem 1.1. This requires some computational results given in the forthcoming subsection.

Let $\bar{\mathcal{X}}$ be an elliptic curve with 2-rank $\bar{\gamma} = 1$. An affine equation of $\bar{\mathcal{X}}$ is

$$f(x, y) = y^2 + xy + x^3 + \nu x^2 + \mu \tag{14}$$

where $\mu, \nu \in \mathbb{K}$ and $\mu \neq 0$. Since $\bar{\gamma} = 1$, the zero divisor class group $\mathrm{Pic}_0(\bar{\mathcal{X}})$ of $K(\bar{\mathcal{X}})$ (isomorphic to the group defined by the point addition on $\bar{\mathcal{X}}$), contains a unique cyclic subgroup of order 2^m for every $m \geq 1$. Therefore, for every $m \geq 1$, $\mathrm{Aut}(\bar{\mathcal{X}})$ has a cyclic

subgroup $\mathbf{C}_n$ of order $n = 2^m$ such that no non-trivial element of $\mathbf{C}_n$ fixes a point of $\bar{\mathcal{X}}$. Let g be a generator of $\mathbf{C}_n$.

There exists a cyclic extension $\mathcal{X}$ of $\bar{\mathcal{X}}$, and all such cyclic extensions are obtained in the following way, see [22, Section V].

For $\xi \in \mathbb{K}(\bar{\mathcal{X}})$, the relative g-trace of ξ is defined to be

$$\mathrm{Tr}_g(\xi) = \xi + g(\xi) + \ldots + g^{2^m-1}(\xi). \tag{15}$$

Take an element $d \in \mathbb{K}(\bar{\mathcal{X}})$ with $\mathrm{Tr}_g(d) = 1$, and let $a = d^2 + d$. For $a \in \mathbb{K}(\bar{\mathcal{X}})$ and $v = 0, 1, \ldots, n-1$, let

$$a_{g^0} = 0, \quad \text{and} \quad a_{g^v} = a + g(a) + \ldots + g^{v-1}(a) \quad \text{for } v \geq 1.$$

Furthermore, take $c \in \mathbb{K}(\bar{\mathcal{X}})$ with $\mathrm{Tr}_g(c) \neq 0$. Then

$$e = \frac{1}{\mathrm{Tr}(c)} \sum_{v=0}^{n-1} a_{g^v}\, g^v(c) \tag{16}$$

satisfies the equation $g(e) + e = a$; see [22, Section I]. Here e cannot be written as $\zeta^2 + \zeta$ with $\zeta \in \mathbb{K}(\bar{\mathcal{X}})$; see [23, Section V]. Therefore, $\mathbb{K}(\mathcal{X}) = \mathbb{K}(\bar{\mathcal{X}})(z)$ with $z^2 + z + e = 0$ is an Artin–Schreier extension of $\mathbb{K}(\bar{\mathcal{X}})$. The map

$$\rho : (x, y, z) \to \big(g(x), g(y), z + d\big)$$

is a $\mathbb{K}$-automorphism of $\mathcal{X}$ whose order is equal to $2n = 2^{m+1}$. Also, $\mathbf{C}_{2n} = \langle \rho \rangle$ preserves $\bar{\mathcal{X}}$ and the $\mathbb{K}$-automorphism group $\mathbf{C}_{2n}/\langle \rho^n \rangle$ of $\bar{\mathcal{X}}$ coincides with $\mathbf{C}_n$.

Now, consider the elliptic involution

$$\varphi : (x, y) \to (x, x + y) \tag{17}$$

which is a $\mathbb{K}$-automorphism of $\bar{\mathcal{X}}$. Since $\varphi g \varphi = g^{-1}$, g together with φ generate a $\mathbb{K}$-automorphism group $\bar{D}$ of $\bar{\mathcal{X}}$ that is a dihedral group $\mathbf{D}_n$ of order $2n$.

The question arises whether φ extends to an involutory $\mathbb{K}$-automorphism ψ of $\mathcal{X}$ in such a way that the subgroup generated by ψ and $\mathbf{C}_{2n}$ is isomorphic to a dihedral group $\mathbf{D}_{2n}$ of order $4n$. If $\mathcal{X}$ itself is an elliptic curve, then the answer is affirmative. The main goal in this section is to prove that the answer is still affirmative for non-elliptic curves. This ensures the existence of examples for case (1) of Theorem 1.1. The proof depends on several computations in elliptic function fields. Some details, available in the preliminary version [4], will be omitted for brevity.

5.1. Some computations

Let $\bar{\mathcal{X}}$ be the elliptic curve over $\mathbb{K}$ with 2-rank $\bar{\gamma} = 1$ and affine equation

$$\bar{\mathcal{X}} : y^2 + xy + x^3 + \mu = 0.$$

Fix a power n of 2, and let g_0 be a generator of the cyclic subgroup of order $2n$ in the automorphism group of $\bar{\mathcal{X}}$. Let $g = g_0^2$, and φ be the elliptic involution defined by (17). Let $\oplus$ denote the point addition on $\bar{\mathcal{X}}$ such that the infinite point Y_∞ is the neutral element of $(\bar{\mathcal{X}}, \oplus)$. Also, let

$$[i]P = \underbrace{P \oplus P \oplus \ldots \oplus P}_{i \text{ times}},$$

and $\ominus P$ be the opposite of P in $(\bar{\mathcal{X}}, \oplus)$. For a positive integer r, let

$$\bar{\mathcal{X}}[r] = \{P \in \bar{\mathcal{X}} \mid [r]P = Y_\infty\}.$$

As $\bar{\gamma} = 1$, when r is a power of 2 the group $\bar{\mathcal{X}}[r]$ is a cyclic group of order r.

It will cause no confusion if we use the same letter to designate an automorphism of $\bar{\mathcal{X}}$ and its pull-back. In particular, g_0^i will also denote a map acting on the points of $\bar{\mathcal{X}}$ as follows:

$$g_0^i(P) = P \oplus [i]P_0. \tag{18}$$

Note that for each $\delta \in \mathbb{K}(\bar{\mathcal{X}})$

$$\operatorname{div}(\delta) = \sum_{P \in \bar{\mathcal{X}}} n_P P \quad \Rightarrow \quad \operatorname{div}\big(g_0^i(\delta)\big) = \sum_{P \in \bar{\mathcal{X}}} n_P \big(P \oplus [2n-i]P_0\big). \tag{19}$$

Let $P_0 = (w_1, w_2)$ be a generator of $\bar{\mathcal{X}}[2n]$, that is, P_0 is the point of $\bar{\mathcal{X}}$ such that $g_0(P) = P \oplus P_0$.

Let $\mathcal{P} = \bar{\mathcal{X}}[n]$ and $\mathcal{Z} = \bar{\mathcal{X}}[2n] \setminus \bar{\mathcal{X}}[n]$. Clearly $[2]P_0$ is a generator of $\mathcal{P}$. Also, $\mathcal{P}$ consists of points $[2j]P_0$ with $j = 0, \ldots, n-1$, whereas $\mathcal{Z}$ comprises points $[2j+1]P_0$ with $j = 0, \ldots, n-1$.

From (18) we deduce for $i = 1, \ldots, 2n-1$ that

$$g_0^i\colon \quad x' = \frac{X_i y + X_i x^2 + (X_i^2 + Y_i)x}{(x + X_i)^2}, \quad y' = \frac{y + Y_i}{x + X_i}\big(x' + X_i\big) + x' + Y_i, \tag{20}$$

where $[i]P = (X_i, Y_i)$. Since $\varphi g_0 \varphi = g_0^{-1}$, g_0 together with φ generate a dihedral group of order $4n$.

Lemma 5.1. *Let δ be a $\mathbb{K}$-linear combination of some rational functions $g_0^i(x)$. Then $x\delta$ is a square in $\mathbb{K}(\bar{\mathcal{X}})$. In particular, each zero of δ has even multiplicity.*

Proof. To prove that $x\delta$ is a square, it is enough to show that $xg_0^i(x)$ is a square for each i. Eq. (20) yields

$$xg_0^i(x) = \frac{X_i xy + X_i x^3 + (X_i^2 + Y_i)x^2}{(x + X_i)^2}.$$

As $xy + x^3 = y^2 + \mu$ we obtain

$$xg_0^i(x) = \frac{X_i(y^2+\mu) + (X_i^2+Y_i)x^2}{(x+X_i)^2} = \left(\frac{\sqrt{X_i}(y+\sqrt{\mu}) + x\sqrt{X_i^2+Y_i}}{x+X_i}\right)^2.$$

Since $x\delta$ is a square, $\mathrm{ord}_P(x) + \mathrm{ord}_P(\delta)$ is even for every $P \in \bar{\mathcal{X}}$. Since $\mathrm{ord}_P(x)$ is always even, every zero of δ has even multiplicity. □

For an element $\xi \in \mathbb{K}(\bar{\mathcal{X}})$ and for a non-negative integer v, let

$$\xi_{g^v} = 0 \quad \text{for } v = 0, \qquad \xi_{g^v} = \xi \quad \text{for } v = 1, \quad \text{and} \quad \xi_{g^v} := \sum_{i=0}^{v-1} g^i(\xi) \quad \text{for } v \geq 2.$$

Lemma 5.2. *Let $\xi \in \mathbb{K}(\bar{\mathcal{X}})$ be such that both $\mathrm{Tr}_g(\xi) = 0$ and $\varphi(\xi) = \xi$ hold. Then*

(i) $\xi_{g^{v_1}} = \xi_{g^{v_2}}$ *when* $v_1 \equiv v_2 \pmod n$;
(ii) $\xi_{g^{v_1}} + \xi_{g^{v_2}} = g^{v_1}(\xi_{g^{v_2 - v_1 \pmod n}})$;
(iii) $\varphi(\xi_{g^v}) = \xi_{g^{-v+1 \pmod n}} + \xi$.

Proof. See Lemma 2.5 in [4]. □

For an odd k with $1 \leq k \leq 2n-1$, define, as in Witt's paper [23]

$$d = \frac{x}{\mathrm{Tr}_g(x)}, \qquad a = d^2 + d. \tag{21}$$

Furthermore, let

$$c_k = g_0^k(x), \qquad e_k = \frac{1}{\mathrm{Tr}_g(c_k)} \sum_{v=0}^{n-1} a_{g^v} g^v(c_k). \tag{22}$$

A straightforward computation gives the following result:

$$g(e_k) + e_k = a. \tag{23}$$

Our purpose is to show that $\varphi(e_k) + e_k = a$ also holds, see Proposition 5.8 below. This requires some more computation.

Proposition 5.3. *The rational function e_k is a square.*

Proof. By Lemma 5.1 $d = \frac{x}{\mathrm{Tr}_g(x)} = \frac{x^2}{x\,\mathrm{Tr}_g(x)}$ is a square. Therefore a_{g^v} is a square for each v. Then, we only need to show that $\mathrm{Tr}_g(c_k) \cdot g^v(c_k)$ is a square for each v. This follows from the fact that

$$x^2 \cdot \mathrm{Tr}_g(c_k) \cdot g^v(c_k) = \big(x\,\mathrm{Tr}_g\big(g_0^k(x)\big)\big)\big(xg_0^{2v+k}(x)\big) = \left(x\sum_{i=0}^{n-1} g_0^{2i+k}(x)\right)\big(xg_0^{2v+k}(x)\big)$$

is a square by Lemma 5.1. □

Lemma 5.4. *For the rational function a, both $\mathrm{Tr}_g(a) = 0$ and $\varphi(a) = a$ hold.*

Proof. We have that $\mathrm{Tr}_g(a) = \mathrm{Tr}_g(d^2+d) = \mathrm{Tr}_g(d)^2+\mathrm{Tr}_g(d) = 1+1 = 0$. Moreover, from $\varphi g = g^{-1}\varphi$ it follows that $\varphi(\mathrm{Tr}_g(x)) = \mathrm{Tr}_g(x)$. Therefore $\varphi(d) = d$ and $\varphi(a) = a$. □

Lemma 5.5. $\mathrm{Tr}_g(ag_0(x)) = \mathrm{Tr}_g(g(a)g_0(x))$.

Proof. See Lemma 2.8 in [4]. □

Lemma 5.6. *For each odd k with $1 \le k \le 2n-1$, $\mathrm{Tr}_g(ag_0^k(x)) = \mathrm{Tr}_g(g^k(a)g_0^k(x))$.*

Proof. As k is odd, g_0^k is a generator of $\langle g_0\rangle$. Therefore, by Lemma 5.5, we have $\mathrm{Tr}_{g^k}(\bar{a}g_0^k(x)) = \mathrm{Tr}_{g^k}(g^k(\bar{a})g_0^k(x))$, where $\bar{a} = (x/\mathrm{Tr}_{g^k}(x))^2 + x/\mathrm{Tr}_{g^k}(x)$. But clearly Tr_{g^k} coincides with Tr_g. Thus, $\bar{a} = a$ and

$$\mathrm{Tr}_g\big(ag_0^k(x)\big) = \mathrm{Tr}_g\big(g^k(a)g_0^k(x)\big)$$

also holds. □

Lemma 5.7. *For each odd k with $1 \le k \le 2n-1$,*

$$\mathrm{Tr}_g\big(g_0^k(x)\cdot\big(a+g(a)+\ldots+g^k(a)\big)\big) = 0.$$

Proof. It is by induction on k. The assertion for $k = 1$ is just Lemma 5.5. Now assume that

$$\mathrm{Tr}_g\big(g_0^{k-2}(x)\cdot\big(a+g(a)+\ldots+g^{k-2}(a)\big)\big) = 0.$$

Applying g to the argument of Tr_g gives

$$\mathrm{Tr}_g\big(g_0^k(x)\cdot\big(g(a)+g^2(a)+\ldots+g^{k-1}(a)\big)\big) = 0.$$

By Lemma 5.6 and the additivity of Tr_g, the assertion follows. □

Proposition 5.8. *For each odd k between 1 and $2n-1$,*

$$\phi(e_k) + e_k = a$$

Proof. See Proposition 2.11 in [4]. □

5.2. Proof of the existence

We are in a position to show the existence of curves which provide examples for case (1) of Theorem 1.1.

For this purpose, we consider the Artin–Schreier extension $\mathcal{X}_k$ of $\bar{\mathcal{X}}$ defined by the equation $z^2 + z + e_k = 0$, where k is an odd integer with $1 \le k \le 2n-1$.

We first construct some automorphisms of $\mathcal{X}_k$. Every element in $\mathbb{K}(\mathcal{X}_k)$ can uniquely be written as $(a_1 + a_2 y)z + a_3 y + a_4$ with $a_1, a_2, a_3, a_4 \in \mathbb{K}(x)$. Furthermore, the map

$$\rho : (x, y, z) \to \big(g(x), g(y), z + d\big) \tag{24}$$

is a $\mathbb{K}$-automorphism of $\mathcal{X}_k$. From $\mathrm{Tr}_g(d) = 1$ we have that

$$\iota = \rho^n : (x, y, z) = (x, y, z + 1). \tag{25}$$

Therefore, ι is an involution, $\bar{\mathcal{X}} = \mathcal{X}_k^{\iota}$, and ρ generates a cyclic subgroup $\mathbf{C}_{2n}$ of $\mathrm{Aut}(\mathcal{X}_k)$ of order $2n$. Also, $\mathbf{C}_{2n}$ preserves $\mathcal{X}_k$ and the $\mathbb{K}$-automorphism group $\mathbf{C}_{2n}/\langle\iota\rangle$ of $\bar{\mathcal{X}}$ coincides with the cyclic group of order n generated by g.

A straightforward computation involving Proposition 5.8 gives the following result.

Lemma 5.9. *The map*

$$\psi : (x, y, z) \to \big(\varphi(x), \varphi(y), z + d\big)$$

is a $\mathbb{K}$-automorphism of $\mathcal{X}_k$.

Next, the structure of the group generated by ρ and ψ is described.

Proposition 5.10. *The group S generated by ρ and ψ is isomorphic to $\mathbf{D}_{2n}$.*

Proof. As $\varphi(d) = d$, both ψ and $\psi\rho$ are involutions showing that $S \cong \mathbf{D}_{2n}$. □

To prove Theorem 5.14 it remains to show that $\mathcal{X}_k$ is non-elliptic for some odd k with $1 \le k \le 2n-1$. For this purpose, the following results on the pole divisor of $e_k \in \mathbb{K}(\bar{\mathcal{X}})$ are useful.

Lemma 5.11. *Let k be an odd integer with $1 \le k \le 2n-1$. Then*

(i) *every pole of e_k belongs to $\mathcal{P} \cup \mathcal{Z}$;*
(ii) *the point Y_∞ is not a pole of e_k;*
(iii) *for every $P \in \mathcal{Z}$, $v_P(e_k) \ge -4$;*

(iv) $v_{[-k]P_0}(e_k) \geq -2$ *and equality holds provided that* $[-k]P_0$ *is not a zero of*

$$\sum_{v=1}^{n-1}\big(x^2 + g\big(x^2\big) + \ldots + g^{v-1}\big(x^2\big)\big)g^v(c_k).$$

Proof. See Lemma 2.14 in [4]. □

Proposition 5.12. *Assume that there exist some point* $P \in \bar{\mathcal{X}}$ *such that the order of* e_k *at* P *is equal to* -2*. Then* ι *fixes exactly* n *places of* $\mathcal{X}$*, and* $\mathcal{X}_k$ *has genus* $n+1$*. Also, the* 2*-rank of* $\mathcal{X}_k$ *is equal to* $n+1$*.*

Proof. Let $\mathcal{Y}_k$ be a non-singular model of $\mathcal{X}_k$, so that $\mathbf{D}_{2n}$ can be viewed as an automorphism group of $\mathcal{Y}_k$. Let $\pi : \mathcal{Y}_k \to \bar{\mathcal{X}}$ denote the covering of degree 2 associated with the function field extension $\mathbb{K}(\mathcal{Y}_k) : \mathbb{K}(\mathcal{Y}_k)^\iota$. By the Hurwitz genus formula applied to π, the genus of $\mathcal{X}_k$ is equal to $1 + \frac{1}{2}\sum d_Q$, where, as usual, d_Q denotes the different exponent of a point Q of $\mathcal{Y}_k$ with respect to π (see e.g. [19, Proposition 3.7.8]). Let $\mathcal{E}$ be the set of points Q of $\mathcal{Y}_k$ such that $d_Q > 0$. As $\mathcal{E}$ coincides with the set of points fixed by ι, $\mathcal{E}$ is preserved by $\mathbf{C}_{2n}$. More precisely, as $\mathbf{C}_{2n}/\langle\iota\rangle$ coincides with $\langle g\rangle$, the set $\mathcal{E}$ consists of the points of $\mathcal{Y}_k$ lying over a g-invariant set of points $\mathcal{D}$ of $\bar{\mathcal{X}}$. By [19, Proposition 3.7.8] each point in $\mathcal{D}$ is a pole of e_k. By Lemma 5.11, either $\mathcal{D}$ is empty, or $\mathcal{D} = \mathcal{Z}$. Under our assumption, we prove that the former case cannot actually occur. Let t be a local parameter at P. By Proposition 5.3,

$$e_k = \sigma t^{-2} + e'_k$$

with $\sigma \in \mathbb{K}$, $\sigma \neq 0$ and $v_P(e'_k) = 0$. Then clearly

$$v_P\big(e_k + (\sqrt{\sigma}/t)^2 + (\sqrt{\sigma}/t)\big) = -1.$$

By [19, Proposition 3.7.8(c)], P is totally ramified, and if P' denotes the only point in $\mathcal{X}_k$ lying over P, then the different exponent $d_{P'}$ is equal to 2. This proves that $\mathcal{D} = \mathcal{Z}$. Now let $R \in \mathcal{Z}$ be such that $v_R(e_k) \neq -2$, and let R' be the only point in $\mathcal{E}$ such that $\pi(R') = R$. By (iii) of Lemma 5.11, $v_R(e_k) = -4$ holds. Then, by [19, Proposition 3.7.8], either $d_{R'} = 4$ or $d_{R'} = 2$. If $d_{R'} = 4$, then there exists $\xi \in \mathbb{K}(\bar{\mathcal{X}})$ with $v_R(e_k + \xi^2 + \xi) = -3$. But this is impossible e_k being a square. Therefore, for each $Q \in \mathcal{E}$ we have $d_Q = 2$. Finally, as the size of $\mathcal{E}$ is n, from the Hurwitz genus formula the genus of $\mathcal{X}_k$ is equal to $n+1$. The Deuring–Shafarevich formula, see (3), applied to $S = \langle\iota\rangle$ shows that the 2-rank of $\mathcal{X}_k$ is equal to $n+1$ as well. □

Proposition 5.13. *There exists* k *for which* $\bar{P} = [-k]P_0$ *is not a zero of*

$$\sum_{v=1}^{n-1}\big(x^2 + g\big(x^2\big) + \ldots + g^{v-1}\big(x^2\big)\big)g^v(c_k).$$

Proof. Let $\zeta_v = x + g(x) + \ldots + g^{v-1}(x)$, and consider the rational function ϵ defined as follows:

$$\epsilon(P) = \zeta_1(P)^2 \cdot x\big([2]P_0\big) + \zeta_2(P)^2 \cdot x\big([4]P_0\big) + \ldots + \zeta_{n-1}(P)^2 \cdot x\big([2n-2]P_0\big).$$

As $g^v(g_0^k(x))(\bar{P})$ is the x-coordinate of $[2v]P_0$,

$$\epsilon(\bar{P}) = \left(\sum_{v=1}^{n-1}\big(x^2 + \ldots + g^{v-1}\big(x^2\big)\big)g^v(c_k)\right)(\bar{P}).$$

Therefore, to prove the existence of a suitable k it will be enough to show that ϵ has less than n distinct zeros in $\mathcal{Z}$. Note that the values of $x([2v]P_0)$ are independent of P, and therefore can be viewed as constants. Let $\alpha_v \in \mathbb{K}$ be the square root of $x([2v]P_0)$. Then $\epsilon(P) = \theta(P)^2$, where

$$\theta(P) = \zeta_1(P) \cdot \alpha_1 + \zeta_2(P) \cdot \alpha_2 + \ldots + \zeta_{n-1}(P) \cdot \alpha_{n-1}.$$

We will prove that θ has less than n distinct zeros in $\mathcal{Z}$. Expanding $\zeta_i(P)$ gives

$$\begin{aligned}\theta(P) = {} & x(P)\alpha_1 + \big(x(P) + x\big(P \oplus [2]P_0\big)\big)\alpha_2 \\ & + \big(x(P) + x\big(P \oplus [2]P_0\big) + x\big(P \oplus [4]P_0\big)\big)\alpha_3 \\ & + \ldots + \big(x(P) + \ldots + x\big(P \oplus [2n-4]P_0\big)\big)\alpha_{n-1}.\end{aligned}$$

Note that $\alpha_{n/2} = 0$ and that $\alpha_v = \alpha_{n-v}$. This depends on $[n]P_0 = (0, \sqrt{\mu})$ and on $[2v]P_0$ being the opposite of $[2n-2v]P_0$. Therefore $\alpha_1 + \ldots + \alpha_{n-1} = 0$, and hence there exist constants $\beta_i \in \mathbb{K}$ with

$$\theta(P) = x\big(P \oplus [2]P_0\big) \cdot \beta_1 + \ldots + x\big(P \oplus [2n-4]P_0\big) \cdot \beta_{n-2}.$$

As $x(P \oplus [2i]P_0) = g^i(x)(P)$, θ is a linear combination of some $g^i(x)$'s. Clearly, the only poles of θ are points $[2n-2v]P_0$ for which $\beta_v \neq 0$. Each of those poles has multiplicity 2. Then the number of zeros of θ is at most $2(n-2)$. By Lemma 5.1, each zero of θ has even multiplicity. If $[-k]P_0$ is a zero of θ for each k, then the number of zeros is larger than $2n-4$, which is a contradiction. □

Taking into account (iv) of Lemma 5.11 together with Proposition 5.12, this ends the proof of the following result.

Theorem 5.14. *For every $n = 2^h \geq 8$, some of the above bielliptic curves $\mathcal{X}_k$ is of genus $\mathfrak{g} = n+1 \geq 2$ and it has a dihedral $\mathbb{K}$-automorphism group S such that $|S| = 4(\mathfrak{g}-1)$. Furthermore, $\gamma = \mathfrak{g}$ and the (unique) central involution in S fixes some points of $\mathcal{X}$ and hence it is not inductive.*

5.3. Some more examples

From Theorem 5.14, the question arises whether curves other than $\mathcal{X}_k$ can provide examples for case (1) of Theorem 1.1. To construct such a curve, a different choice for d in (21) is necessary. The possibilities are described in the following result.

Lemma 5.15. *For $d \in \mathbb{K}(\bar{\mathcal{X}})$ with $\mathrm{Tr}_g(d) = 1$, $a = d^2 + d$, $c \in \mathbb{K}(\bar{\mathcal{X}})$ with $\mathrm{Tr}_g(c) \neq 0$, let e be as defined in (16). Assume that $\varphi(a) = a$ and $\varphi(c) = g(c)$. Then $\varphi(e) + e = a$, and either*

(i) $d = \frac{x}{\mathrm{Tr}_g(x)} + \delta$, *or*
(ii) $d = \frac{y}{x} + (\mathrm{Tr}_g(\frac{y}{x}) + 1)\frac{x}{\mathrm{Tr}(x)} + \delta$,

with $\mathrm{Tr}_g(\delta) = 0$ and $\delta \in \mathbb{K}(x)$.

Proof. Since $\mathrm{Tr}_g(c) \neq 0$, we have that $g(c) \neq c$. From $\varphi g = g^{-1}\varphi$,

$$\varphi\big(\mathrm{Tr}_g(c)\big) = g^{-1}\big(\mathrm{Tr}_g(\varphi(e))\big) = g^{-1}\,\mathrm{Tr}_g\big(g(c)\big) = g^{-1}\big(\mathrm{Tr}_g(c)\big) = \mathrm{Tr}_g(c).$$

By (iii) of Lemma 5.2,

$$\begin{aligned}\varphi(e) + e &= \frac{1}{\mathrm{Tr}_g(c)}\left(\sum_{v=0}^{n-1} a_{g^v} g^v(c) + \sum_{v=0}^{n-1}(a + a_{g^{-v+1 \pmod n}} g^{-v+1}(c)\right)\\ &= \frac{1}{\mathrm{Tr}_g(c)}\sum_{v=0}^{n-1} a g^{-v+1}(c) = a\frac{\mathrm{Tr}_g(c)}{\mathrm{Tr}_g(c)} = a.\end{aligned}$$

It has been already noticed that $\mathrm{Tr}_g(x/\mathrm{Tr}_g(x)) = 1$. Hence, if $d \in \mathbb{K}(x)$ then $\delta = d + (x/\mathrm{Tr}_g(x))$ has zero relative trace. Here $\delta \in \mathbb{K}(x)$ because $x/\mathrm{Tr}_g(x) \in \mathbb{K}(x)$.

To show the last assertion, observe that

$$d^2 + d \in \mathbb{K}(x). \tag{26}$$

Assume that $\varphi(d) \neq d$. Then $d \notin \mathbb{K}(x)$ and $d = \omega_1 y + \omega$ with $\omega_1, \omega \in \mathbb{K}(x)$ and $\omega_1 \neq 0$. From (26)

$$\begin{aligned}\omega_1^2 y^2 + \omega_1 y + \omega^2 + \omega &= \omega_1^2\big(xy + x^3 + \mu\big) + \omega_1 y + \omega^2 + \omega\\ &= \omega_1(\omega_1 x + 1)y + \omega_1^2\big(x^3 + \mu\big) + \omega^2 + \omega\end{aligned}$$

belongs to $\mathbb{K}(\mathcal{X})$, whence $\omega_1 = 1/x$. Observe that

$$\varphi\left(\mathrm{Tr}_g\left(\frac{y}{x}\right)\right) = \mathrm{Tr}_g\left(\varphi\left(\frac{y}{x}\right)\right) = \mathrm{Tr}_g\left(\frac{x+y}{x}\right) = \mathrm{Tr}_g\left(\frac{y}{x} + 1\right) = \mathrm{Tr}_g\left(\frac{y}{x}\right).$$

This shows that

$$\mathrm{Tr}_g\left(\frac{y}{x}\right) \in \mathbb{K}(x).$$

Hence

$$\left(\mathrm{Tr}_g\left(\frac{y}{x}\right)+1\right)\frac{x}{\mathrm{Tr}_g(x)} \in \mathbb{K}(x).$$

Since $\mathrm{Tr}_g(d) = 1$ and

$$\mathrm{Tr}_g\left(\frac{y}{x}+\left(\mathrm{Tr}_g\left(\frac{y}{x}\right)+1\right)\frac{x}{\mathrm{Tr}_g(x)}\right) = 1,$$

the assertion follows. □

6. Some explicit examples

In this section, $\mathbb{K}$ is the algebraic closure of the finite field $\mathbb{F}_q$ of order q where $q \geq 4$ is a power of 2, and w a primitive element of $\mathbb{F}_q$. We exhibit several curves with explicit equations that realize the cases in Theorem 1.2.

6.1. Case (ia)

In Section 5, an infinite family of curves $\mathcal{X}_k$ of type (ia) is constructed. Here we single out the case of $\mathfrak{g} = 9$, and illustrate some computational results for $q = 16$. Let $\bar{\mathcal{X}}$ be the elliptic curve of equation $Y^2 + XY + X^3 + \mu = 0$, and $\mathbb{K}(\mathcal{X}) = \mathbb{K}(x, y)$ with $y^2 + xy + x^3 + \mu = 0$ is its function field.

In the first construction, take μ a primitive element in $\mathbb{F}_{16}$, and $k = 1$ in (21). Then definition (22) reads $e_1 = (\tau/\xi)y + (\omega/\xi)$ with

$$\begin{aligned}
\tau &= \mu x^{13} + \mu^2 x^{11} + \mu^{11} x^9 + \mu^{13} x^7 + \mu^{13} x^5 + \mu^5 x^3 + \mu^{11} x,\\
\xi &= x^{16} + \mu^4 x^{12} + \mu x^8 + \mu^6 x^4 + \mu^4,\\
\omega &= \mu^4 x^{16} + \mu x^{15} + \mu^{11} x^{14} + \mu^2 x^{13} + \mu^7 x^{12} + \mu^{11} x^{11} + \mu^5 x^{10} + \mu^{13} x^9\\
&\quad + \mu^{14} x^8 + \mu^{13} x^7 + \mu^{12} x^6 + \mu^5 x^5 + \mu^3 x^4 + \mu^{11} x^3 + \mu^{14} x^2 + \mu^8.
\end{aligned}$$

Let $\mathcal{X}_1$ be a non-singular model of the bielliptic function field which is the extension of $\mathbb{K}(\bar{\mathcal{X}})$ by adjoining z where $z^2 + z + e_1 = 0$. Eliminating y from $z^2 + z + e_1 = 0$ and $y^2 + xy + x^3 + \mu = 0$, gives an affine equation of a plane (singular) model of $\mathcal{X}$:

$$\begin{aligned}
F(X, Z) &= Z^4X^{28} + \mu Z^4X^{26} + \mu^7 Z^4X^{24} + \mu^3 Z^4X^{22} + \mu^8 Z^4X^{20}\\
&\quad + \mu^7 Z^4X^{18} + \mu^4 Z^4X^{16} + \mu^8 Z^4X^{14} + \mu^6 Z^4X^{12} + \mu^{13} Z^4X^{10} + Z^4X^8
\end{aligned}$$

$$
\begin{aligned}
&+\mu^8Z^4X^6+\mu^9Z^4X^4+Z^4X^2+\mu^{11}Z^4+Z^2X^{28}+\mu^7Z^2X^{24}+\mu^13Z^2X^{22}\\
&+\mu^{11}Z^2X^{20}+\mu^{12}Z^2X^{16}+\mu^4Z^2X^{14}+\mu^{11}Z^2X^{12}+\mu^{10}Z^2X^{10}+\mu^3Z^2X^8\\
&+\mu^8Z^2X^6+\mu^{11}Z^2X^4+\mu^{14}Z^2X^2+\mu^{11}Z^2+\mu ZX^{26}+\mu^8ZX^{22}+\mu^7ZX^{20}\\
&+\mu^7ZX^{18}+\mu^6ZX^{16}+\mu^5ZX^{14}+\mu ZX^{12}+\mu^9ZX^{10}+\mu^{14}ZX^8+\mu^2ZX^4\\
&+\mu^3ZX^2+\mu^8X^{28}+\mu^3X^{26}+\mu^{13}X^{24}+\mu^9X^{22}+\mu^{13}X^{18}+\mu^8X^{16}\\
&+\mu^5X^{14}+\mu^5X^{12}+\mu^{12}X^{10}+\mu^{10}X^8+X^6+\mu^5X^4+\mu^4=0.
\end{aligned}
$$

Obviously, $\mathcal{X}_1$ is defined over $\mathbb{F}_{16}$. According to the results in Section 5, it has genus and 2-rank equal to 9 and a dihedral $\mathbb{K}$-automorphism group S_1 of order 32. Therefore $\mathcal{X}_1$ is an example of case (ia) of Theorem 1.2. A MAGMA aided computation shows that $\mathcal{X}_1$ has exactly 24 places over $\mathbb{F}_{16}$. Therefore, the two short orbits of S_1 on $\mathcal{X}_1$ constitute the set $\mathcal{X}_1(\mathbb{F}_{16})$ of all $\mathbb{F}_{16}$-rational places of $\mathcal{X}_1$. Moreover, $|\mathcal{X}_1(\mathbb{F}_{16^2})|=408$.

In the second construction, $e=(\tau/\xi)y+(\omega/\xi)$ with

$$
\begin{aligned}
\tau &= a^8x^6+ax^5+a^{13}x^4+a^{14}x^3+a^{14}x^2+a^{10}x+a^{13};\\
\omega &= a^2x^8+a^{13}x^7+a^6x^6+a^{13}x^5+a^{10}x^4+a^{10}x^3+x^2+a^4x+a^{12};\\
\xi &= x^8+a^2x^6+a^8x^4+a^3x^2+a^2.
\end{aligned}
$$

This time, we obtain an irreducible plane curve $\mathcal{C}$ with affine equation

$$
\begin{aligned}
F(X,Z) = {} & X^{14}Z^4+X^{14}Z^2+\mu^4X^{14}+\mu^8X^{13}Z^4+\mu^8X^{13}Z+\mu^9X^{13}\\
&+\mu^{11}X^{12}Z^4+\mu^{11}X^{12}Z^2+\mu^{14}X^{12}+\mu^9X^{11}Z^4\\
&+\mu^{14}X^{11}Z^2+\mu^4X^{11}Z+\mu^{12}X^{11}+\mu^4X^{10}Z^4+\mu^{13}X^{10}Z^2\\
&+\mu^{11}X^{10}Z+\mu^{11}X^9Z^4+\mu^{11}X^9Z+\mu^{14}X^9+\mu^2X^8Z^4\\
&+\mu^6X^8Z^2+\mu^3X^8Z+\mu^4X^8+\mu^4X^7Z^4+\mu^2X^7Z^2+\mu^{10}X^7Z\\
&+\mu^{10}X^7+\mu^3X^6Z^4+\mu^{13}X^6Z^2+\mu^8X^6Z+\mu^{10}X^6\\
&+\mu^{14}X^5Z^4+\mu^5X^5Z^2+\mu^{12}X^5Z+\mu^6X^5+X^4Z^4\\
&+\mu^9X^4Z^2+\mu^7X^4Z+\mu^5X^4+\mu^4X^3Z^4+\mu^4X^3Z^2+X^3\\
&+\mu^{12}X^2Z^4+\mu^{13}X^2Z^2+\mu X^2Z+\mu^{10}X^2+XZ^4\\
&+\mu^7XZ^2+\mu^9XZ+\mu^{13}Z^4+\mu^{13}Z^2+\mu^2.
\end{aligned}
$$

A non-singular model $\mathcal{X}_2$ of $\mathcal{C}$ has genus and 2-rank equal to 9 with a dihedral group S_2 of automorphisms of order 32. Therefore, it provides another example of case (ia) of Theorem 1.2.

A MAGMA aided computation shows that $\mathcal{X}_2(\mathbb{F}_{16})$ has the same behavior as $\mathcal{X}_1$ does, as the two short orbits of S_2 on $\mathcal{X}_2$ constitute $\mathcal{X}_2(\mathbb{F}_{16})$. However, $|\mathcal{X}_2(\mathbb{F}_{16^2})| = 472$ which shows that $\mathcal{X}_1$ and $\mathcal{X}_2$ are not isomorphic over $\mathbb{F}_{16}$. It seems plausible that this holds true over $\mathbb{K}$.

6.2. Case (ib)

Let $q = 16$. For a primitive element μ of $\mathbb{F}_{16}$, let $\mathcal{X}$ be the curve which is the non-singular model of the irreducible plane curve $\mathcal{C}$ with affine equation

$$F(X,Y) = Y^4X^7 + \mu^5Y^4X^5 + \mu^{13}Y^4X^3 + \mu^9Y^4X + YX^7\mu^5YX^5 + \mu^{13}YX^3 + \mu^9YX + X^8 + \mu^2X^6 + \mu^8X^4 + \mu^3X^2 + \mu^2 = 0.$$

From a computer aided computation performed by MAGMA, $\mathcal{X}$ has genus 9 and $\mathrm{Aut}(\mathcal{X})$ has a subgroup S of order 32 such that $S \cong D_8 \times C_2$. Furthermore, $\bar{\mathcal{X}} = \mathcal{X}/C_2$ has genus 5 and $\mathrm{Aut}(\bar{\mathcal{X}})$ has a dihedral subgroup of order 8. Therefore, $\bar{\mathcal{X}}$ is a curve of type (ib).

6.3. Case (ii)

Let $\mathcal{X}$ be the hyperelliptic curve which is the non-singular model of the projective irreducible plane curve $\mathcal{C}$ of degree $q+2$ with affine equation

$$\left(Y^2 + Y + X\right)\left(X^q + X\right) + \sum_{\alpha \in \mathbb{F}_q} \frac{X^q + X}{X + \alpha} = 0.$$

It is easily seen that $\mathcal{C}$ has exactly two points at infinity, namely $X_\infty = (1,0,0)$ and $Y_\infty = (0,1,0)$. Both are ordinary singularities. More precisely, X_∞ and Y_∞ are singular points of $\mathcal{C}$ with multiplicity q and 2, respectively. No affine point of $\mathcal{C}$ is singular. Therefore, $\mathcal{X}$ has genus

$$\mathfrak{g} = \frac{1}{2}(q+1)q - 1 - \frac{1}{2}q(q-1) = q - 1,$$

see [8, Theorem 5.57]. For $\beta \in \mathbb{F}_q$, let $\mu \in \mathbb{K}$ be such that $\mu^2 + \mu = \beta$. Then the map

$$\varphi_\mu : (x,y) \to (x + \beta, y + \mu)$$

preserves $\mathcal{C}$ and hence it is $\mathbb{K}$-automorphism of $\mathcal{X}$. These maps form a $\mathbb{K}$-automorphism group S of $\mathcal{X}$. Obviously, S is an elementary abelian group of order $2q$.

Since $2q = 2\mathfrak{g} + 2$, $\mathcal{X}$ provides an example for case (ii) of Theorem 1.2.

6.4. Case (iii)

Let $\mathcal{X}$ be the non-singular model of the projective irreducible plane curve $\mathcal{C}$ of degree $2q$ with affine equation

$$\left(Y^q - Y\right)\left(X^q - X\right) + 1 = 0. \tag{27}$$

As in the preceding example, $\mathcal{C}$ has exactly two points at infinity, namely $X_\infty = (1,0,0)$ and $Y_\infty = (0,1,0)$; both are ordinary singularities of multiplicity q. The tangents to $\mathcal{C}$ at X_∞ are the lines v_μ with equation $Y - \mu = 0$ with $\mu \in \mathbb{F}_q$. Similarly for Y_∞ and the lines h_μ of equation $X - \mu = 0$. No affine point of $\mathcal{C}$ is singular. Therefore $\mathcal{X}$ has genus

$$\mathfrak{g} = \frac{1}{2}(2q-1)(2q-2) - q(q-1) = (q-1)^2,$$

see [8, Theorem 5.57]. For $\alpha, \beta \in \mathbb{F}_q$ the map

$$\varphi_{\alpha,\beta} : (X,Y) \to (X+\alpha, Y+\beta)$$

preserves $\mathcal{C}$ and so it is a $\mathbb{K}$-automorphism of $\mathcal{X}$. Here, $E = \{\varphi_{\alpha,\beta} | \alpha, \beta \in \mathbb{F}_q\}$ is an elementary abelian group of order q^2. Also, the map

$$\rho : (X,Y) \to (Y,X)$$

preserves $\mathcal{C}$ and hence it is a further $\mathbb{K}$-automorphism of $\mathcal{X}$. The group generated by E together with ρ is the semidirect product $E \rtimes \langle\rho\rangle$ and it has order $2q^2$. Since $2q^2 > 2((q-1)^2-1) = 2(\mathfrak{g}-1)$, Nakajima's bound implies that $E \rtimes \langle\rho\rangle$ is not properly contained in a 2-subgroup of $\mathrm{Aut}(\mathcal{X})$. Let $S = E \rtimes \langle\rho\rangle$. It is easily seen that the central involutions of S are the maps $\varphi_{\alpha,\alpha}$ with $\alpha \in \mathbb{F}_q$ and $\alpha \neq 0$.

We show that no non-trivial element in S fixes a point of $\mathcal{X}$. Obviously, no non-trivial element in S fixes an affine point. Since the point $U = (1,1,0)$ is not in $\mathcal{C}$ and ρ interchanges the points X_∞ and Y_∞, no point in $\mathcal{X}$ is fixed by an element in the coset of E containing ρ. This holds true for any non-trivial element in E, since $\varphi_{\alpha,\beta}$ preserves no line of type h_μ or v_μ, and hence it preserves no branch centered either at X_∞ or Y_∞.

Therefore, every central involution of S is inductive, and hence $\mathcal{X}$ is an example for case (iii) in Theorem 1.2 with

$$|S| = 2(\mathfrak{g}-1) + 4q - 2 \quad \text{with } \mathfrak{g} = (q-1)^2 \text{ and } q = 2^h \geq 4. \tag{28}$$

Here, Nakajima's bound is only attained for $q = 4$.

6.5. Example of an inductive sequence of curves

The procedure described in Introduction starting with $\mathcal{X}$ as in Subsection 6.4 and ending with a curve free from inductive central involutions is now illustrated in the smallest case, $q = 4$. With the above notation, $\mathfrak{g} = 9$ and $|S| = 4(\mathfrak{g}-1) = 32$. As we have pointed out, $u = \varphi_{1,1}$ is an inductive central involution of S. From (1) applied to $\langle u\rangle$,

$$16 = 2\mathfrak{g} - 2 = 2(2\bar{\mathfrak{g}} - 2),$$

where $\bar{\mathfrak{g}}$ is the genus of the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/\langle u\rangle$. Hence $\bar{\mathfrak{g}} = 5$. Similarly, $\bar{\mathcal{X}}$ has 2-rank 5. The factor group $\bar{S} = S/\langle u\rangle$ is a subgroup of $\bar{\mathcal{X}}$ of order 16. Thus $|\bar{S}| = 16 = 4(\bar{\mathfrak{g}}-1)$. So, Nakajima's bound is attained by $\bar{\mathcal{X}}$. Since the function field $\mathbb{K}(\mathcal{X})$ is $\mathbb{K}(x, y)$ with $(x^4 + x)(y^4 + y) + 1 = 0$, its subfield generated by $t = x + y$ and $z = y^2 + y$ is the function field $\mathbb{K}(\bar{\mathcal{X}})$. It is easily seen that $(z^2 + z)(t^4 + t + z^2 + z) + 1 = 0$, that is, $\bar{\mathcal{X}}$ is the non-singular model of the projective irreducible plane curve $\bar{\mathcal{C}}$ with equation

$$\left(X^2 + XZ\right)\left(Y^4 + YZ^3 + X^2Z^2 + XZ^3\right) + Z^4 = 0.$$

From computations performed by MAGMA, $\bar{\mathcal{X}}$ has exactly 28 $\mathbb{F}_{16}$-rational points. Since $\bar{\mathcal{X}}$ has genus 5, Nakajima's bound yields that $|\bar{S}| \leq 16$. Actually, the bound is attained as MAGMA computations show that $\mathrm{Aut}(\bar{\mathcal{X}})$ contains the following three $\mathbb{K}$-automorphisms, where μ is a primitive element of $\mathbb{F}_{16}$:

$$\begin{aligned}
\psi_1 &= (X, Y, Z) \to \big(XY^2 + X^2Z + XYZ + \mu^{10}Y^2Z + XZ^2 + \mu^5YZ^2 + \mu^5Z^3,\\
&\qquad XY^2 + X^2Z + XYZ + \mu^{10}Y^2Z + \mu^{10}YZ^2 + \mu^5Z^3, Y^2Z + YZ^2 + Z^3\big);\\
\psi_2 &= (X, Y, Z) \to (X, Y + Z, Z);\\
\psi_3 &= (X, Y, Z) \to (X + Z, Y + Z, Z).
\end{aligned}$$

They generate indeed a subgroup $\bar{S}$ of order 16. More precisely, $\langle\psi_1, \psi_2\rangle$ is a dihedral group D_4 of order 8 and ψ_3 generates a cyclic group C_2 of order 2 so that $\bar{S} = D_4 \times C_2$. The central involutions in $\bar{S}$ are three, namely ψ_3,

$$\psi_4 = (X, Y, Z) \to \left(Y^2 + XZ + YZ + Z^2, YZ + Z^2, Z^2\right)$$

and

$$\psi_5 = (X, Y, Z) \to \left(Y^2 + XZ + YZ, YZ, Z^2\right).$$

Neither ψ_3 nor ψ_4 have fixed point on $\mathcal{X}$ while ψ_5 does have four, namely

$$P_1 = \left(\mu^5, 1, 1\right), \qquad P_2 = \left(\mu^{10}, 1, 1\right), \qquad P_3 = (\mu, 0, 1), \qquad P_4 = \left(\mu^{10}, 0, 1\right).$$

Furthermore, $\bar{S}$ has two orbits on the set of $\mathbb{F}_{16}$-rational points of $\bar{\mathcal{X}}$, of sizes $\ell_1 = 8$ and $\ell_2 = 4$. From Lemma 3.6, both ψ_3 and ψ_4 are inductive involutions of $\bar{S}$.

The quotient curve $\bar{\bar{\mathcal{X}}}_3 = \bar{\mathcal{X}}/\langle\psi_5\rangle$ is an elliptic curve. This follows from (3) applied to $\bar{\mathcal{X}}$ and its $\mathbb{K}$-automorphism group $\langle\psi_5\rangle$.

Therefore, the central involution ψ_5 of $\bar{S}$ is not inductive, and $\bar{\mathcal{X}}$ provides an example for case (ib) of Theorem 1.2.

The quotient curve $\bar{\bar{\mathcal{X}}}_1 = \bar{\mathcal{X}}/\langle\psi_3\rangle$ has genus and 2-rank 3, and equation

$$X^4 + X^2Y^2 + Y^4 + X^2YZ + XY^2Z + X^2Z^2 + XYZ^2 + YZ^3 = 0.$$

Hence $\bar{\bar{\mathcal{X}}}_1$ is a non-singular plane quartic. Also, $\bar{\bar{S}}_1 = \bar{S}/\langle\psi_3\rangle$ is a dihedral group of order 8. This shows that Nakajima's bound is attained by $\bar{\bar{\mathcal{X}}}_1$. As we have already pointed out, ψ_3 is an inductive central involution of $\bar{S}$ as it fixes no point of $\mathcal{X}$. This can also be shown using the fact that $\mathrm{Aut}(\bar{\bar{\mathcal{X}}}_1)$ is the projective group $PSL(2,7)$ and that a dihedral subgroup of $PSL(2,7)$ of order 8 is known to fix no point in the plane. Therefore $\bar{\mathcal{X}}$ is an example for case (iii) in Theorem 1.2, and also illustrates Remark 4.2 with a dihedral group.

The quotient curve $\bar{\bar{\mathcal{X}}}_2 = \bar{\mathcal{X}}/\langle\psi_4\rangle$ is a hyperelliptic curve of genus 3 and 2-rank 3, defined by the affine equation

$$Y^2 + \left(\mu^{10}X^4 + X^3 + 1\right)Y = \mu^{13}X^8 + \mu^5X^7 + \mu^3X^6 + \mu^3X^5 + \mu^{14}X^4 + \mu^7X^3 + \mu^{11}X^2 + X + 1,$$

and $\bar{\bar{S}}_2 = \bar{S}/\langle\psi_4\rangle$ is an elementary abelian group of order 8. As we have already observed, ψ_4 is an inductive central involution. This can also be shown ruling out the possibility that $\bar{\bar{S}}_2$ fixes a point of $\bar{\bar{\mathcal{X}}}_1$. For this purpose, assume on the contrary the existence of a point $P \in \bar{\bar{\mathcal{X}}}_2$ fixed by $\bar{\bar{S}}_2$. We show that there exists another fixed point $P' \in \bar{\bar{\mathcal{X}}}_1$ of $\bar{\bar{S}}_2$. Observe that $\bar{\bar{\mathcal{X}}}_2$ is defined over $\mathbb{F}_{16}$. Furthermore, it has exactly 30 $\mathbb{F}_{16}$-rational points. So, if P is an $\mathbb{F}_{16}$-rational point, $\bar{\bar{S}}_2$ induces a permutation group on the set of the remaining 29 $\mathbb{F}_{16}$-rational points. As 29 is an odd number, $\bar{\bar{S}}_2$ must fix some of those points, and P' may be any of them. If P is not defined over $\mathbb{F}_{16}$, the Frobenius image of P can be taken for P'. Now, (3) applied to $\bar{\bar{S}}_2$ gives $2 \geq 8(-1) + 14$, a contradiction. Therefore $\bar{\bar{\mathcal{X}}}_2$ is another example for case (iii) in Theorem 1.2, and also illustrates Remark 4.2 with an elementary abelian group.

6.6. Example of a curve of genus $\mathfrak{g}$ with a semi-dihedral $\mathbb{K}$-automorphism group of order $2(\mathfrak{g}-1)$

For a primitive element μ of $\mathbb{F}_{16}$, let $\mathcal{X}$ be a non-singular model of the irreducible plane curve defined with an affine equation $F(X,Y) = f_1(X)Y^4 + f_2(X)Y^2 + f_3(X)Y + f_4(X)$ where

$$f_1(X) = X^{70} + \mu^{14}X^{66} + \mu^9 X^{62} + \mu^{10}X^{58} + \mu^{12}X^{54} + \mu^5 X46 + \mu^7 X^{42} + \mu^{13}X^{38} + \mu^2 X^{30} + \mu^9 X^{26} + \mu^{10}X^{22} + X^{18} + \mu^{11}X^{10} + \mu^6 X^6;$$

$$f_2(X) = X^{72} + X^{70} + \mu^{14}X^{68} + \mu^{13}X^{66} + \mu X^{64} + \mu^{14}X^{62} + X^{60} + \mu^{13}X^{58} + X^{56} + \mu^5 X^{54} + \mu X^{52} + X^{50} + \mu^5 X^{48} + \mu^5 X^{46} + \mu^{11}X^{44} + \mu^{13}X^{42} + \mu^9 X^{40} + X^{38} + \mu^8 X^{36} + \mu^3 X^{34} + \mu^{12}X^{32} + \mu^7 X^{30} + \mu^9 X^{28} + \mu^8 X^{26} + \mu^{10}X^{24} + \mu^9 X^{22} + \mu^5 X^{20} + \mu^2 X^{18} + \mu^3 X^{16} + \mu^2 X^{14} + \mu^5 X^{12} + \mu^8 X^{10} + \mu^{11}X^8 + \mu^6 X^6 + \mu^7 X^4$$

$$f_3(X) = X^{72} + \mu^{14}X^{68} + \mu^2 X^{66} + \mu X^{64} + \mu^4 X^{62} + X^{60} + \mu^9 X^{58} + X^{56} + \mu^{14}X^{54} + \mu X^{52} + X^{50} + \mu^5 X^{48} + \mu^{11}X^{44} + \mu^5 X^{42} + \mu^9 X^{40} + \mu^6 X^{38} + \mu^8 X^{36} + \mu^3 X^{34} + \mu^{12}X^{32} + \mu^{12}X^{30} + \mu^9 X^{28} + \mu^{12}X^{26} + \mu^{10}X^{24} + \mu^{13}X^{22} + \mu^5 X^{20} + \mu^8 X^{18} + \mu^3 X^{16} + \mu^2 X^{14} + \mu^5 X^{12} + \mu^7 X^{10} + \mu^{11}X^8 + \mu^7 X^4;$$

$$f_4(X) = X^{76} + \mu^5 X^{74} + \mu^7 X^{72} + \mu^3 X^{70} + \mu^9 X^{68} + \mu^{12}X^{66} + \mu^6 X^{64} + \mu^{12}X^{62} + \mu^3 X^{60} + \mu^9 X^{58} + \mu^{10}X^{56} + \mu^{12}X^{54} + \mu^{12}X^{52} + \mu^{10}X^{50} + \mu X^{48} + \mu^6 X^{46} + \mu^5 X^{44} + \mu^3 X^{42} + \mu^{12}X^{40} + \mu^{14}X^{38} + \mu^{13}X^{36} + \mu^{14}X^{34} + \mu^3 X^{32} + \mu^6 X^{30} + \mu^4 X^{28} + \mu^1 3X^{26} + \mu^6 X^{24} + X^2 2 + \mu^{12}X^{20} + \mu^2 X^{18} + \mu^3 X^{16} + \mu^{10}X^{14} + \mu^6 X^{12} + X^{10} + \mu^{12}X^6 + \mu^6 X^4 + \mu^{13}X^2 + \mu^9.$$

From MAGMA computation, $\mathcal{X}$ has genus 17 and its 2-rank equals 9. Further, $\mathcal{X}(\mathbb{F}_{16})$, the set of all $\mathbb{F}_{16}$-rational points of $\mathcal{X}$, has size 8: all of them are branches centered at Y_∞, while the $\mathbb{F}_{16}$-automorphism group G of $\mathcal{X}$ is a semi-dihedral group of order 32 with the unique central involution $u : (X, Y) \to (X, Y + 1)$. In particular, u is the unique involution of the cyclic subgroup of G of order 16 and fixes $\mathcal{X}(\mathbb{F}_{16})$ pointwise. From (3), u fixes no more points on $\mathcal{X}$.

The function field of the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/\langle u\rangle$ is the subfield $\mathbb{K}(\bar{\mathcal{X}}) = \mathbb{K}(x, z = y^2 + y)$ of $\mathbb{K}(\mathcal{X})$ and hence $\bar{\mathcal{X}}$ is a non-singular model of the plane algebraic curve with affine equation

$$Z^2 + \big(f_1(X) + f_2(X)\big)Z + f_4(X) = 0.$$

Actually, $\bar{\mathcal{X}}$ is an elliptic curve. Therefore, the central involution e is not inductive.

Finally, comparison with Nakajima's bound $|\operatorname{Aut}(\mathcal{X})| \le 4(\gamma - 1) \le 32$ shows that $G = \operatorname{Aut}(\mathcal{X})$.

References

[1] A.A. Albert, Cyclic fields of degree p^n over F of characteristic p, Bull. Amer. Math. Soc. 40 (1934) 625–631.
[2] A.A. Albert, On cyclic fields, Trans. Amer. Math. Soc. 37 (1935) 452–462.
[3] G. Frey, On the structure of the class group of a function field, Arch. Math. 33 (1979/80) 33–40.
[4] M. Giulietti, G. Korchmáros, Large 2-groups of automorphisms of curves with positive 2-rank, arXiv:1104.5159v1 [math.AG], 2011.
[5] M. Giulietti, G. Korchmáros, Large 3-groups of automorphisms of algebraic curves in characteristic 3, arXiv:1312.5108 [math.AG], 2013.
[6] M. Giulietti, G. Korchmáros, Algebraic curves with a large non-tame automorphism group fixing no point, Trans. Amer. Math. Soc. 362 (2010) 5983–6001.
[7] M. Giulietti, G. Korchmáros, Automorphism groups of algebraic curves with p-rank zero, J. Lond. Math. Soc. (2) 81 (2010) 277–296.
[8] J.W.P. Hirschfeld, G. Korchmáros, F. Torres, Algebraic Curves Over a Finite Field, Princeton Univ. Press, Princeton and Oxford, 2008, xx+696 pp.
[9] B. Huppert, Endliche Gruppen. I, Grundlehren Math. Wiss., vol. 134, Springer, Berlin, 1967, xii+793 pp.
[10] S. Lang, Algebra, Grad. Texts in Math., vol. 211, Springer, New York, 2002, xvi+914 pp.
[11] C. Lehr, M. Matignon, Automorphism groups for p-cyclic covers of the affine line, Compos. Math. 141 (2005) 1213–1237.
[12] M. Matignon, M. Rocher, On smooth curves endowed with a large automorphism p-group in characteristic $p > 0$, Algebra Number Theory 2 (2008) 887–926.
[13] S. Nakajima, p-ranks and automorphism groups of algebraic curves, Trans. Amer. Math. Soc. 303 (1987) 595–607.
[14] R. Pries, K. Stevenson, A survey of Galois theory of curves in characteristic p, in: WIN – Women in Numbers, in: Fields Inst. Commun., vol. 60, Amer. Math. Soc., Providence, RI, 2011, pp. 169–191.
[15] M. Rocher, Large p-groups actions with a p-elementary abelian second ramification group, J. Algebra 321 (2009) 704–740.
[16] M. Rocher, Large p-groups actions with $|G|/g^2 > 4/(p^2-1)^2$, arXiv:0801.3494v1 [math.AG], 2008.
[17] H. Stichtenoth, Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. I. Eine Abschätzung der Ordnung der Automorphismengruppe, Arch. Math. 24 (1973) 527–544.
[18] J.-P. Serre, Local Fields, Grad. Texts in Math., vol. 67, Springer, New York, 1979, viii+241 pp.
[19] H. Stichtenoth, Algebraic Function Fields and Codes, 2nd edition, Springer, 2009.
[20] F. Sullivan, p-torsion in the class group of curves with many automorphisms, Arch. Math. 26 (1975) 253–261.
[21] M. Suzuki, A characterization of the simple group $LF(2,p)$, J. Fac. Sci., Univ. Tokyo 6 (1951) 259–293.
[22] E. Witt, Der Existenzsatz für abelsche Funktionenkörper, J. Reine Angew. Math. 173 (1935) 43–51.
[23] E. Witt, Konstruktion von galoischen Körpern der Characteristik p zu vorgegebener Gruppe der Ordnung p^f, J. Reine Angew. Math. 174 (1936) 237–245.