Complex multiplication and canonical lifts

David R. Kohel

Abstract

The problem of constructing CM invariants of higher dimensional abelian varieties presents significant new challenges relative to CM constructions in dimension 1. Algorithms for p-adic canonical lifts give rise to very efficient means of constructing high-precision approximations to CM points on moduli spaces of abelian varieties. In particular, algorithms for 2-adic and 3-adic lifting of Frobenius give rise to CM constructions in dimension 2 (see [6] and [2]). We analyse the Galois-theoretic structure of CM points in higher dimension and combine geometric and arithmetic conditions to derive new p-adic canonical lifting algorithms using the ℓ-adic torsion structure of an ordinary abelian variety.

1 Introduction

The construction of CM invariants of abelian varieties holds interest from both a theoretical point of view, with connections to class field theory, and from a cryptographic point of view, with its application to the construction of abelian varieties over large finite fields with known prime group order. The advancement of canonical lifting algorithms in arithmetic geometry, following the original work of Satoh [13] on computing the zeta function of an elliptic curves, has provided a p-adic approach to constructive CM algorithms (following [3] and in higher dimension [6] and [2]).

In Section 2 we recall the classical theory of complex multiplication and class field theory with the view of understanding the geometry and Galois theory of the zero-dimensional schemes of CM invariants. We illustrate by examples the main pathologies which can arise in dimension 2. In Section 3 we recall the background on canonical lifts and the indicate main mechanism for constructing a canonical lift as the lift of an isogeny together with associated Galois relations. In Section 4 we treat explicit algorithms for constructing canonical lifts, in particular an approach to canonical lifting which lifts the ℓ-adic torsion structure of an abelian variety in characteristic p. We treat in detail an elementary and efficient 2-adic AGM algorithm for genus 2 curves and the ℓ-adic utilization of Richelot isogenies. We conclude with discussion of the main algorithm obstacles and potential directions for resolving them.

2 Complex multiplication

The Main Theorem of Complex Multiplication gives the relation between the ideal classes of a CM order $\mathcal{O}$ and abelian varieties with endomorphism ring $\mathcal{O}$. We recall this relationship for elliptic curves and its generalization to higher dimension.

2.1 Complex multiplication in genus 1

In genus 1, the j-variant of an elliptic curve with CM by a maximal order $\mathcal{O}_K$ in K, generates the Hilbert class field $H = K(j)/K$. More precisely, an embedding $K \to \mathbb{C}$ gives the relation between ideals of $\mathcal{O}_K$ and isomorphism classes of elliptic curves over $\mathbb{C}$:

$$\mathfrak{a} \longmapsto E_{\mathfrak{a}} = \mathbb{C}/\mathfrak{a}^{-1}.$$

The Artin isomorphism $\sigma : \mathrm{Gal}(H/K) \cong \mathrm{Cl}(\mathcal{O}_K)$, determines an action on $\{E_{\mathfrak{a}}\}$ compatible induced isogenies

$$E_{\mathfrak{a}} \to E_{\mathfrak{ap}} \cong_{\mathbb{C}} E_{\mathfrak{a}}^{\sigma(\mathfrak{p})}$$

The Galois action on $\{E_{\mathfrak{a}}\}$ may be determined on any model for $E_{\mathfrak{a}}$ over H.

A CM construction is an algorithm for the construction of invariants of an abelian variety with complex multiplication. The traditional method for elliptic curves is to evaluate the j-function at points τ in the upper half Poincaré plane, which correspond to lattices with complex multiplication. The objective of this algorithm is to determine the minimal polynomial $H_D(x)$ for $j(\tau)$ over $\mathbb{Q}$. Identifying the j-line $\mathbb{A}^1 = \mathrm{Spec}(\mathbb{Q}[x])$, this polynomial defines a zero dimensional subscheme of $\mathbb{A}^1 \subset \mathbb{P}^1 \cong X(1)$.

2.2 Complex multiplication in higher dimension

Suppose now that K is a CM field of degree $2g$ with totally real subfield F. We recall the analogous construction of an abelian variety over $\mathbb{C}$ with complex multiplication by the maximal order $\mathcal{O}_K$ (c.f. Shimura [12, §14]). Let $\Phi = (\phi_1, \dots, \phi_g)$ be a CM-type, consisting of a g-tuple of pairwise non-complex conjugate embeddings of K in $\mathbb{C}$. Then Φ defines a map $K \to \mathbb{C}^g$ by

$$z \longmapsto (z_1, \dots, z_g) = (\phi_1(z), \dots, \phi_g(z)).$$

The embedding Φ determines a complex abelian variety $A(\mathbb{C}) = \mathbb{C}^g/\Phi(\mathfrak{a}^{-1})$ with dual abelian variety $\hat{A}(\mathbb{C}) = \mathbb{C}^g/\Phi(\bar{\mathfrak{a}}\mathfrak{D}_K^{-1})$, where $\mathfrak{D}_K$ is the different $\{\alpha \in \mathcal{O}_K \,:\, \mathrm{Tr}_{\mathbb{Q}}^K(\alpha\mathcal{O}_K) \subseteq \mathbb{Z}\}$.

For any purely imaginary element ζ in K such that $\zeta\mathfrak{D}_K \subset \mathfrak{a}\bar{\mathfrak{a}}$, with $\mathrm{Im}(\phi_j(\zeta)) > 0$ for all j, we have a *polarization* of abelian varieties:

$$\Phi(\zeta) : A(\mathbb{C}) = \mathbb{C}^g/\Phi(\mathfrak{a}^{-1}) \longrightarrow \hat{A}(\mathbb{C}) = \mathbb{C}^g/\Phi(\bar{\mathfrak{a}}\mathfrak{D}_K^{-1}),$$

given by $z \mapsto \Phi(\zeta)z := (\phi_1(\zeta)z_1, \dots, \phi_g(\zeta)z_g)$. The polarization is said to be *principal* if $\Phi(\zeta)$ is an isomorphism, which holds if and only if $\zeta\mathfrak{D}_K = \mathfrak{a}\bar{\mathfrak{a}}$. This motivates the following definition.

Definition. An ideal $\mathfrak{a}$ in $\mathcal{O}_K$ is *principally polarizable* if there exists a purely imaginary element ζ in $\mathcal{O}_K$ with $\mathrm{Im}(\phi_j(\zeta)) > 0$ for all j, and such that $\zeta\mathfrak{D}_K = \mathfrak{a}\bar{\mathfrak{a}}$.

The property of being principally polarizable is a property of the ideal class, hence we may refer to a principally polarizable ideal class in $\mathcal{O}_K$. In general the polarization class is defined to be an ideal $\mathfrak{c}$ of $\mathcal{O}_F$ such that $\mathfrak{c}\zeta\mathfrak{D}_K = \mathfrak{a}\bar{\mathfrak{a}}$, well-defined in $\mathrm{Cl}^+(\mathcal{O}_F)$ for any purely imaginary ζ as above.

The set of polarized abelian varieties with polarization class $\mathfrak{c}$ are acted on by pairs $(\mathfrak{a}, \alpha)$ such that $\mathfrak{a}\bar{\mathfrak{a}} = (\alpha)$ for totally positive α in $\mathcal{O}_F$. The existence of α is equivalent to $\mathfrak{a}$ being in the kernel of the homomorphism

$$\pi : \mathrm{Cl}(\mathcal{O}_K) \longrightarrow \mathrm{Cl}^+(\mathcal{O}_F),$$

where $\pi(\mathfrak{a}) = \mathcal{O}_F \cap \mathfrak{a}\bar{\mathfrak{a}}$. The set of pairs $(\mathfrak{a}, \alpha)$ forms a group $\mathfrak{C}(\mathcal{O}_K)$ with identity $(\mathcal{O}_K, 1)$, which is an extension of $\ker(\pi)$ by the group of totally positive units $(\mathcal{O}_F^*)^+$ modulo $N_F^K(\mathcal{O}_K^*)$ (either trivial or of exponent 2).

In general the maximal order may not be in the principally polarizable class but the following lemma asserts the existence of some polarized abelian variety in each polarization class $\mathfrak{c}$ in $\mathrm{Cl}^+(\mathcal{O}_F)$. It then follows that the isomorphism classes of polarized abelian varieties with CM by $\mathcal{O}_K$ are partioned into polarization classes by $\mathrm{Cl}^+(\mathcal{O}_F)$, each of which is acted on faithfully and transitively by $\mathfrak{C}(\mathcal{O}_K)$.

Lemma 2.1. *Let K be a CM field such that K/F is not unramified. Then for every class $\mathfrak{c}$ in $\mathrm{Cl}^+(\mathcal{O}_F)$ there exists $\mathfrak{a}$ in $\mathrm{Cl}(\mathcal{O}_K)$ with polarization class $\mathfrak{c}$. Moreover there exists an ideal class $\mathfrak{d}$ in $\mathrm{Cl}^+(\mathcal{O}_F)$ such that $\pi^{-1}(\mathfrak{d})$ consists of the set of principally polarizable ideal classes in $\mathrm{Cl}(\mathcal{O}_K)$.*

Proof. Since $\mathfrak{D}_K$ is generated by elements of the form $z - \bar{z}$, both $\mathfrak{a}\bar{\mathfrak{a}}$ and $\zeta\mathfrak{D}_K$ (for any purely imaginary ζ) are generated by ideals of $\mathcal{O}_F$. Since K/F is not unramified, by class field theory $\mathrm{Cl}(\mathcal{O}_F)$ injects into $\mathrm{Cl}(\mathcal{O}_K)$, so we can find $\mathfrak{a}$ and ζ such that $\mathfrak{a}\bar{\mathfrak{a}}$ is in the class as $\mathfrak{c}\zeta\mathfrak{D}_K$. □

We now seek a description for the Galois action on the invariants of principally polarized CM abelian varieties. We specialize to CM abelian surfaces, for which the endomorphism algebra is a quartic CM field K. Generically such a field is non-Galois over $\mathbb{Q}$, and its normal closure is a degree 2 extension L/K with Galois group D_4 over $\mathbb{Q}$. There exist a triple of absolute Igusa invariants (j_1, j_2, j_3) associated to an ideal class in a maximal order $\mathcal{O}_K$ with principal polarization and CM-type Φ, contained in the Hilbert class field H^r of the reflex field K^r:

$$\begin{tikzcd}
 & L & & H^r \supseteq K^r(j_1, j_2, j_3) \\
K \arrow[ur] & & K^r \arrow[ul] \arrow[ur] & \\
F \arrow[u] & & F^r \arrow[u] & \\
 & \mathbb{Q} \arrow[ul] \arrow[ur] & &
\end{tikzcd}$$

The field K^r may be constructed in terms of the CM-type Φ but is unique up to isomorphism.

The class group $\mathrm{Cl}(\mathcal{O}_{K^r})$ acts on the group $\mathfrak{C}(\mathcal{O}_K)$ by means of the homomorphism:

$$\begin{aligned}
\mathrm{Gal}(H^r/K^r) \cong\ \mathrm{Cl}(\mathcal{O}_{K^r}) &\xrightarrow{\qquad\quad} \mathfrak{C}(\mathcal{O}_K) \\
\mathfrak{c} &\xmapsto{\qquad\quad} \big(\mathrm{N}_\Phi(\mathfrak{c}), \mathrm{N}_{\mathbb{Q}}^{K^r}(\mathfrak{c})\big)
\end{aligned} \tag{1}$$

where $\mathrm{N}_\Phi(\mathfrak{c}) = \mathrm{N}_K^L(\mathfrak{c}\mathcal{O}_L)$. Composing with multiplication in $\mathfrak{C}(\mathcal{O}_K)$, we obtain the Galois action:

$$\mathrm{Gal}(H^r/K^r) \times \mathfrak{C}(\mathcal{O}_K) \to \mathfrak{C}(\mathcal{O}_K).$$

The homomorphism (1) can fail to be injective (hence $\{j_1, j_2, j_3\}$ does not generate H^r) or fail to be surjective (in which case the Galois action is not transitive, so there are multiple Galois orbits of invariants).

As an example, failure of injectivity occurs for the CM field $K \cong \mathbb{Q}[x]/(x^4 + 46x^2 + 257)$ of class number 1 and $\mathfrak{C}(\mathcal{O}_K) = \{(\mathcal{O}_K, 1)\}$. The reflex field $K^r \cong \mathbb{Q}[x]/(x^4 + 23x^2 + 68)$, on the other hand, has class number 3, so $\mathrm{Gal}(H^r/K^r)$ maps to the unique trivial class in $\mathfrak{C}(\mathcal{O}_K)$. Note, however, that $\mathfrak{C}(\mathcal{O}_{K^r})$ is also the trivial group since $\mathrm{Cl}^+(\mathcal{O}_{F^r})$ is a group of order 3, so that the Galois action is trivially transitive on both groups. The reflex field also provides an example where the maximal order does not admit a principal polarization since the different is not in the principal ideal class.

The first examples of multiple orbits occur with class number 2. In particular, the CM invariants associated to the maximal order of the quartic CM field $K \cong \mathbb{Q}[x]/(x^4+7x^2+5)$ and its reflex field $K^r \cong \mathbb{Q}[x]/(x^4 + 11x^2 + 29)$ have trivial action by $\mathrm{Gal}(H^r/K^r)$ and $\mathrm{Gal}(H/K)$, respectively. The maximal orders of K and K^r each determine two subschemes of degree 2 over $\mathbb{Q}$, which split over their totally real subfields — the Galois conjugate pairs determine distinct CM-types on the associated CM lattices.

The action of the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, is more a subtle question, but relevant for determining the degree of the corresponding zero-dimensional schemes of CM points. The action of $\mathrm{Gal}(H^r/F^r)$ may be determined from the action of complex conjugation on ideal classes, and in general any automorphism of $\bar{\mathbb{Q}}/\mathbb{Q}$ which acts nontrivially on F^r will change the CM-type of a lattice. Thus the scheme over $\mathbb{Q}$ will represent Galois orbits from each of the possible CM-types.

Constructive CM

An analytic construction for dimension 2 uses theta functions on Siegel upper half space to determine points (j_1, j_2, j_3) in $\mathcal{M}_2(\mathbb{C})$, the moduli space of curves of genus 2 (which we identify with its image in the moduli space $\mathcal{A}_2(\mathbb{C})$ of principally polarized abelian surfaces). The result of a CM construction is an ideal in $\mathbb{Q}[j_1, j_2, j_3]$ defining the zero dimensional scheme over $\mathbb{Q}$ whose defining relations vanish on the Galois orbit of the point (j_1, j_2, j_3). In Section 4 we describe analogous algorithms for constructing these ideals, using p-adic canonical lifts.

Example. The curves $y^2 = x^5 + 1$ and $y^2 = x^6 + 1$ have absolute Igusa invariants (j_1, j_2, j_3) equal to

$$(0, 0, 0) \text{ and } (6400000/3, 440000/9, -32000/81).$$

Thus their respective defining ideals are

$$(j_1, j_2, j_3) \text{ and } (3j_1 - 6400000, 9j_2 - 440000, 81j_3 + 32000).$$

There are 19 such CM curve invariants known to exist over the rationals [14], each of which arises from an order in a cyclic quartic CM field.

In general the set of CM invariants forms a zero-dimensional subscheme of the moduli space $\mathcal{M}_2$ of genus two curves. To take an example of a non-normal quartic CM field of class number one, $K = \mathbb{Q}[x]/(x^4 + 13x^2 + 41)$, the set of absolute Igusa invariants (j_1, j_2, j_4) for a curve whose Jacobian has endormorphism ring $\mathcal{O}_K$ vanishes on the ideal of relations:

$$\begin{gathered}(4j_1^2 + 115322697j_1 - 10896201253125,\\ 64j_2^2 + 26342415j_2 + 74733890625,\\ 1024j_4^2 - 13091625j_4 + 4408171875,\\ 85j_1 - 8973j_2 - 97200j_4,\\ 25j_1 - 2920j_2 - 38016j_4 + 2460375).\end{gathered}$$

This ideal describes a subscheme of $\mathcal{M}_2$ of degree 2, which splits over the real quadratic subfield $\mathbb{Q}(\sqrt{41})$ of the reflex field of K. Here we prefer to work with

$$(j_1, j_2, j_4) = (\frac{J_2^5}{J_{10}}, \frac{J_2^3 J_4}{J_{10}}, \frac{J_2 J_8}{J_{10}}),$$

with $j_3 = J_2^2 J_6 / J_{10}$ replaced by $j_4 = (j3 - j2^2/j_1)/4$, which provides local invariants for ordinary curves in characteristic 2.[1]

3 Canonical lifts

Let A be an ordinary, simple abelian variety over a finite field k of characteristic p, and let $R = W(k)$ be its Witt ring. Then R is an extension of $\mathbb{Z}_p$ such that $[R : \mathbb{Z}_p] = [k : \mathbb{F}_p]$ equipped with a surjective homomorphism $R \to k$. Then the Frobenius automorphism of k given by $\sigma(x) = x^p$ lifts uniquely to a Frobenius automorphism $\sigma : R \to R$.

A canonical lift is an abelian variety $\tilde{A}/R$ such that

$$\tilde{A}/R \times_R k = A/k \text{ and } \mathrm{End}(\tilde{A}) = \mathrm{End}(A).$$

By the theory of Serre and Tate (see [11]), we know that an ordinary abelian variety over a finite field admits a unique canonical lift to R.

3.1 Canonical lifting conditions

We describe the general idea for construction of a canonical lift in terms of isogenies induced by a decomposition of the modules of ℓ-torsion before passing to explicit algorithms in the next section. We assume that a modular correspondence for $(\ell, \dots, \ell)$-isogenies has been precomputed as a subvariety $\mathcal{X}$ in the product $\mathcal{A} \times \mathcal{A}$ of moduli spaces of principally polarized abelian varieties (with prescribed torsion or theta structure). Such correspondences have been used for constructing the canonical lift as a lift of the Frobenius isogeny of ordinary abelian varieties in characteristic $p = \ell$. This makes use of the canonical decomposition

$$A[p] = A[p]^{loc} \oplus A[p]^{et},$$

induced by the kernels of Frobenius and Verschiebung, respectively.

Suppose now that A is ordinary over a finite field of characteristic $p \neq \ell$ and that $\ell\mathcal{O} = \mathfrak{a}\bar{\mathfrak{a}}$ where $\mathcal{O} = \mathrm{End}(A)$. Then we have an analogous decomposition

$$A[\ell] = A[\mathfrak{a}] \oplus A[\bar{\mathfrak{a}}],$$

determined by the ideal factorization. Moreover $A[\mathfrak{a}](\bar{k})$ is isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^g$ and there exists an $(\ell, \dots, \ell)$-isogeny $\varphi : A \longrightarrow B$ with $\ker \varphi = A[\mathfrak{a}]$ and $\mathrm{End}(A) = \mathrm{End}(B)$. Suppose

[1] A curve over a field of characteristic 2 is ordinary if and only if $J_2 \neq 0$, and the equality $4J_8 = J_2 J_6 - J_4^2$ implies that $j_1 j_3$ is congruent to j_2^2 at 2.

moreover that B is a Galois image of A (as happens when the image of $\mathfrak{a}$ under the Artin map is in the group generated by Frobenius at p). The canonical lift $\tilde{A}/R$ of A/k is determined by a lifting of isogenies:

$$\tilde{\varphi} : \tilde{A} \longrightarrow \tilde{B} = \tilde{A}^{\sigma^r},$$

preserving $\tilde{A}[\ell] = \ker(\varphi) \oplus \tilde{\varphi}(\tilde{A}[p])^{\sigma^{-r}}$ for some r.

3.2 Canonical lifts as CM constructions

An algorithm for the construction of the p-adic canonical lift of an elliptic curve was introduced by Satoh [13], to determine the number of points on a given $E/\mathbb{F}_q$ (in small characteristic p). The algorithm constructs the canonically lifted $\tilde{\jmath}$ of an given ordinary j-invariant j in $\mathbb{F}_q$, as the unique point $(\tilde{\jmath}, \tilde{\jmath}^\sigma)$ on

$$X_0(p) \to X(1) \times X(1).$$

An algorithm of Mestre, in 2000, introduced the use of theta functions and the AGM. This algorithm determines canonically lifted invariants $(\tilde{x}, \tilde{x}^\sigma)$ in $X_0(8) \times X_0(8)$ (and residue characteristic 2). The latter method extends naturally to higher dimension.

The idea to apply canonical lifting techniques to CM constructions was introduced in 2002 by Couveignes and Henocq [3], by determining a high precision approximation to moduli of the canonical lift as a means of computing the Hilbert class polynomial on $X(1)$. This idea was extended to abelian surfaces (Jacobians of genus 2 curves) by Gaudry et al. [6] in characteristic 2 and (extending Mestre's AGM to $(3,3)$-isogenies) by Carls et al. [2] in characteristic 3.

Example. The j-invariant $\tilde{\jmath}$ of the canonical lift of $E/\mathbb{F}_p$, whose endomorphism ring is the maximal order of $K = \mathrm{End}(E) \otimes \mathbb{Q}$, is an element of $\mathbb{Z}_p$. Nevertheless, it is algebraic and integral over $\mathbb{Z}$ and generates the Hilbert class field of K. For instance

$$E/\mathbb{F}_{59} : y^2 = x^3 + 31x + 54$$

has j-invariant 20, but its canonical lift in $\mathbb{Z}_{59}$ is

$$\tilde{\jmath} = 20 + 53 \cdot 59 + 0 \cdot 59^2 + 57 \cdot 59^3 + 9 \cdot 59^4 + 3 \cdot 59^5 + 5 \cdot 59^6 + \cdots$$

By lifting to sufficient precision we verify that $\tilde{\jmath}$ is a root of the Hilbert class polynomial

$$x^3 + 3491750x^2 - 5151296875x + 12771880859375.$$

4 Constructive CM algorithms

In general, a p-adic algorithm for constructive CM must

- construct the lifted invariant (to some finite precision), and
- recognize an algebraic number from its approximation.

The first step replaces the p-adic numbers with complex numbers in analogous analytic constructions. Rather than a period lattice, the input is a suitable curve which we lift p-adically. The second step uses an LLL reconstruction, from one or multiple points on the CM subscheme. Finding suitable input curves, whose Jacobian has endomorphism ring which is a maximal order of low class number, is the primary difficulty in the first step. The height of the moduli points (hence the resulting output size) presents the major challenge to the LLL phase. Currently several constructive CM algorithms for genus 2 CM moduli exist:

- 2-adic lifting of $(2,2)$-isogenies (Gaudry, Houtmann, K., Ritzenthaler, Weng [6]), and
- 3-adic lifting of $(3,3)$-isogenies (Carls, K., Lubicz [2]).

We first describe an AGM recursion for 2-adic lifting, which provides a simplified yet efficient algorithm for carrying out Mestre's AGM lift in characteristic 2 (c.f. Lercier and Lubicz's treatment [10] and the construction in terms of Richelot isogenies in [6]). Then we introduce a new p-adic lifting of $(2,2)$-isogenies, by adapting the modular Richelot correspondences used in [6] to any odd characteristic p.

4.1 Canonical 2-adic AGM algorithm

We give an elementary version of the AGM recursion for ordinary curves of genus 2, by finding an explicit parametrisation of theta null points in terms of invariants of curves. We differ from the standard parametrisation of 2-theta null points in a neighborhood of a point $(1:1:1:1)$ which yields a less natural parametrisation.[2] The simplicity and elegance of the equations justify giving particular treatment of the AGM algorithm relevant to the point $(1:0:0:0)$.

Rosenhain invariants in characteristic 2.

Over an extension splitting the Weierstrass points, a genus 2 curve C over a field k of characteristic 2 takes the form:

$$y^2 + x(x+1)y = x(x+1)u(x)$$

where $u(x)$ is a polynomial of degree 3, divisible by a linear factor $x + x_0$ for x_0 not in $\{0,1\}$. We set

$$a_1 = u(0),\ a_2 = u(1),\ a_3 = u(\infty),$$

where $u(\infty)$ is defined to be the leading coefficient of $u(x)$. The geometric isomorphism class of the curve is determined by the triple (a_1, a_2, a_3), independent of the value of x_0 $(\neq 0, 1)$, and provides a characteristic 2 analogue of the Rosenhain invariants $(\lambda_1, \lambda_2, \lambda_3)$ of a curve

$$y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$$

over any field of characteristic different from 2. Indeed, if $R = W(k)$ is the Witt ring of k, the curve

$$y^2 = x(x-1)(x-4\tilde{a}_1)(x-1-4\tilde{a}_2)(-4\tilde{a}_3 x + 1).$$

gives a lift of C to $K = R \otimes \mathbb{Q}$ for arbitrary lifts of a_i to $\tilde{a}_i$ in R. Thus (a_1, a_2, a_3) is a local system of coordinates at 2 for the Rosenhain invariants $(4\tilde{a}_1, 1 + 4\tilde{a}_2, 1/(4\tilde{a}_3))$.

Theta null points.

We refer to a theta null point with respect to a $(\mathbb{Z}/2\mathbb{Z})^g$-theta structure as a 2-theta null point. We consider a projective embedding provided by the system of 2-theta null constants:

$$(x_{00} : x_{01} : x_{10} : x_{11}) = \left(\vartheta\left[\begin{smallmatrix}00\\00\end{smallmatrix}\right](0,\tau) : \vartheta\left[\begin{smallmatrix}01\\00\end{smallmatrix}\right](0,\tau) : \vartheta\left[\begin{smallmatrix}10\\00\end{smallmatrix}\right](0,\tau) : \vartheta\left[\begin{smallmatrix}11\\00\end{smallmatrix}\right](0,\tau)\right).$$

Given a genus 2 curve C/k over a finite field k of characteristic 2 with Witt ring $R = W(k)$, the canonical lift of $\mathrm{Jac}(C)$ to R admits a canonical $(\mathbb{Z}/2\mathbb{Z})^2$-theta null structure over R in the neighborhood of $(1:0:0:0)$, parametrised by (x_1, x_2, x_3), where

$$x_1 = \sqrt{a_2 a_3},\ x_2 = \sqrt{a_1 a_3},\ x_3 = \sqrt{a_1 a_2},$$

by means of the map

$$(x_1, x_2, x_3) \longmapsto (1 : 2x_1 : 2x_2 : 2x_3).$$

Here $2x_i$ is well-defined as an element of $2R/4R \cong R/2R = k$ from x_i in k. Conversely we recover the curve from affine parameters (x_1, x_2, x_3), by setting

$$a_1 = x_2 x_3 / x_1,\ a_2 = x_1 x_3 / x_2,\ a_3 = x_1 x_2 / x_3.$$

This gives an initialisation of 2-theta null points, from which we derive a modular correspondence for 2-theta null points.

[2] In the neighborhood of $(1:1:1:1)$ suggested in Lercier and Lubicz [10] one obtains an affine parametrisation $(1 : 1+4t_1 : 1+4t_2 : 1+4(-t_1-t_2+2t_3))$ which lacks the symmetry and smoothness properties described here for the neighborhood of $(1:0:0:0)$. The use of a neighborhood of the latter point was suggested by Carls [1].

Duplication formulae.

Let $x_\varepsilon = \vartheta\big[{\varepsilon \atop 00}\big](0,\tau)$ and $y_\varepsilon = \vartheta\big[{\varepsilon \atop 00}\big](0,2\tau)$ be 2-theta null constants. Then the classical duplication formulae give the relations between 2-theta null points $\mathbf{x} = (x_{00} : x_{01} : x_{10} : x_{11})$ and $\mathbf{y} = (y_{00} : y_{01} : y_{10} : y_{11})$. Precisely the Riemann duplication formulas [4] are

$$y_\varepsilon^2 = \sum_{\delta\in\mathbb{F}_2^2} x_\varepsilon x_{\varepsilon+\delta}.$$

This yields the following defining relations for the modular correspondence defining 2-theta null points with $(\mathbb{Z}/2\mathbb{Z})^g$-isogenies

$$\begin{aligned}\Phi(\mathbf{x},\mathbf{y}) = \Big(&\frac{(x_{00}x_{02}+x_{20}x_{22})}{2}y_{00}^2 - \frac{(x_{00}^2+x_{02}^2+x_{20}^2+x_{22}^2)}{4}y_{01}^2,\\ &\frac{(x_{00}x_{20}+x_{02}x_{22})}{2}y_{00}^2 - \frac{(x_{00}^2+x_{02}^2+x_{20}^2+x_{22}^2)}{4}y_{10}^2,\\ &\frac{(x_{00}x_{22}+x_{02}x_{20})}{2}y_{00}^2 - \frac{(x_{00}^2+x_{02}^2+x_{20}^2+x_{22}^2)}{4}y_{11}^2\Big) = (0,0,0)\cdot\end{aligned}$$

In terms of our affine parametrisations $\mathbf{x} = (1 : 2x_1 : 2x_2 : 2x_3)$ and $\mathbf{y} = (1 : 2y_1 : 2y_2 : 2y_3)$, this gives the system of local equations:

$$\Phi(\mathbf{x},\mathbf{y}) = (y_1 + 2y_2y_3 - x_1^2u(y),\ y_2 + 2y_1y_3 - x_2^2u(y),\ y_3 + 2y_1y_2 - x_3^2u(y)) = (0,0,0), \quad (2)$$

where $u(y) = 1 + 4(y_1^2 + y_2^2 + y_3^2)$.

$$D_{\mathbf{x}}\Phi(\mathbf{x},\mathbf{y}) = -2u(y)\begin{pmatrix} x_1 & 0 & 0\\ 0 & x_2 & 0\\ 0 & 0 & x_3\end{pmatrix} \equiv 0 \bmod 2$$

and

$$D_{\mathbf{y}}\Phi(\mathbf{x},\mathbf{y}) = \begin{pmatrix} 1-8x_1^2y_1 & 2y_3-8x_2^2y_1 & 2y_2-8x_3^2y_1\\ 2y_3-8x_1^2y_2 & 1-8x_2^2y_2 & 2y_1-8x_3^2y_2\\ 2y_2-8x_1^2y_3 & 2y_1-8x_2^2y_3 & 1-8x_3^2y_3\end{pmatrix} \equiv 1 \bmod 2.$$

Moreover one sees from equations (2) that $(y_1, y_2, y_3) \equiv (x_1^2, x_2^2, x_3^2) \bmod 2$. The simultaneous solution of a root $\Phi(\mathbf{x},\mathbf{y}) = (0,0,0)$ by Newton-Raphson iteration, satisfying $\mathbf{y} = \mathbf{x}^\sigma$, yields an Artin-Schreier equation as described in Lercier and Lubicz [10].

Example. Let $C/\mathbb{F}_2$ be the curve

$$y^2 + (x^3 + x^2 + 1)y = (x^2 + 1)(x^3 + x^2 + 1).$$

By naïve point counting we find the characteristic polynomial of Frobenius $x^4+x^3+x^2+2x+4$, which generates a quartic CM field of class number 1. Over the extension $\mathbb{F}_8 = \mathbb{F}_2[w]/(w^3 + w + 1)$, we obtain a model

$$y^2 + x(x+1)y = x(x+1)(w^5x^3 + w^6x^2 + w^2x + w^3),$$

whence $(a_0, a_1, a_2) = (w^3, w^6, w^5)$. By means of the above canonical lifting algorithm, we determine the lifted invariants and compute the absolute Igusa invariants $(\tilde{\jmath}_1, \tilde{\jmath}_2, \tilde{\jmath}_4)$ to sufficient precision to recover the ideal of relations:

$$\begin{aligned}&4j_1^2 + 8218017j_1 + 146211169851,\\ &32j_2^2 + 1394199j_2 + 12065509143,\\ &2048j_4^2 - 2807745_j4 + 615519801,\\ &644j_1 - 45615j_2 - 484928j_4 + 267501,\\ &777j_1 - 55059j_2 - 584512j_4 - 576156.\end{aligned}$$

The group $\mathfrak{C}(\mathcal{O}_K)$ has order 1, and the resulting scheme splits into two rational points over the totally real subfield $\mathbb{Q}(\sqrt{17})$ of the reflex field, representing the two CM-types on $\mathcal{O}_K$.

4.2 Canonical ℓ-adic Richelot lifting algorithm

We show how the principles of this analytic parametrization can be applied to yield a canonical lifting algorithm where a correspondence is only implicitly defined in the product of rational spaces. The method applies to the above AGM correspondence, but uses the Richelot correspondences of Rosenhain invariants, as in Gaudry et al [6], which in general can be defined over a smaller degree extension of $\mathbb{F}_p$ (and $\mathbb{Z}_p$).

Let $C_{\mathbf{t}}/k$ be the genus 2 curve $y^2 = x(x-1)(x-t_0)(x-t_1)(x-t_2)$ over a finite field k of odd characteristic. A Richelot isogeny of the Jacobian of $C_{\mathbf{t}}$ is determined by a splitting

$$x(x-1)(x-t_0)(x-t_1)(x-t_2) = G_0(x)G_1(x)G_2(x)$$

where $G_0(x) = x(x-t_0)$, $G_2(x) = (x-1)(x-t_1)$, $G_2(x) = x - t_2$.

The codomain is the Jacobian of the curve $C'_{\mathbf{t}} : y^2 = \delta H_0(x)H_1(x)H_2(x)$ where δ is an explicit constant, and over some splitting field of the $H_i(x)$ we have:

$$\begin{aligned}
&H_0(x) = x^2 - 2t_2x + t_1t_2 - t_1 + t_2 = (x-u_0)(x-v_0),\\
&H_1(x) = -x^2 - 2t_2x + t_0t_2 = (x-u_1)(x-v_1),\\
&H_2(x) = (t_0 - t_1 - 1)x^2 + 2t_1x - t_0t_1 = (t_0 - t_1 - 1)(x-u_2)(x-v_2).
\end{aligned}$$

For any such triple $\mathbf{u} = (u_0, u_1, u_2)$, the conjugates v_i are determined from $\mathbf{t} = (t_0, t_1, t_2)$. By a choice of ordering for $\{u_0, u_1, u_2, v_0, v_1, v_2\}$ we obtain an isomorphism

$$C'_{\mathbf{t}} \cong C_{\mathbf{s}} : y^2 = x(x-1)(x-s_0)(x+s_1)(x+s_2).$$

This gives a space $\mathcal{X}$ with two finite morphisms to $\mathcal{M}_2(2)$:

$$\begin{tikzcd}
 & \mathcal{X} \arrow[ddl, "\phi"'] \arrow[ddr, "\psi"] & \\
 & (\mathbf{t},\mathbf{u}) \arrow[ddl, mapsto] \arrow[ddr, mapsto] & \\
\mathcal{M}_2(2) & & \mathcal{M}_2(2) \\
\mathbf{t} = (t_0, t_1, t_2) & & \mathbf{s} = (s_0, s_1, s_2)
\end{tikzcd}$$

such that $\mathbf{s} = (\psi_i(\mathbf{t},\mathbf{u}))$. Then $\mathcal{X}$ is determined in $\mathbb{A}^3 \times \mathbb{A}^3 \times \mathbb{A}^3$ by the polynomial equations

$$\begin{aligned}
&\Phi(\mathbf{t},\mathbf{u}) = (H_0(u_0), H_1(u_1), H_2(u_2)) = (0,0,0)\\
&\Psi(\mathbf{t},\mathbf{u},\mathbf{s}) = (\Psi_0(\mathbf{t},\mathbf{u},\mathbf{s}), \Psi_1(t,u,s), \Psi_2(\mathbf{t},\mathbf{u},\mathbf{s})) = (0,0,0)
\end{aligned}$$

where Ψ_i is the numerator of the rational function $s_i - \psi_i(\mathbf{t},\mathbf{u})$. We want to solve for $\mathbf{t}$ in $\mathbb{A}^3(R)$ to high precision, with auxillary point $\mathbf{u}$, such that $(\mathbf{t},\mathbf{u},\mathbf{s}) = (\mathbf{t},\mathbf{u},\mathbf{t}^{\sigma^r})$ satisfy these equations, given only the image of $\mathbf{t}$ in $\mathbb{A}^3(k)$. Assuming we have already determined $\mathbf{t}$ in $\mathbb{A}^3(R/p^{2m}R)$ such that its image in $\mathbb{A}^3(R/p^mR)$ is the canonical lift, we set

$$\mathbf{t}' = \mathbf{t} + p^m\Delta_{\mathbf{t}}, \text{ and } \mathbf{s}' = \mathbf{s} + p^m\Delta_{\mathbf{s}} = \mathbf{t}^{\sigma^r} + p^m\Delta_{\mathbf{t}}^{\sigma^r}$$

where $\mathbf{t}'$ is the canonical lift to $\mathbb{A}^3(R/p^{2m}R)$. We find $\mathbf{u}$ in $\mathbb{A}^3(R/p^{2m}R)$ by Hensel lifting such that $\Phi(\mathbf{t},\mathbf{u}) = (0,0,0)$, and suppose that

$$\mathbf{u}' = \mathbf{u} + p^m\Delta_{\mathbf{u}}$$

satisfies $\Phi(\mathbf{t}',\mathbf{u}') = (0,0,0)$. This gives the vector-matrix equation

$$\begin{aligned}
(0,0,0) &= \Phi(\mathbf{t},\mathbf{u}) + p^m\Delta_{\mathbf{t}}D_{\mathbf{t}}\Phi(\mathbf{t},\mathbf{u}) + p^m\Delta_{\mathbf{u}}D_{\mathbf{u}}\Phi(\mathbf{t},\mathbf{u})\\
&= p^m\Big(\Delta_{\mathbf{t}}D_{\mathbf{t}}\Phi(\mathbf{t},\mathbf{u}) + \Delta_{\mathbf{u}}D_{\mathbf{u}}\Phi(\mathbf{t},\mathbf{u})\Big).
\end{aligned}$$

Hence we have $\Delta_{\mathbf{u}} = -\Delta_{\mathbf{t}}D_{\mathbf{t}}\Phi(\mathbf{t},\mathbf{u})D_{\mathbf{u}}\Phi(\mathbf{t},\mathbf{u})^{-1}$. Similarly, we solve for $\Delta_{\mathbf{t}}$ such that

$$(0,0,0) = \Psi(\mathbf{t},\mathbf{u},\mathbf{s}) + p^m\Delta_{\mathbf{t}}D_{\mathbf{t}}\Psi(\mathbf{t},\mathbf{u},\mathbf{t}^{\sigma^r}) + p^m\Delta_{\mathbf{u}}D_{\mathbf{u}}\Psi(\mathbf{t},\mathbf{u},\mathbf{t}^{\sigma^r}) + p^m\Delta_{\mathbf{t}}^{\sigma}D_{\mathbf{s}}\Psi(\mathbf{t},\mathbf{u},\mathbf{t}^{\sigma^r}).$$

Dividing by p^m and eliminating $\Delta_{\mathbf{u}}$, we obtain a vector-matrix equation

$$\Delta_{\mathbf{t}}^{\sigma^r}A + \Delta_{\mathbf{t}}B + \mathbf{c} = (0,0,0) \tag{3}$$

Unlike in the case of Frobenius lifts, the vector-matrix equations so obtained in general do not satisfy $B \equiv 0 \bmod p$, thus is not in the form of an Artin–Schreier equation. This means that there generally exist multiple solutions modulo p to equation (3), and one must test whether each extends to the unique solution.

Example. Let $\mathbb{F}_{27} = \mathbb{F}_3[w]/(w^3 - w + 1)$, and let C be the curve

$$y^2 = x(x-1)(x-t_0)(x-t_1)(x-t_2),$$

where $\mathbf{t} = (t_0, t_1, t_2) = (w^{14}, w^8, 2)$. The point $\mathbf{s} = (s_0, s_1, s_2) = (w^{16}, w^{24}, 2)$ is the image of $\mathbf{t}$ by Frobenius and defines a second curve

$$y^2 = x(x-1)(x-s_0)(x-s_1)(x-s_2),$$

connected to the first by a Richelot correspondence (after renormalization). Applying the above lifting algorithm, we obtain a high precision lift of $\mathbf{t} = (t_0, t_1, t_2)$, and compute the absolute Igusa invariants (j_1, j_2, j_4) in $R/p^m R$, and use LLL lattice reduction to recover the algebraic relations among them. This yields the following polynomials for which (j_1, j_2, j_4) are zeros:

$$\begin{aligned}
&10460353203j_1^6 - 25805757743715392 10j_1^5 + \\
&\quad 247624672413238292031 27831j_1^4 - \\
&\quad 1131527415429136225188742076 16931j_1^3 - \\
&\quad 1161428320157216793464434988029 11666288j_1^2 - \\
&\quad 7078277648013508851493784913308602 2245140736j_1 - \\
&\quad 6231730470807703596640272877955131187683246723072, \\
&282429536481j_2^6 - 1017206380678738410j_2^5 + \\
&\quad 24881230456016762392 4547j_2^4 - \\
&\quad 93569901113311479610902034073j_2^3 + \\
&\quad 216371077897466304252792736388 3074j_2^2 - \\
&\quad 1127214603529291375869758062529 85141388j_2 + \\
&\quad 22265377293416386582386758988724792363081576, \\
&843330077059682304j_4^6 - 699281981805777701460 48j_4^5 - \\
&\quad 1402674787133819267135991 84j_4^4 + \\
&\quad 333222744806636241992331514 6997j_4^3 + \\
&\quad 1943175580629626592542035201748 2148j_4^2 - \\
&\quad 3248075318917536354383518465718 9382877j_4 + \\
&\quad 342957608759876088038084082162475778 19433
\end{aligned}$$

5 Conclusion

Several algorithmic obstacles present themselves when applying a p-adic CM construction. Since these algorithms take as input a curve over a small finite field, finding suitable input curves such that the endomorphism ring of the Jacobian is a maximal order of small class number is crucial to their application. For this reason, the determination of the exact endomorphism ring $\mathcal{O} = \mathrm{End}(J)$, with

$$\mathbb{Z}[\pi, \bar{\pi}] \subseteq \mathcal{O} \subseteq \mathcal{O}_K,$$

is necessary in order to determine suitability of a chosen input curve. Recent work of Freeman and Lauter [5] addresses this problem by analysing the Frobenius action on ℓ-torsion points, when only small primes ℓ divide the index $[\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]$. A general method for constructing the graphs of (ℓ, ℓ)-isogenies is still needed to differentiate the orders between $\mathbb{Z}[\pi, \bar{\pi}]$ and $\mathcal{O}_K$ when the index $[\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]$ is divisible by a large prime (applying the same algorithmic approach as for elliptic curves [8]).

Once a suitable input curve has been found, the LLL reconstruction of algebraic relations (over $\mathbb{Q}$) for the invariants remains the limiting step of p-adic CM constructions. Combining the knowledge of the Galois action on CM points with explicit class field constructions has the potential to minimise this phase of the algorithm.

One of the motivations for CM constructions is the cryptographic application to producing abelian varieties whose number of points is prime or nearly prime over a large prime field $\mathbb{F}_p$. Currently, the performance of algorithms for determining the zeta function of genus 2 curves over prime fields place limitations on the use of random genus 2 curves over $\mathbb{F}_p$ in cryptography. Instead curve generation by CM construction is typically used, which we demonstrate in the folowing example.

Example. Let C be the curve $y^2+x(x+1)y = x(x+1)(x^3+x^2+w^2x+w^3)$ over the finite field $\mathbb{F}_8 = \mathbb{F}_2[w]/(w^3+w+1)$. By naïve point counting, we find the characteristic polynomial of Frobenius is $x^4+4x^3+15x^2+32x+64$. The curve is ordinary and has complex multiplication by the maximal order of $K = \mathbb{Q}[x]/(x^4+26x^2+449)$. The maximal order has class number 3, and there exist 6 isomorphism classes of principally polarized abelian varieties.

We construct the ideal of relations in Igusa invariants (j_1, j_2, j_4) from the canonical lift of the Jacobian of C. For example, the invariant j_1 satisfies a minimal polynomial:

$$\begin{aligned} H_1(x) = {} & 2^{18}5^{36}7^{24}\,x^6 \\ & - 11187730399273689774009740470140169672902905436515808105468750000\,x^5 \\ & + 501512527690591679504420832767471421512684501403834547644662988263671875000\,x^4 \\ & - 10112409242787391786676284633730575047614543135572025667468221432704263857808262923\,x^3 \\ & + 118287000250588667564540744739406154398135978447792771928535541240797386992091828213521875\,x^2 \\ & - 2^1 3^{50} 5^{10} 11^1 13^1 53^1 701^1 16319^1 69938793494948953569198870004032131926868578084899317\,x \\ & + 3^{60} 5^{15} 23^5 409^5 179364113^5 \end{aligned}$$

Choosing the 120-bit prime

$$p = 954090659715830612807582649452910809,$$

and solving a norm equation in the endomorphism ring $\mathcal{O}_K$, we determine that the Jacobian of some curve over $\mathbb{F}_p$ with CM by $\mathcal{O}_K$ will have prime order

$$910288986956988885753118558284481029311411128276048027584310525408884449.$$

Solving for a solution to the system of equations over $\mathbb{F}_p$, we find a corresponding curve

$$\begin{aligned} C : y^2 = x^6 & + 827864728926129278937584622188769650\,x^4 \\ & + 102877610579816483342116736180407060\,x^3 \\ & + 335099510136640078379392471445640199\,x^2 \\ & + 351831044709132324687022261714141411\,x \\ & + 274535330436225557527308493450553085. \end{aligned}$$

A test of a random point on the Jacobian verifies the group order.

Cryptographic CM database. A comprehensive database for CM invariants in genera 1 and 2 is being developed to provide a relational interface to CM fields K, their Hilbert class fields, and moduli of CM abelian varieties [9]. This database includes the output of CM constructions using the p-adic algorithms of Gaudry et al. [6], Carls et al. [2], the ℓ-adic variants described in this work, and complex analytic algorithms of Houtmann [7].

Acknowledgements. The author thanks the group CACAO of INRIA/LORIA for the invitation where this article was completed, the organizers of SAGA for the invitation to present this work, and discussions with R. Carls, P. Gaudry, and D. Lubicz.

References

[1] R. Carls. Theta null points of 2-adic canonical lifts, Preprint available at `http://arxiv.org/abs/math.NT/0509092`, 2005.

[2] R. Carls, D. Kohel, D. Lubicz, Higher dimensional 3-adic CM construction, Preprint available at `http://arXiv.org/abs/math.NT/0607583`, 2006.

[3] J.-M. Couveignes and T. Henocq, Action of modular correspondences around CM points, in *Algorithmic number theory (Sydney, 2002)*, *Lecture Notes in Comp. Sci.*, **2369**, 234–243, 2002.

[4] John D. Fay, *Theta functions on Riemann surfaces*, *Lect. Notes in Comp. Sci.*, **389**, Springer–Verlag, 1973.

[5] D. Freeman and K. Lauter, Computing endomorphism rings of Jacobians of genus 2 curves over finite fields, Preprint available at `http://arxiv.org/abs/math.NT/0701305`, 2007.

[6] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng, The 2-adic CM method for genus 2 curves with application to cryptography, *Asiacrypt 2006 (Shanghai) Lect. Notes in Comp. Sci.*, **4284**, 114–129, Springer–Verlag, 2006.

[7] T. Houtmann, These, École Polytechnique, in preparation, 2007.

[8] D. Kohel, *Endomorphism rings of elliptic curves over finite fields*, PhD thesis, University of California, Berkeley, 1996.

[9] *Database of CM invariants*, `http://echidna.maths.usyd.edu.au/~kohel/dbs/`, 2007.

[10] R. Lercier and D. Lubicz. A quasi-quadratic time algorithm for hyperelliptic curve point counting, *Ramanujan J.*, **12**, no. 3, 399–423, 2006.

[11] J. Lubin, J. P. Serre and J. Tate, *Elliptic Curves and formal groups*, Notes available at `http://ma.utexas.edu/users/voloch/lst.html`, 1964.

[12] G. Shimura. *Abelian Varieties with Complex Multiplication and Modular Functions*, Princeton University Press, 1998.

[13] T. Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting, preprint, 1999.

[14] P. van Wamelen. Examples of genus two CM curves defined over the rationals, *Math. Comp.*, **68**, no. 225, 227–320, 1999.