Construction of a k-complete addition law on abelian surfaces with rational theta constants

Christophe Arene, Romain Cosset

CONSTRUCTION OF A $\mathbb{k}$-COMPLETE ADDITION LAW ON ABELIAN SURFACES WITH RATIONAL THETA CONSTANTS

CHRISTOPHE ARENE AND ROMAIN COSSET

Keywords: theta functions, Jacobian, genus 2 curve, addition law, completeness, embedding, line bundle, finite field.

Abstract. In this paper we explain how to construct $\mathbb{F}_q$-complete addition laws on the Jacobian of an hyperelliptic curve of genus 2. This is usefull for robustness and is needed for some applications (like for instance on embedded devices).

1. Introduction

Cryptographic protocols using abelian varieties, specifically elliptic curves and abelian surfaces, are a promising way of research. They are based on the discrete logarithm problem for which the computation of the addition of two points is central. In particular, one pays attention to two aspects. Obviously, the number of operations needed to compute the equations must be as small as possible. It appears that their domain of definition has also to be taken into account. Indeed, with the development of embedded cryptosystems, the theoretical resistance of the discrete logarithm problem is no longer sufficient to ensure the protocol security, we also have to deal with physical attacks. For instance the implementation of the usual formulæ on the Weierstraß model of an elliptic curve is vulnerable against side-channel attacks due to the use of different formulæ for a generic addition or a doubling (see [LM05] for a possible alternative on genus 2 curve cryptosystems).

In this paper we only consider this second problem. Lange and Ruppert [LR85] first considered complete sets of addition laws, *i.e.* for all P, Q in $A\left(\overline{\mathbb{k}}\right)$ there is an addition law defined at (P, Q) (see Definition 1.4). An addition law is said to be $\mathbb{k}$-complete if it is defined over $A \times A(\mathbb{k})$. Examples of $\mathbb{k}$-complete addition laws in genus 1 included the Edwards curves [Edw07, BL07] or the twisted Hessian curves [BKL09, FJ10]. See also [Koh11] for a large study of the structure of the space of addition laws on elliptic curves and the completeness of addition laws acted on by a torsion subgroup. Our aim is to find a $\mathbb{k}$-complete addition law on the Jacobian of genus 2 hyperelliptic curves.

In the first section we introduce the theta coordinates on the Jacobian of an hyperelliptic curve and explain the link with the classical Mumford coordinates. We then sketch the theory of addition laws. In section 2 we explain how to construct in practice an $\mathbb{F}_q$-complete addition law.

The authors acknowledge the financial support by grant ANR-09-BLAN-0020-01 from the French ANR and the AXA Research Fund for the PhD grant of the first author.

1.1. **Theta functions of level 4, Link with genus 2 curves.** In this subsection, we are interested in arithmetic aspects of the Jacobian of a genus 2 curve. We work over $\mathbb{C}$ to simplify the introduction and the use of theta functions. But the results remain true over a non binary finite field (see Remark 1.3). For the classical theory of theta functions, the reader is referred to [Mum83, Mum84]. Let Ω be an element of the Siegel half-space:

$$\left\{\Omega \in \mathrm{Mat}_{2\times 2}(\mathbb{C}),\ {}^t\Omega = \Omega,\ \Im(\Omega) > 0\right\},$$

the classical Riemann theta function is defined by

$$\vartheta\left(z, \Omega\right) = \sum_{n \in \mathbb{Z}^2} \exp\left(i\pi\, {}^t n \Omega n + 2i\pi\, {}^t n\, z\right).$$

For all elements a et b of $\mathbb{Q}^2$, the theta function with characteristics a, b is defined by

$$\begin{aligned}\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z, \Omega) &= \exp\left(i\pi\, {}^t a \Omega a + 2i\pi\, {}^t a\ (z+b)\right) \vartheta\left(z + \Omega a + b, \Omega\right) \\ &= \sum_{n\in\mathbb{Z}^2} \exp\left(i\pi\, {}^t(n+a)\Omega(n+a) + 2i\pi\, {}^t(n+a)\left(z+b\right)\right).\end{aligned}$$

The characteristics are considered modulo $\mathbb{Z}^2$ since for all α, β in $\mathbb{Z}^2$ we have

$$\vartheta\left[\begin{smallmatrix} a+\alpha \\ b+\beta \end{smallmatrix}\right](z, \Omega) = \vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z, \Omega) \exp(2i\pi\, {}^t a \beta)$$

We will consider theta functions of level 4 which means that the characteristics live in $\frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2$.

A classical result of Lefschetz states that the theta functions of level 4 give an embedding of $\mathbb{C}^2/\Omega\mathbb{Z}^2 + \mathbb{Z}^2$ into $\mathbb{P}^{15}(\mathbb{C})$. For a proof see [Mum70, p. 29].

For the sake of readability we use the following notations:

Notation 1.1 ([Gau07, Section 7.1])**.** We index the sixteen theta functions of level 4 as follow:

$$\begin{aligned}
\vartheta_1(z) &= \vartheta\left[\begin{smallmatrix} {}^t(0\ 0) \\ {}^t(0\ 0) \end{smallmatrix}\right](z,\Omega), & \vartheta_2(z) &= \vartheta\left[\begin{smallmatrix} {}^t(0\ 0) \\ {}^t(\frac12\ \frac12) \end{smallmatrix}\right](z,\Omega),\\
\vartheta_3(z) &= \vartheta\left[\begin{smallmatrix} {}^t(0\ 0) \\ {}^t(\frac12\ 0) \end{smallmatrix}\right](z,\Omega), & \vartheta_4(z) &= \vartheta\left[\begin{smallmatrix} {}^t(0\ 0) \\ {}^t(0\ \frac12) \end{smallmatrix}\right](z,\Omega),\\
\vartheta_5(z) &= \vartheta\left[\begin{smallmatrix} {}^t(\frac12\ 0) \\ {}^t(0\ 0) \end{smallmatrix}\right](z,\Omega), & \vartheta_6(z) &= \vartheta\left[\begin{smallmatrix} {}^t(\frac12\ 0) \\ {}^t(0\ \frac12) \end{smallmatrix}\right](z,\Omega),\\
\vartheta_7(z) &= \vartheta\left[\begin{smallmatrix} {}^t(0\ \frac12) \\ {}^t(0\ 0) \end{smallmatrix}\right](z,\Omega), & \vartheta_8(z) &= \vartheta\left[\begin{smallmatrix} {}^t(\frac12\ \frac12) \\ {}^t(0\ 0) \end{smallmatrix}\right](z,\Omega),\\
\vartheta_9(z) &= \vartheta\left[\begin{smallmatrix} {}^t(0\ \frac12) \\ {}^t(\frac12\ 0) \end{smallmatrix}\right](z,\Omega), & \vartheta_{10}(z) &= \vartheta\left[\begin{smallmatrix} {}^t(\frac12\ \frac12) \\ {}^t(\frac12\ \frac12) \end{smallmatrix}\right](z,\Omega),\\
\vartheta_{11}(z) &= \vartheta\left[\begin{smallmatrix} {}^t(0\ \frac12) \\ {}^t(0\ \frac12) \end{smallmatrix}\right](z,\Omega), & \vartheta_{12}(z) &= \vartheta\left[\begin{smallmatrix} {}^t(0\ \frac12) \\ {}^t(\frac12\ \frac12) \end{smallmatrix}\right](z,\Omega),\\
\vartheta_{13}(z) &= \vartheta\left[\begin{smallmatrix} {}^t(\frac12\ 0) \\ {}^t(\frac12\ 0) \end{smallmatrix}\right](z,\Omega), & \vartheta_{14}(z) &= \vartheta\left[\begin{smallmatrix} {}^t(\frac12\ \frac12) \\ {}^t(\frac12\ 0) \end{smallmatrix}\right](z,\Omega),\\
\vartheta_{15}(z) &= \vartheta\left[\begin{smallmatrix} {}^t(\frac12\ 0) \\ {}^t(\frac12\ \frac12) \end{smallmatrix}\right](z,\Omega), & \vartheta_{16}(z) &= \vartheta\left[\begin{smallmatrix} {}^t(\frac12\ \frac12) \\ {}^t(0\ \frac12) \end{smallmatrix}\right](z,\Omega).
\end{aligned}$$

Remark that the first ten theta functions are the even ones and the last six are the odd ones. For simplicity, we drop the Ω. The evaluation at 0 of these functions are called theta constants. We write them ϑ_i instead of $\vartheta_i(0)$.

Consider an hyperelliptic curve $\mathcal{C}$ of genus 2. Associated to this curve is its period matrix Ω which is an element of the Siegel half-space. The Abel-Jacobi map is an analytic isomorphism between $\mathrm{Jac}(\mathcal{C})$ and $\mathbb{C}^2/\Omega\mathbb{Z}^2+\mathbb{Z}^2$.

The Thomae formulæ [Tho70] (see also [Mum84, III.8]) link the 4th power of the theta constants with the parameters of the curve. Up to isomorphisms, we can recover the theta constants by taking well chosen roots [CR11]. Assume that the curve is in Rosenhain form:

$$\mathcal{C}: \quad y^2 = f(x) = x(x-1)(x-\lambda)(x-\mu)(x-\nu),$$

then the ordering $\{0,1,\lambda,\mu,\nu\}$ leads to the following relations:

$$\left(\frac{\vartheta_5}{\vartheta_1}\right)^4 = \frac{\mu}{\lambda\nu}, \qquad \left(\frac{\vartheta_7}{\vartheta_1}\right)^4 = \frac{\mu\,(\nu-1)\,(\lambda-\mu)\,\mu}{\nu\,(\mu-1)\,(\lambda-\nu)},$$

$$\left(\frac{\vartheta_3}{\vartheta_1}\right)^4 = \frac{\mu\,(\nu-1)\,(\lambda-1)}{\lambda\nu\,(\mu-1)}, \qquad \left(\frac{\vartheta_4}{\vartheta_1}\right)^4 = \frac{\mu\,(\lambda-1)\,(\nu-\mu)}{\lambda\,(\mu-1)\,(\nu-\lambda)}.$$

We can take a square root of the preceeding quotients in an arbitrary way. The other squares of theta constants of level 4 are given by the formulæ:

$$\vartheta_6^2 = \frac{1}{\nu}\frac{\vartheta_1^2\vartheta_4^2}{\vartheta_5^2}, \qquad \vartheta_8^2 = \frac{1}{\lambda}\frac{\vartheta_1^2\vartheta_7^2}{\vartheta_5^2},$$

$$\vartheta_2^2 = (\nu-1)\,\frac{\vartheta_5^2\vartheta_6^2}{\vartheta_3^2}, \qquad \vartheta_9^2 = (\lambda-1)\,\frac{\vartheta_5^2\vartheta_8^2}{\vartheta_3^2},$$

$$\vartheta_{10}^2 = \frac{\vartheta_1^2\vartheta_2^2 - \vartheta_3^2\vartheta_4^2}{\vartheta_8^2},$$

where arbitrary square roots can be taken. Note that we have to take a field extension to take these roots.

We need to have an explicit algebraic morphism between $\mathrm{Jac}(\mathcal{C})$ and the image in $\mathbb{P}^{15}(\mathbb{C})$ of the embedding by the theta functions of level 4. These formulæ can be found in [CR11] for the genus 2 case and in [Cos11] for the general case. Let $\{a_1,\ldots,a_5\}$ be the ordered roots of f and let

$$\eta_1 := {}^t\left[\tfrac{1}{2},0;0,0\right], \qquad \eta_2 := {}^t\left[\tfrac{1}{2},0;\tfrac{1}{2},0\right], \qquad \eta_3 := {}^t\left[0,\tfrac{1}{2};\tfrac{1}{2},0\right],$$

$$\eta_4 := {}^t\left[0,\tfrac{1}{2};\tfrac{1}{2},\tfrac{1}{2}\right], \qquad \eta_5 := {}^t\left[0,0;\tfrac{1}{2},\tfrac{1}{2}\right], \qquad \eta_\infty := {}^t\left[0,0;0,0\right].$$

For a subset S in $\{1,\ldots,5,\infty\}$, we set

$$\eta_S = \sum_{i\in S}\eta_i,$$

and we define η'_S and η''_S to be the first and second part of η_S. This notation comes from the fact that if we denote ∞ the point at infinity of $\mathcal{C}$ and A_i the point with affine coordinate equal to $(a_i,0)$ for $i=1,\ldots,5$ and $A_\infty=\infty$, then the divisor $\sum_{i\in S}(A_i) - \#S(\infty)$ is mapped to $\Omega\eta'_S+\eta''_S$ by the Abel-Jacobi map.

Let $\circ$ denote the symmetric difference of two sets. All theta functions of level 4 can be written as $\vartheta\left[\eta_{\mathcal{U}\circ V}\right]$ with $\mathcal{U} := \{1,3,5\}$ and a subset V of $\{1,\ldots,5\}$ of odd cardinality. For each such subset, Van Wamelen [vW98] defines the function $t_V(z)$ to be $t_V(z) = f_V \vartheta\left[\eta_{\mathcal{U}\circ V}\right](z)$, where f_V is a constant which is $f_V = \vartheta[0]/\vartheta\left[\eta_{\mathcal{U}\circ V}\right]$ for the even functions (i.e. $\#V = 3$) and which is, for the others,

$$
\begin{aligned}
f_1 &= \frac{-1}{\sqrt{a_2-a_1}} \frac{\vartheta_1\vartheta_5\vartheta_6\vartheta_8}{\vartheta_2\vartheta_3\vartheta_9\vartheta_{10}}, & f_2 &= \frac{-1}{\sqrt{a_2-a_1}} \frac{\vartheta_5\vartheta_6\vartheta_8}{\vartheta_4\vartheta_7\vartheta_{10}},\\
f_3 &= \frac{-1}{\sqrt{a_2-a_1}} \frac{\vartheta_1\vartheta_6}{\vartheta_2\vartheta_4}, & f_4 &= \frac{1}{\sqrt{a_2-a_1}} \frac{\vartheta_5}{\vartheta_3},\\
f_5 &= \frac{-1}{\sqrt{a_2-a_1}} \frac{\vartheta_1\vartheta_8}{\vartheta_7\vartheta_9}, & f_\emptyset &= f_{\{1,2,3,4,5\}} = \frac{-1}{\sqrt{a_2-a_1}^3} \frac{\vartheta_5^2\vartheta_6^2\vartheta_8^2}{\vartheta_2\vartheta_3\vartheta_4\vartheta_7\vartheta_9\vartheta_{10}}.
\end{aligned}
$$

The following theorem is a sum up of results from Van Wamelen.

Theorem 1.2. *Let $D = (P_1) + (P_2) - 2(\infty)$ be a non theta divisor which corresponds to a vector $z \in \mathbb{C}^2/(\Omega\mathbb{Z}^2 + \mathbb{Z}^2)$. Let (x_i, y_i) be the coordinates of the point P_i, $i = 1, 2$. Write (u, v) for the Mumford's polynomials of D. For $k \in \{1, \dots, 5\}$, and l, m two distinct elements of $\{1, \dots, 5\} \setminus \{k\}$ we have*

$$
u(a_k) = \frac{t_k^2(z)}{t_\emptyset^2(z)}, \qquad v(a_k) = \frac{Y_{k,m} - Y_{k,l}}{a_l - a_m},
$$

$$
Y_{l,m} := \frac{y_1(x_2-a_l)(x_2-a_m) - y_2(x_1-a_l)(x_1-a_m)}{x_2-x_1} = c_{1,2} \frac{t_l(z)t_m(z)t_{\{l,m\}}(z)}{t_\emptyset^3(z)},
$$

$$
Y := y_1y_2 = \prod_{l=1}^{5} \frac{t_l(z)}{t_\emptyset(z)},
$$

where $c_{1,2}$ is just a sign ± 1.

By evaluating u at the roots of f, we obtain formulæ for computing all the $\vartheta_i(z)^2/\vartheta_{16}(z)^2$ with $1 \leq i \leq 16$. To get the theta functions of level 4, we will use the doubling formulæ [Gau07]:

$$
4\vartheta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](2z)\,\vartheta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right]\vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]^2 = \sum_{\alpha,\beta\in\frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2} \exp\left(-4i\pi{}^t a\beta\right)\vartheta\left[\begin{smallmatrix}a+\alpha\\b+\beta\end{smallmatrix}\right](z)^2\,\vartheta\left[\begin{smallmatrix}\alpha\\\beta\end{smallmatrix}\right](z)^2,
$$

$$
\begin{aligned}
&4\vartheta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](2z)\,\vartheta\left[\begin{smallmatrix}a\\0\end{smallmatrix}\right]\vartheta\left[\begin{smallmatrix}0\\b\end{smallmatrix}\right]\vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right] = \\
&\quad \sum_{\alpha,\beta\in\frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2} \exp\left(-4i\pi{}^t a\beta\right)\vartheta\left[\begin{smallmatrix}a+\alpha\\b+\beta\end{smallmatrix}\right](z)\,\vartheta\left[\begin{smallmatrix}a+\alpha\\\beta\end{smallmatrix}\right](z)\,\vartheta\left[\begin{smallmatrix}\alpha\\b+\beta\end{smallmatrix}\right](z)\,\vartheta\left[\begin{smallmatrix}\alpha\\\beta\end{smallmatrix}\right](z).
\end{aligned}
$$

The first formula allows to recover the even theta functions. For the odd theta functions, we will use the second formula. The products on the right side can be expressed in terms of the constants f_V and the functions $Y_{l,m}$, Y and $u(a_i)$. Since we need to divide by some $u(a_i)$, we make the hypothesis that the divisor is not of 2-torsion. For instance, the second formula gives

$$\begin{aligned}\vartheta_{16}(2z)\vartheta_1\vartheta_4\vartheta_8 &= \vartheta_1(z)\vartheta_4(z)\vartheta_8(z)\vartheta_{16}(z) - \vartheta_9(z)\vartheta_{12}(z)\vartheta_{13}(z)\vartheta_{15}(z)\\ &\quad + \vartheta_5(z)\vartheta_6(z)\vartheta_7(z)\vartheta_{11}(z) - \vartheta_2(z)\vartheta_3(z)\vartheta_{10}(z)\vartheta_{14}(z),\\ \vartheta_{16}(2z)\vartheta_1\vartheta_4\vartheta_8 &= \frac{t_{2,4}(z)t_{2,3}(z)t_{3,4}(z)t_\emptyset(z)}{f_{2,4}f_{2,3}f_{3,4}f_\emptyset} + \frac{t_{1,5}(z)t_2(z)t_4(z)t_3(z)}{f_{1,5}f_2f_4f_3}\\ &\quad + \frac{t_{3,5}(z)t_{4,5}(z)t_{2,5}(z)t_1(z)}{f_{3,5}f_{4,5}f_{2,5}f_1} + \frac{t_{1,3}(z)t_{1,4}(z)t_{1,2}(z)t_5(z)}{f_{1,3}f_{1,4}f_{1,2}f_5},\\ \frac{\vartheta_{16}(2z)\vartheta_1\vartheta_4\vartheta_8}{t_\emptyset^4(z)} &= \frac{Y_{2,4}Y_{2,3}Y_{3,4}}{u(a_2)u(a_3)u(a_4)}\frac{1}{f_{2,4}f_{2,3}f_{3,4}f_\emptyset} + \frac{Y_{1,5}Y}{u(a_1)u(a_5)}\frac{1}{f_{1,5}f_2f_3f_4}\\ &\quad + \frac{Y_{2,5}Y_{3,5}Y_{4,5}Y}{u(a_2)u(a_3)u(a_4)u(a_5)^2}\frac{1}{f_{2,5}f_{3,5}f_{4,5}f_1}\\ &\quad + \frac{Y_{1,2}Y_{1,3}Y_{1,4}Y}{u(a_1)^2u(a_2)u(a_3)u(a_4)}\frac{1}{f_{1,2}f_{1,3}f_{1,4}f_5}.\end{aligned}$$

Remark 1.3. Although we have defined our theta function over $\mathbb{C}$, our results apply to other fields (of characteristic different from 2). To prove this over a finite field (the relevant case in cryptography), we can use Lefschetz's principle and reduction to prove all the results for ordinary varieties. In general we can always use the algebraic theory of theta functions [Mum66, Mum67a, Mum67b].

1.2. **Addition laws.** Now, we focus on the notion of addition law. Let $\Bbbk$ be a field and $A/\Bbbk$ be an abelian variety of dimension g. We assume an embedding of A in some projective space $\mathbb{P}^r$ is fixed and given by a very ample line bundle $\mathcal{L} = \mathcal{L}(D)$ for D an effective divisor. We denote by $\iota : A \hookrightarrow \mathbb{P}^r$ the corresponding morphism and also assume in the sequel that this embedding is projectively normal. Recall that by definition this means that for every $n \geq 1$ the restriction map $H^0\big(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(n)\big) \to H^0(A, \mathcal{L}^n)$ is surjective. This is the case in the classical settings where $\mathcal{L} = \mathcal{L}_0^{n_0}$ with $\mathcal{L}_0$ an ample line bundle and $n_0 \geq 3$ [BL04, p.187].

Let I_1 (resp. I_2) be the homogeneous ideal in $\Bbbk[X_0, \ldots, X_r]$ (resp. in $\Bbbk[Y_0, \ldots, Y_r]$) defined by A. The *group law*

$$\mu : A \times A \to A, (X, Y) \mapsto X + Y$$

can be locally described by bihomogenous polynomials. More precisely, an *addition law* $\mathfrak{p}$ of bidegree (m, n) on $\iota(A) \subset \mathbb{P}^r$ is the data of $r+1$ polynomials

$$p_0, \ldots, p_r \in \Bbbk[X_0, \ldots, X_r]/I_1 \otimes \Bbbk[Y_0, \ldots, Y_r]/I_2,$$

not all zero, bihomogeneous of degree m in $X_0, \ldots, X_r$ and degree n in $Y_0, \ldots, Y_r$ such that we have

$$\iota \circ \mu\,(X, Y) = \Big(p_0\big(\iota(X), \iota(Y)\big) : \ldots : p_r\big(\iota(X), \iota(Y)\big)\Big)$$

for all points $(X, Y) \in A \times A\left(\overline{\Bbbk}\right)$ where these polynomials are not all zero. The set of points where an addition law is not defined is called its *exceptional subset.* It will be convenient for our purpose in Section 2 to use the structure of $\Bbbk$-vector space of addition laws having fixed bidegree. In this sense we need to define the *zero addition law* (independent of the bidegree) given by zero polynomials. It is denoted by 0 and its exceptional subset is $A \times A\left(\overline{\mathbb{k}}\right)$.

In this paper we are interested in the construction of a single addition law which describes the group morphism μ on $A \times A\,(\mathbb{k})$ where $\mathbb{k}$ is a non binary finite field and $A/\mathbb{k}$ an abelian surface (*i.e.* the Jacobian of a genus 2 curve) embedded in $\mathbb{P}^{15}$.

Definition 1.4. A set S of addition laws is said to be $\mathbb{k}$-*complete* if for any point $(X, Y) \in A \times A\,(\mathbb{k})$ there is an addition law in S defined on an open subset containing (X, Y). The set S is said to be *complete* if the previous property is true over $\overline{\mathbb{k}}$. If $S = \{\mathfrak{p}\}$ is a singleton, we say the addition law $\mathfrak{p}$ is $\mathbb{k}$-*complete* (or *complete* when $\mathbb{k} = \overline{\mathbb{k}}$).

Given $m, n \geq 2$ the following proposition interprets the addition laws of bidegree (m, n) as global sections of a certain line bundle $\mathcal{M}_{m,n}$. A more explicit description of this link can be found in [AKR11, Section 2].

Proposition 1.5 ([LR85, Lemma 2.1]). *Let $\pi_1, \pi_2 : A \times A \to A$ be the projection maps on the first and second factor. There is an addition law (respectively a complete set of addition laws) of bidegree (m, n) on A with respect to the embedding in $\mathbb{P}^r$ determined by $\mathcal{L}$ if and only if*

$$H^0(A \times A, \mathcal{M}_{m,n}) \neq 0$$

(respectively the linear system $\mid \mathcal{M}_{m,n} \mid$ is base point-free), where

$$\mathcal{M}_{m,n} = \mu^*\mathcal{L}^{-1} \otimes \pi_1^*\mathcal{L}^m \otimes \pi_2^*\mathcal{L}^n.$$

The next lemma is specific to the *biquadratic* case (m=n=2) and gives a nice description of the line bundle $\mathcal{M}_{2,2}$ which have no equivalent statement for others bidegrees that we currently know.

Lemma 1.6 ([LR85, Propositions 2.2 and 2.3]). *Let $\mathcal{L}$ be an ample line bundle on A and $\delta : A \times A \to A$ be the difference map $(X, Y) \mapsto X - Y$.*

1) if $\mathcal{L}$ is not symmetric then $H^0(A \times A, \mathcal{M}_{2,2}) = 0$.
2) if $\mathcal{L}$ is symmetric, then $\mathcal{M}_{2,2} = \delta^*\mathcal{L}$. Moreover $\mathcal{M}_{2,2}$ is base point-free and $h^0(A \times A, \mathcal{M}_{2,2}) = h^0(A, \mathcal{L})$.

We end this section with the statement of the existence of the addition law we want to construct.

Proposition 1.7 ([AKR11, Statement and Proof of Theorem 4.8]). *Let $\mathbb{k} = \mathbb{F}_q, q \geq 7$, be a finite field and $\mathcal{C}/\mathbb{F}_q$ be a genus 2 curve. There exists an $\mathbb{F}_q$-complete biquadratic addition law on the embedding of* $\mathrm{Jac}(\mathcal{C})$ *in $\mathbb{P}^{15}$ by 4Θ. Moreover its exceptional subset is explicitely determined.*

2. Construction

2.1. **A basis of biquadratic addition laws on Jac($\mathcal{C}$) $\hookrightarrow$ $\mathbf{P^{15}}$.** Riemann's addition formulæ are widely known and common in the litterature. We use the general formulæ given by Baily [Bai62] and apply it to obtain the following formulæ for theta function of level 4.

Proposition 2.1 ([Bai62, Section 2.2, Formulæ (9)]). *Let $a_k, b_l \in \frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2$, $k, l = 1, \dots, 4$. Assume we have*

$$-a_1 + a_2 + a_3 + a_4 = 2a, \qquad -b_1 + b_2 + b_3 + b_4 = 2b$$

with a and b in $\frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2$ then for all z_1, z_2 in $\mathbb{C}^2$ we have

$$4\,\vartheta\begin{bmatrix} a_1 \\ b_1 \end{bmatrix}(z_1+z_2)\,\vartheta\begin{bmatrix} a_2 \\ b_2 \end{bmatrix}(z_1-z_2)\,\vartheta\begin{bmatrix} a_3 \\ b_3 \end{bmatrix}(0)\,\vartheta\begin{bmatrix} a_4 \\ b_4 \end{bmatrix}(0) =$$
$$\sum_{\alpha,\beta\in\frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2} \vartheta\begin{bmatrix} a_1+a+\alpha \\ b_1+b+\beta \end{bmatrix}(z_2)\,\vartheta\begin{bmatrix} a_2-a+\alpha \\ b_2-b+\beta \end{bmatrix}(z_2)\,\vartheta\begin{bmatrix} a_3-a+\alpha \\ b_3-b+\beta \end{bmatrix}(z_1)\,\vartheta\begin{bmatrix} a_4-a+\alpha \\ b_4-b+\beta \end{bmatrix}(z_1).$$

For all a_1, a_2, b_1, b_2 in $\frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2$, there exists a_3, a_4, b_3, b_4 in $\frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2$ verifying the condition of the proposition and such that the constant $\vartheta\begin{bmatrix} a_3 \\ b_3 \end{bmatrix}\ \vartheta\begin{bmatrix} a_4 \\ b_4 \end{bmatrix}$ is non zero. We now go back to notation 1.1.

Remark 2.2. The embedding Jac($\mathcal{C}$) $\hookrightarrow \mathbb{P}^{15}$ is given by the line bundle $\mathcal{L} = \mathcal{L}(4\Theta)$. From now on we cosider the functions ϑ_i as global sections of this line bundle.

Remark 2.3. The formulæ above express for $i, j = 1, \dots, 16$ the product $\vartheta_i(z_1+z_2)\vartheta_j(z_1-z_2)$ as a biquadratic bihomogeneous polynomial in the level 4 theta functions $\big(\vartheta_1(z_1), \dots, \vartheta_{16}(z_1)\big)$ and $\big(\vartheta_1(z_2), \dots, \vartheta_{16}(z_2)\big)$. Note also that they are defined over the field of definition of the theta constants.

Next, fixing the index j, if z_1, z_2 are such that $\vartheta_j(z_1-z_2) \neq 0$, there exists biquadratic bihomogeneous polynomials $p_{i,j}$ such that

$$\vartheta_i(z_1+z_2)\vartheta_j(z_1-z_2) = p_{i,j}\big((\vartheta_1(z_1), \dots, \vartheta_{16}(z_1)), (\vartheta_1(z_2), \dots, \vartheta_{16}(z_2))\big).$$

This allows us to construct an addition law $\mathfrak{p}_j = (p_{1,j}, \dots, p_{16,j})$ defined outside the exceptional subset $\delta^*(\vartheta_j)_0$. Indeed, let

$$X_k = \big(\vartheta_1(z_k) : \dots : \vartheta_{16}(z_k)\big) \in \mathrm{Jac}(\mathcal{C}), \quad k = 1, 2,$$

be two points such that $X_1 - X_2 \notin (\vartheta_j)_0$ (or satisfying $\vartheta_j(z_1-z_2) \neq 0$). We have

$$\begin{aligned} \iota \circ \mu\,(X_1, X_2) &= \big(\vartheta_1(z_1+z_2) : \dots : \vartheta_{16}(z_1+z_2)\big) \\ &= \big(\vartheta_j(z_1-z_2)\vartheta_1(z_1+z_2) : \dots : \vartheta_j(z_1-z_2)\vartheta_{16}(z_1+z_2)\big) \\ &= \mathfrak{p}_j(X_1, X_2). \end{aligned}$$

Notation 2.4. For $j = 1, \dots, 16$, we denote $\mathfrak{p}_j$ the addition law on Jac($\mathcal{C}$) whose exceptional subset is $\delta^*(\vartheta_j)_0$ presented above.

Clearly the set of addition laws $\{\mathfrak{p}_1, \dots, \mathfrak{p}_{16}\}$ is complete. Moreover we have the following proposition:

Proposition 2.5. *Let $\mathcal{C}$ be a genus 2 curve. The set $\{\mathfrak{p}_1, \dots, \mathfrak{p}_{16}\}$ is a basis of the set of biquadratic addition laws on* $\mathrm{Jac}(\mathcal{C}) \hookrightarrow \mathbb{P}^{15}$.

Proof. We have $\dim_{\mathbb{k}}\big(\mathcal{L}(4\Theta)\big) = 16$, so by Lemma 1.6 case 2) we only need to show that the family is free. Let assume there exists a linear relation

$$\sum \lambda_j \mathfrak{p}_j = 0. \tag{1}$$

Let denote by O_J the neutral element of $\mathrm{Jac}(\mathcal{C})$, then for all $X = \big(\vartheta_1(z) : \dots : \vartheta_{16}(z)\big) \in \mathrm{Jac}(\mathcal{C})$, the relation $\sum \lambda_j \mathfrak{p}_j(X, O_J) = 0$ gives $\sum \lambda_j p_{i,j}(X, O_J) = 0$ for all $i = 1, \dots, 16$. Moreover there exists a k_0 such that $\vartheta_{k_0}(z) \neq 0$, so

$$0 = \sum \lambda_j p_{k_0,j}(X, O_J) = \sum \lambda_j \vartheta_{k_0}(z+0)\vartheta_j(z-0) = \vartheta_{k_0}(z) \sum \lambda_j \vartheta_j(z).$$

The dependance in k_0 being eliminated we finally get

$$\sum \lambda_j \vartheta_j = 0$$

which is wrong because the family $\{\vartheta_j,\ j = 1, \dots, 16\}$ is a basis for the theta functions of level 4. Hence the assumption of the existence of the relation (1) is not true, and $\{\mathfrak{p}_1, \dots, \mathfrak{p}_{16}\}$ is a free family. □

2.2. **Idea of the construction.** From now on and without mention of the contrary we assume that $\mathbb{k} = \mathbb{F}_q$, where q is greater than 7 and is odd. In the previous subsection we built a basis for the space of addition laws we are interested in. We want here to construct the addition law announced in Proposition 1.7. We denote it $\mathfrak{p}$. According to Lemma 1.6 case 2) its exceptional subset is of the form $\delta^* D$ with $D \in \mathrm{Div}(\mathrm{Jac}(\mathcal{C}))$ and $D \sim 4\Theta$. We recall below the expression of D but suppose here we know it. Our aim is to find a projective solution $(\lambda_1 : \dots : \lambda_{16})$ for the relation

$$\mathfrak{p} = \sum \lambda_j \mathfrak{p}_j \tag{2}$$

using an interpolation method. To get this, let $X \in D$. As we want $\mathfrak{p}$ not to be defined on $\delta^* D$, in particular at (X, O_J), we search for solutions of the linear system

$$0 = \sum \lambda_j \mathfrak{p}_j(X, O_J).$$

Varying $X \in D$ we expect to get a linear system of rank 15. Note that the solution is projective because the exceptional subset of an addition law defines it up to scalar multiplications.

We recall here the construction of the divisor $D \in \mathrm{Div}_{\mathbb{k}}\big(\mathrm{Jac}(\mathcal{C})\big)$ introduced above. The assumption $q \geq 7$ implies the existence of a degree 4 closed point of the form $\big\{P_0, P_0^\sigma, \overline{P_0}, \overline{P_0}^\sigma\big\}$, with σ the Frobenius over $\mathbb{F}_q$. Let define $\alpha_0 := (P_0) + (P_0^\sigma) - 2(\infty)$ and for $l = 0, 1, 2$, $\alpha_{l+1} := \alpha_l^\sigma$. Then the divisor $D = \sum \Theta_{\alpha_l}$ has the desired properties to induce an $\mathbb{F}_q$-complete biquadratic addition law (namely it is $\mathbb{k}$-rational without $\mathbb{k}$-rational points and linearly equivalent to 4Θ [AKR11]), where Θ_{α_l}, $l = 0, \dots, 3$, is the translation by α_l of the theta divisor Θ on $\mathrm{Jac}(\mathcal{C})$. In the sequel, D is taken of this form.

The following proposition allows to avoid the computation of the last six coefficients (the odd ones) and then to reduce significantly the running time. Recall that the addition laws $\mathfrak{p}_j$ have $\delta^*(\vartheta_j)_0$ as exceptional subset (Notation 2.4).

Theorem 2.6. *Assume* $\Bbbk = \mathbb{F}_q$*, with* $q \geq 7$ *and* $(2, q) = 1$*. Let* $\mathfrak{p}$ *be the addition law introduced above and* $\mathfrak{p} = \sum \lambda_j \mathfrak{p}_j$ *the desired linear relation. We have* $\lambda_{11} = \cdots = \lambda_{16} = 0$*.*

Proof. Remark that by construction for all $X \in D$ we have $-X \in D$. We have

$$\forall X \in D, \qquad \mathfrak{p}(X, O_J) = \mathfrak{p}(O_J, X) = 0. \tag{3}$$

Using the parity of the theta functions ϑ_j we get that the second equality becomes

$$\mathfrak{p}(O_J, X) = \sum \lambda_j \mathfrak{p}_j(O_J, X) = \sum_{j=1}^{10} \lambda_j \mathfrak{p}_j(X, O_J) - \sum_{j=11}^{16} \lambda_j \mathfrak{p}_j(X, O_J).$$

We use it in the formulæ (3) and are led to consider the two next equations

$$\forall X \in D, \qquad \sum_{j=1}^{10} \lambda_j \mathfrak{p}_j(X, O_J) = 0, \text{ and } \sum_{j=11}^{16} \lambda_j \mathfrak{p}_j(X, O_J) = 0. \tag{4}$$

Let us define the two biquadratic addition laws appearing here

$$\mathfrak{p}_1 := \sum_{j=1}^{10} \lambda_j \mathfrak{p}_j, \qquad \mathfrak{p}_2 := \sum_{j=11}^{16} \lambda_j \mathfrak{p}_j.$$

Let $\delta^* D_1, \delta^* D_2$, with D_1, D_2 be two divisors on $\mathrm{Jac}(\mathcal{C})$, be their respective exceptional subsets. We want to prove that $\mathfrak{p}_2$ is zero. They verify for $k = 1, 2$ either $D_k \sim 4\Theta$ or $\mathfrak{p}_k = 0$. The formulæ (4) imply $D \leq D_k$, hence either $D = D_k$ $\big($and then $\mathfrak{p}_k = \lambda \mathfrak{p}$ for some $\lambda \in \overline{\mathbb{F}_q}\big)$ or $\mathfrak{p}_k = 0$ for $k = 1, 2$. But $\mathfrak{p}_2(O_J, O_J) = 0$ because the theta constants involved are zero, moreover the $\Bbbk$-rational point (O_J, O_J) is not an element of $\delta^* D$, hence the second addition law $\mathfrak{p}_2$ is zero. A fortiori $\lambda_{11} = \cdots = \lambda_{16} = 0$ and $\mathfrak{p} = \mathfrak{p}_1$. □

Remark 2.7. We did not get more information on the coefficients λ_j using that $\mathfrak{p}(-X, O_J) = \mathfrak{p}(O_J, -X) = 0$ for $X \in D$.

2.3. **Numerical results.** AVIsogenies is a Magma package for working with genus 2 curves (and more generally with abelian varieties) using theta functions[1]. Using some already implemented functions, we wrote codes to compute the coefficients λ_i given an hyperelliptic curves. This code is now part of the AVIsogenies package.

Example 2.8. Consider the curve

$$\mathcal{C}: \quad y^2 = f(x) = x^5 + 5782x^4 + 2517x^3 + 2312x^2 + 9402x$$

defined over $\mathbb{F}_{10007}$. The non-zero associated theta constants are

$$\begin{array}{llll} \vartheta_1 = 1, & \vartheta_2 = 5242, & \vartheta_3 = 7727, & \vartheta_4 = 678, \\ \vartheta_5 = 3926, & \vartheta_6 = 7092, & \vartheta_7 = 5628, & \vartheta_8 = 7556, \\ \vartheta_9 = 3666, & \vartheta_{10} = 904. & & \end{array}$$

[1]It can be found at `http://avisogenies.gforge.inria.fr/`.

Let

$$K = \mathbb{F}_{10007}[X]/X^2 + 1 \simeq \mathbb{F}_{10007^2}$$

and $x_0 = 8310 + 2164\sqrt{-1}$. The point $P_0 = \left(x_0, \sqrt{f(x_0)}\right)$ is a point of the curve $\mathcal{C}\left(\mathbb{F}_{10007^4}\right)$ which doesn't belong to $\mathcal{C}\left(\mathbb{F}_{10007^2}\right)$. The corresponding non-zero λ_i are given by

$$\begin{array}{llll} \lambda_1 = 1, & \lambda_2 = 6924, & \lambda_3 = 1940, & \lambda_4 = 9380, \\ \lambda_5 = 5155, & \lambda_6 = 1278, & \lambda_7 = 7239, & \lambda_8 = 1761, \\ \lambda_9 = 6859, & \lambda_{10} = 5891. & & \end{array}$$

This compution took less than a minute. It is possible to check that the addition law is $\mathbb{F}_{10007}$-complete by an exhaustive computation. Note that it is enough to check $\mathfrak{p}(D, O_J) = D$ for all divisor $\pm D$ of $\mathrm{Jac}(\mathcal{C})\left(\mathbb{F}_{10007}\right)$. This verification took almost a week.

Concerning the efficiency of these addition laws, it is clearly not to their advantage when we look at $\mathfrak{p}_1$ expressed below in Example A.1. One verifies in this appendix that the total cost to compute the desired addition law $\mathfrak{p}$ is

$$736\mathbf{m} + 32\mathbf{s} + 124\mathbf{m}_\vartheta,$$

where $\mathbf{m}$ denotes a multiplication, $\mathbf{s}$ is for a squaring and $\mathbf{m}_\vartheta$ represents a multiplication by a coefficient that only depends on the theta constants, which can be precomputed.

In comparison, the classical representation of points in $\mathrm{Jac}(\mathcal{C})$ as elements of the divisor class group of $\mathcal{C}$ and the use of Mumford's representation and Cantor's algorithm provides extremly cheaper costs, *e.g.* $47\mathbf{m} + 4\mathbf{s}$ for a general addition in even characteristic (see [Lan05]). There also exist pseudo-addition laws on the Kummer surface of the variety that can be computed much faster [Duq04, Gau07].

Appendix A. Operation count

We start by computing the addition laws $\mathfrak{p}_i$, $i = 1, \ldots, 10$ and then use the Formula (2). We remark that there are eight bihomogeneous monomials appearing in $\mathfrak{p}_{i,j}, i \neq j$. Also, $\mathfrak{p}_{i,j}$ and $\mathfrak{p}_{j,i}$ are defined by the same monomials up to a sign; this is the case for the $\mathfrak{p}_{i,i}$, $i = 1, \ldots, 10$, too. Now we describe the cost of their computation. We do not take into account additions or sign changes costs. Given two points $\left(X_1 : \cdots : X_{16}\right)$ and $\left(Y_1 : \cdots : Y_{16}\right)$ we first compute all the products X_iX_j and Y_iY_j, this costs $240\mathbf{m} + 32\mathbf{s}$ and the products $X_iX_jY_iY_j$ in $256\mathbf{m}$. These monomials are exactly the one included in the ten first polynomials of the addition laws $\mathfrak{p}_i$ (see Example A.1), so the polynomials $\mathfrak{p}_{i,i}$ are calculated in $10\mathbf{m}_\vartheta$ and the $\mathfrak{p}_{i,j}$, $1 \le i, j \le 10$, in $\binom{10}{2}\mathbf{m}_\vartheta = 45\mathbf{m}_\vartheta$. For the remaining $\mathfrak{p}_{i,j}$ with $11 \le i \le 16$ and $1 \le j \le 10$, we point out that if a monomial $X_{i_0}X_{j_0}Y_{k_0}Y_{l_0}$ appears, so does $X_{k_0}X_{l_0}Y_{i_0}Y_{j_0}$ with the same sign. We use then the relation

$$X_{i_0}X_{j_0}Y_{k_0}Y_{l_0} + X_{k_0}X_{l_0}Y_{i_0}Y_{j_0} = \\ \left(X_{i_0}X_{j_0} + X_{k_0}X_{l_0}\right)\left(Y_{i_0}Y_{j_0} + Y_{k_0}Y_{l_0}\right) - X_{i_0}X_{j_0}Y_{i_0}Y_{j_0} - X_{k_0}X_{l_0}Y_{k_0}Y_{l_0}$$

to calculate each $\mathfrak{p}_{i,j}$ with $4\mathbf{m}+1\mathbf{m}_\vartheta$. Hence, the ten addition laws $\mathfrak{p}_1,\dots,\mathfrak{p}_{10}$ can be computed in $736\mathbf{m}+32\mathbf{s}+115\mathbf{m}_\vartheta$. Finally the computation of the $\Bbbk$-complete addition law $\mathfrak{p}$ requires the 9 multiplications by the coefficients λ_i which also can be precomputed, so we count them as $9\mathbf{m}_\vartheta$.

Example A.1. As an illustrative exemple, we present the addition law $\mathfrak{p}_1$.

$$\mathfrak{p}_{1,1}=\frac{1}{\vartheta_1^2}\big(X_1^2Y_1^2+X_2^2Y_2^2+X_3^2Y_3^2+X_4^2Y_4^2+X_5^2Y_5^2+X_6^2Y_6^2+X_7^2Y_7^2+X_8^2Y_8^2+X_9^2Y_9^2+X_{10}^2Y_{10}^2+X_{11}^2Y_{11}^2+X_{12}^2Y_{12}^2+X_{13}^2Y_{13}^2+X_{14}^2Y_{14}^2+X_{15}^2Y_{15}^2+X_{16}^2Y_{16}^2\big),$$

$$\mathfrak{p}_{2,1}=\frac{2}{\vartheta_1\vartheta_2}\big(X_1X_2Y_1Y_2+X_3X_4Y_3Y_4+X_5X_{15}Y_5Y_{15}+X_6X_{13}Y_6Y_{13}+X_7X_{12}Y_7Y_{12}+X_8X_{10}Y_8Y_{10}+X_9X_{11}Y_9Y_{11}+X_{14}X_{16}Y_{14}Y_{16}\big),$$

$$\mathfrak{p}_{3,1}=\frac{2}{\vartheta_1\vartheta_3}\big(X_1X_3Y_1Y_3+X_2X_4Y_2Y_4+X_5X_{13}Y_5Y_{13}+X_6X_{15}Y_6Y_{15}+X_7X_9Y_7Y_9+X_8X_{14}Y_8Y_{14}+X_{11}X_{12}Y_{11}Y_{12}+X_{10}X_{16}Y_{10}Y_{16}\big),$$

$$\mathfrak{p}_{4,1}=\frac{2}{\vartheta_1\vartheta_4}\big(X_1X_4Y_1Y_4+X_2X_3Y_2Y_3+X_5X_6Y_5Y_6+X_7X_{11}Y_7Y_{11}+X_8X_{16}Y_8Y_{16}+X_9X_{12}Y_9Y_{12}+X_{10}X_{14}Y_{10}Y_{14}+X_{13}X_{15}Y_{13}Y_{15}\big),$$

$$\mathfrak{p}_{5,1}=\frac{2}{\vartheta_1\vartheta_5}\big(X_1X_5Y_1Y_5-X_2X_{15}Y_2Y_{15}-X_3X_{13}Y_3Y_{13}+X_4X_6Y_4Y_6+X_7X_8Y_7Y_8-X_9X_{14}Y_9Y_{14}-X_{10}X_{12}Y_{10}Y_{12}+X_{11}X_{16}Y_{11}Y_{16}\big),$$

$$\mathfrak{p}_{6,1}=\frac{2}{\vartheta_1\vartheta_6}\big(X_1X_6Y_1Y_6-X_2X_{13}Y_2Y_{13}-X_3X_{15}Y_3Y_{15}+X_4X_5Y_4Y_5+X_7X_{16}Y_7Y_{16}+X_8X_{11}Y_8Y_{11}-X_9X_{10}Y_9Y_{10}-X_{12}X_{14}Y_{12}Y_{14}\big),$$

$$\mathfrak{p}_{7,1}=\frac{2}{\vartheta_1\vartheta_7}\big(X_1X_7Y_1Y_7-X_2X_{12}Y_2Y_{12}+X_3X_9Y_3Y_9-X_4X_{11}Y_4Y_{11}+X_5X_8Y_5Y_8-X_6X_{16}Y_6Y_{16}-X_{10}X_{15}Y_{10}Y_{15}+X_{13}X_{14}Y_{13}Y_{14}\big),$$

$$\mathfrak{p}_{8,1}=\frac{2}{\vartheta_1\vartheta_8}\big(X_1X_8Y_1Y_8+X_2X_{10}Y_2Y_{10}-X_3X_{14}Y_3Y_{14}-X_4X_{16}Y_4Y_{16}+X_5X_7Y_5Y_7-X_6X_{11}Y_6Y_{11}-X_9X_{13}Y_9Y_{13}+X_{12}X_{15}Y_{12}Y_{15}\big),$$

$$\mathfrak{p}_{9,1}=\frac{2}{\vartheta_1\vartheta_9}\big(X_1X_9Y_1Y_9-X_2X_{11}Y_2Y_{11}+X_3X_7Y_3Y_7-X_4X_{12}Y_4Y_{12}+X_5X_{14}Y_5Y_{14}-X_6X_{10}Y_6Y_{10}+X_8X_{13}Y_8Y_{13}-X_{15}X_{16}Y_{15}Y_{16}\big),$$

$$\mathfrak{p}_{10,1}=\frac{2}{\vartheta_1\vartheta_{10}}\big(X_1X_{10}Y_1Y_{10}+X_2X_8Y_2Y_8-X_3X_{16}Y_3Y_{16}-X_4X_{14}Y_4Y_{14}+X_5X_{12}Y_5Y_{12}-X_6X_9Y_6Y_9+X_7X_{15}Y_7Y_{15}-X_{11}X_{13}Y_{11}Y_{13}\big),$$

$$\mathfrak{p}_{11,1}=\frac{2}{\vartheta_8\vartheta_6}\big(X_1X_{11}Y_6Y_8+X_2X_9Y_{10}Y_{13}+X_3X_{12}Y_{14}Y_{15}+X_4X_7Y_5Y_{16}+X_5X_{16}Y_4Y_7+X_6X_8Y_1Y_{11}+X_{10}X_{13}Y_2Y_9+X_{14}X_{15}Y_3Y_{12}\big),$$

$$\mathfrak{p}_{12,1}=\frac{2}{\vartheta_7\vartheta_2}\big(X_1X_{12}Y_2Y_7+X_2X_7Y_1Y_{12}+X_3X_{11}Y_4Y_9+X_4X_9Y_3Y_{11}+X_5X_{10}Y_8Y_{15}+X_6X_{14}Y_{13}Y_{16}+X_8X_{15}Y_5Y_{10}+X_{13}X_{16}Y_6Y_{14}\big),$$

$$\mathfrak{p}_{13,1}=\frac{2}{\vartheta_6\vartheta_2}\big(X_1X_{13}Y_2Y_6+X_2X_6Y_1Y_{13}+X_3X_5Y_4Y_{15}+X_4X_{15}Y_3Y_5-X_7X_{14}Y_{12}Y_{16}-X_8X_9Y_{10}Y_{11}-X_{10}X_{11}Y_8Y_9-X_{12}X_{16}Y_7Y_{14}\big),$$

$$\mathfrak{p}_{14,1}=\frac{2}{\vartheta_5\vartheta_9}\big(X_1X_{14}Y_5Y_9-X_2X_{16}Y_{11}Y_{15}+X_3X_8Y_7Y_{13}-X_4X_{10}Y_6Y_{12}+X_5X_9Y_1Y_{14}-X_6X_{12}Y_4Y_{10}+X_7X_{13}Y_8Y_3-X_{11}X_{15}Y_2Y_{16}\big),$$

$$\mathfrak{p}_{15,1}=\frac{2}{\vartheta_5\vartheta_2}\big(X_1X_{15}Y_2Y_5+X_2X_5Y_1Y_{15}+X_3X_6Y_4Y_{13}+X_4X_{13}Y_3Y_6+X_7X_{10}Y_8Y_{12}+X_8X_{12}Y_7Y_{10}+X_9X_{16}Y_{11}Y_{14}+X_{11}X_{14}Y_9Y_{16}\big),$$

$$\mathfrak{p}_{16,1}=\frac{2}{\vartheta_3\vartheta_{10}}\big(X_1X_{16}Y_3Y_{10}-X_2X_{14}Y_4Y_8+X_3X_{10}Y_1Y_{16}-X_4X_8Y_2Y_{14}-X_5X_{11}Y_{12}Y_{13}+X_6X_7Y_9Y_{15}+X_9X_{15}Y_6Y_7-X_{12}X_{13}Y_5Y_{11}\big).$$

References

[AKR11] C. Arene, D. Kohel, and C. Ritzenthaler. Complete addition laws on abelian varieties. eprint arXiv:1102.2349, February 2011. `http://arxiv.org/abs/1102.2349`.

[Bai62] W. L. Baily, Jr. On the Theory of θ-Functions, the Moduli of Abelian Varieties, and the Moduli of Curves. *Ann. of Math. (2)*, 75:342–381, March 1962.

[BKL09] D. J. Bernstein, D. Kohel, and T. Lange. Twisted Hessian curves. Preprint, 2009.

[BL04] C. Birkenhake and H. Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2004.

[BL07] D. J. Bernstein and T. Lange. Faster Addition and Doubling on Elliptic Curves. In K. Kurosawa, editor, *Advances in Cryptology – ASIACRYPT 2007*, volume 4833 of *Lecture Notes in Comput. Sci.*, pages 29–50. Springer Berlin / Heidelberg, 2007.

[Cos11] R. Cosset. *Applications des fonctions thêta à la cryptographie sur courbes hyperelliptiques*. PhD thesis, Université Henri-Poincarré, Nancy 1, France, 2011.

[CR11] R. Cosset and D. Robert. Computing (ℓ, ℓ)-isogenies in polynomial time on jacobians of genus 2 curves. Cryptology ePrint Archive, Report 2011/143, March 2011. `http://eprint.iacr.org/2011/143`.

[Duq04] S. Duquesne. Montgomery scalar multiplication for genus 2 curves. In D. Buell, editor, *ANTS-VI*, volume 3076 of *Lecture Notes in Comput. Sci.*, pages 153–168. Springer–Verlag, 2004.

[Edw07] H. M. Edwards. A normal form for elliptic curves. *Bull. Amer. Math. Soc.*, 44:393–422, April 2007.

[FJ10] R. Farashahi and M. Joye. Efficient Arithmetic on Hessian Curves. In P. Nguyen and D. Pointcheval, editors, *Public Key Cryptography – PKC 2010*, volume 6056 of *Lecture Notes in Comput. Sci.*, pages 243–260. Springer Berlin / Heidelberg, 2010.

[Gau07] P. Gaudry. Fast genus 2 arithmetic based on theta functions. *J. Math. Cryptol.*, 1(3):243–265, 2007.

[Koh11] David Kohel. Addition law structure of elliptic curves. *J. Number Theory*, 131(5):894–919, 2011.

[Lan05] T. Lange. Formulae for arithmetic on genus 2 hyperelliptic curves. *Appl. Algebra Engrg. Comm. Comput.*, 15(5):295–328, 2005.

[LM05] Tanja Lange and Pradeep Kumar Mishra. SCA resistant parallel explicit formula for addition and doubling of divisors in the Jacobian of hyperelliptic curves of genus 2. In *Progress in cryptology—INDOCRYPT 2005*, volume 3797 of *Lecture Notes in Comput. Sci.*, pages 403–416. Springer, Berlin, 2005.

[LR85] H. Lange and W. Ruppert. Complete systems of addition laws on abelian varieties. *Invent. Math.*, 79:603–610, 1985.

[Mum66] D. Mumford. On the equations defining abelian varieties. I. *Invent. Math.*, 1:287–354, 1966.

[Mum67a] D. Mumford. On the equations defining abelian varieties. II. *Invent. Math.*, 3:75–135, 1967.

[Mum67b] D. Mumford. On the equations defining abelian varieties. III. *Invent. Math.*, 3:215–244, 1967.

[Mum70] D. Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay, 1970.

[Mum83] D. Mumford. *Tata lectures on theta. I*, volume 28 of *Progr. Math.* Birkhäuser Boston Inc., Boston, MA, 1983. With the assistance of C. Musili, M. Nori, E. Previato and M. Stillman.

[Mum84] D. Mumford. *Tata lectures on theta. II*, volume 43 of *Progr. Math.* Birkhäuser Boston Inc., Boston, MA, 1984. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura.

[Tho70] J. Thomae. Beitrag zur Bestimmung von $\vartheta\,(0, 0, \ldots 0)$ durch die Klassbmodulb agebraischer Functionnen. *J. Reine Angew. Math.*, 70:201–222, 1870.

[vW98] P. van Wamelen. Equations for the Jacobian of a hyperelliptic curve. *Trans. Amer. Math. Soc.*, 350(8):3083–3106, 1998.

Institut de Mathématiques de Luminy, UMR 6206, Campus de Luminy, Case 907, 13288 Marseille, France.
E-mail address: `arene@iml.univ-mrs.fr`

Laboratoire Lorrain de Recherche en Informatique et ses Applications, UMR 7503, Campus scientifique, BP 239, 54506 Vandoeuvre-lès-Nancy, France.
E-mail address: `romain.cosset@loria.fr`