COMMENTARII MATHEMATICI
UNIVERSITATIS SANCTI PAULI
Vol. 70 2022

ed. RIKKYO UNIV/MATH
IKEBUKURO TOKYO
171–8501 JAPAN

Algorithmic Study of Superspecial Hyperelliptic Curves over Finite Fields

by

Momonari KUDO* and Shushi HARASHITA†

(Received December 7, 2021)
(Revised May 30, 2022)

Abstract. This paper presents algorithmic approaches to study *superspecial* hyperelliptic curves. The algorithms proposed in this paper are: an algorithm to enumerate superspecial hyperelliptic curves of genus g over finite fields $\mathbb{F}_q$, and an algorithm to compute the automorphism group of a (not necessarily superspecial) hyperelliptic curve over finite fields. The first algorithm works for any (g, q) such that q and $2g + 2$ are coprime and $q > 2g + 1$. As an application, we enumerate superspecial hyperelliptic curves of genus $g = 4$ over $\mathbb{F}_p$ for $11 \leq p \leq 23$ and over $\mathbb{F}_{p^2}$ for $11 \leq p \leq 19$ with our implementation on a computer algebra system Magma. Moreover, we find *maximal* hyperelliptic curves and *minimal* hyperelliptic curves over $\mathbb{F}_{p^2}$ from among enumerated superspecial ones. The second algorithm computes an automorphism as a concrete element in (a quotient of) a linear group in the general linear group of degree 2.

1. Introduction

By a curve, we mean a projective, geometrically irreducible, and non-singular algebraic curve. Let C be a curve of genus g over a field K of positive characteristic $p > 0$. We call C *superspecial* (*s.sp.* for short) if its Jacobian variety is $\overline{K}$-isomorphic to the product of g supersingular elliptic curves, where $\overline{K}$ denotes the algebraic closure of K.

The problem which we mainly consider in this paper is to enumerate $\mathbb{F}_q$-isomorphism (resp. $\overline{\mathbb{F}_q}$-isomorphism) classes of s.sp. curves of genus g over the finite field $\mathbb{F}_q$ of q elements, where q is a power of p. Note that it suffices to consider the case of $q = p$ and p^2 since the number of isomorphism classes of s.sp. curves over $\mathbb{F}_{p^a}$ depends on the parity of a (cf. [11, Proposition 2.3.1]). If $g \leq 3$, there are some theoretical approaches based on Torelli's theorem to find s.sp. curves (cf. [2], [22, Prop. 4.4] for $g = 1$, [6], [8], [16] for $g = 2$, and [5], [7] for $g = 3$). Different from the case of $g \leq 3$, these approaches are considered to be not so effective for $g \geq 4$ by the following reason: The dimension of the moduli space of curves of genus $g \geq 4$ is strictly less than that of the moduli space of principally polarized abelian varieties of dimension g.

In the *non-hyperelliptic* case for $g \geq 4$, computational approaches to enumerate s.sp. curves were proposed, and the enumeration in some small particular characteristic has been

---

2010 *Mathematics Subject Classification*. 14G05, 14G15, 14G50, 14H45, 14Q05, 68W30
Key words and phrases. Hyperelliptic curves, superspecial curves, maximal curves, rational points
*Graduate School of Information Science and Technology, The University of Tokyo.
†Graduate School of Environment and Information Sciences, Yokohama National University.

completed (cf. [9], [11], [10] for $g = 4$, and [12] for $g = 5$). In particular, the isomorphism classes of s.sp. non-hyperelliptic curves of genus 4 over $\mathbb{F}_q$ are determined for $q = 5^{2e-1}$, 5^{2e}, 7^{2e-1}, 7^{2e}, and 11^{2e-1}, where e is a natural number.

A fascinating fact in the hyperelliptic case is that the existence of a s.sp. hyperelliptic curve of genus g in characteristic p implies that of a maximal (resp. minimal) curve of genus g over $\mathbb{F}_{p^2}$, see [10, Subsection 2.2] for a review of this fact. Ekedahl [3, Theorem 1.1] showed $p \geq 2g + 1$ if a s.sp. hyperelliptic curve exists for $(g, p) \neq (1, 2)$. While the existence of s.sp. hyperelliptic curves of given genus is known for many p with some congruent relations (e.g., [18], [20], and see also [17], [19], [21] for the existence of maximal curves of various types), the enumeration of s.sp. ones of genus $g \geq 4$ has not been completed yet even for small particular p.

This paper is the full-version of our conference paper [10] which enumerates s.sp. hyperelliptic curves of genus 4 for $q = 11^{2e-1}$, 11^{2e}, 13^{2e-1}, 13^{2e}, 17^{2e-1}, 17^{2e}, and 19^{2e-1}. The following (Theorems 1 and 2) are the main theorems of [10]:

THEOREM 1 ([10], Theorem 1). *There is no s.sp. hyperelliptic curve of genus* 4 *in characteristic* 11 *and* 13.

THEOREM 2 ([10], Theorem 2). *There exist exactly five* (*resp.* 25) *s.sp. 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 exactly two s.sp. hyperelliptic curves of genus* 4 *over the algebraic closure in characteristic* 17 *up to isomorphism.*

In particular, Theorem 1 relaxes the restriction on non-hyperelliptic curves in [11, Theorem B].

COROLLARY 1 ([10], Corollary 2). *There exist exactly* 30 (*resp. nine*) *s.sp. curves of genus* 4 *over* $\mathbb{F}_{11}$*, up to isomorphism over* $\mathbb{F}_{11}$ (*resp.* $\overline{\mathbb{F}_{11}}$).

Additional and new results, that are not given in [10], of this paper are as follows:

(1) Complete proofs of computational results in [10],
(2) New results on enumeration for $q = 19^2$ and 23 (Theorems 3 and 4 below),
(3) Computation of automorphism groups of enumerated s.sp. hyperelliptic curves.

THEOREM 3. *There exist exactly* 12 (*resp.* 18) *s.sp. 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 exactly two s.sp. hyperelliptic curves of genus* 4 *over the algebraic closure in characteristic* 19 *up to isomorphism.*

THEOREM 4. *There exist exactly* 14 *s.sp. hyperelliptic curves of genus* 4 *over* $\mathbb{F}_{23}$ *up to isomorphism over* $\mathbb{F}_{23}$. *Moreover, there exist exactly four s.sp. hyperelliptic curves of genus* 4 *over* $\mathbb{F}_{23}$ *up to isomorphism over the algebraic closure.*

All the computations to obtain our main results were done on Magma V2.26-10 [1], and codes and log files are available at [24].

The rest of this paper is organized as follows. Section 2 gives a review of general facts on hyperelliptic curves over finite fields. In Section 2.3, we review the enumeration method given in [10]. The method consists of the following three ingredients: (A) Algorithm to list up s.sp. hyperelliptic curves, (B) Reduction of defining equations of hyperelliptic curves, and (C) Isomorphism testing. Section 3 gives complete proofs of computational results in [10], and new results on enumeration for $q = 19^2$ and 23. Section 4 studies automorphism groups of enumerated s.sp. hyperelliptic curves. Specifically, we give an algorithm to compute the automorphism group of a (not necessarily s.sp.) hyperelliptic curve. Note that in this paper we do not mention the asymptotic complexity but the practicality of our algorithms only.

2. Preliminaries

In this section, we review a realization of hyperelliptic curves, a criterion for their superspeciality and a method to enumerate s.sp. hyperelliptic curves.

2.1. Hyperelliptic curves

Let K be a field of characteristic $\neq 2$. Let C be a hyperelliptic curve over K, i.e., a curve over K admitting a morphism over K of degree 2 from C to the projective line $\mathbf{P}^1$. As seen in [10, Subsection 2.1], if the cardinality of K is greater than $2g+1$, then C is realized as the desingularization of the homogenization of

$$y^2 = f(x), \tag{2.1.1}$$

where $f(x)$ is a polynomial over K of degree $2g+2$ with non-zero discriminant.

The next lemma tells us when two hyperelliptic curves C_1 and C_2 are isomorphic.

LEMMA 2.1.1 (cf. [10], Lemma 2.1). *Let $f_1(x)$ and $f_2(x)$ be elements of $K[x]$ of degree $2g+2$ with non-zero discriminants. Let C_1 and C_2 be the hyperelliptic curves over K defined by $y^2 = f_1(x)$ and $y^2 = f_2(x)$ respectively. Set $F_i(X, Z) = Z^{2g+2} f_i(X/Z) \in K[X, Z]$. Let k be a field containing K. There exists a k-isomorphism from C_1 to C_2 if and only if there exists $(h, \lambda) \in \mathrm{GL}_2(k) \times k^{\times}$ such that $F_1((X, Z) \cdot {}^t h) = \lambda^2 F_2(X, Z)$.*

2.2. Cartier-Manin matrix and superspeciality

Let K be a perfect field and let $\overline{K}$ denote the algebraic closure of K. Let C be a nonsingular projective curve over K. We say that C is *superspecial* (s.sp. for short) if its Jacobian $\mathrm{Jac}(C)$ is $\overline{K}$-isomorphic to the product of some supersingular elliptic curves.

For a curve C over K, its *Cartier-Manin matrix* is defined as a matrix representing the Cartier operator on the space $H^0(C, \Omega_C^1)$ of holomorphic differentials of C (cf. [23, Section 2]), which is uniquely determined as soon as we choose a basis of $H^0(C, \Omega_C^1)$. Here is a well-known method (cf. [4], [14], [23, Section 2]) to compute a Cartier-Manin matrix of a hyperelliptic curve.

PROPOSITION 2.2.1. *Let C be a hyperelliptic curve $y^2 = f(x)$ of genus g over K, where* $\deg(f)$ *is either $2g+1$ or $2g+2$. Then the $g \times g$ matrix whose (i, j)-entry is the coefficient of x^{pi-j} in $f^{(p-1)/2}$ for $1 \leq i, j \leq g$ is a Cartier-Manin matrix of C.*

The next corollary follows immediately from the fact that C is s.sp. if and only if the Cartier operator on the cohomology group $H^0(C, \Omega_C^1)$ is zero (cf. [15]).

COROLLARY 2.2.2. *Let C be a hyperelliptic curve $y^2 = f(x)$ of genus g over K, where* $\deg(f)$ *is either $2g+1$ or $2g+2$. Then C is s.sp. if and only if the coefficients of x^{pi-j} in $f^{(p-1)/2}$ are equal to 0 for all integers i, j with $1 \leq i, j \leq g$.*

2.3. Ingredients to enumerate superspecial hyperelliptic curves

Assume that K is the finite filed $\mathbb{F}_q$ or its algebraic closure $\overline{\mathbb{F}_q}$, where q is a power of an odd prime p. This subsection reviews a method in [10] to enumerate s.sp. hyperelliptic curves over $\mathbb{F}_q$. The same method shall be applied to prove main theorems (Theorems 3 and 4 in

Section 1) in this paper, and it consists of the following three ingredients described precisely in [10, Section 3]: (A) Algorithm to list up s.sp. hyperelliptic curves, (B) Reduction of defining equations of hyperelliptic curves, and (C) Isomorphism testing. Since concrete algorithms for (A) and (C) and a proof of (B) are already given in [10], we here describe only the idea of each ingredient.

(A) Algorithm to list up superspecial hyperelliptic curves: In [10, Section 3.1], we constructed an algorithm with a pseudocode to list up all s.sp. hyperelliptic curves of genus g over $\mathbb{F}_q$ for a given (g, q). The idea is reducing the enumeration of s.sp. curves into solving multivariate systems over finite fields (the same idea is also used in a series of papers [9], [11], [10], [12]). By Lemma 2.3.1 below, any hyperelliptic curve of genus g over $\mathbb{F}_q$ is given by the equation $cy^2 = f(x)$ for $c = 1$ or ϵ with $\epsilon \in \mathbb{F}_q^\times \smallsetminus (\mathbb{F}_q^\times)^2$, where $f \in \mathbb{F}_q[x]$ is a degree $(2g + 2)$-polynomial of the form (2.3.1) with non-zero discriminant. For each c and b, we derive a multivariate system of algebraic equations from the condition that $cy^2 = f(x)$ is s.sp. (i.e., the Cartier-Manin matrix is zero), that is,

$$\left(\text{the coefficient of } x^{pi-j} \text{ in } f^{(p-1)/2}\right) = 0$$

for each $1 \leq i, j \leq g$, where we regard unknown coefficients a_i for $0 \leq i \leq 2g - 1$ as indeterminates. For each root of the system, we check whether f has no double root in $\overline{\mathbb{F}_q}$ by constructing the minimal splitting field of f. In this way, we can collect all f of the form (2.3.1) with non-zero discriminant such that $cy^2 = f(x)$ is s.sp..

(B) Reduction of defining equations of hyperelliptic curves: In [10, Section 3.2], we gave the following elementary reduction of defining equations of hyperelliptic curves:

LEMMA 2.3.1 ([10], Lemma 2). *Assume that p and $2g+2$ are coprime. Let $\epsilon \in K^\times \smallsetminus (K^\times)^2$. Any hyperelliptic curve C of genus g over K is K-isomorphic to the desingularization of the homogenization of*

$$cy^2 = x^{2g+2} + bx^{2g} + a_{2g-1}x^{2g-1} + \cdots + a_1x + a_0 \tag{2.3.1}$$

for $a_i \in K$ with $i = 0, 1, \ldots, 2g - 1$ where $b = 0, 1, \epsilon$ and $c = 1, \epsilon$.

REMARK 2.3.2.
(1) As we pointed out in [10, Section 3.2], a good method of reduction over an algebraically closed field is to translate three ramified points of the corresponding morphism $C \to \mathbf{P}^1$ of degree 2 to $\{0, 1, \infty\}$. However, we can not adopt this method in Lemma 2.3.1 since the ramified points are not necessarily K-rational points.
(2) Let $h(x)$ be a monic polynomial over K with non-zero discriminant. As mentioned in [10, Remark 3], the hyperelliptic curves $C_1 : y^2 = h(x)$ and $C_2 : \epsilon y^2 = h(x)$ with $\epsilon \in K^\times \smallsetminus (K^\times)^2$ are isomorphic to each other over $K[\sqrt{\epsilon}]$ via $(x, y) \mapsto (x, \sqrt{\epsilon}y)$. In particular, the superspeciality of C_1 is equivalent to that of C_2.

(C) Isomorphism testing: We suppose that p and $2g + 2$ are coprime. Determining whether two hyperelliptic curves are isomorphic to each other over K is reduced into testing whether a multivariate system has a root over K or not. Let C_1 and C_2 be hyperelliptic curves of genus g over $\mathbb{F}_q$. Recall from Lemma 2.3.1 that each hyperelliptic curve C_i is the desingularization of the homogenization of $c_i y^2 = f_i(x)$ for $c_i = 1$ or ϵ with $\epsilon \in \mathbb{F}_q^\times \smallsetminus (\mathbb{F}_q^\times)^2$, where $f_i(x)$ is a polynomial in $\mathbb{F}_q[x]$ of degree $2g + 2$ with non-zero discriminant. For each $1 \leq i \leq 2$, let F_i denote the homogenization of $c_i^{-1} f_i$ with respect to an extra variable z. Lemma 2.1.1 shows that C_1 and C_2 are isomorphic over K if and only if there exist $\lambda \in K^\times$ and $h \in \mathrm{GL}_2(K)$ such that $h \cdot F_1 = \lambda^2 F_2$, where $h \cdot F_1(x, z) := F_1((x, z) \cdot {}^t h)$. This is equivalent to that the following multivariate system has a root over K:

$$\begin{cases} \big(\text{all the coefficients in } h \cdot F_1 - \lambda^2 F_2\big) = 0 \\ \lambda\mu = 1 \\ \det(h)\nu = 1 \end{cases} \tag{2.3.2}$$

where λ, μ, ν and all entries of h are indeterminates. One can decide whether the system (2.3.2) has a root over K or not by computing Gröbner bases of the corresponding ideal. Note that adding field equations such as $\lambda^q = \lambda$ is necessary if $K = \mathbb{F}_q$.

3. Enumeration of superspecial hyperelliptic curves

This section proves Theorems 1 – 4 stated in Section 1. In Section 3.1, we give complete proofs of computational results in [10] for $p \leq 19$ with $g = 4$. New enumeration results for $(g, q) = (4, 19^2)$ and $(4, 23)$ are stated and proved in Section 3.2. The three ingredients in Section 2.3 are applied to computational enumeration for obtaining computational results in Sections 3.1 and 3.2. As a further application, $\mathbb{F}_{p^2}$-maximal curves and $\mathbb{F}_{p^2}$-minimal curves are found in Section 3.3 from among enumerated s.sp. hyperelliptic curves.

3.1. Complete proofs of computational results in [10]

After stating results in [10] (Propositions 3.1.1–3.1.4 below), we prove them by executing enumeration method based on the ingredients in Section 2.3. Our enumeration method was implemented on Magma V2.26-10 [1] in its 64-bit version on a PC with macOS Monterey 12.0.1, at 2.6 GHz CPU 6 Core (Intel Core i7) and 16GB memory. We succeeded in finishing required computation within a day in total. The source codes and the log files together with detailed information on timing are available at [24].

Proposition 3.1.1 ([10], Propositions 2 and 3). *There does not exist any s.sp. hyperelliptic curve of genus* 4 *over* $\mathbb{F}_q$ *defined by an equation of the form* (2.3.1) *for each of* $q = 11^2$ *and* $q = 13^2$.

Proposition 3.1.2 ([10], Proposition 4). *There exist exactly five* (*resp. two*) *s.sp. hyperelliptic curves of genus* 4 *over* $\mathbb{F}_{17}$*, up to isomorphism over* $\mathbb{F}_{17}$ (*resp.* $\overline{\mathbb{F}_{17}}$). *Specifically, the five* $\mathbb{F}_{17}$*-isomorphisms classes are represented by*

(1) $C_1 : y^2 = x^{10} + x$,
(2) $C_2 : y^2 = x^{10} + x^7 + 13x^4 + 12x$,
(3) $C_3 : y^2 = x^{10} + x^7 + 14x^6 + 6x^5 + 12x^3 + 5x^2 + 7x + 6$,
(4) $C_4 : y^2 = x^{10} + x^8 + x^7 + 15x^6 + 4x^5 + 12x^4 + 15x^3 + 11x^2 + 9x + 4$, *and*
(5) $C_5 : y^2 = x^{10} + x^8 + 2x^7 + 9x^5 + x^4 + 10x^3 + 8x^2 + 11x + 16y^2 + 5$.

The two $\overline{\mathbb{F}_{17}}$*-isomorphism classes are represented by*

(1) $C_1^{(\mathrm{alc})} : y^2 = x^{10} + x$, *and*
(2) $C_2^{(\mathrm{alc})} : y^2 = x^{10} + x^7 + 13x^4 + 12x$.

(The subscript "alc" stands for algebraic closure.)

Proposition 3.1.3 ([10], Proposition 5). *There exist exactly* 25 (*resp. two*) *s.sp. hyperelliptic curves of genus* 4 *over* $\mathbb{F}_{17^2}$*, up to isomorphism over* $\mathbb{F}_{17^2}$ (*resp.* $\overline{\mathbb{F}_{17^2}}$). *Specifically, the* 25 $\mathbb{F}_{17^2}$*-isomorphisms classes are represented by*

(1) $y^2 = x^{10} + x$,
(2) $y^2 = x^{10} + \zeta x$,
(3) $y^2 = x^{10} + \zeta^2 x$,
(4) $y^2 = x^{10} + \zeta^3 x$,
(5) $y^2 = x^{10} + \zeta^4 x$,
(6) $y^2 = x^{10} + \zeta^5 x$,
(7) $y^2 = x^{10} + \zeta^6 x$,
(8) $y^2 = x^{10} + \zeta^7 x$,
(9) $y^2 = x^{10} + \zeta^8 x$,
(10) $y^2 = x^{10} + x^7 + 13x^4 + 12x$,
(11) $y^2 = x^{10} + x^7 + \zeta^{66}x^6 + \zeta^{78}x^5 + \zeta^{138}x^3 + \zeta^{186}x^2 + 7x + \zeta^{174}$,
(12) $y^2 = x^{10} + \zeta x^7 + \zeta^{74}x^4 + \zeta^{237}x$,
(13) $y^2 = x^{10} + \zeta^2 x^7 + \zeta^{76}x^4 + \zeta^{240}x$,
(14) $y^2 = x^{10} + x^8 + \zeta^3 x^7 + \zeta^{98}x^6 + \zeta^{153}x^5 + \zeta^{287}x^4 + \zeta^{71}x^3 + \zeta^8 x^2 + \zeta^{71}x + \zeta^{254}$,
(15) $y^2 = x^{10} + x^8 + \zeta^3 x^7 + \zeta^{226}x^6 + \zeta^{37}x^4 + \zeta^{147}x^3 + \zeta^{91}x^2 + \zeta^{145}x + \zeta^{127}$,
(16) $y^2 = x^{10} + x^8 + \zeta^5 x^7 + \zeta^{138}x^6 + \zeta^{60}x^5 + \zeta^{222}x^4 + \zeta^{128}x^3 + \zeta^{278}x^2 + \zeta^{41}x + \zeta^{24}$,
(17) $y^2 = x^{10} + x^8 + \zeta^8 x^7 + \zeta^{267}x^6 + \zeta^{50}x^5 + \zeta^{39}x^4 + \zeta^{94}x^3 + \zeta^{58}x^2 + \zeta^{191}x + \zeta^{166}$,
(18) $y^2 = x^{10} + x^8 + \zeta^{10}x^7 + \zeta^{219}x^6 + \zeta^{137}x^5 + \zeta^{103}x^4 + \zeta^{158}x^3 + \zeta^{152}x^2 + \zeta^2 x + \zeta^{220}$,
(19) $y^2 = x^{10} + x^8 + \zeta^{13}x^7 + \zeta^{69}x^6 + \zeta^{210}x^5 + \zeta^{22}x^4 + \zeta^{245}x^3 + \zeta^{25}x^2 + \zeta^{35}x + \zeta^{10}$,
(20) $y^2 = x^{10} + x^8 + \zeta^{14}x^7 + \zeta^{104}x^6 + \zeta^{187}x^5 + \zeta^{188}x^4 + 11x^3 + \zeta^{68}x^2 + \zeta^{148}x + \zeta^{280}$,
(21) $y^2 = x^{10} + x^8 + \zeta^{16}x^7 + \zeta^{83}x^6 + \zeta^{276}x^5 + \zeta^{164}x^4 + \zeta^{102}x^3 + \zeta^{111}x^2 + \zeta^2 x + \zeta^{152}$,
(22) $y^2 = x^{10} + x^8 + \zeta^{16}x^7 + \zeta^{130}x^6 + \zeta^{274}x^5 + \zeta^{133}x^4 + \zeta^9 x^3 + \zeta^{55}x^2 + \zeta^{175}x + \zeta^{193}$,
(23) $y^2 = x^{10} + x^8 + \zeta^{19}x^7 + \zeta^{120}x^6 + \zeta^{239}x^5 + \zeta^{123}x^4 + \zeta^{229}x^3 + \zeta^{47}x^2 + \zeta^{145}x + \zeta^{253}$,
(24) $y^2 = x^{10} + x^8 + \zeta^{22}x^7 + \zeta^{250}x^6 + \zeta^{89}x^5 + \zeta^{182}x^4 + \zeta^9 x^3 + \zeta^{225}x^2 + \zeta^{282}x + \zeta^{113}$,
(25) $y^2 = x^{10} + x^8 + \zeta^{41}x^7 + \zeta^{41}x^6 + \zeta^{149}x^5 + \zeta^{169}x^4 + 5x^3 + \zeta^{197}x^2 + \zeta^{26}x + \zeta^{66}$,

where we take $\zeta = -8 + \sqrt{61} \in \mathbb{F}_{17^2}$, *and the two* $\overline{\mathbb{F}_{17^2}}$*-isomorphism classes are represented by the same equations as those in* Proposition 3.1.2.

PROPOSITION 3.1.4 ([10], Proposition 6). *There exist exactly* 12 (*resp. two*) *s.sp. hyperelliptic curves of genus* 4 *over* $\mathbb{F}_{19}$*, up to isomorphism over* $\mathbb{F}_{19}$ (*resp.* $\overline{\mathbb{F}_{19}}$). *Specifically, the* 12 $\mathbb{F}_{19}$*-isomorphisms classes are represented by*

(1) $C_1 : y^2 = x^{10} + 1$,
(2) $C_2 : y^2 = x^{10} + 2$,
(3) $C_3 : y^2 = x^{10} + x^7 + 4x^6 + 15x^5 + 6x^4 + 8x^3 + 5x^2 + 12x + 1$,
(4) $C_4 : y^2 = x^{10} + x^8 + 7x^6 + x^4 + x^2 + 7$,
(5) $C_5 : y^2 = x^{10} + x^8 + x^7 + 12x^6 + x^5 + 10x^4 + 9x^3 + 8x^2 + 9x + 3$,
(6) $C_6 : y^2 = x^{10} + x^8 + x^7 + 13x^6 + 9x^5 + 14x^4 + 4x^3 + 11x^2 + 3x + 8$,
(7) $C_7 : y^2 = x^{10} + x^8 + 2x^7 + 6x^6 + 18x^5 + 4x^4 + 13x^3 + 18x^2 + 10x + 14$,
(8) $C_8 : y^2 = x^{10} + x^8 + 2x^7 + 12x^6 + 18x^4 + 5x^3 + x^2 + 7$,
(9) $C_9 : y^2 = x^{10} + x^8 + 4x^7 + 8x^6 + 8x^5 + 3x^4 + 11x^3 + 8x^2 + 8x + 4$,
(10) $C_{10} : y^2 = x^{10} + 2x^8 + 9x^6 + 8x^4 + 16x^2 + 15$,
(11) $C_{11} : y^2 = x^{10} + 2x^8 + x^7 + 12x^6 + 9x^5 + 2x^3 + 4x^2 + 7x + 4$, *and*
(12) $C_{12} : y^2 = x^{10} + 2x^8 + 3x^7 + 17x^6 + 9x^5 + 2x^3 + 12x^2 + 2x + 4$.

The two $\overline{\mathbb{F}_{19}}$*-isomorphism classes are represented by*

(1) $C_1^{(\mathrm{alc})} : y^2 = x^{10} + 1$, *and*
(2) $C_2^{(\mathrm{alc})} : y^2 = x^{10} + x^7 + 4x^6 + 15x^5 + 6x^4 + 8x^3 + 5x^2 + 12x + 1$.

Proofs of Propositions 3.1.1–3.1.4. Let $g = 4$. In the procedures 1–4 below, we set the following parameters:

- $(q = 11^2)$ $s_1 := 2g + 1 = 9$ and $s_2 := 2g - 2 = 8$,
- $(q = 13^2)$ $s_1 := 2g + 1 = 9$ and $s_2 := 2g - 1 = 7$,
- $(q = 17$ and $19)$ $s_1 := 2g + 1 = 9$ and $s_2 := 2g - 2 = 6$,
- $(q = 17^2)$ $s_1 := 2g = 8$ and $s_2 := 2g - 2 = 6$.

By the computer described at the beginning of this section, we conduct the following four procedures:

1. Let a_i for $0 \leq i \leq s_1 - 1$ be indeterminates.

For each $(c_{s_1}, \ldots c_{2g-1}) \in (\mathbb{F}_q)^{\oplus 2g-s_1}$ and $c_{2g} \in \{0, 1, \epsilon\}$ with $\epsilon \in \mathbb{F}_q^\times \setminus (\mathbb{F}_q^\times)^2$, proceed with the following procedures:

2. Put $f(x) := x^{2g+2}+c_{2g}x^{2g}+c_{2g-1}x^{2g-1}+\cdots+c_{s_1}x^{s_1}+a_{s_1-1}x^{s_1-1}+\cdots+a_1x+a_0$, and compute $h := f^{(p-1)/2}$ over $\mathbb{F}_q[a_0, \ldots, a_{s_1-1}][x]$.
3. Let $\mathcal{S} \subset \mathbb{F}_q[a_0, \ldots, a_{s_1-1}]$ be the set of the coefficients of the g^2 monomials in $h = f^{(p-1)/2}$, given in Proposition 2.2.1.
4. For each $(c_{s_2}, \ldots c_{s_1-1}) \in (\mathbb{F}_q)^{\oplus 2g-s_1-s_2}$, proceed with the following three steps 4a–4c:
   4a. Substitute $(c_{s_2}, \ldots c_{s_1-1})$ into $(a_{s_2}, \ldots a_{s_1-1})$ of the coefficients in each $P \in \mathcal{S}$, and put
   $$\mathcal{S}' := \{P(a_0, \ldots, a_{s_2-1}, c_{s_2}, \ldots, c_{s_1-1}) : P \in \mathcal{S}\} \cup \{a_i - c_i : s_2 \leq i \leq s_1 - 1\} .$$
   4b. With Gröbner basis algorithms, compute the roots in $(\mathbb{F}_q)^{\oplus s_1}$ of the multivariate system $P' = 0$ for all $P' \in \mathcal{S}'$ with variables $a_0, \ldots, a_{s_1-1}$.
   4c. For each solution $(c_0, \ldots, c_{s_1-1})$ to the system constructed in Step 4b, we set $f_{\rm sol} := x^{2g+2}+c_{2g}x^{2g}+c_{2g-1}x^{2g-1}+\cdots+c_{s_1}x^{s_1}+c_{s_1-1}x^{s_1-1}+\cdots+c_1x+c_0$ (the subscript "sol" stands for solution). By constructing the minimal splitting field of $f_{\rm sol}$, test whether $f_{\rm sol}$ has no double root in $\overline{\mathbb{F}_q}$ or not. If $f_{\rm sol}$ has no double root in $\overline{\mathbb{F}_q}$, store $f_{\rm sol}$.

As a computational result for each q, we obtain the set $\mathcal{F}$ of all the polynomials $f(x)$ of the form in the right hand side of (2.3.1) such that $y^2 = f(x)$ are s.sp. hyperelliptic curves of genus g over $\mathbb{F}_q$. Put $\mathcal{H}_0 := \{cy^2 - f(x) : c = 1, \epsilon \text{ and } f(x) \in \mathcal{F}\}$. For each pair (H_1, H_2) of elements in $\mathcal{H}_0$ with $H_1 \neq H_2$, the method given in the paragraph (C) of Section 2.3 decides whether $C_1 : H_1(x, y) = 0$ and $C_2 : H_2(x, y) = 0$ are isomorphic or not. Finally we obtain the set $\mathcal{H}_K \subset \mathcal{H}_0$ of representatives of K-isomorphism classes of s.sp. hyperelliptic curves of genus g over $\mathbb{F}_q$, where K is either of $\mathbb{F}_q$ and $\overline{\mathbb{F}_q}$. Propositions 3.1.1 – 3.1.4 follow from the resulting sets $\mathcal{H}_K$ with $K = \mathbb{F}_q$ or $\overline{\mathbb{F}_q}$ for $q = 11^2$, 13^2, 17, 17^2, and 19. □

REMARK 3.1.5. In our implementation, Magma's built-in function Variety was used to solve multivariate systems over finite fields.

3.2. New results in characteristic 19 and 23

We here state new enumeration results for $(g, q) = (4, 19^2)$ and $(4, 23)$. The proofs are omitted to write down since they are done in a way similar to the proofs of Propositions 3.1.1–3.1.4, where the parameters are

- $(q = 19^2)$ $s_1 := 2g = 8$ and $s_2 := 2g - 2 = 6$,
- $(q = 23)$ $s_1 := 2g = 8$ and $s_2 := 2g - 3 = 5$.

PROPOSITION 3.2.1. *There exist exactly* 18 (*resp.* two) *s.sp. hyperelliptic curves of genus* 4 *over* $\mathbb{F}_{19^2}$, *up to isomorphism over* $\mathbb{F}_{19^2}$ (*resp.* $\overline{\mathbb{F}_{19^2}}$). *Specifically, the* 18 $\mathbb{F}_{19^2}$-*isomorphisms classes are represented by*

(1) $y^2 = x^{10} + 1$,
(2) $y^2 = x^{10} + \zeta$,
(3) $y^2 = x^{10} + \zeta^2$,
(4) $y^2 = x^{10} + \zeta^3$,
(5) $y^2 = x^{10} + \zeta^4$,
(6) $y^2 = x^{10} + \zeta^5$,
(7) $y^2 = x^{10} + \zeta^7$,
(8) $y^2 = x^{10} + \zeta^9$,
(9) $y^2 = x^{10} + x^7 + 4x^6 + 15x^5 + 6x^4 + 8x^3 + 5x^2 + 12x + 1$
(10) $y^2 = x^{10} + \zeta^2x^7 + \zeta^{31}x^6 + \zeta^{169}x^5 + \zeta^{322}x^4 + \zeta^{257}x^3 + \zeta^{352}x^2 + \zeta^{227}x + \zeta^{13}$,
(11) $y^2 = x^{10} + \zeta^2x^7 + \zeta^{61}x^6 + \zeta^{31}x^5 + \zeta^{286}x^4 + \zeta^{359}x^3 + \zeta^{232}x^2 + \zeta^{245}x + \zeta^7$,
(12) $y^2 = x^{10} + x^8 + 2x^6 + \zeta^{110}x^5 + 7x^4 + \zeta^{330}x^3 + 9x^2 + \zeta^{30}x + 17$,
(13) $y^2 = x^{10} + x^8 + x^7 + 13x^6 + 9x^5 + 14x^4 + 4x^3 + 11x^2 + 3x + 8$,
(14) $y^2 = x^{10} + x^8 + \zeta^2x^7 + \zeta x^6 + \zeta^{54}x^5 + \zeta^{151}x^4 + \zeta^{76}x^3 + \zeta^{205}x^2 + 15x + \zeta^{335}$,
(15) $y^2 = x^{10} + x^8 + \zeta^2x^7 + \zeta^{57}x^6 + \zeta^{179}x^5 + x^4 + \zeta^{298}x^3 + \zeta^{89}x^2 + \zeta^{204}x + \zeta^{171}$,
(16) $y^2 = x^{10} + x^8 + \zeta^{12}x^7 + \zeta^{196}x^6 + \zeta^{193}x^5 + \zeta^{281}x^4 + \zeta^{293}x^3 + \zeta^{107}x^2 + \zeta^{316}x + \zeta^{74}$,
(17) $y^2 = x^{10} + x^8 + 2x^7 + 12x^6 + 18x^4 + 5x^3 + x^2 + 7$,
(18) $y^2 = x^{10} + \zeta x^8 + \zeta^{122}x^6 + \zeta^3x^4 + \zeta^4x^2 + \zeta^{125}$,

where we take $\zeta = -9 - \sqrt{79} \in \mathbb{F}_{19^2}$, *and the two* $\overline{\mathbb{F}_{19^2}}$-*isomorphism classes are represented by the same equations as those in* Proposition 3.1.4.

PROPOSITION 3.2.2. *There exist exactly* 14 (*resp.* four) *s.sp. hyperelliptic curves of genus* 4 *over* $\mathbb{F}_{23}$, *up to isomorphism over* $\mathbb{F}_{23}$ (*resp.* $\overline{\mathbb{F}_{23}}$). *Specifically, the* 14 $\mathbb{F}_{23}$-*isomorphisms classes are represented by*

(1) $C_1 : y^2 = x^{10} + x^7 + 3x^4 + 10x$,
(2) $C_2 : y^2 = x^{10} + x^7 + 18x^4 + 6x$,
(3) $C_3 : y^2 = x^{10} + x^7 + 5x^6 + 3x^5 + 21x^4 + 3x^3 + 9x^2 + 4x + 21$,
(4) $C_4 : y^2 = x^{10} + x^7 + 9x^6 + 11x^5 + 19x^4 + 10x^3 + 16x^2 + 8x + 21$,
(5) $C_5 : y^2 = x^{10} + x^7 + 16x^6 + 9x^5 + 14x^4 + 2x^3 + 5x^2 + 6x + 1$,
(6) $C_6 : y^2 = x^{10} + x^7 + 17x^6 + 13x^5 + 3x^3 + 14x^2 + 20x + 15$,
(7) $C_7 : y^2 = x^{10} + x^7 + 18x^6 + 21x^4 + x^3 + 8x^2 + 20x + 21$,
(8) $C_8 : y^2 = x^{10} + x^8 + 3x^6 + 2x^4 + 2x^2 + 6$,
(9) $C_9 : y^2 = x^{10} + x^8 + 6x^6 + 22x^4 + 4x^2 + 3$,
(10) $C_{10} : y^2 = x^{10} + x^8 + 8x^6 + 7x^4 + 15x^2 + 14$,
(11) $C_{11} : y^2 = x^{10} + x^8 + 2x^7 + 6x^6 + 3x^5 + 14x^4 + 16x^3 + 11x^2 + 19$,
(12) $C_{12} : y^2 = x^{10} + x^8 + 3x^7 + x^6 + 13x^4 + 22x^3 + 12x^2 + 4$,
(13) $C_{13} : y^2 = x^{10} + x^8 + 4x^7 + 12x^6 + 2x^5 + 12x^2 + 11x + 18$, *and*
(14) $C_{14} : y^2 = x^{10} + x^8 + 5x^7 + 15x^6 + 22x^5 + 11x^4 + 7x^2 + 18x + 17$.

The four $\overline{\mathbb{F}_{23}}$-*isomorphism classes are represented by*

(1) $C_1^{(\mathrm{alc})} : y^2 = x^{10} + x^7 + 3x^4 + 10x$,
(2) $C_2^{(\mathrm{alc})} : y^2 = x^{10} + x^7 + 18x^4 + 6x$,
(3) $C_3^{(\mathrm{alc})} : y^2 = x^{10} + x^7 + 5x^6 + 3x^5 + 21x^4 + 3x^3 + 9x^2 + 4x + 21$, *and*

(4) $C_4^{(\mathrm{alc})} : y^2 = x^{10} + x^7 + 9x^6 + 11x^5 + 19x^4 + 10x^3 + 16x^2 + 8x + 21$.

3.3. Application to finding maximal curves and minimal curves

Since any maximal or minimal curve over $\mathbb{F}_{p^2}$ is s.sp., it is included in enumerated s.sp. curves over $\mathbb{F}_{p^2}$ if exists. We have non-existence results (Corollary 3.3.1 below) from Theorem 1 for $p = 11$ and 13, whereas we find $\mathbb{F}_{p^2}$-maximal curves and $\mathbb{F}_{p^2}$-minimal curves for $p = 17$, 19, and 23 (Corollaries 3.3.2–3.3.4 below). Using a computer, we find them by computing the number of $\mathbb{F}_{p^2}$-rational points on s.sp. curves in Propositions 3.1.2–3.2.2.

COROLLARY 3.3.1 ([10], Corollaries 3 and 4). *There does not exist any $\mathbb{F}_{p^2}$-maximal (resp. minimal) hyperelliptic curve of genus 4 for each of $p = 11$ and 13.*

COROLLARY 3.3.2 ([10], Corollary 5). *There exists exactly two (resp. two) $\mathbb{F}_{17^2}$-maximal (resp. $\mathbb{F}_{17^2}$-minimal) hyperelliptic curves of genus 4 over $\mathbb{F}_{17^2}$ up to isomorphism over $\mathbb{F}_{17^2}$. Specifically, the two maximal curves are given by*

$$y^2 = x^{10} + x,$$
$$y^2 = x^{10} + x^7 + 13x^4 + 12x,$$

respectively. The two minimal curves are given by

$$y^2 = x^{10} + x^8 + \zeta^{16}x^7 + \zeta^{83}x^6 + \zeta^{276}x^5 + \zeta^{164}x^4 + \zeta^{102}x^3 + \zeta^{111}x^2 + \zeta^2 x + \zeta^{152},$$
$$y^2 = x^{10} + x^8 + \zeta^{22}x^7 + \zeta^{250}x^6 + \zeta^{89}x^5 + \zeta^{182}x^4 + \zeta^9x^3 + \zeta^{225}x^2 + \zeta^{282}x + \zeta^{113},$$

respectively, where we take $\zeta = -8 + \sqrt{61} \in \mathbb{F}_{17^2}$.

COROLLARY 3.3.3 ([10], Corollary 6). *There exists exactly two (resp. two) $\mathbb{F}_{19^2}$-maximal (resp. $\mathbb{F}_{19^2}$-minimal) hyperelliptic curves of genus 4 over $\mathbb{F}_{19^2}$ up to isomorphism over $\mathbb{F}_{19^2}$. Specifically, the two maximal curves are given by*

$$y^2 = x^{10} + 1,$$
$$y^2 = x^{10} + x^7 + 4x^6 + 15x^5 + 6x^4 + 8x^3 + 5x^2 + 12x + 1,$$

respectively. The two minimal curves are given by

$$y^2 = x^{10} + x^8 + \zeta^2x^7 + \zeta^{57}x^6 + \zeta^{179}x^5 + x^4 + \zeta^{298}x^3 + \zeta^{89}x^2 + \zeta^{204}x + \zeta^{171},$$
$$y^2 = x^{10} + x^8 + 2x^7 + 12x^6 + 18x^4 + 5x^3 + x^2 + 7,$$

respectively, where we take $\zeta = -9 - \sqrt{79} \in \mathbb{F}_{19^2}$.

COROLLARY 3.3.4. *There exist $\mathbb{F}_{23^2}$-maximal hyperelliptic curves of genus 4 defined over $\mathbb{F}_{23}$. There also exists an $\mathbb{F}_{23^2}$-minimal hyperelliptic curve of genus 4 over $\mathbb{F}_{23}$. Specifically, the following 11 hyperelliptic curves over $\mathbb{F}_{23}$ are $\mathbb{F}_{23^2}$-maximal:*

$$y^2 = x^{10} + x^7 + 3x^4 + 10x,$$
$$y^2 = x^{10} + x^7 + 18x^4 + 6x,$$
$$y^2 = x^{10} + x^7 + 5x^6 + 3x^5 + 21x^4 + 3x^3 + 9x^2 + 4x + 21,$$
$$y^2 = x^{10} + x^7 + 9x^6 + 11x^5 + 19x^4 + 10x^3 + 16x^2 + 8x + 21,$$
$$y^2 = x^{10} + x^7 + 16x^6 + 9x^5 + 14x^4 + 2x^3 + 5x^2 + 6x + 1,$$
$$y^2 = x^{10} + x^7 + 18x^6 + 21x^4 + x^3 + 8x^2 + 20x + 21,$$
$$y^2 = x^{10} + x^8 + 3x^6 + 2x^4 + 2x^2 + 6,$$
$$y^2 = x^{10} + x^8 + 6x^6 + 22x^4 + 4x^2 + 3,$$

$$y^2 = x^{10} + x^8 + 8x^6 + 7x^4 + 15x^2 + 14,$$
$$y^2 = x^{10} + x^8 + 4x^7 + 12x^6 + 2x^5 + 12x^2 + 11x + 18,$$
$$y^2 = x^{10} + x^8 + 5x^7 + 15x^6 + 22x^5 + 11x^4 + 7x^2 + 18x + 17\,.$$

On the other hand, the following curve over $\mathbb{F}_{23}$ is $\mathbb{F}_{23^2}$-minimal:

$$y^2 = x^{10} + x^8 + 2x^7 + 6x^6 + 3x^5 + 14x^4 + 16x^3 + 11x^2 + 19\,.$$

REMARK 3.3.5. The maximal hyperelliptic curve $y^2 = x^{10} + x$ (resp. $y^2 = x^{10} + 1$) over $\mathbb{F}_{17^2}$ (resp. $\mathbb{F}_{19^2}$) is of known type, see e.g., [18] for more general results on the existence of such a kind of maximal hyperelliptic curves.

4. Computing automorphism groups of enumerated hyperelliptic curves

In this section, we present an algorithm to compute the automorphism group of a hyperelliptic curve over $K = \mathbb{F}_q$ or $\overline{\mathbb{F}_q}$, where q is a power of a prime $p > 2$. Note that our algorithm works for not only s.sp. but also arbitrary hyperelliptic one such that p and $2g + 2$ are coprime. As an application of the algorithm, this section also studies the automorphism groups of s.sp. hyperelliptic curves of genus 4 enumerated in Section 3. Moreover, we check that our enumeration in Section 3 is compatible with the Galois cohomology theory.

4.1. Description of automorphism groups of hyperelliptic curves

Assume that p and $2g + 2$ are coprime. Let C be a hyperelliptic curve of genus g over K defined by $y^2 = f(x)$ for some monic polynomial $f(x)$ in $K[x]$ of degree $2g + 2$. Let F denote the homogenization of f with respect to an extra variable z.

In order to describe the automorphism group of C, we consider the groups

$$\tilde{G}_K = \{(h, \lambda) \in \mathrm{GL}_2(K) \times K^\times \mid F(h \cdot {}^t(X, Z)) = \lambda^2 F(X, Z)\},$$
$$G_K = \{h \in \mathrm{GL}_2(K) \mid F(h \cdot {}^t(X, Z)) = F(X, Z)\},$$

and $\mu_{g+1}(K) = \{a \in K^\times \mid a^{g+1} = 1\}$, where G_K is considered as a subgroup of $\tilde{G}_K$, via the homomorphism sending $h \in G_K$ to $(h, 1) \in \tilde{G}_K$.

LEMMA 4.1.1. *There exists a diagram*

$$\begin{tikzcd}
1 \arrow[r] & K^\times \arrow[r, "\psi"] & \tilde{G}_K \arrow[r, "\varphi"] & \mathrm{Aut}_K(C) \arrow[r] & 1 \\
1 \arrow[r] & \mu_{g+1}(K) \arrow[r] \arrow[u, hook, "\cup"'] & G_K \arrow[r, "\varphi|_{G_K}"] \arrow[u, hook, "\cup"'] & \mathrm{Aut}_K(C) \arrow[u, equal]
\end{tikzcd}$$

with exact horizontal sequences, where φ sends $\left(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \lambda\right)$ to the automorphism mapping (x, y) to $\left(\frac{\alpha x+\beta}{\gamma x+\delta}, \frac{\lambda y}{(\gamma x+\delta)^{g+1}}\right)$ and ψ sends u to $\left(\begin{pmatrix} u & 0 \\ 0 & u \end{pmatrix}, u^{g+1}\right)$. Moreover, if the $(g + 1)$-th power map on $K^\times$ is surjective, then, $\varphi|_{G_K}$ is surjective.

Proof. The surjectivity of φ holds, as any automorphism is given in the form as in the lemma (cf. the proof of [10, Lemma 1]). Then obviously the kernel of φ is equal to the image of ψ. The lower exact sequence is immediately obtained by restricting the upper one to G_K. If the $(g + 1)$-th power map on $K^\times$ is surjective, then any automorphism determined by

$\left(\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}, \lambda\right) \in \tilde{G}_K$ is equal to that determined by $\left(\mu^{-1}\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}, 1\right)$ for μ with $\mu^{g+1} = \lambda$, whence $\varphi|_{G_K}$ is surjective. $\square$

Consider the case of $g = 4$. Applying this lemma for an algebraically closed field k, we have $\mathrm{Aut}(C) \simeq G_k/\boldsymbol{\mu}_5(k)$. If $K = \mathbb{F}_p$ for $p = 17, 19, 23$, the group $\boldsymbol{\mu}_5(K)$ is trivial, whence we have $\mathrm{Aut}_K(C) \simeq G_K$.

4.2. Algorithm to compute automorphism groups

In this subsection, we present an algorithm to compute the automorphism group of a hyperelliptic curve over $K = \mathbb{F}_q$ or $\overline{\mathbb{F}_q}$. Note that our algorithm works for not only s.sp. but also arbitrary hyperelliptic one such that p and $2g+2$ are coprime, and such that the $(g+1)$-th power map on $K^\times$ is surjective. Let C be a hyperelliptic curve of genus g over K defined by $cy^2 = f(x)$ for some polynomial $f(x)$ in $K[x]$ of degree $2g+2$. Let F denote the homogenization of f with respect to an extra variable Z.

The algorithm below computes $\mathrm{Aut}_K(C)$ as the set of complete representatives of $G_K/\boldsymbol{\mu}_{g+1}(K)$ in Lemma 4.1.1. Note that G_K is finite since both $\mathrm{Aut}_K(C) \simeq G_K/\boldsymbol{\mu}_{g+1}(K)$ and $\boldsymbol{\mu}_{g+1}(K)$ are finite.

Algorithm to compute $\mathrm{Aut_K(C)}$**.** For the input $(c, f(x))$, and q as above, the following five steps compute G_K for $K = \mathbb{F}_q$, or $K = \overline{\mathbb{F}_q}$:

(1) Let b_1, b_2, b_3, b_4, and ν be indeterminates, and set

$$F(X, Z) := c^{-1}Z^{2g+2}f(X/Z) \quad \text{and} \quad h := \begin{pmatrix}b_1 & b_2\\ b_3 & b_4\end{pmatrix},$$

where h is a square matrix whose entries are indeterminates.

(2) Compute $F'(X, Z) := F((X, Z)\cdot{}^t h) - F(X, Z)$ over the polynomial ring $K[b_1, b_2, b_3, b_4, \nu][X, Z]$ whose coefficient ring is also a polynomial ring.

(3) Let $\mathcal{C}_F$ be the set of the coefficients of the non-zero terms in $F'(X, Z)$. We put

$$\mathcal{C} := \mathcal{C}_F \cup \{\det(h)\nu - 1\}.$$

For $K = \mathbb{F}_q$, we replace $\mathcal{C}$ by

$$\mathcal{C} \cup \{b_i^q - b_i : 1 \le i \le 4\} \cup \{\nu^q - \nu\}.$$

(4) Compute $V_K(\langle \mathcal{C}\rangle)$ in $\mathbb{A}^5(K)$, where $V_K(\langle \mathcal{C}\rangle)$ denotes the set of zeros of the ideal $\langle \mathcal{C}\rangle \subset K[b_1, b_2, b_3, b_4, \nu]$. One can do this by computing Gröbner bases; for $K = \overline{\mathbb{F}_q}$, field extensions are constructed.

(5) For the computed finite group G_K given by

$$G_K = \left\{\begin{pmatrix}b_1 & b_2\\ b_3 & b_4\end{pmatrix} : (b_1, b_2, b_3, b_4, \nu) \in V_K(\langle \mathcal{C}\rangle) \text{ for some } \nu \in K^\times\right\},$$

compute $G_K/\boldsymbol{\mu}_5(K)$, and then output it.

4.3. Automorphism groups of enumerated superspecial hyperelliptic curves

Executing the algorithm in Section 4.2 on the computer algebra system Magma, we compute automorphism groups of s.sp. hyperelliptic curves of genus 4 enumerated in Section 3. All elements of G_K for each automorphism group $\mathrm{Aut}_K(C)$ is computed, and $\mathrm{Aut}_K(C)$ is also computed as the set of representatives of a quotient group of G_K. The orders of automorphism groups over $\mathbb{F}_p$ with those over $\overline{\mathbb{F}_p}$ are summarized in Table 1. Note that the group structure of each automorphism group is determined by Magma's built-in function GroupName. For each integer $t > 0$, we denote by $\mathbb{Z}_t$, S_t, and D_t the cyclic group of order t, the symmetric group of degree t, and the dihedral group of order $2t$, respectively.

REMARK 4.3.1. For each s.sp. curve C over $K = \mathbb{F}_p$ (resp. $\overline{\mathbb{F}_p}$) listed in Table 1, we also computed the automorphism group $\mathrm{Aut}_K(C)$ (as an abstract group) by using Magma's built-in function AutomorphismGroupOfHyperellipticCurve (resp. GoemetricAutomorphismGroup), which was recently implemented (since Magma V.2.25-7 in 2021, based on an algorithm in [13]). Note that the ideas of [13] and ours are essentially the same, while our algorithm had been proposed in a preprint (arXiv: 1907.00894 [math.AG]) of this paper before the above built-in functions were implemented.

As a result, we confirmed that the results obtained from our algorithm coincide with those obtained from Magma's built-in function(s). For example, both the automorphism groups of C_1 with $p = 17$ computed by our algorithm and Magma's built-in function(s) are $\mathbb{Z}_2$.

p	Superspecial hyperelliptic curves C over $\overline{\mathbb{F}_p}$	$\mathrm{Aut}(C)$	$\#\mathrm{Aut}(C)$	$\mathbb{F}_p$-forms C' of C	$\mathrm{Aut}_{\mathbb{F}_p}(C')$	$\#\mathrm{Aut}_{\mathbb{F}_p}(C')$
17	$C_1^{(\mathrm{alc})}$	$\mathbb{Z}_{18}$	18	C_1	$\mathbb{Z}_2$	2
				C_4	$\mathbb{Z}_2$	2
	$C_2^{(\mathrm{alc})}$	$\mathrm{SL}_2(\mathbb{F}_3)$	24	C_2	$\mathbb{Z}_2$	2
				C_3	$\mathbb{Z}_4$	4
				C_5	$\mathbb{Z}_4$	4
19	$C_1^{(\mathrm{alc})}$	$\mathbb{Z}_5 \rtimes \mathrm{D}_4$	40	C_1	D_4	8
				C_2	$\mathbb{Z}_2 \times \mathbb{Z}_2$	4
				C_4	D_4	8
				C_6	$\mathbb{Z}_{10}$	10
				C_8	$\mathbb{Z}_5 \rtimes \mathbb{Z}_4$	20
				C_9	$\mathbb{Z}_{10}$	10
				C_{10}	D_{10}	20
				C_{11}	$\mathbb{Z}_{10}$	10
				C_{12}	$\mathbb{Z}_{10}$	10
	$C_2^{(\mathrm{alc})}$	D_4	8	C_3	S_2	2
				C_5	$\mathbb{Z}_4$	4
				C_7	$\mathbb{Z}_4$	4
23	$C_1^{(\mathrm{alc})}$	$\mathbb{Z}_6$	6	C_1	$\mathbb{Z}_2$	2
				C_5	$\mathbb{Z}_2$	2
	$C_2^{(\mathrm{alc})}$	$\mathrm{SL}_2(\mathbb{F}_3)$	24	C_2	$\mathbb{Z}_2$	2
				C_6	$\mathbb{Z}_4$	4
				C_{12}	$\mathbb{Z}_4$	4
	$C_3^{(\mathrm{alc})}$	D_4	8	C_3	$\mathbb{Z}_2 \times \mathbb{Z}_2$	4
				C_8	D_4	8
				C_{10}	$\mathbb{Z}_2 \times \mathbb{Z}_2$	4
				C_{11}	$\mathbb{Z}_4$	4
				C_{14}	D_4	8
	$C_4^{(\mathrm{alc})}$	$\mathbb{Z}_2 \times \mathbb{Z}_2$	4	C_4	$\mathbb{Z}_2 \times \mathbb{Z}_2$	4
				C_7	$\mathbb{Z}_2 \times \mathbb{Z}_2$	4
				C_9	$\mathbb{Z}_2 \times \mathbb{Z}_2$	4
				C_{13}	$\mathbb{Z}_2 \times \mathbb{Z}_2$	4

Table 1. The automorphism groups $\mathrm{Aut}(C) := \mathrm{Aut}_{\overline{\mathbb{F}_p}}(C)$ of s.sp. hyperelliptic curves C over $\overline{\mathbb{F}_p}$ and the automorphism groups $\mathrm{Aut}_{\mathbb{F}_p}(C_i)$ of the s.sp. hyperelliptic curves C_i over $\mathbb{F}_p$ for $17 \leq p \leq 23$.

4.4. Compatibility with the Galois cohomology theory

This subsection shows that our enumeration in Section 3 is compatible with the Galois cohomology theory. Specifically, we check the below equalities (4.4.1) – (4.4.3) deduced from the Galois cohomology theory for each of enumerated s.sp. hyperelliptic curves over an algebraic closure.

For a hyperelliptic curve C over $\overline{\mathbb{F}_q}$, two elements a and b in $\mathrm{Aut}(C)$ are said to be *σ-conjugate* if $a = g^{-1}bg^{\sigma}$ for some $g \in \mathrm{Aut}(C)$, where σ is the q-th power Frobenius action on $\mathrm{Aut}(C)$. For an element $a \in \mathrm{Aut}(C)$, we denote by $\mathrm{Orb}(a)$ the orbit of a, i.e., $\mathrm{Orb}(a) := \{g^{-1}ag^{\sigma} : g \in \mathrm{Aut}(C)\}$, called the σ-conjugacy class of a. The σ-stabilizer of a is defined as the subgroup $\{g \in \mathrm{Aut}(C) : a = g^{-1}ag^{\sigma}\}$, written $\mathrm{Aut}(C)_a$.

By the Galois cohomology theory, we have the following well-known facts:

- For a hyperelliptic curve C over $\overline{\mathbb{F}_q}$, we have

$$(4.4.1) \qquad |\mathrm{Aut}(C)/\sigma\text{-conjugacy}| = (\text{the number of } \mathbb{F}_q\text{-forms of } C),$$

  and thus

$$(4.4.2) \qquad \sum_{C \in \mathrm{SSp}\text{-}\mathrm{Hyp}_g(\overline{\mathbb{F}_q})} |\mathrm{Aut}(C)/\sigma\text{-conjugacy}| = |\mathrm{SSp}\text{-}\mathrm{Hyp}_g(\mathbb{F}_q)|,$$

  where $\mathrm{SSp}\text{-}\mathrm{Hyp}_g(K)$ denotes the set of K-isomorphism classes of s.sp. hyperelliptic curves over K, where K is a finite field or its algebraic closure.
- For a hyperelliptic curve C over $\overline{\mathbb{F}_q}$ and for each element $a \in \mathrm{Aut}(C)$, there exists a bijection $\mathrm{Aut}(C)_a \simeq \mathrm{Aut}_{\mathbb{F}_q}(C^{(a)})$. Here $C^{(a)}$ denotes the $\mathbb{F}_q$-form associated to a via the isomorphism

$$H^1(\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q), \mathrm{Aut}(C)) \cong \mathrm{Aut}(C)/\sigma\text{-conjugacy}.$$

  From the orbit-stabilizer theorem, we have $|\mathrm{Aut}(C)|/|\mathrm{Orb}(a)| = |\mathrm{Aut}(C)_a|$, and thus

$$(4.4.3) \qquad |\mathrm{Aut}(C)|/|\mathrm{Orb}(a)| = |\mathrm{Aut}_{\mathbb{F}_q}(C^{(a)})| .$$

For each $\mathrm{Aut}(C)$ in Table 1, we determine the left hand side of each of (4.4.1)–(4.4.3) with $(g, q) = (4, 17)$, $(4, 19)$ or $(4, 23)$ by computing σ-conjugacy classes of $\mathrm{Aut}(C)$ on Magma. As a result, we confirmed that the equalities (4.4.1)–(4.4.3) hold, where the value of the right hand side of (4.4.1) (resp. (4.4.3)) is already obtained in computation to prove Propositions 3.1.2, 3.1.4 and 3.2.2 (resp. results in Table 1). As it needs many pages to explain all cases, we refer to [24] for details of computational results, and let us here exhibit only one example:

EXAMPLE 4.4.1. Consider $C := C_1^{(\mathrm{alc})} : y^2 = x^{10} + x^7 + 3x^4 + 10x$ for $p = 23$. The automorphism group $\mathrm{Aut}(C)$ is isomorphic to $G_k/\mu_5(k)$ with $k = \overline{\mathbb{F}_{23}}$, which is a cyclic group of order 6. The cyclic group is generated by the equivalence class of $h := \begin{pmatrix} \zeta^{83952} & 0 \\ 0 & \zeta^{177232} \end{pmatrix} \in G_k \subset \mathrm{GL}_2(k)$, where ζ is a root of $P := t^4 + 3t^2 + 19t + 5 \in \mathbb{F}_{23}[t]$ in $\mathbb{F}_{23^4} \cong \mathbb{F}_{23}[t]/\langle P \rangle$. The minimal natural number n such that $h^{\sigma} = h^n$ is five. One can easily check that $|\mathrm{Aut}(C)/\sigma\text{-conjugacy}| = 2$ and $|\mathrm{Orb}(a)| = 3$ for every $a \in \mathrm{Aut}(C)$. This is compatible with the facts that there are exactly two $\mathbb{F}_{23}$-forms of C (which are C_1 and C_5 in Proposition 3.2.2, see Table 1) and that $\mathrm{Aut}_{\mathbb{F}_{23}}(C_1)$ and $\mathrm{Aut}_{\mathbb{F}_{23}}(C_5)$ are of order two.

Acknowledgment. The authors thank the anonymous referee for valuable comments and suggestions. This work was supported by JSPS Grant-in-Aid for Research Activity Start-up 18H05836 and 19K21026, JSPS Grant-in-Aid for Young Scientists 20K14301, JST CREST Grant Number JPMJCR2113, and JSPS Grant-in-Aid for Scientific Research (C) 17K05196.

References

[1] Bosma, W., Cannon, J. and Playoust, C.: *The Magma algebra system. I. The user language*, Journal of Symbolic Computation **24** (1997), 235–265.

[2] Deuring, M.: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Univ. Hamburg **14** (1941), no. 1, 197–272.

[3] Ekedahl, T.: *On supersingular curves and abelian varieties*, Math. Scand. **60** (1987), 151–178.

[4] González, J.: *Hasse-Witt matrices for the Fermat curves of prime degree*, Tohoku Math. J. (2) **49** (1997), no. 2, pp. 149–163. MR 1447179 (98b:11064)

[5] Hashimoto K.: *Class numbers of positive definite ternary quaternion Hermitian forms.* Proc. Japan Acad. Ser. A Math. Sci. **59** (1983), no. 10, 490–493.

[6] Hashimoto, K. and Ibukiyama, T.: *On class numbers of positive definite binary quaternion Hermitian forms. II*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), no. 3, 695–699 (1982).

[7] Ibukiyama, T.: *On rational points of curves of genus* 3 *over finite fields*, Tohoku Math. J. **45** (1993), 311–329.

[8] Ibukiyama, T. and Katsura, T.: *On the field of definition of superspecial polarized abelian varieties and type numbers*, Compositio Math. **91** (1994), no. 1, 37–46.

[9] Kudo, M. and Harashita, S.: *Superspecial curves of genus* 4 *in small characteristic*, Finite Fields and Their Applications, **45**, 131–169, 2017.

[10] Kudo, M. and 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, Lecture Notes in Computer Science, Vol. **11321**, pp. 58-73, Springer, Cham, 2018.

[11] Kudo, M. and Harashita, S.: *Computational approach to enumerate non-hyperelliptic superspecial curves of genus 4*, Tokyo Journal of Mathematics, Vol. **43**, Number 1, 259–278, 2020.

[12] Kudo, M. and Harashita, S.: *Superspecial trigonal curves of genus 5*, Experimental Mathematics, Vol. **31**, Issue 3, 908-919, 2022.

[13] Lercier, R., Sijsling, J. and Ritzenthaler, C.: *Functionalities for genus 2 and 3 curves*, arXiv:2102.04372 [math.AG], 2021.

[14] Manin, J. I.: *On the theory of Abelian varieties over a field of finite characteristic*, AMS Translations, Series 2, **50**, pp. 127–140, 1966, translated by G. Wagner (originally published in Izv. Akad. Nauk SSSR Ser. Mat. **26**, pp. 281–292, 1962).

[15] Nygaard, N. O.: *Slopes of powers of Frobenius on crystalline cohomology*, Ann. Sci. École Norm. Sup. (4), **14**, No. 4, 369–401 (1982), 1981.

[16] Serre, J.-P.: *Nombre des points des courbes algebrique sur* $\mathbb{F}_q$, Sém. Théor. Nombres Bordeaux (2) 1982/83, 22 (1983).

[17] Tafazolian, S., Torres, F.: *A note on certain maximal curves*, Commun. Algebra **45** (2), pp. 764–773, 2017, DOI: 10.1080/00927872.2016.1175460.

[18] Tafazolian, S.: *A note on certain maximal hyperelliptic curves*, Finite Fields and Their Applications, **18** (2012), 1013–1016.

[19] Tafazolian, S., Torres, F.: *On maximal curves of fermat type*, Adv. Geom., **13** (4), pp. 613–617, 2013.

[20] Tafazolian, S. and Torres, F.: *On the curve* $y^n = x^m + x$ *over finite fields*, Journal of Number Theory, **145** (2014), 51–66.

[21] Tafazolian, S., Torres, F.: *On the curve* $y^n = x^\ell(x^m + 1)$ *over finite fields*, Adv. Geom. **19** (2), pp. 263–268, 2018.

[22] Xue, J., Yang, T.-C. and Yu, C.-F.: *On superspecial abelian surfaces over finite fields*, Doc. Math. **21** (2016) 1607–1643.

[23] Yui, N.: *On the Jacobian varieties of hyperelliptic curves over fields of characterisctic* $p > 2$, Journal of algebra, **52** (1978), 378–410.

[24] `https://sites.google.com/view/m-kudo-official-website/english/code/genus4-ssp-hyper`

E-mail: address of the first author: kudo@mist.i.u-tokyo.ac.jp
E-mail: address of the second author: harasita@ynu.ac.jp