On the existence of superspecial nonhyperelliptic curves of genus 4

Momonari Kudo*†

June 25, 2019

Abstract

A curve over a perfect field K of characteristic $p > 0$ is said to be *superspecial* if its Jacobian is isomorphic to a product of supersingular elliptic curves over the algebraic closure $\overline{K}$. In recent years, isomorphism classes of superspecial nonhyperelliptic curves of genus 4 over finite fields in small characteristic have been enumerated. In particular, the non-existence of superspecial curves of genus 4 in characteristic $p = 7$ was proved. In this note, we give an elementary proof of the existence of superspecial nonhyperelliptic curves of genus 4 for infinitely many primes p. Specifically, we prove that the variety $C_p : x^3 + y^3 + w^3 = 2yw + z^2 = 0$ in the projective 3-space with $p > 2$ is a superspecial curve of genus 4 if and only if $p \equiv 2 \pmod 3$. Our computational results show that C_p with $p \equiv 2 \pmod 3$ are *maximal* curves over $\mathbb{F}_{p^2}$ for all $3 \leq p \leq 269$.

Key words— Nonhyperelliptic curves, Superspecial curves, Maximal curves

1 Introduction

Let p be a rational prime greater than 2, and let $\mathbb{F}_q$ denote the finite field of q elements, where q is a power of prime. Let K be an arbitrary perfect field of characteristic p. We denote by $\overline{K}$ the algebraic closure of K. By a curve, we mean a non-singular projective variety of dimension one. Let C be a curve of genus g over K. We say that C is *superspecial* if its Jacobian is isomorphic to the product of g supersingular elliptic curves over $\overline{K}$. The existence of a superspecial curve over an algebraically closed field in characteristic p implies that there exists a maximal or minimal curve over $\mathbb{F}_{p^2}$. Here a curve over $\mathbb{F}_q$ is called a maximal (resp. minimal) curve if the number of its $\mathbb{F}_q$-rational points attains the Hasse-Weil upper (resp. lower) bound $q + 1 + 2g\sqrt{q}$ (resp. $q + 1 - 2g\sqrt{q}$). Conversely, any maximal or minimal curve over $\mathbb{F}_{p^2}$ is superspecial. This work aims to find a lot of superspecial curves and maximal curves for a given genus. Note that for a fixed pair (g, q), superspecial curves over $\overline{\mathbb{F}_q}$ of genus g are very rare: the number of such curves is finite, whereas the whole set of curves over $\overline{\mathbb{F}_q}$ of genus g has dimension $3g - 3$. Thus, finding superspecial curves over $\mathbb{F}_q$ of higher genus g is more difficult than finding those of lower genus g.

In the case of $g \leq 3$ and in the case of hyperelliptic curves, many results on the existence and enumeration of superspecial/maximal curves are known, see e.g., [2], [17, Prop. 4.4] for $g = 1$, [7], [9], [13] for $g = 2$, [6], [8] for $g = 3$, and [15], [16] for hyperelliptic curves. In particular, it is well-known that there exist supersingular (and thus superspecial) elliptic curves in characteristic p for infinitely many primes p (see, e.g., [14, Examples 4.4 and 4.5])). For example, the elliptic curve

*Kobe City College of Technology.
†Institute of Mathematics for Industry, Kyushu University. E-mail: m-kudo@math.kyushu-u.ac.jp

$E_p : y^2 = x^3 + 1$ with $p \geq 5$ is supersingular if and only if $p \equiv 2 \pmod 3$. Moreover, the set of primes p for which E_p is supersingular has natural density $1/2$.

In the case of *nonhyperelliptic* curves of genus $g = 4$, Fuhrmann-Garcia-Torres proved in [4] that there exists a maximal (and superspecial) curve C_0 of $g = 4$ over $K = \mathbb{F}_{5^2}$, and that it gives a unique $\overline{K}$-isomorphism class. In [10], [11] and [12], the isomorphism classes of superspecial nonhyperelliptic curves of genus 4 over finite fields are enumerated in characteristic $p \leq 11$. Results in [10], [11] and [12] also show that there exist superspecial nonhyperelliptic curves of genus 4 in characteristic 5 and 11, whereas there does not exist such a curve in characteristic 7.

The objective of this note is to investigate whether a superspecial nonhyperelliptic curve of genus $g = 4$ exists or not for $p \geq 13$. In contrast to the rarity of superspecial curves of higher genus, our main results (Theorem 3.1 and Corollary 3.2 below) show the existence of superspecial curves of genus $g = 4$ in characteristic p for half of the primes as well as the case of $g = 1$.

Theorem 3.1. *Put $Q := 2yw + z^2$ and $P := x^3 + y^3 + w^3$. Let $C_p = V(Q, P)$ denote the projective zero-locus in $\mathbf{P}^3 = \mathrm{Proj}(\overline{K}[x, y, z, w])$ defined by $Q = 0$ and $P = 0$. Then C_p is a superspecial nonhyperelliptic curve of genus 4 if and only if $p \equiv 2 \pmod 3$.*

We prove Theorem 3.1 by simple computations in linear and fundamental commutative algebra and in combinatorics together with results in [10], [11] and [12] (so this note also complements results in these three previous papers). As a corollary of this theorem, we have the following:

Corollary 3.2. *There exist superspecial nonhyperelliptic curves of genus 4 in characteristic p for infinitely many primes p. The set of primes p for which C_p is superspecial has natural density $1/2$.*

Theorem 3.1 and Corollary 3.2 also give a partial answer to the genus 4 case of the problem proposed by Ekedahl in 1987, see p. 173 of [3]. In Section 4, we give a table of the number of $\mathbb{F}_{p^2}$-rational points on C_p for $3 \leq p \leq 269$ obtained by using a computer algebra system Magma [1]. As computational results, we found maximal nonhyperelliptic curves of genus 4 over $\mathbb{F}_{p^2}$. Specifically, we have that for all $3 \leq p \leq 269$ with $p \equiv 2 \pmod 3$, the curves C_p are maximal over $\mathbb{F}_{p^2}$.

Acknowledgments

The author thanks Shushi Harashita for his comments to the preliminary version of this note. He gave the author information on the existence of superspecial curves of genus g over $\mathbb{F}_q$ in the case of $g \leq 3$, in the case of $(g, q) = (4, 13)$, and in the hyperelliptic case. He also pointed out that computing the rational points of our curves is reduced into solving a diagonal equation.

2 Superspecialty of curves $x^3 + y^3 + w^3 = 2yw + z^2 = 0$

As in the previous section, let K be a perfect field of characteristic $p > 2$. Let $K[x, y, z, w]$ denote the polynomial ring of the four variables x, y, z and w over K. As examples of superspecial curves of genus $g = 4$ in characteristic $p = 5$ and 11, we have the projective varieties in the projective 3-space $\mathbf{P}^3 = \mathrm{Proj}(\overline{K}[x, y, z, w])$ defined by the same systems of equations: $x^3 + y^3 + w^3 = 0$ and $2yw + z^2 = 0$, see [10, Exmaple 6.2.1] and [11, Proposition 4.4.4].

In this section, we shall prove that the variety $x^3 + y^3 + w^3 = 2yw + z^2 = 0$ over K is (resp. not) a superspecial curve of genus 4 if $p \equiv 2 \pmod 3$ (resp. $p \equiv 1 \pmod 3$). Throughout this section, we set $Q := 2yw + z^2$ and $P := x^3 + y^3 + w^3$. Let C_p denote the projective variety $V(Q, P)$ in $\mathbf{P}^3$

defined by $P = Q = 0$ in characteristic p. First, we prove that the variety C_p is non-singular (resp. singular) if $p > 3$ (resp. $p = 3$).

Lemma 2.1. *If $p > 3$ (resp. $p = 3$), then the variety $C_p = V(Q, P)$ is non-singular (resp. singular).*

Proof. Let $J(P, Q)$ denote the set of all the minors of degree 2 of the Jacobian matrix

$$\begin{pmatrix} \frac{\partial P}{\partial x} & \frac{\partial P}{\partial y} & \frac{\partial P}{\partial z} & \frac{\partial P}{\partial w} \\ \frac{\partial Q}{\partial x} & \frac{\partial Q}{\partial y} & \frac{\partial Q}{\partial z} & \frac{\partial Q}{\partial w} \end{pmatrix} = \begin{pmatrix} 3x^2 & 3y^2 & 0 & 3w^2 \\ 0 & 2w & 2z & 2y \end{pmatrix}.$$

Namely, the set $J(P, Q)$ consists of the following 6 elements:

$$\begin{aligned}
f_1 &:= \frac{\partial P}{\partial x} \cdot \frac{\partial Q}{\partial y} - \frac{\partial P}{\partial y} \cdot \frac{\partial Q}{\partial x} = 6x^2 w, \\
f_2 &:= \frac{\partial P}{\partial x} \cdot \frac{\partial Q}{\partial z} - \frac{\partial P}{\partial z} \cdot \frac{\partial Q}{\partial x} = 6x^2 z, \\
f_3 &:= \frac{\partial P}{\partial x} \cdot \frac{\partial Q}{\partial w} - \frac{\partial P}{\partial w} \cdot \frac{\partial Q}{\partial x} = 6x^2 y, \\
f_4 &:= \frac{\partial P}{\partial y} \cdot \frac{\partial Q}{\partial z} - \frac{\partial P}{\partial z} \cdot \frac{\partial Q}{\partial y} = 6y^2 z, \\
f_5 &:= \frac{\partial P}{\partial y} \cdot \frac{\partial Q}{\partial w} - \frac{\partial P}{\partial w} \cdot \frac{\partial Q}{\partial y} = 6y^3 - 6w^3, \\
f_6 &:= \frac{\partial P}{\partial z} \cdot \frac{\partial Q}{\partial w} - \frac{\partial P}{\partial w} \cdot \frac{\partial Q}{\partial z} = -6zw^2.
\end{aligned}$$

Assume $p > 3$. It suffices to show that x, y, z and w belong to the radical of the ideal generated by P, Q and $J(P, Q)$. By straightforward computations, we have

$$\begin{aligned}
x^2 P - (6^{-1} y^2) f_3 - (6^{-1} w^2) f_1 &= x^5, \\
yP - (6^{-1} x) f_3 - (6^{-1} y) f_5 &= 2y^4, \\
(-2yzw + z^3) Q + (2 \cdot 3^{-1} w^2) f_4 &= z^5, \\
wP - (6^{-1} x) f_1 - (6^{-1} w) f_5 &= 2w^4,
\end{aligned}$$

which belong to the ideal $\langle P, Q, J(P, Q) \rangle$ in $K[x, y, z, w]$. Thus, x, y, z and w belong to its radical.

If $p = 3$, then $J(P, Q) = \{0\}$, and hence all the points on $V(Q, P)$ are singular points. $\square$

In the following, we suppose $p > 3$. It is shown in [10] that we can decide whether C_p is superspecial or not by computing the coefficients of certain monomials in $(QP)^{p-1}$.

Proposition 2.2 ([10], Corollary 3.1.6)**.** *With notation as above, the curve C_p is superspecial if and only if the coefficients of all the following 16 monomials of degree $5(p-1)$ in $(QP)^{p-1}$ are zero:*

$$\begin{array}{cccc}
(x^2yzw)^{p-1}, & x^{2p-1}y^{p-2}z^{p-1}w^{p-1}, & x^{2p-1}y^{p-1}z^{p-2}w^{p-1}, & x^{2p-1}y^{p-1}z^{p-1}w^{p-2}, \\
x^{p-2}y^{2p-1}z^{p-1}w^{p-1}, & (xy^2zw)^{p-1}, & x^{p-1}y^{2p-1}z^{p-2}w^{p-1}, & x^{p-1}y^{2p-1}z^{p-1}w^{p-2}, \\
x^{p-2}y^{p-1}z^{2p-1}w^{p-1}, & x^{p-1}y^{p-2}z^{2p-1}w^{p-1}, & (xyz^2w)^{p-1}, & x^{p-1}y^{p-1}z^{2p-1}w^{p-2}, \\
x^{p-2}y^{p-1}z^{p-1}w^{2p-1}, & x^{p-1}y^{p-2}z^{p-1}w^{2p-1}, & x^{p-1}y^{p-1}z^{p-2}w^{2p-1}, & (xyzw^2)^{p-1}.
\end{array}$$

To prove Theorem 3.1 stated in Section 1 (and in Section 3), we compute the 16 coefficients given in Proposition 2.2. Note that we have $QP = x^3z^2 + y^3z^2 + 2x^3yw + 2y^4w + z^2w^3 + 2yw^4$, and

$$\begin{aligned}
(QP)^{p-1} &= \sum_{a+b+c+d+e+f=p-1} \binom{p-1}{a,b,c,d,e,f} (x^3z^2)^a (y^3z^2)^b (2x^3yw)^c (2y^4w)^d (z^2w^3)^e (2yw^4)^f \\
&= \sum_{a+b+c+d+e+f=p-1} \binom{p-1}{a,b,c,d,e,f} (x^{3a}z^{2a})(y^{3b}z^{2b})(2^c x^{3c} y^c w^c)(2^d y^{4d} w^d)(z^{2e}w^{3e})(2^f y^f w^{4f}) \\
&= \sum_{a+b+c+d+e+f=p-1} 2^{c+d+f} \cdot \binom{p-1}{a,b,c,d,e,f} x^{3a+3c} y^{3b+c+4d+f} z^{2a+2b+2e} w^{c+d+3e+4f} \qquad (2.1)
\end{aligned}$$

by the multinomial theorem. To express $(QP)^{p-1}$ as a sum of the form

$$(QP)^{p-1} = \sum_{(i,j,k,\ell)\in(\mathbb{Z}_{\geq 0})^{\oplus 4}} c_{i,j,k,\ell} x^i y^j z^k w^\ell,$$

we consider the linear system

$$\begin{cases} a+b+c+d+e+f = p-1, \\ 3a+3c = i, \\ 3b+c+4d+f = j, \\ 2a+2b+2e = k, \\ c+d+3e+4f = \ell, \end{cases} \qquad (2.2)$$

and put

$$S(i,j,k,\ell) := \{(a,b,c,d,e,f) \in [0,p-1]^{\oplus 6} : (a,b,c,d,e,f) \text{ satisfies } (2.2)\} \qquad (2.3)$$

for each $(i,j,k,\ell) \in (\mathbb{Z}_{\geq 0})^{\oplus 4}$. Using the notation $S(i,j,k,\ell)$, we have

$$(QP)^{p-1} = \sum_{(i,j,k,\ell)\in(\mathbb{Z}_{\geq 0})^{\oplus 4}} \left(\sum_{(a,b,c,d,e,f)\in S(i,j,k,\ell)} 2^{c+d+f} \cdot \binom{p-1}{a,b,c,d,e,f} \right) x^i y^j z^k w^\ell. \qquad (2.4)$$

Lemma 2.3. *With notation as above, the coefficients of the monomials $x^iy^jz^{p-2}w^\ell$ and $x^iy^jz^{2p-1}w^\ell$ in $(QP)^{p-1}$ are zero for all $(i,j,\ell) \in (\mathbb{Z}_{\geq 0})^{\oplus 3}$.*

Proof. Recall from (2.1) that the z-exponent of each monomial in $(QP)^{p-1}$ is $2a+2b+2e$, which is an even number. On the other hand, the z-exponents of the monomials $x^iy^jz^{p-2}w^\ell$ and $x^iy^jz^{2p-1}w^\ell$ are odd numbers, and thus their coefficients in $(QP)^{p-1}$ are all zero. □

Let $\mathcal{M}$ be the set of the 16 monomials given in Proposition 2.2, and set

$$E(\mathcal{M}) := \{(i,j,k,\ell) \in (\mathbb{Z}_{\geq 0})^{\oplus 4} : x^iy^jz^kw^\ell = m \text{ for some } m \in \mathcal{M}\},$$

which is the set of the exponent vectors of the monomials in $\mathcal{M}$.

Lemma 2.4. *Assume $p \equiv 2 \pmod 3$. Then we have $S(i,j,k,\ell) = \emptyset$ for any $(i,j,k,\ell) \in E(\mathcal{M})$.*

Proof. Note that for each $(i,j,k,\ell) \in E(\mathcal{M})$, we have $i+j+k+\ell = 5(p-1)$, see Proposition 2.2. Using matrices, we write the system (2.2) as

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 3 & 0 & 3 & 0 & 0 & 0 \\ 0 & 3 & 1 & 4 & 0 & 1 \\ 2 & 2 & 0 & 0 & 2 & 0 \\ 0 & 0 & 1 & 1 & 3 & 4 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \\ e \\ f \end{pmatrix} = \begin{pmatrix} p-1 \\ i \\ j \\ k \\ \ell \end{pmatrix}, \tag{2.5}$$

whose extended coefficient matrix is transformed as follows:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & p-1 \\ 3 & 0 & 3 & 0 & 0 & 0 & i \\ 0 & 3 & 1 & 4 & 0 & 1 & j \\ 2 & 2 & 0 & 0 & 2 & 0 & k \\ 0 & 0 & 1 & 1 & 3 & 4 & \ell \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & p-1 \\ 0 & 3 & 1 & 4 & 0 & 1 & j \\ 0 & 0 & 1 & 1 & -3 & -2 & i+j-3(p-1) \\ 0 & 0 & 0 & 0 & 6 & 6 & \ell-(i+j-3(p-1)) \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Considering modulo 3, we have the following linear system over $\mathbb{F}_3$:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} a' \\ b' \\ c' \\ d' \\ e' \\ f' \end{pmatrix} = \begin{pmatrix} p-1 \\ j \\ i+j \\ \ell-(i+j) \\ 0 \end{pmatrix},$$

which is equivalent to

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} a' \\ b' \\ c' \\ d' \\ e' \\ f' \end{pmatrix} = \begin{pmatrix} p-1 \\ j \\ i \\ \ell-(i+j) \\ 0 \end{pmatrix}. \tag{2.6}$$

Note that the system (2.6) over $\mathbb{F}_3$ has a solution if and only if $i \equiv 0 \pmod 3$ and $\ell \equiv j \pmod 3$. We claim that if $p \equiv 2 \pmod 3$, the original system (2.5) over $\mathbb{Z}$ has no solution in $[0,p-1]^{\oplus 6}$ for any $(i,j,k,\ell) \in E(\mathcal{M})$. Indeed, if $p \equiv 2 \pmod 3$ and if the system (2.5) has a solution in $[0,p-1]^{\oplus 6}$ for some $(i,j,k,\ell) \in E(\mathcal{M})$, the system (2.6) has a solution. By Lemma 2.3, we may assume $k \neq p-2$ and $k \neq 2p-1$, i.e., $k = 2p-2$ or $k = p-1$. Since $i \equiv 0 \pmod 3$ and since $p \equiv 2 \pmod 3$, the integer i is equal to $2p-1$ or $p-2$, and thus $(i,j,k,\ell) = (2p-1, p-2, p-1, p-1)$, $(2p-1, p-1, p-1, p-2)$, $(p-2, 2p-1, p-1, p-1)$ or $(p-2, p-1, p-1, 2p-1)$. However, any of the above four candidates for (i,j,k,ℓ) does not satisfy $\ell \equiv j \pmod 3$, which is a contradiction. □

Proposition 2.5. *Assume $p \equiv 2 \pmod 3$. Then the curve $C_p = V(Q,P)$ is superspecial.*

Proof. It follows from Lemma 2.4 that the coefficient of $x^i y^j z^k w^\ell$ in (2.4) is zero for each $(i,j,k,\ell) \in E(\mathcal{M})$. By Proposition 2.2, the curve $V(Q,P)$ is superspecial. □

It follows from the proof of Lemma 2.4 that (2.2) is equivalent to the following system:

$$\begin{cases} a+b+c+d+e+f=p-1, \\ 3b+c+4d+f=j, \\ c+d-3e-2f=i+j-3(p-1), \\ 6e+6f=\ell-(i+j-3(p-1)). \end{cases} \tag{2.7}$$

Next, we consider the case of $p \equiv 1 \pmod 3$.

Lemma 2.6. *Assume $p \equiv 1 \pmod 3$. Then we have $\#S(p-1,p-1,2p-2,p-1)=1$. In other words, the system (2.7) with $(i,j,k,\ell)=(p-1,p-1,2p-2,p-1)$ has a unique solution in $[0,p-1]^{\oplus 6}$. The solution is given by*

$$\begin{pmatrix} a, & b, & c, & d, & e, & f \end{pmatrix} = \begin{pmatrix} (p-1)/3, & (p-1)/3, & 0, & 0, & (p-1)/3, & 0 \end{pmatrix}. \tag{2.8}$$

Proof. The system to be solved with $(i,j,k,\ell)=(p-1,p-1,2p-2,p-1)$ is given by

$$\begin{cases} a+b+c+d+e+f=p-1, & (2.9) \\ 3b+c+4d+f=p-1, & (2.10) \\ c+d-3e-2f=-(p-1), & (2.11) \\ 6e+6f=2(p-1) & (2.12) \end{cases}$$

with $(a,b,c,d,e,f) \in [0,p-1]^{\oplus 6}$. Since $c+d-3e-2f=c+d+f-(3e+3f)$, it follows from (2.11) and (2.12) that $c+d+f=0$, and thus $c=d=f=0$. By (2.10) and (2.12), we have $b=e=(p-1)/3$. From (2.9), we also have $a=(p-1)/3$. □

Lemma 2.7. *Assume $p \equiv 1 \pmod 3$. Then the coefficient of the monomial $x^{p-1}y^{p-1}z^{2p-2}w^{p-1}$ in $(QP)^{p-1}$ is not zero.*

Proof. Let $c_{p-1,p-1,2p-2,p-1}$ be the coefficient of $x^{p-1}y^{p-1}z^{2p-2}w^{p-1}$ in $(QP)^{p-1}$. Recall from (2.4) that $c_{p-1,p-1,2p-2,p-1}$ is given by

$$\sum_{(a,b,c,d,e,f)\in S(p-1,p-1,2p-2,p-1)} 2^{c+d+f} \cdot \binom{p-1}{a,b,c,d,e,f},$$

where $S(p-1,p-1,2p-2,p-1)$ is defined in (2.3). By Lemma 2.6, the set $S(p-1,p-1,2p-2,p-1)$ consists of only the element given by (2.8), and hence

$$c_{p-1,p-1,2p-2,p-1} = \frac{(p-1)!}{\left(\frac{p-1}{3}\right)!\left(\frac{p-1}{3}\right)!\left(\frac{p-1}{3}\right)!},$$

which is not divisible by p. □

Proposition 2.8. *Assume $p \equiv 1 \pmod 3$. Then the curve $C_p = V(Q,P)$ is not superspecial.*

Proof. It follows from Lemma 2.7 that the coefficient of $x^{p-1}y^{p-1}z^{2p-2}w^{p-1}$ in $(QP)^{p-1}$ is not zero. By Proposition 2.2, the curve $V(Q,P)$ is not superspecial. □

3 Proofs of main results and some further problems

As in the previous section, let K be a perfect field of characteristic $p > 2$. Here, we re-state Theorem 3.1 and Corollary 3.2 in Section 1 and prove them:

Theorem 3.1. *Put $Q := 2yw + z^2$ and $P := x^3 + y^3 + w^3$. Let $C_p = V(Q, P)$ denote the projective zero-locus in $\mathbf{P}^3 = \mathrm{Proj}(\overline{K}[x, y, z, w])$ defined by $Q = 0$ and $P = 0$. Then C_p is a superspecial nonhyperelliptic curve of genus 4 if and only if $p \equiv 2 \pmod 3$.*

Proof. Recall from Lemma 2.1 that C_p is singular if $p = 3$, and non-singular if $p > 3$. We may assume $p > 3$. Since C_p is the set of the zeros of the quadratic form Q and the cubic form P over K, it is a nonhyperelliptic curve of genus 4 over K, see [10, Section 2]. It follows from Propositions 2.5 and 2.8 that the non-singular curve C_p is superspecial if and only if $p \equiv 2 \pmod 3$. □

Corollary 3.2. *There exist superspecial nonhyperelliptic curves of genus 4 in characteristic p for infinitely many primes p. The set of primes p for which C_p is superspecial has natural density $1/2$.*

Proof. The first claim immediately follows from Theorem 3.1 and Dirichlet's Theorem. The second claim is deduced from the fact that the natural density of primes equal to 2 modulo 3 is $1/\varphi(3) = 1/2$, where φ is Euler's totient function. □

Problem 3.3. *Does there exist a superspecial curve of genus 4 in characteristic p for any $p > 13$ with $p \equiv 1 \pmod 3$? Cf. the non-existence for $p = 7$ is already shown in* [10]*, whereas the existence for $p = 13$ is shown, see e.g.,* [5].

Problem 3.4. *Find a different condition from $p \equiv 2 \pmod 3$ such that there exists a nonhyperelliptic superspecial curve of genus 4 in characteristic p. Cf. in the case of $g = 1$, the elliptic curve $E : y^2 = x^3 + x$ is supersingular if $p \equiv 3 \pmod 4$ and ordinary if $p \equiv 1 \pmod 4$. (Also for hyperelliptic curves, such conditions are already found, see e.g.,* [15] *and* [16].)

4 Application: Finding maximal curves over $K = \mathbb{F}_{p^2}$ for large p

In the following, we set $K := \mathbb{F}_{p^2}$ with $p > 2$. It is known that any maximal or minimal curve over $\mathbb{F}_{p^2}$ is supersepcial. 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 [10, Proposition 2.2.1]. Recall from Theorem 3.1 that $C_p = V(Q, P)$ with $Q = 2yw + z^2$ and $P = x^3 + y^3 + w^3$ is a superspecial curve of genus 4 if and only if $p \equiv 2 \pmod 3$. We computed the number of $\mathbb{F}_{p^2}$-rational points on C_p for $3 \leq p \leq 269$ using a computer algebra system Magma [1]. Table 1 shows our computational results for $3 \leq p \leq 100$. We see from Table 1 that any superspecial C_p is maximal over $\mathbb{F}_{p^2}$ for $3 \leq p \leq 100$ (also for $101 \leq p \leq 269$, but omit to write them in the table). From our computational results, let us give a conjecture on the existence of $\mathbb{F}_{p^2}$-maximal nonhyperelliptic curves of genus 4.

Conjecture 4.1. *For any p with $p \equiv 2 \pmod 3$, the curve C_p over $\mathbb{F}_{p^2}$ is maximal.*

Remark 4.2. We can reduce computing the number of $\mathbb{F}_{p^2}$-rational points on C_p into computing that of zeros of a *diagonal* equation. Specifically, by $2yw + z^2 = 0$ and $x^3 + y^3 + w^3 = 0$, we have $x^3 + y^3 + (-z^2/(2y)^{-1})^3 = 0$ and thus $8x^3y^3 + 8y^6 - z^6 = 0$ if $y \neq 0$. Putting $X = xy$, one has the diagonal equation $8X^3 + 8y^6 - z^6 = 0$. Hence, we may apply known methods to count the number of rational points of diagonal equations, see e.g., [18] and [19]. At the time of this writing (as of April 24, 2018), however, we have not succeeded in applying any known method.

Table 1: The number of $\mathbb{F}_{p^2}$-rational points on $C_p = V(Q, P)$ for $3 \leq p \leq 100$, where $Q = 2yw + z^2$ and $P = x^3 + y^3 + w^3$. We denote by $\#C_p(\mathbb{F}_{p^2})$ the number of $\mathbb{F}_{p^2}$-rational points on C_p for each p.

p	p mod 3	S.sp. or not	$\#C_p(\mathbb{F}_{p^2})$	p	p mod 3	S.sp. or not	$\#C_p(\mathbb{F}_{p^2})$
3	0	Not S.sp.	10	43	1	Not S.sp.	1938
5	2	S.sp.	66 (Max.)	47	2	S.sp.	2586 (Max.)
7	1	Not S.sp.	48	53	2	S.sp.	3234 (Max.)
13	1	Not S.sp.	192	59	2	S.sp.	3954 (Max.)
11	2	S.sp.	210 (Max.)	61	1	Not S.sp.	3648
17	2	S.sp.	426 (Max.)	67	1	Not S.sp.	4368
19	1	Not S.sp.	336	71	2	S.sp.	5610 (Max.)
23	2	S.sp.	714 (Max.)	73	1	Not S.sp.	5376
29	2	S.sp.	1074 (Max.)	79	1	Not S.sp.	6384
31	1	Not S.sp.	1146	83	2	S.sp.	7554 (Max.)
37	1	S.sp.	1334	89	2	S.sp.	8634 (Max.)
41	2	S.sp.	2010 (Max.)	97	1	Not S.sp.	9408

References

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

[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] Fuhrmann R., Garcia, A., Torres, F.: *On maximal curves*, J. of Number Theory **67**, 29–51, 1997

[5] van der Geer, et al.: *Tables of Curves with Many Points*, 2009, `http://www.manypoints.org`, Retrieved at 20th April, 2018.

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

[7] 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).

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

[9] 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.

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

[11] Kudo, M. and Harashita, S.: *Enumerating superspecial curves of genus* 4 *over prime fields*, arXiv: 1702.05313 [math.AG], 2017.

[12] Kudo, M. and Harashita, S.: *Enumerating Superspecial Curves of Genus* 4 *over Prime Fields* (abstract version of [11]), 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`

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

[14] Silverman, J. H.: *The Arithmetic of Elliptic curves*, GTM **106**, Springer-Verlag New York, 2009.

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

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

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

[18] Wan, D.: *Zeros of Diagonal Equations over Finite Fields*, Proceedings of the American Mathematical Society, Vol. **103**, No. 4 (1988), pp. 1049-1052.

[19] Weil, A.: *Numbers of solutions of equations in finite fields*, Bulletin of the American Mathematical Society, Vol. **55**, No. 5 (1949), 497-508.