Superspecial Hyperelliptic Curves of Genus 4 over Small Finite Fields

Momonari Kudo[1,2] and Shushi Harashita[3]

[1] Kobe City College of Technology,
8-3, Gakuen-Higashimachi, Nishi-ku, Kobe, 651-2194, Japan
m-kudo@math.kyushu-u.ac.jp

[2] Graduate School of Environment and Information Sciences, Yokohama National University.
79-7, Tokiwadai, Hodogaya-ku, Yokohama, 240-8501, Japan
harasita@ynu.ac.jp

Abstract. In this paper, we enumerate *superspecial* hyperelliptic curves of genus 4 over finite fields $\mathbb{F}_q$ for small q. This complements our preceding results in the non-hyperelliptic case. We give a feasible algorithm to enumerate superspecial hyperelliptic curves of genus g over $\mathbb{F}_q$ in the case that q and $2g+2$ are coprime and $q > 2g+1$. We executed the algorithm for $(g, q) = (4, 11^2)$, $(4, 13^2)$, $(4, 17^2)$ and $(4, 19)$ with our implementation on a computer algebra system Magma. Moreover, we found many *maximal* hyperelliptic curves and some *minimal* hyperelliptic curves over $\mathbb{F}_q$ from among enumerated superspecial curves.

Key words: Hyperelliptic curves, superspecial curves, maximal curves.

1 Introduction

Let $\mathbb{F}_q$ denote the finite field with q elements. A curve C of genus g over $\mathbb{F}_q$ is called *maximal* (resp. *minimal*) if the number of $\mathbb{F}_q$-rational points on C attains the Hasse-Weil upper bound $q + 1 + 2g\sqrt{q}$ (resp. the Hasse-Weil lower bound $q + 1 - 2g\sqrt{q}$). These curves are interesting objects in their own right, and also are useful in applications such as coding theory (e.g., [11], [21]). Specifically, algebraic geometric codes produced from curves with many rational points have both high information rate and high error-correcting rate; for such curves the sum of these two quantities is large. Thus, it has been a central problem to find maximal curves. However, the number of maximal curves over $\mathbb{F}_q$ of genus g for a fixed pair (g, q) is very small, compared with the whole set of curves over $\mathbb{F}_q$ of genus g, and thus it is not easy at all to find maximal curves. The notion of *superspecial* curves helps us to find such curves. In general, a curve over a field K of positive characteristic is said to be *superspecial* if its Jacobian is isomorphic to a product of supersingular elliptic curves over the algebraic closure $\overline{K}$ of K. It is known that any maximal or minimal curve C over $\mathbb{F}_{p^2}$ is superspecial, where p is a prime. Conversely any superspecial curve over an algebraically closed field descends to a maximal *or* minimal curve over $\mathbb{F}_{p^2}$, see the proof of

[4, Theorem 1.1]. In the hyperelliptic case, we can say *more*: The existence of a superspecial hyperelliptic curve of genus g in characteristic p implies that there exists a maximal curve of genus g over $\mathbb{F}_{p^2}$ *and also* a minimal curve of genus g over $\mathbb{F}_{p^2}$. We will review this fact in §2.2. This work focuses on enumerating superspecial curves to find *all* maximal hyperelliptic curves among them.

In the literature, there are many works on the enumeration of superspecial curves of genus g:

– If $g \leq 3$, some theoretical approaches to enumerate superspecial/maximal curves are available, which are based on Torelli's theorem (cf. [3], [25, Prop. 4.4] for $g = 1$, [10], [13], [22] for $g = 2$, and [9], [12] for $g = 3$). In particular, there exists a maximal curve of genus g over $\mathbb{F}_{p^{2e}}$ if $g = 2$ and $p^{2e} \neq 4, 9$ (cf. [22, Théorème 3]) and if $g = 3$, $p \geq 3$ and e is odd (cf. [12, Theorem 1]).

– If $g \geq 4$, however, these approaches are not so effective; different from the case of $g \leq 3$, the dimension of the moduli space of curves of genus g is strictly less than that of the moduli space of principally polarized abelian varieties of dimension g. Thus the case of $g = 4$ is the next target. For $p = 5$, Fuhrmann-Garcia-Torres [5] found a maximal curve C_0 of genus 4 over $K = \mathbb{F}_{5^2}$, and proved that it gives a unique isomorphism class over $\overline{K}$. In recent years, enumerations of superspecial curves of genus 4 in some small characteristic have been completed in [14], [16] and [17]. Specifically, the isomorphism classes of superspecial *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. Note that all the maximal curves over $K = \mathbb{F}_{5^2}$ enumerated in [14] are included in the unique isomorphism class of C_0 over $\overline{K}$. In the hyperelliptic case, the existence of superspecial curves is known for some q (e.g., [23], [24]). Note that this study is motivated to enumerate *all* superspecial curves, while the papers [23] and [24] characterize *specific* superspecial curves. In particular, the paper [24] uses Serre's covering result in order to study the maximality of a specific curve.

In this work, we enumerate superspecial *hyperelliptic* curves of genus 4 in characteristic $p \leq 19$. Note that we do not use Serre's covering result, but apply techniques in computer algebra such as Gröbner bases. This work also complements our preceding results in [14], [16] and [17] for non-hyperelliptic curves. Thanks to Ekedahl [4, Theorem 1.1], there is no superspecial hyperelliptic curve of genus 4 if $p \leq 7$. Our results are the following theorems (Theorems 1 – 3), see Table 1 for a summary of results in $g = 4$. Note that the number of isomorphism classes of superspecial curves over $\mathbb{F}_{p^a}$ depends on the parity of a (cf. [16, Proposition 2.3.1]).

Theorem 1. *There is no superspecial hyperelliptic curve of genus* 4 *in characteristic* 11 *and* 13.

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 the algebraic closure in characteristic* 17 *up to isomorphism.*

Table 1. Main references to enumerations of isomorphism classes of superspecial curves of genus $g = 4$ over $\mathbb{F}_q$, where q is a power of a prime p.

q	Non-Hyperelliptic	Hyperelliptic	q	Non-Hyperelliptic	Hyperelliptic
$p \leq 3$	Non-Existence by Ekedahl [4]		13^{2e-1}	Not yet	Non-Existence by **Thm. 1**
			13^{2e}		
5^{2e-1}	[16, Thm. A]	Non-Existence by Ekedahl [4]	17^{2e-1}		**Thm. 2**
5^{2e}	[14, Thm. A]		17^{2e}		
7^{2e-1}	Non-Existence by [14, Thm. B]		19^{2e-1}		**Thm. 3**
7^{2e}			19^{2e}		Not yet
11^{2e-1}	[16, Thm. B]	Non-Existence by **Thm. 1**	$p \geq 23$	Not yet (Existences for some p, cf. [6], [23])	
11^{2e}	Not yet				

Theorem 3. *There exist precisely* 12 *superspecial hyperelliptic curves of genus* 4 *over* $\mathbb{F}_{19}$ *up to isomorphism over* $\mathbb{F}_{19}$*. Moreover, there exist precisely* 2 *superspecial hyperelliptic curves of genus* 4 *over* $\mathbb{F}_{19}$ *up to isomorphism over the algebraic closure.*

Note that we have explicit defining equations of the superspecial hyperelliptic curves in Theorems 2 and 3 (but omit them in the statements). Such explicit equations also define maximal or minimal curves over $\mathbb{F}_{p^2}$. For example, we found the following superspecial curve over $\mathbb{F}_{17^2}$; for each $a \in \mathbb{F}_{17}^{\times}$ consider the hyperelliptic curve $C_a : H_a(x, y) = y^2 - (x^{10} + ax^7 + (13a^2)x^4 + (12a^3)x) = 0$ over $\mathbb{F}_{17^2}$, which is included in one of the 25 isomorphism classes of the superspecial hyperelliptic curves over $\mathbb{F}_{17^2}$. Then $C_a : H_a(x, y) = 0$ is a maximal curve over $\mathbb{F}_{17^2}$. Indeed, the number of its $\mathbb{F}_{17^2}$-rational points is 426, which coincides with the Hasse-Weil upper bound $q + 1 + 2g\sqrt{q}$ for $q = 17^2$. Moreover, each C_a is not $\mathbb{F}_{17^2}$-isomorphic to $y^2 = x^{10} + x$, which is a maximal curve of known type (cf. [23], [24]). This means that we obtain a maximal curve of new type. For the other equations, see a table of the web page of the first author [27].

We prove Theorems 1 – 3 with help of computational results. Our computational methods are (A) Algorithm to enumerate superspecial hyperelliptic curves, (B) Reduction of defining equations of hyperelliptic curves, and (C) Isomorphism testing. Our enumeration method (A) is based on the computation of Cartier-Manin matrices (cf. [7], [19], [26, Section 2]), and reduces our enumeration problem into solving multivariate systems over finite fields. The method (A) is also viewed as a hyperelliptic curve-version of algorithms for non-hyperelliptic curves given in [14], [16] and [17]. The method (B) reduces parameters of defining equations as much as possible. Namely, it reduces the number of variables in multivariate systems to be solved, which clearly makes our algorithm (A) efficient. The method (C) gives an algorithm to classify isomorphism classes of arbitrary hyperelliptic curves of given genus over a finite field. Note that in this paper we do not mention the asymptotic complexity but the practicality of our enumeration algorithm only.

Notation. For a field K, we denote by $K^\times$ its multiplicative group. The general linear group of degree n over K is denoted by $\mathrm{GL}_n(K)$.

2 Preliminaries

Let K be a field of odd characteristic $p > 0$. In this section, we review some basic facts on hyperelliptic curves over K and their superspeciality.

2.1 Hyperelliptic curves

Let C be a hyperelliptic curve over K. By definition, there exists a morphism $\pi : C \to \mathbf{P}^1$ of degree 2 over $\overline{K}$, where $\mathbf{P}^1$ denotes the projective line. It is known (cf. [8, Prop. 5.3]) that the pencil π is unique up to automorphisms of $\mathbf{P}^1$, whence we may assume that π is defined over K. Let g be the genus of C. It is known that π is ramified over distinct $2g + 2$ points. Write $\mathbf{P}^1 := \mathrm{Proj}(K[X, Z])$. Let $K(C)$ (resp. $K(x)$) be the field of rational functions on C (resp. in $x = X/Z$). The π induces a quadratic extension $K(C)/K(x)$. Let $y \in K(C)$ be a generator of the different ideal of $K(C)/K(x)$ with respect to $K[x]$, the ring of integers of $K(x)$. As y^2 belongs to $K[x]$, we see that C is realized as the desingularization of the homogenization of

$$y^2 = f(x), \tag{1}$$

where $f(x)$ is a polynomial over K with non-zero discriminant. Assume that the cardinality of K is greater than $2g+1$. If necessarily, by an automorphism of $\mathbf{P}^1$ over K we translate the ramified points of π outside $\infty := (1 : 0) \in \mathbf{P}^1$. Then $f(x)$ is of degree $2g + 2$.

Remark 1. If $f(x) = 0$ has a root α in K, by the transformation $x' = 1/(x - \alpha)$ and $y' = y/(x - \alpha)^g$ we have another realization of the curve:

$${y'}^2 = \phi(x'), \tag{2}$$

where $\phi(x')$ is a polynomial over K of degree $2g + 1$. However as $f(x)$ does not always have a rational root, we can not use the model of odd degree.

The next lemma describes the set of isomorphisms between two hyperelliptic curves C_1 and C_2. This in particular gives a criterion for whether C_1 and C_2 are isomorphic to each other or not.

Lemma 1. *Let $f_1(x)$ and $f_2(x)$ be elements of $K[x]$ of degree $2g + 2$. 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. The set of k-isomorphisms from C_1 to C_2 is bijective to*

$$\left(\{h \in \mathrm{GL}_2(k) \mid F_1(h \cdot {}^t(X, Z)) = \lambda^2 F_2(X, Z) \textit{ for some } \lambda \in k^\times\}/\sim\right) \times \{\pm 1\},$$

where we say $h_1 \sim h_2$ if $h_1 = \mu h_2$ for some $\mu \in k^\times$.

Proof. Let φ be a k-isomorphism from C_1 to C_2. Let π_i be morphisms from C_i to $\mathbf{P}^1$ of degree 2 (chosen over K as above). The composition $\pi_2 \circ \varphi$ is a morphism C_1 to $\mathbf{P}^1$ of degree 2 over k. The uniqueness of such morphisms implies that there exists a k-automorphism ψ of $\mathbf{P}^1$ commuting the diagram

$$\begin{tikzcd} C_1 \arrow[r, "\varphi"] \arrow[d, "\pi_1"'] & C_2 \arrow[d, "\pi_2"] \\ \mathbf{P}^1 \arrow[r, "\psi"] & \mathbf{P}^1 \end{tikzcd}$$

The automorphism ψ is represented by an element $h \in \mathrm{GL}_2(k)$ up to scalar multiplications. Clearly φ sends the different ideal $\mathfrak{d}_1$ of $k(C_1)/k(\mathbf{P}^1)$ to the different ideal $\mathfrak{d}_2$ of $k(C_2)/k(\mathbf{P}^1)$, whence the generator y of $\mathfrak{d}_1$ of the equation $y^2 = f_1(x)$ defining C_1 is sent to that of $\mathfrak{d}_2$ up to a scalar multiplication. Thus, for some scalar $\lambda \in k^\times$ we have the equation

$$F_1((X,Z) \cdot {}^t h) = \lambda^2 F_2(X,Z). \tag{3}$$

Conversely for $h = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(k)$ satisfying (3) for some $\lambda \in k^\times$, we have the two isomorphisms $C_1 \to C_2$ defined by $(x,y) \mapsto \left(\frac{ax+b}{cx+d}, \pm\lambda \frac{y}{(cx+d)^{g+1}}\right)$. □

2.2 Superspecial curves and maximal curves

Let C be a nonsingular projective curve over a perfect field K. We say that C is *superspecial* if its Jacobian $\mathrm{Jac}(C)$ is the product of some supersingular elliptic curves over the algebraic closure $\overline{K}$. It is well-known that C is superspecial if and only if the Cartier operator on the cohomology group $H^0(C, \Omega^1_C)$ is zero (cf. [20]). The Cartier operator on $H^0(C, \Omega^1_C)$ with respect to a fixed basis of $H^0(C, \Omega^1_C)$ is called a Cartier-Manin matrix of C, which for hyperelliptic curves will be reviewed in the next subsection.

As mentioned in the introduction, it is known that any superspecial hyperelliptic curve over an algebraically closed field can descend to a maximal curve over $\mathbb{F}_{p^2}$ *and also* to a minimal curve over $\mathbb{F}_{p^2}$. This is deduced from the following facts.

1. If C is hyperelliptic, then the automorphism group of C is isomorphic to the automorphism group of the Jacobian variety $\mathrm{Jac}(C)$ with the principal polarization of C. This fact implies that giving a descent datum of C is equivalent to giving that of its Jacobian with the principal polarization.
2. For superspecial C, by definition we have $\mathrm{Jac}(C) \simeq E^g$ for a supersingular elliptic curve E, where g is the genus of C. It is known that E descends to an elliptic curve E_0 over $\mathbb{F}_{p^2}$ over which the Frobenius is the multiplication by p and $-p$ respectively.

3. A polarization on E^g is, by definition, a homomorphism from E^g to its dual (which is isomorphic to E^g), but such a homomorphism is always defined over $\mathbb{F}_{p^2}$, i.e., is induced from an $\mathbb{F}_{p^2}$-homomorphism from E_0^g to itself.

See the proof of [4, Theorem 1.1] and [18, 1.2] for the second and third facts. The second and third facts imply that $\mathrm{Jac}(C)$ with the principal polarization descend to $\mathbb{F}_{p^2}$ with the Frobenius is p and $-p$ respectively. By the first fact, C descends to a curve C_0 over $\mathbb{F}_{p^2}$ such that the Frobenius on the first étale cohomology group $H^1_{\text{ét}}(C_0, \mathbb{Z}_l)$ for a prime $l \neq p$ is the multiplication by p and $-p$ respectively. The curve C_0 is minimal in the former case and is maximal in the latter case.

Thus, we conclude that the existence of a superspecial hyperelliptic curve of genus g in characteristic p implies the existence of a maximal curve of genus g over $\mathbb{F}_{p^2}$ and that of a minimal curve of genus g over $\mathbb{F}_{p^2}$.

2.3 Cartier-Manin matrices of hyperelliptic curves

As in the previous subsection, let K be a perfect field of odd characteristic $p > 0$. The *Cartier-Manin matrix* of a curve C over K is defined as the matrix representing the Cartier operator on $H^0(C, \Omega^1_C)$, see [26, Section 2]. Here $H^0(C, \Omega^1_C)$ is the space of holomorphic differentials of C. In the following proposition, we introduce a well-known method (cf. [7], [19], [26, Section 2]) to obtain the Cartier-Manin matrix of a hyperelliptic curve.

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

As we have seen in §2.2, a non-singular curve is superspecial if and only if its Cartier-Manin matrix is the zero matrix. From Proposition 1, we have the following corollary. By this corollary, one can decide whether a given hyperelliptic curve is superspecial or not by computing its Cartier-Manin matrix.

Corollary 1. *Let C be a hyperelliptic curve $y^2 = f(x)$ of genus g over K. Then C is superspecial if and only if the coefficients of x^{pi-j} in $f^{(p-1)/2}$ are equal to 0 for all positive integers $1 \leq i, j \leq g$.*

3 Enumeration of superspecial hyperelliptic curves

Let $K = \mathbb{F}_q$ be a finite field of odd characteristic p, where q is a power of p. In this section, we give algorithms to enumerate superspecial hyperelliptic curves and to determine their isomorphism classes. As we mentioned in §1 and §2.2, a curve over K is superspecial if and only if its Cartier-Manin matrix is zero. Recall from Proposition 1 of §2.3 that the Cartier-Manin matrix of a hyperelliptic curve $y^2 = f(x)$ of genus g with $\deg(f) = 2g+1$ or $2g+2$ is determined from certain coefficients in the multiple $f^{(p-1)/2}$.

In this section, we give three computational techniques for determining the isomorphism classes of superspecial hyperelliptic curves of genus g over finite fields: (A) Algorithm to enumerate superspecial hyperelliptic curves, (B) Reduction of defining equations of hyperelliptic curves, and (C) Isomorphism testing. Specifically, based on Corollary 1, we shall reduce our enumeration problem into a computational problem that we solve multivariate systems over finite fields.

3.1 (A): Algorithm to enumerate superspecial hyperelliptic curves

Recall from §2.1 that a hyperelliptic curve of genus g over K is given by the equation $y^2 = f(x)$ for some polynomial f of degree $2g+2$ with non-zero discriminant. Write $f(x) = a_d x^d + a_{d-1}x^{d-1} + a_{d-2}x^{d-2} + \cdots + a_1 x + a_0$ with $a_k \in K$ for $0 \leq k \leq d$. Let $\mathcal{S}$ be the set of the coefficients of the g^2 monomials in $f(x)^{(p-1)/2}$ given in Proposition 1. Based on Proposition 1 together with Corollary 1, we give a strategy to enumerate superspecial hyperelliptic curves of genus g over K:

- Enumerate $(a_0, \ldots, a_d) \in K^{d+1}$ such that all elements of $\mathcal{S}$ are zero and such that the discriminant of $f(x)$ is not zero.

In other words, by regarding all elements of $\mathcal{S}$ as algebraic relations on a_i's, it suffices to compute all roots $(a_0, \ldots, a_d) \in K^{d+1}$ of the multivariate system $P = 0$ for all $P \in \mathcal{S} \subset K[a_0, \ldots, a_d]$ such that f has no double root in the algebraic closure $\overline{K}$. Here, we show a concrete method (*Enumeration Method* below) for the enumeration, and write down its pseudocode in Algorithm 1. This method is viewed as a hyperelliptic curve-version of algorithms given in [14], [16] and [17] for non-hyperelliptic curves.

Enumeration Method. With notation as above, we conduct the following:

0. Regard some unknown coefficients in $f(x)$ as indeterminates. Choose an integer $0 \leq s_1 \leq d+1$. For simplicity, let $a_0, \ldots, a_{s_1-1}$ be indeterminates here. The remaining part $(a_{s_1}, \ldots, a_d)$ runs through $K^{\oplus d+1-s_1}$.

For each element $(c_{s_1}, \ldots, c_d) \in K^{\oplus d+1-s_1}$, proceed with the following four steps:

1. Put
$$f(x) := c_d x^d + c_{d-1}x^{d-1} + \cdots + c_{s_1}x^{s_1} + a_{s_1-1}x^{s_1-1} + \cdots + a_1 x + a_0.$$
Compute $h := f^{p-1}$ over $K[a_0, \ldots, a_{s_1-1}][x]$.
2. Let $\mathcal{S}$ be the set of the coefficients of the g^2 monomials in $h = f^{p-1}$, given in Proposition 1. Note that $\mathcal{S} \subset K[a_0, \ldots, a_{s_1-1}]$.
3. Regard some unknown coefficients among $a_0, \ldots, a_{s_1-1}$ as indeterminates. For simplicity, let $a_0, \ldots, a_{s_2-1}$ with $s_2 \leq s_1$ be indeterminates here. The remaining part $(a_{s_2}, \ldots, a_{s_1-1})$ runs through $K^{\oplus s_1-s_2}$.
4. For each $(c_{s_2}, \ldots, c_{s_1-1}) \in K^{\oplus s_1-s_2}$, proceed with the following three steps 4a – 4c:

Algorithm 1 Algorithm to enumerate superspecial hyperelliptic curves

```
Input: An integer $g$, a prime number $p$, and $q = p^s$ for some $s \geq 1$
Output: The set $\mathcal{F}$ of polynomials $f(x)$ over $K = \mathbb{F}_q$ of degree $2g+2$ such that the
    curves $y^2 = f(x)$ are superspecial hyperelliptic curves of genus $g$
$\mathcal{F} \leftarrow \emptyset$
$d \leftarrow 2g + 2$
Choose an integer $0 \leq s_1 \leq d + 1$ and let $a_0, \ldots, a_{s_1-1}$ be indeterminates
for $(c_{s_1}, \ldots, c_d) \in K^{\oplus d+1-s_1}$ do
    $f(x) \leftarrow c_d x^d + c_{d-1} x^{d-1} + \cdots + c_{s_1} x^{s_1} + a_{s_1-1} x^{s_1-1} + \cdots + a_1 x + a_0$
    Compute $h := f^{(p-1)/2}$ over $K[a_0, \ldots, a_{s_1-1}][x]$
    $\mathcal{S} \leftarrow$ the set of the coefficients of the $g^2$ monomials in $h$, given in Proposition 1.
    Choose an integer $0 \leq s_2 \leq s_1$
    for $(c_{s_2}, \ldots, c_{s_1-1}) \in K^{\oplus s_1 - s_2}$ do
        $\mathcal{S}' \leftarrow \{P(a_0, \ldots, a_{s_2-1}, c_{s_2}, \ldots, c_{s_1-1}) : P \in \mathcal{S}\}$
        Compute the roots of the system (4) over $K$ (with Gröbner basis algorithms)
        $V \leftarrow \{(c_0, \ldots, c_{s_2-1}) \in K^{\oplus s_2} : P'(c_0, \ldots, c_{s_2-1}) = 0$ for all $P' \in \mathcal{S}'\}$
        for $(c_0, \ldots, c_{s_2-1}) \in V$ do
            $f_{\mathrm{sol}} \leftarrow c_d x^d + c_{d-1} x^{d-1} + \cdots + c_{s_2} x^{s_2} + c_{s_2-1} x^{s_2-1} + \cdots + c_1 x + c_0$
            Decide whether $f_{\mathrm{sol}}$ has no double root in $\overline{K}$ or not (this can be done by
            constructing the minimal splitting field of $f_{\mathrm{sol}}$)
            if $f_{\mathrm{sol}}$ has no double root in $\overline{K}$ then
                $\mathcal{F} \leftarrow \mathcal{F} \cup \{f_{\mathrm{sol}}\}$
            end if
        end for
    end for
end for
return $\mathcal{F}$
```

4a. For each $P \in \mathcal{S}$, substitute respectively $c_{s_2}, \ldots, c_{s_1-1}$ into $a_{s_2}, \ldots, a_{s_1-1}$ of the coefficients in P. Put

$$\mathcal{S}' := \{P(a_0, \ldots, a_{s_2-1}, c_{s_2}, \ldots, c_{s_1-1}) : P \in \mathcal{S}\}.$$

Note that $\mathcal{S}' \subset K[a_0, \ldots, a_{s_2-1}]$.

4b. Compute the roots of the multivariate system

$$P'(a_0, \ldots, a_{s_2-1}) = 0 \text{ for all } P' \in \mathcal{S}' \tag{4}$$

over K with Gröbner basis algorithms.

4c. For each root of the above system, substitute it into unknown coefficients in f, and decide whether f has no double root in $\overline{K}$ or not (this can be done by constructing the minimal splitting field of f). If f has no double root in $\overline{K}$, store f.

Remark 2. Our enumeration method adopts the *hybrid approach* by Bettale, Faugère and Perret [1] to solve multivariate systems over finite fields. In their approach, exhaustive search and Gröbner basis algorithms are mixed for efficiency, but there is a trade-off between them. Note that an optimal choice of coefficients to be regarded as indeterminants is not unique, and deeply depends on the situation. In our case, such a choice is heuristically decided from experimental computations for each situation (Propositions 2 – 6 in the next section).

3.2 (B): Reduction of defining equations of hyperelliptic curves

In this subsection, we give a reduction of defining equations of hyperelliptic curves. Let C be a hyperelliptic curve over K. Let $y^2 = f(x)$ be a defining equation of C. Remark that 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 $\{0, 1, \infty\}$, but we can not adopt this method, because the ramified points are not necessarily K-rational points. In this paper we use an elementary reduction:

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 the desingularization of the homogenization of*

$$cy^2 = x^{2g+2} + bx^{2g} + a_{2g-1}x^{2g-1} + \cdots + a_1 x + a_0$$

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

Proof. As in §2.1, a hyperelliptic curve C over K is realized as $y^2 = f(x)$ for a polynomial $f(x)$ of degree $2g+2$ over K. This can be expressed as $cy^2 = h(x)$ for $c \in K^\times$ and for a monic polynomial $h(x)$ of degree $2g+2$ over K. Considering the transformation $(x, y) \mapsto (x, \alpha y)$ for some $\alpha \in K^\times$, one may assume $c = 1$ or ϵ. Considering $x \to x + a$, we can transform $h(x)$ to a polynomial with no x^{2g+1}-term, i.e., we may assume C is defined by an equation of the form

$$cy^2 = x^{2g+2} + a_{2g}x^{2g} + a_{2g-1}x^{2g-1} + \cdots + a_1 x + a_0.$$

The transformation $(x, y) \mapsto (\beta x, \beta^{g+1} y)$ for some $\beta \in K^\times$ and the multiplication by $\beta^{-(2g+2)}$ to the whole, we may assume that $a_{2g} = 0, 1$ or ϵ.

Remark 3. Let $h(x)$ be a monic polynomial over K with non-zero discriminant. Let $\epsilon \in K^\times \smallsetminus (K^\times)^2$. Let C_1 and C_2 be the hyperelliptic curves defined by $y^2 = h(x)$ and $\epsilon y^2 = h(x)$ respectively. The transformation $(x, y) \mapsto (x, \sqrt{\epsilon} y)$ gives an isomorphism from C_1 to C_2 over $K[\sqrt{\epsilon}]$. In particular, C_1 is superspecial if and only if C_2 is superspecial.

3.3 (C): Isomorphism testing

We suppose that p and $2g+2$ are coprime. Let C_1 and C_2 be hyperelliptic curves of genus g over K. As we showed in §2.1 and in Lemma 2, defining equations of C_1 and C_2 are given by $H_1(x, y) = c_1 y^2 - f_1(x)$ and $H_2(x, y) = c_2 y^2 - f_2(x)$ respectively for some c_1 and c_2 in $K^\times$ and for some polynomials $f_1(x)$ and $f_2(x)$ in $K[x]$ of degree $2g+2$. Let F_i denote the homogenization of f_i with respect to an extra variable z for each $1 \leq i \leq 2$. By Lemma 1, we have a fact that C_1 and C_2 are isomorphic over K if and only if there exists $h \in \mathrm{GL}_2(K)$ such that $h \cdot F_1 = \lambda^2 F_2$ for some $\lambda \in K^{\times}$. In other words, there exist $h \in \mathrm{GL}_2(K)$ and $\lambda \in K^{\times}$ such that all the coefficients in $F := h \cdot F_1 - \lambda F_2$ are zero, where $h \cdot F_1(x, z) := F_1((x, z) \cdot {}^t h)$. Based on this fact, we write down a method (*Isomorphism Testing Method* below) to determine whether C_1 and C_2 are isomorphic over K (or over $\overline{K}$) for $K = \mathbb{F}_q$. Here q is a power of the characteristic p of K. The correctness of this computational method is straightforward from its construction.

Isomorphism Testing Method. For the inputs $H_1(x, y) = c_1 y^2 - f_1(x)$, $H_2(x, y) = c_2 y^2 - f_2(x)$, and q as above, the following 5 steps decide whether $C_1 : H_1(x, y) = 0$ and $C_2 : H_2(x, y) = 0$ are isomorphic over K or not (resp. $\overline{K}$ or not):

1. Let b_1, b_2, b_3, b_4, b_5, λ and μ be indeterminates, and set
$$F_i(x, z) := c_i^{-1} z^{2g+2} f_i(x/z) \text{ for } i = 1, 2, \quad \text{and} \quad h := \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}$$
where h is a square matrix whose entries are indeterminates.
2. Compute $F(x, z) := F_1((x, z) \cdot {}^t h) - \lambda^2 F_2(x, z)$ over the polynomial ring $K[b_1, b_2, b_3, b_4, b_5, \lambda, \mu][x, z]$ 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
$$\mathcal{C} := \mathcal{C}_F \cup \{(b_1 b_4 - b_2 b_3) b_5 - 1\} \cup \{\lambda\mu - 1\},$$
and $\mathcal{C}' := \mathcal{C} \cup \{b_i^q - b_i : 1 \leq i \leq 4\} \cup \{\lambda^q - \lambda\}$ (resp. $\mathcal{C}' := \mathcal{C}$). Note that $b_1 b_4 - b_2 b_3 = \det(g)$.
4. Test whether the multivariate system defined by the ideal $\langle \mathcal{C}' \rangle$ has a root over K (resp. $\overline{K}$) or not. One can do this by computing the reduced Gröbner basis in $K[b_1, b_2, b_3, b_4, b_5, \lambda, \mu]$ with respect to some term order.
5. If the system in Step 4 has a root over K (resp. $\overline{K}$), then $C_1 : H_1(x, y) = 0$ and $C_2 : H_2(x, y) = 0$ are isomorphic over K (resp. $\overline{K}$). Otherwise C_1 and C_2 are not isomorphic over K (resp. $\overline{K}$).

4 Main results

In this section, we prove Theorems 1 – 3 stated in §1. As an application of the theorems, we also found hyperelliptic curves of genus 4 over $\mathbb{F}_q$ such that they are maximal as curves over $\mathbb{F}_{p^2}$ for $q = 17$, 17^2 and 19. We choose a primitive element ζ of $\mathbb{F}_q$ for each 17, 17^2 and 19. Specifically, we take $\zeta = 3$ for $q = 17$, $\zeta = -8 + \sqrt{61}$ for $q = 17^2$, and $\zeta = 2$ for $q = 19$.

4.1 Proofs of and corollaries of the main theorems

In the following proofs, we use computational results, which shall be given in the next subsection (§4.2).

Proofs of Theorems 1 – 3. We here prove the case of $q = 11^2$ only since the other cases are proved by a similar idea together with Propositions 3 – 6. Let C be a hyperelliptic curve of genus $g = 4$ over $K = \mathbb{F}_q$. Since $p = 11$ is coprime to $2g + 2 = 2 \cdot 4 + 2 = 10$, it follows from Lemma 2 that C is given by $y^2 - f(x)$ or $\epsilon y^2 - f(x)$ for $\epsilon \in K^\times \smallsetminus (K^\times)^2$. Here $f(x)$ is a polynomial of the form

$$f(x) = x^{10} + a_8 x^8 + a_7 x^7 + \cdots + a_1 x + a_0$$

for some $a_i \in K$ with $0 \leq i \leq 8$ such that it has no double root over the algebraic closure $\overline{K}$. By Proposition 2 in the next subsection (§4.2), there does not exist such an $f(x)$ that $C : y^2 = f(x)$ is superspecial. It follows from Remark 3 that there is no such an $f(x)$ that $C : \epsilon y^2 = f(x)$ is superspecial. □

Some Corollaries By Theorem 1, we relax the restriction on non-hyperelliptic curves in [16, Theorem B] (or [17, Main Theorem]).

Corollary 2. *There exist precisely* 30 (*resp.* 9) *superspecial curves of genus* 4 *over* $\mathbb{F}_{11}$ *up to isomorphism over* $\mathbb{F}_{11}$ (*resp. the algebraic closure of* $\mathbb{F}_{11}$).

Since a maximal or minimal (hyperelliptic) curve over $\mathbb{F}_{p^2}$ is superspecial, we have the following corollaries (Corollaries 3 and 4 below) from Theorem 1:

Corollary 3. *There does not exist any maximal* (*resp. minimal*) *hyperelliptic curve of genus* 4 *over* $\mathbb{F}_{121}$.

Corollary 4. *There does not exist any maximal* (*resp. minimal*) *hyperelliptic curve of genus* 4 *over* $\mathbb{F}_{169}$.

In contrast to the cases of $p \leq 13$, it is shown in Theorems 2 and 3 that there exist superspecial hyperelliptic curves of genus 4 over $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$ in the cases of $p = 17$ and 19. Computing the number of rational points of the enumerated curves by a computer, we have the following corollaries.

Corollary 5. *There exists precisely* 2 (*resp.* 2) *maximal* (*resp. minimal*) *hyperelliptic curves of genus* 4 *over* $\mathbb{F}_{17^2}$ *up to isomorphism over* $\mathbb{F}_{17^2}$.

Corollary 6. *There exist maximal hyperelliptic curves of genus* 4 *over* $\mathbb{F}_{19^2}$. *There also exists a minimal hyperelliptic curve of genus* 4 *over* $\mathbb{F}_{19^2}$.

Maximal curves and minimal curves in Corollaries 5 and 6 will be introduced in §4.3.

4.2 Computational parts of our proofs of the main theorems

We show computational results for the proofs of the main theorems. The computational results are proved by executing *Enumeration Method* in §3.1 and *Isomorphism Testing Method* in §3.3. All our computations were conducted on a computer with ubuntu 16.04 LTS OS at 3.40 GHz CPU (Intel Core i7-6700) and

15.6 GB memory We implemented and executed the computations over Magma V2.22-7 [2] in its 64-bit version.

In Propositions 2, 3, 4, 5 and 6, below, we show our computational results for $q = 11^2$, 13^2, 17, 17^2 and 19, respectively. We give a computational proof of Proposition 5 only, and omit those of the other propositions since our computational settings in all the proofs are almost the same (our proofs of Propositions 2, 3, 4 and 6 will be given in a separated pdf [15]). We also note that the enumeration for $q = 17^2$ is more expensive than those for $q = 11^2$, 13^2, 17 and 19 due to the largest cardinality of $\mathbb{F}_q$.

Proposition 2. *Consider the polynomial $f(x) \in \mathbb{F}_{121}[x]$ of the form*

$$f(x) = x^{10} + a_8x^8 + a_7x^7 + \cdots + a_1x + a_0 \tag{5}$$

for $a_i \in \mathbb{F}_{121}$ with $0 \leq i \leq 8$. Then there does not exist $(a_0, \ldots, a_8) \in (\mathbb{F}_{121})^{\oplus 9}$ such that $C : y^2 = f(x)$ is a superspecial hyperelliptic curve of genus 4 over $\mathbb{F}_{121}$.

Proposition 3. *Consider the polynomial $f(x) \in \mathbb{F}_{169}[x]$ of the form*

$$f(x) = x^{10} + a_8x^8 + a_7x^7 + \cdots + a_1x + a_0 \tag{6}$$

for $a_i \in \mathbb{F}_{169}$ with $0 \leq i \leq 8$. Then there does not exist $(a_0, \ldots, a_8) \in (\mathbb{F}_{169})^{\oplus 9}$ such that $C : y^2 = f(x)$ is a superspecial hyperelliptic curve of genus 4 over $\mathbb{F}_{169}$.

Proposition 4. *Consider the polynomial $f(x) \in \mathbb{F}_{17}[x]$ of the form*

$$f(x) = x^{10} + a_8x^8 + a_7x^7 + \cdots + a_1x + a_0, \tag{7}$$

for $a_i \in \mathbb{F}_{17}$ with $0 \leq i \leq 8$. Then there exist precisely 5 (resp. 2) superspecial hyperelliptic curves $C : cy^2 = f(x)$ with $c = 1$ or ϵ, up to isomorphism over $\mathbb{F}_{17}$ (resp. the algebraic closure of $\mathbb{F}_{17}$), such that $f(x)$ are of the form (7). Here ϵ is an element of $\mathbb{F}_{17}^{\times} \smallsetminus (\mathbb{F}_{17}^{\times})^2$. Representatives of the 5 isomorphisms classes over $\mathbb{F}_{17}$ are given by

1. $y^2 = x^{10} + x$,
2. $y^2 = x^{10} + x^7 + 13x^4 + 12x$,
3. $y^2 = x^{10} + x^7 + 14x^6 + 6x^5 + 12x^3 + 5x^2 + 7x + 6$,
4. $y^2 = x^{10} + x^8 + x^7 + 15x^6 + 4x^5 + 12x^4 + 15x^3 + 11x^2 + 9x + 4$, *and*
5. $y^2 = x^{10} + x^8 + 2x^7 + 9x^5 + x^4 + 10x^3 + 8x^2 + 11x + 16y^2 + 5$,

and those of the 2 isomorphism classes over the algebraic closure are given by

1. $y^2 = x^{10} + x$, *and*
2. $y^2 = x^{10} + x^7 + 13x^4 + 12x$.

Proposition 5. *Consider the polynomial $f(x) \in \mathbb{F}_{17^2}[x]$ of the form*

$$f(x) = x^{10} + a_8x^8 + a_7x^7 + \cdots + a_1x + a_0, \tag{8}$$

for $a_i \in K = \mathbb{F}_{17^2}$ with $0 \leq i \leq 8$. Then there exist precisely 25 (resp. 2) superspecial hyperelliptic curves $C : cy^2 = f(x)$ with $c = 1$ or ϵ, up to isomorphism over $\mathbb{F}_{17^2}$ (resp. the algebraic closure of $\mathbb{F}_{17^2}$), such that $f(x)$ are of the form (8).

Proof. We prove the assertion by executing *Enumeration Method* (Algorithm 1 for its pseudocode) and *Isomorphism Testing Method* given in §3.1 and §3.3 respectively. We first conduct *Enumeration Method.* In the following, we describe details of our computation, and also show our choices of coefficients to be regarded as indeterminates and a term ordering in the algorithm.

0. We regard the $s_1 := 8$ coefficients a_i for $0 \leq i \leq 7$ as indeterminates. For the Gröbner basis computation in $\mathbb{F}_{17^2}[a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7]$ below, we adopt the graded reverse lexicographic (grevlex) order with $a_7 \prec a_6 \prec a_5 \prec a_4 \prec a_3 \prec a_2 \prec a_1 \prec a_0$.

For each $c_8 \in \{0, 1, \zeta\}$, we proceed with the following four steps:

1. Put $f(x) := x^{10} + c_8 x^8 + a_7 x^7 + \cdots + a_1 x + a_0$, and compute $h := f^{p-1}$ over $\mathbb{F}_{17^2}[a_0, \ldots, a_7][x]$.
2. Let $\mathcal{S}$ be the set of the coefficients of the g^2 monomials in $h = f^{p-1}$, given in Proposition 1. Note that $\mathcal{S} \subset \mathbb{F}_{17^2}[a_0, \ldots, a_7]$.
3. We regard 6 unknown coefficients in f as indeterminates. Specifically, we keep $a_0, \ldots, a_5$ being indeterminates, whereas we substitute some elements of $\mathbb{F}_{17^2}$ into a_6 and a_7 in the next step.
4. For each $(c_6, c_7) \in (\mathbb{F}_{17^2})^{\oplus 2}$, proceed with the following three steps 4a – 4c:
   - 4a. For each $P \in \mathcal{S}$, substitute (c_6, c_7) into (a_6, a_7) of the coefficients in P. Put $\mathcal{S}' := \{P(a_0, \ldots, a_5, c_6, c_7) : P \in \mathcal{S}\}$. Note that $\mathcal{S}' \subset \mathbb{F}_{17^2}[a_0, \ldots, a_5]$.
   - 4b. Compute the roots of the multivariate system $P'(a_0, \ldots, a_5) = 0$ for all $P' \in \mathcal{S}'$ over $\mathbb{F}_{17^2}$ with Gröbner basis algorithms.
   - 4c. For each root $(c_0, \ldots, c_5)$ of the system constructed in Step 4b, substitute it into unknown coefficients in f. Namely, we set $f_{\mathrm{sol}} := x^{10} + c_8 x^8 + c_7 x^7 + \cdots + c_1 x + c_0$. Decide whether f_{sol} has no double root in the algebraic closure or not (this can be done by constructing the minimal splitting field of f_{sol}). If f_{sol} has no double root in the algebraic closure, store f_{sol}.

As a computational result, we obtain the set $\mathcal{F}$ of all the polynomials $f(x)$ of the form (8) such that $C : y^2 = f(x)$ are superspecial hyperelliptic curves of genus 4 over $\mathbb{F}_{17^2}$. 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 $H_1 \neq H_2$, we execute *Isomorphism Testing Method* given in §3.3. We obtain a subset $\mathcal{H} \subset \mathcal{H}_0$ such that for each pair (H_1, H_2) of elements in $\mathcal{H}$ with $H_1 \neq H_2$, the two hyperelliptic curves $C_1 : H_1(x, y) = 0$ and $C_2 : H_2(x, y) = 0$ are not isomorphic over $\mathbb{F}_{17^2}$. The obtained set $\mathcal{H}$ consists of 25 elements. This shows the assertion over $\mathbb{F}_{17^2}$. Similarly, by executing *Isomorphism Testing Method* again for pairs of elements in $\mathcal{H}$, we obtain representatives of the isomorphism classes over the algebraic closure of $\mathbb{F}_{17^2}$. The resulting set consists of 2 elements. □

Proposition 6. *Consider the polynomial $f(x) \in \mathbb{F}_{19}[x]$ of the form*

$$f(x) = x^{10} + a_8 x^8 + a_7 x^7 + \cdots + a_1 x + a_0 \tag{9}$$

for $a_i \in \mathbb{F}_{19}$ with $0 \leq i \leq 8$. Then there exist precisely 12 *(resp.* 2*) superspecial hyperelliptic curves $C : cy^2 = f(x)$ with $c = 1$ or ϵ, up to isomorphism over $\mathbb{F}_{19}$ (resp. the algebraic closure of $\mathbb{F}_{19}$), such that $f(x)$ are of the form* (9)*. Representatives of the* 12 *isomorphisms classes over $\mathbb{F}_{19}$ are given by*

1. $y^2 = x^{10} + 1$,
2. $y^2 = x^{10} + 2$,
3. $y^2 = x^{10} + x^7 + 4x^6 + 15x^5 + 6x^4 + 8x^3 + 5x^2 + 12x + 1$,
4. $y^2 = x^{10} + x^8 + 7x^6 + x^4 + x^2 + 7$,
5. $y^2 = x^{10} + x^8 + x^7 + 12x^6 + x^5 + 10x^4 + 9x^3 + 8x^2 + 9x + 3$,
6. $y^2 = x^{10} + x^8 + x^7 + 13x^6 + 9x^5 + 14x^4 + 4x^3 + 11x^2 + 3x + 8$,
7. $y^2 = x^{10} + x^8 + 2x^7 + 6x^6 + 18x^5 + 4x^4 + 13x^3 + 18x^2 + 10x + 14$,
8. $y^2 = x^{10} + x^8 + 2x^7 + 12x^6 + 18x^4 + 5x^3 + x^2 + 7$,
9. $y^2 = x^{10} + x^8 + 4x^7 + 8x^6 + 8x^5 + 3x^4 + 11x^3 + 8x^2 + 8x + 4$,
10. $y^2 = x^{10} + 2x^8 + 9x^6 + 8x^4 + 16x^2 + 15$,
11. $y^2 = x^{10} + 2x^8 + x^7 + 12x^6 + 9x^5 + 2x^3 + 4x^2 + 7x + 4$, *and*
12. $y^2 = x^{10} + 2x^8 + 3x^7 + 17x^6 + 9x^5 + 2x^3 + 12x^2 + 2x + 4$,

and those of the 2 *isomorphism classes over the algebraic closure are given by*

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

Remark 4. 1. We have explicit defining equations of the 25 superspecial curves in Proposition 5 but omit them in the statement. See a table at [27] for the equations.
2. The source codes and the log files together with detailed information on timing are available at [27].
3. In our implementations, we used the Magma function Variety to solve multivariate systems over finite fields. We also used FactorisationOverSplittingField in order to decide whether a univariate polynomial over a finite field has no double root or not.

4.3 Application to finding maximal curves and minimal curves

We found maximal curves and minimal curves over $\mathbb{F}_{p^2}$ for $p = 17$ and 19 among enumerated superspecial hyperelliptic curves, see also a table on the web page of the first author [27]. We here introduce several explicit equations (cf. the example C_a given in §1 is included in one of the $\mathbb{F}_{17}$-isomorphism classes of superspecial hyperelliptic curves over $\mathbb{F}_{17}$ enumerated in Proposition 4).

1. Recall from Corollary 5 that there exist precisely 2 (resp. 2) maximal (resp. minimal) hyperelliptic curves over $\mathbb{F}_{17^2}$ up to isomorphism over $\mathbb{F}_{17^2}$. Specifically, the two maximal curves are given by $y^2 = x^{10} + x$ and $y^2 = x^{10} + x^7 + 13x^4 + 12x$, respectively. The two minimal curves are given by

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

respectively, where we take $\zeta = -8 + \sqrt{61} \in \mathbb{F}_{17^2}$. The above four equations are obtained in Proposition 5 as representatives of the $\mathbb{F}_{17^2}$-isomorphism classes of the superspecial hyperelliptic curves of genus 4 over $\mathbb{F}_{17^2}$.

2. There exist maximal curves and minimal curves over $\mathbb{F}_{19^2}$, see Corollary 6. Specifically, the following hyperelliptic curves (1) – (5) are maximal as curves over $\mathbb{F}_{19^2}$: (1) $y^2 = x^{10} + 1$, (2) $y^2 = x^{10} + 2$, (3) $y^2 = x^{10} + x^7 + 4x^6 + 15x^5 + 6x^4 + 8x^3 + 5x^2 + 12x + 1$, (4) $y^2 = x^{10} + x^8 + 7x^6 + x^4 + x^2 + 7$, and (5) $y^2 = x^{10} + 2x^8 + 9x^6 + 8x^4 + 16x^2 + 15$. On the other hand, the following curve is minimal: (6) $y^2 = x^{10} + x^8 + 2x^7 + 12x^6 + 18x^4 + 5x^3 + x^2 + 7$. The above six equations are listed in Proposition 6 as representatives of the $\mathbb{F}_{19}$-isomorphism classes of the superspecial hyperelliptic curves of genus 4 over $\mathbb{F}_{19}$.

Remark 5. 1. We have that 3 of the defining equations listed in Proposition 4 define maximal curves over $\mathbb{F}_{17^2}$, but omit them here (cf. [27]).

2. Note that 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., [23] for more general results on the existence of such a kind of maximal hyperelliptic curves.

5 Concluding remark

We enumerated the isomorphism classes of superspecial hyperelliptic curves of genus 4 over finite fields $\mathbb{F}_q$ for $q = 11$, 11^2, 13, 13^2, 17, 17^2 and 19. Specifically, the enumerations were theoretically reduced into computational problems. To solve the problems in real time, we proposed three computational methods. With our methods, we have succeeded in finishing all required computations within a day in total. Our computational results show the non-existence of a superspecial hyperelliptic curve in characteristic $p = 11$ and 13. They also provide explicit defining equations for the enumerated superspecial hyperelliptic curves in characteristic $p = 17$ and 19. Many of them are maximal curves over $\mathbb{F}_{17^2}$ and $\mathbb{F}_{19^2}$, respectively. Indeed, we found that 3 (resp. 2) among the 5 (resp. 25) superspecial curves over $\mathbb{F}_{17}$ (resp. $\mathbb{F}_{17^2}$) are maximal curves over $\mathbb{F}_{17^2}$, and that 5 among the 12 superspecial curves over $\mathbb{F}_{19}$ are those over $\mathbb{F}_{19^2}$.

References

1. Bettale, L., Faugère, J.-C. and Perret, L.: *Hybrid approach for solving multivariate systems over finite fields*, J. Math. Crypt. **3** (2009), 177–197.
2. Bosma, W., Cannon, J. and Playoust, C.: *The Magma algebra system. I. The user language*, Journal of Symbolic Computation **24**, 235–265 (1997)
3. Deuring, M.: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Univ. Hamburg **14** (1941), no. 1, 197–272.
4. Ekedahl, T.: *On supersingular curves and abelian varieties*, Math. Scand. **60** (1987), 151–178.
5. Fuhrmann R., Garcia, A., Torres, F.: *On maximal curves*, Journal of number theory **67**, 29–51 (1997)

6. van der Geer, et al.: *Tables of Curves with Many Points*, 2009, `http://www.manypoints.org`, Retrieved at 5th April, 2018.
7. 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)
8. Hartshorne, R.: *Algebraic Geometry*, GTM **52**, Springer-Verlag (1977)
9. Hashimoto K.: *Class numbers of positive definite ternary quaternion Hermitian forms.* Proc. Japan Acad. Ser. A Math. Sci. **59** (1983), no. 10, 490–493.
10. 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).
11. Hurt, N. E.: *Many Rational Points: Coding Theory and Algebraic Geometry*, Kluwer Academic Publishers, 2003.
12. Ibukiyama, T.: *On rational points of curves of genus* 3 *over finite fields*, Tohoku Math. J. **45** (1993), 311-329.
13. 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.
14. Kudo, M. and Harashita, S.: *Superspecial curves of genus* 4 *in small characteristic*, Finite Fields and Their Applications, **45**, 131–169, 2017.
15. Kudo, M. and Harashita, *Enumerating superspecial hyperelliptic curves of genus* 4 *over small finite fields*, in preparation.
16. Kudo, M. and Harashita, S.: *Enumerating superspecial curves of genus* 4 *over prime fields*, arXiv: 1702.05313 [math.AG], 2017.
17. Kudo, M. and Harashita, S.: *Enumerating Superspecial Curves of Genus* 4 *over Prime Fields* (abstract version of [16]), In: Proceedings of The Tenth International Workshop on Coding and Cryptography 2017 (WCC2017), September 18-22, 2017, Saint-Petersburg, Russia, available at `http://wcc2017.suai.ru/proceedings.html`
18. Li, K.-Z. and Oort, F.: *Moduli of Supersingular Abelian Varieties*, Lecture Notes in Mathematics, **1680**. Springer-Verlag, Berlin, 1998.
19. 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).
20. Nygaard, N. O.: *Slopes of powers of Frobenius on crystalline cohomology*, Ann. Sci. École Norm. Sup. (4), **14**, No. 4, 369–401 (1982), 1981.
21. Özbudak, F. and Saygı, Z.: *Explicit maximal and minimal curves over finite fields of odd characteristics*, Finite Fields and Their Applications, **42**, 81–92, 2016.
22. Serre, J.-P.: *Nombre des points des courbes algebrique sur* $\mathbb{F}_q$, Sém. Théor. Nombres Bordeaux (2) 1982/83, 22 (1983).
23. Tafazolian, S.: *A note on certain maximal hyperelliptic curves*, Finite Fields and Their Applications, **18**, 1013–1016, 2012.
24. Tafazolian, S. and Torres, F.: *On the curve* $y^n = x^m + x$ *over finite fields*, Journal of Number Theory, **145**, 51–66, 2014.
25. Xue, J., Yang, T.-C. and Yu, C.-F.: *On superspecial abelian surfaces over finite fields*, Doc. Math. **21** (2016) 1607–1643.
26. Yui, N.: *On the Jacobian varieties of hyperelliptic curves over fields of characterisctic* $p > 2$, Journal of algebra, **52**, 378–410 (1978).
27. *Data base of superspecial curves of genus* 4 *over finite fields and their algebraic closures*, `http://www2.math.kyushu-u.ac.jp/~m-kudo/Ssp-curves-genus-4.html`