FIBRE PRODUCTS OF THREE HYPERELLIPTIC CURVES WITH MANY POINTS

MOTOKO QIU KAWAKITA

Abstract. We find that the Fricke–Macbeath curve attains the Hasse–Weil–Serre bound over some finite fields of order p or p^3 for a prime p, and the Howe curves of genus 7 attain the Hasse–Weil–Serre bound over some finite fields of order p^2 or p^3. We determine the precise condition on the finite field over which they attain the Hasse–Weil–Serre bound.

Next, we study curves constructed by the normalisation of the fibre product of three hyperelliptic curves. Among them, we focus on two types of curves of genera 9 and 11. In particular, under certain assumptions, we are able to decompose the Jacobian of one type of curves of genus 9 completely and to determine the precise condition on the finite field over which they are maximal. Also, we are able to update several entries of genera 9 and 11 in `manypoints.org`.

1. Introduction

Let p be a prime, k be a field of characteristic p and $\mathbb{F}_q$ be a finite field with q elements where q is a power of p. A curve C is a projective, absolutely irreducible, non-singular algebraic curve defined over k. A curve C over $\mathbb{F}_q$ is said to be *maximal* if the number of its rational points attains the Hasse–Weil upper bound

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

where g is the genus of C. In 1983, Serre provided a non-trivial improvement of the Hasse–Weil bound when q is not a square root in [28], namely

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

where $\lfloor \cdot \rfloor$ is the floor function. We refer to this bound as the *Serre bound*.

Curves attaining the Hasse–Weil or the Serre bound are interesting objects not only in their own right but also for their applications in coding theory. Indeed, Goppa described a way to use algebraic curves to construct linear error-correcting codes in [8], the so-called algebraic geometric codes; see [30]. The existence of curves with many rational points with respect to their genus guarantee efficient error-correcting codes. For this reason, maximal curves and curves attaining the Serre bound have been widely investigated in the last years, see for instance [4, 5, 7].

In 2003, we constructed curves by the fibre product of two Kummer curves, and find new curves with many points; see [17]. Curves with many points which are constructed by fibre products of Kummer curves are also studied in [9, 24, 25, 26]. In 2017, Howe constructed curves of genus 5, 6 and 7 by the fibre product of curves of genus 1 or 2 in [12], and found curves of genus 5, 6 and 7 with many points which updated the manypoints site [6]. Katsura and Takashima defined a generalised Howe curve in [16] by the fibre product of two hyperelliptic curves. In [20], we found generalised Howe curves of genus 5 attaining the Serre bound.

The paper are organised as follows. Section 2 and 3 are preparations. Section 2 provides a necessary and sufficient condition for certain elliptic curves to attain the Serre bound over

2020 *Mathematics Subject Classification.* Primary: 11G20, 14G05; Secondary: 14G50.

Key words and phrases. Rational points, Hasse–Weil–Serre bound, Fricke–Macbeath curves, Howe curves.

$\mathbb{F}_p$, $\mathbb{F}_{p^2}$ or $\mathbb{F}_{p^3}$. In Section 3, we decompose the Jacobian of a hyperelliptic curve of genus 2. In Section 4 we study on the Fricke–Macbeath curve and the Howe curves of genus 7 in [12]. We obtain not only non-maximal curves attaining the Serre bound but also maximal curves. These results inspired us to construct curves by the fibre product of three hyperelliptic curves in Section 5. We decompose their Jacobian to seven hyperelliptic curves by Kani and Rosen's theorem. Also we determine their genera exactly by their degrees. The idea comes from [12, 16, 17, 20]. Among them, we study on curves of genera 9 and 11. In Section 6, we study on two types of curves of genus 9. We decompose the Jacobian of one type of curves of genus 9 completely under certain assumptions and determine the precise condition on the finite field over which they are maximal. In Section 7, we search on two types of curves of genus 11. Furthermore, we discover new curves of genera 9 and 11 which are able to update the manypoints site [6].

2. Elliptic curves attaining the Serre bound

Let E be an elliptic curve with Weierstrass equation

$$E\colon y^2 = f(x),$$

where $f(x) \in \mathbb{F}_p[x]$ is a cubic polynomial with distinct roots. Set $m = (p-1)/2$ throughout this paper. Denote the coefficients of x^m in $f(x)^m$ by $\overline{A}$.

Theorem 2.1. (i) [18, Theorem 2] *Let $p \geq 17$. E attains the Serre bound over $\mathbb{F}_p$ if and only if*

$$\overline{A} \equiv -\lfloor 2\sqrt{p} \rfloor \mod p.$$

(ii) [29, Section V.4] *E is maximal over $\mathbb{F}_{p^2}$ if and only if*

$$\overline{A} \equiv 0 \mod p.$$

(iii) [18, Theorem 4] *For $\overline{A} \in \mathbb{F}_p$, set A as the integer such that $\overline{A} \equiv A \bmod p$ and $0 \leq A < p$. Let $p \geq 11$. E over $\mathbb{F}_{p^3}$ attains the Serre bound if and only if*

$$A^3 - 3pA = -\lfloor 2p\sqrt{p} \rfloor.$$

Next we introduce results of twisted Legendre elliptic curve. Let $\theta \in \mathbb{F}_p \backslash \{0\}$ and $\lambda \in \mathbb{F}_p \backslash \{0, 1\}$, and a twisted Legendre elliptic curve is defined by

$$E_\lambda^{(\theta)}\colon y^2 = \theta x(x-1)(x-\lambda).$$

Let $p \geq 3$. We define a polynomial

$$H_p(t) = \sum_{i=0}^{m} \binom{m}{i}^2 t^i$$

as in Chapter V.4, Theorem 4.1 of [29]. We recall the next theorem.

Theorem 2.2. [20, Theorem 6]

(i) *A curve $E_\lambda^{(\theta)}$ over $\mathbb{F}_{p^2}$ is maximal if and only if*

$$H_p(\lambda) \equiv 0 \mod p.$$

Further, if $E_\lambda^{(\theta)}$ over $\mathbb{F}_{p^2}$ is maximal then $p \equiv 3 \mod 4$.

(ii) *Let $p \geq 11$. Set h as the integer such that $h \equiv (-\theta)^m H_p(\lambda) \bmod p$ and $0 \leqq h < p$. Then a curve $E_\lambda^{(\theta)}$ over $\mathbb{F}_{p^3}$ attains the Serre bound if and only if*

$$h^3 - 3ph = -\lfloor 2p\sqrt{p} \rfloor.$$

Lemma 2.3. [20, Lemma 7] *The number of rational points of $E_\lambda^{(\theta)}$ over $\mathbb{F}_q$ satisfies*

$$\#E_\lambda^{(\theta)}(\mathbb{F}_q) \equiv 0 \mod 4.$$

3. The Jacobian decomposition of curves

First, we introduce the result of Kani and Rosen in [14].

Theorem 3.1. [14, Theorem B] *Let C be a curve over k and G a finite subgroup of the automorphism group $\mathrm{Aut}(C)$ such that $G = H_1 \cup \cdots \cup H_n$, where the H_i's are subgroups of G such that $H_i \cap H_j = \{1_G\}$ for $i \neq j$. Then we have the isogeny relation*:

$$J(C)^{n-1} \times J(C/G)^g \sim J(C/H_1)^{h_1} \times \cdots \times J(C/H_n)^{h_n}$$

where $g = |G|$ and $h_i = |H_i|$.

The next corollaries follow immediately, which we will use several times later.

Corollary 3.2. [27, Section 3] *Let C be a curve, $\sigma_1, \sigma_2 \in \mathrm{Aut}(C)$ where $\sigma_1 \neq \sigma_2$, $\sigma_1\sigma_2 = \sigma_2\sigma_1$, $|\sigma_1| = |\sigma_2| = 2$ Then we have the following isogeny relation*:

$$J(C) \times J(C/\langle\sigma_1, \sigma_2\rangle)^2 \sim J(C/\langle\sigma_1\rangle) \times J(C/\langle\sigma_2\rangle) \times J(C/\langle\sigma_1\sigma_2\rangle).$$

Corollary 3.3. *Let C be a curve, $\sigma_i \in \mathrm{Aut}(C)$ where $\sigma_i \neq \sigma_j$, $\sigma_i\sigma_j = \sigma_j\sigma_i$, $|\sigma_i| = |\sigma_i\sigma_j| = |\sigma_i\sigma_j\sigma_k| = 2$ for $1 \leq i, j, k \leq 3$ where i, j, k are all different. Then we have the following isogeny relation*:

$$\begin{aligned} J(C)^3 \times J(C/\langle\sigma_1, \sigma_2, \sigma_3\rangle)^4 \sim & J(C/\langle\sigma_1\rangle) \times J(C/\langle\sigma_2\rangle) \times J(C/\langle\sigma_3\rangle) \\ & \times J(C/\langle\sigma_2\sigma_3\rangle) \times J(C/\langle\sigma_3\sigma_1\rangle) \times J(C/\langle\sigma_1\sigma_2\rangle) \\ & \times J(C/\langle\sigma_1\sigma_2\sigma_3\rangle). \end{aligned}$$

Proof. Let $G = \langle\sigma_1, \sigma_2, \sigma_3\rangle$, $H_1 = \langle\sigma_1\rangle$, $H_2 = \langle\sigma_2\rangle$, $H_3 = \langle\sigma_3\rangle$, $H_4 = \langle\sigma_2\sigma_3\rangle$, $H_5 = \langle\sigma_3\sigma_1\rangle$, $H_6 = \langle\sigma_1\sigma_2\rangle$, $H_7 = \langle\sigma_1\sigma_2\sigma_3\rangle$. From Theorem 3.1, we have the next isogeny relation:

$$\begin{aligned} J(C)^{7-1} \times J(C/\langle\sigma_1, \sigma_2, \sigma_3\rangle)^8 \sim & J(C/\langle\sigma_1\rangle)^2 \times J(C/\langle\sigma_2\rangle)^2 \times J(C/\langle\sigma_3\rangle)^2 \\ & \times J(C/\langle\sigma_2\sigma_3\rangle)^2 \times J(C/\langle\sigma_3\sigma_1\rangle)^2 \times J(C/\langle\sigma_1\sigma_2\rangle)^2 \\ & \times J(C/\langle\sigma_1\sigma_2\sigma_3\rangle)^2. \end{aligned}$$

Hence, we can prove it. □

To completely decompose the Howe curves in Section 4 and the curves of type I of genus 9 in Section 6, we bring in the next theorem. The idea of the proof is similar to that of Theorem 3.5.

Theorem 3.4. *Let a curve of genus 2 be defined by*

$$D\colon y^2 = cx(x - b_1)(x - b_2)(x - b_3)(x - b_4)$$

with $c, b_i \in k\backslash\{0\}$, b_i for $1 \leq i \leq 4$ are all different and $b_2(b_1 - b_3) = b_4(b_1 - b_2)$. Assume that there exists a square root of $b_2(b_2 - b_3)$ in k^*.

Then the Jacobian of the curve D decomposes over k as

$$J(D) \sim E_+ \times E_-,$$

where we have the following defining equations:

$$s^2 = \frac{c\, b_1(b_1 - b_3)}{b_1 - b_2} t(t-1)\Big(t - \frac{(b_1 - b_2)\big(b_3 - 2b_2 \pm 2(b_2^2 - b_2b_3)^{1/2}\big)}{b_1(b_3 - b_1)}\Big)$$

for E_+ and E_- respectively.

Proof. D is isomorphic to $y^2 = cb_1x(x-1)(x-b_2/b_1)(x-b_3/b_1)(x-b_4/b_1)$. Set $\lambda = b_2/b_1$, $\mu = b_3/b_1$, $\nu = b_4/b_1$. We have that $\nu = \lambda(1-\mu)/(1-\lambda)$ is equivalent to $b_2(b_1-b_3) = b_4(b_1-b_2)$. Hence D is isomorphic to

$$y^2 = cb_1x(x-1)(x-\lambda)(x-\mu)\big(x - \frac{\lambda(1-\mu)}{1-\lambda}\big). \tag{1}$$

On Equation (1) the three maps

$$\sigma\colon (x,y) \mapsto \big(\frac{\lambda(x-\mu)}{x-\lambda}, \frac{\lambda^{3/2}(\lambda-\mu)^{3/2}}{(x-\lambda)^3}\big),$$

$\iota\colon (x,y) \mapsto (x,-y)$ and $\tau = \sigma\iota$ define three automorphisms of D.

Let E_+ and E_- be the quotient curves $D/\langle\sigma\rangle$ and $D/\langle\tau\rangle$ respectively. By setting

$$t = x + \frac{\lambda(x-\mu)}{x-\lambda}, \quad s = y\frac{x - (\lambda \mp (\lambda^2-\lambda\mu)^{1/2})}{(x-\lambda)^2},$$

we have the following defining equations for E_+ and E_-:

$$s^2 = cb_1(t-\mu)\big(t - \frac{1-\lambda\mu}{1-\lambda}\big)\big(t - 2(\lambda \mp (\lambda^2-\lambda\mu)^{1/2})\big),$$

which are birationally equivalent to

$$s^2 = \frac{cb_1(1-\mu)}{1-\lambda}t(t-1)\big(t - \frac{(1-\lambda)(\mu - 2\lambda \pm 2(\lambda^2-\lambda\mu)^{1/2})}{\mu-1}\big).$$

Hence, we have that $\mathrm{Jac}(D) \sim E_+ \times E_-$ by Corollary 3.2. □

We recall one more theorem here.

Theorem 3.5. [13, Theorem 2] *Let a hyperelliptic curve of genus 2 be defined by*

$$D\colon y^2 = c(x-b_1)(x-b_2)(x-b_3)(x-b_4)(x-b_5)(x-b_6)$$

with $c \in k\backslash\{0\}$, $b_i \in k$, b_i for $1 \le i \le 6$ are all different and

$$(b_2-b_4)(b_1-b_6)(b_3-b_5) = (b_2-b_6)(b_1-b_5)(b_3-b_4).$$

Set $\theta = c\cdot(b_2-b_3)(b_1-b_4)(b_1-b_5)(b_1-b_6)$,

$$\lambda = \frac{(b_1-b_3)(b_2-b_4)}{(b_2-b_3)(b_1-b_4)}, \quad \mu = \frac{(b_1-b_3)(b_2-b_5)}{(b_2-b_3)(b_1-b_5)}.$$

Assume that there exists a square root of $\lambda(\lambda-\mu)$ in k^*.

Then the Jacobian of the curve D decomposes over k as

$$J(D) \sim E_+ \times E_-,$$

where we have the following defining equations:

$$s^2 = \frac{\theta(1-\mu)}{1-\lambda}t(t-1)\Big(t - \frac{(1-\lambda)\big(\mu - 2\lambda \pm 2(\lambda^2-\lambda\mu)^{1/2}\big)}{\mu-1}\Big)$$

for E_+ and E_- respectively.

4. Curves of genus 7 attaining the Serre bound

The Fricke–Macbeath curve $\mathcal{F}$ in [23] is a smooth projective curve of genus 7 with automorphism group $\mathrm{PSL}_2(\mathbb{F}_8)$. A plane model by Brock in [10] is

$$\mathcal{F}\colon 1 + 7xy + 21x^2y^2 + 35x^3y^3 + 28x^4y^4 + 2x^7 + 2y^7 = 0.$$

It is isomorphic to the normalisation of the fibre product of three elliptic curves; see [1, 10, 12, 23] for the detail and its interesting property.

Top and Verschoor [31] determine its Jacobian decomposition and count its number of rational points over a finite field $\mathbb{F}_q$ as Theorem 4.1. They also updated the manypoints site [6]. The maximal Fricke–Macbeath curves are studied in [1].

Theorem 4.1 (Theorem 2.6 [31])**.** *The Fricke–Macbeath curve $\mathcal{F}$ has good reduction modulo every prime number $p \neq 2, 7$. Let the elliptic curve E defined by $y^2 = x^3 + x^2 - 114x - 127$. If $q = p^n$ is a positive power of such a prime p, then $\#\mathcal{F}(\mathbb{F}_q) = \#E(\mathbb{F}_q)$ if $q \not\equiv \pm 1 \mod 7$; $\#\mathcal{F}(\mathbb{F}_q) = \#E(\mathbb{F}_q) - 6q - 6$ if $q \equiv \pm 1 \mod 7$.*

We immediately have the next corollary.

Corollary 4.2. *The curve $\mathcal{F}$ attains the Serre bound over $\mathbb{F}_q$ if and only if $q \equiv \pm 1$ mod 7 and $E\colon y^2 = x^3 + x^2 - 114x - 127$ attains the Serre bound over $\mathbb{F}_q$.*

By Magma, we find E over $\mathbb{F}_p$ attaining the Serre bound with $p \equiv \pm 1 \bmod 7$. Hence we have the next example. This is the first case of genus 7 over $\mathbb{F}_p$ attaining the Serre bound as we know.

Example 4.3. The curve $\mathcal{F}$ attains the Serre bound over $\mathbb{F}_p$ for $p =$213813599, 427838767, 681220511, 683578601.

Also, we implement Algorithm 17 in [19] which is based on the theory of zeta function, and find E over $\mathbb{F}_{p^3}$ attaining the Serre bound with $p^3 \equiv \pm 1 \bmod 7$. Hence we have the next example. We note that Example 20 of [19] are sextics over $\mathbb{F}_{p^3}$ of genus 7 attaining the Serre bound.

Example 4.4. The curve $\mathcal{F}$ attains the Serre bound over $\mathbb{F}_{p^3}$ for $p = 562493$, 3214831, 14130029, 26183671 and so on.

Let A be the coefficient of x^{p-1} in a polynomial $(x^3 + x^2 - 114x - 127)^m$. Then

$$\begin{aligned} A &= \sum_{j=0}^{m} \sum_{i=\lceil \frac{p-1-2j}{4} \rceil}^{\lfloor \frac{p-1-2j}{3} \rfloor} \binom{m}{i} \cdot \binom{m-i}{j} \cdot \binom{m-i-j}{p-1-3i-2j} (-114)^{p-1-3i-2j} \cdot (-127)^{2i+j-m} \\ &= \sum_{j=0}^{m} \sum_{i=\lceil \frac{p-1-2j}{4} \rceil}^{\lfloor \frac{p-1-2j}{3} \rfloor} \frac{m!}{i! \cdot j! \cdot (p-1-3i-2j)! \cdot (2i+j-m)!} (-114)^{p-1-3i-2j} \cdot (-127)^{2i+j-m}, \end{aligned}$$

where $\lceil \cdot \rceil$ is the ceiling function.

Theorem 4.5. (i) *Let $p \geq 17$. The curve $\mathcal{F}$ attains the Serre bound over $\mathbb{F}_p$ if and only if $p \equiv \pm 1$ mod 7 and*

$$\overline{A} \equiv -\lfloor 2\sqrt{p} \rfloor \mod p.$$

(ii) *Let $b \in \mathbb{F}_p$. The curve $\mathcal{F}$ is maximal over $\mathbb{F}_{p^2}$ if and only if $p^2 \equiv \pm 1$ mod 7 and*

$$\overline{A} \equiv 0 \mod p.$$

(iii) *Set A as the integer such that $\overline{A} \equiv A \bmod p$ and $0 \leq A < p$. Let $p \geq 11$. The curve $\mathcal{F}$ over $\mathbb{F}_{p^3}$ attains the Serre bound if and only if $p^3 \equiv \pm 1 \bmod 7$ and*

$$A^3 - 3pA = -\lfloor 2p\sqrt{p} \rfloor.$$

Proof. By Corollary 4.2 and Theorem 2.1 (i), (ii) and (iii), we are able to prove (i), (ii) and (iii) respectively. □

Howe [12] construct a curve $\mathcal{H}$ of genus 7 by the normalisation of the fibre product of the following three curves:

$$C_1 \colon y_1^2 = s_1(x-1)g_1,$$
$$C_2 \colon y_2^2 = s_2(x-1)g_2,$$
$$C_3 \colon y_3^2 = s\,x,$$

where g_1 and g_2 are monic quadratic polynomials that are coprime to one another and to $x-1$. The manypoints site [6] is updated by this curve.

Afterwards throughout this section, we set $g_1 = (x-a_1)(x-a_3)$, $g_2 = (x-a_2)(x-a_4)$, with $s, s_1, s_2 \in k\backslash\{0\}$, $a_1, a_2, a_3, a_4 \in k\backslash\{0,1\}$ are all different. The Jacobian of $\mathcal{H}$ are decomposed as follows:

$$J(\mathcal{H}) \sim E_1 \times \cdots \times E_5 \times D \tag{2}$$

where $E_1 \colon y^2 = s_1(x-1)(x-a_1)(x-a_3)$, $E_2 \colon y^2 = s_2(x-1)(x-a_2)(x-a_4)$, $E_3 \colon y^2 = ss_2x(x-1)(x-a_2)(x-a_4)$, $E_4 \colon y^2 = ss_1x(x-1)(x-a_1)(x-a_3)$, $E_5 \colon y^2 = s_1s_2(x-a_1)(x-a_3)(x-a_2)(x-a_4)$, $D \colon y^2 = ss_1s_2x(x-a_1)(x-a_2)(x-a_3)(x-a_4)$ from [12].

We are able to decompose the Jacobian of $\mathcal{H}$ over k completely under certain conditions.

Theorem 4.6. *Assume that $a_2(a_1-a_3) = a_4(a_1-a_2)$ and there exists a square root of $a_2(a_2-a_3)$ in k^*. Then the Jacobian of the curve $\mathcal{H}$ has the following isogeny relation over k:*

$$J(\mathcal{H}) \sim E_1 \times \cdots \times E_7$$

with the seven elliptic curves defined by

$$E_i \colon y^2 = \theta_i x(x-1)(x-\lambda_i) \quad \text{for } 1 \leq i \leq 7,$$

where

$$\theta_1 = s_1(a_1-1), \qquad \lambda_1 = \frac{a_3-1}{a_1-1},$$
$$\theta_2 = s_2(a_2-1), \qquad \lambda_2 = \frac{a_4-1}{a_2-1},$$
$$\theta_3 = -ss_2a_4(1-a_2), \qquad \lambda_3 = \frac{a_2(1-a_4)}{a_4(1-a_2)},$$
$$\theta_4 = -ss_1a_3(1-a_1), \qquad \lambda_4 = \frac{a_1(1-a_3)}{a_3(1-a_1)},$$
$$\theta_5 = -s_1s_2(a_4-a_1)(a_2-a_3), \qquad \lambda_5 = \frac{(a_3-a_1)(a_2-a_4)}{(a_2-a_3)(a_4-a_1)},$$
$$\theta_6 = \theta_7 = \frac{ss_1s_2a_1(a_1-a_3)}{a_1-a_2}, \qquad \lambda_6, \lambda_7 = \frac{(a_1-a_2)\big(a_3-2a_2 \pm 2(a_2^2-a_2a_3)^{1/2}\big)}{a_1(a_3-a_1)}.$$

In particular, if $k = \mathbb{F}_q$ then the number of rational points of $\mathcal{H}$ over $\mathbb{F}_q$ is given as

$$\#\mathcal{H}(\mathbb{F}_q) = \sum_{i=1}^{7} \#E_i(\mathbb{F}_q) - 6(q+1).$$

Proof. From (2), we have that $J(\mathcal{H}) \sim E_1 \times \cdots \times E_5 \times D$, where E_i are birational equivalent to $y^2 = \theta_i x(x-1)(x-\lambda_i)$ for $1 \leq i \leq 5$. From Theorem 3.4, $J(D) \sim E_6 \times E_7$. Hence we can prove it. □

We have the next theorem immediately.

Theorem 4.7. *Suppose that $s, s_1, s_2 \in \mathbb{F}_p \backslash \{0\}$, $a_1, a_2, a_3, a_4 \in \mathbb{F}_p \backslash \{0, 1\}$ are all different, $a_2(a_1 - a_3) = a_4(a_1 - a_2)$ and there exists a square root of $a_2(a_2 - a_3)$ in $\mathbb{F}_p^*$.*

(i) *The curve $\mathcal{H}$ over $\mathbb{F}_{p^2}$ is maximal if and only if the polynomial*

$$H_p(\lambda_i) \equiv 0 \mod p \qquad \text{for } 1 \leq i \leq 7,$$

where λ_i are defined as in Theorem 4.6. Further, if $\mathcal{H}$ over $\mathbb{F}_{p^2}$ is maximal then $p \equiv 3 \mod 4$.

(ii) *Let $p \geq 11$. Set h_i as the integer such that $h_i \equiv (-\theta_i)^m H_p(\lambda_i)$ mod p and $0 \leqq h_i < p$. The curve $\mathcal{H}$ over $\mathbb{F}_{p^3}$ attains the Serre bound if and only if*

$$h_i^3 - 3ph_i = -\lfloor 2p\sqrt{p} \rfloor \qquad \text{for } 1 \leq i \leq 7.$$

(iii) *The number of rational points of $\mathcal{H}$ over $\mathbb{F}_q$ satisfies $\#\mathcal{H}(\mathbb{F}_q) \equiv 0$ mod 4.*

Proof. (i) From Theorem 2.2 (i) and Theorem 4.6, we can prove it.
(ii) From Theorem 2.2 (ii) and Theorem 4.6, we can prove it.
(iii) From Lemma 2.3 and Theorem 4.6, we can prove it.

□

Table 1 lists explicit values $(p, s_1, s_2, a_1, a_2, a_3, a_4)$ satisfying the necessary and sufficient conditions of Theorem 4.7 (i). They are maximal curves of genus 7 over $\mathbb{F}_{p^2}$. In Example 4.8, we shall explain the case of $p = 23$ in Table 1. The other cases in the table are similar.

Example 18 of [19] are maximal curves of genus 7. Their orders of automorphism groups are 48 by direct checking with Magma. The orders of automorphism groups of curves in Table 1 are 8. Hence they are not isomorphic.

TABLE 1. Maximal curves of genus 7 over $\mathbb{F}_{p^2}$

p	s	s_1	s_2	a_1	a_2	a_3	a_4
23	1	1	1	2	7	9	19
31	1	1	1	7	10	22	19
47	1	1	1	2	13	40	15
71	1	1	1	2	10	24	63
79	1	1	1	11	35	51	32
167	1	1	1	2	162	69	24
191	1	1	1	3	27	186	182
199	1	1	1	76	147	42	123

Example 4.8. The curve $\mathcal{H}$ defined by the normalisation of the fibre product $C_1 \times_{\mathbb{P}^1} C_2 \times_{\mathbb{P}^1} C_3$ with the following three curves is a maximal curve of genus 7 over $\mathbb{F}_{23^2}$.

$$C_1 \colon y_1^2 = (x-1)(x-2)(x-9),$$
$$C_2 \colon y_2^2 = (x-1)(x-7)(x-19),$$
$$C_3 \colon y_3^2 = x.$$

From Theorem 4.6, the Jacobian have the isogeny relation: $J(\mathcal{H}) \sim E_1 \times \cdots \times E_7$, where $E_1 \colon y^2 = x(x-1)(x-8)$, $E_2 \colon y^2 = 6x(x-1)(x-3)$, $E_3 \colon y^2 = 22x(x-1)(x-12)$, $E_4 \colon y^2 = 9x(x-1)(x-12)$, $E_5 \colon y^2 = 11x(x-1)(x-16)$, $E_6 \colon y^2 = 12x(x-1)(x-21)$, $E_7 \colon y^2 = 12x(x-1)(x-22)$.

Table 2 lists explicit values $(p, s_1, s_2, a_1, a_2, a_3, a_4)$ satisfying the necessary and sufficient conditions of Theorem 4.7 (ii). They are curves of genus 7 over $\mathbb{F}_{p^3}$ attaining the Serre bound. We shall explain the case of $p = 193$ in Example 4.9.

TABLE 2. Curves of genus 7 attaining the Serre bound over $\mathbb{F}_{p^3}$

p	s	s_1	s_2	a_1	a_2	a_3	a_4
193	5	1	1	19	143	168	80
787	1	1	1	104	384	206	747

Example 4.9. The curve $\mathcal{H}$ defined by the normalisation of the fibre product $C_1 \times_{\mathbb{P}^1} C_2 \times_{\mathbb{P}^1} C_3$ with the following three curves attains the Serre bound over $\mathbb{F}_{193^3}$. The genus is 7.

$$\begin{aligned} C_1 &: y_1^2 = (x-1)(x-19)(x-168), \\ C_2 &: y_2^2 = (x-1)(x-143)(x-80), \\ C_3 &: y_3^2 = 5x. \end{aligned}$$

From Theorem 4.6, the Jacobian have the isogeny relation: $J(\mathcal{H}) \sim E_1 \times \cdots \times E_7$, where $E_1 : y^2 = 18x(x-1)(x-20)$, $E_2 : y^2 = 142x(x-1)(x-59)$, $E_3 : y^2 = 58x(x-1)(x-132)$, $E_4 : y^2 = 66x(x-1)(x-62)$, $E_5 : y^2 = 174x(x-1)(x-169)$, $E_6 : y^2 = 41x(x-1)(x-8)$, $E_7 : y^2 = 41x(x-1)(x-162)$.

5. Fibre products of three hyperelliptic curves

Let k be a field of characteristic $p > 2$. Let C_1, C_2 and C_3 be hyperelliptic curves defined by

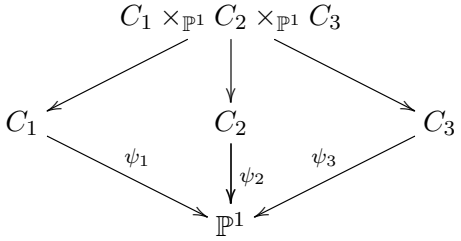
$$\begin{aligned} C_1 &: y_1^2 = s_1 f_2(x) f_5(x), \\ C_2 &: y_2^2 = s_2 f_1(x) f_2(x) f_3(x), \\ C_3 &: y_3^2 = s_3\, f_1(x) f_4(x), \end{aligned}$$

where $s_1, s_2, s_3 \in k \backslash \{0\}$. The polynomials are defined as the following:

$$\begin{aligned} f_1(x) &= (x - b_{1\,1}) \times \cdots \times (x - b_{1\,i_1}), \\ f_2(x) &= (x - b_{2\,1}) \times \cdots \times (x - b_{2\,i_2}), \\ f_3(x) &= (x - b_{3\,1}) \times \cdots \times (x - b_{3\,i_3}), \\ f_4(x) &= (x - b_{4\,1}) \times \cdots \times (x - b_{4\,i_4}), \\ f_5(x) &= (x - b_{5\,1}) \times \cdots \times (x - b_{5\,i_5}) \end{aligned}$$

where $b_{i\,i_j} \in k$ are all different with $0 \le i_1$, $1 \le i_2, i_3, i_4$ and $2 \le i_5$. If $i_1 = 0$ then we set $f_1(x) = 1$. We note that the degree of the polynomial $f_j(x)$ is i_j for $1 \le j \le 5$.

Let $\psi_1 : C_1 \to \mathbb{P}^1$, $\psi_2 : C_2 \to \mathbb{P}^1$ and $\psi_3 : C_3 \to \mathbb{P}^1$ be the hyperelliptic structures. Consider the fibre product $C_1 \times_{\mathbb{P}^1} C_2 \times_{\mathbb{P}^1} C_3$.



Assume that there exists no isomorphism $\varphi\colon C_1 \longrightarrow C_2$ such that $\psi_2 \circ \varphi = \psi_1$, $\varphi\colon C_2 \longrightarrow C_3$ such that $\psi_3 \circ \varphi = \psi_2$, $\varphi\colon C_3 \longrightarrow C_1$ such that $\psi_1 \circ \varphi = \psi_3$. Denote by C the normalisation of the fibre product $C_1 \times_{\mathbb{P}^1} C_2 \times_{\mathbb{P}^1} C_3$.

We are able to decompose the Jacobian of the curve C.

Theorem 5.1. *The Jacobian of the curve C decomposes over k as follows*: *if $i_1 = 0$ and $i_4 = 1$ then*

$$J(C) \sim J(C_1) \times J(C_2) \times J(C_4) \times J(C_5) \times J(C_6) \times J(C_7),$$

else

$$J(C) \sim J(C_1) \times \cdots \times J(C_7),$$

with

$$\begin{aligned} C_4\colon y_4^2 &= s_1 s_2 f_1(x) f_3(x) f_5(x), \\ C_5\colon y_5^2 &= s_1 s_3 f_1(x) f_2(x) f_4(x) f_5(x), \\ C_6\colon y_6^2 &= s_2 s_3 f_2(x) f_3(x) f_4(x), \\ C_7\colon y_7^2 &= s_1 s_2 s_3 f_3(x) f_4(x) f_5(x). \end{aligned}$$

Proof. The case of $i_1 = 0$ and $i_4 = 1$ is similar to the other cases. So we omit it here.

Assume $i_1 \neq 0$ or $i_4 \neq 1$. Three automorphisms of the curve C is given by

$$\begin{aligned} \sigma_1\colon (x, y_1, y_2, y_3) &\mapsto (x, -y_1, y_2, y_3), \\ \sigma_2\colon (x, y_1, y_2, y_3) &\mapsto (x, y_1, -y_2, y_3), \\ \sigma_3\colon (x, y_1, y_2, y_3) &\mapsto (x, y_1, y_2, -y_3). \end{aligned}$$

The quotients $C/\langle\sigma_1\rangle$ is birational equivalent to the curve defined by the normalisation of the fibre product of $C_2 \times_{\mathbb{P}^1} C_3$. From Corollary 3.2,

$$\begin{aligned} &J(C_2 \times_{\mathbb{P}^1} C_3) \times J((C_2 \times_{\mathbb{P}^1} C_3)/\langle\sigma_2, \sigma_3\rangle)^2 \\ &\sim J((C_2 \times_{\mathbb{P}^1} C_3)/\langle\sigma_2\rangle) \times J((C_2 \times_{\mathbb{P}^1} C_3)/\langle\sigma_3\rangle) \times J((C_2 \times_{\mathbb{P}^1} C_3)/\langle\sigma_2\sigma_3\rangle). \end{aligned}$$

Hence we have $J(C/\langle\sigma_1\rangle) \sim J(C_2) \times J(C_3) \times J(C_6)$. Similarly we have $J(C/\langle\sigma_2\rangle) \sim J(C_1) \times J(C_3) \times J(C_5)$ and $J(C/\langle\sigma_3\rangle) \sim J(C_1) \times J(C_2) \times J(C_4)$.

The quotients $C/\langle\sigma_2\sigma_3\rangle$ is birational equivalent to the curve defined by the normalisation of the fibre product $C_1 \times_{\mathbb{P}^1} C_6$. Let $\sigma_1\colon (x, y_1, y_6) \mapsto (x, -y_1, y_6)$, $\sigma_5\colon (x, y_1, y_6) \mapsto (x, y_1, -y_6)$. From Corollary 3.2,

$$\begin{aligned} &J(C_1 \times_{\mathbb{P}^1} C_6) \times J((C_1 \times_{\mathbb{P}^1} C_6)/\langle\sigma_1, \sigma_6\rangle)^2 \\ &\sim J((C_1 \times_{\mathbb{P}^1} C_6)/\langle\sigma_1\rangle) \times J((C_1 \times_{\mathbb{P}^1} C_6)/\langle\sigma_6\rangle) \times J((C_1 \times_{\mathbb{P}^1} C_6)/\langle\sigma_1\sigma_6\rangle). \end{aligned}$$

Hence we have $J(C/\langle\sigma_2\sigma_3\rangle) \sim J(C_6) \times J(C_1) \times J(C_7)$. Similarly we have $J(C/\langle\sigma_3\sigma_1\rangle) \sim J(C_5) \times J(C_2) \times J(C_7)$ and $J(C/\langle\sigma_1\sigma_2\rangle) \sim J(C_4) \times J(C_3) \times J(C_7)$.

From Corollary 3.2,

$$J(C) \times J(C/\langle\sigma_1\sigma_2, \sigma_3\rangle)^2 \sim J(C/\langle\sigma_1\sigma_2\rangle) \times J(C/\langle\sigma_3\rangle) \times J(C/\langle\sigma_1\sigma_2\sigma_3\rangle),$$

which means that $J(C) \times J(C_4)^2 \sim J(C/\langle\sigma_1\sigma_2\rangle) \times J(C/\langle\sigma_3\rangle) \times J(C/\langle\sigma_1\sigma_2\sigma_3\rangle)$. Similarly, we have that $J(C) \times J(C_6)^2 \sim J(C/\langle\sigma_2\sigma_3\rangle) \times J(C/\langle\sigma_1\rangle) \times J(C/\langle\sigma_1\sigma_2\sigma_3\rangle)$ and $J(C) \times J(C_5)^2 \sim J(C/\langle\sigma_1\sigma_3\rangle) \times J(C/\langle\sigma_2\rangle) \times J(C/\langle\sigma_1\sigma_2\sigma_3\rangle)$.

According to the above results, we have that

$$J(C) \sim J(C_1) \times J(C_2) \times J(C_3) \times J(C_7) \times J(C/\langle\sigma_1\sigma_2\sigma_3\rangle).$$

Combining the above results and Corollary 3.3, we have that

$$J(C)^3 \sim J(C_1)^3 \times J(C_2)^3 \times J(C_3)^3 \times J(C_4)^2 \times J(C_5)^2 \times J(C_6)^2 \times J(C_7)^3 \times J(C/\langle\sigma_1\sigma_2\sigma_3\rangle).$$

Therefor we can prove it. □

At this moment, we are able to exactly determine the genus of a curve C by the degrees of polynomials $f_i(x)$ for $1 \leq i \leq 5$.

Corollary 5.2. *The genus of the cure C is given as*

$$\begin{aligned} g(C) =& \lfloor\frac{i_2+i_5-1}{2}\rfloor + \lfloor\frac{i_1+i_2+i_3-1}{2}\rfloor + \lfloor\frac{i_1+i_4-1}{2}\rfloor + \lfloor\frac{i_1+i_3+i_5-1}{2}\rfloor \\ &+ \lfloor\frac{i_1+i_2+i_4+i_5-1}{2}\rfloor + \lfloor\frac{i_2+i_3+i_4-1}{2}\rfloor + \lfloor\frac{i_3+i_4+i_5-1}{2}\rfloor. \end{aligned}$$

Proof. Since the genera of curves C_i for $1 \leq i \leq 7$ are determined as the following: $g(C_1) = \lfloor(i_2+i_5-1)/2\rfloor$, $g(C_2) = \lfloor(i_1+i_2+i_3-1)/2\rfloor$, $g(C_3) = \lfloor(i_1+i_4-1)/2\rfloor$, $g(C_4) = \lfloor(i_1+i_3+i_5-1)/2\rfloor$, $g(C_5) = \lfloor(i_1+i_2+i_4+i_5-1)/2\rfloor$, $g(C_6) = \lfloor(i_2+i_3+i_4-1)/2\rfloor$ and $g(C_7) = \lfloor(i_3+i_4+i_5-1)/2\rfloor$. Hence we have $g(C)$ from Theorem 5.1 immediately. □

Corollary 5.3. *If $k = \mathbb{F}_q$ then the number of rational points of the curve C over $\mathbb{F}_q$ are as the following*:

if $i_1 = 0$ and $i_4 = 1$ then

$$\#C(\mathbb{F}_q) = \sum_{j=1, j\neq 3}^{7} \#C_j(\mathbb{F}_q) - 5(q+1),$$

else

$$\#C(\mathbb{F}_q) = \sum_{j=1}^{7} \#C_j(\mathbb{F}_q) - 6(q+1).$$

Proof. Since the case of $i_1 = 0$ and $i_4 = 1$ is similar to the other cases. So we omit it here.

Let $i_1 \neq 0$ or $i_4 \neq 1$. It is well known that $\#C(\mathbb{F}_q) = q+1-t$, where t is the trace of the Frobenius endomorphism acting on a Tate module of $J(C)$. Since $J(C) \sim J(C_1)\times\cdots\times J(C_7)$, then the Tate module of $J(C)$ is isomorphic to the direct sum of the Tate modules of $J(C_1), \ldots, J(C_7)$. Hence $t = t_1 + \cdots + t_7$, where $t_1, \ldots, t_7$ are the traces of the Frobenius on the Tate modules of $J(C_1), \ldots, J(C_7)$ respectively. The result follows by recalling that $t_i = q + 1 - \#C_i(\mathbb{F}_q)$ for $1 \leq i \leq 7$. □

6. Curves of genus 9 with many points

We define curves of type I and II and study on them in this section.

Definition 6.1. We call a curve $\mathcal{C}_\mathrm{I}$ defined by the normalisation of the fibre product $C_1 \times_{\mathbb{P}^1} C_2 \times_{\mathbb{P}^1} C_3$ with the following equations a *curve of type* I:

$$\begin{aligned} C_1 &: y_1^2 = s_1(x-1)(x-a_2)(x-a_3), \\ C_2 &: y_2^2 = s_2(x-a_1)(x-a_2)(x-a_3)(x-a_4), \\ C_3 &: y_3^2 = s_3x(x-a_1)(x-a_5), \end{aligned}$$

where $s_1, s_2, s_3 \in k\backslash\{0\}$, $a_i \in k\backslash\{0,1\}$ for $1 \leq i \leq 5$ are all different.

From Theorem 5.1, Corollary 5.2 and 5.3, we have the next corollary immediately.

Corollary 6.2. (i) *The Jacobian of the curve of type* I *has the following isogeny relation*:

$$J(\mathcal{C}_{\mathrm{I}}) \sim J(C_1) \times \cdots \times J(C_7),$$

where $C_4\colon y^2 = s_1s_2(x-1)(x-a_1)(x-a_4)$, $C_5\colon y^2 = s_1s_3x(x-1)(x-a_1)(x-a_2)(x-a_3)(x-a_5)$, $C_6\colon y^2 = s_2s_3x(x-a_2)(x-a_3)(x-a_4)(x-a_5)$, $C_7\colon y^2 = s_1s_2s_3x(x-1)(x-a_4)(x-a_5)$.

(ii) *The genus of a curve of type* I *is* 9.

(iii) *When* $k = \mathbb{F}_q$, *we have* $\#\mathcal{C}_{\mathrm{I}}(\mathbb{F}_q) = \sum_{j=1}^{7} \#C_j(\mathbb{F}_q) - 6(q+1)$.

Table 3 lists explicit values $(p, s_1, s_2, s_3, a_1, a_2, a_3, a_4, a_5, \#\mathcal{C}_{\mathrm{I}}(\mathbb{F}_p))$ which are able to update the manypoints site [6]. We shall explain the case of $p = 17$ in Example 6.3. The other cases are similar.

TABLE 3. Curves of type I of genus 9 with many points

q	s_1	s_2	s_3	a_1	a_2	a_3	a_4	a_5	$\#\mathcal{C}_{\mathrm{I}}(\mathbb{F}_p)$	old entry	new entry
17	1	1	1	4	12	16	3	15	72	64-83	72-83
29	1	2	1	8	18	24	19	4	104	100-120	104-120
37	1	1	1	5	17	35	29	30	120	116-142	120-142
43	1	1	1	2	25	27	14	7	132	128-155	132-155
47	1	1	1	4	21	25	20	38	144	132-162	144-162
53	1	1	1	2	33	44	11	51	152	148-176	152-176
59	1	1	1	14	38	58	4	43	164	160-189	164-189
61	1	1	1	20	55	58	3	29	172	168-193	172-193
67	2	1	2	5	59	66	19	47	184	180-206	184-206
71	1	1	7	22	39	50	26	27	200	192-213	200-213
73	1	5	1	17	26	56	27	35	200	184-218	200-218
79	1	1	1	6	16	54	14	37	208	200-230	208-230
97	1	5	1	4	60	79	69	95	244	228-266	244-266
11^3	1	2	1	2	5	10	4	3	1920	1812-1980	1920-1980
19^3	1	1	1	4	2	6	9	18	8120	8057-8345	8120-8345
13^5	1	1	1	3	11	12	2	9	382104	382096-382256	382104-382256
17^5	1	1	1	6	10	15	4	13	1439708	1438108-1441305	1439708-1441305

Example 6.3. The curve $\mathcal{C}_{\mathrm{I}}$ which is defined by the normalisation of the fibre product $C_1 \times_{\mathbb{P}^1} C_2 \times_{\mathbb{P}^1} C_3$ with

$$\begin{aligned} C_1\colon y_1^2 &= (x-1)(x-12)(x-16), \\ C_2\colon y_2^2 &= (x-4)(x-12)(x-16)(x-3), \\ C_3\colon y_3^2 &= x(x-4)(x-15) \end{aligned}$$

has 72 rational points over $\mathbb{F}_{17}$. The genus is 9. From Corollary 6.2 (i) its Jacobian has the isogeny relation: $J(\mathcal{C}_{\mathrm{I}}) \sim J(C_1) \times \cdots \times J(C_7)$ where $C_4\colon y^2 = (x-1)(x-4)(x-3)$, $C_5\colon y^2 = x(x-1)(x-4)(x-12)(x-16)(x-15)$, $C_6\colon y^2 = x(x-12)(x-16)(x-3)(x-15)$, $C_7\colon y^2 = x(x-1)(x-3)(x-15)$.

In this case the best known lower bound is 64, so we can give a new entry in [6].

We are able to completely decompose the Jacobian of a curve $\mathcal{C}_{\mathrm{I}}$ of type I under certain conditions.

Theorem 6.4. *Assume that* $(1-a_2)a_5(a_1-a_3) = (1-a_5)a_3(a_1-a_2)$, $a_3(a_2-a_4) = a_5(a_2-a_3)$, *there exists square roots of* $a_3(1-a_2)(a_3-a_2)$ *and* $a_3(a_3-a_4)$ *in* k^*. *Then the Jacobian of a curve* $\mathcal{C}_{\mathrm{I}}$ *of type* I *has the following isogeny relation*:

$$J(\mathcal{C}_{\mathrm{I}}) \sim E_1 \times \cdots \times E_9$$

where

$$E_i \colon y^2 = \theta_i x(x-1)(x-\lambda_i)$$

with

$$\begin{aligned}
&\theta_1 = s_1(a_2-1), && \lambda_1 = \frac{a_3-1}{a_2-1},\\
&\theta_2 = s_2(a_1-a_4)(a_2-a_3), && \lambda_2 = \frac{(a_1-a_3)(a_2-a_4)}{(a_2-a_3)(a_1-a_4)},\\
&\theta_3 = s_3a_1, && \lambda_3 = \frac{a_5}{a_1},\\
&\theta_4 = s_1s_2(a_1-1), && \lambda_4 = \frac{a_4-1}{a_1-1},\\
&\theta_5 = \theta_6 = \frac{\gamma(1-\beta)}{1-\alpha}, && \lambda_5, \lambda_6 = \frac{(1-\alpha)\big(\beta-2\alpha \pm 2(\alpha^2-\alpha\beta)^{1/2}\big)}{\beta-1},\\
&\theta_7 = \theta_8 = \frac{s_2s_3a_2(a_2-a_4)}{a_2-a_3}, && \lambda_7, \lambda_8 = \frac{(a_2-a_3)\big(a_4-2a_3 \pm 2(a_3^2-a_3a_4)^{1/2}\big)}{a_2(a_4-a_2)},\\
&\theta_9 = s_1s_2s_3a_5(a_4-1), && \lambda_9 = \frac{a_4(1-a_5)}{a_5(1-a_4)}.
\end{aligned}$$

Here $\alpha = a_1(1-a_2)/(a_2(1-a_1))$, $\beta = a_1(1-a_3)/(a_3(1-a_1))$, $\gamma = s_1s_3a_2a_3a_5(a_1-1)$.

In particular, if $k = \mathbb{F}_q$ *then the number of rational points of* $\mathcal{C}_{\mathrm{I}}$ *over* $\mathbb{F}_q$ *is given as*

$$\#\mathcal{C}_{\mathrm{I}}(\mathbb{F}_q) = \sum_{i=1}^{9} \#E_i(\mathbb{F}_q) - 8(q+1).$$

Proof. We have the Jacobian decomposition $J(\mathcal{C}_{\mathrm{I}}) \sim J(C_1) \times \cdots \times J(C_7)$ as Corollary 6.2 (i). C_i is birational equivalent to E_i for $1 \le i \le 4$. From Theorem 3.5, we have $J(C_5) \sim E_5 \times E_6$. From Theorem 3.4, we have $J(C_6) \sim E_7 \times E_8$. At last, C_7 is birational to E_9. Hence we can prove it. □

Theorem 6.5. *Suppose that* $s_1, s_2, s_3 \in \mathbb{F}_p\backslash\{0\}$, $a_i \in \mathbb{F}_p\backslash\{0,1\}$ *for* $1 \le i \le 5$ *are all different. Assume that* $(1-a_2)a_5(a_1-a_3) = (1-a_5)a_3(a_1-a_2)$, $a_3(a_2-a_4) = a_5(a_2-a_3)$, *there exists square roots of* $(1-a_2)(a_3^2-a_2a_3)$ *and* $a_3(a_3-a_4)$ *in* $\mathbb{F}_p^*$ *respectively.*

(i) *The curve* $\mathcal{C}_{\mathrm{I}}$ *of type* I *over* $\mathbb{F}_{p^2}$ *is maximal if and only if*

$$H_p(\lambda_i) \equiv 0 \mod p \qquad \text{for } 1 \le i \le 9.$$

Further, if $\mathcal{C}_{\mathrm{I}}$ *over* $\mathbb{F}_{p^2}$ *is maximal then* $p \equiv 3 \mod 4$.

(ii) *The number of rational points of* $\mathcal{C}_{\mathrm{I}}$ *over* $\mathbb{F}_q$ *satisfies* $\#\mathcal{C}_{\mathrm{I}}(\mathbb{F}_q) \equiv 0$ *mod* 4.

Proof. (i) By Theorem 2.2 (i) and Theorem 6.4.

(ii) By Lemma 2.3 and Theorem 6.4.

□

Table 4 lists explicit values $(p, s_1, s_2, s_3, a_1, a_2, a_3, a_4, a_5)$ satisfying the necessary and sufficient conditions of Theorem 6.5 (i). They are maximal curves of type I over $\mathbb{F}_{p^2}$. We shall explain the case of $p = 47$ in Example 6.6. The other cases in the table are similar.

TABLE 4. Maximal curves of type I of genus 9 over $\mathbb{F}_{p^2}$

p	s_1	s_2	s_3	a_1	a_2	a_3	a_4	a_5
47	1	1	1	30	5	29	19	13
71	1	1	1	25	9	6	20	49
191	1	1	1	34	163	30	67	115
239	1	1	1	200	121	120	40	160
311	1	1	1	28	152	305	57	83

Example 6.6. The curve defined by the normalisation of the fibre product $C_1 \times_{\mathbb{P}^1} C_2 \times_{\mathbb{P}^1} C_3$ with

$$\begin{aligned} C_1 &: y_1^2 = (x-1)(x-5)(x-29), \\ C_2 &: y_2^2 = (x-30)(x-5)(x-29)(x-19), \\ C_3 &: y_3^2 = x(x-30)(x-13) \end{aligned}$$

is a maximal curve of genus 9 over $\mathbb{F}_{47^2}$. From Theorem 6.4, the Jacobian have the isogeny relation: $J(\mathcal{C}_{\mathrm{I}}) \sim E_1 \times \cdots \times E_9$, where $E_1 : y^2 = 4x(x-1)(x-7)$, $E_2 : y^2 = 18x(x-1)(x-41)$, $E_3 : y^2 = 30x(x-1)(x-2)$, $E_4 : y^2 = 29x(x-1)(x-46)$, $E_5 : y^2 = 16x(x-1)(x-39)$, $E_6 : y^2 = 16x(x-1)(x-46)$, $E_7 : y^2 = 42x(x-1)(x-37)$, $E_8 : y^2 = 42x(x-1)(x-28)$, $E_9 : y^2 = 46x(x-1)(x-7)$.

Next, we define one more type of curves.

Definition 6.7. We call a curve $\mathcal{C}_{\mathrm{II}}$ defined by the normalisation of the fibre product $C_1 \times_{\mathbb{P}^1} C_2 \times_{\mathbb{P}^1} C_3$ with the following equations a *curve of type* II:

$$\begin{aligned} C_1 &: y_1^2 = s_1(x-1)(x-a_1)(x-a_2)(x-a_3), \\ C_2 &: y_2^2 = s_2(x-1)(x-a_1)(x-a_4)(x-a_5), \\ C_3 &: y_3^2 = s_3\, x. \end{aligned}$$

From Theorem 5.1, Corollary 5.2 and 5.3, we have the next corollary immediately.

Corollary 6.8. (i) *The Jacobian of the curve of type* II *has the isogeny relation*:

$$J(\mathcal{C}_{\mathrm{II}}) \sim J(C_1) \times J(C_2) \times J(C_4) \times J(C_5) \times J(C_6) \times J(C_7),$$

where $C_4 : y^2 = s_1 s_2 (x-a_2)(x-a_3)(x-a_4)(x-a_5)$, $C_5 : y^2 = s_1 s_3 x(x-1)(x-a_1)(x-a_2)(x-a_3)$, $C_6 : y^2 = s_2 s_3 x(x-1)(x-a_1)(x-a_4)(x-a_5)$, $C_7 : y^2 = s_1 s_2 s_3 x(x-a_2)(x-a_3)(x-a_4)(x-a_5)$.

(ii) *The genus of a curve of type* II *is* 9.

(iii) *When* $k = \mathbb{F}_q$, *we have* $\#\mathcal{C}_{\mathrm{II}}(\mathbb{F}_q) = \sum_{j=1, j\neq 3}^{7} \#C_j(\mathbb{F}_q) - 5(q+1)$.

Table 5 lists explicit values $(q, s_1, s_2, s_3, a_1, a_2, a_3, a_4, a_5, \#\mathcal{C}_{\mathrm{II}}(\mathbb{F}_q))$ which are able to update the manypoints site [6]. In Example 6.9 below, we shall explain the case of $p = 83$ in the table. The other cases are similar.

TABLE 5. Curves of type II of genus 9 with many points

q	s_1	s_2	s_3	a_1	a_2	a_3	a_4	a_5	$\#\mathcal{C}_{\mathrm{II}}(\mathbb{F}_q)$	old entry	new entry
83	1	2	1	2	37	44	51	67	216	208-238	216-238
89	3	3	3	31	45	47	51	68	224	216-249	224-249
17^4	1	1	1	5	9	11	14	13	88688	87272-88724	88688-88724
19^5	1	1	1	2	11	12	13	14	2500100	-2504423	2500100-2504423

Example 6.9. The curve $\mathcal{C}_{\mathrm{II}}$ which is defined by the normalisation of the fibre product of $C_1 \times_{\mathbb{P}^1} C_2 \times_{\mathbb{P}^1} C_3$ with

$$\begin{aligned} C_1 &: y_1^2 = (x-1)(x-2)(x-37)(x-44), \\ C_2 &: y_2^2 = 2(x-1)(x-2)(x-51)(x-67), \\ C_3 &: y_3^2 = x \end{aligned}$$

has 216 rational points over $\mathbb{F}_{83}$. The genus is 9. From Corollary 6.8(i) its Jacobian has the isogeny relation: $J(\mathcal{C}_{\mathrm{II}}) \sim J(C_1) \times J(C_2) \times J(C_4) \times J(C_5) \times J(C_6) \times J(C_7)$ where $C_4 : y^2 = 2(x-37)(x-44)(x-51)(x-67)$, $C_5 : y^2 = x(x-1)(x-2)(x-37)(x-44)$, $C_6 : y^2 = 2x(x-1)(x-2)(x-51)(x-67)$, $C_7 : y^2 = 2x(x-37)(x-44)(x-51)(x-67)$.

In this case the best known lower bound is 208, so we can give a new entry in [6].

7. Curves of genus 11 with many points

We define curves of type III and type IV and study on them in this section.

Definition 7.1. We call a curve $\mathcal{C}_{\mathrm{III}}$ defined by the normalisation of the fibre product $C_1 \times_{\mathbb{P}^1} C_2 \times_{\mathbb{P}^1} C_3$ with the following equations a *curve of type* III:

$$\begin{aligned} C_1 &: y_1^2 = s_1(x-1)(x-a_2)(x-a_3), \\ C_2 &: y_2^2 = s_2(x-a_1)(x-a_2)(x-a_3)(x-a_4)(x-a_5), \\ C_3 &: y_3^2 = s_3\, x(x-a_1)(x-a_4)(x-a_6). \end{aligned}$$

From Theorem 5.1, Corollary 5.2 and 5.3, we have the next corollary immediately.

Corollary 7.2. (i) *The Jacobian of a curve of type* III *has the isogeny relation*:

$$J(\mathcal{C}_{\mathrm{III}}) \sim J(C_1) \times \cdots \times J(C_7),$$

where $C_4 : y^2 = s_1 s_2 (x-1)(x-a_1)(x-a_4)(x-a_5)$, $C_5 : y^2 = s_1 s_3 x(x-1)(x-a_1)(x-a_2)(x-a_3)(x-a_4)(x-a_6)$, $C_6 : y^2 = s_2 s_3 x(x-a_2)(x-a_3)(x-a_5)(x-a_6)$, $C_7 : y^2 = s_1 s_2 s_3 x(x-1)(x-a_5)(x-a_6)$.

(ii) *The genus of a curve of type* III *is* 11.

(iii) *When* $k = \mathbb{F}_q$, *we have* $\#\mathcal{C}_{\mathrm{III}}(\mathbb{F}_q) = \sum_{j=1}^{7} \#C_j(\mathbb{F}_q) - 6(q+1)$.

Table 6 lists explicit values $(q, s_1, s_2, s_3, a_1, a_2, a_3, a_4, a_5, a_6, \#\mathcal{C}_{\mathrm{III}}(\mathbb{F}_q))$ which are able to update the manypoints site [6]. In Example 7.3 below, we shall explain the case of $p = 41$ in the table. The other cases in the table are similar.

Example 7.3. The curve $\mathcal{C}_{\mathrm{III}}$ which is defined by the normalisation of the fibre product $C_1 \times_{\mathbb{P}^1} C_2 \times_{\mathbb{P}^1} C_3$ with

$$\begin{aligned} C_1 &: y_1^2 = (x-1)(x-23)(x-37), \\ C_2 &: y_2^2 = 3(x-16)(x-23)(x-37)(x-10)(x-14), \\ C_3 &: y_3^2 = x(x-16)(x-10)(x-39) \end{aligned}$$

has 140 rational points over $\mathbb{F}_{41}$. Its genus is 11. From Corollary 7.2(i) its Jacobian has the isogeny relation: $J(\mathcal{C}_{\mathrm{III}}) \sim J(C_1) \times \cdots \times J(C_7)$, where $C_4 : y^2 = 3(x-1)(x-16)(x-10)(x-14)$, $C_5 : y^2 = x(x-1)(x-16)(x-23)(x-37)(x-10)(x-39)$, $C_6 : y^2 = 3x(x-23)(x-37)(x-14)(x-39)$, $C_7 : y^2 = 3x(x-1)(x-14)(x-39)$.

In this case there are no lower bound, so we can give a new entry in [6].

Next, we define one more type of curves.

TABLE 6. Curves of type III of genus 11 with many points

q	s_1	s_2	s_3	a_1	a_2	a_3	a_4	a_5	a_6	$\#\mathcal{C}_{\mathrm{III}}(\mathbb{F}_q)$	old entry	new entry
41	1	3	1	16	23	37	10	14	39	140	-174	140-174
47	5	1	1	17	20	32	33	39	42	152	-191	152-191
53	1	1	1	18	43	50	33	34	42	168	-208	168-208
59	1	1	1	6	16	50	37	48	51	176	-221	176-221
61	2	2	1	8	47	56	21	30	41	192	-227	192-227
67	1	1	2	17	21	24	4	7	37	196	-240	196-240
71	7	1	1	2	7	19	23	42	45	208	-248	208-248
73	5	1	5	3	4	5	35	44	55	208	-253	208-253
79	1	1	1	13	27	37	63	67	77	216	-264	216-264
83	1	1	2	26	43	54	65	68	70	228	-274	228-274
89	1	1	1	14	24	51	71	80	87	236	-285	236-285
97	1	5	1	4	28	36	44	68	82	256	-303	256-303
11^3	1	1	2	2	4	5	6	7	8	1920	-2124	1920-2124
13^5	1	2	2	2	3	4	5	10	11	384492	-384692	384492-384692

Definition 7.4. We call a curve $\mathcal{C}_{\mathrm{IV}}$ defined by the normalisation of the fibre product $C_1 \times_{\mathbb{P}^1} C_2 \times_{\mathbb{P}^1} C_3$ with the following equations a *curve of type* IV:

$$\begin{aligned} C_1 &: y_1^2 = s_1(x-1)(x-a_1)(x-a_2)(x-a_3)(x-a_4), \\ C_2 &: y_2^2 = s_2(x-1)(x-a_1)(x-a_2)(x-a_5)(x-a_6), \\ C_3 &: y_3^2 = s_3\, x. \end{aligned}$$

From Theorem 5.1, Corollary 5.2 and 5.3, we have the next corollary immediately.

Corollary 7.5. (i) *The Jacobian of a curve of type* IV *has the isogeny relation*:

$$J(\mathcal{C}_{\mathrm{IV}}) \sim J(C_1) \times J(C_2) \times J(C_4) \times J(C_5) \times J(C_6) \times J(C_7),$$

where $C_4 : y^2 = s_1s_2(x-a_3)(x-a_4)(x-a_5)(x-a_6)$, $C_5 : y^2 = s_1s_3x(x-1)(x-a_1)(x-a_2)(x-a_3)(x-a_4)$, $C_6 : y^2 = s_2s_3x(x-1)(x-a_1)(x-a_2)(x-a_5)(x-a_6)$, $C_7 : y^2 = s_1s_2s_3x(x-a_3)(x-a_4)(x-a_5)(x-a_6)$.

(ii) *The genus of a curve of type* IV *is* 11.

(iii) *When* $k = \mathbb{F}_q$, *we have* $\#\mathcal{C}_{\mathrm{IV}}(\mathbb{F}_q) = \sum_{j=1,j\neq 3}^{7} \#C_j(\mathbb{F}_q) - 5(q+1)$.

Table 7 lists explicit values $(q, s_1, s_2, s_3, a_1, a_2, a_3, a_4, a_5, a_6, \#\mathcal{C}_{\mathrm{IV}}(\mathbb{F}_q))$ which are able to update the manypoints site [6]. In Example 7.6, we shall explain the case of $q = 19^2$ in the table. The other cases in the table are similar.

TABLE 7. Curves of type IV of genus 11 with many points

q	s_1	s_2	s_3	a_1	a_2	a_3	a_4	a_5	a_6	$\#\mathcal{C}_{\mathrm{IV}}(\mathbb{F}_q)$	old entry	new entry
19^2	1	1	1	4	5	6	9	16	17	732	724-780	732-780
19^3	1	2	2	5	6	10	12	13	18	8448	-8675	8448-8675
17^4	1	1	1	4	5	6	7	11	15	89836	88580-89880	89836-89880
19^4	1	1	1	2	5	7	10	11	18	137036	136612-138264	137036-138264
17^5	1	1	3	2	4	5	8	9	11	1443208	1438748-1446071	1443208-1446071

Example 7.6. The curve $\mathcal{C}_{\mathrm{IV}}$ which is defined by the normalisation of the fibre product $C_1 \times_{\mathbb{P}^1} C_2 \times_{\mathbb{P}^1} C_3$ with

$$\begin{aligned} C_1 &: y_1^2 = (x-1)(x-4)(x-5)(x-6)(x-9), \\ C_2 &: y_2^2 = (x-1)(x-4)(x-5)(x-16)(x-17), \\ C_3 &: y_3^2 = x \end{aligned}$$

has 732 rational points over $\mathbb{F}_{19^2}$. Its genus is 11. From Corollary 7.5(i) its Jacobian has the isogeny relation: $J(\mathcal{C}_{\mathrm{IV}}) \sim J(C_1) \times J(C_2) \times J(C_4) \times J(C_5) \times J(C_6) \times J(C_7)$, where $C_4 : y^2 = (x-6)(x-9)(x-16)(x-17)$, $C_5 : y^2 = x(x-1)(x-4)(x-5)(x-6)(x-9)$, $C_6 : y^2 = x(x-1)(x-4)(x-5)(x-16)(x-17)$, $C_7 : y^2 = x(x-6)(x-9)(x-16)(x-17)$.

In this case the best known lower bound is 724, so we can give a new entry in [6].

At last, we find a maximal curve of type IV of genus 11 over $\mathbb{F}_{47^2}$.

Example 7.7. The curve $\mathcal{C}_{\mathrm{IV}}$ which is defined by the normalisation of the fibre product $C_1 \times_{\mathbb{P}^1} C_2 \times_{\mathbb{P}^1} C_3$ with

$$\begin{aligned} C_1 &: y_1^2 = (x-1)(x-4)(x-5)(x-18)(x-25), \\ C_2 &: y_2^2 = (x-1)(x-4)(x-5)(x-27)(x-34), \\ C_3 &: y_3^2 = x \end{aligned}$$

is a maximal curve of genus 11 over $\mathbb{F}_{47^2}$. From Corollary 7.5(i) its Jacobian has the isogeny relation: $J(\mathcal{C}_{\mathrm{IV}}) \sim J(C_1) \times J(C_2) \times J(C_4) \times J(C_5) \times J(C_6) \times J(C_7)$, where $C_4 : y^2 = (x-18)(x-25)(x-27)(x-34)$, $C_5 : y^2 = x(x-1)(x-4)(x-5)(x-18)(x-25)$, $C_6 : y^2 = x(x-1)(x-4)(x-5)(x-27)(x-34)$, $C_7 : y^2 = x(x-18)(x-25)(x-27)(x-34)$.

Acknowledgements

This research was partially supported by JSPS Grant-in-Aid for Scientific Research (C) 23K03199.

References

[1] D. Bartoli, M. Montanucci, F. Torres, $\mathbb{F}_{p^2}$-maximal curves with many automorphisms are Galois-covered by the Hermitian curve, Adv. Geom.**21**(3) (2021), 325–336.
[2] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. **24** (1997), 235–265.
[3] C. Costello, B. Smith, The supersingular isogeny problem in genus 2 and beyond, PQCrypto 2020, LNCS **12100** (2020), 151–168.
[4] A. Garcia, G. Güneri, H. Stichtenoth, A generalization of the Giulietti–Korchmáros maximal curve, Adv. Geom. **10**(3) (2010), 427–434.
[5] A. Garcia, S. Tafazolian, Certain maximal curves and Cartier operators, Acta Arith. **135**(39) (2008), 199–218.
[6] G. van der Geer, E. Howe, K. Lauter, C. Ritzenthaler, Table of curves with many points, `http://www.manypoints.org`.
[7] M. Giulietti, M. Montanucci, G. Zini, On maximal curves that are not quotients of the Hermitian curve, Finite Fields Appl. **41** (2016), 72–88.
[8] V. D. Goppa, Codes on algebraic curves, Dokl. Akad. nauk SSSR **259**(6) (1981), 1289–1290.
[9] R. Gupta, E. A. R. Mendoza, L. Quoos, Reciprocal polynomials and curves with many points over a finite field, Res. Number Theory **9**,60 (2023).
[10] R. A. Hidalgo, About the Fricke–Macbeath curve, Eur. J. Math. **4**(1) (2018), 313–325.
[11] E. W. Howe, Quickly constructing curves of genus 4 with many points, Comtemp. Math. **663** (2016), 149–173.
[12] E. W. Howe, Curves of medium genus with many points, Finite Fields Appl. **47** (2017), 145–160.
[13] A. Iezzi, M. Q. Kawakita, M. Timpanella, New sextics of genus 6 and 10 attaining the Serre bound, Adv. Geometry **24**(1) (2024), 99–109.
[14] E. Kani, M. Rosen, Idempotent relations and factors of Jacobians, Math. Ann. **284**(2) (1989), 307–327.

[15] T. Katsura, K. Takashima, Counting Richelot isogenies between superspecial abelian surfaces, ANTS 2020, The open book series **4** (2020), 283–300.
[16] T. Katsura, K. Takashima, Decomposed Richelot isogenies of Jacobian varieties of hyperelliptic curves and generalized Howe curves, Comment. MathUniv. St. Pauli **72**(2024), 3–17.
[17] M. Q. Kawakita, Kummer curves and their fibre products with many rational points, Appl. Algebra Engrg. Comm. Comput. **14** (2003), 55–64.
[18] M. Q. Kawakita, Wiman's and Edge's sextic attaining Serre's bound II, Contemp. Math. **637** (2015), 191–203.
[19] M. Q. Kawakita, Some sextics of genera five and seven attaining the Serre bound, LNCS **11321** (2018), 264–271.
[20] M. Q. Kawakita, Generalised Howe curves of genus five attaining the Serre bound, arXiv:2412.03071.
[21] M. Kudo, S. Harashita, E. Howe, Algorithms to enumerate superspecial Howe curves of genus four, ANTS 2020, The open book series **4** (2020), 301–316.
[22] M. Kudo, S. Harashita, H. Senda, The existence of supersingular curves of genus 4 in arbitrary characteristic, Res. Number Theory **6**,44 (2020).
[23] A. M. Macbeath, On a curve of genus 7, Proc. London Math. Sci. **s3-15**(1) (1965), 527–542.
[24] F. Özbudak, B. G. Temur, Fibre products of Kummer covers and curves with many points Appl. Algebra Engrg. Comm. Comput. **18** (2007), 433–443.
[25] F. Özbudak, B. G. Temür Finite number of fibre products of Kummer covers and curves with many points over finite fields, Designs, Codes and Cryptography **70** (2014), 385–404.
[26] F. Özbudak, B. G. Temür, O. Yayla, Further results on fibre products of Kummer covers and curves with many points over finite fields, Adv. Math. Commun. **10** (2016), 151-–162.
[27] J. Paulhus, Decomposing Jacobians of curves with extra automorphisms, Acta Arith. **132**,3(2008), 231–244.
[28] J-P. Serre, Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini, C. R. Acad. Sci. Paris Sér. I Math. **296**(9) (1983), 397–402.
[29] J. H. Silverman, The arithmetic of elliptic curves 2nd Ed., GTM **106**, Springer 2009.
[30] H. Stichtenoth, Algebraic function fields and codes 2nd Ed., GTM **254**, Springer 2009.
[31] J. Top, C. Verschoor, Counting points on the Fricke–Macbeath curve over finite fields, J. Théor. Nombres Bordeaux **30**(1) (2018), 117–129.

Division of Mathematics, Shiga University of Medical Science, Seta Tsukinowa-cho, Otsu, Shiga, 520-2192 Japan
Email address: kawakita@belle.shiga-med.ac.jp