COMPUTING SQUARE-FREE POLARIZED ABELIAN VARIETIES OVER FINITE FIELDS

STEFANO MARSEGLIA

Abstract. We give algorithms to compute isomorphism classes of ordinary abelian varieties defined over a finite field $\mathbb{F}_q$ whose characteristic polynomial (of Frobenius) is square-free and of abelian varieties defined over the prime field $\mathbb{F}_p$ whose characteristic polynomial is square-free and does not have real roots. In the ordinary case we are also able to compute the polarizations and the group of automorphisms (of the polarized variety) and, when the polarization is principal, the period matrix.

1. Introduction

It is well known that the abelian varieties of dimension g defined over the complex numbers can be functorially (and explicitly) described in terms of full lattices L in $\mathbb{C}^g$ such that the associated complex torus $\mathbb{C}^g/L$ admits a Riemann form, see for example [Ros86].

When we move to the world of positive characteristic p, thanks to Serre, we know that we cannot describe the whole category of abelian varieties of dimension g in terms of lattices of rank $2g$. This is due to the existence of objects such as supersingular elliptic curves whose endomorphism algebra is quaternionic and hence does not admit a 2-dimensional representation over $\mathbb{Q}$.

Nevertheless, if we restrict our attention to some subcategories of the category of abelian varieties defined over a finite field we have equivalences with the category of finitely generated free $\mathbb{Z}$-modules with extra structure satisfying some easy-to-state axioms. More precisely, this was proved by Deligne in [Del69] for ordinary abelian varieties over a finite field $\mathbb{F}_q$, where $q = p^r$ is an arbitrary prime power, and by Centeleghe-Stix in [CS15] for abelian varieties over the prime field $\mathbb{F}_p$ whose characteristic polynomial of Frobenius does not have real roots, or equivalently, such that $\sqrt{p}$ is not an eigenvalue of the action of Frobenius on the associated l-adic Tate module, for any prime $l \neq p$. Other functors (which we do not use in this paper) defined on the subcategory of powers of elliptic curves are studied in the Appendix in [Lau02], in [Kan11] and in [JKP$^+$18].

The *main result* of this paper is an algorithm to compute the isomorphism classes of abelian varieties in the isogeny class determined by a *square-free* characteristic polynomial h of Frobenius using Deligne and Centeleghe-Stix' results. The key point to perform this computation is that the target category of Deligne's and Centeleghe-Stix equivalences is equivalent to the category of fractional ideals of the order $\mathbb{Z}[F, V]$, where F is a root of h and $V = q/F$ in the Deligne case and $V = p/F$ in Centeleghe-Stix case. Fractional ideals for orders that are not domains will be

2010 *Mathematics Subject Classification.* Primary 14K15; Secondary: 14G15, 11G10, 11G25, 14-04.

defined in Section 2. The order $\mathbb{Z}[F,V]$ might not be maximal and so the fractional ideals might not be invertible, even in their own multiplicator ring. In [Mar20] we describe a method to compute the isomorphism classes of such ideals and hence we are able to compute the isomorphism classes of abelian varieties in the isogeny class determined by h, see Algorithm 1.

In the ordinary case, translating the results of [How95] into our ideal-theoretic description allows us to compute polarizations of arbitrary degree and the automorphism group of the polarized abelian varieties, see Algorithms 3 and 4.

The present algorithm could be used to provide computational evidence for extending the formulas counting the number of isomorphism classes of principally polarized abelian varieties such as in [AW15] and [AG17].

We would like to stress that the shift from $\mathbb{Z}[F,V]$-modules to $\mathbb{Z}[F,V]$-fractional ideals (for certain isogeny classes) is very natural and it has already been used in the past, sometimes implicitly. A list of papers where such a shift is applied to simple ordinary varieties includes: the work of Howe, see for example [How95, Section 6] where the focus is on abelian varieties with maximal endomorphism ring and [How04, Section 2] for abelian surfaces; a paper by Lenstra, cf. [Len96, Section 6]; a paper by Lenstra, Pila and Pomerance, with focus on for abelian surfaces, cf. [LPP02, Section 8]; a paper by Shankar and Tsimerman, mainly for geometrically simple isogeny classes, cf. [ST18, Section 3.1]. The shift is also described using categorical language for simple ordinary abelian varieties in previous work of the author [Mar16], and in Martindale's thesis [Mar18b, Sections 1.2,1.4]. Results analogous to the one contained in the present paper for simple almost ordinary abelian varieties in odd characteristic can be found in Oswal and Shankar's paper [OS, Section 4].

The paper is structured as follows. In Section 2 we recall the definition of fractional ideal of an order and we introduce the notion of an ideal class monoid. In Section 3 we describe the categories of abelian varieties and Deligne's and Centeleghe-Stix' equivalences. In Section 4 we focus on the square-free case and prove an equivalence with the category of fractional ideals of certain orders. Such an equivalence allows us to describe the endomorphism ring, the automorphism group and the group of rational points of the abelian varieties. In Section 5 we translate the notion of a polarization of an ordinary abelian variety over a finite field into the ideal-theoretic language and we describe how to compute the polarizations of a given degree up to isomorphisms. We also describe how to compute the automorphism group of the polarized abelian variety. In Section 6 we present the algorithms from the previous sections and in Section 7 we present the output of some computations. Finally, in Section 8 we explain how to compute a period matrix of the canonical lift of an ordinary principally polarized abelian variety using the tools provided. The algorithms have been implemented in Magma [BCP97]. The packages and the code to reproduce the examples contained in this paper are available at `https://github.com/stmar89/AbVarFq`. The author is currently running a big computation of isomorphisms classes of abelian varieties over finite fields. The output will be published on [LMF13].

Acknowledgments. The author would like to thank Jonas Bergström for helpful discussions and Rachel Newton and Christophe Ritzhentaler for comments on a previous version of the paper, which is part of the author's Ph.D thesis [Mar18a]. The author would also like to express his gratitude to the Max Planck Institute for Mathematics in Bonn for their hospitality. The author thanks the anonymous reviewer of Mathematics of Computation for useful comments and suggestions.

Conventions. All rings are commutative and unital. All morphisms between abelian varieties A and B over a field k are also defined over k, unless otherwise specified. In particular we write $\mathrm{Hom}(A,B)$ for $\mathrm{Hom}_k(A,B)$. An abelian variety A is simple if it is so over the field of definition.

2. Orders and Ideal classes

Let $f \in \mathbb{Q}[x]$ be a monic square-free polynomial and denote by K the étale $\mathbb{Q}$-algebra $\mathbb{Q}[x]/(f)$. Note that K is a finite product of number fields. An *order* in K is a subring R of K whose underlying abelian group is isomorphic to $\mathbb{Z}^n$ where $n = \deg f$. In particular, we have that $R \otimes_{\mathbb{Z}} \mathbb{Q} = K$ and that K is the total ring of quotients of R. Among all orders of K there is one maximal with respect to inclusion called the *maximal order of* K. It is a Dedekind ring and we denote it by $\mathcal{O}_K$.

A *fractional R-ideal* is a finitely generated sub-R-module I of K such that $K = I \otimes_{\mathbb{Z}} \mathbb{Q}$, or, equivalently, it contains a non-zero divisor of K. Given two fractional R-ideals I and J we have that IJ, $I+J$, $I \cap J$ and $(I:J) = \{x \in K : xJ \subseteq I\}$ are also fractional R-ideals. Note that the fractional R-ideals are precisely the lattices in K which are R-modules.

An *over-order* of R is an order containing R.

To every fractional R-ideal I we can associate a particular order S, the *multiplicator ring* of I, defined as the biggest subring of K for which I is an S-module. Note that $S = (I:I)$ and that S is an over-order of R. A fractional ideal I is *invertible* if $I(S:I) = S$, where S is its multiplicator ring.

Observe that two fractional R-ideals I and J are isomorphic as R-modules if and only if there exists $a \in K^\times$ such that $I = aJ$. Indeed, every R-linear morphism $\alpha\colon I \to J$ induces a unique K-linear endomorphism $\alpha \otimes \mathbb{Q}$ of K which is uniquely determined by the image of 1, say a. Moreover α is injective if and only if a is not a zero-divisor. We will denote by $\mathcal{I}(R)$ the category of fractional R-ideals with R-linear morphisms.

The set of fractional R-ideals up to isomorphism is called the *ideal class monoid* of R and it is denoted $\mathrm{ICM}(R)$. It is a multiplicative monoid under the operation induced by ideal multiplication and contains a group $\mathrm{Pic}(R)$ consisting of the classes of invertible R-ideals, with equality if and only if $R = \mathcal{O}_K$. More generally, we have that

$$\mathrm{ICM}(R) \supseteq \bigsqcup_S \mathrm{Pic}(S),$$

where the disjoint union is taken over all the over-orders S of R. We will write $[I]$ for the isomorphism class of the fractional R-ideal I.

In [Mar20] we describe an algorithm that computes $\mathrm{ICM}(R)$.

3. The category of abelian varieties over a finite field

Let $q = p^r$ be a power of a prime p. Denote with $\mathrm{AV}(q)$ the category of abelian varieties over $\mathbb{F}_q$. For A in $\mathrm{AV}(q)$ let h_A be the characteristic polynomial of the Frobenius acting on the Tate module $T_l A$ for a prime $l \neq p$. Recall that the definition of h_A does not depend on the choice of the prime l. It follows from the results of Honda [Hon68] and Tate [Tat66] that the polynomial h_A characterizes the isogeny class of A. Their results can be summarized as follows. Consider the following conditions for a polynomial h in $\mathbb{Q}[x]$:

(a) h is monic, of even degree and with integer coefficients;
(b) every complex root of h has absolute value $\sqrt{q}$;
(c) $h = m^n$, where m is irreducible and n is the least common denominator of the rational numbers $\{v_p(f(0))/r\}$, where f runs over the irreducible factors of m over $\mathbb{Q}_p$ and v_p is the p-adic valuation normalized such that $r = v_p(q)$. If m has a real root then one needs to add $1/2$ to the set of rational numbers.

Let $\mathcal{W}(q)$ be the set of finite products of polynomials satisfying (a), (b) and (c).

Proposition 3.1 (Honda-Tate theory, see [Tat71])**.** *If A is an abelian variety in $\mathrm{AV}(q)$ then h_A is in $\mathcal{W}(q)$. Conversely, for every h in $\mathcal{W}(q)$ there exists an abelian variety A in $\mathrm{AV}(q)$ such that $h = h_A$. Given two abelian varieties A and A' in $\mathrm{AV}(q)$ we have $h_A = h_{A'}$ if and only if A and A' are isogenous. Moreover, if A has dimension g then h_A has degree $2g$.*

For h in $\mathcal{W}(q)$ we will denote by $\mathrm{AV}(h)$ the full subcategory of $\mathrm{AV}(q)$ consisting of abelian varieties in the isogeny class determined by h. A polynomial h in $\mathcal{W}(q)$ will be called *ordinary* if exactly half of the roots of h are p-adic units. An abelian variety A is called ordinary if h_A is ordinary, or, equivalently, if $h_A \mod p$ is not divisible by x^{g+1}, where g is the dimension of A.

The main theoretical tools we will use to understand the category $\mathrm{AV}(q)$ are certain functors to the category of finitely generated free $\mathbb{Z}$-modules with some extra structure, which become equivalences when we restrict to subcategories of $\mathrm{AV}(q)$. More precisely, we will consider the following categories:

- $\mathrm{AV}^{ord}(q)$: ordinary abelian varieties over $\mathbb{F}_q$;
- $\mathrm{AV}^{cs}(p)$: abelian varieties A over $\mathbb{F}_p$ such that h_A has no real root.
- $\mathcal{M}^{ord}(q)$: free finitely generated $\mathbb{Z}$-modules T with an endomorphism F such that:
  - $F \otimes_{\mathbb{Z}} \mathbb{Q}$ acts semi-simply on $T \otimes_{\mathbb{Z}} \mathbb{Q}$;
  - the characteristic polynomial h_F of $F \otimes_{\mathbb{Z}} \mathbb{Q}$ is in $\mathcal{W}(q)$;
  - h_F is ordinary;
  - there exists an endomorphism V of T such that $F \circ V = q$.
- $\mathcal{M}^{cs}(p)$: free finitely generated $\mathbb{Z}$-modules T with an endomorphism F such that:
  - $F \otimes_{\mathbb{Z}} \mathbb{Q}$ acts semi-simply on $T \otimes_{\mathbb{Z}} \mathbb{Q}$;
  - the characteristic polynomial h_F of $F \otimes_{\mathbb{Z}} \mathbb{Q}$ is in $\mathcal{W}(p)$;
  - h_F has no real roots, that is, $h_F(\pm\sqrt{p}) \neq 0$;
  - there exists an endomorphism V of T such that $F \circ V = p$.

A morphism from (T, F) to (T', F') for objects in $\mathcal{M}^{ord}(q)$ (or in $\mathcal{M}^{cs}(p)$) is a $\mathbb{Z}$-linear morphism $\varphi\colon T \to T'$ such that the following diagram commutes:

$$\begin{tikzcd}
T \arrow[r, "\varphi"] \arrow[d, "F"'] & T' \arrow[d, "F'"] \\
T \arrow[r, "\varphi"] & T'
\end{tikzcd}$$

Theorem 3.2. *There are equivalences of categories*

$$\mathcal{F}^{ord} : \mathrm{AV}^{ord}(q) \to \mathcal{M}^{ord}(q)$$

and

$$\mathcal{F}^{cs} : \mathrm{AV}^{cs}(p) \to \mathcal{M}^{cs}(p),$$

such that if

$$A \mapsto (T, F)$$

then $\mathrm{Rank}_{\mathbb{Z}}(T) = 2 \dim A$ *and* F *corresponds to the Frobenius endomorphism of* A.

Proof. See [Del69, Theorem 7] and the covariant version of [CS15, Theorem 1] given in [CS15, 7.4]. □

Remark 3.3. Let A be in $\mathrm{AV}^{ord}(q)$. We will recall the construction of $\mathcal{F}^{ord}(A) = (T, F)$ given in [Del69] since it will be used later in computing the polarizations. Denote by W the ring of Witt vectors over $\mathbb{F}_q$. Since A is ordinary it admits a *canonical lift* to an abelian variety $\tilde{A}$ over W, characterized by $\mathrm{End}_{\overline{\mathbb{F}}_q}(A) = \mathrm{End}_W(\tilde{A})$. Fix an embedding $\varepsilon\colon W \hookrightarrow \mathbb{C}$ and define $A' = \tilde{A} \otimes_\varepsilon \mathbb{C}$. Finally put $T = H_1(A', \mathbb{Z})$. Note that this construction is functorial in A and in particular T comes equipped with an endomorphism F corresponding to the Frobenius of A.

Remark 3.4. The construction of the functor $\mathcal{F}^{cs}$ depend also on a choice, see [CS15, Section 7.3]. For any choice of embedding $\varepsilon\colon W \hookrightarrow \mathbb{C}$ the functor $\mathcal{F}^{cs}$ can be constructed in a way that extends $\mathcal{F}^{ord}$ on $\mathrm{AV}^{ord}(p)$. See [CS15, Proposition 45].

As Serre has pointed out, functorial descriptions such as the ones in Theorem 3.2 cannot be extended to the whole category of abelian varieties. This is a consequence of the existence of objects like supersingular elliptic curves, whose endomorphism algebra is a quaternionic algebra which does not admit a 2-dimensional representation.

4. The square-free case

In this section h will be either a *square-free* ordinary polynomial in $\mathcal{W}(q)$ or a *square-free* polynomial in $\mathcal{W}(p)$ with no real roots. We will denote with $\mathcal{M}(h)$ the image of $\mathrm{AV}(h)$ under the functor $\mathcal{F}^{ord}$ (or $\mathcal{F}^{cs}$, respectively).

Remark 4.1. Let A an abelian variety in $\mathrm{AV}(h)$. The Poincaré reducibility theorem states that there are simple and pairwise non-isogenous abelian varieties $B_1, \ldots, B_r$ and an isogeny such that

$$A \sim B_1 \times \ldots \times B_r.$$

In particular $h = \prod_i h_{B_i}$ and, since h is square-free, it follows that each h_{B_i} is irreducible. Observe that the converse holds in both cases of interest to us: the characteristic polynomial of a simple abelian variety B is irreducible, hence equal to the minimal polynomial of the Frobenius, if B is in $\mathrm{AV}^{ord}(q)$, see [How95, Theorem 3.3], or in $\mathrm{AV}^{cs}(p)$, because in the condition (c) stated at the beginning of Section 3 all denominators are equal to 1.

One observes that the proportion of square-free polynomials among non-ordinary p-Weil polynomials is smaller than the proportion of square-free polynomials among ordinary p-Weil. Nevertheless it accounts for the vast majority of them. For example by looking at [LMF13] one sees that among the 105600 ordinary isogeny classes of abelian fourfolds over $\mathbb{F}_5$ exactly 104746 are square-free. Among the 27239 non-ordinary isogeny classes of abelian fourfolds over $\mathbb{F}_5$ we have 26765 which are square-free.

Remark 4.2. Note that being square-free is not a geometric condition, in the sense that in general it is not stable under extensions of the base field. For example, if A is an abelian surface over $\mathbb{F}_{31}$ with characteristic polynomial

$$h_A = (x^2 - 3x + 31)(x^2 + 3x + 31)$$

then A is isogenous to the product of two non-isogenous elliptic curves E_1 and E_2. On the other hand E_1 and E_2 become isogenous over $\mathbb{F}_{31^2}$ and indeed the characteristic polynomial of $A' := A \otimes \mathbb{F}_{31^2}$ is

$$h_{A'} = (x^2 + 53x + 961)^2.$$

Denote with K the étale algebra $\mathbb{Q}[x]/(h)$. Put $\alpha = x \mod (h)$. Let R be the order in K generated by α and q/α. Observe that our order R is the order R_w defined in [CS15, Section 2] for the Weil support w identified by the polynomial h and, similarly, R equals the order $R_{\mathbb{C}}$ defined in [How95]. Recall that $\mathcal{I}(R)$ denotes the category of fractional R-ideals.

Theorem 4.3. *There is an equivalence of categories $\Psi\colon \mathcal{M}(h) \to \mathcal{I}(R)$.*

Proof. Let g be the dimension of any abelian variety in $\mathrm{AV}(h)$, or equivalently let $2g$ be the degree of h. Pick an object (T, F) in $\mathcal{M}(h)$. Note that by definition T is a $\mathbb{Z}[F, V]$-module. Since h is square-free it is the minimal polynomial of F and hence the morphism $F \mapsto \alpha$ induces an isomorphism $\mathbb{Z}[F, V] \simeq R$ and hence an R-module structure on T. Since T is torsion-free it can be embedded in $R \otimes_{\mathbb{Z}} \mathbb{Q} = K$ and hence it can be identified with a sub-R-module I of K. Since T is an abelian group of rank $2g$ it follows that I is a fractional R-ideal, hence an object of $\mathcal{I}(R)$. Denote this association $(T, F) \mapsto I$ by Ψ. Observe that Ψ is a functor. Indeed if $\varphi\colon (T, F) \to (T', F')$ is a morphism in $\mathcal{M}(h)$, then the compatibility rule $\varphi \circ F = F' \circ \varphi$ implies that $\Psi(\varphi)$ will be an R-linear morphism, as required, and that it respects composition and that it sends the identity morphism to the identity morphism. By construction it is clear that Ψ is fully faithful and essentially surjective, hence an equivalence of categories. □

Corollary 4.4. *If h is ordinary or if h is over $\mathbb{F}_p$ with no real roots then there is an equivalence of categories*

$$\mathcal{F}\colon\ \mathrm{AV}(h) \to \mathcal{I}(R).$$

In particular, $\mathcal{F}$ induces a bijection

$$\frac{\mathrm{AV}(h)}{\simeq} \longrightarrow \mathrm{ICM}(R).$$

Proof. The functor $\mathcal{F}$ is the composition of the functor $\mathcal{F}^{ord}$ (or $\mathcal{F}^{cs}$) from Theorem 3.2 together with the functor Ψ from Theorem 4.3, which are all equivalences. □

Remark 4.5. Theorem 4.3 and Corollary 4.4 tell us that the abelian varieties in the isogeny class $\mathrm{AV}(h)$ correspond to the different $\mathbb{Z}[x, y]/(h(x), xy - q)$-structures that one can put on $\mathbb{Z}^{2g}$.

Corollary 4.6. *If $\mathcal{F}(A) = I$, then*

(a) $\mathcal{F}(\mathrm{End}(A)) = (I : I)$*;*

(b) $\mathcal{F}(\mathrm{Aut}(A)) = (I : I)^{\times}$*;*

(c) *A is isomorphic to a product of abelian varieties if and only if $(I : I)$ is a product of orders.*

Proof. Observe that (a) and (b) follow immediately from the previous proposition. Statement (c) holds by functoriality and the fact that an ideal I admits a decomposition $I_1 \oplus I_2$ if and only if the same holds for its multiplicator ring. Indeed, let $S = (I : I)$. If $S = S_1 \oplus S_2$, denote with e_1 and e_2 the units of S_1 and S_2, respectively, then $I = I_1 \oplus I_2$ where $I_i = e_i I$. The other implication follows from the fact that if $I = I_1 \oplus I_2$ then $(I : I) = (I_1 : I_1) \oplus (I_2 : I_2)$. □

Recall that for a fractional R-ideal J the trace dual is defined as

$$J^t = \left\{ z \in K : \mathrm{Tr}_{K/\mathbb{Q}}(zJ) \subseteq \mathbb{Z} \right\},$$

which is also a fractional R-ideal, with the same multiplicator ring as that of J. Moreover, if $J = \alpha_1\mathbb{Z} \oplus \ldots \oplus \alpha_n\mathbb{Z}$, then $J^t = \alpha_1^*\mathbb{Z} \oplus \ldots \oplus \alpha_n^*\mathbb{Z}$, where the α_j^*'s are uniquely defined by the relations $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j^*) = 1$ if $i = j$ and 0 otherwise.

Corollary 4.7. *If $\mathcal{F}(A) = I$, then there is an isomorphism*

$$A(\mathbb{F}_q) \simeq \frac{I}{(1-F)I}.$$

Proof. Observe that $A(\mathbb{F}_q)$ is the kernel of $1 - \pi_A$, where π_A is the Frobenius endomorphism of A. Moreover, notice that the action of F on $I/(1-F)I$ is invertible. Now, if A is ordinary, the statement follows from [How95, Lemma 4.13, Proposition 4.14].

If $A \in \mathrm{AV}^{cs}(p)$ we will obtain the result by looking at the ℓ-primary parts for every prime ℓ diving the number of $\mathbb{F}_p$-points of A. For a fractional R-ideal J put $J_\ell = J \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. Also denote by N_ℓ the ℓ-primary part of $A(\mathbb{F}_p)$.

By [CS15, Propositions 21 and 28] we have $T_p(A) \simeq I \otimes R_p \simeq I_p$ and hence

$$N_p \simeq \frac{I_p}{(1-F)I_p}.$$

For a prime $\ell \neq p$ by [CS15, Propositions 21 and 27] we have an isomorphism $T_\ell(A) \simeq \mathrm{Hom}_{R_\ell}(I_\ell, R_\ell)$ and hence

$$N_\ell \simeq \frac{(R_\ell : I_\ell)}{(1-F)(R_\ell : I_\ell)}.$$

Recall that R_ℓ is Gorenstein if and only if R_ℓ^t is principal. Hence we have that $(R_\ell : I_\ell) = (R_\ell^t I)^t \simeq I_\ell^t$. Also, recall that for fractional ideals J_1 and J_2 we have an isomorphism of abelian groups $J_1^t/J_2^t \simeq J_2/J_1$. Hence we obtain isomorphisms of abelian groups

$$\frac{(R_\ell : I_\ell)}{(1-F)(R_\ell : I_\ell)} \simeq \frac{I_\ell^t}{(1-F)I_\ell^t} \simeq \frac{\frac{1}{(1-F)}I_\ell}{I_\ell} \simeq \frac{I_\ell}{(1-F)I_\ell},$$

which concludes the proof at $\ell \neq p$. □

5. Polarizations and automorphisms in $\mathrm{AV}^{ord}(q)$

Let h be an ordinary square-free polynomial in $\mathcal{W}(q)$ and define K and R as above. Observe that K is a CM-algebra with involution defined by $\overline{\alpha} = q/\alpha$. Note that $\overline{R} = R$.

Lemma 5.1. *Let I be a fractional R-ideal. Then*

$$(\overline{I})^t = \overline{(I^t)}.$$

Proof. For $z \in K$, let m_z be its minimal polynomial over $\mathbb{Q}$. Observe that $m_{\overline{z}} = m_z$ and in particular $\mathrm{Tr}_{K/\mathbb{Q}}(z) = \mathrm{Tr}_{K/\mathbb{Q}}(\overline{z})$. It follows that

$$\begin{aligned} a \in (\overline{I})^t \iff \mathrm{Tr}_{K/\mathbb{Q}}(a\overline{i}) \in \mathbb{Z} \text{ for every } i \in I \iff \\ \iff \mathrm{Tr}_{K/\mathbb{Q}}(\overline{a}i) \in \mathbb{Z} \text{ for every } i \in I \iff a \in \overline{(I^t)}, \end{aligned}$$

which concludes the proof. □

In this section we describe how to compute the dual abelian variety, polarizations and automorphisms of a polarized abelian variety in $\mathrm{AV}(h)$.

Theorem 5.2. *Let A be an abelian variety in $\mathrm{AV}(h)$ and $I = \mathcal{F}(A)$ be the corresponding ideal in $\mathcal{I}(R)$, where $\mathcal{F}$ is the functor of Corollary 4.4. Then $\overline{I}^t = \mathcal{F}(A^\vee)$, where $A^\vee$ denotes the dual abelian variety of A. Moreover, if*

$$\mathcal{F}(\lambda\colon A \to B) = I \overset{\dot{a}}{\to} J$$

then

$$\mathcal{F}(\lambda^\vee\colon B^\vee \to A^\vee) = \overline{J}^t \overset{\dot{\overline{a}}}{\to} \overline{I}^t,$$

where $\lambda^\vee$ is the morphism dual to λ and $\dot{a}$ (resp. $\dot{\overline{a}}$) denotes the R-linear morphism multiplication-by-a (resp. multiplication-by-$\overline{a}$).

Proof. Let $(T, F) = (T_A, F_A)$ be the module in $\mathcal{M}(h)$ corresponding to A. By [How95, Proposition 4.5] the dual abelian variety $A^\vee$ corresponds to

$$(T_{A^\vee}, F_{A^\vee}) = (T^\vee, F^\vee),$$

where $T^\vee = \mathrm{Hom}_{\mathbb{Z}}(T, \mathbb{Z})$ and $F^\vee(\psi) = \psi \circ V$, for every $\psi \in T^\vee$. Let n be the degree of h. Fix a $\mathbb{Z}$-basis $\alpha_1, \ldots, \alpha_n$ of I and consider the $\mathbb{Z}$-linear maps:

$$\begin{aligned} \mathrm{Hom}_{\mathbb{Z}}(I, \mathbb{Z}) &\longrightarrow \overline{I}^t & \text{and} \qquad \overline{I}^t &\longrightarrow \mathrm{Hom}_{\mathbb{Z}}(I, \mathbb{Z}) \\ \psi &\longmapsto \sum_{i=1}^n \psi(\alpha_i)\overline{\alpha_i^*} & z &\longmapsto \mathrm{Tr}_{K/\mathbb{Q}}(\overline{z} \cdot -) \end{aligned}$$

These maps are clearly inverses of each other and hence we have that

$$\Psi((T^\vee, F^\vee)) = \overline{I}^t,$$

where Ψ is the functor defined in the proof of Theorem 4.3, or equivalently, that $\mathcal{F}(A^\vee) = \overline{I}^t$. The second statement follows in an analogous manner. □

A morphism $\lambda : (T, F) \to (T', F')$ in $\mathcal{M}^{ord}(q)$ corresponds to an isogeny if the induced linear map $\lambda \otimes \mathbb{Q}$ is invertible, see [How95, Section 4, p.2368]. In particular, if $\lambda : A \to B$ is a morphism in $\mathrm{AV}(h)$ then it is an isogeny if and only if $\mathcal{F}(\lambda) = a$ is not a zero-divisor, that is $a \in K^\times$.

An isogeny $\lambda : (T,F) \to (T^\vee, F^\vee)$ defines a bilinear map $b : T \times T \to \mathbb{Z}$ by $b(s,t) = \lambda(t)(s)$. For such b, by [Knu91, Theorem 1.7.4.1,p.44], there exists a unique R-sesquilinear form S on $T \otimes \mathbb{Q}$ such that $b = \mathrm{Tr}_{K/\mathbb{Q}} \circ S$.

Since K is a CM-algebra, homomorphisms $K \to \mathbb{C}$ come in conjugate pairs. A *CM-type* of K is a choice of pairwise non-conjugate morphisms $\varphi_1, \dots, \varphi_g : K \to \mathbb{C}$, where $2g = \dim_{\mathbb{Q}} K$. Consider the set

$$\Phi := \{\varphi : K \to \mathbb{C} : v_p(\varphi(F)) > 0\}, \tag{5.1}$$

where v_p is the p-adic valuation induced by the embedding $\varepsilon\colon W \to \mathbb{C}$ as in Remark 3.3. Note that Φ is a CM-type of K since the polynomial h is ordinary.

An element $a \in K$ is called *totally imaginary* if $a = -\overline{a}$, or equivalently, if $\psi(a)$ is totally imaginary for every $\psi : K \to \mathbb{C}$. Such an element is said to be Φ-positive (resp. non-positive) if $\Im(\varphi(a)) > 0$ (resp. $\Im(\varphi(a)) \le 0$) for every φ in Φ.

Proposition 5.3 ([How95, Proposition 4.9])**.** *An isogeny $\lambda : (T,F) \to (T^\vee, F^\vee)$ corresponds to a polarization if and only if*

- *S is a skew-Hermitian form, that is $S(t_1,t_2) = -\overline{S(t_2,t_1)}$ for every $t_1, t_2 \in T \otimes \mathbb{Q}$, and*
- *$S(t,t)$ is Φ-non-positive for every $t \in T \otimes \mathbb{Q}$.*

Theorem 5.4. *Let h be a square-free ordinary polynomial in $\mathcal{W}(q)$ and let A be an abelian variety in $\mathrm{AV}(h)$. Define R and K as above and put $I = \mathcal{F}(A)$. Then:*

(a) given an isogeny $\lambda\colon A \to A^\vee$ put $a = \mathcal{F}(\lambda)$. Then λ is a polarization if and only if a satisfies:
- *$aI \subseteq \overline{I}^t$,*
- *a is totally imaginary, and*
- *a is Φ-positive.*

Moreover, we have $\deg \lambda = [\overline{I}^t : aI]$.

(b) given two polarizations λ and λ' of A, there is an isomorphism $(A,\lambda) \simeq (A,\lambda')$ if and only if there exists $v \in (I : I)^\times$ such that

$$a = \overline{v} a' v,$$

where $a = \mathcal{F}(\lambda)$ and $a' = \mathcal{F}(\lambda')$. In particular, we have

$$\mathrm{Aut}((A,\lambda)) = (I : I)^\times \cap \mu_K,$$

where μ_K is the group of torsion units of K.

Proof. (a) Let T be the module associated to A. Let $b\colon T \times T \to \mathbb{Z}$ and $S\colon T_{\mathbb{Q}} \times T_{\mathbb{Q}} \to K$ be the forms associated to the polarization λ. We will use the same letters to denote the forms induced after applying the functor $\mathcal{F}$. Using Theorem 5.2 we see that

$$b(s,t) = \mathrm{Tr}(\overline{at}s),$$

which implies that

$$S(s,t) = \overline{at}s.$$

So by Proposition 5.3 we have that a corresponds to a polarization if and only if $a = -\overline{a}$ and $\overline{a}$ is Φ-non-positive. For the statement about the degree, see [How04, Section 4].

(b) The element v must be an automorphism of I, hence must be a unit of the multiplicator ring $(I:I)$. The diagram

$$\begin{tikzcd}
I \arrow[r, "a"] \arrow[d, "v"'] & \overline{I}^t \\
I \arrow[r, "a'"] & \overline{I}^t \arrow[u, "\overline{v}"']
\end{tikzcd}$$

must commute, i.e. $a = \overline{v}a'v$. In particular, if $a' = a$ then, a being a non-zero divisor (since it corresponds to an isogeny), this is equivalent to $v\overline{v} = 1$, that is v is a torsion unit, see [Neu99, Proposition 7.1].

□

Note that such an ideal theoretic description was already used in [How04, Section 4] for simple abelian surfaces.

Recall that given an abelian variety A, a polarization a is said to be *decomposable* if there exist two polarized abelian varieties (B_1, b_1) and (B_2, b_2) and an isomorphism $\psi\colon A \to B_1 \times B_2$ such that $a = \psi^\vee \circ (b_1 \times b_2) \circ \psi$.

Corollary 5.5. *Let A be an abelian variety in* $\mathrm{AV}(h)$ *and put $I = \mathcal{F}(A)$. Assume that A admits a principal polarization λ. Then $(I:I)$ is a product of orders if and only if (A, λ) is decomposable and hence it is not (geometrically) isomorphic to the Jacobian of a curve. In particular, if R is a product of orders, then the isogeny class associated to h does not contain a Jacobian.*

Proof. Put $S = (I:I)$. Then by Corollary 4.6 S is a product if and only if every abelian variety with endomorphism ring S is isomorphic to a product of abelian varieties. In particular, if any one of them admits a principal polarization, this would be decomposable by Theorem 5.4 and hence cannot be isomorphic (as a polarized abelian variety) to the Jacobian of a curve. □

Remark 5.6. We cannot state a result analogous to Corollary 5.5 without assuming that h is squarefree.

6. Algorithms

The algorithms in this section have been implemented in Magma [BCP97] and the code is abailable on the author's webpage. We will use without mentioning a lot of algorithms for abelian groups, which can all be found in [Coh93, Section 2.4].

Algorithm 1: Isomorphism classes in a given isogeny class

```
Input: $h$ a square-free ordinary polynomial in $\mathcal{W}(q)$ or a square-free
       polynomial in $\mathcal{W}(p)$ with no real roots;
Output: a list of fractional ideals representing the isomorphism classes of the
        abelian varieties in the isogeny class determined by $h$;
$K := \mathbb{Q}[x]/(h)$;
$F := x \mod (h)$;
$V := qF^{-1}$;
$R := \mathbb{Z}[F, V]$;
return $\mathrm{ICM}(R)$;
```

Theorem 6.1. *Algorithm 1 is correct.*

Proof. The correctness follows from Theorem 4.3. □

Remark 6.2. In [Mar20] we describe in detail how to compute $\mathrm{ICM}(R)$ for any order R in a finite product of number fields K.

```
Algorithm 2: CM-type
  Input: $h$ a square-free ordinary polynomial in $\mathcal{W}(q)$;
  Output: a CM-type $\Phi$ as in (5.1);
  write $h = \prod_{i=1}^{r} h_i$ with $h_i$ irreducible;
  $\mathbb{Q}(F) := \mathbb{Q}[x]/(h)$;
  $M :=$ SplittingField($h$);
  $\mathfrak{P} :=$ a maximal ideal of $M$ above $p$;
  $\psi_0 :=$ a homomorphism $M \to \mathbb{C}$;
  for $i = 1 \dots r$ do
      $d_i := \deg(h_i)$;
      $\mathbb{Q}(F_i) := \mathbb{Q}[x]/(h_i)$;
      let $F_{i,1}, \dots, F_{i,d_i}$ be the conjugates of $F_i$ in $M$;
  end
  $\Phi := \{\ \}$;
  for $\varphi \in \mathrm{Hom}(\mathbb{Q}(F), \mathbb{C})$ do
      if $\varphi(F) = (\psi_0(F_{1,j_1}) \times \dots \times \psi_0(F_{r,j_r}))$ with $F_{1,j_1}, \dots, F_{r,j_r} \in \mathfrak{P}$ then
          add $\varphi$ to $\Phi$;
      end
  end
  return $\Phi$;
```

Theorem 6.3. *Algorithm 2 is correct.*

Proof. Use the notation as in the Algorithm. Fixing an embedding of $\varepsilon \colon W \to \mathbb{C}$ as in Remark 3.3 encompasses fixing prime above p and an embedding for each extension containing the fields $\mathbb{Q}(F_i)$, $i = 1 \dots r$ in a compatible way. Since we need a field containing all the conjugates of F_i for all i, the most efficient choice is to work with the compositum M of the Galois closures of the fields $\mathbb{Q}(F_i)$, which is precisely the splitting field of the polynomial h. Under these identifications, we get

$$\begin{aligned} \varphi \in \Phi &\iff v_p(\varphi|_{\mathbb{Q}(F_i)}(F_i)) > 0 \text{ for } i = 1, \dots, r \\ &\iff \psi_0^{-1}(\varphi|_{\mathbb{Q}(F_i)}(F_i)) \in \mathfrak{P} \text{ for } i = 1, \dots, r. \end{aligned}$$

Since the polynomial h is ordinary, the set Φ consists of exactly half of the homomorphisms $K \to \mathbb{C}$, one for each conjugate pair. □

Theorem 6.4. *Algorithm 3 is correct.*

Proof. For each unit $u \in S^\times$ and homomorphism $\varphi : K \to \mathbb{C}$ we have that $\varphi(u/\overline{u})$ lies on the unit circle. Hence by [Neu99, Proposition 7.1] the quotient $\zeta = u/\overline{u}$ has finite multiplicative order, say n. Then $u^{2n} = u^n(u\zeta)^n = u^n\overline{u}^n = (u\overline{u})^n$. In particular the abelian group Q is torsion. By the Dirichlet Unit Theorem the unit group $S^\times$ is a finitely generated abelian group, and therefore it follows that Q is finite. Observe that given two fractional R-ideals H and I, they are isomorphic if

```
Algorithm 3: Polarizations of a given abelian variety
Let $h$ be a square-free ordinary polynomial in $\mathcal{W}(q)$;
Put $K := \mathbb{Q}[x]/(h)$, $F := x \mod (h)$, $V := qF^{-1}$ and $R := \mathbb{Z}[F,V]$;
Input: a fractional $R$-ideal $I$ corresponding to an abelian variety $A$; a
       positive integer $N$;
Output: a sequence $\mathcal{P}$ of elements of $K^\times$ corresponding to all pairwise
        non-isomorphic polarizations of $A$ of degree $N$;
Compute the CM-type $\Phi$ using Algorithm 2;
$S := (I:I)$;
$\mathcal{K} := \langle v\overline{v} : v \in S^\times \rangle$ ;    // consider $S^\times$ and $\mathcal{K}$ as subgroups of $(S\overline{S})^\times$
$Q := S^\times/\mathcal{K} \cap S^\times$;
$\mathcal{Q} := \{$representatives in $S^\times$ of the elements of $Q\}$;
$\mathcal{S}' := \left\{\text{subgroups } H \text{ of } \overline{I}^t \text{ such that } [\overline{I}^t : H] = N\right\}$;
$\mathcal{S} := \{H \in \mathcal{S}' : H$ is an $R$-module with multiplicator ring $S\}$;
$\mathcal{P} := \{\ \}$;
for $H \in \mathcal{S}$ do
    if $(H:I) = x_0S$ then
        $\mathcal{P}_H := \{\ \}$;
        for $u \in \mathcal{Q}$ do
            $y := x_0u$;
            if $\overline{y} = -y$ and $y$ is $\Phi$-positive then
                Append $y$ to $\mathcal{P}_H$;
            end
        end
    end
end
$\mathcal{P}' := \bigcup_{H\in\mathcal{S}} \mathcal{P}_H$;
for $\lambda \in \mathcal{P}'$ do
    if there is no $\lambda' \in \mathcal{P}$ such that $\lambda/\lambda' \in \mathcal{K}$ then
        Append $\lambda$ to $\mathcal{P}$;
    end
end
return $\mathcal{P}$;
```

and only if they have the same multiplicator ring and $(H : I)$ is a principal ideal, see [Mar20, Proposition 4.1.(c), Corollary 4.5]. Note that once we know that $(H : I)$ is invertible in S, checking whether it is a principal ideal it is a finite problem and can be done efficiently if have already computed $\operatorname{Pic}(S)$, see for example [Coh93, 6.5.5]. For each $H \in \mathcal{S}$ with $x_0I = H$, the set $\mathcal{P}_H$ contains all polarizations of I with image H up to isomorphism by Theorem 5.4. So in particular the set $\mathcal{P}'$ contains all polarizations of I of degree N. By Part (b) of Theorem 5.4 λ and λ' in $\mathcal{P}'$ are isomorphic if and only if λ/λ' is in $\mathcal{K}$. This concludes the proof of the correctness of Algorithm 3. □

Remark 6.5. Observe that Algorithm 3 can be simplified if $S^\times = \overline{S^\times}$. In this is the case, the set $\mathcal{P}$ coincides with $\mathcal{P}'$, that is, we can skip the last loop. Indeed assume that λ and λ' are in $\mathcal{P}'$, and satisfy $\lambda I = H$ and $\lambda' I = H'$. If $\lambda = v\overline{v}\lambda'$ for some $v \in S^\times = \overline{S^\times}$ then $H = v\overline{v}H' = H'$, and hence λ and λ' are both in $\mathcal{P}_H$ which implies that they must coincide, since $\mathcal{P}_H$ contains only one representative for each isomorphism class. This observation is particularly useful when we compute principal polarizations, because if I admits a principally polarization then $S = \overline{S}$.

```
Algorithm 4: Automorphism of a polarized abelian variety
  Input: a pair $(I, x)$ corresponding to a polarized abelian variety $(A, \mu)$;
  Output: a finite abelian group $H$ corresponding to $\mathrm{Aut}((A, \mu))$;
  $S := (I : I)$;
  $H := \mathrm{torsion}(S^\times)$;
  return $H$;
```

Theorem 6.6. *Algorithm 4 is correct.*

Proof. It follows from Part (b) of Theorem 5.4. □

7. Examples

Elliptic curves. Every elliptic curve E comes with a unique principal polarization. This means that counting the isomorphism classes of elliptic curves over $\mathbb{F}_q$ is the same as counting the principally polarized ones. The characteristic polynomial of the Frobenius endomorphism of an elliptic curve over $\mathbb{F}_q$ has the form $x^2 + \beta x + q$ with $|\beta| \leq 2\sqrt{q}$ by Hasse's Theorem. Not every β in this range gives rise to an isogeny class of an elliptic curve. See [Wat69, Theorem 4.1] for a complete list. Let $N_q(\beta)$ be the number of isomorphism classes of elliptic curves over $\mathbb{F}_q$ in the isogeny class determined by the characteristic polynomial $h = x^2 + \beta x + q$ weighted with the reciprocal of the number of automorphisms over $\mathbb{F}_q$. As a consequence of Corollary 4.4 we get the following Proposition, which reproves a well known result by Deuring and Waterhouse. See [Wat69], [Deu41] and also [Sch87, Theorem 4.6].

Proposition 7.1. *Let $q = p^r$, where p is a prime number and r is a positive integer. Let β be an integer satisfying $\beta^2 < 4q$. If $r > 1$ assume also that β is coprime with p. Then*

$$N_q(\beta) = \frac{\#\,\mathrm{Pic}(\mathcal{O}_K)}{\mathcal{O}_K^\times} \sum_{n|f} n \prod_{p|n} \left(1 - \left(\frac{\Delta_K}{p}\right)\frac{1}{p}\right),$$

where $K = \mathbb{Q}[x]/(h)$, $R = \mathbb{Z}[x]/(h)$ and $f = [\mathcal{O}_K : R]$ with $h = x^2 + \beta x + q$.

Proof. The assumptions on β mean that, for an elliptic curve E in the isogeny class determined by β, we have $E \in \mathrm{AV}^{ord}(q)$ or $E \in \mathrm{AV}^{cs}(p)$, since there is no characteristic polynomial of an elliptic curve over $\mathbb{F}_p$ with root $\sqrt{p}$. Observe that if we write $R = \mathbb{Z}[\alpha]$ then q/α is in R. In a quadratic field every order is Bass and hence by [Mar20, Proposition 3.7] we have

$$\mathrm{ICM}(R) = \bigsqcup_{R \subseteq S \subseteq \mathcal{O}_K} \mathrm{Pic}(S).$$

Therefore, by Corollary 4.4 and Corollary 4.6.(b), we obtain

$$N_q(\beta) = \sum_{R\subseteq S\subseteq \mathcal{O}_K} \frac{\#\operatorname{Pic}(S)}{\# S^\times}.$$

Since K is a quadratic field we know that each order S is uniquely determined by its index $[\mathcal{O}_K : S]$ and these are precisely the divisors of f. To conclude we just need to observe that if $[\mathcal{O}_K : S] = n$ then we have that

$$\#\operatorname{Pic}(S) = \frac{\#\operatorname{Pic}(\mathcal{O}_K)}{[\mathcal{O}_K^\times : S^\times]} n \prod_{p\mid n}\left(1 - \left(\frac{\Delta_K}{p}\right)\frac{1}{p}\right),$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol for p odd and the Kronecker symbol for $p = 2$, see [Cox13, Theorem 7.24]. □

Higher dimension. Here we present some examples in dimension greater than 1. The code to recompute them is available at `https://raw.githubusercontent.com/stmar89/AbVarFq/master/e`

Example 7.2. Consider the polynomial $h = x^4 + 2x^3 - 7x^2 + 22x + 121$. By [How95, Theorem 1.3] we know that the corresponding isogeny class of simple abelian surfaces over $\mathbb{F}_{11}$ does not contain a principally polarized variety. Put $K = \mathbb{Q}[x]/h = \mathbb{Q}(\alpha)$. Let R be the order $\mathbb{Z}[\alpha, 11/\alpha]$. The only proper over-order of R is the maximal order $\mathcal{O}_K$. Since both orders are Gorenstein, the isomorphism classes of the abelian varieties in the isogeny class determined by h functorially correspond to

$$\operatorname{Pic}(R) \sqcup \operatorname{Pic}(\mathcal{O}_K).$$

Moreover we have $\operatorname{Pic}(R) \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ and $\operatorname{Pic}(\mathcal{O}_K) \simeq \mathbb{Z}/2\mathbb{Z}$, so in particular we have 6 isomorphism classes of abelian varieties. Two of the 4 isomorphism classes with endomorphism ring R have 2 non-isomorphic polarizations of degree 4 while the other 2 have 2 non-isomorphic polarizations of degree 25. One of the isomorphism classes with endomorphism ring $\mathcal{O}_K$ has 2 non-isomorphic polarizations of degree 4 while the other has 2 non-isomorphic polarizations of degree 25. The degrees mentioned above are minimal, in the sense that the isomorphism class does not admit a polarization of smaller degree. All the above polarized varieties have automorphism groups of order 2.

Example 7.3. Let $h = x^6 - 2x^5 - 3x^4 + 24x^3 - 15x^2 - 50x + 125$. This is the characteristic polynomial of an isogeny class of simple abelian varieties over $\mathbb{F}_5$ of dimension 3. Put $K = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/h$ and denote by R the order $\mathbb{Z}[\alpha, 5/\alpha]$. There are 5 over-orders of R, all stable under complex conjugation. One of the over orders is not Gorenstein. We denote this order by S. Moreover denote by T the unique over-order of R such that $[\mathcal{O}_K : T] = 2$ and the group of torsion units is $\mu(T^\times) \simeq \mathbb{Z}/2\mathbb{Z}$.

The $\operatorname{ICM}(R)$ consists of 14 classes, so there are 14 isomorphism classes of abelian threefolds over $\mathbb{F}_5$ with characteristic polynomial h. Among these 14 classes 2 are not invertible in their multiplicator ring S.

We compute that 8 isomorphism classes are principally polarized. They are all invertible in their multiplicator rings. More precisely, they correspond to isomorphism classes in

$$\operatorname{Pic}(R) \sqcup \operatorname{Pic}(T) \sqcup \operatorname{Pic}(\mathcal{O}_K)$$

and all admit a unique principal polarization up to isomorphism. The polarized isomorphism classes with endomorphism ring R and T have 2 automorphisms and the one with maximal endomorphism ring have automorphism group $\mathbb{Z}/4\mathbb{Z}$.

Example 7.4. Let

$$h = x^8 - 5x^7 + 13x^6 - 25x^5 + 44x^4 - 75x^3 + 117x^2 - 135x + 81.$$

This is the characteristic polynomial of an isogeny class of simple abelian varieties over $\mathbb{F}_3$ of dimension 4. Let $K = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/h$ and denote by R the order $\mathbb{Z}[\alpha, 3/\alpha]$. There are 8 over-orders of R.

The ICM(R) consists of 18 classes, so there are 18 isomorphism classes of abelian fourfolds over $\mathbb{F}_3$ with characteristic polynomial h. Among these 18 classes, 5 are not invertible in their multiplicator rings. It turns out that 10 out of the 18 ideal classes are isomorphic to the class of the conjugate of the trace dual ideal and 2 of them are non-invertible. This means that the corresponding abelian varieties are isomorphic to their dual. Not all of them are principally polarized.

There are 8 isomorphism classes which are principally polarized, all admitting a unique principal polarization up to isomorphism. The ideals corresponding to 2 of them are not invertible in their multiplicator ring. All the principal polarized abelian varieties have automorphism group of order 2, but the ones with maximal endomorphism ring which have 10 automorphisms.

We also notice that in this example there are abelian varieties with the same endomorphism ring, but non-isomorphic groups of rational points.

Example 7.5. In the following table we present the results of our computations of the isomorphism classes of all ordinary square-free isogeny classes of abelian surface over $\mathbb{F}_p$ for $p = 2, 3, 5, 7$ and 11. We will use the following notation:

- N_1: ordinary square-free isogeny classes over $\mathbb{F}_p$,
- N_2: isomorphism classes of abelian varieties,
- N_3: isomorphism classes of abelian varieties which do not admit a principal polarization,
- N_4: polarized isomorphism classes of principally polarized abelian varieties,
- N_5: isomorphism classes of abelian varieties with maximal endomorphism ring,
- N_6: isomorphism classes of abelian varieties with maximal endomorphism ring which do not admit a principal polarization.

p	N_1	N_2	N_3	N_4	N_5	N_6
2	14	21	7	15	15	3
3	36	76	23	59	43	6
5	94	457	203	290	159	34
7	168	1324	636	797	387	88
11	352	4925	2675	2797	1476	459

We remark that the proportion of abelian surfaces that do not admit a principal polarization is much lower when we restrict ourselves to the surfaces with endomorphism ring which is the maximal order of the endomorphism algebra. We have on-going computations for $g = 3$ that show that this difference becomes much more pronounced.

8. Period Matrices

Let A be an abelian variety in $\mathrm{AV}(h)$ for a square-free ordinary polynomial h in $\mathcal{W}(q)$ of degree $2g$ and I be the corresponding fractional R-ideal, where $R = \mathbb{Z}[F,V]$ as usual. Let A' be the complex abelian variety $\tilde{A} \otimes_\varepsilon \mathbb{C}$ as in Remark 3.3. Recall that $I = H_1(A',\mathbb{Z})$ as abelian groups and choose a $\mathbb{Z}$-basis of I, say

$$I = \alpha_1\mathbb{Z} \oplus \ldots \oplus \alpha_{2g}\mathbb{Z}.$$

Assume also that A admits a principal polarization λ, which corresponds to multiplication by an element a in $K^\times$. Denote with λ' the polarization induced by λ on A'. Let $\Phi = \{\varphi_1, \ldots, \varphi_g\}$ be the CM-type found by Algorithm 2. Recall by [Del69, Section 8] that this particular CM-type characterizes the complex structure on $I \otimes \mathbb{R}$ induced by the identification with the lie algebra of the complex abelian variety A', via the isomorphism of complex tori

$$A'(\mathbb{C}) \simeq \frac{\mathbb{C}^g}{\Phi(I)},$$

where $\Phi(I)$ is the lattice in $\mathbb{C}^g$ spanned by the complex vectors

$$(\varphi_1(\alpha_i), \ldots, \varphi_g(\alpha_i)) \qquad i = 1, \ldots, 2g.$$

A *period matrix* associated to A' is a $g \times 2g$ complex matrix whose columns are the coordinates of a $\mathbb{Z}$-basis of the full lattice $\Phi(I)$. We are interested in a matrix that captures the Riemann form induced by the polarization λ' of A'.

More precisely, as in the proof of Theorem 5.4 we obtain that the Riemann form associated to a is given by

$$b\colon I \times I \to \mathbb{Z} \quad (s,t) \mapsto \mathrm{Tr}(\overline{ta}s).$$

We can choose now a symplectic $\mathbb{Z}$-basis of I with respect to the form b, that is,

$$I = \gamma_1\mathbb{Z} \oplus \ldots \oplus \gamma_g\mathbb{Z} \oplus \beta_1\mathbb{Z} \oplus \ldots \oplus \beta_g\mathbb{Z},$$

and

$$b(\gamma_i, \beta_i) = 1 \text{ for all } i, \text{ and}$$

$$b(\gamma_h, \gamma_k) = b(\beta_h, \beta_k) = b(\gamma_h, \beta_k) = 0 \text{ for all } h \neq k.$$

Such symplectic basis can be computed with appropriate modifications of the Gram-Schmidt orthogonalization process, see for example [CdS01, Theorem 1.1].

Consider the $g \times 2g$ matrix Ω whose i-th row is

$$(\varphi_i(\gamma_1), \ldots, \varphi_i(\gamma_g), \varphi_i(\beta_1), \ldots, \varphi_i(\beta_g)).$$

This is what is usually called the *big period matrix* of (A', λ'). If we write $\Omega = (\Omega_1, \Omega_2)$ we can recover the $g \times g$ *small period matrix* or *Riemann matrix* τ by

$$\tau = \Omega_2^{-1}\Omega_1.$$

Example 8.1. Let $f = (x^4 - 4x^3 + 8x^2 - 12x + 9)(x^4 - 2x^3 + 2x^2 - 6x + 9)$, which identifies an isogeny class of abelian four-folds over $\mathbb{F}_3$. We compute the principally polarized abelian varieties and we find that 4 isomorphism classes admit a unique principal polarization. Here we present one of them with the corresponding (approximations of the) big and small period matrices.

$$\begin{aligned}
I &= \frac{1}{54}\left(432 - 549\alpha + 441\alpha^2 - 331\alpha^3 + 186\alpha^4 - 81\alpha^5 + 33\alpha^6 - 7\alpha^7\right)\mathbb{Z}\oplus\\
&\oplus \frac{1}{6}\left(63 - 78\alpha + 65\alpha^2 - 49\alpha^3 + 27\alpha^4 - 12\alpha^5 + 5\alpha^6 - 1\alpha^7\right)\mathbb{Z}\oplus\\
&\oplus \frac{1}{6}\left(81 - 99\alpha + 84\alpha^2 - 61\alpha^3 + 33\alpha^4 - 15\alpha^5 + 6\alpha^6 - 1\alpha^7\right)\mathbb{Z}\oplus\\
&\oplus \frac{1}{18}\left(-63 + 96\alpha - 86\alpha^2 + 68\alpha^3 - 39\alpha^4 + 18\alpha^5 - 8\alpha^6 + 2\alpha^7\right)\mathbb{Z}\oplus(-1)\mathbb{Z}\oplus\\
&\oplus (-\alpha)\mathbb{Z}\oplus(-\alpha^2)\mathbb{Z}\oplus\frac{1}{9}\left(81 - 96\alpha + 81\alpha^2 - 64\alpha^3 + 33\alpha^4 - 15\alpha^5 + 6\alpha^6 - \alpha^7\right)\mathbb{Z}\\
\mathrm{End}(I) &= \frac{1}{54}\left(432 - 549\alpha + 441\alpha^2 - 331\alpha^3 + 186\alpha^4 - 81\alpha^5 + 33\alpha^6 - 7\alpha^7\right)\mathbb{Z}\oplus\\
&\oplus \frac{1}{6}\left(63 - 78\alpha + 65\alpha^2 - 49\alpha^3 + 27\alpha^4 - 12\alpha^5 + 5\alpha^6 - 1\alpha^7\right)\mathbb{Z}\oplus\\
&\oplus \frac{1}{6}\left(81 - 99\alpha + 84\alpha^2 - 61\alpha^3 + 33\alpha^4 - 15\alpha^5 + 6\alpha^6 - 1\alpha^7\right)\mathbb{Z}\oplus\\
&\oplus \frac{1}{18}\left(-63 + 96\alpha - 86\alpha^2 + 68\alpha^3 - 39\alpha^4 + 18\alpha^5 - 8\alpha^6 + 2\alpha^7\right)\mathbb{Z}\oplus\\
&\oplus \frac{1}{54}\left(-378 + 549\alpha - 441\alpha^2 + 331\alpha^3 - 186\alpha^4 + 81\alpha^5 - 33\alpha^6 + 7\alpha^7\right)\mathbb{Z}\oplus\\
&\oplus \frac{1}{6}\left(-63 + 84\alpha - 65\alpha^2 + 49\alpha^3 - 27\alpha^4 + 12\alpha^5 - 5\alpha^6 + \alpha^7\right)\mathbb{Z}\oplus\\
&\oplus \frac{1}{6}\left(-81 + 99\alpha - 78\alpha^2 + 61\alpha^3 - 33\alpha^4 + 15\alpha^5 - 6\alpha^6 + \alpha^7\right)\mathbb{Z}\oplus\\
&\oplus \frac{1}{18}\left(-99 + 96\alpha - 76\alpha^2 + 60\alpha^3 - 27\alpha^4 + 12\alpha^5 - 4\alpha^6\right)\mathbb{Z}\\
x &= \frac{537}{80} - \frac{1343}{120}\alpha + \frac{1343}{144}\alpha^2 - \frac{419}{60}\alpha^3 + \frac{337}{80}\alpha^4 - \frac{15}{8}\alpha^5 + \frac{559}{720}\alpha^6 - \frac{1}{5}\alpha^7
\end{aligned}$$

$$\Omega = \begin{pmatrix} 2.8 - i & -2.8 + 0.59i & 0 & 0 & 1 & 1.7 - 0.29i & 0 & 0\\ -2.8 + i & 2.8 - 3.4i & 0 & 0 & 1 & 0.29 + 1.7i & 0 & 0\\ 0 & 0 & -1 & -0.38 - 0.15i & 0 & 0 & -1.6 - 0.62i & -0.15 - 0.15i\\ 0 & 0 & -1 & -2.6 + 6.9i & 0 & 0 & 0.62 - 1.6i & -6.9 + 6.9i \end{pmatrix},$$

$$\tau = \begin{pmatrix} -1 - 2.8i & 2 + 1.4i & 0 & 0\\ 2 + 1.4i & -2.7 - 0.95i & 0 & 0\\ 0 & 0 & 0.52 - 0.21i & 0.14\\ 0 & 0 & 0.14 & 0.71 - 0.31i \end{pmatrix}$$

References

[AG17] Jeffrey D. Achter and Julia Gordon, *Elliptic curves, random matrices and orbital integrals*, Pacific J. Math. **286** (2017), no. 1, 1–24, With an appendix by S. Ali Altuğ.

[AW15] Jeffrey Achter and Cassandra Williams, *Local heuristics and an exact formula for abelian surfaces over finite fields*, Canad. Math. Bull. **58** (2015), no. 4, 673–691.

[BCP97] 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.

[CdS01] Ana Cannas da Silva, *Lectures on symplectic geometry*, Lecture Notes in Mathematics, vol. 1764, Springer-Verlag, Berlin, 2001.

[Coh93] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993.

[Cox13] David A. Cox, *Primes of the form $x^2 + ny^2$*, second ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2013.

[CS15] Tommaso Giorgio Centeleghe and Jakob Stix, *Categories of abelian varieties over finite fields, I: Abelian varieties over $\mathbb{F}_p$*, Algebra Number Theory **9** (2015), no. 1, 225–265.

[Del69] Pierre Deligne, *Variétés abéliennes ordinaires sur un corps fini*, Invent. Math. **8** (1969), 238–243.

[Deu41] Max Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Univ. Hamburg **14** (1941), no. 1, 197–272.

[Hon68] Taira Honda, *Isogeny classes of abelian varieties over finite fields*, J. Math. Soc. Japan **20** (1968), 83–95.

[How95] Everett W. Howe, *Principally polarized ordinary abelian varieties over finite fields*, Trans. Amer. Math. Soc. **347** (1995), no. 7, 2361–2401.

[How04] ———, *On the non-existence of certain curves of genus two*, Compos. Math. **140** (2004), no. 3, 581–592.

[JKP$^+$18] Bruce W. Jordan, Allan G. Keeton, Bjorn Poonen, Eric M. Rains, Nicholas Shepherd-Barron, and John T. Tate, *Abelian varieties isogenous to a power of an elliptic curve*, Compos. Math. **154** (2018), no. 5, 934–959.

[Kan11] Ernst Kani, *Products of CM elliptic curves*, Collect. Math. **62** (2011), no. 3, 297–339.

[Knu91] Max-Albert Knus, *Quadratic and Hermitian forms over rings*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 294, Springer-Verlag, Berlin, 1991, With a foreword by I. Bertuccioni.

[Lau02] Kristin Lauter, *The maximum or minimum number of rational points on genus three curves over finite fields*, Compositio Math. **134** (2002), no. 1, 87–111, With an appendix by Jean-Pierre Serre.

[Len96] H. W. Lenstra, Jr., *Complex multiplication structure of elliptic curves*, J. Number Theory **56** (1996), no. 2, 227–241.

[LMF13] The LMFDB Collaboration, *The l-functions and modular forms database*, `http://www.lmfdb.org`, 2013, [Online; accessed 16 September 2013].

[LPP02] H. W. Lenstra, Jr., J. Pila, and Carl Pomerance, *A hyperelliptic smoothness test. II*, Proc. London Math. Soc. (3) **84** (2002), no. 1, 105–146.

[Mar16] Stefano Marseglia, *Isomorphism classes of abelian varieties over finite fields*, Stockholm University, 2016.

[Mar18a] ———, *Computing abelian varieties over finite fields*, Stockholm University, 2018.

[Mar18b] Chloe Martindale, *Isogeny graphs, modular polynomials, and applications*, Universit de Bordeaux,, 2018.

[Mar20] Stefano Marseglia, *Computing the ideal class monoid of an order*, Journal of the London Mathematical Society **101** (2020), no. 3, 984–1007.

[Neu99] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[OS] Abhishek Oswal and Ananth N. Shankar, *Almost ordinary abelian varieties over finite fields*, Journal of the London Mathematical Society **101** (2020), no. 3, 923–937.

[Ros86] Michael Rosen, *Abelian varieties over* **C**, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 79–101.

[Sch87] René Schoof, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory Ser. A **46** (1987), no. 2, 183–211.

[ST18] Ananth N. Shankar and Jacob Tsimerman, *Unlikely intersections in finite characteristic*, Forum Math. Sigma **6** (2018), e13, 17.

[Tat66] John Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144.

[Tat71] ———, *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)*, Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363, Lecture Notes in Math., vol. 175, Springer, Berlin, 1971, pp. Exp. No. 352, 95–110.

[Wat69] William C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560.

Matematiska institutionen, Stockholms universitet, Sweden
Current address: Mathematical Institute, Utrecht University, The Netherlands
E-mail address: `s.marseglia@uu.nl`