Math.Comput.Sci. (2023) 17:21
https://doi.org/10.1007/s11786-023-00571-w

Mathematics in Computer Science

# Efficient Search for Superspecial Hyperelliptic Curves of Genus Four with Automorphism Group Containing $C_6$

**Momonari Kudo · Tasuku Nakagawa · Tsuyoshi Takagi**

Received: 13 October 2022 / Accepted: 10 May 2023 / Published online: 1 September 2023


**Abstract** In arithmetic and algebraic geometry, superspecial (s.sp. for short) curves are one of the most important objects to be studied, with applications to cryptography and coding theory. If $g \geq 4$, it is not even known whether there exists such a curve of genus $g$ in general characteristic $p > 0$, and in the case of $g = 4$, several computational approaches to search for those curves have been proposed. In the genus-4 hyperelliptic case, Kudo-Harashita proposed a generic algorithm to enumerate all s.sp. curves, and recently Ohashi-Kudo-Harashita presented an algorithm specific to the case where automorphism group contains the Klein 4-group as a subgroup. In this paper, we propose an algorithm with complexity $\tilde{O}(p^4)$ in theory but $\tilde{O}(p^3)$ in practice to enumerate s.sp. hyperelliptic curves of genus 4 with automorphism group containing the cyclic group of order 6. By executing the algorithm over Magma, we enumerate those curves for $p$ up to 1000. We also succeeded in finding a s.sp. hyperelliptic curve of genus 4 in every $p$ with $p \equiv 2 \pmod 3$.

**Keywords** Algebraic curves · Hyperelliptic curves · Curves of genus four · Superspecial curves · Automorphism groups

**Mathematics Subject Classification** 11G20 · 14G15 · 14H25 · 14H37 · 14H45 · 14Q05 · 14Q25

## 1 Introduction

Throughout, all the complexities are measured by the number of arithmetic operations in $\mathbb{F}_{p^2}$ for a prime $p$, unless otherwise noted. Soft-O notation $\tilde{O}$ omits logarithmic factors, namely we write $f(n) = \tilde{O}(g(n))$ if $f(n) =$

M. Kudo (✉)
Department of Information and Communication Engineering, Faculty of Information Engineering, Fukuoka Institute of Technology, Fukuoka, Japan
e-mail: m-kudo@fit.ac.jp

T. Nakagawa
Department of Mathematical Engineering and Information Physics, School of Engineering, The University of Tokyo, Tokyo, Japan
e-mail: nakagawa-tasuku705@g.ecc.u-tokyo.ac.jp

T. Takagi
Department of Mathematical Informatics, Graduate School of Information Science and Technology, The University of Tokyo, Tokyo, Japan
e-mail: takagi@mist.i.u-tokyo.ac.jp

$g(n)\log^k n$ for some $k$. A curve means a non-singular projective variety of dimension one. Let $K$ be a field of characteristic $p > 0$, and $\overline{K}$ its algebraic closure. A curve $C$ of genus $g$ over $K$ is said to be *superspecial* (*s.sp.* for short) if its Jacobian variety is isomorphic to a product of supersingular elliptic curves. S.sp. curves are of course important objects in theory, but also in practical applications such as cryptography using algebraic curves, see e.g., [5], where s.sp. genus-2 curves are used to construct Hash function.

Given a pair $(g, p)$, only finite s.sp. curves of genus $g$ over $\overline{\mathbb{F}_p}$ exist, and the problem of finding or enumerating them is known to be classically important. For the field of definition, the most important case is $\mathbb{F}_{p^2}$, since any s.sp. curve over $K$ is $\overline{K}$-isomorphic to one over $\mathbb{F}_{p^2}$, see the proof of [8, Theorem 1.1]. For $g \leq 3$, the problem is solved for all $p > 0$, based on the theory of principally polarized abelian varieties. Specifically, for $g = 1$ (resp. 2 and 3), Deuring [6] (resp. Ibukiyama-Katsura-Oort [18, Theorem 2.10]) showed that the number of $\overline{\mathbb{F}_p}$-isomorphism classes of s.sp. curves is determined by computing the class numbers of a quaternion algebra (resp. quaternion hermitian lattices). These class numbers were computed in [7] (resp. [16], [15]) for $g = 1$ (resp. 2, 3).

On the other hand, the problem for $g \geq 4$ has not been solved in all primes, but in recent years, Kudo-Harashita developed several algorithms to count genus-4 or 5 s.sp. curves [21], [22], [24]. In particular, an algorithm for enumerating s.sp. *hyperelliptic* curves of genus 4 was proposed in [22] and [23], but is practical only for small $p$ (in fact $p \leq 23$), due to the cost of solving multivariate systems (cf. Sect. 2.4 below). Recently, Ohashi-Kudo-Harashita [34] (resp. Kudo-Harashita-Howe [25]) presented an algorithm for enumerating s.sp. hyperelliptic (resp. non-hyperelliptic) curves of genus 4 with automorphism group containing a subgroup isomorphic to the Klein 4-group $\mathbf{V}_4 = \mathbf{C}_2 \times \mathbf{C}_2$, with complexity $O(p^3)$ (resp. $\tilde{O}(p^4)$), where $\mathbf{C}_n$ denotes the cyclic group of order $n$. They also succeeded in enumerating such s.sp. curves for every prime $p$ up to 200.

This paper proposes a more efficient algorithm than [22] to produce s.sp. hyperelliptic curves of genus 4, which is practical for $p$ extremely larger than some number mentioned in [22]. For this, we focus on a family of hyperelliptic curves given by $H_{a,b} : y^2 = f_{a,b}(x) := x^{10} + x^7 + ax^4 + bx$, where $a, b \in \mathbb{F}_{p^2}$. This kind of a curve appears as a s.sp. curve over $\mathbb{F}_{17^2}$ enumerated in [22] (see also Table 2 in Sect. 2.4 below), and it tends to be s.sp. from our preliminary computation; by exhaustive search for $(a, b)$, we confirmed that there exists (resp. does not exist) $(a, b)$ such that $H_{a,b}$ is s.sp. for any $17 \leq p < 100$ with $p \equiv 2 \bmod 3$ (resp. $p \equiv 1 \bmod 3$). We also note that the full (resp. reduced) automorphism group of $H_{a,b}$ contains a subgroup isomorphic to $\mathbf{C}_6$ (resp. $\mathbf{C}_3$), see Theorem 2.1.5 for a complete classification of reduced and full automorphism groups of hyperelliptic curves of genus 4. Note that the proof of Theorem 2.1.5 is given in the appendix of the preprint version of this paper [26]. With this classification, we see that our family $H_{a,b}$ is included in the cases **3**, **7**, and **9** of Table 1, while Ohashi-Kudo-Harashita's recent work [34] treats the cases **2-1**, **4-1**, **5**, **6**, **8**, and **10** of the table. A relationship between $H_{a,b}$ and the family $C_{A,B} : y^2 = x^{10} + Ax^7 + Bx^4 + x$ in the cases **3**, **7**, and **9** of Table 1 will be described in Sect. 3.1 below.

Here, main results of this paper are summarized in Theorems A and B below.

**Theorem A** *There exists an algorithm (Main Algorithm in Theorem 4.1.1) with complexity $\tilde{O}(p^4)$ to enumerate the $\overline{\mathbb{F}_p}$-isomorphism classes of all s.sp. $H_{a,b}$'s with $a, b \in \mathbb{F}_{p^2}$. Assuming the gcd of resultants appearing in the algorithm has degree $O(p)$, the complexity becomes $\tilde{O}(p^3)$.*

While the outline of our algorithm is same as that of our previous algorithm in [22], we shall develop various computational techniques specific to our family $H_{a,b}$. Specifically, we prove in Lemma 3.2.1 that the Cartier-Manin matrix $M_{a,b}$ of $H_{a,b}$ with *parameters* $a$ and $b$ can be computed very efficiently, in $O(p^3)$, only with linear algebra. We then solve the equation $M_{a,b} = 0$ in $\tilde{O}(p^4)$ with bivariate resultants, where the complexity becomes $\tilde{O}(p^3)$ assuming the gcd of computed resultants has degree $O(p)$; we see from our computational results that this assumption is practical. To make isomorphism classification of s.sp. $H_{a,b}$'s obtained as above efficient, we also present some criteria. For instance, it will be proved in Lemma 3.1.1 that two curves $H_{a,b}$ and $H_{a',b'}$ with reduced automorphism groups $\mathbf{C}_3$ or $\mathbf{C}_9$ are isomorphic, then $(a, b) = (a', b')$. These criteria reduce the cost of isomorphism classification from $O(p^4)$ to $O(p^2)$ (in practice $O(p)$).

By implementing and executing our algorithm on Magma [1], we succeeded in enumerating s.sp. $H_{a,b}$'s with $a, b \in \mathbb{F}_{p^2}$ up to isomorphisms over $\overline{\mathbb{F}_p}$ for every prime $p$ between 17 and 1000. More precisely, we obtain the following computational results:

**Theorem B** *For every prime $p$ with $17 \leq p < 1000$, the number of $\overline{\mathbb{F}_p}$-isomorphism classes of s.sp. $H_{a,b}$'s with $a, b \in \mathbb{F}_{p^2}$ are summarized in Table 3 below. In particular, for each $17 \leq p < 1000$ with $p \equiv 2 \bmod 3$ (resp. $p \equiv 1 \bmod 3$), there exists (resp. does not exist) $(a, b) \in \mathbb{F}_{p^2}^2$ such that $H_{a,b}$ is a s.sp. hyperelliptic curve.*

The upper bound on $p$ in Theorem B is much larger than those of [22] and [23], and it can be increased easily; for instance, on a PC with macOS Monterey 12.0.1, at 2.6 GHz CPU 6 Core (Intel Core i7) and 16GB memory, it took 6,300 s (about 1.75 h) in total for computing the $\overline{\mathbb{F}_p}$-isomorphicm classes of s.sp. $H_{a,b}$'s with $a, b \in \mathbb{F}_{p^2}$ for all $17 \leq p < 1000$, and the execution time for $p = 997$ was only 195 seconds.

The rest of this paper is organized as follows. Section 2 is devoted to preliminaries, where we review some known facts on hyperelliptic curves and their automorphisms, Cartier-Manin matrices, and enumeration results in [22], [23] on s.sp. hyperelliptic curves. Section 3 studies our parametric family $H_{a,b} : y^2 = x^{10} + x^7 + ax^4 + bx$. In Sect. 4, we present the main algorithm and computational results. Section 5 is conclusion.

## 2 Preliminaries

This section reviews some known facts on hyperelliptic curves and their automorphisms, and recalls the definition of Cartier-Manin matrices and the superspeciality of curves. In particular, a classification of hyperelliptic curves of genus 4 in terms of automorphism groups will be recalled in Sect. 2.1. In Sect. 2.2, we will describe a method to compute the Cartier-Manin matrix of a hyperelliptic curve. Section 2.3 briefly reviews Elkin's results [9] on the rank of the Cartier operator of a cyclic cover. In Sect. 2.4, we also review Kudo-Harashita's algorithm [22], [23] to enumerate superspecial hyperelliptic curves, and their enumeration results.

Let $K$ be a field of characteristic $p$ with $p \neq 2$, and $k = \overline{K}$ its algebraic closure. For $n \geq 2$, we denote respectively by $\mathbf{C}_n$, $\mathbf{D}_n$, $\mathbf{A}_n$, $\mathbf{V}_4$, and $\mathbf{Q}_8$ the cyclic group of order $n$, the dihedral group of order $2n$, the alternating group of order $n!/2$, the Klein 4-group $\mathbf{C}_2 \times \mathbf{C}_2$, and the quaternion group.

### 2.1 Hyperelliptic Curves and Their Isomorphisms

For a curve $C$ of genus $g \geq 2$ over $K$, let $\mathrm{Aut}_K(C)$ denote the automorphism group of $C$ over $K$, and $\mathrm{Aut}_k(C)$ is denoted simply by $\mathrm{Aut}(C)$. It is well-known that $\mathrm{Aut}(C)$ is finite for an arbitrary $C$, and has size $\leq 16g^4$ unless $C$ is a Hermitian curve [38]. If the characteristic of $K$ exceeds $g + 1$, we have a quite more strong bound $\mathrm{Aut}(C) \leq 84(g-1)$, see [35]. A *hyperelliptic curve* $H$ over $K$ is a curve $H$ over $K$ admitting a degree-2 morphism over $K$ from $H$ to the projective line $\mathbb{P}^1_k$. Let $\iota$ be the *hyperelliptic involution* of $H$, that is, the unique involution over $k$ on $C$ such that the quotient curve $C/\langle\iota\rangle$ is rational. We call the quotient group $\overline{\mathrm{Aut}}(H) := \mathrm{Aut}(H)/\langle\iota\rangle$ the *reduced automorphism group* of $H$, while $\mathrm{Aut}(H)$ and $\mathrm{Aut}_K(H)$ are often called *full* automorphism groups.

A typical way to represent a hyperelliptic curve $H$ explicitly is realizing it as the desingularization of the projective closure of an affine plane curve $y^2 = f(x)$, where $f(x) \in k[x]$ is a separable polynomial of degree $2g + 1$ or $2g + 2$. In this situation, we simply write $H : y^2 = f(x)$, and call the equation $y^2 = f(x)$ a (hyperelliptic) equation of $H$. We can also write down an equation of $H$ in terms of a field $K$ of definition for $H$:

**Lemma 2.1.1** ( [22, Lemma 2]) *Let $H$ be a hyperelliptic curve of genus $g$ over $K$. Assume that $p$ and $2g + 2$ are coprime, and let $\varepsilon \in K^\times \setminus (K^\times)^2$. Then $H$ is birational to the projective closure of*

$$cy^2 = f(x) = x^{2g+2} + bx^{2g} + a_{2g-1}x^{2g-1} + \cdots + a_1 x + a_0, \tag{2.1.1}$$

*where $a_i \in K$ for $0 \leq i \leq 2g - 1$, and where $b = 0, 1, \varepsilon$ and $c = 1, \varepsilon$.*

The following lemma gives a criterion to test whether two hyperelliptic curves over $K$ are $K$-isomorphic to each other, or not:

**Lemma 2.1.2** ( [28, Section 1.2] or [22, Lemma 1]) *Let $H_i : c_i y^2 = f_i(x)$ be hyperelliptic curves of genus $g$ over $K$ for $i = 1$ and 2, where $c_i y^2 = f_i(x)$ is of the form (2.1.1). For any $K$-isomorphism $\sigma : H_1 \to H_2$, there exists $(P, \lambda) \in \mathrm{GL}_2(K) \times K^\times$ with*

$$P = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

*such that*

$$\sigma(x, y) = \left( \frac{\alpha x + \beta}{\gamma x + \delta}, \frac{\lambda y}{(\gamma x + \delta)^{g+1}} \right)$$

*for all $(x, y)$ on $H_1$. The representation of $\sigma$ is unique up to the equivalence $(P, \lambda) \sim (\mu P, \mu^{g+1}\lambda)$ for $\mu \in K^\times$.*

*Remark 2.1.3* Considering a hyperelliptic curve $H : y^2 = f(x)$ over an algebraically closed field $k$, we may assume that the coefficients of the highest and lowest degree terms in $f(x)$ are 1. Indeed, writing $f(x) = \sum_{i=s}^{d} a_i x^i$ with $d = 2g + 1, 2g + 2$, $s = 0, 1$, $a_d \neq 0$, and $a_s \neq 0$, an isomorphism $(x, y) \mapsto \left( \frac{\alpha x}{\delta}, \frac{y}{\delta^{g+1}} \right)$ transforms $y^2 = f(x)$ into $y^2 = \sum_{i=s}^{d} a_i \alpha^i \delta^{2g+2-i} x^i$ choosing $\alpha$ and $\delta$ so that $a_d \alpha^d \delta^{2g+2-d} = 1$ and $a_s \alpha^s \delta^{2g+2-s} = 1$, as desired.

As a particular case of Lemma 2.1.2, any $K$-automorphism of a hyperelliptic curve $H$ of genus $g$ over $K$ can be represented by $(P, \lambda) \in \mathrm{GL}_2(K) \times K^\times$ as in the lemma. Based on this, we can compute automorphisms of a given $H$ by e.g., the Gröbner basis computation with help of computer calculation (cf. [31] and [23, Section 4]). For instance, the computer algebra system Magma [1] has the function `AutomorphismsOfHyperellipticCurve` implemented by Lercier-Sijsling-Ritzenthaler [31]. Once all $K$-automorphisms of $H$ are computed, the group structure of $\mathrm{Aut}_K(H)$ can be also determined.

When $K$ is algebraically closed, namely $k = K$, possible finite groups isomorphic to $\mathrm{Aut}(H)$ can be determined from ones isomorphic to the *reduced* automorhism group $\overline{\mathrm{Aut}}(H)$, which is canonically embedded into the projective linear group $\mathrm{PGL}_2(k)$ (see e.g., [32, Section 2.2] for an explicit description). Indeed, in the case of characteristic zero, Shaska [36], [37] applied a classification of finite subgroups of $\mathrm{PGL}_2$ to determining possible types of $\overline{\mathrm{Aut}}(H)$, and then he also found an equation (in reduced form) defining $H$ for each type and the structure of $\mathrm{Aut}(H)$, with the action of elements in $\overline{\mathrm{Aut}}(H)$ as matrices. His idea can be applied to the positive characteristic case, with carefully considering some exceptional cases depending on $p$ and $g$ such as the existence of $p$-subgroups of $\mathrm{PGL}_2$. For the case of genus 2, 3, and 4, explicit classifications in characteristic $p$ are given in [19] (and [18]), [30, Table 2], and [24, Table 6] respectively.

We here recall the classification in the case where $g = 4$. A key ingredient for the classification is the fact (this is noted in [12, Section 2] without proof) that any automorphism $\sigma$ of a hyperelliptic curve is represented by $\mathrm{diag}(\mu, 1) \in \mathrm{GL}_2(k)$ for a primitive $\ell$-th root $\mu$ of unity with $\ell = \mathrm{ord}(\sigma)$ (the order of $\sigma$ as an element of $\overline{\mathrm{Aut}}(H)$), if $\ell$ is coprime to the characteristic of $k$. An explicit proof of this fact is given in [32], and we here state assertions only:

**Proposition 2.1.4** ( [32, Proposition 2.2.2]) *Let $H$ be a hyperelliptic curve of genus $g$ over an algebraically closed field $k$, and $\ell$ a positive integer coprime to* $\mathrm{char}(k)$. *Assume that $\sigma$ has order $\ell$ in the reduced automorphism group of $H$. Then there exists a hyperelliptic curve $H' : y^2 = f(x)$ over $k$ and an isomorphism $\rho : H' \to H$ such that the automorphism $\rho^{-1}\sigma\rho$ of $H'$ is represented by* $(\mathrm{diag}(\mu, 1), \mu') \in \mathrm{GL}_2(k) \times k^\times$, *where $\mu$ is a primitive $\ell$-th root of* 1, *and where $\mu'$ is an element satisfying $(\mu')^\ell = 1$ or $-1$. We also have $\mu' = \pm\mu^{g+1}$ if $\deg(f) = 2g + 2$, and $\mu' = \pm\sqrt{\mu^{2g+1}}$ if $\deg(f) = 2g + 1$. Moreover, $\sigma$ is the hyperelliptic involution (i.e., $\ell = 1$) if and only if $\mu = 1$.*

Based on this proposition together with the classification of subgroups of $\mathrm{PGL}_2(k)$, we can determine possible finite groups isomorphic to the reduced automorphism groups of hyperelliptic curves over $k$ of given genus $g$. In the case where $g = 4$, we can prove the following theorem:

**Table 1** Possible finite groups isomorphic to $\overline{\mathrm{Aut}}(H)$ for hyperelliptic curves $H$ of genus 4 over an algebraically closed field $k$ of characteristic $p \geq 7$, and hyperelliptic equations $y^2 = f(x)$ defining $H$, where $A, B, C, D \in k$

| Type | $\overline{\mathrm{Aut}}(H)$ | $\#\overline{\mathrm{Aut}}(H)$ | $y^2 = f(x)$ birational to $H$ | $\mathrm{Aut}(H)$ | $\#\mathrm{Aut}(H)$ |
|---|---|---|---|---|---|
| **1** | $\{0\}$ | 1 | $y^2 =$ (square-free polynomial in $x$ of degree 9 or 10) | $\mathbf{C}_2$ | 2 |
| **2-1** | $\mathbf{C}_2$ | 2 | $y^2 = x^{10} + Ax^8 + Bx^6 + Cx^4 + Dx^2 + 1$ | $\mathbf{V}_4$ | 4 |
| **2-2** | $\mathbf{C}_2$ | 2 | $y^2 = x^9 + Ax^7 + Bx^5 + Cx^3 + x$ | $\mathbf{C}_4$ | 4 |
| **3** | $\mathbf{C}_3$ | 3 | $y^2 = x^{10} + Ax^7 + Bx^4 + x$ | $\mathbf{C}_6$ | 6 |
| **4-1** | $\mathbf{V}_4$ | 4 | $y^2 = x^{10} + Ax^8 + Bx^6 + Bx^4 + Ax^2 + 1$, or | $\mathbf{D}_4$ | 8 |
| | | | $y^2 = x^9 + Ax^7 + Bx^5 + Ax^3 + x$ | | 8 |
| **4-2** | $\mathbf{V}_4$ | 4 | $y^2 = x(x^4 - 1)(x^4 + Ax^2 + 1)$ | $\mathbf{Q}_8$ | 8 |
| **5** | $\mathbf{D}_4$ | 8 | $y^2 = x^9 + Ax^5 + x$ | $\mathbf{D}_8$ | 16 |
| **6** | $\mathbf{D}_5$ | 10 | $y^2 = x^{10} + Ax^5 + 1$ | $\mathbf{D}_{10}$ | 20 |
| **7** | $\mathbf{A}_4$ | 12 | $y^2 = x(x^4 - 1)(x^4 + 2\sqrt{-3}x^2 + 1)$ | $\mathrm{SL}_2(\mathbb{F}_3)$ | 24 |
| **8** | $\mathbf{D}_8$ | 16 | $y^2 = x^9 + x$ | $\mathbf{C}_{16} \rtimes \mathbf{C}_2$ | 32 |
| **9** | $\mathbf{C}_9$ | 9 | $y^2 = x^{10} + x$ | $\mathbf{C}_{18}$ | 18 |
| **10** | $\mathbf{D}_{10}$ | 20 | $y^2 = x^{10} + 1$ | $\mathbf{C}_5 \rtimes \mathbf{D}_4$ | 40 |

**Theorem 2.1.5** ( [26, Theorem C]) *Assume that $p \geq 7$. The reduced automorphism group $\overline{\mathrm{Aut}}(H)$ of a hyperelliptic curve $H$ of genus 4 over an algebraically closed field $k$ of characteristic $p$ is isomorphic to either of the 10 finite groups listed in Table 1. In each type of $\overline{\mathrm{Aut}}(H)$, the hyperelliptic curve $H$ is isomorphic to $y^2 = f(x)$ given in the fourth column of Table 1, and the finite group isomorphic to $\mathrm{Aut}(H)$ is provided in the fifth column of the table.*

In particular, the reduced automorphism group contains a subgroup isomorphic to $\mathbf{C}_3$ (or equivalently $\mathrm{Aut}(H)$ contains a subgroup isomorphic to $\mathbf{C}_6$), then it is isomorphic to $\mathbf{C}_3$, $\mathbf{C}_9$ or $\mathbf{A}_4$. Moreover, in each case, $H$ is isomorphic to $y^2 = f(x)$ given as follows:

- $(\overline{\mathrm{Aut}}(H)) \cong \mathbf{C}_3)$ $y^2 = x^{10} + Ax^7 + Bx^4 + x$ for some $A, B \in k$ with $(A, B) \neq (0, 0)$.
- $(\overline{\mathrm{Aut}}(H)) \cong \mathbf{C}_9)$ $y^2 = x^{10} + x$.
- $(\overline{\mathrm{Aut}}(H)) \cong \mathbf{A}_4)$ $y^2 = x(x^4 - 1)(x^4 + 2\sqrt{-3}x^2 + 1)$.

## 2.2 Cartier–Manin Matrices and Superspeciality

In this section, we review how to compute the Cartier-Manin matrix of a hyperelliptic curve.

We start with recalling the definition of the Cartier operator and the Cartier-Manin matrix for a general curve $C$ of genus $g$ over an algebraically closed field $k$ which admits an affine plane model. Assume for simplicity that $C$ is birational to an affine plane (possibly singular) curve $F(x, y) = 0$ in the affine plane $\mathbb{A}^2$ over $k$ with coordinate ring $R{:=}k[x, y]/\langle F\rangle$, where $F$ is an irreducible polynomial over $k$ in $x$ and $y$. We can take $x$ as a separating element, i.e., $x$ is transcendental over $k$, and the function field $k(C)$ is a finite separable extension of $k(x)$. We may identify $k(C)$ and the field of fractions $K{:=}k(x, y)$ for $R$. Under this identification, every regular differential form $\omega \in H^0(C, \Omega^1_C)$ is uniquely written as $\omega = d\phi + \eta^p x^{p-1} dx$ for $\phi, \eta \in k(C)$. Here we define a map

$$\mathscr{C} : H^0(C, \Omega^1_C) \to H^0(C, \Omega^1_C)$$

by $\mathscr{C}(\omega){:=}\eta dx$, and call it the (modified) *Cartier operator* on $H^0(C, \Omega^1_C)$. Moreover, the matrix representing $\mathscr{C}$ with respect to a basis $\mathcal{A}$ for the $g$-dimensional space $H^0(C, \Omega^1_C)$ is called the *Cartier-Manin matrix* of $C$ (with respect to the basis $\mathcal{A}$). We here also recall Nygaard's criterion for superspeciality in terms of the Cartier operator:

**Theorem 2.2.1** ( [33, Theorem 4.1]) *With notation as above, the Jacobian variety $J(C)$ of a curve $C$ is isomorphic to a product of supersingular elliptic curves if and only if $\mathscr{C}$ vanishes.*

In the case where $C$ is hyperelliptic, we have a well-known explicit formula (Lemma 2.2.2 below) by Yui [41] to compute the Cartier-Manin matrix of $C$, and so recall it here. As in the previous subsection, assume that $C$ is a hyperelliptic curve of genus $g$ over $k$ defined by $y^2 = f(x)$, where $f(x)$ is a polynomial in $k[x]$ of degree $2g+1$ or $2g+2$ with no multiple root. First, it is well-known that a basis of $H^0(C, \Omega^1_C)$ is given by

$$\mathcal{A} = \left\{ \omega_j := \frac{x^{j-1}}{y} dx : 1 \leq j \leq g \right\}.$$

Writing $f(x)^{(p-1)/2} = \sum_\ell c_\ell x^\ell$ for $c_\ell \in k$, it follows from $y^{p-1} = f(x)^{(p-1)/2}$ in $k(C)$ that

$$\begin{aligned}\omega_j &= y^{-p} f(x)^{(p-1)/2} x^{j-1} dx \\ &= d\left( y^{-p} \sum_{\substack{\ell \\ j+\ell \not\equiv 0 \pmod p}} \frac{c_\ell}{j+\ell} x^{j+\ell} \right) + \sum_{i \geq 1} c_{ip-j} \frac{x^{(i-1)p}}{y^p} x^{p-1} dx.\end{aligned}$$

Therefore

$$\mathscr{C}(\omega_j) = \sum_{i=1}^{g} c_{ip-j}^{1/p} \omega_i$$

by the definition of the Cartier operator described above, and hence we have the following lemma:

**Lemma 2.2.2** ( [41, Section 2]) *With notation as above, the Cartier-Manin matrix of $C$ is the $g \times g$ matrix whose $(i, j)$-entry is the coefficient $c_{ip-j}$ of $x^{pi-j}$ in $f^{(p-1)/2}$ for $1 \leq i, j \leq g$. Hence, by Theorem 2.2.1, $C$ is superspecial if and only if the coefficients of $x^{pi-j}$ in $f^{(p-1)/2}$ are equal to 0 for all pairs of integers $1 \leq i, j \leq g$.*

*Example 2.2.3* Consider the hyperelliptic curves $H_1 : y^2 = x^{2g+2} + x$, $H_2 : y^2 = x^{2g+1} + x$, and $H_3 : y^2 = x^{2g+2} + 1$ over $\mathbb{F}_p$. The reduced automorphism group of the first curve has a subgroup isomorphic to $\mathbf{C}_{2g+1}$, and those of the second and third ones are isomorphic to $\mathbf{D}_{2g}$ and $\mathbf{D}_{2g+2}$ respectively, by [26, Lemma A.2.1]. Since $(x^{2g+2}+x)^{\frac{p-1}{2}} = \sum_{\ell=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{\ell} x^{(2g+1)\ell + \frac{p-1}{2}}$, the Cartier-Manin matrix of $H_1$ is zero if $ip - j \not\equiv \frac{p-1}{2} \pmod{2g+1}$ for any $1 \leq i, j \leq g$. For instance, if $p \equiv -1 \pmod{2g+1}$, then $H_1$ is superspecial. Similarly, $H_2$ (resp. $H_3$) is superspecial if $p \equiv -1 \pmod{2g}$ (resp. $p \equiv -1 \pmod{2g+2}$).

More strongly, it is proved in [39] that $H_1$ (resp. $H_2$) is $\mathbb{F}_{p^2}$-maximal if and only if $p \equiv -1 \pmod{2g+1}$ (resp. $p \equiv -1, 2g+1 \pmod{4g}$).

Lemma 2.2.2 reduces the computation of the Cartier-Manin matrix of $C : y^2 = f(x)$ into that of $g^2$ (particular) coefficients in the power $f^{(p-1)/2}$. In the case where all the coefficients of $f$ belong to a finite field (there is no parameter in the coefficients), several efficient algorithms to compute the coefficients have been proposed by Bostan-Gaudry-Schost [2], Komoto-Kozaki-Matsuo [20], and Harvey-Sutherland [13], [14]. These algorithms commonly use a linear recurrence by Flajolet-Salvy [11] (described also in e.g., [2, Section 4]) which is used in the general method to compute the power of a given univariate polynomial.

We here recall the recurrence since it will be required to analyze the complexity of our main algorithm. Let $h(x)$ be a univariate polynomial of degree $d$, and let $\frac{dh}{dx}$ denote its derivative with respect to $x$. We also denote by $h_i$ its $x^i$-coefficient for each $0 \leq i \leq d$, say $h(x) = \sum_{i=0}^{d} h_i x^i$. Let $n$ be a positive integer, and we consider to compute the power $h^n$. For each $\ell$ with $0 \leq \ell \leq (n+1)d$, it follows from $h^{n+1} = hh^n$ that

$$(h^{n+1})_\ell = \sum_{j=0}^{d} h_j (h^n)_{\ell - j}, \tag{2.2.1}$$

where $(h^n)_{-d} = (h^n)_{-d+1} = \cdots = (h^n)_{-1} = (h^n)_{nd+1} = (h^n)_{nd+2} = \cdots = (h^n)_{(n+1)d} = 0$. On the other hand, it also follows from $\frac{d}{dx}(h^{n+1}) = (n+1)\frac{dh}{dx} \cdot h^n$ that

$$\ell(h^{n+1})_\ell = (n+1)\sum_{i=0}^{d-1}\left(\frac{dh}{dx}\right)_i (h^n)_{\ell-1-i} = (n+1)\sum_{j=1}^{d} j h_j (h^n)_{\ell-j} \tag{2.2.2}$$

by comparing the $x^{\ell-1}$-coefficient. Multiplying (2.2.1) by $\ell$ and subtracting (2.2.2), we have a linear recurrence

$$\sum_{j=0}^{d}(nj-\ell+j)h_j(h^n)_{\ell-j} = 0, \tag{2.2.3}$$

equivalently,

$$\ell h_0 (h^n)_\ell = \sum_{j=1}^{d}(nj-\ell+j)h_j(h^n)_{\ell-j}.$$

Thus, if both $h_0$ and $\ell$ are not equal to zero in the coefficient ring of $h$, the coefficient $(h^n)_\ell$ is a linear combination of $d$ *lower*-degree coefficients $(h^n)_{\ell-1}, \ldots, (h^n)_{\ell-d}$, say

$$(h^n)_\ell = \sum_{j=1}^{d}\frac{nj-\ell+j}{h_0\ell}h_j(h^n)_{\ell-j}, \tag{2.2.4}$$

and hence

$$U_\ell := \begin{pmatrix} (h^n)_{\ell-d+1} \\ (h^n)_{\ell-d+2} \\ \vdots \\ (h^n)_\ell \end{pmatrix} = A(\ell)U_{\ell-1} = A(\ell)A(\ell-1)\cdots A(1)U_0, \tag{2.2.5}$$

where we set

$$A(\ell) := \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ r_d(\ell) & r_{d-1}(\ell) & \cdots & r_2(\ell) & r_1(\ell) \end{pmatrix}$$

with

$$r_j(\ell) = \frac{(nj-\ell+j)h_j}{h_0\ell}$$

for $1 \le j \le d$ . Note that blank entries in $A(\ell)$ mean zero. Therefore, the coefficients $(h^n)_\ell$ for all $1 \le \ell \le m$ can be obtained by recursively computing the vectors $U_\ell$ with (2.2.5), starting from $\ell = 1$ up to $m$, for the initial value $U_0$ with $(h^n)_{-d+1} = (h^n)_{-d+2} = \cdots = (h^n)_{-1} = 0$ and $(h^n)_0 = (h_0)^n$. Note that each $U_\ell$ is computed unless $\ell \neq 0$ in the coefficient ring of $h$. Therefore, this recursive computation is always valid for the characteristic 0 case, but it may not be applied directly in the positive characteristic case since the value of $\ell$ can be zero in the coefficient ring of $h$: One solution is lifting to characteristic 0 such as $\mathbb{F}_p$ to $\mathbb{Q}_p$.

This method (with lifting to characteristic zero if necessary) can be applied to computing the Cartier-Manin matrix of the hyperelliptic curve $C : y^2 = f(x)$ as follows: If $f_0 \neq 0$, simply put $n = (p-1)/2$ and $h = f$, and then the $(ip-j)$-th coefficients $(f^n)_{ip-j}$ with $1 \le i, j \le g$ are computed as entries of $U_\ell$ for $1 \le \ell \le gp-1$. Otherwise, putting $f = xh(x)$, it follows from $f^n = x^n h^n$ that $(f^n)_{ip-j}$ is equal to the $\left(\frac{(2i-1)p-(2j-1)}{2}\right)$-th coefficient of $h^n$. Hence, it suffices to compute $U_\ell$ for $1 \le \ell \le \frac{(2g-1)p-1}{2}$.

Bostan-Gaudry-Schost [2] constructed an efficient algorithm to compute the Cartier-Manin matrix of $C$ over $\mathbb{F}_{p^r}$, by using the above recurrences with lifting to the unramified extension of $\mathbb{Q}_p$ of degree $r$.

*Remark 2.2.4* Unlike (2.2.4), each coefficient $(h^n)_\ell$ can be represented as a linear combination of $d$ *higher*-degree coefficients $(h^n)_{\ell+1}, \dots, (h^n)_{\ell+d}$. More precisely, it follows from (2.2.3) that

$$(nd - \ell + d)h_d(h^n)_{\ell-d} = -\sum_{j=0}^{d-1}(nj - \ell + j)h_j(h^n)_{\ell-j}.$$

Replacing $\ell$ by $\ell + d$, one has

$$(nd - \ell)h_d(h^n)_\ell = -\sum_{j=0}^{d-1}(nj - \ell - (d - j))h_j(h^n)_{\ell+d-j}$$

for $-d \le \ell \le nd$. Putting $i = d - j$, one also has

$$(nd - \ell)h_d(h^n)_\ell = -\sum_{i=1}^{d}(n(d - i) - \ell - i)h_{d-i}(h^n)_{\ell+i} \tag{2.2.6}$$

for $-d \le \ell \le nd$. Therefore, we can compute $(h^n)_\ell$ from $(h^n)_{\ell+1}, \dots, (h^n)_{\ell+d}$ as in (2.2.4) unless $nd - \ell \ne 0$, and can consider a recursive computation as in (2.2.5) starting from $(h^n)_{nd} = (h_d)^n$.

## 2.3 Cyclic Covers of the Projective Line and Their Cartier Operators

In this subsection, we briefly review Elkin's results [9] on the rank of the Cartier operator for a cyclic cover, since they will be applied in Sect. 3.2 below to our family of hyperelliptic curves $H_{a,b}$ having order-6 automorphisms.

Let $C$ be a (non-singular) curve of genus $g$ over an algebraically closed field $k$ of characteristic $p > 2$. Assume that there exists a ramified Galois cover $\pi : C \to \mathbb{P}^1$ of degree $n$, and let $r$ be the number of ramification points in $\mathbb{P}^1$ of $\pi$, where $n$ is coprime to $p$. In this case, for each ramification point $P_i$ in $\mathbb{P}^1$of $\pi$, its preimage $\pi^{-1}(\{P_i\})$ consists of $n/v_i$ branched points in $C$ with the same ramification index $v_i$ with $2 \le v_i \le n$ dividing $n$. By Hurwitz's formula, we have

$$2g - 2 + 2n = \sum_{i=1}^{r}\frac{n}{v_i}(v_i - 1),$$

and $C$ is birational to the homogenization of

$$Y^n = (X - a_1)^{n_1} \cdots (X - a_r)^{n_r} \tag{2.3.1}$$

for some mutually distinct elements $a_1, \dots, a_r \in k$, and some integers $n_i$ with $1 \le n_i < n$, $v_i = n/\gcd(n, n_i)$, $\gcd(n, n_1, \dots, n_r) = 1$, and $\sum_{i=1}^{r} n_i \equiv 0 \pmod n$. In this case, we say that $C \to \mathbb{P}^1$ (or $C$ simply) is a cyclic cover of type $(n; n_1, \dots, n_r)$.

The group of $n$-th roots of unity in $k$ acts on $H^0(C, \Omega^1_C)$. More precisely, let $\zeta_n$ be a primitive $n$-th root of unity in $k$, and $\delta$ the automorphism on $C$ defined by $(X, Y) \mapsto (X, \zeta_n^{-1}Y)$ (namely $\delta$ is a generator of $\mathrm{Aut}(C)$). Then $\delta$ induces an automorphism $\delta^*$ of the linear space $H^0(C, \Omega^1_C)$. Denoting by $D_i$ the $\zeta_n^i$-eigenspace of $\delta^*$, we decompose

$$H^0(C, \Omega^1_C) = \bigoplus_{i=0}^{n-1} D_i, \tag{2.3.2}$$

where the dimension $d_i$ of $D_i$ is given as

$$d_i = \left(\sum_{j=1}^{r}\frac{(in_j \bmod n)}{n}\right) - 1. \tag{2.3.3}$$

By the $p^{-1}$-linearity of the Cartier operator $\mathscr{C}$, we have $\mathscr{C}(\lambda^{pi}\omega) = \lambda^i \mathscr{C}(\omega)$ for any differential $\omega$, and thus

$$\mathscr{C}(D_{pi \bmod n}) \subset D_i \tag{2.3.4}$$

for every $0 \leq i \leq n-1$.

By the decomposition (2.3.2), we have

$$\operatorname{rank}(\mathscr{C}) = \sum_{i=0}^{n-1} \dim(\mathscr{C}(D_i)), \tag{2.3.5}$$

each term of which satisfies the following:

**Theorem 2.3.1** ( [9, Theorem 1.1]) *With notation as above, we have the following inequalities:*

$$\min(2\lfloor d_i/p \rfloor, d_{\sigma(i)}) \leq \dim(\mathscr{C}(D_i)) \leq \min(d_i, d_{\sigma(i)}),$$

*where* $\lfloor \cdot \rfloor$ *denotes the floor function, and where* $\sigma$ *is the inverse of a permutation map on the set* $\{0, 1, \ldots, n-1\}$ *given by* $i \mapsto pi \bmod n$.

Therefore, it follows from (2.3.5) that we obtain:

$$\sum_{i=0}^{n-1} \min(2\lfloor d_i/p \rfloor, d_{\sigma(i)}) \leq \operatorname{rank}(\mathscr{C}) \leq \sum_{i=0}^{n-1} \min(d_i, d_{\sigma(i)}),$$

see [9, Corollary 4.3].

## 2.4 Kudo-Harashita's Enumeration of Superspecial Hyperelliptic Curves

Based on Lemmas 2.1.1, 2.1.2, and 2.2.2, an algorithm for enumerating superspecial hyperelliptic curves over $K = \mathbb{F}_q$ with $q = p$ or $p^2$ was proposed by Kudo-Harashita [22], [23], and it consists of the following three steps:

1. Regarding unknown coefficients in (2.1.1) as variables, compute the Cartier-Manin matrix of $H$ given in Lemma 2.2.2.
2. Fixed constants $b$ and $c$ in (2.1.1), compute the roots over $\mathbb{F}_q$ of the multivariate system "the Cartier-Manin matrix is zero" with $2g$ variables $a_{2g-1}, \ldots, a_0$ by the hybrid approach [4] mixing Gröbner basis computation and exhaustive search.
3. Classify the collected curves corresponding to the roots of the system into isomorphism classes, by Lemma 2.1.2.

Kudo-Harashita implemented the algorithm on Magma [1], and executed it for the case $g = 4$ with $q = 11^2, 13^2, 17^2, 19^2, 23$. According to [23, Section 3.1], they succeeded in finishing required computation within a day in total. The main results in [22] and [23] are the following:

**Theorem 2.4.1** ( [22, Theorem 1]) *There is no superspecial hyperelliptic curve of genus* 4 *in characteristic* $p$ *with* $p \leq 13$.

**Theorem 2.4.2** ( [22, Theorem 2]) *There exist precisely* 5 (*resp.* 25) *superspecial hyperelliptic curves of genus* 4 *over* $\mathbb{F}_{17}$ (*resp.* $\mathbb{F}_{17^2}$) *up to isomorphism over* $\mathbb{F}_{17}$ (*resp.* $\mathbb{F}_{17^2}$). *Moreover, there exist precisely* 2 *superspecial hyperelliptic curves of genus* 4 *over* $\overline{\mathbb{F}_{17}}$ *up to isomorphism.*

**Theorem 2.4.3** ( [22, Theorem 3], [23, Theorem 3]) *There exist precisely* 12 (*resp.* 18) *superspecial hyperelliptic curves of genus* 4 *over* $\mathbb{F}_{19}$ (*resp.* $\mathbb{F}_{19^2}$) *up to isomorphism over* $\mathbb{F}_{19}$ (*resp.* $\mathbb{F}_{19^2}$). *Moreover, there exist precisely* 2 *superspecial hyperelliptic curves of genus* 4 *over* $\overline{\mathbb{F}_{19}}$ *up to isomorphism.*

**Table 2** The $\overline{\mathbb{F}_p}$-isomorphism classes of all superspecial hyperelliptic curves $H$ of genus 4 over the prime field $\mathbb{F}_p$ for $p = 17$, 19, and 23

| $p$ | Equation of $H$ representing an isomorphism class | $\overline{\mathrm{Aut}}(H)$ | $\mathrm{Aut}(H)$ | Case in Table 1 |
|---|---|---|---|---|
| 17 | $y^2 = x^{10} + x$ | $\mathbf{C}_9$ | $\mathbf{C}_{18}$ | **9** |
| | $y^2 = x^{10} + x^7 + 13x^4 + 12x$ | $\mathbf{A}_4$ | $\mathrm{SL}_2(\mathbb{F}_3)$ | **7** |
| 19 | $y^2 = x^{10} + 1$ | $\mathbf{D}_{10}$ | $\mathbf{C}_5 \rtimes \mathbf{D}_4$ | **10** |
| | $y^2 = x^{10} + x^7 + 4x^6 + 15x^5 + 6x^4 + 8x^3 + 5x^2 + 12x + 1$ | $\mathbf{V}_4$ | $\mathbf{D}_4$ | **4-1** |
| 23 | $y^2 = x^{10} + x^7 + 3x^4 + 10x$ | $\mathbf{C}_3$ | $\mathbf{C}_6$ | **3** |
| | $y^2 = x^{10} + x^7 + 18x^4 + 6x$ | $\mathbf{A}_4$ | $\mathrm{SL}_2(\mathbb{F}_3)$ | **7** |
| | $y^2 = x^{10} + x^7 + 5x^6 + 3x^5 + 21x^4 + 3x^3 + 9x^2 + 4x + 21$ | $\mathbf{V}_4$ | $\mathbf{D}_4$ | **4-1** |
| | $y^2 = x^{10} + x^7 + 9x^6 + 11x^5 + 19x^4 + 10x^3 + 16x^2 + 8x + 21$ | $\mathbf{C}_2$ | $\mathbf{V}_4$ | **2-1** |

**Theorem 2.4.4** ( [23, Theorem 4]) *There exist precisely* 14 *superspecial hyperelliptic curves of genus* 4 *over* $\mathbb{F}_{23}$ *up to isomorphism over* $\mathbb{F}_{23}$. *Moreover, there exist precisely* 4 *superspecial hyperelliptic curves of genus* 4 *over* $\mathbb{F}_{23}$ *up to isomorphism over* $\overline{\mathbb{F}_{23}}$.

As examples, the $\overline{\mathbb{F}_p}$-isomorphism classes of superspecial hyperelliptic curves of genus 4 defined over the prime field $\mathbb{F}_p$ are summarized in Table 2. Note that the reduced automorphism group of *every* superspecial curve in Table 2 is non-trivial.

While Kudo-Harashita succeeded in enumerating superspecial hyperelliptic curves for concrete $p$, the complexity of their algorithm has not been investigated, due to the difficulty of estimating the cost of Gröbner basis computation. In fact, it might be exponential with respect to $p$, since the multivariate system to be solved in Step 2 has the maximal total-degree $(p-1)/2$. Moreover, Step 3 might also be costly, due to the growth of the number of solutions found in Step 2.

To overcome the limitation of the enumeration in practical time, Ohashi-Kudo-Harashita [34] recently proposed an efficient algorithm with complexity $O(p^3)$ for enumerating superspecial hyperelliptic curves of genus 4, focusing on the space of those curves with extra involution (see also [32] for the genus-3 case, and [25] for the genus-4 non-hyperelliptic case). Namely, the algorithm in [34] treats just the case **2-1** (and the cases **4-1**, **5**, **6**, **8**, **10**) of Table 1, i.e., $\mathrm{Aut}(H) \supset \mathbf{V}_4$ whereas this paper focuses on the cases **3**, **7**, and **9**, i.e., $\mathrm{Aut}(H) \supset \mathbf{C}_6$.

## 3 Hyperelliptic Curves of Genus Four with Automorphism Group Containing $\mathbf{C}_6$

Let $K$ be a field of characteristic $p$ with $p \geq 7$, and $k = \overline{K}$ its algebraic closure. Assume that $K$ contains $\mathbb{F}_{p^2}$. In this section, we study hyperelliptic curves of genus 4 over $K$ with automorphism group containing the cyclic group of order 6, namely the cases **3**, **7**, and **9** of Table 1 in Theorem 2.1.5. In particular, we focus on the following parametric family of hyperelliptic curves of genus 4:

$$H_{a,b} : y^2 = f_{a,b}(x) := x^{10} + x^7 + ax^4 + bx, \tag{3.0.1}$$

where $a, b \in k$. The reason why we focus on this family is described in Sect. 1, and we will use this family in the main algorithm provided in Sect. 4 below. Let $\iota$ be the hyperelliptic involution of $H_{a,b}$, say $(x, y) \to (x, -y)$. Denoting by $\zeta_3$ a primitive 3rd root of unity in $k$, this curve has an order-3 automorphism $\sigma_3 : (x, y) \mapsto (\zeta_3 x, \zeta_3^2 y)$ represented by $(A, \lambda)$ with $A = \mathrm{diag}(\zeta_3, 1)$ and $\lambda = \zeta_3^2$. The automorphism $\sigma_6 := \sigma_3 \circ \iota$ has order-6, say $\sigma_6 : (x, y) \to (\zeta_3 x, -\zeta_3^2 y)$. Note that $\zeta_3 \in \mathbb{F}_{p^2}$ since $\zeta_3$ is a root of $x^2 + x + 1 \in \mathbb{F}_p[x]$. It is also straightforward that there exists a degree-3 map $H_{a,b} \to H_{a,b}/\langle\sigma_3\rangle$, where the quotient curve $H_{a,b}/\langle\sigma_3\rangle$ is a genus-one curve given by $Y^2 = X(X^3 + X^2 + aX + b)$.

### 3.1 Our Paramteric Family $H_{a,b} : y^2 = x^{10} + x^7 + ax^4 + bx$

We start with describing a relationship between $H_{a,b}$ and $C_{A,B} : y^2 = x^{10} + Ax^7 + Bx^4 + x$ in Table 1, in particular a merit to use $H_{a,b}$, not $C_{A,B}$, in our enumeration of superspecial curves. Recall from Theorem 2.1.5 that any hyperelliptic curve $H$ of genus 4 over $K$ with $\mathrm{Aut}(H) \supset \mathbf{C}_6$ is $k$-isomorphic to $C_{A,B}$ for some $A, B \in k$. Note that $A$ or $B$ not necessarily belongs to $K$, but it follows from the proof of Proposition 2.1.4 that they belong to a finite extension $K'$ of $K$, and we can take $K'$ so that it does not depend on $a$ nor $b$ but only on $g$ and $K$. For the central topic of this paper, we can use the family $C_{A,B}$ by restricting ourselves to the case where $A, B \in \mathbb{F}_{p^2}$. However, different choices of $A$ and $B$ lead to isomorphic curves, which causes that the isomorphism classification might be inefficient. (This kind of question also motivates the notion of "representative family", see [29] for the case of genus 3.) For example, over $\mathbb{F}_{29^2}$, the extension of $\mathbb{F}_{29}$ defined by $t^2 + 24t + 1$, the curves $y^2 = x^{10} + 11x^7 + 7x^4 + x$ and $y^2 = x^{10} + (9t + 1)x^7 + (18t + 24)x^4 + x$ are isomorphic to each other, where the authors learned this example from one of the reviewers.

On the other hand, the curve $C_{A,B}$ for $A, B \in K'$ with $A \neq 0$ is $k$-isomorphic to $H_{a,b}$ for some $a, b \in K'$, so that the family $H_{a,b}$ for $a, b \in \mathbb{F}_{p^2}$ covers the family $C_{A,B}$ for $A, B \in \mathbb{F}_{p^2}$ with $A \neq 0$. Indeed, taking $\delta \in k$ so that $\delta^3 = A^{-1}$, the isomorphism $(x, y) \mapsto (\frac{x}{\delta}, \frac{y}{\delta^{g+1}})$ transforms $C_{A,B}$ into $y^2 = x^{10} + x^7 + B\delta^6 x^4 + \delta^9 x$ whose coefficients of $x^4$ and $x$ belong to $K'$ by $\delta^3 \in K'$. Although the family $H_{a,b}$ for $a, b \in K$ (as well as $C_{A,B}$ for $A, B \in K$) does not represents all curves over $K$ whose automorphism group contains $\mathbf{C}_6$, we can see by the following lemma that it is better behaved with respect to isomorphism classes than $C_{A,B}$:

**Lemma 3.1.1** *Let $a$ and $b$ be elements in $k$. If two hyperelliptic curves $H_{a,b}$ and $H_{a',b'}$ with reduced automorphism groups $\mathbf{C}_3$ or $\mathbf{C}_9$ are isomorphic, then $(a, b) = (a', b')$.*

*Proof* Assume that there exists an isomorphism $\rho : H_{a,b} \to H_{a',b'}$. Then $\rho$ is represented by $(P, \lambda) \in \mathrm{GL}_2(k) \times k^\times$ as in Lemma 2.1.2. Let $\zeta := \zeta_3$ be a primitive 3rd root of unity in $k$. For an order-3 automorphism $\sigma_3 : (x, y) \mapsto (\zeta x, \zeta^2 y)$ on $H_{a,b}$ represented by $A{:=}\mathrm{diag}(\zeta, 1)$, we set $\sigma := \sigma_3$ and $\tau{:=}\rho^{-1}\sigma\rho$;

$$\begin{array}{ccc} H_{a,b} & \xrightarrow{\sigma} & H_{a,b} \\ {\scriptstyle\rho}\uparrow & & \downarrow{\scriptstyle\rho^{-1}} \\ H_{a',b'} & \xrightarrow{\tau} & H_{a',b'}. \end{array}$$

Since $\tau$ also has order 3 in $\overline{\mathrm{Aut}}(H)$, and since $\mathbf{C}_9$ has a unique subgroup of order 3, we have that $\tau$ is given by $(x, y) \mapsto (\zeta^i x, \pm\zeta^{2i} y)$ for $i = 1$ or 2. Thus, comparing the matrices corresponding to the both sides of $\tau = \rho^{-1}\sigma\rho$, we obtain an equation $P^{-1}AP = A^i$ in $\mathrm{PGL}_2(k)$, say

$$\begin{pmatrix} \zeta\alpha & \zeta\beta \\ \gamma & \delta \end{pmatrix} = \mu \begin{pmatrix} \zeta^i\alpha & \beta \\ \zeta^i\gamma & \delta \end{pmatrix}$$

for some $\mu \in k^\times$.

If $\delta \neq 0$, then $\mu = 1$, $\beta = \gamma = 0$, and $i = 1$. In this case, $\rho$ is $(x, y) \mapsto (\alpha\delta^{-1}x, \delta^{-5}\lambda y)$, and thus $y^2 = f_{a,b}(x)$ is transformed into $\lambda^2 y^2 = \alpha^{10}x^{10} + \alpha^7\delta^3 x^7 + a\alpha^4\delta^6 x^4 + b\alpha\delta^9 x = \lambda^2 f_{a',b'}(x)$. Therefore, $\alpha^{10} = \alpha^7\delta^3 = \lambda^2$, and hence $\alpha = \zeta^j\delta$ for some $j$. Since $\zeta^j\delta^{10} = \lambda^2$, it follows also from $a\zeta^j\delta^{10} = a'\lambda^2$ and $b\zeta^j\delta^{10} = b'\lambda^2$ that $a = a'$ and $b = b'$.

Suppose $\delta = 0$; then $\mu = \zeta$, $\alpha = 0$, and $i = 2$. In this case, $\rho$ is $(x, y) \mapsto (\frac{\beta}{\gamma x}, \frac{\lambda y}{\gamma^5 x^5})$, and thus $y^2 = f_{a,b}(x)$ is transformed into $\lambda^2 y^2 = \beta^{10} + \beta^7\gamma^3 x^3 + a\beta^4\gamma^6 x^6 + b\beta\gamma^9 x^9 = \lambda^2 f_{a',b'}(x)$. This is a contradiction since $f_{a',b'}$ has degree 10. □

Thanks to the above lemma, we need not conduct the isomorphism classification on $H_{a,b}$'s with $\overline{\mathrm{Aut}}(H_{a,b}) \cong \mathbf{C}_3$ or $\mathbf{C}_9$ collected in Step 2 of the main algorithm provided in Sect. 4 below.

If $\overline{\mathrm{Aut}}(H_{a,b})$ is not isomorphic to $\mathbf{C}_3$ nor $\mathbf{C}_9$, recall from Sect. 2.1 that $\overline{\mathrm{Aut}}(H_{a,b}) \cong \mathbf{A}_4$ and $\mathrm{Aut}(H_{a,b}) \cong \mathrm{SL}_2(\mathbb{F}_3)$. In this case, by considering elements in $\mathrm{SL}_2(\mathbb{F}_3)$, there exists an order-2 element in $\overline{\mathrm{Aut}}(H_{a,b})$ whose order in $\mathrm{Aut}(H_{a,b})$ is 4. Any two of such $H_{a,b}$'s are isomorphic to $y^2 = x(x^4-1)(x^4+2\sqrt{-3}x^2+1)$, and one of them is detected by Lemma 3.1.3 below; more generally, we have the following lemma, whose proof is essentially same as that of [32, Theorem 3.1.1]:

**Lemma 3.1.2** *Let $H : y^2 = f(x)$ be a hyperelliptic curve of genus $g$ over an algebraically closed field $k$, where $f(x)$ is a separable polynomial over $k$ of degree $2g+2$. Then, the following are equivalent:*

*(1)* $\overline{\mathrm{Aut}}(H)$ *has an element $\sigma$ of order 2 which has order 4 as an element in* $\mathrm{Aut}(H)$.
*(2) There exist roots $a_1$ and $a_2$ in $k$ of $f$ such that*

$$\left\{\frac{a_i - a_2}{a_i - a_1} : 3 \le i \le 2g\right\} = \left\{-\frac{a_i - a_2}{a_i - a_1} : 3 \le i \le 2g\right\},$$

*where $a_3, \ldots, a_{2g+2}$ are the other roots in $k$ of $f$.*

*Proof* Assume (1). By Proposition 2.1.4, there exists a hyperelliptic curve $H' : y^2 = f'(x)$ over $k$ and an isomorphism $\rho : H' \to H$ such that the automorphism $\tau := \rho^{-1}\sigma\rho$ of $H'$ is represented by $(\mathrm{diag}(-1,1), \mu') \in \mathrm{GL}_2(k) \times k^\times$;

$$\begin{array}{ccc} H & \xrightarrow{\sigma} & H \\ {\scriptstyle\rho}\uparrow & & \downarrow{\scriptstyle\rho^{-1}} \\ H' & \xrightarrow{\tau} & H', \end{array}$$

where $\mu'$ is an element in $k$ satisfying $(\mu')^2 = \pm 1$. Since $\tau$ also has order 4 in $\mathrm{Aut}(H)$, we have $(\mu')^2 = -1$ and thus $\mu' = \pm\sqrt{-1}$. Moreover, it follows from $\tau \in \mathrm{Aut}(H)$ that $-f'(-x) = f'(x)$. Therefore, $f'(x)$ is of degree $2g+1$ and is divided by $x$.

As for the form of a matrix representing $\rho$, we may assume from the proof of [32, Theorem 3.1.1] that it is either of the following:

$$\textbf{(A):}\ \begin{pmatrix} a_1 & a_2 \\ 1 & 1 \end{pmatrix} \quad \text{or} \quad \textbf{(B):}\ \begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix},$$

where $a_1, a_2, b_1 \in k$. The case **(B)** is impossible since $\rho$ does not send the point at infinity to itself. In the case **(A)**, the inverse map $\rho^{-1}$ is represented by

$$\begin{pmatrix} a_1 & a_2 \\ 1 & 1 \end{pmatrix}^{-1} = \frac{1}{a_1 - a_2}\begin{pmatrix} 1 & -a_2 \\ -1 & a_1 \end{pmatrix}.$$

For a ramification point $(\alpha, 0)$ of $H$ with a root $\alpha$ of $f$, its image in $H'$ by $\rho^{-1}$ is $\left(-\frac{\alpha - a_2}{\alpha - a_1}, 0\right)$. Since $H'$ has 0 and $\infty$ as ramification points, we have that $a_1$ and $a_2$ are (mutually different) roots of $f$. The condition $\tau \in \mathrm{Aut}(H)$ implies the assertion (2).

Conversely, if (2) holds, then we define $\rho$ as in **(A)** with roots $a_1$ and $a_2$ of $f$, and then the domain of $\rho$ is a hyperelliptic curve $H'$ with ramification points $\infty$, $(0,0)$, and $(\pm b_j, 0)$ for some $b_j \in k^\times$ with $1 \le j \le g$. Therefore $H'$ has an automorphism $(x, y) \mapsto (-x, \sqrt{-1}y)$, as desired. □

As a particular case of Lemma 3.1.2, we have the following:

**Lemma 3.1.3** $\overline{\mathrm{Aut}}(H_{a,b}) \cong \mathbf{A}_4$ *if and only if there exist roots $a_1$ and $a_2$ of $f_{a,b}$ satisfying the condition (2) of Lemma 3.1.2 for $f = f_{a,b}$ and $g = 4$.*

### 3.2 Cartier-Manin Matrices

In this subsection, we determine the form of the Cartier-Manin matrix $M_{a,b}$ of $H_{a,b} : y^2 = f_{a,b}(x)$ with respect to the basis $\mathcal{A}:=\{\frac{1}{y}dx, \frac{x}{y}dx, \frac{x^2}{y}dx, \frac{x^3}{y}dx\}$ of $H^0(H_{a,b}, \Omega^1_{H_{a,b}})$ given in Sect. 2.2. For each $\ell$ with $0 \leq \ell \leq 5(p-1)$, we denote by $c_\ell$ the $x^\ell$-coefficient of $f_{a,b}^{(p-1)/2}$.

**Lemma 3.2.1** *With notation as above, the Cartier-Manin matrix $M_{a,b}$ of $H_{a,b}$ is given as follows:*

*(1) If $p \equiv 1 \pmod 3$, then*

$$M_{a,b} = \begin{pmatrix} c_{p-1} & 0 & 0 & c_{p-4} \\ 0 & c_{2p-2} & 0 & 0 \\ 0 & 0 & c_{3p-3} & 0 \\ c_{4p-1} & 0 & 0 & c_{4p-4} \end{pmatrix}.$$

*(2) If $p \equiv 2 \pmod 3$, then*

$$M_{a,b} = \begin{pmatrix} 0 & 0 & c_{p-3} & 0 \\ 0 & c_{2p-2} & 0 & 0 \\ c_{3p-1} & 0 & 0 & c_{3p-4} \\ 0 & 0 & c_{4p-3} & 0 \end{pmatrix},$$

*and hence the rank of $M_{a,b}$ is equal to or smaller than 3.*

*Proof* Since

$$f_{a,b}(x)^{\frac{p-1}{2}} = \sum_{k_1+k_2+k_3+k_4=\frac{p-1}{2}} \binom{\frac{p-1}{2}}{k_1, k_2, k_3, k_4} a^{k_3} b^{k_4} x^{9k_1+6k_2+3k_3+\frac{p-1}{2}},$$

the coefficient of each $x^\ell$ in $f_{a,b}(x)^{\frac{p-1}{2}}$ is zero if $\ell \not\equiv \frac{p-1}{2} \pmod 3$. Computing $1 \leq i, j \leq 4$ with $ip - j \equiv \frac{p-1}{2} \pmod 3$ dividing the case into $p \equiv 1 \pmod 3$ and $p \equiv 2 \pmod 3$, we obtain the assertion by Lemma 2.2.2. □

*Remark 3.2.2* We can also determine the form of the Cartier-Manin matrix $M'_{a,b}$ (with respect to a basis different from $\mathcal{A}$) constructed by Elkin's method reviewed in Sect. 2.3. Similarly to $M_{a,b}$ as in Lemma 3.2.1, there are many zero entries in $M'_{a,b}$, but a transformation between these two matrices is not explicitly given, and also a relation between the entries of $M'_{a,b}$ and the coefficients of $f$ is not clear. In the following, we describe how to apply Elkin's method.

First, $H_{a,b}$ is a cyclic cover of type $(6; 1, 2, 3, 3, 3)$, which is birational to

$$Y^6 = (X - a_1)(X - a_2)^2(X - a_3)^3(X - a_4)^3(X - a_5)^3 \tag{3.2.1}$$

for some mutually different $a_1, a_2, a_3, a_4, a_5 \in k$. Indeed, writing $f_{a,b}(x) = x\prod_{i=1}^3(x^3 - A_i)$ for some $A_i \in k$ with $1 \leq i \leq 3$, a straightforward computation shows that the ramification points in $H_{a,b}/\langle\sigma_3 \circ \iota\rangle$ of the degree-6 cyclic cover $\pi : H_{a,b} \to H_{a,b}/\langle\sigma_3 \circ \iota\rangle$ ; $(x : y : z) \mapsto (x^3 : x^2y^2 : z)$ are $(0 : 0 : 1)$, $(0 : 1 : 0)$, and $(A_i : 0 : 1)$ for $1 \leq i \leq 3$, whose ramification indexes are 6, 3, and 2 respectively. Hence, $H_{a,b}$ is birational to an affine plane curve of the form (2.3.1) with $n = 6$ and $r = 5$, so that we can take $(n_1, n_2, n_3, n_4, n_5) = (1, 2, 3, 3, 3)$.

Letting $\zeta_6$ be a primitive 6-th root of unity in $k$, we decompose $H^0(H_{a,b}, \Omega^1_{H_{a,b}}) = \sum_{i=0}^5 D_i$ as in Sect. 2.3, where $D_i$ is the $\zeta_6^i$-eigenspace. The dimensions $d_i$ of $D_i$ for $1 \leq i \leq 5$ are computed by (2.3.3), say $d_0 = 0, d_1 = 1$, $d_2 = 0, d_3 = 1, d_4 = 0$, and $d_5 = 2$. Choosing a basis $\mathcal{B} = \{w^{(1)}, w^{(3)}, w_1^{(5)}, w_2^{(5)}\}$ of $H^0(H_{a,b}, \Omega^1_{H_{a,b}})$ such that $\{w^{(1)}\}$, $\{w^{(3)}\}$, and $\{w_1^{(5)}, w_2^{(5)}\}$ are bases of $D_1$, $D_3$, and $D_5$ respectively, it follows form (2.3.4) that we have the following:

- For $p \equiv 1 \pmod 6$, we have $\mathscr{C}(D_i) \subset D_i$ for any $i$. In this case, $M'_{a,b}$ is a matrix whose entries are zero except for $(1, 1)$, $(2, 2)$, $(3, 3)$, $(3, 4)$, $(4, 3)$, and $(4, 4)$-th ones.

- For $p \equiv 5 \pmod 6$, we have $\mathscr{C}(D_5) \subset D_1$, $\mathscr{C}(D_3) \subset D_3$, and $\mathscr{C}(D_1) \subset D_5$. In this case, $M'_{a,b}$ is a matrix whose entries are zero except for (1, 3), (1, 4), (2, 2), (3, 1), and (4, 1)-th ones. Therefore, the rank of $M'_{a,b}$ is equal to or smaller than 3.

Note that, however, since any explicit birational map between $H_{a,b}$ and (3.2.1) is not given, we cannot compute the change-of-basis matrix between $\mathcal{A}$ and $\mathcal{B}$.

## 4 Algorithm and Computational Results

As in the previous sections, let $k$ be an algebraically closed field of characteristic $p$ with $p \geq 7$. In this section, we shall present an algorithm to efficiently produce superspecial hyperelliptic curves of genus 4, by focusing on the family $H_{a,b} : y^2 = x^{10} + x^7 + ax^4 + bx$ with $a, b \in k$ as in (3.0.1).

### 4.1 Main Algorithm and Its Complexity

Now, we construct an algorithm to enumerate superspecial hyperelliptic curves $H_{a,b}$. For the efficiency, let us here restrict ourselves to the case where $a$ and $b$ belong to $\mathbb{F}_{p^2}$.

**Theorem 4.1.1** *Main Algorithm below outputs the $k$-isomorphism classes of all s.sp. hyperelliptic curves of the form (3.0.1) with $a, b \in \mathbb{F}_{p^2}$ in time $\tilde{O}(p^4)$. Moreover, if the gcd of resultants of non-zero entries of the Cartier-Manin matrix of $H_{a,b}$ has degree $O(p)$, the complexity becomes $\tilde{O}(p^3)$.*
*Main Algorithm. For a prime $p \geq 7$ as the input, conduct the following:*

1. *Regarding $a$ and $b$ as variables, compute the Cartier-Manin matrix $M_{a,b}$ of $H_{a,b}$.*
2. *Collect all $(a, b) \in \mathbb{F}_{p^2}^2$ such that $H_{a,b}$ is a s.sp. hyperelliptic curve, as follows:*
   - 2-1. *Compute the solutions $(a_0, b_0) \in \mathbb{F}_{p^2}^2$ to $M_{a,b} = 0$.*
   - 2-2. *For each solution $(a_0, b_0)$ computed in Step 2-1, check if the equation $y^2 = f_{a,b}(x)$ in (3.0.1) for $(a, b) = (a_0, b_0)$ defines a hyperelliptic curve, by computing $\gcd(f_{a,b}, f'_{a,b})$.*
3. *For each of $H_{a,b}$'s collected in Step 2, check the condition of Lemma 3.1.3 to decide whether $\overline{\mathrm{Aut}}(H_{a,b}) \cong \mathbf{A}_4$ or not. Output one $H_{a,b}$ with $\overline{\mathrm{Aut}}(H_{a,b}) \cong \mathbf{A}_4$ (if exists) and all of $H_{a,b}$'s such that $\overline{\mathrm{Aut}}(H_{a,b})$ is not isomorphic to $\mathbf{A}_4$.*

*Proof* The correctness follows from Lemmas 2.2.2, 3.1.1, 3.1.3, and Theorem 2.1.5. The complexity of Step 1 is estimated as $O(p^3)$ by Lemma 4.1.2 below. The most generic and efficient method for Step 2-1 is the following resultant-based method:

(1) Compute resultants of non-zero entries of $M_{a,b}$ with respect to $a$ (or $b$).
(2) Compute the gcd in $\mathbb{F}_{p^2}[b]$ of the resultants and its roots in $\mathbb{F}_{p^2}$.
(3) For each root $b_0$, evaluate it to $b$ in $M_{a,b}$, and then compute the gcd in $\mathbb{F}_{p^2}[a]$ of non-zero entries of $M_{a,b_0}$ and its roots in $\mathbb{F}_{p^2}$.

We here note that, for a given univariate polynomial $h(t)$ of degree $D \leq p^2$ over $\mathbb{F}_{p^2}$, one can compute its roots in $\mathbb{F}_{p^2}$ with complexity $\tilde{O}(p^2 + D^2)$. Indeed, the gcd of $h(t)$ and $t^{p^2} - t$ is computed in $\tilde{O}(p^2)$ with fast gcd algorithm, and it is a separable polynomial of degree $\leq D$. Hence, computing the roots of the gcd is done just by equal-degree factorization, and its complexity is estimated as $\tilde{O}(D^2)$.

Since the degree of each non-zero entry of $M_{a,b}$ is $O(p)$ (both in $a$ and $b$), the resultants are computed in $\tilde{O}(p^3)$ [40], and their gcd in (2) is computed in $\tilde{O}(p^2)$. Letting the degree of the gcd be $d = O(p^2)$, one can compute its roots in $\mathbb{F}_{p^2}$ with complexity $\tilde{O}(d^2)$. For each root $b_0$ ($O(d)$ possible choices), evaluate it to $b$ of $M_{a,b}$ in time

$O(p)$, and compute the gcd of non-zero entries of $M_{a,b_0}$ in time $\tilde{O}(p)$. The roots in $\mathbb{F}_{p^2}$ of the second gcd are also computed in $\tilde{O}(p^2)$. Step 2-2 is clearly done in constant time. Thus, the complexity of Step 2 is upper-bounded by $\tilde{O}(p^3 + d^2 + dp^2)$. Note that the number of roots $(a_0, b_0)$ is $O(p^2)$.

As for Step 3, checking the condition in Lemma 3.1.3 is done in constant time for each root $(a_0, b_0)$, so that the complexity of Step 3 is $O(p^2)$. □

We remark that $d$ and the number of roots $(a_0, b_0)$ are both $O(p)$ in practice, see tables in a pdf (named as `NKT_table.pdf`) available at [17]. From this, the complexities of Steps 2 and 3 are expected to be $\tilde{O}(p^3)$ and $O(p)$, and in this case the total complexity of Main Algorithm is $\tilde{O}(p^3)$.

**Lemma 4.1.2** *The Cartier-Manin matrix $M_{a,b}$ in Step 1 is computed in time $O(p^3)$.*

*Proof* Recall from Lemma 2.2.2 that each $(i, j)$-entry of $M_{a,b}$ is the $x^{ip-j}$-coefficient of $f^n$ with $f := f_{a,b}$ and $n := (p-1)/2$. Putting $g = x^9 + x^6 + ax^3 + b$, it follows from $f^n = x^n g^n$ that $x^{ip-j}$-coefficient of $f^n$ is equal to the $x^\ell$-coefficient of $g^n$ for $\ell = \frac{(2i-1)p-(2j-1)}{2}$. Moreover, since $g^n$ is a polynomial in $x^3$, the coefficient of $x^\ell$ in $g^n$ is zero if $\ell \not\equiv 0 \pmod 3$. Here, it follows from (2.2.3) that

$$\ell b(g^n)_\ell = (3(n+1)-\ell)a(g^n)_{\ell-3} + (6(n+1)-\ell)(g^n)_{\ell-6} + (9(n+1)-\ell)(g^n)_{\ell-9},$$

for any $\ell = 3, 6, 9, \ldots, 3p-3$, where we used $g_9 = g_6 = 1, g_3 = a$, and $g_0 = b$. Hence, we can recursively compute $(g^n)_\ell$ for all $\ell \le 3p-3$, starting from $(g^n)_0 = b^{\frac{p-1}{2}}$. In particular, the coefficients $(g^n)_\ell$ with $\ell = \frac{(2i-1)p-(2j-1)}{2}$ for $1 \le i \le 3$ and $1 \le j \le 4$ are computed, since the maximal value $(5p-1)/2$ of such $\ell$ is less than $3p$. The number of required iteration is at most $(5p-1)/2 = O(p)$. The cost of computing each $(g^n)_\ell$ is $O(p^2)$. Indeed, each $(g^n)_\ell$ is a polynomial in $a$ and $b$ of total degree $\le n = \frac{p-1}{2}$, and thus the number of its non-zero terms is $\binom{n+2}{2} = O(p^2)$. Therefore, the total cost of computing the $(i, j)$-entries of $M_{a,b}$ for $1 \le i \le 3$ and $1 \le j \le 4$ is $O(p^3)$.

Next, we consider to compute the $x^\ell$-coefficients of $g^n$ for $\ell = \frac{(2i-1)p-(2j-1)}{2}$ with $i = 4$ and $1 \le j \le 4$, namely, $\frac{7p-7}{2}$, $\frac{7p-5}{2}$, $\frac{7p-3}{2}$, and $\frac{7p-1}{2}$. It follows from (2.2.6) that

$$(9n-\ell)(g^n)_\ell = (\ell+9)b(g^n)_{\ell+9} + (\ell+6-3n)a(g^n)_{\ell+6} + (\ell+3-6n)(g^n)_{\ell+3}.$$

for $\ell = 9n-3, 9n-6, \ldots, 6n+3 = 3p$. When $\ell \in 3\mathbb{Z}$ with $0 < \ell < 9n$, the only case where $9n-\ell$ is divided by $p$ is $9n-\ell = 3p$, i.e., $\ell = 3n-3$. Hence, we can recursively compute $(g^n)_\ell$ for all $\ell \in 3\mathbb{Z}$ with $3p = 6n+3 \le \ell \le 9n$, starting from $(g^n)_{9n} = 1$. In particular, the coefficients $(g^n)_\ell$ for $\ell = \frac{7p-7}{2}$, $\frac{7p-5}{2}$, $\frac{7p-3}{2}$, and $\frac{7p-1}{2}$ are computed. Hence, the total cost of computing the $(i, j)$-entries of $M_{a,b}$ for $i = 4$ and $1 \le j \le 4$ is $O(p^3)$, similarly to the case where $1 \le i \le 3$ and $1 \le j \le 4$. □

*Remark 4.1.3* Here, we list possible variants of Main Algorithm with $q := p^2$, and provide upper-bounds of their complexities; Our bounds for Main Algorithm in Theorem 4.1.1 does not exceed each of the bounds below:

1. Brute force on $(a, b) \in \mathbb{F}_q^2$. For each $(a, b) \in \mathbb{F}_q^2$, test $\gcd(f, f') = 1$ or not in constant time. If $\gcd(f, f') = 1$, compute $M_{a,b}$ in time $\tilde{O}(\sqrt{p})$ (cf. [2]). The total complexity is $\tilde{O}(q^2\sqrt{p})$.
2. For each $a \in \mathbb{F}_q$, compute $M_{a,b}$ in time $O(p^2)$ keeping $b$ as a parameter. Then brute force on $b$: Test $\gcd(f, f') = 1$ or not in constant time. If $\gcd(f, f') = 1$, evaluate it to $M_{a,b}$ in time $O(p)$. The total complexity is $O(q^2 q)$.
3. For each $a \in \mathbb{F}_q$, compute $M_{a,b}$ in time $O(p^2)$ keeping $b$ as a parameter. Compute the gcd of non-zero entries of $M_{a,b}$ in time $\tilde{O}(p)$. Compute the roots in $\mathbb{F}_{p^2}$ of the gcd in time $\tilde{O}(p^2)$. For each root $b$, test $\gcd(f, f') = 1$ or not in constant time. The total complexity is $\tilde{O}(qp^2)$.
4. Compute $M_{a,b}$ in time $O(p^3)$ keeping $a$ and $b$ as parameters. Then brute force on $(a, b)$: Test $\gcd(f, f') = 1$ or not in constant time. If $\gcd(f, f') = 1$, evaluate it to $M_{a,b}$ in time $O(p)$. The total complexity is $O(p^3 + q^2 p)$.
5. Compute $M_{a,b}$ in time $O(p^3)$ keeping $a$ and $b$ as parameters. Then brute force on $a$: Evaluate it to $M_{a,b}$ in time $O(p)$, and compute the gcd of non-zero entries of $M_{a,b}$ in time $\tilde{O}(p)$. Compute the roots in $\mathbb{F}_{p^2}$ of the gcd in time $\tilde{O}(p^2)$. For each root $b$, test $\gcd(f, f') = 1$ or not in constant time. The total complexity is $\tilde{O}(p^3 + qp^2)$.

**Table 3** Computational results for $17 \leq p < 1000$ obtained by the execution of Main Algorithm in Theorem 4.1.1. "Num. of $H_{a,b}$" denotes the number of $\overline{\mathbb{F}_p}$-isomorphism classes of obtained $H_{a,b}$'s

| $p$ | Num. of $H_{a,b}$ | $p$ | Num. of $H_{a,b}$ | $p$ | Num. of $H_{a,b}$ | $p$ | Num. of $H_{a,b}$ |
|---|---|---|---|---|---|---|---|
| 17 | 1 | 227 | 29 | 461 | 54 | 719 | 112 |
| 23 | 2 | 233 | 30 | 467 | 73 | 743 | 124 |
| 29 | 1 | 239 | 36 | 479 | 82 | 761 | 129 |
| 41 | 4 | 251 | 28 | 491 | 79 | 773 | 106 |
| 47 | 5 | 257 | 28 | 503 | 93 | 797 | 90 |
| 53 | 4 | 263 | 58 | 509 | 59 | 809 | 94 |
| 59 | 6 | 269 | 32 | 521 | 70 | 821 | 107 |
| 71 | 9 | 281 | 34 | 557 | 67 | 827 | 120 |
| 83 | 8 | 293 | 29 | 563 | 75 | 839 | 119 |
| 89 | 7 | 311 | 62 | 569 | 78 | 857 | 121 |
| 101 | 8 | 317 | 21 | 587 | 89 | 863 | 138 |
| 107 | 4 | 347 | 61 | 593 | 94 | 881 | 112 |
| 113 | 14 | 353 | 25 | 599 | 108 | 887 | 156 |
| 131 | 18 | 359 | 55 | 617 | 60 | 911 | 182 |
| 137 | 12 | 383 | 72 | 641 | 84 | 929 | 89 |
| 149 | 18 | 389 | 49 | 647 | 106 | 941 | 126 |
| 167 | 26 | 401 | 44 | 653 | 54 | 947 | 95 |
| 173 | 22 | 419 | 61 | 659 | 89 | 953 | 109 |
| 179 | 17 | 431 | 72 | 677 | 59 | 971 | 122 |
| 191 | 32 | 443 | 50 | 683 | 102 | 977 | 120 |
| 197 | 21 | 449 | 38 | 701 | 68 | 983 | 115 |

## 4.2 Implementation and Computational Results

We implemented Main Algorithm on Magma V2.26-10 on a PC with macOS Monterey 12.0.1, at 2.6 GHz CPU 6 Core (Intel Core i7) and 16GB memory (cf. [17] for the source code "NKT_enum4.txt"). Executing the implemented algorithm, we obtain Theorem B in Sect. 1. Our computational results are summarized in Table 3. For any $p$ with $17 \leq p < 1000$ and $p \equiv 1 \pmod 3$, there is no $(a, b) \in \mathbb{F}_{p^2}^2$ such that $H_{a,b}$ is a s.sp. hyperelliptic curve, and hence we write the computational results only for $p$ with $p \equiv 2 \pmod 3$ in the table. As for the timings, the degrees of the gcds computed in Step 2, and other detailed information, we summarize them in a separated pdf (named as `NKT_table.pdf`) which is available at [17].

We can easily increase the upper bound on $p$ in Theorem B. For example, on the PC described above, computing the $\overline{\mathbb{F}_p}$-isomorphicm classes of s.sp. $H_{a,b}$'s with $a, b \in \mathbb{F}_{p^2}$ for all $17 \leq p < 1000$ took 6,300 s (about 1.75 h) in total, and the execution for $p = 997$ took only 195 seconds.

The degree of the gcd of the resultants computed in Step 2 and the number of isomorphism classes of obtained $H_{a,b}$'s might follow $O(p)$, which implies that the complexity of Step 2 is $\tilde{O}(p^3)$ in practice, see Theorem 4.1.1.

Most of time is spent at Step 2. We see from tables in a pdf (named as `NKT_table.pdf`) available at [17] that Steps 1 and 2 might follow our estimations $O(p^3)$ and $\tilde{O}(p^3)$ respectively. As for Step 3, our estimation in the proof of Theorem 4.1.1 is $O(p^2)$, but it might be $O(p)$ in practice since the number of $(a, b)$ for which $H_{a,b}$ is a s.sp. hyperelliptic curve would be $O(p)$.

*Remark 4.2.1* When $p \equiv 1 \pmod 3$, the non-superspeciality of $H_{a,b}$ for *some* $(a, b)$ with $b \neq 0$ is deduced from that of $E_{a,b} : Y^2 = X(X^3+X^2+aX+b)$, which is a quotient curve of $H_{a,b}$ by the order-3 automorphism $\sigma_3$ defined

at the begining of Sect. 3. Indeed, the genus-one curve $E_{a,b}$ is isomorphic to $Y^2 = X^3 + (a/b)X^2 + (1/b)X + (1/b)$ via the transformation $(X, Y) \mapsto (1/X, \sqrt{b}Y/X^2)$. Eliminating the $X^2$-coefficient by $X \mapsto X - \frac{a}{3b}$, one obtains the equation $Y^2 = X^3 + \frac{3b-a^2}{3b^2}X + (\text{const.})$. If $3b = a^2$, the genus-one curve $E_{a,b}$ is isomorphic to $Y^2 = X^3 + A$ for some constant $A \in k^\times$ which is supersingular if and only if $p \equiv 2 \pmod 3$. Thus, if $p \equiv 1 \pmod 3$, the curve $H_{a,b}$ is not superspecial for any $(a, b) \in k^2$ with $3b = a^2$ by Serre's covering result: A subcover of a superspecial curve is also superspecial (cf. [27] and [10, Corollary 2.8].

We observe that the non-superspeciality of $H_{a,b}$ for *any* $(a, b) \in \mathbb{F}_{p^2}^2$ with $p \equiv 1 \pmod 3$ is not deduced directly from that of $E_{a,b}$: We computationally examined that there exists $(a, b) \in \mathbb{F}_{p^2}^2$ such that $E_{a,b}$ is supersingular but $H_{a,b}$ is not superspecial. We leave the problem to prove it open.

## 5 Concluding Remarks

We realized an algorithm with complexity $\tilde{O}(p^4)$ in theory but $\tilde{O}(p^3)$ in practice, specific to producing s.sp. hyperelliptic curves of genus 4, restricting to a parametric family of curves $H_{a,b}$ given by $y^2 = x^{10} + x^7 + ax^4 + bx$. Our case is included in the case where $\mathrm{Aut}(H) \supset \mathbf{C}_6$ in Theorem 2.1.5, while a recent work [34] presented at WAIFI2022 treats the case where $\mathrm{Aut}(H) \supset \mathbf{V}_4 := \mathbf{C}_2 \times \mathbf{C}_2$ (Klein 4-group). Our algorithm cannot enumerate all s.sp. hyperelliptic curves of genus 4 different from the algorithm in [22] at WAIFI2018, but it is expected from Theorem B to surely find such a curve for arbitrary $p \geq 17$ with $p \equiv 2 \bmod 3$. By executing the algorithm on Magma, we succeeded in enumerating s.sp. hyperelliptic curves $H_{a,b}$ with $(a, b) \in \mathbb{F}_{p^2}^2$ for every $p$ between 17 to 1000, which is much larger than $p = 17, 19$ as in the enumeration of [22].

A future work is to present the (representative) family that covers *all* hyperelliptic curves of genus 4 over $\mathbb{F}_{p^2}$ with automorphism group containing $\mathbf{C}_6$, which enables us to enumerate *all* s.sp. those curves. A similar problem can be considered also in the other cases $\mathrm{Aut}(H) \supset \mathbf{V}_4$ and $\mathrm{Aut}(H) \supset \mathbf{C}_4$ in Theorem 2.1.5: As far as the authors' knowledge, any representative family as in [29] has not been explicitly given in both cases. In the former case, Ohashi-Kudo-Harashita [34] already provided an algorithm efficiently enumerating all s.sp. curves without any representative family, but it is still interesting problem to find such a family, in terms of efficiently parameterizing the moduli space of curves. As for the case where $\mathrm{Aut}(H) \supset \mathbf{C}_4$, since there are a small number of parameters (at most 3 parameters, see cases **2-2** and **4-2** in Table 1), we can produce s.sp. curves by the resultant computation, similarly to the main algorithm of this paper. Then the problem is to implement the efficient isomorphism classification of produced curves.

**Acknowledgements** The authors thank the anonymous referees for their comments and suggestions, which have helped the authors significantly improve the paper. All of them are taken into account for improving the presentation of the paper. The authors are also grateful to Evan O'Dorney, Shushi Harashita and Ryo Ohashi for hepful comments. This work was supported by JSPS Grantin-Aid for Young Scientists 20K14301, 23K12949, and JST CREST Grant Number JPMJCR2113.



## References

1. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symb. Comput. **24**, 235–265 (1997)
2. Bostan, A., Gaudry, P., Schost, É.: Linear Recurrences with Polynomial Coefficients and Computation of the Cartier-Manin Operator on Hyperelliptic Curves, In: G. L. Mullen, A. Poli and H. Stichtenoth (eds.), Finite Fields and Applications. Fq 2003. LNCS, **2948**, Springer, Berlin-Heidelberg (2004)
3. Beauville, A.: Finite subgroups of $\mathrm{PGL}_2(\mathrm{K})$, In: Vector bundles and complex geometry, volume **522** of Contemp. Math., pp. 23–29, Amer. Math. Soc., Providence, RI (2010)

4. Bettale, L., Faugere, J.-C., Perret, L.: Hybrid approach for solving multivariate systems over finite fields. J. Math. Cryptol. **3**, 177–197 (2009)
5. Castryck, W., Decru, T., Smith, B.: Hash functions from superspecial genus 2 curves using Richelot isogenies. J. Math. Cryptol. **14**(1), 268–292 (2020)
6. Deuring, M.: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Univ. Hamburg **14**(1), 197–272 (1941)
7. Eichler, M.: Über die Idealklassenzahl total definiter Quaternionenalgebren. Math. Z. **43**, 102–109 (1938)
8. Ekedahl, T.: On supersingular curves and abelian varieties. Math. Scand. **60**, 151–178 (1987)
9. Elkin, E.A.: The rank of the Cartier operator on cyclic covers of the projective line. J. Algebra **327**, 1–12 (2011)
10. Faber, X.: Finite $p$-irregular subgroups of $\mathrm{PGL}_2(\mathrm{k})$, arXiv:1112.1999 (2021)
11. Flajolet, P., Salvy, B.: The SIGSAM challenges: symbolic asymptotics in practice. SIGSAM Bull. **31**(4), 36–47 (1997)
12. Gutierrez, J., Shaska, T.: Hyperelliptic curves with extra involutions. LMS J. Comput. Math. **8**, 102–115 (2005)
13. Gutierrez, J., Sevilla, D., Shaska, T.: Hyperelliptic curves of genus 3 with prescribed automorphism group, In: Computational Aspects of Algebraic Curves, In: Lecture Notes Ser. Comput., vol. **13**, pp. 109–123, World Sci. Publ., Hackensack, NJ (2003)
14. Harvey, D., Sutherland, A.V.: Computing Hasse–Witt matrices of hyperelliptic curves in average polynomial time. LMS J. Comput. Math. **17**, 257–273 (2014)
15. Hashimoto, K.: Class numbers of positive definite ternary quaternion Hermitian forms. Proc. Jpn. Acad. Ser. A Math. Sci. **59**(10), 490–493 (1983)
16. Hashimoto, K., Ibukiyama, T.: On class numbers of positive definite binary quaternion Hermitian forms II. J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28**(3), 695–699 (1982)
17. https://sites.google.com/view/m-kudo-official-website/english/code/hyp
18. Ibukiyama, T., Katsura, T., Oort, F.: Supersingular curves of genus two and class numbers. Compos. Math. **57**, 127–152 (1986)
19. Igusa, J.: Arithmetic variety of moduli for genus two. Ann. Math. **72**, 612–649 (1960)
20. Komoto, H., Kozaki, S., Matsuo, K.: Improvements in the computation of the Hasse–Witt matrix. JSIAM Lett. **2**, 17–20 (2010)
21. Kudo, M., Harashita, S.: Superspecial curves of genus 4 in small characteristic. Finite Fields Appl. **45**, 131–169 (2017)
22. Kudo, M., Harashita, S.: Superspecial Hyperelliptic Curves of Genus 4 over Small Finite Fields. In: Budaghyan, L., Rodriguez-Henriquez, F. (eds.) Arithmetic of Finite Fields WAIFI 2018, LNCS, 11321., pp. 58–73. Springer, Cham (2018)
23. Kudo, M., Harashita, S.: Algorithmic study of superspecial hyperelliptic curves over finite fields, Commentarii Mathematici Universitatis Sancti Pauli, Vol. **70**, 49–64 (2022)
24. Kudo, M., Harashita, S.: Computational approach to enumerate non-hyperelliptic superspecial curves of genus 4. Tokyo J. Math. **43**(1), 259–278 (2020)
25. Kudo, M., Harashita, S., Howe, E. W.: Algorithms to enumerate superspecial Howe curves of genus four, In: Proceedings of Fourteenth Algorithmic Number Theory Symposium (ANTS-XIV), Open Book Series, Vol. **4**, No. 1, 301–316 (2020)
26. Kudo, M.: Appendix A. Automorphism groups of hyperelliptic curves of genus four, In: Kudo, M., Nakagawa, T., and Takagi, T.: Efficient search for superspecial hyperelliptic curves of genus four with automorphism group containing $\mathbb{Z}_6$, arXiv: 2210.14822 [math.AG], 2022 (the preprint version of this article)
27. Lachaud, G.: Sommes d'Eisenstein et nombre de points de certaines courbes alg'ebriques sur les corps finis, C.R. Acad. Sci. Paris 305, S'erie I (1987), 729–732
28. Lercier, R., Ritzenthaler, C.: Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects. J. Algebra **372**, 595–636 (2012)
29. Lercier, R., Ritzenthaler, C., Rovetta, F., Sijsling, J.: Parametrizing the moduli space of curves and applications to smooth plane quartics over finite fields. LMS J. Comput. Math. **17**, 128–147 (2014)
30. Lercier, R., Ritzenthaler, C., Sijsling, J.: Fast computation of isomorphisms of hyperelliptic curves and explicit Galois descent. In: Proceedings of Fourteenth Algorithmic Number Theory Symposium (ANTS-X), Open Book Series, Vol. **1**(1), pp. 463–486 (2013)
31. Lercier, R., Sijsling, J.,Ritzenthaler, C.: Functionalities for genus 2 and 3 curves, MEGA (2021), arXiv:2102.04372
32. Moriya, T., Kudo, M.: Some explicit arithmetics on curves of genus three and their applications, arXiv: 2209.02926 [math.AG] (2022)
33. Nygaard, N.O.: Slopes of powers of Frobenius on crystalline cohomology. Ann. Sci. Éc. Norm. Supér. **4**(14), 369–401 (1981)
34. Ohashi, R., Kudo, M., Harashita, S.: Fast enumeration of superspecial hyperelliptic curves of genus 4 with automorphism group $V_4$, to appear in Proceedings of WAIFI2022, (2022)
35. Roquette, P.: Abschätzung der Automorphismenanzahl von Funktionenkörpern bei Primzahlcharakteristik. Math. Z. **117**, 157–163 (1970)
36. Shaska, T.: Determining the automorphism group of a hyperelliptic curve, In: Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation (ISSAC'03), August (2003), pp. 248–254
37. Shaska, T.: Some special families of hyperelliptic curves. J. Algebra Appl. **3**(1), 75–89 (2004)
38. Stichtenoth, H.: Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. I. Eine Abschätzung der Ordnung der Automorphismengruppe. Arch. Math. **24**, 527–544 (1973)
39. Tafazolian, S.: A note on certain maximal hyperelliptic curves. Finite Fields Their Appl. **18**, 1013–1016 (2012)
40. van der Hoeven, J., Lecerf, G.: Fast computation of generic bivariate resultants. J. Complex. **62**, 101499 (2021)
41. Yui, N.: On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$. J. Algebra **52**, 378–410 (1978)