MATHEMATICS OF COMPUTATION
Volume 84, Number 294, July 2015, Pages 1977–1989
S 0025-5718(2015)02938-X
Article electronically published on January 20, 2015

# COMPUTING ENDOMORPHISM RINGS OF ABELIAN VARIETIES OF DIMENSION TWO

GAETAN BISSON

Abstract. Generalizing a method of Sutherland and the author for elliptic cur ves we design a subexponential algorithm for computing the endomorphism rings of ordinary abelian varieties of dimension two over finite fields. Although its correctness and complexity analysis rest on several assumptions, we report on practical computations showing that it performs very well and can easily handle previously intractable cases.

**Note**. Some results of this paper previously appeared in the author's thesis, [*Endomorphism Rings in Cryptography*, Ph.D. Thesis. Eindhoven University of Technology and Institut National Polytechnique de Lorraine, 2011. ISBN: 90-386-2519-7].

## 1. Introduction

Let $\mathcal{A}$ be an absolutely simple abelian variety of dimension $g$ defined over a field with $q$ elements; its Frobenius endomorphism $\pi$ admits a characteristic polynomial $\chi_\pi \in \mathbb{Z}[t]$ of which the $2g$ complex roots have absolute value $\sqrt{q}$. Tate [25] shows that $\chi_\pi$ not only encodes the cardinality of $\mathcal{A}$ over extension fields but also uniquely identifies its isogeny class; Pila [22] later made this seminal result effective by establishing that $\chi_\pi$ can be computed using polynomially many elementary operations in $\log(q)$.

For principally polarized abelian varieties, the computation of isogenies can also be done efficiently [20] and is particularly relevant to number theory and cryptography [16]. In the generic case where $\mathcal{A}$ is ordinary, the endomorphisms of $\mathcal{A}$ form a discrete subring of maximal rank, *an order*, $\mathrm{End}(\mathcal{A})$ of $\mathbb{Q}(\pi)$ that is stable under complex conjugation and unchanged by base field extensions; this order $\mathrm{End}(\mathcal{A})$ is a finer invariant than $\chi_\pi$, better suited to isogeny-related problems such as [24].

Its computation was first addressed by Kohel who obtained an exponential-time method for ordinary elliptic curves [17]. This method was recently improved by Sutherland and the author [5] yielding an algorithm of subexponential complexity under heuristic assumptions that were later shown to follow from the generalized Riemann hypothesis [1]. While Kohel's approach does not extend to dimension $g > 1$ [8, Example 8.3], other exponential methods exist for arbitrary $g$, namely those of Eisenträger and Lauter [14] and of Wagner [27].

This paper generalizes the techniques of [5], [1] to absolutely simple, ordinary, principally polarized abelian varieties of dimension $g = 2$ and obtains the first subexponential algorithm for computing their endomorphism rings; its asymptotic

Received by the editor September 24, 2012 and, in revised form, October 15, 2013.
2010 *Mathematics Subject Classification.* Primary 11Y40, 14Q15.

complexity is

$$L(q)^{g^2\sqrt{3}/2+o(1)} \qquad \text{where} \qquad L(q) = \exp\sqrt{\log(q)\cdot\log\log(q)}.$$

Both its correctness and complexity bound rest on heuristic assumptions besides the generalized Riemann hypothesis, and require the exclusion of a zero-density set of worst-case varieties. Nevertheless, we find that it performs very well on examples of moderate size which were previously intractable. Although most of the techniques developed here apply to abelian varieties of arbitrary dimension, we focus our analysis on the case $g = 2$ which is of most interest to cryptography.

Section 2 discusses the connection between isogenies and endomorphisms. Sections 3 and 4 then describe how to compute isogenies and endomorphisms that allow us to exploit this connection, and Section 5 puts this together into an algorithm for comparing candidate rings; Section 6 then explains how to identify a lattice, from which the endomorphism ring is eventually recovered in Section 7. Finally, Section 8 reports on practical computations.

## 2. Isogenies and endomorphism rings

We assume some familiarity with abelian varieties, isogenies, and endomorphism rings; we refer to [11, Chapter V] for background material and to [23] for complex multiplication.

Again, consider an absolutely simple, ordinary, principally polarized abelian variety $\mathcal{A}$ of dimension $g$ over a field with $q$ elements, and fix an isomorphism of its endomorphism algebra $\mathbb{Q}(\pi) = \mathbb{Q} \otimes \mathrm{End}(\mathcal{A})$ with a number field $K$; this field is called the *complex multiplication field* of $\mathcal{A}$ and is a totally imaginary quadratic extension of a totally real number field $K_0$ of degree $g$. Waterhouse [28] shows that the endomorphism rings of abelian varieties isogenous to $\mathcal{A}$ are exactly those orders of $K$ stable under complex conjugation that contain $\mathbb{Z}[\pi, \overline{\pi}]$, where $\overline{\pi} = q/\pi$; they form a finite lattice (in the set-theoretic sense) with supremum the ring of integers $\mathcal{O}_K$.

Following Fouquet and Morain [15], we say that an isogeny $\phi : \mathcal{A} \to \mathcal{B}$ is *horizontal* when $\mathrm{End}(\mathcal{A})$ and $\mathrm{End}(\mathcal{B})$ are the same order in $K$, and *vertical* otherwise. In a sense, horizontal isogenies are the prevalent case:

**Lemma 2.1.** *If $\phi : \mathcal{A} \to \mathcal{B}$ is an isogeny with kernel isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^g$, the index $[\mathrm{End}(\mathcal{A}) + \mathrm{End}(\mathcal{B}) : \mathrm{End}(\mathcal{A}) \cap \mathrm{End}(\mathcal{B})]$, which we call the* distance *between the orders $\mathrm{End}(\mathcal{A})$ and $\mathrm{End}(\mathcal{B})$, is a divisor of $\ell^{2g-1}$.*

*Proof.* Since $\phi$ splits the multiplication-by-$\ell$ map, we have $\ell\,\mathrm{End}(\mathcal{A}) \subset \mathrm{End}(\mathcal{B})$ and, the latter being an order, we further have $\mathbb{Z} + \ell\,\mathrm{End}(\mathcal{A}) \subset \mathrm{End}(\mathcal{B})$; we thus obtain the lattice of Figure 1. As they are indices of the form $[\mathcal{O} : \mathbb{Z} + \ell\mathcal{O}]$, the products $bcd$, $ace$, and $cde$ are all equal to $\ell^{2g-1}$ which implies $bcd \cdot ace/cde = \ell^{2g-1}$ and hence $ab = \ell^{2g-1}/c$. □

Since the distance between endomorphism rings of isogenous abelian varieties divides the index $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$, vertical isogenies only exist for finitely many primes $\ell$. On the other hand, horizontal isogenies occur for a positive density of primes $\ell$ and their graph structure is relatively well understood; as we will see, they form a Cayley graph for the following group.

**Definition 2.2.** For any order $\mathcal{O}$ in a complex multiplication field $K$, denote by $I_{\mathcal{O}}$ the group consisting of all pairs $(\mathfrak{a}, \rho)$ satisfying $\mathfrak{a}\overline{\mathfrak{a}} = \rho\mathcal{O}$ with $\mathfrak{a}$ an invertible

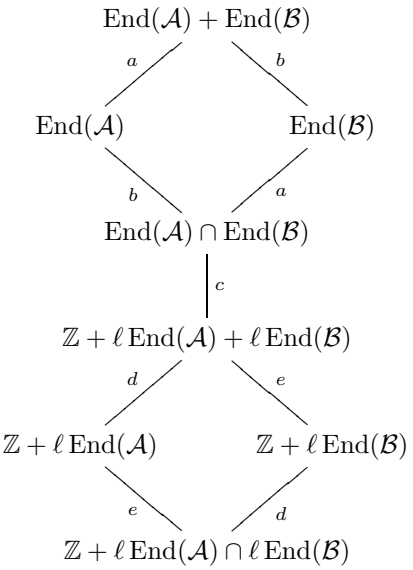


FIGURE 1. Lattice of orders for an isogeny $\mathcal{A} \to \mathcal{B}$ of kernel $(\mathbb{Z}/\ell\mathbb{Z})^g$.

fractional ideal of $\mathcal{O}$ and $\rho$ a totally positive element of $K_0$, endowed with componentwise multiplication; also, let $P_{\mathcal{O}}$ be its subgroup formed by pairs of the form $(\mu\mathcal{O}, \mu\overline{\mu})$ for $\mu \in K$. The quotient group $I_{\mathcal{O}}/P_{\mathcal{O}}$ is called the *polarized class group* of $\mathcal{O}$ and is denoted by $\mathfrak{C}(\mathcal{O})$.

Note that this group is unchanged if we additionally require that $\mathfrak{a}$ (and $\mu$) be coprime to a fixed integer $\nu$; to allow us to compare ideals of $I_{\mathcal{O}}$ as $\mathcal{O}$ varies, we will from now on only consider class representatives of this type with $\nu = \mathrm{disc}(\mathbb{Z}[\pi, \overline{\pi}])$. For maximal orders, the theorem below shows that such elements correspond to horizontal isogenies.

**Theorem 2.3** ([23, §14]). *When* $\mathrm{End}(\mathcal{A})$ *is maximal, one can associate a horizontal isogeny of degree* $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})$ *to every* $(\mathfrak{a}, \rho) \in I_{\mathrm{End}(\mathcal{A})}$ *with* $\mathfrak{a}$ *coprime to the characteristic, so as to induce a free action of* $\mathfrak{C}(\mathrm{End}(\mathcal{A}))$ *on the isogeny class of* $\mathcal{A}$ *up to isomorphisms.*

The corresponding result for non-polarized abelian varieties, which sees the polarized class group replaced by the classical ideal class group, also holds for arbitrary orders [23, §7], [28, §7]. While only the case of maximal endomorphism rings has been treated in the literature, the above theorem is expected to hold for arbitrary orders too, and we assume that it does as one of our heuristics in this paper.

**Hypothesis** (A). *Theorem* 2.3 *holds even if* $\mathrm{End}(\mathcal{A})$ *is not maximal.*

## 3. Evaluating Isogenies

Until recently, isogenies could only be efficiently evaluated for elliptic curves [26] and special families in higher dimension [7]. The work of Lubicz and Robert [20] has made it possible to efficiently compute general, polarization-preserving isogenies in dimension $g > 1$; more precisely, we have:

**Proposition 3.1** ([12, Theorem 1.2])**.** *Let $\mathcal{H}$ be a rational isotropic subgroup isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^g$ of an abelian variety of dimension $g = 2$ with $\ell$ a prime different from the characteristic. The separable isogeny with kernel $\mathcal{H}$ can be evaluated with a worst-case complexity of $\ell^{3g+o(1)}$ operations in the base field.*

The isogenies we are concerned with correspond to elements $(\mathfrak{a}, \ell)$ of $\mathfrak{C}(\mathbb{Z}[\pi, \overline{\pi}])$; to evaluate them, we first need to identify the kernel $\mathcal{H}$ corresponding to a given $(\mathfrak{a}, \ell)$. Note that we can write $\mathfrak{a} = \ell\mathcal{O} + f(\pi)\mathcal{O}$ for some factor $f$ of $\chi_\pi \bmod \ell$. Now we take $\mathcal{H}$ to be the subgroup of $\mathcal{A}[\ell]$ on which the Frobenius acts with characteristic polynomial $f$; it is unique since we restrict to ideals $\mathfrak{a}$ coprime to $\nu = \operatorname{disc}(\mathbb{Z}[\pi, \overline{\pi}])$. In effect, this identification fixes an isomorphism between $\mathbb{Q}\otimes\operatorname{End}(\mathcal{A})$ and the complex multiplication field $K$ (mapping a fixed root of $\chi_\pi$ to the Frobenius endomorphism) as was required in Section 2, and it only matters that this be done consistently within a given isogeny class.

Points of $\mathcal{H}$ are defined over an extension field whose degree is the multiplicative order of $x$ in $\mathbb{Z}[x]/(f)/(\ell)$, that is, at most $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}) - 1$. Over that extension, an algorithm of Couveignes [13, §8] may be used to compute the $\ell$-torsion subgroup of $\mathcal{A}$ assuming that points of $\mathcal{A}$ can be drawn uniformly at random. This can be done efficiently for Jacobian varieties by using the underlying curve.

The algorithm implicitly referred to by this theorem returns a representative of the isogenous isomorphism class $\mathcal{A}/\mathcal{H}$ defined over the field of definition of individual points of $\mathcal{H}$, even if $\mathcal{H}$ itself and therefore $\mathcal{A}/\mathcal{H}$ are rational. For abelian varieties of dimension $g = 2$ represented as Jacobians of genus-two curves, one can use a method of Mestre [21] to find, after each isogeny evaluation step, a representative of the isomorphism class $\mathcal{A}/\mathcal{H}$ defined over the minimal field. See [12], [3] for details.

Abelian varieties of arbitrary dimension may be represented by theta constants. The points on such varieties are the roots of the Riemann equations, and can therefore be drawn quasi-uniformly at random by solving this system using a Gröbner basis algorithm, once enough variables are specialized to random values so that its rank is full. Isomorphism classes of abelian varieties correspond to orbits of theta constants under the action of the symplectic group, and can thus also be identified efficiently. From now on, we will, however, focus on the case where $g = 2$ and hence restrict to abelian varieties given as Jacobians of hyperelliptic curves.

## 4. Generating short relations

First recall a well-known elementary result about (polarized) class groups.

**Lemma 4.1.** *For any two orders $\mathcal{O} \subset \mathcal{O}'$ containing $\mathbb{Z}[\pi, \overline{\pi}]$, the map $(\mathfrak{a}, \rho) \in I_{\mathcal{O}} \to (\mathfrak{a}\mathcal{O}', \rho) \in I_{\mathcal{O}'}$ induces a natural morphism of polarized class groups $\mathfrak{C}(\mathcal{O}) \to \mathfrak{C}(\mathcal{O}')$; this morphism is surjective when restricted and corestricted to elements satisfying $\rho \in \mathbb{Q}$.*

The above result allows us to compare the polarized class group $\mathfrak{C}(\mathcal{O})$ as the order $\mathcal{O}$ varies. More explicitly, we use *relations* to characterize polarized class groups.

**Definition 4.2.** We call a *relation* any tuple $(\alpha_1, \ldots, \alpha_k)$ of elements of $\mathfrak{C}(\mathbb{Z}[\pi, \overline{\pi}])$. We say that this relation *holds in* $\mathcal{O}$ if the product $\alpha_1 \cdots \alpha_k$ is trivial in $\mathfrak{C}(\mathcal{O})$ through the map of the above lemma, and that it *holds in* $\mathcal{A}$ if the corresponding isogeny chain $\phi_{\alpha_1} \circ \cdots \circ \phi_{\alpha_k}$ maps $\mathcal{A}$ to an isomorphic abelian variety.

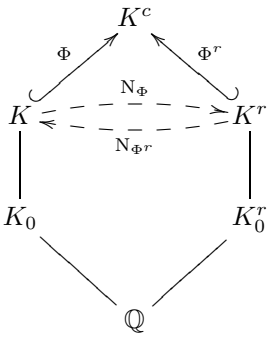


FIGURE 2. The complex multiplication field, its reflex field, and type norm maps.

By Theorem 2.3, if every relation that holds in $\mathcal{O}$ also does in $\mathcal{A}$, the group $\mathfrak{C}(\mathrm{End}(\mathcal{A}))$ must be a quotient of $\mathfrak{C}(\mathcal{O})$, and we will see later that this implies that $\mathcal{O} \subset \mathrm{End}(\mathcal{A})$ locally at almost all primes.

The computation of class groups of algebraic orders is a classical topic that has led to the development of advanced algorithms for generating ideal relations. However, to effectively compare $\mathfrak{C}(\mathcal{O})$ with $\mathfrak{C}(\mathrm{End}(\mathcal{A}))$ we require that the isogenies corresponding to the relations we select be computable in reasonable time; this places two additional constraints:

- Elements $(\alpha_i)$ of our relations must correspond to maximal isotropic isogenies.
- Their number $k$ and norms $(\mathrm{N}_{K/\mathbb{Q}}(\alpha_i))$ must be bounded.

The latter constraint is already addressed in [1, §6] whose results and proofs carry directly over to orders in CM-fields of arbitrary degree. Let us now explain how to additionally satisfy the former.

Let $\Phi$ be a type for $K$, that is, a set of representatives for embeddings of $K$ into its normal closure $K^c$ up to complex conjugation. Its *type norm*

$$\mathrm{N}_\Phi : x \longmapsto \prod_{\phi \in \Phi} \phi(x)$$

maps $K$ to its reflex field $K^r$, the fixed field of $\{\sigma \in \mathrm{Gal}(K^c/\mathbb{Q}) : \sigma\Phi = \Phi\}$, and induces a morphism taking ideals $\mathfrak{a}$ of $K$ to elements $(\mathrm{N}_\Phi(\mathfrak{a}), \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}))$ of $\mathfrak{C}(\mathcal{O}^r)$ for any order $\mathcal{O}^r$ of $K^r$ with discriminant coprime to $\nu$. Types of absolutely simple abelian varieties are primitive, which implies that $K^{r\,r} = K$; hence the type norm of the reflex type $\Phi^r$, the restriction to $K^r$ of inverses of automorphisms of $K^c$ induced by $\Phi$, or *reflex type norm*, maps ideals of $K^r$ to $\mathfrak{C}(\mathcal{O})$ for any order $\mathcal{O}$ containing $\mathbb{Z}[\pi, \overline{\pi}]$; see Figure 2.

Images through $\mathrm{N}_{\Phi^r}$ of prime ideals of $K^r$ are polarized ideals of which the corresponding isogenies can be computed using Proposition 3.1. Therefore, to obtain relations that hold in a given order $\mathcal{O}$ and whose corresponding isogenies can be efficiently evaluated, we first generate tuples of ideals $(\mathfrak{a}_i)$ of $\mathcal{O}$ whose product is principal using the method of Buchmann [9] as modified in [1, §6], and then take its

image through $\mathrm{N}_{\Phi^r} \circ \mathrm{N}_\Phi$; the total norm of the resulting relation is $\sum_i \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}_i)^{g^2}$. Formally, we obtain:

**Algorithm 4.3.**

INPUT: *An order $\mathcal{O}$ and a parameter $\gamma > 0$.*

OUTPUT: *A relation holding in $\mathcal{O}$ of which the corresponding isogeny can be computed efficiently.*

1. *Form the set $\mathfrak{B}$ of prime ideals $\mathfrak{p}$ of $\mathcal{O}$ with norm less than $L(\mathrm{disc}(\mathcal{O}))^\gamma$.*
2. *Draw a vector $x \in \mathbb{Z}^{\mathfrak{B}}$ uniformly at random with coordinates $|x_\mathfrak{p}| < \log(\mathrm{disc}(\mathcal{O}))^{4+\epsilon}$ when $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}) < \log(\mathrm{disc}(\mathcal{O}))^{2+\epsilon}$ and $x_\mathfrak{p} = 0$ otherwise.*
3. *Compute the reduced ideal representative $\mathfrak{a}$ of $\prod \mathfrak{p}^{x_\mathfrak{p}}$.*
4. *If $\mathfrak{a}$ factors over $\mathfrak{B}$ as $\prod \mathfrak{p}^{y_\mathfrak{p}}$:*
5. *Return the relation containing $\mathrm{N}_{\Phi^r}(\mathrm{N}_\Phi(\mathfrak{p}))$ with multiplicity $x_\mathfrak{p} - y_\mathfrak{p}$ for $\mathfrak{p} \in \mathfrak{B}$.*
6. *Go back to Step 2.*

For details on Step 4, and more generally on computing ideal relations in number fields, we refer to [10]. All steps above have previously been analyzed except for the evaluation of $\mathrm{N}_{\Phi^r} \circ \mathrm{N}_\Phi$ which only uses polynomial time; we therefore borrow the assumptions and complexity bound of [9] for Algorithm 4.3:

**Hypothesis** (B)**.** *The generalized Riemann hypothesis holds, and reduced ideals have the smoothness properties of integers of comparable size.*

**Proposition 4.4.** *Under Hypothesis (B), this algorithm generates a relation with total norm $L(\mathrm{disc}(\mathcal{O}))^{g^2\gamma+o(1)}$ in expected time*

$$L(\mathrm{disc}(\mathcal{O}))^{\gamma+o(1)} + L(\mathrm{disc}(\mathcal{O}))^{1/(4\gamma)+o(1)}.$$

## 5. Comparing candidate endomorphism rings

Our main idea to compute $\mathrm{End}(\mathcal{A})$ is to exploit Theorem 2.3: we compare the structure of polarized class groups of candidate endomorphism rings $\mathcal{O}$ with that of isogenies from the variety $\mathcal{A}$. For this, we generate relations that hold in $\mathcal{O}$ using Algorithm 4.3 and test whether the corresponding isogenies map to isomorphic varieties.

It is important to observe that Algorithm 4.3 only outputs relations whose elements lie in the image of $\mathrm{N}_{\Phi^r} \circ \mathrm{N}_\Phi$; these may not be all the relations that hold in $\mathcal{O}$, but only a sublattice $\Lambda_\Phi(\mathcal{O})$ of them. We start by computing this lattice and, for this, use the following algorithm.

**Algorithm 5.1.**

INPUT: *An absolutely simple, ordinary, principally polarized abelian variety $\mathcal{A}$ of dimension $g$ defined over $\mathbb{F}_q$ and an order $\mathcal{O}$ containing $\mathbb{Z}[\pi, \overline{\pi}]$.*

OUTPUT: *Whether $\Lambda_\Phi(\mathcal{O}) \subset \Lambda_\Phi(\mathrm{End}(\mathcal{A}))$.*

1. *Repeat $5g^2 \log_2(q)$ times:*
2. *Find a relation $(\alpha_1, \ldots, \alpha_k)$ of $\mathfrak{C}(\mathcal{O})$ using Algorithm 4.3.*
3. *If $\phi_{\alpha_1} \circ \cdots \circ \phi_{\alpha_k}$ does not map $\mathcal{A}$ to an isomorphic variety, return false.*
4. *Return true.*

If $\mathcal{O}' \subset \mathcal{O}$ are two orders containing $\mathbb{Z}[\pi, \overline{\pi}]$ stable under complex conjugation, it follows from Hypothesis (B) that the relations generated by Algorithm 4.3 are quasi-uniformly distributed in the quotient $\Lambda_\Phi(\mathcal{O})/\Lambda_\Phi(\mathcal{O}')$; see [1, §6] for a proof stated for imaginary quadratic fields but which readily carries over to arbitrary CM-fields. Therefore, the relations output after $5g^2 \log_2(q)$ runs of Algorithm 4.3 characterize $\Lambda_\Phi(\mathcal{O})$ with error probability at most $(1/2)^{5g^2 \log_2(q)} = 1/q^{5g^2}$.

To balance the cost of generating relations using Algorithm 4.3 with that of evaluating the corresponding isogenies, we set $\gamma = 1/(2g\sqrt{3})$ in Step 2, and obtain the following result.

**Proposition 5.2.** *Under Hypotheses (A), (B), Algorithm* 5.1 *determines whether the relation lattice* $\Lambda_\Phi$ *of* $\mathrm{End}(\mathcal{A})$ *contains that of a prescribed order* $\mathcal{O}$ *with error probability* $1/q^{5g^2}$ *using an expected*

$$L(|\operatorname{disc}(\mathcal{O})|)^{g\sqrt{3}/2+o(1)}$$

*operations in the base field.*

**Note.** Rather than generating independent relations for each order $\mathcal{O}$ of the lattice to be tested, one might be tempted to first compute the full class group structure of the maximal order $\mathcal{O}_K$ and then deduce relations of smaller orders $\mathcal{O}$ via the exact sequence:

$$1 \to \mathcal{O}^\times \to \mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{f})^\times/(\mathcal{O}/\mathfrak{f})^\times \to \mathrm{Pic}(\mathcal{O}) \to \mathrm{Pic}(\mathcal{O}_K) \to 1$$

where $\mathfrak{f}$ is the conductor of $\mathcal{O}$, that is, the largest ideal of both $\mathcal{O}$ and $\mathcal{O}_K$. This has two disadvantages: first, computing class groups is much more expensive than generating just $O(\log(q))$ relations; second, the relations of $\mathcal{O}$ given directly by the exact sequence above grow linearly in the index $[\mathcal{O}_K : \mathcal{O}]$, and deriving subexponential-size relations requires using an algorithm similar to 4.3 anyhow.

## 6. Locating the relation lattice

Before identifying orders $\mathcal{O}$ satisfying $\Lambda_\Phi(\mathcal{O}) = \Lambda_\Phi(\mathrm{End}(\mathcal{A}))$, let us first bound the number of candidates, that is, orders containing $\mathbb{Z}[\pi, \overline{\pi}]$ stable under complex conjugation, and their discriminants.

**Lemma 6.1.** *We have:*

$$|\operatorname{disc}(\mathbb{Z}[\pi, \overline{\pi}])| < 4^{g(2g-1)} q^{g^2},$$

$$[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]] < 2^{g(2g-1)} q^{g^2/2}.$$

*Proof.* All $2g$ complex roots of $\chi_\pi$ have absolute value $\sqrt{q}$, so we have $|\operatorname{disc}(\chi_\pi)| < (2\sqrt{q})^{2g(2g-1)}$. The bounds then follow from the classical relation $[\mathcal{O} : \mathcal{O}']^2 = \operatorname{disc}(\mathcal{O}')/\operatorname{disc}(\mathcal{O})$ and, for the first one, the identity $[\mathbb{Z}[\pi, \overline{\pi}] : \mathbb{Z}[\pi]] = q^{g(g-1)/2}$ and, for the second one, the triviality $|\operatorname{disc}(\mathcal{O}_K)| > 1$. □

These bounds are nearly tight so there might be exponentially many candidate endomorphism rings; to efficiently identify $\Lambda_\Phi(\mathrm{End}(\mathcal{A}))$ among them, we exploit the identity $\mathcal{O} \subset \mathcal{O}' \Rightarrow \Lambda_\Phi(\mathcal{O}) \subset \Lambda_\Phi(\mathcal{O}')$ by performing an $n$-ary search in the lattice of orders using the following algorithm adapted from [1].

**Algorithm 6.2.**

INPUT: *An absolutely simple, ordinary, principally polarized abelian variety $\mathcal{A}$ of dimension $g$ defined over a field with $q$ elements.*

OUTPUT: *The relation lattice of its endomorphism ring.*

1. *Compute the Frobenius polynomial $\chi_\pi$ of $\mathcal{A}$.*
2. *Factor its discriminant and construct the order $\mathcal{O}' = \mathbb{Z}[\pi, \overline{\pi}]$.*
3. *For orders $\mathcal{O}$ directly above $\mathcal{O}'$:*
4. *If $\Lambda_\Phi(\mathcal{O}) \subset \Lambda_\Phi(\mathrm{End}(\mathcal{A}))$, set $\mathcal{O}' \leftarrow \mathcal{O}$ and go to Step 3.*
6. *Return $\Lambda_\Phi(\mathcal{O}')$.*

For Step 2, we use the unconditional factoring method of Lenstra and Pomerance [19]; its complexity is $L(|\operatorname{disc}(\chi_\pi)|)^{1+o(1)}$, that is, at most $L(q)^{g\sqrt{2}+o(1)}$. Alternatively, one may rely on the number field sieve [18] which has a heuristically better run time.

By *directly above*, we mean that $\mathcal{O}$ contains $\mathcal{O}'$ and no order lies strictly between them; the distance between two such orders necessarily divides $\ell^{2g-1}$ for some prime factor $\ell$ of $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$, since $\mathcal{O}'$ must then contain $\mathbb{Z} + \ell\mathcal{O}$.

Recall that Step 4 fails with error probability at most $1/q^{5g^2}$. By Lemma 6.1, the number of orders $\mathcal{O}$ considered in Step 3 is at most $q^{\frac{5}{2}g^2}$, and the number of times this step is reached is bounded by $\log(q^{\frac{5}{2}g^2})$; the probability that Algorithm 6.2 fails is therefore less than $1/q^{g^2}$. We will later explain how a candidate endomorphism ring may be unconditionally certified and verified so that, in the unlikely event that Algorithm 6.2 does fail, one notices and may start it over again.

The lattice of orders containing $\mathbb{Z}[\pi, \overline{\pi}]$ typically consists entirely of orders that are either minimal or maximal locally at large primes $\ell$; indeed, integers $v = [\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$ are not likely to be divisible by squares of large primes. More precisely, for any $\tau > 0$, we have

$$\#\left\{v \in \{1, \dots, n\} : \exists \ell \in \mathcal{P}_{>L(n)^\tau}, \ell^2 | v\right\} \leq \sum_{\ell \in \mathcal{P}_{>L(n)^\tau}} \frac{n}{\ell^2} \leq \frac{n}{L(n)^\tau},$$

which is negligible compared to $n$ as it goes to infinity; therefore, assuming that $v$ has similar divisibility properties to random integers less than $n = 2^{g(2g-1)}q^{g^2/2}$ (as per Lemma 6.1), only a zero-density set of abelian varieties of dimension $g$ over $\mathbb{F}_q$ have lattices of orders that, locally at some prime $\ell > L(n)^\tau$, have height greater than 1.

Discarding that set, there is only one order directly above (resp. below) any given one locally at large primes $\ell$, and they can be found using a Gröbner basis algorithm [2, §III.2.3] in time subexponential in $\log(q)$. Locally at primes $\ell \leq L(n)^\tau$, we resort to the much more direct method of enumerating all subgroups of $\frac{1}{\ell}\mathcal{O}/\mathcal{O}$ and selecting those which are orders; this takes time polynomial in $\ell$, that is, subexponential in $\log(q)$, and we select $\tau$ small enough so that this complexity is negligible compared to our overall complexity bound.

Putting all the above together, we obtain:

**Hypothesis** (C)**.** *The integers $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$ have the divisibility properties of random integers, so that orders directly above a given one may be enumerated efficiently as described above.*

**Theorem 6.3.** *Subject to Hypotheses (A)–(C) the expected running time of Algorithm* 6.2 *is bounded by*

$$L(q)^{g^2\sqrt{3}/2+o(1)}.$$

*Proof.* The bottleneck of this algorithm is Step 4, using $L(|\operatorname{disc}(\mathbb{Z}[\pi,\overline{\pi}])|)^{g\sqrt{3}/2+o(1)}$ operations by Proposition 5.2. Using Lemma 6.1, we may therefore bound the total complexity by $L(q)^{g^2\sqrt{3}/2+o(1)}$. □

## 7. Orders from relation lattices

The relation sublattice $\Lambda_\Phi(\mathcal{O})$ suffices to characterize $\mathcal{O}$ locally at almost all primes:

**Theorem 7.1** ([4, Proposition 20])**.** *Let $(\mathcal{A}_i/\mathbb{F}_{q_i})_{i\in\mathbb{N}}$ be a sequence of ordinary abelian varieties defined over fields of monotonously increasing cardinality $q_i \to \infty$. Denote by $v_i = [\mathcal{O}_{\mathbb{Q}(\pi_i)} : \mathbb{Z}[\pi_i, \overline{\pi}_i]]$ their conductor gaps, and by $n_i = \mathrm{N}_{K_0/\mathbb{Q}}(\Delta_{K/K_0})$ the norm of the relative discriminant of their CM-fields $K = \mathbb{Q}(\pi_i)$. Assume that there exists a constant $C$ such that, for all positive integers $u$ and $m$:*

- *the proportion of indices $i < m$ for which $u|v_i$ is at most $C/u$;*
- *the proportion of indices $i < m$ for which $u|v_i$ and $u|n_i$ is at most $C/u^2$.*

*For any $\tau > 0$, the density of indices $i$ for which there exists two orders $\mathcal{O}$ and $\mathcal{O}'$ containing $\mathbb{Z}[\pi_i, \overline{\pi}_i]$, stable under complex conjugation, satisfying $\Lambda_\Phi(\mathcal{O}) = \Lambda_\Phi(\mathcal{O}')$, and such that $\ell^{\mathrm{val}_\ell v_i} > L(q_i)^\tau$ for some prime factor $\ell$ of the index $[\mathcal{O}+\mathcal{O}' : \mathcal{O}\cap\mathcal{O}']$, is zero.*

The above result essentially means that, excluding a zero-density set of Weil numbers $\pi$, the lattice $\Lambda_\Phi(\mathcal{O})$ uniquely characterizes the order $\mathcal{O}$ from other orders containing $\mathbb{Z}[\pi,\overline{\pi}]$ except locally at small primes.

Note that the smoothness assumptions are not strong and very similar to that of Hypothesis (C): if the $v_i$ were drawn uniformly at random from $\{1,\dots,(8q_i)^2\}$ and independently from the $n_i$, they would be satisfied with $C = 1$. In practice, they are also found to hold for abelian varieties to which this work is of most interest: random isomorphism classes of abelian varieties with complex multiplication by a prescribed field defined over finite fields of increasing cardinality. At any rate, we assume this heuristic:

**Hypothesis** (D)**.** *The conductor gap and relative discriminant of families of abelian varieties considered here satisfies the smoothness conditions of the above theorem.*

Under this hypothesis, once an order $\mathcal{O}$ with $\Lambda_\Phi(\mathcal{O}) = \Lambda_\Phi(\mathrm{End}(\mathcal{A}))$ is found, it only remains to identify $\mathrm{End}(\mathcal{A})$ to compute it locally at all prime factors of $\mathrm{disc}(\pi)$ less than $L(q)^\tau$.

To compute endomorphism rings locally at small primes $\ell$, we rely on the direct method of Eisenträger and Lauter [14, §6.5], which uses $\ell^{2gv+o(1)}$ operations in the base field, where $v$ is the valuation of $[\mathcal{O}_K : \mathbb{Z}[\pi,\overline{\pi}]]$ at $\ell$. As above, to ensure that this cost is negligible relative to our overall complexity bound, we make $\tau > 0$ small enough and omit the zero-density set of abelian varieties for which this index is divisible by a power greater than $L(q)^\tau$ of a prime less than $L(q)^\tau$. This gives:

**Theorem 7.2.** *Subject to Hypotheses (A), (B), (C) and (D), the endomorphism ring of an absolutely simple, ordinary, principally polarized abelian variety of dimension $g = 2$ defined over a finite field with $q$ elements may be computed in average*

*probabilistic time*

$$L(q)^{g^2\sqrt{3}/2+o(1)}$$

*with error probability less than* $1/q^{g^2}$.

As an aside, we now describe how one may certify the output endomorphism ring $\mathcal{O}$ using relations that discriminate $\mathcal{O}$ from other orders of the lattice, so that it can subsequently be verified solely under Hypothesis (A).

**Definition 7.3.** A *certificate* for an order $\mathcal{O}$ consists of:

- a family of orders $\mathcal{O}_i$ and relations $r_i$ that hold in $\mathcal{O}_i$ but not in $\mathcal{O}$,
- a family of orders $\mathcal{O}_j$ and relations $r_j$ that hold in $\mathcal{O}$ but not in $\mathcal{O}_j$,

such that $\mathcal{O}$ is the only order containing $\mathbb{Z}[\pi,\overline{\pi}]$ satisfying $\mathcal{O}_i \not\subset \mathcal{O}$ and $\mathcal{O}_j \not\supset \mathcal{O}$ for all $i$ and $j$.

As a direct consequence of Hypothesis (A), if $\mathcal{A}$ is an absolutely simple, ordinary, principally polarized abelian variety with Frobenius endomorphism $\pi$, the relation lattice $\Lambda_\Phi(\mathrm{End}(A))$ and $\Lambda_\Phi(\mathcal{O})$ are equal if and only if the isogenies corresponding to the $r_j$'s map $\mathcal{A}$ to isomorphic varieties while those corresponding to the $r_i$'s do not. In practice, the $\mathcal{O}_i$'s can be chosen to be all orders considered in Step 3 of Algorithm 6.2 for which $\Lambda_\Phi(\mathcal{O}_i) \not\subset \Lambda_\Phi(\mathcal{O} = \mathrm{End}(\mathcal{A}))$ and the $\mathcal{O}_j$'s to be all orders directly below $\mathcal{O}$.

A certificate therefore allows anyone to check that the relation lattice of $\mathrm{End}(\mathcal{A})$ is that of the claimed endomorphism ring $\mathcal{O}$. By Propositions 3.1 and 4.4, under Hypotheses (A)–(D) and for any $\gamma > 0$, it takes $L(q)^{g\gamma+o(1)} + L(q)^{g/(4\gamma)+o(1)}$ time to generate a certificate that can subsequently be verified under only Hypotheses (C) in $L(q)^{3g^3\gamma+o(1)}$ operations. Then, to verify that $\mathcal{O} = \mathrm{End}(\mathcal{A})$ and not another order with the same relation lattice, this equality must be verified locally at primes less than $L(q)^\tau$ as per Theorem 7.1; for $\tau$ small enough, this additional verification is asymptotically negligible.

## 8. Practical computations

We give two examples illustrating different patterns for the index $v = [\mathcal{O}_K : \mathbb{Z}[\pi,\overline{\pi}]]$. Previous algorithms [14], [27] compute endomorphism rings efficiently when $\mathcal{A}[\ell^n]$ remains defined over small extension fields as $\ell^n$ ranges through prime-power factors of $v$, while ours performs well as soon as no order directly above $\mathbb{Z}[\pi,\overline{\pi}]$ has an overly large discriminant.

Computations reported here were performed by a straightforward Magma [6] implementation using the AVIsogenies library [3] and running on one Intel i7-2620M core.

8.1. **Example with nearly prime $v$.** Let us first consider a very favorable case where $v$ is both large and nearly prime, that of the Jacobian variety $\mathcal{A}$ of the hyperelliptic curve with equation

$$y^2 = x^5 + 523747x^4 + 306186x^3 + 744660x^2 + 415524x + 261884$$

over the field with $q = 1250407$ elements; its Frobenius endomorphism $\pi$ admits the characteristic polynomial $z^4 + 1251z^3 + 1772074z^2 + 1251qz + q^2$ from which one can derive that $\mathbb{Z}[\pi,\overline{\pi}]$ is an order of index $v = 2 \cdot 538259$ in the ring of integers of $K = \mathbb{Q}(\pi)$.

We start by computing $\mathrm{End}(\mathcal{A})$ locally at 2, that is, determining whether it contains the order in which $\mathbb{Z}[\pi, \overline{\pi}]$ has index 2; this order is generated by $\pi$ and $\alpha/(2q)$ where

$$\alpha = 417q + 1346084914086\pi + 497115559392\pi^2 + \pi^3.$$

To determine whether $\alpha/(2q)$ belongs to $\mathrm{End}(\mathcal{A})$ or, equivalently, whether $\alpha/2$ does (as $q$ is coprime to $v$), we use the method of Eisenträger and Lauter [14]: it takes 102ms to determine that $\alpha$ kills the full 2-torsion of $\mathcal{A}$, which establishes that $\mathrm{End}(\mathcal{A})$ is locally maximal at 2.

Now denote by $\mathfrak{p}\overline{\mathfrak{p}}$ the factorization of 7 in $\mathbb{Z}[\pi, \overline{\pi}]$ and observe that $\mathfrak{p}$ is principal in $\mathcal{O}_K$. We evaluate the corresponding isogeny, spending 10.9s to find its kernel and 1.37s to identify the isogenous variety; since it is not isomorphic to $\mathcal{A}$ we have established, in just 12.3s, that

$$\mathrm{End}(\mathcal{A}) \simeq \mathbb{Z}[\pi, \alpha/(2q)].$$

This computation is clearly intractable using previous algorithms: the full 538259-torsion of $\mathcal{A}$ is defined over an extension of degree $e = 869166638466$, so it would require a rough minimum of $\log(q^e)\log(q^{eg}) \approx 2^{90}$ operations just to find a random 538259-torsion point.

8.2. **Example with composite $v$.** For a less degenerate case, let $\mathcal{A}$ be the Jacobian variety of the curve with equation

$$y^2 = x^5 + 800x^4 + 2471x^3 + 6695x^2 + 1082x + 7062$$

over the field with $q = 7681$ elements. It takes just 60ms to compute that the characteristic polynomial of its Frobenius endomorphism is $z^4 + 114z^3 + 7566z^2 + 114qz + q^2$ from which it takes negligible time to derive that $\mathbb{Z}[\pi, \overline{\pi}]$ has index $2^2 \cdot 47^2 \cdot 379$ in $\mathcal{O}_K$.

Again, we start by computing the endomorphism ring locally at 2 using the method of Eisenträger and Lauter [14]. Only 75ms are needed to find a basis for the full 2-torsion (the 4-torsion is not needed) and evaluate the relevant endomorphism on it; this determined that $\mathrm{End}(\mathcal{A})$ contains the order $\mathcal{O}_2 = \mathbb{Z}[\pi, \overline{\pi}] + 47^2 \cdot 379 \cdot \mathcal{O}_K$. Having established that, we may start Algorithm 6.2 from the order $\mathcal{O}_2$ instead of $\mathbb{Z}[\pi, \overline{\pi}]$; the two orders directly above $\mathcal{O}_2$ have index 379 and $47^2$ in $\mathcal{O}_K$.

First consider that of index $47^2$: in just 100ms we find that ideals of norm $3^2$ have order 92 in its class group. Computing the 92 corresponding isogenies takes 37s, that is, 400ms on average. As the isogenous variety is not isomorphic to $\mathcal{A}$, we deduce that $\mathrm{End}(\mathcal{A})$ is minimal locally at 47.

Next we consider the order with index 379; after 150ms, we find that the ideal $\mathfrak{p}^{62}(\mathfrak{r}\mathfrak{s})^2$ is principal in it, where the primes appear in the splittings $3 = \mathfrak{p}\overline{\mathfrak{p}}$ and $19 = \mathfrak{r}\mathfrak{s}\overline{\mathfrak{r}\mathfrak{s}}$. We therefore proceed to test whether the corresponding relation holds in $\mathcal{A}$: it takes 67s on average to compute each of the two 19-isogenies, and 400ms for each of the 3-isogenies. The isogenous variety, which is determined after a total of 157s, is not found to be isomorphic to $\mathcal{A}$, hence we deduce that $\mathrm{End}(\mathcal{A})$ is the order containing $\mathbb{Z}[\pi, \overline{\pi}]$ with index 4.

Note that the full 47-torsion and full 379-torsion live over extensions of degree 34592 and 13609890 respectively, which again makes computing $\mathrm{End}(\mathcal{A})$ using previous methods quite expensive.

This illustrates that, even when the orders in which we look for relations have moderate class numbers, the bottleneck of our algorithm remains the evaluation of

isogenies. Accordingly, in both computations above, we have used a simple baby-step giant-step method in place of Algorithm 4.3, which allowed us to find much smaller relations and therefore to better balance the cost of evaluating isogenies with that of searching for relations.

Overall, we find that our algorithm clearly outperforms previous methods as soon as the index $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$ has prime power factors $\ell^n$ for which the torsion points live over significant extensions of the base field, although those methods are still very useful to compute the endomorphism ring locally at small primes.

## Acknowledgments

This work would never have seen the light of day without the author's prior collaborations with Andrew V. Sutherland, constant encouragements from Pierrick Gaudry, and invaluable discussions with Andreas Enge, Igor Shparlinski, and Marco Streng.

## References

[1] Gaetan Bisson, *Computing endomorphism rings of elliptic curves under the GRH*, J. Math. Cryptol. **5** (2011), no. 2, 101–113, DOI 10.1515/JMC.2011.008. MR2838371 (2012k:11201)

[2] Gaetan Bisson, *Endomorphism Rings in Cryptography*, Ph.D. thesis. Eindhoven University of Technology and Institut National Polytechnique de Lorraine, 2011. ISBN: 90-386-2519-7.

[3] Gaetan Bisson, Romain Cosset and Damien Robert, *AVIsogenies, A library for computing isogenies between abelian varieties*, 2010. http://avisogenies.gforge.inria.fr/.

[4] Gaetan Bisson and Marco Steng, *On polarised class groups of orders in quartic CM-fields*, 2013. arXiv.org: 1302.3756.

[5] Gaetan Bisson and Andrew V. Sutherland, *Computing the endomorphism ring of an ordinary elliptic curve over a finite field*, J. Number Theory **131** (2011), no. 5, 815–831, DOI 10.1016/j.jnt.2009.11.003. MR2772473 (2012a:11080)

[6] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. MR1484478

[7] Jean-Benoît Bost and Jean-François Mestre, *Moyenne arithmético-géométrique et périodes des courbes de genre* 1 *et* 2 (French), Gaz. Math. **38** (1988), 36–64. MR970659 (89k:14072)

[8] Reinier Bröker, David Gruenewald, and Kristin Lauter, *Explicit CM theory for level 2-structures on abelian surfaces*, Algebra Number Theory **5** (2011), no. 4, 495–528, DOI 10.2140/ant.2011.5.495. MR2870099

[9] Johannes Buchmann, *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields*, Séminaire de Théorie des Nombres, Paris 1988–1989, Progr. Math., vol. 91, Birkhäuser Boston, Boston, MA, 1990, pp. 27–41. MR1104698 (92g:11125)

[10] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier, *Subexponential algorithms for class group and unit computions*, Journal of Symbolic Computation 24.3-4 (1997): *Special Issue on Computational Algebra and Number Theory*: *Proceedings of the First MAGMA Conference*, pp. 433–441. DOI:10.1006/jsco.1996.0143.

[11] Gary Cornell and Joseph H. Silverman (eds.), *Arithmetic geometry*, Springer-Verlag, New York, 1986. Papers from the conference held at the University of Connecticut, Storrs, Connecticut, July 30–August 10, 1984. MR861969 (89b:14029)

[12] Romain Cosset and Damien Robert, *Computing* $(l, l)$*-isogenies in polynomial time on Jacobians of genus 2 curves*, 2011. IACR ePrint: 2011/143.

[13] J.-M. Couveignes, *Linearizing torsion classes in the Picard group of algebraic curves over finite fields*, J. Algebra **321** (2009), no. 8, 2085–2118, DOI 10.1016/j.jalgebra.2008.09.032. MR2501511 (2010e:14019)

[14] Kirsten Eisenträger and Kristin Lauter, *A CRT algorithm for constructing genus 2 curves over finite fields*, Arithmetics, Geometry, and Coding Theory (AGCT 2005), Sémin. Congr., vol. 21, Soc. Math. France, Paris, 2010, pp. 161–176. MR2856565

[15] Mireille Fouquet and François Morain, *Isogeny volcanoes and the SEA algorithm, Algorithmic Number Theory — ANTS-V*, edited by Claus Ficker and David R. Kohel, vol. 2369, Lecture Notes in Computer Science, Springer, 2002, pp. 47–62. DOI: 10.1007/3-540-45455-1-23.

[16] Steven D. Galbraith, *Constructing isogenies between elliptic curves over finite fields*, LMS J. Comput. Math. **2** (1999), 118–138 (electronic), DOI 10.1112/S1461157000000097. MR1728955 (2001k:11113)

[17] David Russell Kohel, *Endomorphism Rings of Elliptic Curves over Finite Fields*, ProQuest LLC, Ann Arbor, MI, 1996. Thesis (Ph.D.)–University of California, Berkeley. MR2695524

[18] Arjen K. Lenstra and Hendrik W. Lenstra, editors, *The Development of the Number Field Sieve*, vol. 1554, Lecture Notes in Mathematics, Springer, 1993. ISBN: 3-540-57013-4.

[19] H. W. Lenstra Jr. and Carl Pomerance, *A rigorous time bound for factoring integers*, J. Amer. Math. Soc. **5** (1992), no. 3, 483–516, DOI 10.2307/2152702. MR1137100 (92m:11145)

[20] David Lubicz and Damien Robert, *Computing isogenies between abelian varieties*, Compos. Math. **148** (2012), no. 5, 1483–1515, DOI 10.1112/S0010437X12000243. MR2982438

[21] Jean-François Mestre, *Construction de courbes de genre* 2 *à partir de leurs modules* (French), Effective Methods in Algebraic Geometry (Castiglioncello, 1990), Progr. Math., vol. 94, Birkhäuser Boston, Boston, MA, 1991, pp. 313–334. MR1106431 (92g:14022)

[22] J. Pila, *Frobenius maps of abelian varieties and finding roots of unity in finite fields*, Math. Comp. **55** (1990), no. 192, 745–763, DOI 10.2307/2008445. MR1035941 (91a:11071)

[23] Goro Shimura and Yutaka Taniyama, *Complex Multiplication of Abelian Varieties and Its Applications to Number Theory*, Publications of the Mathematical Society of Japan, vol. 6, The Mathematical Society of Japan, Tokyo, 1961. MR0125113 (23 #A2419)

[24] Andrew V. Sutherland, *Computing Hilbert class polynomials with the Chinese remainder theorem*, Math. Comp. **80** (2011), no. 273, 501–538, DOI 10.1090/S0025-5718-2010-02373-7. MR2728992 (2011k:11177)

[25] John Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144. MR0206004 (34 #5829)

[26] Jacques Vélu, *Isogénies entre courbes elliptiques* (French), C. R. Acad. Sci. Paris Sér. A-B **273** (1971), A238–A241. MR0294345 (45 #3414)

[27] Markus Wagner, *Über Korrespondenzen zwischen algebraischen Funktionenkörper*, Ph.D. thesis, Technische Universität Berlin, 2009. http://www.math.tu-berlin.de/~wagner/Diss.pdf.

[28] William C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560. MR0265369 (42 #279)

University of French Polynesia, BP6570, 98702 Faaa, French Polynesia
*E-mail address*: bisson@gaati.org