On the maximality of hyperelliptic Howe curves of genus 3

Ryo Ohashi

February 1, 2022

Abstract

In this paper, we study a Howe curve $C$ in positive characteristic $p \geq 3$ which is of genus 3 and is hyperelliptic. We will show that if $C$ is superspecial, then its standard form is maximal or minimal over $\mathbb{F}_{p^2}$ without taking its $\mathbb{F}_{p^2}$-form.

Keywords: Algebraic curve, Superspecial curve, Maximal curve, Positive characteristic

2010 Mathematical Subject Classification: 14G05, 14G17, 14H45, 14H50

1 Introduction

Throughout this paper, a curve always means a projective variety in positive characteristic $p \geq 3$ of dimension one. It is well-known that any nonsingular genus-$g$ curve $C$ defined over $\mathbb{F}_q$ with $q = p^n$ satisfies the Hasse-Weil inequality

$$1 + q - 2g\sqrt{q} \leq \#C(\mathbb{F}_q) \leq 1 + q + 2g\sqrt{q},$$

where $C(\mathbb{F}_q)$ denotes the set of $\mathbb{F}_q$-rational points of $C$. Now, a nonsingular curve $C$ is called maximal (resp. minimal) when the number of $\mathbb{F}_q$-rational points of $C$ attains the upper (resp. lower) bound. Maximal curves have been investigated for their applications to coding theory. On the other hand, a genus-$g$ curve $C$ is called superspecial when $\text{Jac}(C)$ is isomorphic to the product of supersingular elliptic curves. This is equivalent to saying that the $a$-number of $C$ is equal to $g$. Here the $a$-number of $C$ is defined to be the dimension of $\text{Hom}(\alpha_p, \text{Jac}(C)[p])$, where $\alpha_p$ is the Frobenius kernel on the additive group $\mathbb{G}_a$. It is also known that all maximal or minimal curves over $\mathbb{F}_{p^2}$ are superspecial, while superspecial curves over $\mathbb{F}_{p^2}$ are not necessarily maximal nor minimal.

Ibukiyama [7] showed that there exists a superspecial genus-3 curve $C$ over $\mathbb{F}_p$ such that $C$ is maximal over $\mathbb{F}_{p^2}$. However, the curve $C$ is not necessarily hyperelliptic. Kodama-Top-Washio [11] studied the maximality of some specific hyperelliptic curves of genus 3. In this paper, we study the maximality of hyperelliptic Howe curves of genus 3. A Howe curve is the desingularization of the fiber product over $\mathbb{P}^1$ of two elliptic curves. See Section 2, for the precise definition of Howe curves. Such curves were studied in genus 4 by Howe [6] to construct quickly curves having many rational points, and were called Howe curves in Kudo-Harashita-Senda [12]. Before this, Oort constructed a hyperelliptic superspecial curve of genus 3 by using a Howe curve in [14].

We see a hyperelliptic Howe curve $C$ of genus 3 is written as $y^2 = (x^4 - ax^2 + 1)(x^4 - bx^2 + 1)$ in Section 3, and we call it the standard form of $C$. Our main result is as below:

**Theorem 1.1.** Assume that $C : y^2 = (x^4 - ax^2 + 1)(x^4 - bx^2 + 1)$ is nonsingular and superspecial. Then $a$ and $b$ belong to $\mathbb{F}_{p^2}$. Moreover, the followings are true:

- If $p \equiv 3 \pmod{4}$, then $C$ is maximal over $\mathbb{F}_{p^2}$.
- If $p \equiv 1 \pmod{4}$, then $C$ is minimal over $\mathbb{F}_{p^2}$.

See Corollary 4.4, for the maximality of the curve of the form $\varepsilon y^2 = (x^4 - ax^2 + 1)(x^4 - bx^2 + 1)$. 


The remainder of this paper is structured as follows. In Section 2, we review the definition of Howe curves. Proposition 2.4 gives the new condition that Howe curves of genus 3 are hyperelliptic. In Section 3, we look into the structures of a hyperelliptic Howe curve $C$ of genus 3. In particular, we describe explicitly the elliptic curves appearing as quotients of $C$ by involutions. In Section 4, we prove Theorem 1.1. See Example 4.3, for the number of superspecial hyperelliptic Howe curves in small characteristic.

Acknowledgments
This paper was written while the author is a Ph.D. student at Yokohama National University, and I would like to express my special thanks to my supervisor Prof. Shushi Harashita for his guidance. The author thank Toshiyuki Katsura and Tomoyoshi Ibukiyama for their helpful comments.

2 Howe curve of genus 3

In this section, we recall the definition of a Howe curve $C$ of genus 3 and find conditions that $C$ is hyperelliptic. Let $K$ be a perfect field of characteristic $p \geq 3$. Consider two elliptic curves
\[ E_1 : y^2 = x(x - 1)(x - \lambda_1), \]
\[ E_2 : y^2 = x(x - \mu)(x - \mu \lambda_2) \]
where $\lambda_1, \lambda_2$ and $\mu$ are not 0 nor 1. This condition is a condition for $E_1$ and $E_2$ to be nonsingular. Let $f_i : E_i \to \mathbb{P}^1$ be the usual double cover for $i \in \{1, 2\}$. Here $f_1$ is ramified over $S_1 = \{0, 1, \lambda_1, \infty\}$ and $f_2$ is ramified over $S_2 = \{0, \mu, \mu \lambda_2, \infty\}$. The fiber product $E_1 \times_{\mathbb{P}^1} E_2$ is irreducible if and only if $|S_1 \cap S_2| \leq 3$, and then the desingularization $C$ of the fiber product $E_1 \times_{\mathbb{P}^1} E_2$ is called a Howe curve, see [10, Section 4]. It is known [9, Proposition 6.1] that the genus of a Howe curve $C$ is equal to $5 - |S_1 \cap S_2|$. More precisely, we obtain the followings:

- If $\mu = \lambda_1$ and $\mu \lambda_2 = 1$, then $C$ is not irreducible since $|S_1 \cap S_2| = 4$.
- Else if $\mu \lambda_2 = 1, \lambda_1$ or $\lambda_1 \lambda_2$, then $C$ is a genus-2 curve since $|S_1 \cap S_2| = 3$.
- Otherwise (i.e. 1, $\lambda_1, \mu$ and $\mu \lambda_2$ are all different), then $C$ is a genus-3 curve since $|S_1 \cap S_2| = 2$.

We are interested in genus-3 curves, so we make the assumption that 1, $\lambda_1, \mu$ and $\mu \lambda_2$ are all different from now on. Remark that nonhyperelliptic Howe curves of genus 3 are called Ciani curves (cf. [4]).

Then, we have the following diagram

\[ \begin{array}{ccc}
C & \xrightarrow{f_1} & E_1 \\
\downarrow & & \downarrow \uparrow \\
E_3 & \xleftarrow{f_2} & E_2
\end{array} \]

where $E_3$ is defined by
\[ E_3 : y^2 = (x - 1)(x - \lambda_1)(x - \mu)(x - \mu \lambda_2). \]

The diagram (2.1) induces an isogeny $\text{Jac}(C) \to E_1 \times E_2 \times E_3$ by [8, Section 3] of degree $2^3$, thus we have $\text{Jac}(C)[p] \cong (E_1 \times E_2 \times E_3)[p]$ since the degree of the isogeny is coprime to $p$. Hence $C$ is superspecial if and only if $E_i$ are all supersingular. Let us transform $E_3$ into the Legendre form:
Lemma 2.1. The elliptic curve $E_3 : y^2 = (x - 1)(x - \lambda_1)(x - \mu)(x - \mu\lambda_2)$ is isomorphic to

$$y^2 = x(x - 1)(x - \lambda_3), \quad \lambda_3 = \frac{(\mu\lambda_2 - 1)(\mu - \lambda_1)}{\mu\lambda_2 - \lambda_1}(\mu - 1). \quad (2.2)$$

Note that $\lambda_3 \notin \{0, 1, \infty\}$ is just the condition that $\lambda_1, \lambda_2$ and $\mu$ are not 0 nor 1.

Proof. The change of variables

$$X = \frac{x - 1}{x - \lambda_1}, \quad Y = \frac{(\lambda_1 - 1)(\mu - \lambda_1)}{(\mu - 1)} \cdot \frac{y}{(x - \lambda_1)^2}$$

gives an equation

$$\frac{\mu\lambda_2 - \lambda_1}{\mu - 1} \cdot Y^2 = X(X - 1)(X - \lambda_3).$$

This is isomorphic to the elliptic curve in the Legendre form $y^2 = x(x - 1)(x - \lambda_3)$ clearly. □

We have seen how the Legendre forms $y^2 = x(x - 1)(x - \lambda_i)$ of $E_1, E_2$ and $E_3$ are obtained from the Howe curve associated to $\lambda_1, \lambda_2$ and $\mu$. Conversely we can find $\mu$ from $\lambda_1, \lambda_2$ and $\lambda_3$. Recall the definition of $\lambda_3$ in (2.2), then we obtain

$$(\mu\lambda_2 - 1)(\mu - \lambda_1) = \lambda_3(\mu\lambda_2 - \lambda_1)(\mu - 1)$$

and this equation can be rearranged as

$$\mu^2\lambda_2(1 - \lambda_3) - \mu(\lambda_1\lambda_2 - \lambda_2\lambda_3 - \lambda_3\lambda_1 + 1) + \lambda_1(1 - \lambda_3) = 0. \quad (2.3)$$

Solving this quadratic equation for $\mu$, we get

$$\mu = \frac{(\lambda_1\lambda_2 - \lambda_2\lambda_3 - \lambda_3\lambda_1 + 1) \pm \sqrt{D}}{2\lambda_2(1 - \lambda_3)}$$

with $D = (\lambda_1\lambda_2 - \lambda_2\lambda_3 - \lambda_3\lambda_1 + 1)^2 - 4\lambda_1\lambda_2(1 - \lambda_3)^2$.

Proposition 2.2. A Howe curve $C$ is hyperelliptic if and only if $\mu^2\lambda_2 = \lambda_1$.

Proof. See [14, Section 5.11]. □

Here is a paraphrase of the criterion in terms of the discriminant $D$.

Proposition 2.3. A Howe curve $C$ is hyperelliptic if and only if $D = 0$.

Proof. Suppose that $D = 0$, then it follows from $(\lambda_1\lambda_2 - \lambda_2\lambda_3 - \lambda_3\lambda_1 + 1)^2 = 4\lambda_1\lambda_2(1 - \lambda_3)^2$ that

$$\mu^2\lambda_2 = \frac{(\lambda_1\lambda_2 - \lambda_2\lambda_3 - \lambda_3\lambda_1 + 1)^2}{4\lambda_2(1 - \lambda_3)^2} = \frac{4\lambda_1\lambda_2(1 - \lambda_3)^2}{4\lambda_2(1 - \lambda_3)^2} = \lambda_1.$$ 

Therefore $C$ is hyperelliptic by Proposition 2.3. On the other hand, suppose that $C$ is hyperelliptic. By substituting $\mu^2\lambda_2 = \lambda_1$ for (2.3), we have

$$\mu(\lambda_1\lambda_2 - \lambda_2\lambda_3 - \lambda_3\lambda_1 + 1) = 2\lambda_1(1 - \lambda_3).$$

Square both sides and multiplying both sides by $\lambda_2$, then we have

$$\mu^2\lambda_2(\lambda_1\lambda_2 - \lambda_2\lambda_3 - \lambda_3\lambda_1 + 1)^2 = 4\lambda_1^2\lambda_2(1 - \lambda_3)^2.$$

Substituting $\mu^2\lambda_2 = \lambda_1$ again yields $(\lambda_1\lambda_2 - \lambda_2\lambda_3 - \lambda_3\lambda_1 + 1)^2 = 4\lambda_1\lambda_2(1 - \lambda_3)^2$. This means $D = 0$, thus the proposition is true. □
In the hyperelliptic case, only at most two values of $\lambda_3$ are possible for given $\lambda_1$ and $\lambda_2$ by using Proposition 2.3. The equation $D = 0$ can be rearranged into

$$(\lambda_1 - \lambda_2)^2 \lambda_3^2 - 2\lambda_3 + (\lambda_1^2 - 1)^2 = 0,$$

and we can solve this equation as follows:

$$\lambda_3 = \begin{cases} \frac{\sqrt{\lambda_1(\lambda_2 - 1)} \pm \sqrt{\lambda_2(\lambda_1 - 1)}}{(\lambda_1 - \lambda_2)^2} & (\lambda_1 \neq \lambda_2), \\ \frac{(\lambda_1 + 1)^2}{4\lambda_1} & (\lambda_1 = \lambda_2). \end{cases} \quad (2.4)$$

This result will be used in Section 4.

**Example 2.4.** Consider the case that $\lambda_1 = \lambda_2$. Put $\lambda := \lambda_1 = \lambda_2$ and $\mu = -1$, that is,

$$E_1 : y^2 = x(x - 1)(x - \lambda),$$

$$E_2 : y^2 = x(x + 1)(x + \lambda),$$

$$E_3 : y^2 = (x^2 - 1)(x^2 - \lambda^2).$$

Then, the Howe curve $C$ is hyperelliptic by using Proposition 2.2. Moreover, the elliptic curve $E_3$ is isogenous to $Y^2 = X(X - 1)(X - \lambda^2)$, and thus $C$ is superspecial if and only if $H_p(\lambda) = H_p(\lambda^2) = 0$ where we define

$$H_p(t) := \frac{(p-1)/2}{\sum_{i=0}^{(p-1)/2} \left(\frac{p-1}{2}\right)^i} t^i.$$

### 3 Hyperelliptic Howe curve of genus 3

Let $K$ be a perfect field of characteristic $p \geq 3$. In this section, we consider the desingularization $C$ of a hyperelliptic curve of genus 3

$$y^2 = x^8 + Mx^6 + Nx^4 + Mx^2 + 1 \quad (3.1)$$

at the infinity point with $M, N \in K$. We shall show that the curve $C$ is a hyperelliptic Howe curve of genus 3 if it is nonsingular and that any hyperelliptic Howe curve of genus 3 is realized as a curve of the form (3.1). Firstly, we study the nonsingularity of the curve $C$. Factorizing the right-hand side of (3.1), we get

$$y^2 = (x^4 - ax^2 + 1)(x^4 - bx^2 + 1) \quad (3.2)$$

where $a + b = -M$ and $ab = N - 2$ holds.

**Lemma 3.1.** The curve $C$ is nonsingular if and only if $a, b \neq \pm 2$ and $a - b \neq 0$.

*Proof.* Recall that a hyperelliptic curve $y^2 = f(x)$ is nonsingular except at the infinity point if and only if $f(x)$ does not have any multiple root, so it suffices to show that $(x^4 - ax^2 + 1)(x^4 - bx^2 + 1)$ has a multiple root if and only if $a, b = \pm 2$ or $a - b = 0$.

Here, the polynomials $x^4 - ax^2 + 1$ and $x^4 - bx^2 + 1$ has a common root if and only if $a - b = 0$. Moreover, one can confirm that the polynomial $x^4 - ax^2 + 1$ (resp. $x^4 - bx^2 + 1$) has a multiple root if and only if $a = \pm 2$ (resp. $b = \pm 2$). The proof is completed. \qed
Remark 3.2. The curve $C$ is nonsingular if and only if
\[ 2M + N + 2 \neq 0, \quad -2M + N + 2 \neq 0, \quad M^2 - 4N + 8 \neq 0. \]

Indeed, by using $M = -(a + b)$ and $N = ab + 2$, then we can compute $2M + N + 2 = (a + 2)(b + 2)$, $-2M + N + 2 = (a - 2)(b - 2)$ and $M^2 - 4N + 8 = (a - b)^2$ directly.

Next, let $\sigma_1, \sigma_2, \sigma_3$ be automorphisms be a nonsingular curve $C$ as below:
\[ \sigma_1 : (x, y) \mapsto (1/x, y/x^4), \quad \sigma_2 : (x, y) \mapsto (-1/x, y/x^4), \quad \sigma_3 : (x, y) \mapsto (-x, y). \]

Put $E_i := C/\langle \sigma_i \rangle$ for $i \in \{1, 2, 3\}$, then we obtain the equations of genus-1 curves
\[
\begin{align*}
E_1 : v^2 &= (u^2 - a - 2)(u^2 - b - 2), \quad u = x + 1/x, \quad v = y/x^2, \\
E_2 : v^2 &= (u^2 - a + 2)(u^2 - b + 2), \quad u = x - 1/x, \quad v = y/x^2, \\
E_3 : v^2 &= (u^2 - au + 1)(u^2 - bu + 1), \quad u = x^2, \quad v = y
\end{align*}
\]

and we can regard the curve
\[ P : v^2 = (u - a)(u - b), \quad u = x^2 + 1/x^2, \quad v = y/x^2 \]
as the quotient $C/\langle \sigma_1, \sigma_2 \rangle$. The genus of $P$ is 0, and thus the curve $P$ is isomorphic to the projective line $\mathbb{P}^1$. For the above discussion, we obtain the following diagram:

This means that $C$ is a Howe curve of genus 3 as studied in Section 2. Conversely, any hyperelliptic Howe curve of genus 3 is written as (3.2) by [2, Section 5]. We choose $\alpha_+, \alpha_-, \beta_+$ and $\beta_-$ such that
\begin{equation}
(\alpha_+)^2 = a + 2, \quad (\alpha_-)^2 = a - 2, \quad (\beta_+)^2 = b + 2, \quad (\beta_-)^2 = b - 2. \tag{3.3}
\end{equation}

Lemma 3.3. We can transform $E_i$ into the Legendre forms $y^2 = x(x - 1)(x - \lambda_i)$ with
\[
\begin{align*}
\lambda_1 &= \left(\frac{\alpha_+ + \beta_+}{\alpha_+ - \beta_-}\right)^2, \\
\lambda_2 &= \left(\frac{\alpha_- - \beta_-}{\alpha_- + \beta_+}\right)^2, \\
\lambda_3 &= \left(\frac{\alpha_+ \beta_- - \alpha_- \beta_+}{\alpha_+ \beta_- + \alpha_- \beta_+}\right)^2. \tag{3.4}
\end{align*}
\]

Proof. Factorizing the right hand side of the equation of $E_1$, we have
\[ E_1 : v^2 = (u + \alpha_+)(u - \alpha_+)(u + \beta_+)(u - \beta_+). \]
The map

\[ u \mapsto \frac{u - \alpha_+}{u + \alpha_+} \cdot \frac{\beta_+ + \alpha_+}{\beta_+ - \alpha_+} \]

transforms \( E_1 \) into the Legendre form:

\[ v^2 = u(u-1) \left( u - \frac{(\beta_+ + \alpha_+)^2}{(\beta_+ - \alpha_+)^2} \right) = u(u-1)(u - \lambda_1). \]

Therefore, we obtain the equation of \( \lambda_1 \) in (3.4). This equality can be simplified as

\[ \sqrt{\lambda_1} \text{transforms } E_1 \text{ into the Legendre form:} \]

\[ v^2 = u(u-1) \left( u - \frac{(\beta_+ + \alpha_+)^2}{(\beta_+ - \alpha_+)^2} \right) = u(u-1)(u - \lambda_1). \]

Secondly, we factorize the right-hand side of the equation of \( \lambda_1 \) into the Legendre form:

\[ E_3 : v^2 = (u - \gamma_1)(u - \gamma_2)(u - \gamma_3)(u - \gamma_4) \]

where

\[ \gamma_1 = \frac{a + \alpha_+ \alpha_-}{2}, \quad \gamma_2 = \frac{a - \alpha_+ \alpha_-}{2}, \quad \gamma_3 = \frac{b + \beta_+ \beta_-}{2}, \quad \gamma_4 = \frac{b - \beta_+ \beta_-}{2}. \]

The map

\[ u \mapsto \frac{u - \gamma_1}{u - \gamma_2} \cdot \frac{\gamma_3 - \gamma_2}{\gamma_3 - \gamma_1} \]

transforms \( E_3 \) into the Legendre form:

\[ v^2 = u(u-1) \left( u - \frac{(\gamma_4 - \gamma_2)(\gamma_3 - \gamma_1)}{(\gamma_4 - \gamma_1)(\gamma_3 - \gamma_2)} \right) = u(u-1) \left( u - \frac{\gamma_1 \gamma_4 + \gamma_2 \gamma_3 - \gamma_1 \gamma_2 - \gamma_3 \gamma_4}{\gamma_1 \gamma_3 + \gamma_2 \gamma_4 - \gamma_1 \gamma_2 - \gamma_3 \gamma_4} \right) \quad (3.5) \]

Here, we obtain

\[ ab = (\gamma_1 + \gamma_2)(\gamma_3 + \gamma_4) = \gamma_1 \gamma_3 + \gamma_1 \gamma_4 + \gamma_2 \gamma_3 + \gamma_2 \gamma_4, \]

\[ \alpha_+ \alpha_- \beta_+ \beta_- = (\gamma_1 - \gamma_2)(\gamma_3 - \gamma_4) = \gamma_1 \gamma_3 - \gamma_1 \gamma_4 - \gamma_2 \gamma_3 + \gamma_2 \gamma_4. \]

By adding or subtracting these equalities, we have

\[ \gamma_1 \gamma_3 + \gamma_2 \gamma_4 = \frac{ab + \alpha_+ \alpha_- \beta_+ \beta_-}{2}, \quad \gamma_1 \gamma_4 + \gamma_2 \gamma_3 = \frac{ab - \alpha_+ \alpha_- \beta_+ \beta_-}{2}. \quad (3.6) \]

Substituting (3.6) and \( \gamma_1 \gamma_2 = \gamma_3 \gamma_4 = 1 \) for (3.5), we obtain the equation of \( \lambda_3 \) in (3.4).

As square roots of \( \lambda_1 \) and \( \lambda_2 \), we choose

\[ \sqrt{\lambda_1} := \frac{\alpha_+ + \beta_+}{\alpha_+ - \beta_+}, \quad \sqrt{\lambda_2} := \frac{\alpha_- - \beta_-}{\alpha_- + \beta_-} \quad (3.7) \]

and set \( \sqrt{\lambda_1 \lambda_2} := \sqrt{\lambda_1} \sqrt{\lambda_2} \) and \( \sqrt{\lambda_1 / \lambda_2} := \sqrt{\lambda_1} \sqrt{\lambda_2} \).

**Remark 3.4.** Remark that \( \sqrt{\lambda_1} - \sqrt{\lambda_2} \neq 0 \) and \( \sqrt{\lambda_1 / \lambda_2} - 1 \neq 0 \) by assumption of \( a - b \neq 0 \). Indeed, suppose that \( \sqrt{\lambda_1} - \sqrt{\lambda_2} = 0 \), then we obtain

\[ (\alpha_+ + \beta_+)(\alpha_- + \beta_-) = (\alpha_- + \beta_+)(\alpha_- - \beta_-) \]

by (3.7). This equality can be simplified as \( \alpha_+ \beta_- = -\alpha_- \beta_+ \). Squaring both sides, we have \( a = b \). Hence, we obtain \( \sqrt{\lambda_1} - \sqrt{\lambda_2} \neq 0 \). We can prove \( \sqrt{\lambda_1 \lambda_2} - 1 \neq 0 \) in a similar way.
Proposition 3.5. The reverse transformation of that in Lemma 3.3 is given by
\[
a = \frac{2(\sqrt{\lambda_1} + \sqrt{\lambda_2} + 4\sqrt{\lambda_1\lambda_2} + \sqrt{\lambda_1} + \sqrt{\lambda_2})}{(\sqrt{\lambda_1} - \sqrt{\lambda_2})(\sqrt{\lambda_1\lambda_2} - 1)},
\]
\[
b = \frac{2(\sqrt{\lambda_1} - \sqrt{\lambda_2} - 4\sqrt{\lambda_1\lambda_2} + \sqrt{\lambda_1} + \sqrt{\lambda_2})}{(\sqrt{\lambda_1} - \sqrt{\lambda_2})(\sqrt{\lambda_1\lambda_2} - 1)}.
\]

Proof. By (3.7), we have
\[
\sqrt{\lambda_1\lambda_2} = \frac{(\alpha_+ + \beta_+)(\alpha_- - \beta_-)}{\alpha_- - \beta_+}(\alpha_- + \beta_-);
\]
\[
\sqrt{\lambda_1/\lambda_2} = \frac{(\alpha_+ + \beta_+)(\alpha_- + \beta_-)}{\alpha_- - \beta_+}(\alpha_- - \beta_-).
\]

A tedious computation shows
\[
\sqrt{\lambda_1\lambda_2} + 1, \sqrt{\lambda_1/\lambda_2} + 1 = \frac{\alpha_+ \alpha_- - \beta_+ \beta_-}{\alpha_- \beta_+ - \alpha_+ \beta_-},
\]
\[
\sqrt{\lambda_1\lambda_2} - 1, \sqrt{\lambda_1/\lambda_2} - 1 = \frac{\alpha_+ \alpha_- + \beta_+ \beta_-}{\alpha_- \beta_+ + \alpha_+ \beta_-}.
\]

Hence, we have
\[
\frac{\sqrt{\lambda_1\lambda_2} + 1}{\sqrt{\lambda_1\lambda_2} - 1}, \frac{\sqrt{\lambda_1/\lambda_2} + 1}{\sqrt{\lambda_1/\lambda_2} - 1} = \frac{(a^2 - 4) - (b^2 - 4)}{(a - 2)(b + 2) - (a + 2)(b - 2)} = \frac{(a + b)(a - b)}{4(a - b)}.
\]

By assumption of \(a - b \neq 0\), thus we obtain
\[
a + b = 4 \cdot \frac{\sqrt{\lambda_1 + \sqrt{\lambda_2}}(\sqrt{\lambda_1\lambda_2} + 1)}{(\sqrt{\lambda_1} + \lambda_2)(\sqrt{\lambda_1\lambda_2} - 1)} \quad (3.8)
\]

On the other hand, we can compute
\[
\sqrt{\lambda_1} - \sqrt{\lambda_2} = \frac{2(\alpha_- \beta_+ + \alpha_+ \beta_-)}{(\alpha_+ - \beta_+)(\alpha_- + \beta_-)},
\]
\[
\sqrt{\lambda_1/\lambda_2} - 1 = \frac{2(\alpha_- \beta_+ + \alpha_+ \beta_-)}{(\alpha_+ - \beta_+)(\alpha_- + \beta_-)} \quad (3.9)
\]

and one can check that
\[
a - b = 16 \cdot \frac{\sqrt{\lambda_1\lambda_2}}{(\sqrt{\lambda_1} - \sqrt{\lambda_2})(\sqrt{\lambda_1\lambda_2} - 1)}.
\]

The proposition follows from (3.8) and (3.10).

Remark 3.6. By using Lemma 3.3 and (3.9), we obtain
\[
\lambda_3 = \left(\frac{\sqrt{\lambda_1\lambda_2} - 1}{\sqrt{\lambda_1} - \sqrt{\lambda_2}}\right)^2.
\]

One can see that this equation coincides with (2.4).
4 Proof of the main theorem

In this section, we will show the theorem stated in Introduction.

**Theorem 1.1.** Assume that $C : y^2 = (x^4 - ax^2 + 1)(x^4 - bx^2 + 1)$ is nonsingular and superspecial. Then $a$ and $b$ belong to $\mathbb{F}_{p^2}$. Moreover, the followings are true:

- If $p \equiv 3 \pmod{4}$, then $C$ is maximal over $\mathbb{F}_{p^2}$.
- If $p \equiv 1 \pmod{4}$, then $C$ is minimal over $\mathbb{F}_{p^2}$.

In particular, the curve $C$ is maximal or minimal over $\mathbb{F}_{p^2}$.

A key to the proof is the following result by Auer and Top [1, Proposition 2.2].

**Proposition 4.1.** Let $E : y^2 = x(x - 1)(x - \lambda)$ be a supersingular elliptic curve, then $\lambda$ is a 4th power in $(\mathbb{F}_{p^2})^\times$. Moreover, the followings are true:

- If $p \equiv 3 \pmod{4}$, then an elliptic curve $E$ is maximal over $\mathbb{F}_{p^2}$.
- If $p \equiv 1 \pmod{4}$, then an elliptic curve $E$ is minimal over $\mathbb{F}_{p^2}$.

In particular, the elliptic curve $E$ is maximal or minimal over $\mathbb{F}_{p^2}$.

Recall the discussions in Section 3. Let $E_1, E_2$ and $E_3$ be the following three elliptic curves:

$$
E_1 : v^2 = (u^2 - a - 2)(u^2 - b - 2),
E_2 : v^2 = (u^2 - a + 2)(u^2 - b + 2),
E_3 : v^2 = (u^2 - au + 1)(u^2 - bu + 1).
$$

Then, there exist morphisms $C \to E_i$ of degree 2. The morphisms are defined over $\mathbb{F}_{p^2}$, since so are the involutions defining these quotient.

**Proof of the first half of Theorem 1.1.** The elliptic curves $E_i$ are supersingular by the assumption since the quotient of supersingular curve is supersingular. By Lemma 3.3, each elliptic curve $E_i$ is isomorphic to $y^2 = x(x - 1)(x - \lambda_i)$. By Proposition 4.1, we obtain $\lambda_i$ is a 4th power in $(\mathbb{F}_{p^2})^\times$ and thus $\sqrt[4]{\lambda_i} \in \mathbb{F}_{p^2}$. Hence, it follows from Proposition 3.4 that $a, b \in \mathbb{F}_{p^2}$. \qed

We have shown that $C$ is defined over $\mathbb{F}_{p^2}$. Next, let us discuss whether $C$ is maximal or minimal over $\mathbb{F}_{p^2}$. Here, we prepare the following lemma:

**Lemma 4.2.** If $C$ is superspecial, then $\alpha_+, \alpha_-, \beta_+$ and $\beta_-$ in (3.3) are elements of $\mathbb{F}_{p^2}$.

**Proof.** The elliptic curve $E_i$ is supersingular by the assumption, thus $\lambda_1, \lambda_2$ and $\lambda_3$ in (3.4) are 4th powers in $(\mathbb{F}_{p^2})^\times$ by Proposition 4.1. Here, one can compute that

$$
a - 2 = \frac{4\sqrt[4]{\lambda_1}(\sqrt[4]{\lambda_2} + 1)^2}{(\sqrt[4]{\lambda_1} - \sqrt[4]{\lambda_2})(\sqrt[4]{\lambda_1\lambda_2} - 1)}, \quad a + 2 = \frac{4\sqrt[4]{\lambda_2}(\sqrt[4]{\lambda_1} + 1)^2}{(\sqrt[4]{\lambda_1} - \sqrt[4]{\lambda_2})(\sqrt[4]{\lambda_1\lambda_2} - 1)},
$$

$$
b - 2 = \frac{4\sqrt[4]{\lambda_1}(\sqrt[4]{\lambda_2} - 1)^2}{(\sqrt[4]{\lambda_1} - \sqrt[4]{\lambda_2})(\sqrt[4]{\lambda_1\lambda_2} - 1)}, \quad b + 2 = \frac{4\sqrt[4]{\lambda_2}(\sqrt[4]{\lambda_1} - 1)^2}{(\sqrt[4]{\lambda_1} - \sqrt[4]{\lambda_2})(\sqrt[4]{\lambda_1\lambda_2} - 1)}
$$

by using Proposition 3.4, and so it suffices to show that $(\sqrt[4]{\lambda_1} - \sqrt[4]{\lambda_2})(\sqrt[4]{\lambda_1\lambda_2} - 1)$ is a square in $\mathbb{F}_{p^2}$.
It follows from Remark 3.6 that
\[ \sqrt[3]{\lambda_3} = \frac{\sqrt[2]{\lambda_1\lambda_2} - 1}{\sqrt[2]{\lambda_1} - \sqrt[2]{\lambda_2}} \]
is a square in \( \mathbb{F}_{p^2} \), and thus whether \( \sqrt[2]{\lambda_1} - \sqrt[2]{\lambda_2} \) is a square in \( \mathbb{F}_{p^2} \) is in accord with whether \( \sqrt[2]{\lambda_1\lambda_2} - 1 \) is a square in \( \mathbb{F}_{p^2} \). This means that a product \((\sqrt[2]{\lambda_1} - \sqrt[2]{\lambda_2})(\sqrt[2]{\lambda_1\lambda_2} - 1)\) is a square in \( \mathbb{F}_{p^2} \).

**Proof of the second half of Theorem 1.1.** In the proof of Lemma 3.3, we defined isomorphisms from the elliptic curve \( E_i \) to its Legendre form \( y^2 = x(x-1)(x-\lambda_i) \) by using \( \alpha_+, \alpha_- \), \( \beta_+ \) and \( \beta_- \). Hence, these isomorphisms are defined over \( \mathbb{F}_{p^2} \) by Lemma 4.2. Therefore \( C \) is maximal (resp. minimal) if and only if all \( y^2 = x(x-1)(x-\lambda_i) \) are maximal (resp. minimal). Suppose that \( C \) is superspecial, and the elliptic curves \( E_1, E_2 \) and \( E_3 \) are all superspecial.

- If \( p \equiv 3 \pmod{4} \), then the elliptic curve \( y^2 = x(x-1)(x-\lambda_i) \) is maximal by Proposition 4.1. Hence \( C \) is maximal over \( \mathbb{F}_{p^2} \).
- If \( p \equiv 1 \pmod{4} \), then the elliptic curve \( y^2 = x(x-1)(x-\lambda_i) \) is minimal by Proposition 4.1. Hence \( C \) is minimal over \( \mathbb{F}_{p^2} \).

Therefore, the proof of Theorem 1.1 is completed.

Finally, we give examples of superspecial hyperelliptic Howe curves.

**Example 4.3.** The automorphism group \( G \) of a hyperelliptic Howe curve of genus 3 in characteristic \( p > 7 \) is either \( C_2 \times C_2 \times C_2 \), \( C_2 \times D_8 \), \( V_8 \) or \( C_2 \times S_4 \), see [13, Section 3.1]:

(i) If \( G \cong C_2 \times C_2 \times C_2 \), then \( C \) is isomorphic to \( y^2 = (x^4 - ax^2 + 1)(x^4 - bx^2 + 1) \) with \( a + b \neq 0 \);
(ii) If \( G \cong C_2 \times D_8 \), then \( C \) is isomorphic to \( y^2 = x^8 - ax^4 + 1 \) with \( a \neq 0, \pm 14 \);
(iii) If \( G \cong V_8 \), then \( C \) is isomorphic to \( y^2 = x^8 - 1 \);
(iv) If \( G \cong C_2 \times S_4 \), then \( C \) is isomorphic to \( y^2 = x^8 \pm 14x^4 + 1 \).

If \( C \) is superspecial, then \( C \) is maximal or minimal in every case. Indeed, apply Theorem 1.1, after we factorize the right hand side of the defining equation as the form of (i) over an algebraic closed field, where in the case (iii) we use \( y^2 = x^8 + 1 \) instead of \( y^2 = x^8 - 1 \). Remark that \( y^2 = x^8 - 1 \) is superspecial if and only if \( p \equiv 7 \pmod{8} \), in case \( y^2 = x^8 - 1 \) and \( y^2 = x^8 + 1 \) are isomorphic.

Here, for \( 7 < p < 100 \), the number of hyperelliptic superspecial Howe curves \( C \) of genus 3 with automorphism group is as follows if the number is positive (cf. [3, Theorem 3.15]):

| Aut(\( \mathbb{C} \)) | \( p = 17 \) | \( p = 23 \) | \( p = 31 \) | \( p = 41 \) | \( p = 47 \) | \( p = 71 \) | \( p = 73 \) | \( p = 79 \) | \( p = 89 \) | \( p = 97 \) |
|-----------------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| \( C_2 \times C_2 \times C_2 \) | 0 | 2 | 3 | 0 | 4 | 10 | 2 | 9 | 0 | 4 |
| \( C_2 \times D_8 \) | 1 | 0 | 1 | 1 | 2 | 0 | 3 | 1 | 1 | 1 |
| \( V_8 \) | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| \( C_2 \times S_4 \) | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |

We use Magma calculator to obtain the above table. We compute the Hasse-Witt matrix of the curve \( C : y^2 = (x^4 - ax^2 + 1)(x^4 - bx^2 + 1) \), and find \( a, b \in \mathbb{F}_{p^2} \) such that \( C \) is superspecial. Then, we decide whether these curves are isomorphic by using Shioda invariants (cf. [15]).
Lastly, let us discuss the maximality of twists of the curve $C$. Note that in general, a hyperelliptic curve $C: y^2 = f(x)$ is maximal (resp. minimal) over $\mathbb{F}_{p^{2e}}$ if and only if $C': \varepsilon y^2 = f(x)$ is minimal (resp. maximal) over $\mathbb{F}_{p^{2e}}$ for non-square $\varepsilon \in (\mathbb{F}_{p^{2e}})\times$.

**Corollary 4.4.** Assume that a hyperelliptic curve $C: y^2 = (x^4 - ax^2 + 1)(x^4 - bx^2 + 1)$ is superspecial. Let $\varepsilon \in (\mathbb{F}_{p^{2e}})\times$ and $C': \varepsilon y^2 = (x^4 - ax^2 + 1)(x^4 - bx^2 + 1)$.

1. When $e$ is odd, then the followings are true:
   - If $p \equiv 3 \pmod{4}$, then $C'$ is maximal over $\mathbb{F}_{p^{2e}}$ if and only if $\varepsilon$ is a square in $\mathbb{F}_{p^{2e}}$.
   - If $p \equiv 1 \pmod{4}$, then $C'$ is maximal over $\mathbb{F}_{p^{2e}}$ if and only if $\varepsilon$ is not a square in $\mathbb{F}_{p^{2e}}$.

2. When $e$ is even, then $C'$ is maximal over $\mathbb{F}_{p^{2e}}$ if and only if $\varepsilon$ is not a square in $\mathbb{F}_{p^{2e}}$.

**Proof.** Suppose that a curve $\Gamma$ over $\mathbb{F}_{p^{2}}$ is maximal (resp. minimal), then $\Gamma$ over $\mathbb{F}_{p^{2e}}$ is also maximal (resp. minimal) when $e$ is odd, and is minimal when $e$ is even. This follows from the Weil conjecture (cf. [5, Appendix C, Exercise 5.7]) and the fact that $\Gamma$ over $\mathbb{F}_{p^{2}}$ is maximal (resp. minimal) if and only if all the eigenvalues of the Frobenius on the first étale cohomology group are $-p$ (resp. $p$).

**References**

[1] R. Auer and J. Top: *Legendre elliptic curves over finite fields*, Journal of Number Theory 95, 303–312, 2002.

[2] I. Bouw, N. Coppola, P. Kilicer, S. Kunzweiler, E. L. García and A. Somoza: *Reduction type of genus-3 curves in a special stratum of their moduli space*, arXiv: 2003.07633, 2020.

[3] B. W. Brock: *Superspecial curves of genera two and three*, Thesis (Ph.D.)-Princeton University, 1993.

[4] E. Ciani: *I varii tipi possibili di quartiche piane più volte omologico-armoniche*, Rendiconti del Circolo Matematico di Palermo 13, 347–373, 1899.

[5] R. Hartshorne: *Algebraic Geometry*, GTM 52, Springer–Verlag, 1977.

[6] E. W. Howe: *Quickly constructing curves of genus 4 with many points*, Contemporary Mathematics 663, 149–173, 2016.

[7] T. Ibukiyama: *On rational points of curves of genus 3 over finite fields*, Tôhoku Mathematical Journal 45, 311–329, 1993.

[8] E. Kani and M. Rosen: *Idempotent relations and factors of Jacobians*, Mathematische Annalen 284, 307–327, 1989.

[9] T. Katsura: *Decomposed Richelot isogenies of Jacobian varieties of curves of genus 3*, Journal of Algebra 588, 129–147, 2021.

[10] T. Katsura and K. Takashima: *Decomposed Richelot isogenies of Jacobian varieties of hyperelliptic curves and generalized Howe curves*, arXiv:2108.06936, 2021.

[11] T. Kodama, J. Top and T. Washio: *Maximal hyperelliptic curves of genus three*, Finite Fields and Their Applications 15, 392–403, 2009.
[12] M. Kudo, S. Harashita and H. Senda: *The existence of supersingular curves of genus 4 in arbitrary characteristic*, Research in Number Theory *6*, Article number: 44, 2020.

[13] R. Lercier and C. Ritzenthaler: *Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects*, Journal of Algebra *372*, 595–636, 2012.

[14] F. Oort: *Hyperelliptic supersingular curves*, Progress in Mathematics *89*, 247–284, 1991.

[15] T. Shioda: *On the graded ring of invariants of binary octavics*, American Journal of Mathematics *89*, 1022–1046, 1967.