Computing the 2-adic Canonical Lift of Genus 2 Curves

Abdoulaye Maïga, Damien Robert

Computing the 2-adic Canonical Lift of Genus 2 Curves

ABDOULAYE MAIGA AND DAMIEN ROBERT

Abstract. Let $\Bbbk$ be a field of even characteristic and $\mathcal{M}_2(\Bbbk)$ the moduli space of the genus 2 curves defined over $\Bbbk$. We first compute a characteristic reducible modular polynomials in function of invariant that reduce to the absolute Igusa arithmetic invariants. These modular polynomials provide a canonical lifting of the genus 2 curves in even characteristic. The lifted Frobenius is characterized by the reduction behaviors of the Weierstrass points over $\Bbbk$. We success to compute the cardinality of the Jacobian variety. We give a detailed description with the necessary optimizations for an efficient implementation.

Key words: Arithmetic invariants of genus 2 curves, Modular polynomials, Canonical lift, Point counting.

1. Introduction

Let $\mathcal{A}/\mathbb{F}_q$ (with $q = p^n$) be an ordinary abelian variety. A classical result due to Lubin, Serre and Tate [LST64] states that there exists a unique abelian variety $\tilde{\mathcal{A}}$ over $\mathbb{Z}_q$ such that the modulo p reduction of $\tilde{\mathcal{A}}$ is $\mathcal{A}$ and $\mathrm{End}(\tilde{\mathcal{A}}) \cong \mathrm{End}(\mathcal{A})$ as a ring.

When $\Bbbk$ is a field, an absolutely irreducible principally polarised abelian surface over $\Bbbk$ is the Jacobian $\mathrm{Jac}(\mathcal{C})$ of a genus 2 hyperelliptic curve $\mathcal{C}$. If $\mathcal{A}$ is not absolutely simple, then it is isomorphic to the product of two elliptic curves, $\mathcal{A} = E_1 \times E_2$, and lifting $\mathcal{A}$ amount to lifting the two elliptic curves, which is well known. Hence in this article we focus on how to compute a canonical lift of $\mathrm{Jac}(\mathcal{C})$ (hence of $\mathcal{C}$), in the particular case of when the characteristic of $\Bbbk$ is equal to 2. We remark that lifting $\mathcal{C}$ may mean different things: lifting modular invariants, lifting modular forms, or lifting the curve itself. In this article we explain how to lift a curve along with its canonical basis of differential form; from this data it is easy to compute lifts of modular functions or even lifts of vectorial modular forms.

A standard strategy to compute canonical lifts is to use modular polynomials for some specific modular invariants. Over $\mathbb{C}$, the isogeny class of a generic Jacobian variety of a genus 2 curves is given by its tuple of three Igusa's invariants (j_1, j_2, j_3). For p a prime number, the modular polynomials encode the p-isogenous abelian surfaces in term of these Igusa's invariants. More precisely, a birational model of the (coarse) moduli space $\mathfrak{A}_2(p) = \mathfrak{H}_2/\Gamma^0(p)$ is given by $\mathbb{C}(\mathfrak{A}_2(p)) = \mathbb{C}(j_1, j_2, j_3, j_{1,p}, j_{2,p}, j_{3,p})$ where $j_{i,p} = j_i(\tau/p)$, and $\mathfrak{H}_2$ is the Siegel moduli space. We can now define the p^{th}-modular polynomials as follow: $\phi_{1,p}(X)$ is the minimal polynomial of $j_{1,p}$ over $K = \mathbb{C}(\mathfrak{A}_2) = \mathbb{C}(j_1, j_2, j_3)$, and $j_{2,p} = \phi_{2,p}(j_{1,p})$, $j_{3,p} = \phi_{3,p}(j_{1,p})$ for $\phi_{2,p}(X)$ and $\phi_{3,p}(X)$ monic polynomials in $\mathbb{C}(j_1, j_2, j_3)[X]$ of degree less than $\deg(\phi_{1,p}(X))$. If x goes through the roots over $\mathbb{C}$ of $\phi_{1,p}(X)$, then $(x, \phi_{2,p}(x), \phi_{3,p}(x))$ are the absolute j-invariants of a principally polarized abelian surfaces (p,p)-isogenous to an abelian variety with invariants (j_1, j_2, j_3) . Hence the schematic locus of the 2-dimensional p-modular polynomials:

$$\phi_{1,p}(X_1, X_2, X_3, Y_1) = 0, \quad Y_2 = \phi_{2,p}(X_1, X_2, X_3, Y_1) \quad \text{and} \quad Y_3 = \phi_{3,p}(X_1, X_2, X_3, Y_1)$$

Date: November 22, 2020.

2010 *Mathematics Subject Classification.* Primary... Secondary...

Key words and phrases. canonical lift, point counting.

We thank the FAST team.

describe a birational model of $\mathfrak{A}_2(p)$.

These polynomials were first computed by R.Dupont in his thesis [Dup06]. Some improvements have been proposed by others [BL09b] and E.Milio in [Mil15] computed modular polynomials using Streng's [Str10] and Gundlach [Gun63] invariants in order to reduce their size. However Streng's invariants have bad reduction modulo 2, hence these modular polynomials too.

An alternative in characteristic 2 is to use theta functions (of level 2 and 4) since they can be defined for ordinary abelian varieties [Car03; CL08; Rit03]. Modular polynomials in theta functions are derived from the duplication formula [Mes01; Mes02], a generalisation of the AGM, and have also been used to compute canonical lifts for point counting [LL06]. However these are not suitable for our purpose, since they require to take a field extension. Indeed theta functions are modular forms of level $\Gamma(2,4)$ or $\Gamma(4,8)$, so they are not rational in general. While not necessarily a problem for applications to point counting (from the asymptotic point of view), computing curves from lifts of theta functions would give us a curve defined over an extension of $\mathbb{Z}_q$. One would then need to employ a delicate Galois descent algorithm, controlling the p-adic precision to descend back to $\mathbb{Z}_q$. Furthermore the field extension is only really manageable when working over a finite field. Our whole algorithm can be adapted to functions fields of characteristic two, and in these cases we really want to use modular invariants of level 1.

Our goal is as follow: first use the specific arithmetic of genus 2 hyperelliptic curves, as described by Igusa, to compute modular polynomials with good reduction modulo 2. Secondly use this arithmetic to lift the curves.

In characteristic 2, using Artin-Scheier theory it is easy to see that a genus 2 curves is birationally equivalent to one of the three following curves :

$$Y^2 - Y = \begin{cases} \alpha X + \beta X^{-1} + \gamma (X-1)^{-1}, & (1,1,1) \\ X^3 + \alpha X + \beta X^{-1}, & (3,1) \\ X^5 + \alpha X^3, & (5) \end{cases}$$

according to the number and the degree of the ramified Weierstrass points [Igu60, §2]. This classification can be seen on the Jacobian has the rank of the étale p-torsion. So type $(1,1,1)$ correspond to ordinary Jacobians (which we also call ordinary curves), type $(3,1)$ correspond to a p-rank 1, and type (5) to supersingular Jacobians (or curves).

More generally, in all characteristics, a genus 2 curve has birationally equivalent equation

$$XY^2 + (1 + aX + bX^2)Y + X^2(c + dX + X^2) = 0$$

called its *normal form*; that is equivalent to the knowledge of the quintuple $(J_2, J_4, J_6, J_8, J_{10})$ with $J_2 J_6 - J_4^2 - 4J_8 = 0$ called *Igusa arithmetic invariants* [Igu60, §3]. Furthermore, J. Igusa [Igu60, §7] has shown that the arithmetic variety of moduli $\mathcal{M}_2$ of genus 2 curves is generated over $\mathbb{Z}$ by ten absolute invariants in function of J_{2i}'s denoted by γ_i by Goren-Lauter [GL12].

These ten absolute invariants allow us to prove in Section 2 that in the case where $\mathrm{char}(\Bbbk) = 2$, the absolute arithmetic invariants $\mathfrak{a}_1 = J_4/J_2^2$, $\mathfrak{a}_2 = J_8/J_2^4$ and $\mathfrak{a}_3 = J_{10}/J_2^5$ generates the open set $\mathcal{M}_2[J_2^{-1}] \otimes \Bbbk$ of curves birationally equivalent to type $(1,1,1)$. The tuple $(0,\ J_8^3/J_6^4,\ J_{10}^3/J_6^5)$ generates the set (which lives inside $\mathcal{M}_2[J_6^{-1}] \otimes \Bbbk$) of curves birationally equivalent to type $(3,1)$. And the set representing the type (5) (which, except for one point, live inside $\mathcal{M}_2[J_8^{-1}] \otimes \Bbbk$) can be defined using the tuple $(0, 0, J_{10}^4/J_8^5)$ of invariants.

These three sub-varieties $\mathcal{M}_2[J_2^{-1}] \otimes \Bbbk$, $\mathcal{M}_2[J_6^{-1}] \otimes \Bbbk$ and $\mathcal{M}_2[J_8^{-1}] \otimes \Bbbk$, and the invariants above, admit a lifts in $\mathcal{M}_2$ over $\mathbb{Z}_q$. Our first goal is to compute, using these invariants with good reduction, the modular polynomials that parameterize $(2,2)$-isogenous principally polarized abelian surfaces, with J_2 invertible. Thereafter, using those polynomials we want to compute the canonical lift of ordinary genus 2 curves defined over $\mathbb{F}_{2^n}$ with $n > 1$.

Like in Satoh's original approach [Sat00] for elliptic curves the computation of the canonical lift provides a point counting algorithm for the Jacobian variety of the genus 2 curves. As explained, we work directly with modular invariants of level 1, with have the advantage to stay on the field of definition in order to speed up the computation time.

Furthermore, we also explain how to directly lift the curve $\mathcal{C}$. Indeed, the conic equation used during Mestre's algorithm to reconstruct the curve from its invariant has bad reduction modulo 2, so we cannot use the point on the conic corresponding to $\mathcal{C}$ modulo 2 to find a rational point over $\mathbb{Z}_q$ via a Newton lift. Lifting the curve allows us to compute any covariant, hence modular form on it, which can be used to compute class polynomials [CKL08].

We organize this paper as follow. In Section 2, we introduce the absolute Igusa's arithmetic invariants that describe each sub-variety corresponding to the decomposition type of the curves. We propose a conversion of those lifted invariants in order to extend the known computation of modular polynomials [Dup06; Mil14]. The computation of these Siegel modular polynomials is briefly detailed in Section 3, in particular we explain how to adapt it to a given set of modular invariants. In Section 4, we propose an algorithm to lift ordinary Jacobian varieties over $\mathbb{Z}_q$ with $q = 2^n$ from the normal form of the associated genus 2 curves. We give the characteristic reduction properties of the Weierstrass points to compute the Frobenius using Richelot algorithm.

The last Section 5 exposes an extension to genus 2 of Satoh's point counting. We use Richelot [Ric36] algorithm in order to evaluate the lifted Verschiebung and to reconstitute the characteristic polynomial using the product of Frobenius eigenvalues. Our lifting algorithm could also be used to compute class polynomials as in [GHK+06], without going through Rosenhain invariants (which can have negative valuations).

1.1. **Notation and Convention.** Let p be a prime, $\mathbb{Q}_p$ denotes the field of p-adic numbers and $\mathbb{Z}_p$ its ring of valuation. The field $\mathbb{Q}_q$ denotes the unramified extension of $\mathbb{Q}_p$ and $\mathbb{Z}_q$ its valuation ring which is also the ring $W(\mathbb{F}_q)$ of the Witt vectors over $\mathbb{F}_q$. And $\mathbb{Z}_q^{ur}$ be the maximal unramified extension of $\mathbb{Z}_q$.

Given $\mathbb{F}_q$ by $\mathbb{F}_p[X]/m(X)$ where $m(X)$ is a monic irreducible polynomial over $\mathbb{F}_p$ then $\mathbb{Q}_q$ is $\mathbb{Q}_p[X]/M(X)$ with M irreducible polynomial over $\mathbb{Z}_p[X]$ such that $M(X) = m(X) \mod p$. The complexity of an elementary operation over $\mathbb{Z}/p^k\mathbb{Z}[X]/M(X)$ requires $\tilde{\mathrm{O}}(nk \log p)$ with Kronecker-Schönhage method.

The extension $\mathbb{Q}_q/\mathbb{Q}_p$ has a cyclic Galois group of order n, generated by an element Σ that reduces to the p^{th}-power Frobenius automorphism σ on the residue field $\mathbb{F}_q$.

To obtain an efficient Frobenius substitution Σ one takes m as sparse as possible and M its Teichmuller lift polynomial. We denote by : $\tilde{\mathcal{A}}$ the lift of any variety $\mathcal{A}$, and $\tilde{x}$ the lift of any element x of $\mathbb{F}_q$.

We let σ be the small Frobenius in $\mathbb{F}_q$, and σ_q the big Frobenius, and Σ, Σ_q be the lifts to $\mathbb{Q}_q$.

The coarce moduli space over $\mathbb{Z}$ of hyperelliptic curves is denoted by $\mathcal{M}_2$, it embeds via the Torelli morphism into the coarce moduli space $\mathfrak{A}_2$ of abelian schemes of relative dimension 2. We recall that a point of $\mathcal{M}_2 \otimes \Bbbk$ corresponds to the $\overline{\Bbbk}$-isomorphism class of an hyperelliptic curve C of genus 2 whose field of moduli is $\Bbbk$. It is of dimension 3, normal [Igu60, Theorem 1] and birational to $\mathbb{A}^3_{\Bbbk}$ [Igu60, Theorem 5].

2. Arithmetic Invariant Theory of genus 2 hyperelliptic curves {sec:artinv}

We let $\Bbbk$ be a field and $\mathcal{C}$ a genus 2 curve over $\Bbbk$; then $\mathcal{C}$ admit an hyperelliptic model (which we call the standard model): $\mathcal{C} : y^2 + h(x)y = f(x)$ over $\Bbbk[x, y]$, where $\deg(h) \leqslant 2$, and f is a monic polynomial of degree 5 or 6.

In fact $\mathcal{C}$ is completely determined by its function field $K = \Bbbk(\mathcal{C})$. Indeed since $\mathcal{C}$ is smooth, it is the normalisation of any birational model of K. The hyperelliptic involution shows that K is a

degree 2 extension of $\mathbb{k}(\mathbb{P}^1_{\mathbb{k}}) = \mathbb{k}(x)$, and since $\mathcal{C}$ is smooth $K/\mathbb{k}(x)$ is separable. Hence K can be described using Kummer theory in characteristic different from 2 or Artin-Schreier theory in characteristic 2.

2.1. **Invariants of Sextic Forms.** When the characteristic of $\mathbb{k}$ is $char(\mathbb{k}) \neq 2$, the equation of $\mathcal{C}$ reduces to $y^2 = f(x)$ and one defines the sextic :

$$F(x_1, x_2) = x_2^6 f(x_1/x_2)$$

and F has following form :

$$F(x_1, x_2) = a_0x_1^6 + a_1x_1^5x_2 + ... + a_5x_1x_2^5 + a_6x_2^6.$$

Following the *Algebraic Invariants Theory of Hilbert* [Mes91], a *covariant* of order n, degree k and index j is a polynomial $C \in \mathbb{k}[a_0, ..., a_6, x_1, x_2]$ in function of the coefficients of the sextic form, of degree n in x_1, x_2 and k in a_i such that : every variable change

$$(x_1, x_2) \longrightarrow (\alpha x_1 + \beta x_2, \gamma x_1 + \delta x_2)$$

associated to the matrix $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in GL_2(\overline{\mathbb{k}})$, transforms C by a fixed power of $\det(M)$ i.e

$$C(a_0', ..., a_6', \alpha x_1 + \beta x_2, \gamma x_1 + \delta x_2) = \det(M)^j C(a_0, ..., a_6, x_1, x_2)$$

where the a_i''s with $i \in \{0, \cdots 6\}$ are the coefficients after the variable change. We then have $j = 3k - n/2$. Hence for a scalar covariant ($n = 0$), we also call k the weight.

The invariants I of a sextic form F are its covariants of order 0. We denote by $I(\mathcal{C})$ or $I(F)$ the value of I associated to a sextic F or to a genus 2 curves $\mathcal{C}$. Then the sextic forms F and F' are linearly equivalent if and only if there exists $r \in \overline{\mathbb{k}}^*$ such that for every invariant I, we have $I(F) = r^d I(F')$, where d is the degree of I.

In characteristic 0, let f and g be binary forms of degrees n and m, to compute covariants of sextic forms, Clebsh introduced [Cle72] the *Ueberschiebung* operation defined by :

$$(fg)_k = \frac{(m-k)!(n-k)!}{m!n!}\left(\frac{\partial f}{\partial x}\frac{\partial g}{\partial y} - \frac{\partial f}{\partial y}\frac{\partial g}{\partial x}\right)^k$$

where in the binomial expression $\left(\frac{\partial f}{\partial x}\right)^r\left(\frac{\partial f}{\partial y}\right)^s$ means $\frac{\partial^{r+s} f}{\partial x^r \partial y^s}$. Using the Ueberschiebung, Clebsh showed that the algebra of invariants is generated by fives invariants denoted A, B, C, D and R of respective degrees $2, 4, 6, 10$ and 15 [Cle72]. Since R^2 admits a polynomial expression in function of A, B, C and D then these four invariants suffice to characterize the linear equivalence classification of sextic forms. They are called *Clebsh invariants*.

Now let's consider a hyperelliptic model a of genus 2 curves $\mathcal{C} : y^2 = f(x) = u_0x^6 + u_1x^5 + ... + u_5x + u_6$ and $\alpha_1, \cdots, \alpha_6$ the distinct roots of f. If we denote by (ij) the difference $(\alpha_{\sigma(i)} - \alpha_{\sigma(j)})$ such that :

$$I_2 = u_0^2 \sum_{15} (12)^2(34)^2(56)^2 \ ,$$

$$I_4 = u_0^4 \sum_{10} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2 \ ,$$

$$I_6 = u_0^6 \sum_{60} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2(14)^2(25)^2(36)^2 \ ,$$

$$I_{10} = u_0^{10} \prod_{i<j} (\alpha_i - \alpha_j)^2$$

where every α_i appears in each expression m times equal to the power of u_0. Then J.Igusa has shown in [Igu60, p. 620] that I_2, I_4, I_6 and I_{10} are homogenous invariants of degree $2, 4, 6$ and

10 with integers coefficients . They are called *Igusa-Clebsh invariants* because of the following relations with Clebsh invariants :

$$\begin{aligned} I_2 &= -120A\,,\\ I_4 &= -720A^2 + 6750B\,,\\ I_6 &= 8640A^3 - 108000AB + 202500C\,,\\ I_{10} &= -62208A^5 + 972000A^3B + 1620000A^2C - 3037500AB^2 - 6075000BC - 4556250D. \end{aligned}$$

{subsec:artinv}

2.2. **Arithmetic invariants.** We are interested in Igusa's results [Igu60] about the construction of the moduli of genus 2 curves. In characteristic 0 the knowledge of the quadruplet (A, B, C, D) (equivalently I_{2i}'s) in the weighted projective space corresponds exactly to a genus 2 curve in the coarse moduli space $\mathcal{M}_2$. However those invariants have bad reduction in characteristic 2. In fact, the Clebsh invariants (A, B, C, D) have bad reduction in characteristic $2, 3, 5$, and the Igusa-Clebsh invariants only have bad reduction in characteristic $2, 3$ (their reduction is well defined, but they do not classify genus 2 curves anymore).

In general every hyperelliptic curves of genus 2 admit a *universal normal form* [Igu60, p. 617]

$$XY^2 + (1 + aX + bX^2)Y + X^2(c + dX + X^2) = 0$$

such that in characteristic different from 2, the Weierstrass points of the associated sextic form are the roots of the equation :

$$(1 + aX + bX^2)^2 - 4X^3(c + dX + X^2) = 0.$$

In characteristic 2, a genus 2 curve can also be defined via an Artin-Schreier equation: $y^2 - y = R(x)$, where R is a rational function in x with pole divisors. The isomorphism classes of these curves are in bijection with the orbits of $R(x)$ under the double actions by the Artin-Schreier group $\mathrm{AS}(\Bbbk(x))$ and the linear projective group $\mathrm{PGL}_2(\Bbbk)$ [Igu60; GNP]. From the ramifications of the Weierstrass points one deduces three types $(1, 1, 1)$, $(3, 1)$, (5) of birationnally equivalence classes defined by the following affine equations [Igu60, p. 618]:

$$Y^2 - Y = \begin{cases} \alpha X + \beta X^{-1} + \gamma(X-1)^{-1}, & \alpha\beta\gamma \neq 0 \qquad (1,1,1)\\ X^3 + \alpha X + \beta X^{-1}, & \beta \neq 0 \qquad (3,1)\\ X^5 + \alpha X^3, & \qquad (5) \end{cases}$$

Recall that in Deuring's *Invariants Theory of Elliptic Curves* [Deu58]: $\mathbb{Z}[j]$ is the ring of *characteristic preserving functions* depending on birationally equivalence classes of elliptic curves with values in an arithmetic universal domain. Igusa introduced an *integral invariant* as a continuous characteristic preserving function defined on the set of all sextic forms with values in an arithmetic universal domain and covariant under the orbit action [Igu60, §3]. Those depending only on birational classes of hyperelliptic curves of genus 2 are called the *absolute invariants*. In modern terminology, an integral invariant is a global section of the stack quotient by this action, in other word a section of the fine moduli space $\mathfrak{M}_2$, an algebraic stack, hence also of its coarce moduli space $\mathcal{M}_2$.

Igusa defines the following integral arithmetical invariants:

$$\begin{gathered} J_2 = 2^{-3}I_2, \quad J_4 = 2^{-5}3^{-1}(4J_2^2 - I_4),\\ J_6 = 2^{-6}3^{-2}(8J_2^3 - 160J_2J_4 - I_6),\\ J_8 = 2^{-2}(J_2J_6 - J_4^2), \quad J_{10} = 2^{-12}I_{10}. \end{gathered}$$

are arithmetic invariants associated to the curves of equation :

$$XY^2 + (1 + aX + bX^2)Y + X^2(c + dX + X^2) = 0$$

[Igu60, p. 621]. And every J_{2i} reduces well modulo 2, and $J_{10} \neq 0$. Indeed, J_{10} encode the fact that $\mathcal{C}$ is smooth (for instance in characteristic different from 2, I_{10} is the discriminant), so is invertible on $\mathcal{M}_2$, since a curve is smooth over its base. If we express J_{2i}, as polynomials in a, b, c, d, we get a quantity that depends only on the bi-rational class of the genus 2 curves. In characteristic different from 2, it is a consequence of the invariance property of J_{2i}, and in the characteristic 2, it is a consequence of the explicit relations 5,6 and 7.

Reciprocally Igusa shows that from the quintuplet $(J_2, J_4, J_6, J_8, J_{10})$, with $J_{10} \neq 0$, one can construct a normal form with arithmetic invariants those J_{2i}'s (possibly under a field extension) [Igu60, §3, §5]. For the characteristic different from two this can be done algorithmically using the Igusa-Clebsh construction [Mes91] and in characteristic 2 it is a consequence of the three relations from Section 2 and Equation (5) below. Also by considering the relation $J_2J_6 - J_4^2 - 4J_8 = 0$ the invariant J_8 can be disregarded in characteristic different from 2 (but it is crucial in characteristic 2).

Let us consider the graded ring generated over $\mathbb{Z}$ by J_{2i}, $i = 1, 2, 3, 4, 5$ and localized at J_{10}. We denote by $\mathcal{R}$ the integral domain generated by its homogeneous elements of degree zero. Then Igusa shows [Igu60, §7] that $\mathcal{R}$ is generated over $\mathbb{Z}$ by the elements of the form $J_2^{e_1}J_4^{e_2}J_6^{e_3}J_8^{e_4}J_{10}^{-e_5}$ with e_i a non negative integers verifying $e_1 + 2e_2 + 3e_3 + 4e_4 = 5e_5$.

In particular, if y_1, y_2, y_3 and y_4 are an independent variables with $4y_4 = y_1y_3 - y_2^2$, then the correspondence :

$$J_2^{e_1}J_4^{e_2}J_6^{e_3}J_8^{e_4}J_{10}^{-e_5} \longmapsto y_1^{e_1}y_2^{e_2}y_3^{e_3}y_4^{e_4}$$

from $\mathcal{R}$ to $\mathbb{Z}[y_1, y_2, y_3, y_4]^{\mu_5}$ defines an isomorphism between $\mathcal{R}$ and the elements of $\mathbb{Z}[y_1, y_2, y_3, y_4]$ that are invariant under the transformation $y^i \to \zeta_5^i y_i$ for $i = 1, 2, 3, 4$, where ζ_5 is a primitive fifth root of unity.

By considering the condition $J_2J_6 - J_4^2 - 4J_8 = 0$, Igusa shows that the monoid of the powers of e_i's appearing in the elements of $\mathbb{Z}[y_1, y_2, y_3, y_4]^{\mu_5}$ is generated by ten elements (only eight are needed in characteristics different form 2) [Igu60, §7]. Therefore $\mathcal{R}$ is generated by ten elements called γ_i in [GL10]:

$$\gamma_1 = J_2^5/J_{10}, \quad \gamma_2 = J_2^3J_4/J_{10}, \quad \gamma_3 = J_2^2J_6/J_{10}, \quad \gamma_4 = J_2J_8/J_{10},$$
$$\gamma_5 = J_2J_6/J_{10}, \quad \gamma_6 = J_4J_8^2/J_{10}^2, \quad \gamma_7 = J_6^2J_8/J_{10}^2, \quad \gamma_8 = J_6^5/J_{10}^3,$$
$$\gamma_9 = J_6J_8^3/J_{10}^3, \quad \gamma_{10} = J_8^5/J_{10}^4.$$

In summary, we have:

{thm:igusa}

Theorem 2.1. *Let μ_5 be the group of the fifth root of unity, the moduli space $\mathcal{M}_2$ of the genus 2 curves is isomorphic to* $\mathrm{Proj}\,(\mathbb{Z}[J_2, J_4, J_6, J_8, J_{10}])_{(J_{10})} = \mathrm{Spec}\,(\mathbb{Z}[y_1, y_2, y_3, y_4]^{\mu_5}) = \mathrm{Spec}\,(\mathbb{Z}[\gamma_1, \ldots, \gamma_{10}])$ *[Igu60, Theorem 2] (with a weighted grading on the* Proj*). And the variety $\mathcal{M}_2$ can be embedded as a subvariety of an affine space over $\mathbb{Z}$ of dimension ten and not less than ten [Igu60, Theorem 6].*

Corollary 2.2. *Let $\gamma_i(\mathcal{C})$ be the evaluation of γ_i at a representative model of $\mathcal{C}$.*

- *If $\mathcal{C}$ is a curve defined over a number field $\mathbb{K}$, then $\mathcal{C}$ has good reduction modulo a prime $\mathfrak{p}$ of $\mathbb{K}$ if and only if :*

$$ord_{\mathfrak{p}}\,(\gamma_i(\mathcal{C})) \geqslant 0, \quad i = 1, \cdots, 10.$$

- *And if $\mathcal{C}_1$ and $\mathcal{C}_2$ are curves over $\overline{\mathbb{k}}$, then [Igu60, Corollary p.632] :*

$$\mathcal{C}_1 \simeq \mathcal{C}_2 \iff (\gamma_1(\mathcal{C}_1), \cdots, \gamma(\mathcal{C}_1)) = (\gamma_1(\mathcal{C}_2), \cdots, \gamma(\mathcal{C}_2))$$
$$\iff (J_2(\mathcal{C}_1) : J_4(\mathcal{C}_1) : J_6(\mathcal{C}_1) : J_8(\mathcal{C}_1) : J_{10}(\mathcal{C}_1)) = (J_2(\mathcal{C}_2) : J_4(\mathcal{C}_2) : J_6(\mathcal{C}_2) : J_8(\mathcal{C}_2) : J_{10}(\mathcal{C}_2))$$

(with the weighted gradings).

2.3. **Converting between models and invariants.** Converting between the standard hyperelliptic model $y^2+h(x)=f(x)$ to the normal form is explained in Appendix A. And conversely the equations of the Weierstrass points of a normal form $(1+aX+bX^2)^2-4X^3(c+dX+X^2)=0$ (in characteristic different from 2) allows to recover the standard model from it.

Plugging the Igusa-Clebsh formula allows to express the I_2, I_4, I_6, I_{10}, hence the $J_2, J_4, J_6, J_8, J_{10}$ as rational functions in term of a, b, c, d. The rational functions expressing the J_i in terms of a, b, c, d then are still valid in characteristic 2, since both the covariants and the equation has good reduction modulo 2.

Also in characteristic two, one can go from the standard hyperelliptic model to the normal form to the form defined by the three types $(1,1,1)$, $(3,1)$ and (5) (and vice versa) using Artin-Schreier theory (see Appendix A and Section 2.4). Hence we can also express the J_i in terms of the α, β, γ, and conversely using Equations (5) to (7).

From the J_i, which are covariants with weights, we can compute the 10 invariants γ_i. Conversely, from the knowledge of γ_i, we may rescale the covariants so that $J_{10}=1$, hence recover J_6 (up to a 5-th root of unity) from γ_8. This allows to recover J_2, J_4, J_8. The correct 5-th root of unity may be found using γ_7 and γ_9. Then we scale back by J_{10} to get a rational weighted projective point.

However, using the γ_i is not convenient when defining modular polynomials. Indeed we would like to describe the moduli space $\mathcal{M}_2$ using only three invariants (at least birationally). Indeed, by [Igu60, Theorem 5], a generic point of the variety of moduli $\mathcal{M}_2 \otimes \Bbbk$ generates a purely transcendental extension of dimension three. As a corollary we get that $\mathcal{M}_2 \otimes \Bbbk$ is birational to $\mathbb{A}^3_\Bbbk$.

In the next section, we will actually describe an affine cover of an open subscheme of the smooth locus of $\mathcal{M}_2$ by affines isomorphic to a standard open of $\mathbb{A}^3_\mathbb{Z}$ (so completely determined by only three invariants). This cover induce a full cover of the smooth locus of $\mathcal{M}_2 \otimes \Bbbk$ in all characteristics.

{alphabetaclass}

2.4. **Absolute invariants.** We say that a set of three invariants (i_1, i_2, i_3) are absolute invariants for $\mathcal{M}_2 \otimes \Bbbk$ if they generate the function field $\Bbbk(\mathcal{M}_2 \otimes \Bbbk)$. Equivalently, an absolute invariants define a birational morphism $\mathcal{M}_2 \otimes \Bbbk \to \mathbb{A}^3_\Bbbk$, hence define coordinates on an open U of $\mathcal{M}_2 \otimes \Bbbk$. We say that (i_1, i_2, i_3) are well defined at $\mathcal{C}$ if $\mathcal{C}$ corresponds to a geometric point of U. It is stronger than just the i_j having no poles at $\mathcal{C}$, we also require that the birationnal class of $\mathcal{C}$ can be recovered from the $(i_1(\mathcal{C}), i_2(\mathcal{C}), i_3(\mathcal{C}))$, or equivalently by Theorem 2.1, that $(J_2(\mathcal{C}) : J_4(\mathcal{C}) : J_6(\mathcal{C}) : J_8(\mathcal{C}) : J_{10}(\mathcal{C})$ can be recovered.

A standard set of invariants used for computation of class or modular polynomials was $I_2^5/I_{10}, I_2^3 I4/I_{10}, I_2^2 I_6/I_{10}$, the corresponding U is $I_2 \neq 0$. To reduce the size of these polynomials, Streng introduced the absolute invariants $I_4 I_6'/I_{10}, I_2 I_4^2/I_{10}, I_4^5/I_{10}^2$ where $I_6' = 1/2(I_2 I_4 - 3I_6)$. The corresponding U is given by $I_4 \neq 0$. See Section 3.2 for the explanation for this choice: they correspond to nice modular forms defined in terms of theta constants.

These invariants have bad reduction modulo 2. (Their reductions are defined, but they are not absolute invariants on $\mathcal{M}_2 \otimes \Bbbk$ in characteristic 2).

To describe the whole of $\mathcal{M}_2 \otimes \Bbbk$, we need a system of invariants. We say that such a system of invariants $\{i, i', i" \ldots\}$ is fully covering if they give coordinates on a stratification of $\mathcal{M}_2 \otimes \Bbbk$. Typically one use a system of absolute invariants i on an open U_0, then another set of invariants i' on an open U_1 of $\mathcal{M}_2 \otimes \Bbbk \setminus U_0$, and so on. Here i_1 need not be an absolute invariant since we only require it to be defined on a locally closed subscheme rather than an open subscheme. We only require it to induce an isomorphism on U_1 to an open of $\mathbb{A}^{m_1}_\Bbbk$. In fact in characteristic 2 we relax this last condition to a radicial morphism (that is an universally injective morphism) on U_1.

We say that a fully covering system of invariants is optimal if it induce a bijection $\mathcal{M}_2 \otimes \Bbbk \to \mathbb{A}^3_\Bbbk$ (be careful that since the system is defined on a stratification, the map is not a morphism).

In characteristic different from 2. One can define absolute invariants [CQ05, § 1], hence coordinates on the moduli space using the invariants J_{2i}'s. Knowing that the invariant J_{10} defines the discriminant of the curve, so is not null, we obtain that:

- The class of genus 2 curves with a nonzero J_2, is an open set of $\mathcal{M}_2$ on which we have the tuple of absolute invariants : $\left(J_2^5/J_{10}, J_2^3J_4/J_{10}, J_2^2J_6/J_{10}\right)$.
- The genus 2 curves that annihilate in J_2 with a nonzero J_4, is a subspace of $\mathcal{M}_2$ where coordinates can be defined by : $\left(0, J_4^5/J_{10}^2, J_4J_6/J_{10}\right)$.
- The others curves lie in set with coordinates defined by : $\left(0,\ 0, J_6^5/J_{10}^3\right)$.

Then the set of points of $\mathcal{M}_2 \otimes \Bbbk$ is in bijection with the set of tuples defined previously, so in bijection with $\mathbb{A}^3_{\Bbbk}$. In other words, these invariants (k_1, k_2, k_3) on the above stratification are optimal.

Remark 2.3. Reciprocally we can recover the projective J_{2i}'s from any tuple $(k_1, k_2, k_3) \in \mathbb{A}^3_{\Bbbk}$ (a point of $\mathcal{M}_2 \otimes \Bbbk$) using the following way from [CQ05, Lemma 1] :

$$(J_2, J_4, J_6, J_{10}) = \begin{cases} (k_1, k_1k_2, k_1^2k_3, k_1^4), & \text{if} \quad k_1 \neq 0, \\ (0, k_2, k_2k_3, k_2^2), & \text{else if} \quad k_1 = 0,\ k_2 \neq 0, \\ (0, 0, k_3^2, k_3^3), & \text{otherwise.} \end{cases}$$

In characteristic 2. We recall that every hyperelliptic curves of genus 2 is birationally equivalent to one of the three following types according to the number and the degree of the ramified Weierstrass points:

$$Y^2 - Y = \begin{cases} \alpha X + \beta X^{-1} + \gamma (X-1)^{-1}, & (1,1,1) \\ X^3 + \alpha X + \beta X^{-1}, & (3,1) \\ X^5 + \alpha X^3, & (5) \end{cases}$$

When $\Bbbk$ has q elements the number $\overline{\Bbbk}$-isomorphism classes of smooth projective curves of genus two defined over $\Bbbk$ is given in the following table according to the type [GNP, Th 20]:

Type	Number
(1,1,1)	$q^3 - q^2$
(3,1)	$q^2 - q$
(5)	q

{tab:table}

Let's consider the normal form equation :

$$XY^2 + (1 + aX + bX^2)Y + X^2(c + dX + X^2) = 0.$$

If ab is different from 0, we get three Weierstrass points; it corresponds to the type $(1, 1, 1)$. After a technical variable change in [Igu60, §3], one can obtain :

$$\alpha = ab^{-3}, \tag{1}$$

$$\beta = a^{-3}b\xi^{-2}\left(c + \xi^{-2} + a(c\xi + d + \xi^{-1})^{1/2}\right), \tag{2}$$

$$\gamma = a^{-3}b\eta^{-2}\left(c + \eta^{-2} + a(c\eta + d + \eta^{-1})^{1/2}\right) \tag{3}$$

in which $\xi + \eta = a$, $\eta\xi = b$;
But if a or b is nonzero and $ab = 0$, it corresponds the type $(3, 1)$; and if $a \neq 0$ and $b = 0$, one can transform :

$$XY^2 + (1 + aX + bX^2)Y + X^2(c + dX + X^2) = 0$$

into

$$Y^2 - Y = X^3 + \alpha X + \beta X^{-1}$$

with

$$(4)\quad \alpha = a^{5/3}\left(a^{-3}c + (a^{-5} + a^{-4}d)^{1/2}\right), \quad \beta = a^{-5/3}\left(a^{-5} + a^{-3}c + (a^{-5} + a^{-4}d + a^{-3}c)^{1/2}\right).$$

If $b \neq 0$ and $a = 0$, we obtain α, β in terms of b, c, d via a more complicated expressions for which we refer to Igusa.
The type (5) corresponds to $a = b = 0$ and the associated normal form $XY^2 + Y + X^2(c + dX + X^2) = 0$ can be transformed into $Y^2 - Y = X^5 + \alpha X^3$ with $\alpha = c$.

The open set $\mathcal{M}_2[J_2^{-1}] \otimes \Bbbk$ describes in $\mathcal{M}_2 \otimes \Bbbk$, the curves birationaly equivalent to a curve of type $(1, 1, 1)$. It is characterized by the non vanishing of J_2 modulo 2, and can be defined using the following three absolute arithmetic invariants: $\mathfrak{a}_1 = J_4/J_2^2$, $\mathfrak{a}_2 = J_8/J_2^4$ and $\mathfrak{a}_3 = J_{10}/J_2^5$. Indeed one can recover these invariants from the coefficients of the normal form using the following relation [Igu60, §3]:

$$(5)\quad \texttt{\{\{abcd1\}\}} \qquad \begin{cases} \alpha^2 + \beta^2 + \gamma^2 &= & J_4/J_2^2, \\ \alpha^2\beta^2\gamma^2 &= & J_{10}/J_2^5, \\ \alpha^2\beta^2 + \beta^2\gamma^2 + \gamma^2\alpha^2 &= & J_8/J_2^4 + (J_4/J_2^2)^3 + (J_4/J_2^2)^4 \end{cases}$$

And Igusa shows in [Igu60, §2] that birational invariants are given by the three standard symmetric invariants: $\alpha + \beta + \gamma$, $\alpha\beta + \beta\gamma + \gamma\alpha$, $\alpha\beta\gamma$, they are also used by Cardona and al. in [GNP, §2]: Although they are ramified over the symmetric invariants, there is one important advantage to the three invariants $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3$: they come from modular functions over $\mathbb{C}$ and are actually defined over $\mathbb{Z}$. By contrast, the symmetric invariants do not lift to modular forms (without characters) in characteristic 0. More precisely, it is proven in Theorem 2.4 that these invariants describe $\mathcal{M}_2[J_2^{-1}]$ over $\mathbb{Z}$. In particular, over $\mathbb{Z}_2$ these invariants describe the open set $\mathcal{M}_2[J_2^{-1}]$ of $\mathcal{M}_2$ that reduces to $\mathcal{M}_2[J_2^{-1}] \otimes \Bbbk$ modulo 2, in other words of curves with good reduction modulo 2, and whose reduction is of type $(1, 1, 1)$.

The type $(3, 1)$ is characterized by $J_2 = 0$ and the non-vanishing of J_6 over $\Bbbk$, this corresponds to a closed subscheme of $\mathcal{M}_2[J_6^{-1}] \otimes \Bbbk$, hence a locally closed subscheme in $\mathcal{M}_2 \otimes \Bbbk$, of curves birationally equivalent to that type. Coordinates on this subscheme are defined using the following tuple of absolute invariants: $(0,\ J_8J_{10}/J_6^3,\ J_{10}^3/J_6^5)$. Indeed from the equation $(3, 1)$, one recovers this tuple using:

$$(6)\quad \texttt{\{\{abcd2\}\}} \qquad \begin{cases} \alpha^6 &= & J_8^{3/4}/J_6^1, \\ \beta^6 &= & J_{10}^3/J_6^5, \\ \alpha^2\beta^2 &= & J_8^{1/4}J_{10}/J_6^2. \end{cases}$$

And birational invariants are given by $\alpha^3, \alpha\beta$ [Igu60, §2].

The type (5) is characterized by $J_2 = J_6 = 0$. The corresponding closed subset of $\mathcal{M}_2 \otimes \Bbbk$, can be defined using the tuple $(0, 0, J_8^5/J_{10}^4)$ of invariants. And the following relation holds :

$$(7)\quad \texttt{\{\{abcd3\}\}} \qquad \begin{cases} \alpha^{10} = J_8^{5/4}/J_{10}. \end{cases}$$

And α^5 is a birational invariant [Igu60, §2].

From this discussion, we see that the invariants $(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3) = (J_4/J_2^2, J_8/J_2^4, J_{10}/J_2^5)$ when $J_2 \neq 0$, $(0,\ J_8J_{10}/J_6^3,\ J_{10}^3/J_6^5)$ when $J_2 = 0, J_6 \neq 0$, and $(0, 0, J_8^5/J_{10}^4)$ induces a bijection between the set of points of $\mathcal{M}_2 \otimes \Bbbk$ and $\mathbb{A}^3_{\Bbbk}$, hence are optimal. Indeed the above formula show how to recover α, β, γ from these invariants. A drawback compared to the optimal invariants defined above in characteristic different from 2 is that they do not share a common denominator. It would be interesting to combine the two versions to have optimal invariants working in all characteristic at once.

2.5. **Absolute invariants in all characteristic.** Igusa shows in [Igu60, Theorem 4] that:

- If $char(\Bbbk) \neq 2$, the variety $\mathcal{M}_2 \otimes \Bbbk$ has one and only one singular point, which corresponds to $J_2 = J_6 = J_8 = 0$.
- If $char(\Bbbk) = 2$, the singular locus of $\mathcal{M}_2 \otimes \Bbbk$ is a rational curve corresponding to $J_2 = J_6 = 0$ i.e, the curves of type (5) having only one Weierstrass point.

We give a set of three invariants over each of the four opens $\mathcal{M}_2[J_2^{-1}]$, $\mathcal{M}_2[J_4^{-1}]$, $\mathcal{M}_2[J_6^{-1}]$, $\mathcal{M}_2[J_8^{-1}]$ in $\mathcal{M}_2$ over $\mathbb{Z}$. These opens reduce in all characteristic to a cover of $\mathcal{M}_2 \otimes \Bbbk$, except for the one curve defined by $J_2 = J_4 = J_6 = J_8 = 0$. This is the curve defined by the equation $y^2 + y = x^5$ over $\mathbb{Q}$, which has potential good reduction everywhere [Qin93, Exemple 1], and reduces modulo 2 to a curve of type (5) with $\alpha = 0$.

Furthermore these three invariants actually induce an isomorphism with a standard open of $\mathbb{A}^3$ for the first three opens (over $\mathbb{Z}[1/2]$ for $\mathcal{M}_2[J_4^{-1}]$, and over $\mathbb{Z}$ for the other two). In other words they are absolute invariants, well defined on the above opens.

These three open $\mathcal{M}_2[J_2^{-1}]$, $\mathcal{M}_2[J_4^{-1}]$, $\mathcal{M}_2[J_6^{-1}]$ are sufficient to cover $\mathcal{M}_2 \otimes \Bbbk$ in characteristic different from 2, minus the only non smooth point $y^2 + y = x^5$ from above. In characteristic 2, the first open corresponds to curves of type $(1, 1, 1)$, and the third open includes the curves of type $(3, 1)$. We cannot hope for the three invariants on the last open to yield an isomorphism to an open of $\mathbb{A}^3$, since $\mathcal{M}_2[J_8^{-1}]$ contains a non smooth locus.

From the preceding section, we see that our choice of cover and absolute invariants is particularly well adapted to the reduction of a curve in $\mathcal{M}_2 \otimes \mathbb{Z}_{(2)}$. Hence, in particular in characteristic two and zero, and even more precisely to represent lifts over $\mathbb{Z}_q$ of the genus 2 curves defined over $\mathbb{F}_q$, with $q = 2^n$.

{thm:goodinvariants}

Theorem 2.4. *To the affine cover described above, we associate the set of three invariants:*

- $\mathfrak{a}_1 = J_4/J_2^2$, $\mathfrak{a}_2 = J_8/J_2^4$ *and* $\mathfrak{a}_3 = J_{10}/J_2^5$ *for* $\mathcal{M}_2[J_2^{-1}]$,
- $\mathfrak{d}_1 = J_2^2/J_4$, $\mathfrak{d}_2 = J_6^2/J_4^3$ *and* $\mathfrak{d}_3 = J_{10}^2/J_4^5$ *for* $\mathcal{M}_2[J_4^{-1}]$,
- $\mathfrak{u}_1 = J_4^3/J_6^2$, $\mathfrak{u}_2 = J_8 J_{10}/J_6^3$, *and* $\mathfrak{u}_3 = J_{10}^3/J_6^5$ *for* $\mathcal{M}_2[J_6^{-1}]$,
- $\mathfrak{w}_1 = J_2^4/J_8$, $\mathfrak{w}_2 = J_6^4/J_8^3$, *and* $\mathfrak{w}_3 = J_{10}^4/J_8^5$ *for* $\mathcal{M}_2[J_8^{-1}]$.

Then these invariants induce an isomorphism of $\mathcal{M}_2[J_2^{-1}]$, $\mathcal{M}_2[J_4^{-1}]$ *and* $\mathcal{M}_2[J_6^{-1}]$ *with the standard open of* $\mathbb{A}^3$ *defined by* $\mathfrak{a}_3^{-1}$, $\mathfrak{d}_3^{-1}$, $\mathfrak{u}_3^{-1}$ *respectively, over* $\mathbb{Z}$, $\mathbb{Z}[1/2]$ *and* $\mathbb{Z}$ *respectively.*

The last set of three invariants give a finite covering of $\mathcal{M}_2[J_8^{-1}]$ *to the standard open* $\mathbb{A}^3[\mathfrak{w}_3^{-1}]$ *over* $\mathbb{Z}$. *In characteristic two, they restrict on the non smooth locus* $J_2 = J_6 = 0$ *to a radicial morphism with image* $\mathbb{A}^1_{\Bbbk} \setminus \{0\}$.

Proof. Since the J_{2i} have good reduction, these invariants too. We need to check that they define local coordinates, in other words that they generate $\mathbb{Z}_{(2)}[\mathcal{M}_2]$ locally. By the results from Section 2.2 it suffices to prove that we can recover all the γ_i.

We can prove this result by calculation :

- For the set $\mathcal{M}_2[J_2^{-1}]$, we express the invariants γ_i's in function of $\mathfrak{a}_1$, $\mathfrak{a}_2$ and $\mathfrak{a}_3$.

$$\gamma_1 = \frac{1}{\mathfrak{a}_3}, \quad \gamma_2 = \frac{\mathfrak{a}_1}{\mathfrak{a}_3}, \quad \gamma_3 = \frac{\mathfrak{a}_1^2}{\mathfrak{a}_3} + 4\frac{\mathfrak{a}_2}{\mathfrak{a}_3}, \quad \gamma_4 = \frac{\mathfrak{a}_2}{\mathfrak{a}_3}, \quad \gamma_5 = \frac{\mathfrak{a}_1^3}{\mathfrak{c}} + 4\frac{\mathfrak{a}_1\mathfrak{a}_2}{\mathfrak{a}_3}, \quad \gamma_6 = \frac{\mathfrak{a}_1\mathfrak{a}_2^2}{\mathfrak{a}_3^2},$$

$$\gamma_7 = \frac{\mathfrak{a}_1^4\mathfrak{a}_2}{\mathfrak{a}_3^2} + 8\frac{\mathfrak{a}_1^2\mathfrak{a}_2^2}{\mathfrak{a}_3^2} + 16\frac{\mathfrak{a}_2^3}{\mathfrak{a}_3^2}, \quad \gamma_8 = \frac{1}{\mathfrak{a}_3^3}\left(\mathfrak{a}_1^{10} + 20\mathfrak{a}_1^8\mathfrak{a}_2 + 160\mathfrak{a}_1^6\mathfrak{a}_2^2 + 640\mathfrak{a}_1^4\mathfrak{a}_2^3 + 1280\mathfrak{a}_1^2\mathfrak{a}_2^4 + 1024\mathfrak{a}_2^5\right),$$

$$\gamma_9 = \frac{1}{\mathfrak{a}_3^3}\left(\mathfrak{a}_1^2\mathfrak{a}_2^3 + 4\mathfrak{a}_2^4\right), \quad \gamma_{10} = \frac{\mathfrak{a}_2^5}{\mathfrak{a}_3^4}.$$

This transformation makes sens over $\mathbb{Z}$. Therefore

$$\mathcal{M}_2[J_2^{-1}] = \mathrm{Spec}\left(\mathbb{Z}[\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3][\mathfrak{a}_3^{-1}]\right)$$

and $\mathcal{M}_2[J_2^{-1}]$ is a subspace of $\mathcal{M}_2$ of dimension three over $\mathbb{Z}$.

• Over $\mathbb{Z}[1/2]$, the invariants γ_i's are expressed in function of $\mathfrak{d}_1$, $\mathfrak{d}_2$ and $\mathfrak{d}_3$ on $\mathcal{M}_2[J_4^{-1}]$ as follow.

$$\gamma_1 = \frac{\mathfrak{d}_1^5}{\mathfrak{d}_3}, \quad \gamma_2 = \frac{\mathfrak{d}_1^3}{\mathfrak{d}_3}, \quad \gamma_3 = \frac{\mathfrak{d}_1^2 s}{\mathfrak{d}_3}, \quad \gamma_4 = \frac{\mathfrak{d}_1^2\mathfrak{d}_2}{4\mathfrak{d}_3} - \frac{\mathfrak{d}_1}{4\mathfrak{d}_3}, \quad \gamma_5 = \frac{\mathfrak{d}_2}{\mathfrak{d}_3}, \quad \gamma_6 = \frac{1}{16\mathfrak{d}_3^2}\left(\mathfrak{d}_1^2\mathfrak{d}_2^2 - 2\mathfrak{d}_1\mathfrak{d}_2 + 1\right),$$
$$\gamma_7 = \frac{1}{4\mathfrak{d}_3^2}\left(\mathfrak{d}_1\mathfrak{d}_2^3 - \mathfrak{d}_2^2\right), \quad \gamma_8 = \frac{\mathfrak{d}_2^5}{\mathfrak{d}_3^3}, \quad \gamma_9 = \frac{1}{64\mathfrak{d}_3^3}\left(\mathfrak{d}_1^3\mathfrak{d}_2^4 - 3\mathfrak{d}_1^2\mathfrak{d}_2^3 + 3\mathfrak{d}_1\mathfrak{d}_2^2 - \mathfrak{d}_2\right),$$
$$\gamma_{10} = \frac{1}{1024\mathfrak{d}_3^4}\left(\mathfrak{d}_1^5\mathfrak{d}_2^5 - 5\mathfrak{d}_1^4\mathfrak{d}_2^4 + 10\mathfrak{d}_1^3\mathfrak{d}_2^3 - 10\mathfrak{d}_1^2\mathfrak{d}_2^2 + 5\mathfrak{d}_1\mathfrak{d}_2 - \mathfrak{d}_3^4\right).$$

• In the case of $\mathcal{M}_2[J_6^{-1}]$, we express the γ_i's in function of $\mathfrak{u}_1$, $\mathfrak{u}_2$ and $\mathfrak{u}_3$. This transformation also makes sens over $\mathbb{Z}$ and the sub-variety $\mathcal{M}_2[J_6^{-1}]$ of $\mathcal{M}_2$ has dimension three over $\mathbb{Z}$.

$$\gamma_1 = \frac{1}{\mathfrak{u}_3^6}(\mathfrak{u}_3^5\mathfrak{u}_1^{10} + 20\mathfrak{u}_3^4\mathfrak{u}_2\mathfrak{u}_1^8 + 160\mathfrak{u}_3^3\mathfrak{u}_2^2\mathfrak{u}_1^6 + 640\mathfrak{u}_3^2\mathfrak{u}_2^3\mathfrak{u}_1^4 + 1280\mathfrak{u}_3\mathfrak{u}_2^4\mathfrak{u}_1^2 + 1024\mathfrak{u}_2^5),$$
$$\gamma_2 = \frac{1}{\mathfrak{u}_3^4}(\mathfrak{u}_3^3\mathfrak{u}_1^7 + 12\mathfrak{u}_3^2\mathfrak{u}_2\mathfrak{u}_1^5 + 48\mathfrak{u}_3\mathfrak{u}_2^2\mathfrak{u}_1^3 + 64\mathfrak{u}_2^3\mathfrak{u}_1), \quad \gamma_3 = \frac{1}{\mathfrak{u}_3^3}(\mathfrak{u}_3^2\mathfrak{u}_1^4 + 8\mathfrak{u}_3\mathfrak{u}_2\mathfrak{u}_1^2 + 16\mathfrak{u}_2^2),$$
$$\gamma_4 = \frac{1}{\mathfrak{u}_3^3}(\mathfrak{u}_3\mathfrak{u}_2\mathfrak{u}_1^2 + 4\mathfrak{u}_2^2), \quad \gamma_5 = \frac{\mathfrak{u}_1}{\mathfrak{u}_3}, \quad \gamma_6 = \frac{\mathfrak{u}_1\mathfrak{u}_2^2}{\mathfrak{u}_3^4}, \quad \gamma_7 = \frac{\mathfrak{u}_2}{\mathfrak{u}_3^3}, \quad \gamma_8 = \frac{1}{\mathfrak{u}_3^3}, \quad \gamma_9 = \frac{\mathfrak{u}_2^3}{\mathfrak{u}_3^6}, \quad \gamma_{10} = \frac{\mathfrak{u}_2^5}{\mathfrak{u}_3^9}.$$

• In the case of $\mathcal{M}_2[J_8^{-1}]$, we express the squares of γ_i's in function of $\mathfrak{w}_1$, $\mathfrak{w}_2$ and $\mathfrak{w}_3$.

$$\gamma_1^2 = \frac{\mathfrak{w}_1^{10}}{\mathfrak{w}_3^2}, \quad \gamma_2^2 = \frac{1}{\mathfrak{w}_3^2}\left(\mathfrak{w}_1^7\mathfrak{w}_2 - 4\mathfrak{w}_1^6\right), \quad \gamma_3^2 = \frac{\mathfrak{w}_1^4\mathfrak{w}_2^2}{\mathfrak{w}_3^2}, \quad \gamma_4^2 = \frac{\mathfrak{w}_1^2}{\mathfrak{w}_3^2}, \quad \gamma_5^2 = \frac{1}{\mathfrak{w}_3^2}\left(\mathfrak{w}_1\mathfrak{w}_2^3 - 4\mathfrak{w}_2^2\right),$$
$$\gamma_6^2 = \frac{1}{\mathfrak{w}_3^4}\left(\mathfrak{w}_1\mathfrak{w}_2 - 4\right), \quad \gamma_7^2 = \frac{\mathfrak{w}_2^4}{\mathfrak{w}_3^4}, \quad \gamma_8^2 = \frac{\mathfrak{w}_2^{10}}{\mathfrak{w}_3^6}, \quad \gamma_9^2 = \frac{\mathfrak{w}_2^2}{\mathfrak{w}_3^6}, \quad \gamma_{10}^2 = \frac{1}{\mathfrak{w}_3^8}.$$

As we have seen, we can't do better in characteristic 2, since $\mathcal{M}_2[J_8^{-1}] \otimes \Bbbk$ contain the singular locus $J_2 = J_6 = 0$ of curves of type (5). If we restrict to this locus in characteristic 2, we get that $\mathfrak{w}_3 = \alpha^{-40}$. Since α^5 is a birational invariant on this locus, we see that the coordinates $\mathfrak{w}_3$ induce a totally ramified cover of degree 8 on the curves of type (5), minus, as usual, the curve $y^2 - y = x^5$.

□

3. Modular Polynomials in Dimension 2

{sec:polmod}

3.1. **Theta functions.** In this section, we consider $\mathbb{C}$ as the base field. For an integer $g > 0$, we denote by $\mathfrak{H}_g$, the *Siegel upper half space*, and by Γ_g the *symplectic group* $\mathrm{Sp}_{2g}(\mathbb{Z})$ such that :

$$\mathfrak{H}_g = \left\{\Omega \in M_g(\mathbb{C}),\ {}^t\Omega = \Omega,\ Im(\Omega) > 0\right\}$$
$$\text{and} \quad \mathrm{Sp}_{2g}(\mathbb{Z}) = \left\{\gamma \in M_{2g}(\mathbb{Z}) :\ \gamma J_{2g}\,{}^t\gamma = J_{2g}\right\}, J_{2g} = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right).$$

A complex abelian variety $\mathcal{A}$ of dimension g is analytically isomorphic to a torus $\mathcal{A}_\Omega = \mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g)$ where $\Omega \in \mathfrak{H}_g$ is called its *period matrix*.

In general the group Γ_g acts on $\mathfrak{H}_g$ by :

$$\gamma\Omega = (A\Omega + B)(C\Omega + D)^{-1} \quad for \quad \gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_g$$

And *two principally polarized abelian varieties* Ω_1 *and* Ω_2 *are isomorphic if and only if* $\Omega_2 = \gamma\Omega_1$ *where* $\gamma \in \Gamma_{2g}$.

We denote by $\mathcal{F}_g$ the fundamental domain of this action; therefore for all $\Omega \in \mathfrak{H}_g$, there exist $\gamma\Gamma_g$ such that $\gamma\Omega \in \mathcal{F}_g$ and γ is unique if $\gamma\Omega$ is an inner point of $\mathcal{F}_g$.

We recall that :

- The Riemann classical theta function is defined by
$$\theta : \mathbb{C} \times \mathfrak{H}_g \to \mathbb{C}, \quad (z, \Omega) \mapsto \sum_{n \in \mathbb{Z}^g} exp(i\pi\, {}^t(n)\Omega n + 2i\pi\, {}^t n z)$$
- For $a, b \in \mathbb{Q}$ the classical theta function with characteristic (a, b) is defined by:
$$\theta \left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z, \Omega) = \sum_{n \in \mathbb{Z}^g} exp(i\pi\, {}^t(n+a)\Omega(n+a) + 2i\pi\, {}^t(n+a)(z+b))$$

These functions satisfy the following fundamental property.

Proposition 3.1. *(Functional Equation). Let $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_g$, and e' (reps. e") the vector defined by the coefficients of the diagonal of $\frac{1}{2}\, {}^t AC$ (resp. $\frac{1}{2}\, {}^t DB$). Then for all $a, b \in \mathbb{Q}^g$, $z \in \mathbb{C}^g$ and $\Omega \in \mathfrak{H}_g$, we have:*

$$\begin{aligned}\theta \left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](\gamma z, \gamma\Omega) =& \zeta_\gamma \sqrt{\det(C\Omega + D)} \exp\left(i\pi\, {}^t z (C\Omega + D)^{-1} C z\right) \\ & \cdot \theta \left[{}^t\gamma \left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) + \left(\begin{smallmatrix} e' \\ e" \end{smallmatrix}\right)\right](z, \Omega) \exp\left(-2i\pi\, {}^t({}^t Aa + {}^t Cb + e')e"\right) \\ & \cdot \exp(-i\pi\, {}^t a A\, {}^t B a) \exp(-i\pi\, {}^t b C\, {}^t D b) \exp(-2i\pi\, {}^t a B\, {}^t C b) \quad ,\end{aligned}$$

where ζ_γ is a eighth root of the unity depending only on γ.

Proof. See [Cos11, Propriété 3.1.24.]. □

These theta functions are sections of powers of the canonical principal polarisation associated to the choice of $\Omega \in \mathfrak{H}_2$ and a well known result from Lefschetz says:

- For $n \geqslant 3$, any linearly independent set of $k = n^g$ theta functions of level n provides an embedding of $\mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g)$ into $\mathbb{P}^{k-1}(\mathbb{C})$.
- For $n = 2$, if the polarisation is irreducible, the theta functions of level 2 embed $(\mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g))/\sim$, where $\sim$ is the equivalence relation $z \sim -z$.

When $\mathcal{C}$ is an hyperelliptic curves of genus g, the Abel-Jacobi's theorem establishes that: the Jacobian $\mathrm{Jac}(\mathcal{C})$ of $\mathcal{C}$ is canonically isomorphic to the analytic Jacobian $\mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g)$ where $\Omega \in \mathfrak{H}_g$ is called the period matrix of $\mathrm{Jac}(\mathcal{C})$ [BL04, thm 11.1.3]. Conversely, *a simple principally polarized abelian variety of dimension $g \leqslant 3$ is: the Jacobian of a smooth curve C of genus g, and C is an hyperelliptic curve if $g \leqslant 2$* [BL04, cor 11.8.2].

{subsec:modfunc}

3.2. **Modular Functions for Γ_2.** We have seen that theta functions give an algebraic structure to the analytic abelian surfaces of Jacobian variety of genus 2 curves. They also provide an analytic definition of covariants associated to the corresponding curves. We define the theta constants of level n as the theta functions of level n evaluated at $z = 0$. We will use Dupont notation in [Dup06] : for all $a = \left(\begin{smallmatrix} a_0 \\ a_1 \end{smallmatrix}\right)$ and $b = \left(\begin{smallmatrix} b_0 \\ b_1 \end{smallmatrix}\right)$ in $\{0, 1\}^2$,

$$\theta_{b_0+2b_1+4a_0+8a_1}(\Omega) := \theta_{a,b}(\Omega) := \theta \begin{bmatrix} a/2 \\ b/2 \end{bmatrix}(0, \Omega).$$

Let Γ be a subgroup of Γ_g of finite index:

- A *modular form of weight k* for Γ is a holomorphic function f defined over $\mathfrak{H}_g$ such that: $f(\gamma\Omega) = \det(C\Omega + D)^k f(\Omega)$ for all $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma$ and $\Omega \in \mathfrak{H}_g$. (By the Koecher principle holomorphy at the cusps is automatic when $g > 1$.)
- And we call *modular function* for Γ over $\mathfrak{H}_g$ a function defined by a quotient of two Γ-modular forms of the same weight.

Example 3.2. Let's denote by : $\mathcal{P} = \{0, 1, 2, 3, 4, 6, 8, 9, 12, 15\}$.

$$h_4 = \sum_{i\in\mathcal{P}} \theta_i^8, \quad h_6 = \sum_{60\, tuples\, (i,j,k)\in\mathcal{P}^3} (\theta_i\theta_j\theta_k)^4$$

$$h_{10} = \prod_{i\in\mathcal{P}} \theta_i^2, \quad h_{12} = \sum_{15\, tuples\, (i,j,k,l,m,n)\in\mathcal{P}^6} (\theta_i\theta_j\theta_k\theta_l\theta_m\theta_n)^4$$

and $h_{16} = \frac{1}{3}(h_{12}h_4 - 2h_6h_{10})$.

The h_i's with $i \in \{4, 6, 10, 12, 16\}$ are Γ_2-modular forms of weight i.

Furthermore we have:

$$h_4 = 2^2\psi_4, \quad h_6 = 2^2\psi_6, \quad h_{10} = -2^{14}\chi_{10} \quad \text{and} \quad h_{12} = 2^{17}3\chi_{12}.$$

where ψ_k are the Eisenstein series of weight $k \geqslant 4$ defined by:

$$\psi_k(\Omega) = \sum_{\gamma\in\Gamma_2} \det(C\Omega + D)^{-k}$$

and χ_{10}, χ_{12} are cusp forms, expressed in function of ψ_k with $k \in \{4, 6, 10, 12\}$. Over $\mathbb{C}$, the graded ring of even-weight Siegel modular forms in genus 2 is generated by the four modular forms ψ_4 ,ψ_6 , χ_{10} , χ_{12} [Igu62].

Therefore we can define the well known Γ_2-modular functions called *j-invariants* [Str10, Chapter 2, § 2.1] defined by:

$$\mathrm{j}_1 = -2^{-10}\frac{\chi_4\chi_6}{\chi_{10}}, \quad \mathrm{j}_2 = 2^{-7}\cdot 3\frac{\chi_4^2\chi_{12}}{\chi_{10}^2}, \quad \mathrm{j}_3 = 2^{-18}\frac{\chi_4}{\chi_{10}^2}.$$

These invariants are birationally equivalent to Igusa's j-invariant [Igu72] which are less convenient algorithmically since they have bigger denominators. We will see below that these are the same invariants as the absolute invariants (j_1, j_2, j_3) introduced in Section 2.4.

Theorem 3.3. *The field $\mathbb{C}(\mathfrak{A}_2)$ of Siegel modular functions in dimension 2, denoted by $\mathbb{C}_{\Gamma_2}$, is $\mathbb{C}(\mathrm{j}_1, \mathrm{j}_2, \mathrm{j}_3)$.*

Proof. Proof see [Igu62]. □

More generally given a finite-dimensional representation $\rho : \mathrm{GL}_2(\mathbb{C}) \to \mathrm{GL}(V)$, a (vectorial) Siegel modular form of weight ρ is a holomorphic function $f : \mathfrak{H}_2 \to V$ satisfying: $f(\gamma\Omega) = \rho(C\Omega + D)f(\Omega)$ for every $\Omega \in \mathfrak{H}_2$, $\gamma \in \Gamma_2$. Therefore we say that f is *scalar-valued* if V has dimension 1, and otherwise f is said to be *vector-valued*. Furthermore if f has no pole at $\Omega \in \mathfrak{H}_2$, for every complex principally polarized abelian surface $\mathcal{A}$ isomorphic to $\mathcal{A}_\Omega$ with a basis $\omega \in \Omega^1(\mathcal{A})$ we have following well defined quantity

$$f(\mathcal{A}, \omega) := \rho({}^t(m^{-1}))f(\Omega)$$

where $m \in \mathrm{GL}_2(\mathbb{C})$ depends only on $\mathcal{A}$, ω and Ω, and is the base change matrix between ω and the canonical basis of differentials $(2\pi i dz_1, 2\pi i dz_2)$ on $\mathcal{A}_\Omega$. See [KPR20, §2.2] for more detail about this construction. This is Katz's algebraic interpretation of modular forms as sections of representations of the Hodge vector bundle. Since $(\mathcal{A}, \omega)$ can be defined over any field $\Bbbk$, if f is defined over some $\mathbb{Z}[1/N]$ (as seen by its Fourier coefficients) with $\mathrm{char}(k) \nmid N$, then the quantity $f(\mathcal{A}, \omega)$ will make sense over $\Bbbk$.

In particular, given the equation of an hyperelliptic curve $\mathcal{C}$, the basis $\omega(\mathcal{C}) = (dx/y, xdx/y)$ provide a basis of $\Omega^1(\mathrm{Jac}(\mathcal{C}))$. In particular a modular form induces a covariant on $\mathcal{C}$ via the following map:

$$\mathrm{Cot}(f) : \mathcal{C} \mapsto f(\mathrm{Jac}(\mathcal{C}), \omega(\mathcal{C})),$$

which allow to express $\mathrm{Cot}(f)$ in terms of the coefficients of the curve. In other words, seeing a modular form is a section of a representation of weight ρ of the Hodge vector bundle on $\mathfrak{A}_2$, the pullback of the Torelli morphism $\mathcal{M}_2 \to \mathfrak{A}_2$ induces a section of the representation of weight ρ of the Hodge vector bundle on $\mathcal{M}_2$.

Therefore, given f a Siegel modular function of weight ρ, $\mathrm{Cot}(f)$ is a fractional covariant (rational in term of the coefficients of the curve) of weight ρ. Note that $\mathrm{Cot}(f)$ is a polynomial covariant if and only if f has no poles at the divisor at infinity in $\overline{\mathfrak{A}_2}$ (a toroidal compactification of $\mathfrak{A}_2$). In particular, if f is a modular form, $\mathrm{Cot}(f)$ is a polynomial covariant by the Koecher principle. Reciprocally, if F is a fractional covariant, there exists a well defined Siegel modular meromorphic form f of the same weight associated to F [KPR20, §3.2]. If F is polynomial, then f is a modular form if it has no pole at Ω such that $\chi_{10}(\Omega) = 0$.

The irreducible representations ρ are of the form $\det^k \mathrm{Sym}^n$ with $k \in \mathbb{Z}$ and $n \in \mathbb{N}$ (see [KPR20, §2.2] for more details). A scalar modular form of weight k is thus a modular form of weight $\det^k$. So the covariants of order n and degree k in Hilbert's Invariant Theory of Section 2.2 will correspond to a polynomial covariant of weight $\det^{(k-n/2)} \mathrm{Sym}^n$. This is because the action of covariants on the sextic f is given by Sym^6, while the action of the curve $y^2 = f(x)$ preserving the differentials is given by $\det^{-2} \mathrm{Sym}^6$.

In particular, the polynomial covariants J_{2i}'s have the following interpretation in term of modular forms (here we use the standard cusp forms χ_{10}, χ_{12} rather than the normalised ones from [KPR20]):

$$\begin{aligned} -3\mathrm{Cot}(\chi_{12}/\chi_{10}) &= J_2, \\ 4\mathrm{Cot}(\psi_4) &= I_4, \\ 4\mathrm{Cot}(\psi_6) &= \frac{1}{2}(I_2 I_4 - 3I_6) = I_6', \\ -2^2\mathrm{Cot}(\chi_{10}) &= J_{10}. \end{aligned}$$

One can then express Igusa's invariants j_i as the following quotients of covariants of the same weight:

$$\begin{aligned} \mathrm{Cot}(\mathrm{j}_1) &= \frac{1}{256 J_{10}} \left(J2^5 - 60 J_4 J_2^3 + 216 J_6 J_2^2 + 864 J_4^2 J_2 - 5184 J_6 J_4 \right), \\ \mathrm{Cot}(\mathrm{j}_2) &= \frac{1}{32 J_{10}} \left(J_2^5 - 48 J_4 J_2^3 + 576 J_4^2 J_2 \right), \\ \mathrm{Cot}(\mathrm{j}_3) &= \frac{1}{16384 J_{10}^2} \left(J_2^{10} - 120 J_4 J_2^8 + 5760 J_4^2 J_2^6 - 138240 J_4^3 J_2^4 + 1658880 J_4^4 J_2^2 - 7962624 J_4^5 \right). \end{aligned}$$

{subsec:modpol}

3.3. **Siegel Modular Polynomials.** The modular polynomials in dimension 2 were first computed by Regis Dupont in his thesis [Dup06] for $p = 2$. The polynomials computed were in function of Igusa's invariants, and recently Enea Milio [Mil15] proposed an extension of this construction to others invariants (not necessarily of level 1) and succeeded to reduce considerably their size. In this section we briefly explain Milio's algorithm on how to compute modular polynomials in dimension 2, to show that it easily adapts to invariants with good reduction modulo 2.

For a subgroup $\Gamma \subset \Gamma_2$, $\mathbb{C}_\Gamma$ denotes the field of modular functions for Γ, $\mathbb{C}_\Gamma/\mathbb{C}_{\Gamma_2}$ is a finite algebraic extension of degree $[\Gamma_2 : \Gamma]$. Let p be a prime, $\Gamma_0(p) := \{\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma_2;\ C \equiv 0 \mod p\}$ and $\mathcal{C}_p$ the set of representative classes of $\Gamma_2/\Gamma_0(p)$ then $[\Gamma_2 : \Gamma_0(p)] = p^3 + p^2 + p + 1$.

The period matrices of the (p,p)-isogenous varieties of a variety Ω are the $p\gamma\Omega$ for $\gamma \in \mathcal{C}_p$. We consider the following definition : for $f \in \mathbb{C}_{\Gamma_2}$ and $\gamma \in \Gamma_2$, the functions f_p and f_p^γ from $\mathfrak{H}_2$ to $\mathbb{C}$

are defined by $f_p(\Omega) = f(p\Omega)$, $f_p^\gamma(\Omega) = f(p\gamma\Omega)$, where

$$\gamma_p := \begin{pmatrix} A & pB \\ C/p & D \end{pmatrix}.$$

Then $p\Omega$ is equivalent to $p\gamma\Omega$ only when $\gamma \in \Gamma_0(p)$, i.e $\mathfrak{j}_l(p\gamma\Omega) = \mathfrak{j}_l(p\Omega)$ for $l = 1, 2, 3$;

{theo1}

Theorem 3.4. *For a prime p, the function $\mathfrak{j}_{l,p} := (\mathfrak{j}_l)_p$ is modular for $\Gamma_0(p)$ and $\mathbb{C}_{\Gamma_0(p)}$ equals $\mathbb{C}(\mathfrak{j}_1, \mathfrak{j}_2, \mathfrak{j}_3, \mathfrak{j}_{l,p})$ for any $l = 1, 2, 3$.*

Proof. See [BL09a, Lemma 4.2]. □

The p^{th} modular polynomial for $\mathfrak{j}_1$ denoted by $\phi_{1,p}(X)$ is the minimal polynomial of $\mathfrak{j}_{1,p}$ over $\mathbb{C}_{\Gamma_2} = \mathbb{C}(\mathfrak{j}_1, \mathfrak{j}_2, \mathfrak{j}_3)$: $\phi_{1,p}(X) = \prod_{\gamma \in \mathcal{C}_p}(X - \mathfrak{j}_{1,p}^\gamma)$. By Theorem 3.4 we know that $\mathfrak{j}_{2,p}$ and $\mathfrak{j}_{3,p}$ are in $\mathbb{C}(\mathfrak{j}_1, \mathfrak{j}_2, \mathfrak{j}_3, \mathfrak{j}_{1,p}) = \mathbb{C}(\mathfrak{j}_1, \mathfrak{j}_2, \mathfrak{j}_3)[\mathfrak{j}_{1,p}]$, so $\mathfrak{j}_{2,p} = \phi_{2,p}(\mathfrak{j}_{1,p})$ and $\mathfrak{j}_{3,p} = \phi_{3,p}(\mathfrak{j}_{1,p})$ for $\phi_{2,p}(X)$ and $\phi_{2,p}(X)$ monic polynomials in $\mathbb{C}(\mathfrak{j}_1, \mathfrak{j}_2, \mathfrak{j}_3)[X]$ of degree less than $\deg(\phi_{1,p}(X))$. The modular polynomials $\phi_{1,p}(X)$, $\phi_{2,p}(X)$, and $\phi_{3,p}(X)$ lie in $\mathbb{Q}(\mathfrak{j}_1, \mathfrak{j}_2, \mathfrak{j}_3)[X]$ [Dup06, Theorem 5.1]. If x is a root over $\mathbb{C}$ of $\phi_{1,p}(X)$, then $(x, \phi_{2,p}(x), \phi_{3,p}(x))$ are the j-invariants of a principally polarized abelian surface (p, p)-isogenous to the variety with invariants $(\mathfrak{j}_1(\Omega), \mathfrak{j}_2(\Omega), \mathfrak{j}_3(\Omega))$.

More generally, let f_1, f_2 and f_3 be three modular functions for Γ such that $\mathbb{C}_\Gamma$ is generated by f_1, f_2 and f_3 (we say that they are Γ-birational invariants), and the level of Γ is prime to $2p$. Then the p^{th}-modular polynomials for f_1, f_2 and f_3 are:

$$\phi_{1,p}(X) = \prod_{\gamma \in \mathcal{C}_p}(X - f_{1,p}^\gamma), \quad \textit{and} \quad \phi_{l,p}(X) = \psi_{l,p}(X)/\phi'_{1,p}(X)$$

$$\text{where} \quad \psi_{l,p}(X) = \sum_{\gamma \in \mathcal{C}_p} f_{l,p}^\gamma \prod_{\gamma' \in \mathcal{C}_p \setminus \{\gamma\}} (X - f_{1,p}^{\gamma'}), \quad \textit{for} \quad l = 2, 3,$$

with $\mathcal{C}_p$ a set of representative classes of $\Gamma/(\Gamma \cap \Gamma_0(p))$.

Let us consider the modular functions for $\Gamma(2, 4)$ defined by :

$$\mathfrak{b}_i(\Omega) := \frac{\theta_i(\Omega/2)}{\theta_0(\Omega/2)} \quad \text{for} \quad i = 1, 2, 3 \quad \text{and} \quad \mathfrak{c}_i = \frac{\theta_i^2(\Omega)}{\theta_0^2(\Omega)} \quad \text{for} \quad i \in \{1, \cdots, 15\} \quad (i \text{ even})$$

and linked by the following relations:

$$\mathfrak{b}_1 = (\mathfrak{c}_1 + \mathfrak{c}_9)(1 + \mathfrak{c}_4 + \mathfrak{c}_8 + \mathfrak{c}_{12})^{-1},$$
$$\mathfrak{b}_2 = (\mathfrak{c}_2 + \mathfrak{c}_6)(1 + \mathfrak{c}_4 + \mathfrak{c}_8 + \mathfrak{c}_{12})^{-1},$$
$$\mathfrak{b}_3 = (\mathfrak{c}_3 + \mathfrak{c}_{15})(1 + \mathfrak{c}_4 + \mathfrak{c}_8 + \mathfrak{c}_{12})^{-1}.$$

Then we have: $\mathbb{C}_{\Gamma(2,4)} = \mathbb{C}(\mathfrak{c}_1, ..., \mathfrak{c}_{15}) = \mathbb{C}(\mathfrak{b}_1, \mathfrak{b}_2, \mathfrak{b}_3)$.

One can compute the polynomials $\phi_{1,p}(X)$, $\phi_{2,p}(X)$, and $\phi_{3,p}(X)$ (or ψ_2, ψ_3) using Evaluation/Interpolation using fast evaluation (and computation of the period matrix) of the $\mathfrak{b}_i$ [Dup06] and the following algorithm is a variant detailed in [Mil15, Chapitre 4]. We give a brief summary of the algorithm in Algorithm 3.1.

We assume that the modular relations $F(f_i, \mathfrak{j}_i)$ are known (alternatively that we have modular relations $F(f_i, \mathfrak{b}_i)$. They allow us to go from the $f_i(\Omega)$ to the j-invariants (or Rosenhain invariants) in the first step of the algorithm. Likewise, they allow us to recover the values of $f_{i,p}^\gamma(\Omega)$ from the values of $\mathfrak{j}_{i,p}^\gamma(\Omega)$ by using Newton's algorithm combined with a low precision computation for its initialization.

Let $n_p = p^3 + p^2 + p + 1$ be the degree of $\phi_{1,p}(X)$. The algorithm 3.1 evaluates $\phi_{1,p}(X)$ in $O(\mathcal{M}(n_p) \log n_p)$.

In the applications of algorithm 3.1, E.Milio has computed 2^{th}, 3^{th}, 5^{th} modular polynomials for several system of invariants. However his 2^{th} modular polynomials using the $\mathfrak{j}_i$ modular

Input $(f_1(\Omega), f_2(\Omega), f_3(\Omega))$ such that $\mathbb{C}_\Gamma = \mathbb{C}(f_1(\Omega), f_2(\Omega), f_3(\Omega))$, a prime p coprime with the level of Γ, $\mathcal{C}_p$ of the representative classes in $\Gamma/(\Gamma \cap \Gamma_0(p))$ and a pre-compute of the action of the representative classes in Γ_2/Γ, a precision $N \in \mathbb{N}$.

Output $\phi_{1,p}(X, f_1(\Omega), f_2(\Omega), f_3(\Omega))$ and $\psi_{l,p}(X, f_1(\Omega), f_2(\Omega), f_3(\Omega))$ at precision N for $l = 2, 3$.

- ➔ Deduce from $f_i(\Omega)$ the j-invariant $\mathrm{j}_i(\Omega)$ or the Rosenhain invariants ;
- ➔ Using these invariants construct a hyperelliptic curve $Y^2 = f(X)$ at precision N ;
- ➔ Deduce the ten $\mathfrak{c}_i(\Omega)$ at precision N using Thomae's formulae and Numerical integration for the choice of roots;
- ➔ Reverse the functions to recover Ω' at precision N using [Dup06];
- ➔ Determine Ω and $\gamma \in \Gamma_2/\Gamma$ such that $\Omega = \gamma\Omega'$ (comparing $f_i(\Omega)$'s and $f_i(\Omega')$'s);
- ➔ Compute at precision N the $\mathfrak{b}^\gamma_{i,p}(\Omega)$ for $\gamma \in \mathcal{C}_p$ using [Dup06] and the corresponding $\mathrm{j}^\gamma_{i,p}(\Omega)$;
- ➔ Compute at precision N the $f^\gamma_{i,p}(\Omega)$ for $\gamma \in \mathcal{C}_p$;
- ➔ Compute $\phi_{1,p}(X, f_1(\Omega), f_2(\Omega), f_3(\Omega))$ and $\psi_{l,p}(X, f_1(\Omega), f_2(\Omega), f_3(\Omega))$ at precision N using a tree of sub-product ;
- ➔ Compute $\phi_{1,p}, \psi_{l,p}$ at precision N for $l = 2, 3$ using fast interpolation of rational functions [Mil14];

Algorithm 3.1 Evaluation of Modular Polynomials

{algo:polmod1

invariants have bad reduction in characteristic 2. We instead used Algorithm 3.1 to compute the modular polynomials for the invariants $(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$ that reduce well modulo 2. Such polynomials parameterize the 2-isogenous Jacobians in $\mathcal{M}_2[J_2^{-1}]$. This open locus is well adapted to curves of type $(1, 1, 1)$ in characteristic two.

Remark 3.5.

- Since the invariants $(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$ and the invariants $(\mathrm{j}_1, \mathrm{j}_2, \mathrm{j}_3)$ are birationally equivalents, we could have compute the modular polynomials for $(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$ using a change of variable in the modular polynomials of $(\mathrm{j}_1, \mathrm{j}_2, \mathrm{j}_3)$. In practice this change of variable involve rational function, this was too expensive to do it directly. We might have computed it using evaluation/interpolation, but it was easier to just reuse Algorithm 3.1.
- The common denominator of $(\mathrm{j}_1, \mathrm{j}_2, \mathrm{j}_3)$ is χ_{10}, which is zero on the locus of product of elliptic curves. Denote by $\mathcal{L}_p$ the locus off the principal polarized abelian surfaces that are (p, p)-isogenous to a product of elliptic curves. It is a 2-dimensional algebraic subvariety of the moduli space $\Gamma_2\backslash\mathfrak{H}_2$ and can be parametrized by an equation $L_p = 0$. The denominator of the coefficients of $\phi_{1,p}(X, f_1(\Omega), f_2(\Omega), f_3(\Omega))$, $\psi_{1,p}(X, f_1(\Omega), f_2(\Omega), f_3(\Omega))$ and $\psi_{2,p}(X, f_1(\Omega), f_2(\Omega), f_3(\Omega))$ are thus all divisible by the polynomial L_p.
- Using $(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$, the denominator of the modular polynomials contain the locus of Jacobians which are (p, p)-isogenous to an abelian surface A with $J_2(A) = 0$. It would be interesting to have a modular interpretation of this locus, similar to the description of $\mathcal{L}_p$ above. We denote by $\mathcal{D}_p$ the locus of the denominators of the modular polynomials $\Phi_{1,p}, \Psi_{1,p}, \Psi_{2,p}$.
- We only applied Algorithm 3.1 to birational invariants of level 1. It would be interesting to find good invariants how higher levels that give smaller polynomials.

4. 2-Adic Canonical Lift of genus 2 curves

{sec:canolift}

In this section we use the modular polynomials to lift the absolute invariants, and then we explain how to lift the curves. The Frobenius induces an isogeny, and we use the modular polynomials to lift this isogeny.

The reduction modulo 2 of curves over $\mathbb{Z}_q$ follows the birational classification given by the type (1,1,1), (3,1) and (5). Note that curves of different type are not isogenous by the Frobenius, so we only need to lift two isogenous curves of the same type.

In this section, we focus on computing a canonical lift, which amount to lifting the Frobenius as above by Lubin-Serre-Tate's theorem. So we assume that $A = \operatorname{Jac} C$ is ordinary over $\mathbb{F}_q$, or equivalently, that C is of type $(1,1,1)$. Hence we can use the modular polynomials with invariants $J = (\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$ as defined in Section 3.3. We give some indications on how to lift the Frobenius for the other types (be careful that in this case the lift is no longer unique).

4.1. **Kronecker Conditions.** Let J be absolute invariants such that $J = (f_1, f_2, f_3)$ where f_i are birational invariants with good reduction modulo 2. To lift the Frobenius, we need to lift the modular relation between J and J^σ.

Let $U = (x, y, z)$ be the variable representing the absolute invariants of the curve $\mathcal{C}$ and $V = (u, v, w)$ the absolute invariants of a (p, p)-isogenous curve to $\mathcal{C}$. We let

$$\begin{aligned}\Phi_{1,p} &= \operatorname{Num}(\phi_{1,p})(u,x,y,z)\\ \Psi_{2,p} &= \operatorname{Num}(\psi_{2,p})(u,x,y,z) - v \cdot \operatorname{Den}(\psi_{2,p})(u,x,y,z)\\ \Psi_{3,p} &= \operatorname{Num}(\psi_{3,p})(u,x,y,z) - w \cdot \operatorname{Den}(\psi_{3,p})(u,x,y,z)\end{aligned}$$

where $\operatorname{Num}(\dots)$ and $\operatorname{Den}(\dots)$ are the numerator and the denominator of the computed modular polynomials. We also denote by Φ_p the column matrix with components: $\Phi_{1,p}$, $\Psi_{2,p}$ and $\Psi_{3,p}$.

We now specialize to $J = (\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$.

{kronecker_2}

Proposition 4.1. *(Kronecker condition) Let $p = 2$ and $\mathcal{A}$ an abelian surface over $\mathbb{F}_q$ such that $J_2(\mathcal{A})J_{10}(\mathcal{A}) \neq 0$. The $\mathcal{A}$ is ordinary, and is the Jacobian of a curve $\mathcal{C}$ of type $(1,1,1)$. Let $J = (\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$ be its absolute invariants (they are well defined by Theorem 2.4). Assume that $q > p^2$. Then i) $\dfrac{\partial \Phi_p}{\partial V}(J, J^\sigma)$ is invertible;*
ii) $\dfrac{\partial \Phi_p}{\partial U}(J, J^\sigma) \equiv 0 \mod p$.

Proof. When $J = (\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$, this can be checked from the coefficients of the modular polynomials computed. Since a birational change of variable induce an invertible differentiable map (at the open locus of definition), Proposition 4.1 is thus also valid for any $J = (f_1, f_2, f_3)$ well defined on the locus $J_2 J_{10} \neq 0$. This Kronecker condition generalizes the well known reduction of elliptic modular polynomials modulo p, and one can prove that it is also valid for $p > 2$ (See [MR20a]). □

Remark 4.2. J is well defined at $\mathcal{A}$ exactly when $J_2(\mathcal{A})J_{10}(\mathcal{A}) \neq 0$, so in this case J is automatically well defined at $\mathcal{A}^\sigma$, since $J(\mathcal{A}^\sigma) = J(\mathcal{A})^\sigma$. It may seem that the modular equation is not well defined if $\mathcal{A}$ is in $\mathcal{D}_p$, the denominator locus. But we can always clear the denominator, and get a modular equation on $\mathcal{A}$ and $\mathcal{A}^\sigma$ since J is well defined at both. More precisely, we can interpret the denominator as a modular form [Kie20] in order to remove the parasite factors [MR20b] introduced by the rewriting procedure [Kie20].

{subsec:liftinvariant

4.2. **Computing the Lift of Invariants.** Let J be the vector of birational invariants as above. It satisfy the Kronecker condition and we want to lift it from $\mathbb{F}_q$ to $\mathbb{Z}_q$. Suppose that we can compute efficiently the Frobenius automorphism σ of $\mathbb{Q}_q$ and $X \in \mathbb{Z}_q^3$ is an approximation of $\tilde{J}$ at precision p^k i.e $\tilde{J} - X = p^k e$ for some error e a vector over $\mathbb{Z}_q$ that we want to find.

Since $\dfrac{\partial \Phi_p}{\partial V}(X, X^\sigma)$ is invertible to have the error e we must solve over $\mathbb{Z}_q$ an equation of the form: $e^\sigma + Ae + B = 0$ (with $A \equiv 0 \mod p$) called "*Artin-Schreier equation*" in [Gau04; MR20a].

Input J, integer N the precision.
Output $\tilde{J}$ the lift of J at precision N.
➔ If $N = 1$ then return J at precision p;
➔ Else $N' = N/2$;
➔ J =HarleyDim2(J, N');
a. $G = \frac{\partial \Phi}{\partial U}(J, J^\sigma)$; $H = \frac{\partial \Phi}{\partial V}(J, J^\sigma)$; $Q = \Phi(J, J^\sigma)$;
b. $a = G.H^{-1}$, $b = Q.H^{-1}$;
c. e =ArtinSchreier(a, b, N');
d. $J = J + p^k e$;
➔ Return J ;

Algorithm 4.1 HarleyDim2

{GenHarley}

An extended Harley algorithm solves the equation $e^\sigma + Ae + B = 0$ over $\mathbb{Z}_q$ and we obtain J at a given precision.

{GenHarleyTh}

Theorem 4.3. *Let $J = (\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$ be the absolute invariants of a polarized abelian surface $\mathcal{A}$ over $\mathbb{F}_q$. If not all $\mathfrak{a}_1$, $\mathfrak{a}_2$ and $\mathfrak{a}_3$ in $\mathbb{F}_p$ then the algorithm 4.1 computes (by doubling precision) the absolute invariants of the lifting curve $\tilde{\mathcal{A}}$ over $\mathbb{Z}_q$, where $\Phi_{1,p}$ is minimal polynomial of the one element of the triple invariants not in $\mathbb{F}_p$.*

Proof. This is a standard application of the Newton lifting described above. See also [MR20a] for a generalisation to $p > 2$. □

{subsec:liftcurve}

4.3. **2-Adic Lift of the Curves.** To reconstruct the lifted curve using the lifted absolute invariants over $\mathbb{Z}_q$ we can avoid Mestre's algorithm by directly lifting a normal form equation of the curves from $\mathbb{F}_q$ to $\mathbb{Z}_q$. Indeed, the conic in Mestre's algorithm has bad reduction modulo 2, so it is not obvious how to find a rational point on it.

Let $q = 2^n$ and $\mathcal{C}$ be a genus 2 curve given over $\mathbb{F}_q$ by its normal form equation :

$$\mathcal{C} : XY^2 + (1 + aX + bX^2)Y + X^2(c + dX + X^2) = 0.$$

Since the J_{2i}'s are expressed in term of the coefficients a, b, c, and d of the equation of $\mathcal{C}$, we can also express the birational invariants (f_1, f_2, f_3) as rational functions in (a, b, c, d). Let $(\tilde{f}_1, \tilde{f}_2, \tilde{f}_3)$ be the lift of (f_1, f_2, f_3) computed in Section 4.2, and $(\tilde{a}, \tilde{b}, \tilde{c}, \tilde{d})$ be the lifts of the normal form equation of $\mathcal{C}$. The relation above provide a system of equations for $(\tilde{a}, \tilde{b}, \tilde{c}, \tilde{d})$, to which we can apply Newton lifting from the solution (a, b, c, d) modulo 2 (since everything has good reduction).

In particular, since the model $\tilde{\mathcal{C}}$ has good reduction modulo 2, the reduction w of a basis of differentials $\tilde{w}$ is well defined. Comparing w with a fixed basis $w_{\mathcal{C}}$ of $\mathcal{C}$, we get that $w = Mw_{\mathcal{C}}$ for a matrix in $\mathrm{GL}_2(\mathbb{F}_q)$. Lifting M to $\tilde{M} \in \mathrm{GL}_2(\mathbb{Z}_q)$, and setting $\tilde{w}_{\tilde{\mathcal{C}}} = \tilde{M}^{-1}\tilde{w}$, we can lift $w_{\mathcal{C}}$. As an application, let g be a vectorial modular form (with good reduction modulo 2), then $g(\mathcal{C}, \tilde{w}_{\tilde{\mathcal{C}}})$ is a lift of $g(\mathcal{C}, w_{\mathcal{C}})$.

As an example we detail the lift of the curves of type $(1, 1, 1)$ which concern all ordinary cases.

Lift of Curves of Type (1,1,1). For the curve of type $(1, 1, 1)$ over $\mathbb{F}_{2^n}$ we can compute the absolute invariants $(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$ using the relation in section 2.4 in term of the coefficients a, b, c, and d. The coefficients $\tilde{a}$, $\tilde{b}$, $\tilde{c}$, and $\tilde{d}$ of the normal form of the curve $\tilde{\mathcal{C}}$ that reduce to $\mathcal{C}$ satisfy

the following system of equations in the variables $\tilde{a}$, $\tilde{b}$, $\tilde{c}$, and $\tilde{d}$:

$$\begin{cases} \tilde{J}_4 - \tilde{J}_2^2\tilde{\mathfrak{a}}_1 &= 0, \\ \tilde{J}_8 - \tilde{J}_2^4\tilde{\mathfrak{a}}_2 &= 0, \\ \tilde{J}_{10} - \tilde{J}_2^5\tilde{\mathfrak{a}}_3 &= 0 \end{cases} \tag{8}$$

Where $(\tilde{\mathfrak{a}_1}, \tilde{\mathfrak{a}_2}, \tilde{\mathfrak{a}_3})$ are the lift of $(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$ given by the algorithm 4.1, and the expression of the J_{2i} in term of the coefficients a, b, c and d is given by [Igu60, §3]. On other hand one compute J_{2i}'s from the hyperelliptic model using the coefficients of the normal form:

$$y^2 + h(x)y = f(x) \quad \text{where} \quad h(x) = 1 + ax + bx^2 \quad \text{and} \quad f(x) = -x^3(c + dx + x^2).$$

Lemma 4.4. *Over $\mathbb{Z}_q$ the intersection of the three surfaces of Equation (8) is non-singular at (a, b, c, d) satisfying the conditions of Theorem 4.3 is non singular at precision > 1. These equations ramify modulo 2.*

Proof. Given a genus 2 curve $\mathcal{C}$ over $\mathbb{Z}_q$, two characterizations of $\mathcal{C}$ reduce well modulo 2: its normal form (a, b, c, d) and the values of J_{2i}'s at $\mathcal{C}$. Furthermore the J_{2i}'s can be expressed in function of (a, b, c, d) using [Igu60, Pages 10-12]. We have modulo 2

$$J_2 \equiv a^2b^2.$$

Over $\mathbb{Z}_q$ and if J_2 is nonzero modulo 2 (i.e $ab \not\equiv 0 \mod 2$), the system 8 defines a non-singular point in $\mathcal{M}_2[J_2^{-1}]$ [Igu60, Theorem 4]. (representing the birational class of $\tilde{C}$). Furthermore at precision 1, we have the following factorization :

$$\begin{cases} J_4 = & J_2^2(\alpha^2 + \beta^2 + \gamma^2), \\ J_8 = & J_2^4(\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2 - \mathfrak{g}^3 - \mathfrak{g}^4), \\ J_{10} = & J_2^5(\alpha^2\beta^2\gamma^2). \end{cases} \quad \text{with} \quad \mathfrak{g} = \alpha^2 + \beta^2 + \gamma^2,$$

where α, β and γ are expressed in function of (a, b, c, d) using the relations Equation (1) and Section 2. We can normalize the new equations of Equation (8) with even powers of ab. Therefore the partial derivatives at a and b of the system Equation (8) vanish. Then the determinant of the Jacobian of Equation (8) (fixing a parameter to get three variables) vanishes too. We remark that the factorization above is only available modulo 2. On other hand at precision 2 when one parameter (for instance a) is fixed, the determinant of the Jacobian matrix of Equation (8) is given by:

$$\begin{gathered} 2a^{12}\left[a^{10} + (b^3 + db)a^9 + (cb^2 + b)a^8 + (d^2b^5 + c^2b)a^7 + \right. \\ (cb^3 + b^2)a^6 + (\mathfrak{a}_3b^{15} + c^2b^7 + b^5)a^5 + \mathfrak{a}_3b^{18}a^4 + \\ (\mathfrak{a}_3db^{19} + c^4b^5)a^3 + (\mathfrak{a}_3cb^{20} + \mathfrak{a}_3b^{19})a^2 + \\ \left.(\mathfrak{a}_3c^2b^{19} + c^2b^9 + b^7)a + (\mathfrak{a}_3cb^{21} + \mathfrak{a}_3b^{20})\right]. \end{gathered}$$

The vanishing modulo 4 of the value above implies the vanishing modulo 2 of the value between the brackets. Plugging the value of $\mathfrak{a}_3$ we get that this polynomial is not identically zero, hence up to changing our (a, b, c, d) by an isomorphism it does not vanishes. Hence the determinant of the system has only 2-valuation 1. □

Remark 4.5. From [MR20a, § 4], we have a Newton algorithm to lift at precision N, (a, b, c, d) knowing that the valuation of the minor of the Jacobian matrix of Equation (8) is 1.

So we know how to compute the canonical lift of every ordinary genus 2 curve defined over $\mathbb{F}_q$, its normal form equation (hence its canonical equation by Appendix A), and lift Siegel modular forms. We now explain how to compute the Zeta function of $\mathcal{C}$ by giving equations of the isogeny induced by the lifted Frobenius. For this we first need to explain how to lift its kernel.We first explain the reduction properties of the Weierstrass points.

4.4. **Reduction of the Weierstrass Points.** Let $\mathcal{C}$ be genus 2 curve given by $XY^2+(1+aX+bX^2)Y+X^2(c+dX+X^2)=0$ over $\mathbb{F}_{2^n}$. Then the lifted coefficients $(\tilde{a},\tilde{b},\tilde{c},\tilde{d})$ determine the curve $\tilde{\mathcal{C}}$ defined over $\mathbb{Z}_q$ by :

$$Y^2+(1+\tilde{a}X+\tilde{b}X^2)Y=-X^3(\tilde{c}+\tilde{d}X+X^2).$$

And such a curve $\tilde{\mathcal{C}}$ is equivalent over $\mathbb{Z}_q$ to the curve defined by :

$$Y^2=(1+\tilde{a}X+\tilde{b}X^2)^2-4X^3(\tilde{c}+\tilde{d}X+X^2).$$

A point P on $\tilde{\mathcal{C}}$ of affine coordinates (x,y) is a Weierstrass point if and only if for $H(x)=1+\tilde{a}x+\tilde{b}x^2$ and $F(x)=x^3(\tilde{c}+\tilde{d}x+x^2)$, we have :

$$2y+H(x)=0, \quad \textit{and} \quad y^2+H(x)y+F(x)=0.$$

The five Weierstrass points of $\tilde{\mathcal{C}}$ reduce as follow :

The case of type (1,1,1). Two points reduce to P , two others reduce Q such that x_P and x_Q are the two roots modulo 2 of the equation : $H(x)=0$. And the fifth point reduces to the point at infinity.

The case of type (3,1). This case is characterized by ($a=0$ and $b\neq 0$) or ($a\neq 0$ and $b=0$) where one can remark that two points reduce to the unique point which abscissa a^{-1} or $1/\sqrt{b}$ depending on the case ($a=0$ and $b\neq 0$) or ($a\neq 0$ and $b=0$). And the three others points reduce all to the point at infinity.

The case of type (5). All the Weierstrass points reduce modulo 2 to the point at infinity .

{subsec:liftfrob}

4.5. **Computing the Lifted Frobenius.** We explain some details about the $(2,2)$-isogeny algorithm introduced by Richelot in [Ric36] and we give a simple way to compute the lifted Frobenius and the lifted Verschiebung. To express Richelot's construction in terms of quadratic splittings we use B. Smith notation in [Smi05].

For a polynomials G_1, G_2 and G_3 in $\Bbbk[X]$ we denote by : $[G_2,G_3]=G_2'G_3-G_2G_3'$ and $\det(G1,G2,G3)$ the determinant of the matrix with as coefficient (ij) the j^{th}-coefficient of G_i.

{subsec:Richelot}

Richelot Algorithm. Let $\Pi(G_1,G_2,G_3)$ be the squarefree polynomial of degree 5 or 6 of a hyperelliptic model of a genus 2 curve $\mathcal{X}$. The Richelot operator $\mathcal{R}$ is defined by :

$$\mathcal{R}(G_1,G_2,G_3):=(\delta[G_2,G_3],\delta[G_3,G_1],\delta[G_1,G_2]),$$

where $\det(G_1,G_2,G_3)\neq 0$ and $\delta=(\det(G_1,G_2,G_3))^{-1}$.

Let $(H_1,H_2,H_3)=\mathcal{R}(G_1,G_2,G_3)$ then :

- $\Pi(H_1,H_2,H_3)$ is a squarefree polynomial of degree 5 or 6 .
- $\mathcal{R}(k_1G_1,k_2G_2,k_3G_3)=(k_1^{-1}H_1,k_2^{-1}H_2,k_3^{-1}H_3)$ for a nonzero k_i's in the base field ;
- $\mathcal{R}(G_2,G_3,G_1)=(H_2,H_3,H_1)$ and $\mathcal{R}(G_3,G_1,G_2)=(H_3,H_1,H_2)$;
- $\mathcal{R}(H_1,H_2,H_3)=(G_1,G_2,G_3)$.

{richelot}

Lemma 4.6. *Let $\mathcal{X}: v^2=f_{\mathcal{X}}(u)$ be a curve of genus 2 . For each nonsingular quadratic splitting $G=(G_1,G_2,G_3)$ of $f_{\mathcal{X}}$, we define $\mathcal{X}_G$ to be the curve given by $\mathcal{X}_G: v^2=f_{\mathcal{X}_G}:=\Pi(\mathcal{R}(G))$. Then $\mathcal{X}_G$ is a curve of genus 2 such that $\operatorname{Jac}\mathcal{X}$ and $\operatorname{Jac}\mathcal{X}_G$ are (2,2)-isogenous by the isogeny ϕ of kernel generated by divisors classes $[(G_1(u),0)]$, $[(G_2(u),0)]$ and $[(G_3(u),0)]$. Further, $\mathcal{R}(G)$ defines the dual isogeny $\widehat{\phi}$ of ϕ on $\operatorname{Jac}\mathcal{X}_G$.*

Proof. By using the Theorem.8.4.11 and Proposition.8.4.12 in [Smi05]. □

It remains to identify the non singular quadratic splitting $G=(G_1,G_2,G_3)$, such that $\Pi(\mathcal{R}(G))$ corresponds to the action of the lift Σ of the p^{th}-Frobenius morphism.

Reduction of the Kernel. Let's consider a symplectic basis P, Q, R and S of $\mathrm{Jac}(\mathcal{C})[2]$ where P and Q étale, R and S moderately ramified, and R is the dual of P, and S the dual of Q for the Weil-Pairing. An isotropic kernel $\tilde{\mathcal{K}}$ of the lifted $(2,2)$-isogeny from $\mathrm{Jac}(\tilde{\mathcal{C}})$ has three possibilities of reduction on $\mathrm{Jac}(\mathcal{C})$:

(1) $\tilde{\mathcal{K}} = \langle \tilde{R}, \tilde{S} \rangle$, the only kernel which reduces to $\langle 0 \rangle$. It corresponds to the kernel of the canonical lift of the Frobenius.
(2) $\tilde{\mathcal{K}}$ reduces to a cyclic group of cardinality 2 modulo p. There are six possibilities: $\langle \tilde{P}, \tilde{S} \rangle, \langle P \tilde{+} R, \tilde{S} \rangle, \langle \tilde{Q}, \tilde{R} \rangle, \langle Q \tilde{+} S, \tilde{R} \rangle, \langle P \tilde{+} Q, R \tilde{+} S \rangle, \langle P + \tilde{Q} + R, R \tilde{+} S \rangle$.
(3) The remaining 8 kernels $\tilde{\mathcal{K}}$ reduce to $\langle P, Q \rangle$ corresponding to the Verschiebung. The canonical lift of the Verschiebung, defined as the dual of the canonical lift of the Frobenius, is the only kernels among these whose points are defined in an étale extension of $\mathbb{Q}_q$. The points of the other kernels live in some moderately ramified extension.

And we get the 15 isogenies (counting with multiplicity)corresponding to the roots of $\phi_{1,p}$.

Note that type (3,1) has p-rank 1 and the type (5) has p-rank 0. And in the both cases several isogenies reduce to the Frobenius.

{Frob}

Proposition 4.7. *In the case of type (1,1,1): The conjugate genus two curve $\tilde{\mathcal{C}}^{\Sigma}$ over $\mathbb{Z}_q$ of $\tilde{\mathcal{C}}$ is defined by the equation : $Y^2 = \Pi\mathcal{R}(G_1, G_2, G_3)$, where : $G_1(u) = (u - x_1)(u - x_2)$ and $G_2(u) = (u - x_3)(u - x_4)$ and $x_1 = x_2 \mod 2$ and $x_3 = x_4 \mod 2$ are the solutions of the equation : $1 + ax + bx^2 = 0$.*

Proof. Using Lemma 4.6 and the kernel's reduction properties we deduce that the nonsingular quadratic splittings G of the equation $\tilde{\mathcal{C}}$ corresponding to the Frobenius $\Sigma : \tilde{\mathcal{C}} \to \tilde{\mathcal{C}}^{\Sigma}$ is defined by the divisors that reduce modulo 2 to a principal divisor.

Set $G_1(u) = (u - x_1)(u - x_2)$ and $G_2(u) = (u - x_3)(u - x_4)$ where $x_1 = x_2 \mod 2$ and $x_3 = x_4 \mod 2$ are the solutions of the equation : $1 + ax + bx^2 = 0$. The corresponding divisors are $\tilde{D}_1 = P_1 + P_2 - 2\infty$ and $\tilde{D}_1 = P_3 + P_4 - 2\infty$ that reduce modulo 2 to $\mathrm{div}(u - x_1)$ and $\mathrm{div}(u - x_3)$. And the divisor defined by G_3 reduce to 0. Then $\mathcal{R}(G_1, G_2, G_3)$ corresponds to the Frobenius computation using Richelot. □

In the case of type (3,1): Set $G_k(u) = (u - x_0)^2 \mod 2$ for a $k \in \{1, 2, 3\}$ where x_0 is the unique solution of the equation $1 + ax = 0$ or $1 + bx^2 = 0$ depending on the case. The divisor defined by $G_k(u)$ reduces to $\mathrm{div}(u - x_0)$ and the others divisors to 0. Thus the non trivial kernels modulo 2 are those defined by (G_1, G_2, G_3) where one $G_k(u) = (u - x_0) \mod 2$ defines the unique non trivial divisor class. The other isogenies reduce to the Frobenius.

In the case of type (5): for every the nonsingular quadratic splittings G of the equation $\tilde{\mathcal{C}}$ the divisors defined by $G_i(u)$ reduce to 0.

{rem:versch}

Remark 4.8. Let's consider,

$$\Sigma : \mathrm{Jac}\,\tilde{\mathcal{C}} \longrightarrow \mathrm{Jac}\,\tilde{\mathcal{C}}^{\Sigma} \quad \textit{and} \quad \widehat{\Sigma} : \mathrm{Jac}\,\tilde{\mathcal{C}}^{\Sigma} \longrightarrow \mathrm{Jac}\,\tilde{\mathcal{C}}$$

If G defines the kernel of the Frobenius Σ, then $\mathcal{R}(G)$ defines the kernel of the Verschiebung $\widehat{\Sigma}$ on $\mathrm{Jac}\,\tilde{\mathcal{C}}^{\Sigma}$. Applying this to $\mathrm{Jac}\,\mathcal{C}^{\Sigma^{-1}}$ this allows us to identify the Verschiebung $\widehat{\Sigma} : \mathrm{Jac}\,\mathcal{C} \to \mathrm{Jac}\,\mathcal{C}^{\Sigma^{-1}}$ on $\mathrm{Jac}\,\mathcal{C}$.

5. Application to point counting

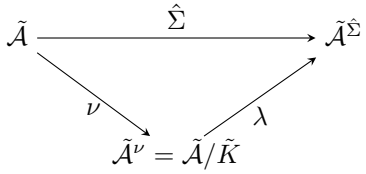
{sec:pointcounting}

In addition to the computation of lift of modular forms using the lifted curves equations, the lifted Verschiebung also gives essential information about the characteristic polynomials of the Frobenius of the ordinary genus 2 curves. For the following we detail an extension of Satoh's method to ordinary genus 2 curves.

5.1. **Description and Complexity of the Algorithm.** Let $\mathcal{C}$ be an ordinary genus 2 curve, $\mathcal{A}$ the Jacobian variety of $\mathcal{C}$ over $\mathbb{Z}_q$. In this section we give a details of the evaluation of the Verschiebung the action on the 2-torsion group. The q^{th}-power Frobenius morphism decomposes as follow :

$$\mathcal{A} \longrightarrow \mathcal{A}^{\sigma} \longrightarrow \cdots \longrightarrow \mathcal{A}^{\sigma^{n-1}}$$

Let Σ from $\tilde{\mathcal{A}}$ to $\tilde{\mathcal{A}}^{\Sigma}$ be the lift of the Frobenius morphism σ from $\mathcal{A}$ to $\mathcal{A}^{\sigma}$. Then $\hat{\Sigma}$ decomposes as follow :



Where ν is normalized Verschiebung computed using the Richelot Formulea and λ is an isomorphism between $\tilde{\mathcal{A}}/\tilde{K}$ and $\tilde{\mathcal{A}}^{\hat{\Sigma}}$. Since ν is normalized its action is trivial on the canonical basis of differential forms, and we only need the action of the isomorphism λ on the differential forms to get the one of the Verschiebung $\hat{\Sigma}$.

More concretely, the abelian surfaces are described explicitly by curves in the algorithm: $\tilde{\mathcal{A}}$, $\tilde{\mathcal{A}}^{\hat{\Sigma}} = \mathrm{Jac}(\tilde{\mathcal{C}}^{\hat{\Sigma}})$, $\tilde{\mathcal{A}}^{\nu} = \mathrm{Jac}(\tilde{\mathcal{C}}^{\nu})$ where $\tilde{\mathcal{C}}^{\nu}$ is described by Richelot's algorithm. We recall that if $X : y^2 + h(x) = f(x)$ is the equation of an hyperelliptic curve of genus 2, its canonical basis of differentials is $w_X = (dx/(2y+h), xdx/(2y+h))$. We let M be the change of base matrix between $\hat{\Sigma}^* w_{\tilde{\mathcal{C}}^{\hat{\Sigma}}}$ and $w_{\tilde{\mathcal{C}}}$, by the above discussion, since ν is normalised, this is the same as the change of base matrix between $\lambda^* w_{\tilde{\mathcal{C}}^{\hat{\Sigma}}}$ and $w_{\tilde{\mathcal{C}}^{\nu}}$.

Then by the Galois action of Σ, it is easy to see that the change of base matrix between the canonical differential basis of $\tilde{\mathcal{C}}^{\hat{\Sigma}^n}$ and $\tilde{\mathcal{C}}^{\hat{\Sigma}^{n+1}}$ is given by $\Sigma^{-n} M$. So if we let $\hat{\Sigma}_q$ be the lift of the big Verschiebung $\hat{\sigma_q}$, the dual of the Frobenius $\pi = \pi_q$, we get that the matrix of the big Verschiebung acting on the differentials of $\tilde{\mathcal{C}}$ is $M_q = N_{\mathbb{Q}_q/\mathbb{Q}_p}(M)$. This matrix is diagonal, with eigenvalues π_1, π_2, the inversible roots of the characteristic polynomial χ_π. The other two roots are q/π_1, q/π_2.

Alternatively, rather than computing M directly, we may compute $I_k(\tilde{\mathcal{C}}^{\hat{\Sigma}})/I_k(\tilde{\mathcal{C}}^{\nu})$ to get $\det M^k$ where I_k is any covariant of degree k. This yields the following algorithm.

Initialization. Let $\mathcal{C}$ be an hyperelliptic curve of genus 2 over a finite field $\mathbb{F}_q$ (with $q = 2^n$) given by its equation : $y^2 + h(x)y = f(x)$ where $h(x) = 1 + ax + bx^2$ and $f(x) = x^3(c + dx + x^2)$. Using relations 5 one can compute the corresponding vector of invariants $J = (\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$ modulo 2.

Lift Invariants. Since the ordinary case corresponds to the type (1,1,1), Harley's algorithm in Section 4 and Algorithm 4.1 computes $\tilde{J}$ using the modular polynomials in function of $\mathfrak{a}_1$, $\mathfrak{a}_2$ and $\mathfrak{a}_3$. This computation can be done in $\tilde{O}(n^2)$, where $N = O(n^2)$ is the p-adic precision.

Lift of the Curves and the Verschiebung. We can use Section 4.3 to lift the curve C by computing $(\tilde{a}, \tilde{b}, \tilde{c}, \tilde{d})$ via a Newton iteration. This costs $\tilde{O}(N)$.

Using the properties in Sections 4 and 4.5 and Proposition 4.7 and Richelot's algorithm 4.6, one computes the normalised curve $\tilde{\mathcal{C}}^{\nu}$ whose Jacobian variety is isomorphic to the one of $\tilde{\mathcal{C}}^{\Sigma}$ in time $\tilde{O}(N)$.

Indeed, the isogenous curve $\tilde{\mathcal{C}}^{\nu}$ (whose Jacobian is $\tilde{\mathcal{A}}/\tilde{K}$) can be computed by applying Richelot algorithm 4.6 to the non singular quadratic splitting (G_1, G_2, G_3) determined using Remark 4.8.

Concretly, if (H_1, H_2, H_3) is the kernel of the Frobenius on $\tilde{\mathcal{C}}^{\hat{\Sigma}}$, the kernel of the Verschiebung on $\tilde{\mathcal{C}}$ is $\mathcal{R}(H_1, H_2, H_3)$, since it is the image of the two torsion under

$$\Sigma : \mathcal{C}^{\widehat{\Sigma}} \longrightarrow \mathcal{C}_0 \simeq \mathcal{C}.$$

Alternatively, we can test directly at weak precision the eight combinations formed by $G_1 = P_1P_3$, $G_2 = P_2P_4$ and P_5 such that $P_1 \equiv P_2 \mod 2$ and $P_3 \equiv P_4 \mod 2$.

{compute_versch}

Computing the Characteristic Polynomial of the Frobenius. Since the Frobenius decomposes as $\sigma \cdot \sigma^2 \cdots \sigma^{n-1}$, the product $\pi_1\pi_2$ of its eigenvalues is given by :

$$(\pi_1\pi_2)^k = N_{\mathbb{Q}_q/\mathbb{Q}_p}\left(\frac{I_k(\tilde{\mathcal{C}}^{\hat{\Sigma}})}{I_k(\tilde{\mathcal{C}}^{\nu})}\right)$$

where I_k is any covariant of degree k. In practice we take the Igusa-Clebsh invariants.

Let χ be characteristic polynomial of the Frobenius of $\mathcal{C}$, then $\#\operatorname{Jac} C(\mathbb{F}_q) = \chi_\pi(1)$ and the Hasse-Weil bound gives the following inequality:

$$\lceil (\sqrt{q}-1)^2 \rceil \leqslant \chi(1) \leqslant \lfloor (\sqrt{q}+1)^2 \rfloor.$$

Following [Rit03; CL08] one can use the LLL algorithm to recover P_{sym} knowing the $\pi_1\pi_2$. Using a quick algorithm in [Rit03, §4.2], $\chi_\pi(\pm X)$ is deduced from the knowledge of P_{sym} when this one is irreducible. From the Hasse-Weil bound, we deduce that the needed precision is $N = 3m/2$ [Mes02].

Theorem 5.1. *Let $\mathcal{C}$ be an ordinary hyperelliptic curve of genus 2 over a finite field $\mathbb{F}_{2^n}$ such that its invariants $(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$ satisfy the Kronecker conditions. One computes $\#JacC(\mathbb{F}_{2^n})$ (and also the characteristic polynomial of the Frobenius) using our algorithm in $\tilde{O}(n^2)$ operations, using modular polynomials in function of $(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$.*

5.2. **Example.** Let $\mathcal{C}$ be defined over $\mathbb{F}_2[T]/(m)$ with $m = T^{15} + T^5 + T^4 + T^2 + 1$ by : $y^2 + h(x)y = f(x)$ where $h(x) = 1 + ax + bx^2$ and $f(x) = -x^3(c + dx + x^2)$, and the coefficients are given by:

$$\begin{aligned}
a &= T^{14} + T^{13} + T^{12} + T^{11} + T^9 + T^7 + T^5 + T^2 + T + 1,\\
b &= T^{14} + T^{13} + T^{12} + T^{10} + T^8 + T^7 + T^5 + T^4 + T^3,\\
c &= T^{14} + T^{13} + T^{10} + T^9 + T^4,\\
d &= T^{14} + T^{13} + T^{12} + T^{11} + T^9 + T^7 + T^5 + T^2 + T;
\end{aligned}$$

Then the birational invariants are given by

$$\begin{aligned}
J = [&T^13 + T^11 + T^10 + T^9 + T^8 + T^7 + T,\\
&T^13 + T^11 + T^10 + T^9 + T^8 + T^7 + T,\\
&T^14 + T^13 + T^11 + T^8 + T^3 + T^2 + T + 1];
\end{aligned}$$

and their lifts by

$$\begin{aligned}\tilde{J} =&[1347494003227200485 0T^{14} + 167545595892549188 89T^{13} + 815200737807359767 2T^{12} + 145727722770296969 95T^{11} + \\ &911947643379713358 7T^{10} + 424052392464041830 7T^{9} + 60426900661709737 59T^{8} + 24468011854689535 757T^{7} + \\ &108790753862078851 02T^{6} + 165430222025617085 34T^{5} + 104573946645012561 90T^{4} + 10084398973515633 14T^{3} + \\ &127706434103837754 08T^{2} + 12442302921457674 557T + 7907936886510960452, \quad 939173176995296245 4T^{14} + \\ &527247181609325869 5T^{13} + 469406110944079368 2T^{12} + 116044408287762850 9T^{11} + 115404495928932374 97T^{10} + \\ &365295094271749 27T^{9} + 44661867335623973 11T^{8} + 782990315529004733 3T^{7} + 112671965422716734 34T^{6} + \\ &172536463507208231 44T^{5} + 603329650096914 934T^{4} + 174717571597380168 32T^{3} + 102166518613626841 6T^{2} + \\ &127493899949797290 51T + 17738635413684739 04, \quad 150312554274479069 39T^{14} + 180387814984792593 95T^{13} + \\ &663296546807588257 8T^{12} + 109587226261110682 3T^{11} + 149704820974398253 96T^{10} + 161407588208445644 88T^{9} + \\ &506652426100233647 5T^{8} + 156081220938228313 02T^{7} + 634684139196288477 8T^{6} + 256920760825331767 0T^{5} + \\ &175602951769292698 76T^{4} + 772991990626853181 T^{3} + 182116418347018109 25T^{2} + 315411075380424624 3T + \\ &10813538131737859899];\end{aligned}$$

The Weierstrass points on the lift are given by:

$$\begin{aligned}P1 =&(x + (-27499397306669T^{14} - 104108864093772T^{13} - 72190469780601T^{12} - 1154343335976 85T^{11} - \\ &130682791175686T^{10} + 714853447378 19T^{9} + 938104230808 62T^{8} - 791733067699 54T^{7} - 127418781818674T^{6} + \\ &168210495993 81T^{5} - 655896142469 55T^{4} + 702515723086 63T^{3} - 808356831636 68T^{2} - 108825539834 11T - \\ &140522863371668));\end{aligned}$$

$$\begin{aligned}P2 =&(x + (319313741718 63T^{14} - 865130992252 24T^{13} - 934576724260 45T^{12} + 1021506717081 27T^{11} - \\ &653055008985 74T^{10} + 111042151260 415T^{9} - 111164785066 26T^{8} - 114569669306 774T^{7} - 505170444149 22T^{6} + \\ &353431025442 49T^{5} + 682845398698 9T^{4} + 178435263333 67T^{3} - 967928823712 72T^{2} + 134680560484 65T + \\ &161612642911 60));\end{aligned}$$

$$\begin{aligned}P3 =&(x + (370584000799 07T^{14} - 908947982708 13T^{13} + 136899047104 414T^{12} + 123980821883020T^{11} + \\ &637869834059 63T^{10} - 555221757922 15T^{9} - 471674055976 72T^{8} - 662327283092 06T^{7} - 139226707950 72T^{6} + \\ &114898854962 428T^{5} + 238159821886 33T^{4} + 198458183126 94T^{3} - 886129398470 82T^{2} - 935985228430 36T + \\ &548545212911 73));\end{aligned}$$

$$\begin{aligned}P4 =&(x + (958767490964 63T^{14} - 462827695475 53T^{13} + 960999014073 66T^{12} - 108440868522 716T^{11} - \\ &108884878509 769T^{10} - 28105265738 995T^{9} - 13481999007 8416T^{8} + 36493467184 354T^{7} + 34610520131 656T^{6} + \\ &586613448212T^{5} - 40588267667 491T^{4} - 68511278224 546T^{3} + 44626765726 166T^{2} + 2692664208 5156T - \\ &192353544241 43));\end{aligned}$$

$$\begin{aligned}P_5 =& -(4x + (-5493864730017 40T^{14} + 185416724591973T^{13} - 2687545533424 94T^{12} - 9010553886254T^{11} - \\ &160744857714336T^{10} - 39559684037 2744T^{9} + 39500688697 0112T^{8} - 23310194778 0155T^{7} - \\ &49539203624752 2T^{6} + 43602604384529 6T^{5} + 30103564498 4107T^{4} - 15658392432 9429T^{3} - \\ &241580812300751T^{2} + 255254170629438T + 354634709659596));\end{aligned}$$

we have $P_1 = P_2 \mod 2$ and $P_3 = P_4 \mod 2$ with $\tilde{\mathcal{C}} : y^2 = P_1P_2P_3P_4P_5$.

Using Sections 5 and 5.1, one determines the non singular quadratic splitting corresponding to the Verschiebung isogeny: And we get :

$$G1 = P_1P_3, \quad G_2 = P_4P_5, \quad G_3 = P_2 \quad \text{and we get} \quad \tilde{\mathcal{C}}^{\nu} : y^2 = \Pi\mathcal{R}(G_1, G_2, G_3).$$

And we can compute the characteristic polynomial :

$$\chi(X) = \left(X^2 + 2482103 \cdot 2^{16}X + 157 \cdot 2^{30}\right)\left(X^2 - 81333551261 \cdot 2X + 129494369717\right)$$

Acknowledgements. We thank Enea Milio for his comments and suggestion on the part concerning the computation of modular polynomials. We are supported by the FAST project and ANR CIAO. Experiments presented in this paper were carried out using PARI/GP [PAR19] and the modular polynomials were computed using https://members.loria.fr/EMilio/modular-polynomials/ .

References

[BL04] C. Birkenhake and H. Lange. *Complex abelian varieties*. Second. Vol. 302. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Berlin: Springer-Verlag, 2004, pp. xii+635. ISBN: 3-540-20488-1 (cit. on p. 12).

[BL09a] R. Bröker and . Lauter. "Modular polynomials for genus 2". In: *LMS Journal of Computation and Mathematics*, 1.12 (2009), pp. 326–339 (cit. on p. 15).

[BL09b] R. Bröker and K. Lauter. "Modular polynomials for genus 2". In: *LMS J. Comput. Math.* 12 (2009), pp. 326–339. ISSN: 1461-1570. arXiv: 0804.1565 (cit. on p. 2).

[CQ05] G. Cardona and J. Quer. "Field of moduli and field of definition for curves of genus 2". In: *Computational aspects of algebraic curves*. World Scientific, 2005, pp. 71–83 (cit. on p. 8).

[Car03] R. Carls. "Generalized AGM sequences and approximation of canonical lifts". PhD thesis. Apr. 2003. URL: http://www.math.leidenuniv.nl/carls (cit. on p. 2).

[CKL08] R. Carls, D. Kohel, and D. Lubicz. "Higher-dimensional 3-adic CM construction". In: *J. Algebra* 319.3 (2008), pp. 971–1006. ISSN: 0021-8693. DOI: 10.1016/j.jalgebra.2007.11.016 (cit. on p. 3).

[CL08] R. Carls and D. Lubicz. "A p-adic quasi-quadratic time and quadratic space point counting algorithm". In: *International Mathematics Research Notices* (2008) (cit. on pp. 2, 23).

[Cle72] A. Clebsh. "Theorie der Binärien Algebraischen Formen". In: *Verlag von B. G.* (1872) (cit. on p. 4).

[Cos11] R. Cosset. "Application des fonctions thêta à la cryptographie sur courbes hyperelliptiques". PhD thesis. 2011 (cit. on p. 12).

[Deu58] M. Deuring. *Die Klassenkörper der komplexen Multiplikation*. Vol. 2. Teubner Stuttgart, 1958 (cit. on p. 5).

[Dup06] R. Dupont. "Moyenne arithmetico-geometrique, suites de Borchardt et applications". PhD thesis. 2006 (cit. on pp. 2, 3, 12, 14–16).

[GNP] C. Gabriel, E. Nart, and J. Pujolàs. "Curves of genus two over fields of even characteristic". In: () (cit. on pp. 5, 8, 9).

[Gau04] P. Gaudry. "Algorithmes de comptage de points d'une courbe définie sur un corps fini". 2004. URL: http://www.loria.fr/~gaudry/publis/pano.pdf (cit. on p. 17).

[GHK+06] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng. "The 2-adic CM method for genus 2 curves with application to cryptography". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2006, pp. 114–129 (cit. on p. 3).

[GL10] E. Goren and K. Lauter. "Genus 2 curves with Complex Multiplication". In: (2010). URL: https://arxiv.org/abs/1003.4759v1 (cit. on p. 6).

[GL12] E. Z. Goren and K. E. Lauter. "Genus 2 curves with complex multiplication". In: *International Mathematics Research Notices* 2012.5 (2012), pp. 1068–1142 (cit. on p. 2).

[Gun63] K. Gundlach. “Die Bestimmung der Funktionen zur Hilbertschen Modulgruppe des Zahlkörpers $\mathbb{Q}\sqrt{5}$”. In: *Math. Ann.* 152 (1963), pp. 226–256 (cit. on p. 2).

[Igu60] J.-I. Igusa. “Arithmetic Variety of Moduli for Genus Two”. In: *Annals of Mathematics* Vol.72, No.3 (1960), pp. 612–649 (cit. on pp. 2–10, 19, 27, 28).

[Igu62] J. Igusa. “On Siegel modular forms of genus 2”. In: *Johns Hopkins University Press* (1962), 84(1) (cit. on p. 13).

[Igu72] J.-i. Igusa. *Theta functions*. Die Grundlehren der mathematischen Wissenschaften, Band 194. New York: Springer-Verlag, 1972, pp. x+232 (cit. on p. 13).

[Kie20] J. Kieffer. “Degree and height estimates for modular equations on PEL Shimura varieties”. In: (2020). arXiv: 2001.04138 [math.AG] (cit. on p. 17).

[KPR20] J. Kieffer, A. Page, and D. Robert. “Computing isogenies from modular equations in genus two”. In: (2020). arXiv: 2001.04137 [math.AG] (cit. on pp. 13, 14).

[LL06] R. Lercier and D. Lubicz. “A quasi-quadratic time algorithm for hyperelliptic curve point counting”. In: *Ramanujan J.* 12.3 (2006), pp. 399–423 (cit. on p. 2).

[LST64] J. Lubin, J. Serre, and J. Tate. *Elliptic curves and formal groups*. 1964. URL: http://ma.utexas.edu/users/voloch/lst.html (cit. on p. 1).

[MR20a] A. Maiga and D. Robert. “Computing the Canonical Lift of Genus 2 Curves in Odd Characteristic”. In preparation. 2020 (cit. on pp. 17–19).

[Mes91] J. Mestre. “Construction de Courbes de Genre 2 à partir de leurs Modules”. In: *In Effective Methods in Algebraic Geometry (Castiglioncello, 1990)* (1991), pp. 313–334 (cit. on pp. 4, 6).

[Mes01] J.-F. Mestre. *Lettre à Gaudry et Harley*. 2001. URL: http://www.math.jussieu.fr/mestre (cit. on p. 2).

[Mes02] J.-F. Mestre. *Notes of a talk given at the Cryptography Seminar Rennes*. 2002. URL: http://www.math.univ-rennes1.fr/crypto/2001-02/mestre.ps (cit. on pp. 2, 23).

[Mil15] E. Milio. “Calcul de polynômes modulaires en dimension 2”. PhD thesis. Dec. 2015. URL: https://members.loria.fr/EMilio (cit. on pp. 2, 14, 15).

[MR20b] E. Milio and D. Robert. “Modular polynomials on Hilbert surfaces”. In: *Journal of Number Theory* (2020) (cit. on p. 17).

[Mil14] E. Milio. “A quasi-linear algorithm for computing modular polynomials in dimension 2”. In: *arXiv preprint arXiv:1411.0409* (2014) (cit. on pp. 3, 16).

[PAR19] PARI Developers. *PARI/GP, version*2.12.1. available from http://pari.math.u-bordeaux.fr/. The PARI Group. 2019 (cit. on p. 25).

[Qin93] L. Qing. “Courbes Stables de genre 2 et leur schéma de modules”. In: *Mthematische Annalen Springer-Verlag, 295, 201-222* (1993) (cit. on p. 10).

[Ric36] F. Richelot. “Essai sur une méthode générale pour déterminer la valeur des intégrales ultra-elliptiques, fondée sur des transformations remarquables de ces transcendantes”. In: *C. R. Acad. Sci. Paris* 2 (1836), pp. 622–627 (cit. on pp. 3, 20).

[Rit03] C. Ritzenthaler. “Problèmes arithmétiques relatifs à certaines familles de courbes sur les corps finis”. PhD thesis. Université Denis Diderot Paris VII, June 2003 (cit. on pp. 2, 23).

[Sat00] T. Satoh. “The canonical lift of an ordinary elliptic curve over a finite field and its point counting”. In: *J. Ramanujan Math. Soc.* 15.4 (2000), pp. 247–270 (cit. on p. 3).

[Smi05] B. Smith. “Explicit Endomorphisms and Correspondences”. PhD thesis. Dec. 2005 (cit. on p. 20).

[Str10] M. Streng. “Complex multiplication of abelian surfaces”. PhD thesis. Leiden,marco.streng@gmail.com, 2010. ISBN: -13/EAN: 978-90-5335-291-5 (cit. on pp. 2, 13).

ubs{appendix}

Appendix A. Computing the Normal Form from an Hyperelliptique Model

Let $\mathcal{C}$ be genus 2 curve over a field $\Bbbk$. We want to compute from its hyperelliptic model the normal equation of $\mathcal{C}$ i.e the coefficients (a, b, c, d) such that $\mathcal{C}$ is defined over $\Bbbk$ by:

$$XY^2 + (1 + aX + bX^2)Y + X^2(c + dX + X^2) = 0$$

If the characteristic of $\Bbbk$ is 2. We recall that the relations between the hyperelliptic model and the coefficients (a, b, c, d) come from the invariants J_{2i}'s through the symmetric functions on α, β, γ (depending on the Artin-Shreier type).
Let $y^2 + h(x)y = f(x)$ be an hyperelliptic model of $\mathcal{C}$ over $\Bbbk$. First we compute the J_{2i}'s:
• If $J_2 \neq 0$ then $\mathcal{C}$ is ordinary which corresponds to type $(1, 1, 1)$;
• If $J_2 = 0$ and $J_6 \neq 0$ then $\mathcal{C}$ has p-rank 1 which corresponds to type $(3, 1)$;
• For the other cases $\mathcal{C}$ has p-rank 2 and the hyperelliptic model reduces $y^2 + y = x^5 + a_3x^3$ which corresponds to the type (5).
For this class of curves, we have $(a, b, c, d) = (0, 0, a_3, 0)$ for the coefficients of the normal form of $\mathcal{C}$ over $\Bbbk$.
For the two others classes the strategy is the same. We derive an isomorphism by considering the Weierstrass points for the both models of $\mathcal{C}$. In the hyperelliptic model, they correspond to the solutions of the equation $h(x) = 0$, and up to a variables change on x we may take them nonzero.
• For instance when $J_2 \neq 0$, we have two non trivial Weierstrass points with abscissa ξ and η, then we take: $b = 1/(\eta\xi)$ and $a = b(\xi + \eta)$. To compute c and d one can use together the relations Equation (1) and Equation (5) in Section 2.
• When $J_2 = 0$ with $J_6 \neq 0$ the curve $\mathcal{C}$ admits only one non trivial Weierstrass point of abscissa x_0. Then one can take $a = 1/x_0$ and $b = 0$. Therefore by solving the relations Equation (4) and Equation (6) in Section 2 we obtain c and d.

We refer to [Igu60, Pages 6-8] for the conversion between the normal model and the Artin-Shreier models.

If the characteristic of $\Bbbk$ is different from 2. Let $y^2 = u \cdot (x - \alpha_1) \cdots (x - \alpha_5)$ be the hyperelliptic model of $\mathcal{C}$ over $\overline{\Bbbk}$, and assume that all α_i's are different from 0 and 1. From [Igu60, Pages 6-8], the α_i's are solutions of the equation

$$(1 + aX + bX^2)^2 - 4X^3(c + dX + X^2) = 0.$$

Pluggint the α_i, this induces a system of equation in (a, b, c, d) which is then easy to solve.

We can also recover the normal model from the hyperelliptic model directly, without computing the Weierstrass points. We have on one hand:

$$\begin{aligned} y^2 &= (1 + ax + bx^2)^2 - 4x^3(c + dx + x^2) \\ &= -4x^5 + (b^2 - 4d)x^4 + (2ab - 4c)x^3 + (a^2 + 2b)x^2 + 2ax + 1 \end{aligned}$$

such that a has weight 1, b has weight 2, c has weight 3 and d has weight 4. And on the other hand we have the starting equation:

$$y^2 = a_5x^5 + \cdots + a_1x + a_0 \quad \text{with} \quad a_0, a_5 \quad \text{non null.}$$

By applying successively the transformations: $y \longmapsto \sqrt{a_0}y$ and $x \longmapsto -\sqrt[5]{\frac{4a_0}{a_5}}.x$ to :

$$y^2 = a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

we get

$$y^2 = -4x^5 + \frac{a_4}{a_0}\left(\frac{4a_0}{a_5}\right)^{4/5}x^4 - \frac{a_3}{a_0}\left(\frac{4a_0}{a_5}\right)^{3/5}x^3 + \frac{a_2}{a_0}\left(\frac{4a_0}{a_5}\right)^{2/5}x^2 - \frac{a_4}{a_0}\left(\frac{4a_0}{a_5}\right)^{1/5}x + 1$$

Set $\zeta = \sqrt[5]{\frac{4a_0}{a_5}}$, then the quadruplet (a, b, c, d) is defined by:

$$a = -\frac{a_4}{2a_0}\zeta, \quad b = \left(\frac{a_2}{2a_0} - \frac{a_4^2}{8a_0^2}\right)\zeta^2,$$
$$c = \left(\frac{a_3}{4a_0} + \frac{a_4^3}{32a_0^3} - \frac{a_2a_4}{8a_0^2}\right)\zeta^3, \quad d = \left[\frac{1}{4}\left(\frac{a_2}{2a_0} - \frac{a_4^2}{8a_0^2}\right)^2 - \frac{a_4}{4a_0}\right]\zeta^4.$$

Like the hyperelliptic model which is not smooth at infinity, the normal model is not smooth at the point $(0 : 1 : 0)$. By [Igu60, Pages 6-8], the normal model is obtained from collapsing a Weierstrass point P and a non Weierstrass point Q together. Once P and Q are fixed, the normal model is unique up to an action of the form (a', b', c', d') and $(a'\xi, b'\xi^2, c'\xi^3, d'\xi^4)$ for a fifth of unity ξ.

Cheikh Anta Diop University, Dakar, SENEGAL

Équipe FAST, LIRIMA (Laboratoire International de Recherche en Informatique et Mathématiques Appliquées)
Email address: abdoulaye.maiga@ucad.edu.sn

INRIA Bordeaux–Sud-Ouest, 200 avenue de la Vieille Tour, 33405 Talence Cedex FRANCE
Email address: damien.robert@inria.fr
URL: http://www.normalesup.org/~robert/

Institut de Mathématiques de Bordeaux, 351 cours de la liberation, 33405 Talence cedex FRANCE

Équipe FAST, LIRIMA (Laboratoire International de Recherche en Informatique et Mathématiques Appliquées)