Almost ordinary abelian varieties over finite fields

Abhishek Oswal and Ananth N. Shankar

October 10, 2019

Abstract

We provide a characterization of simple almost ordinary abelian varieties over finite fields (of odd characteristic) analogous to work of Deligne [3] in the ordinary case, and work of Centeleghe–Stix [1] in the case of abelian varieties over $\mathbb{F}_p$. We then use this characterization to provide lower bounds for the sizes of many almost ordinary isogeny classes.

Contents

2010 *Mathematical Subject Classification* 11G10, 14K10.

1 Introduction

In his work [3], Deligne provides a classification of ordinary abelian varieties over finite fields. The key ingredient required for this classification is the existence of the so-called “canonical lift” to characteristic zero of an ordinary abelian variety. The content of this paper is to provide a similar classification of certain abelian varieties over finite fields with odd characteristic p, which are *almost ordinary*, and use this classification to estimate the size of certain isogeny classes. We note that Centeleghe and Stix in [1] also have a characterization of abelian varieties which aren’t necessarily ordinary (therefore generalizing [3]). However, their characterization is for abelian varieties over the prime field $\mathbb{F}_p$, and their methods do not make use of lifts to characteristic zero.

We define a “simple almost ordinary abelian variety” over a finite field to be a g-dimensional abelian variety over a finite field which is simple and has p-rank equal to $g-1$, where $g \geq 2$. For almost ordinary abelian varieties, the condition that one such is simple is equivalent to the condition that it is geometrically simple. Honda–Tate theory implies that the endomorphism algebra of such an abelian variety equals a CM field K. The slope $1/2$ part of A corresponds to K_{ss}, a quadratic extension of $\mathbb{Q}_p$, which is contained in $K \otimes \mathbb{Q}_p$. We call the almost ordinary abelian variety *ramified* K_{ss} is a ramified extension of $\mathbb{Q}_p$ and *inert* if otherwise.

The main result of this paper is

Theorem 1.1. *Let $\mathcal{C}_h$ denote the category of simple almost ordinary abelian varieties corresponding to the Frobenius-polynomial h. Let $\mathcal{L}_h$ denote the category of almost ordinary Deligne modules* [1]*, also corresponding to the Frobenius polynomial h.*

1. *Suppose that $\mathcal{C}_h$ is ramified. There exists a canonical pair of functors $\mathfrak{T}_1, \mathfrak{T}_2$ from $\mathcal{C}_h$ to $\mathcal{L}_h$, both of which induce an equivalence of categories.*
2. *Suppose that $\mathcal{C}_h$ is inert. There are two full subcategories $\mathcal{C}_{1,h}$ and $\mathcal{C}_{2,h}$ of $\mathcal{C}_h$, and functors $\mathfrak{T}_i$ from $\mathcal{C}_{i,h}$ to $\mathcal{L}_h$, both of which induce an equivalence of categories. Further, the objects of the category $\mathcal{C}_h$ is a disjoint union of the objects of $\mathcal{C}_{1,h}$ and $\mathcal{C}_{2,h}$.*

Our characterization of simple almost ordinary abelian varieties is robust enough to deal with polarizations and duals (see Section 4). Theorem 1.1 can be used to estimate the size of polarized isogeny classes of almost ordinary abelian varieties. To that end, let A denote a simple almost ordinary abelian variety over $\mathbb{F}_q$. We define $I(A, q^n)$ to be the set of principally polarized abelian varieties over $\mathbb{F}_{q^n}$ which are isogenous to A. Then we prove the following result:

[1] See §3 and Definition 3.1 for the precise definitions

Theorem 1.2. *Suppose that the Frobenius torus*[2] *of A has full rank. Then we have the lower bound $\#I(A,q^n) \geq q^{n[g(g+1)/2-1+o(1)]/2}$ for a positive density set of integers n.*

The results of Lenstra–Zarhin [8, Theorem 5.8] show that the Frobenius torus of every simple even dimensional almost ordinary abelian variety has full rank. Therefore, we have the corollary

Corollary 1.3. *Let A be an even-dimensional simple almost ordinary abelian variety defined over $\mathbb{F}_q$. Then, we have the unconditional lower bound $\#I(A,q^n) \geq q^{n[g(g+1)/2-1+o(1)]/2}$ for a positive density set of integers n.*

We prove Theorem 1.2 by constructing an order R_n (see Section 5 for the definition of R_n) inside the endomorphism algebra associated to the isogeny class of A, and proving that the number of principally polarized abelian varieties over $\mathbb{F}_{q^n}$ with endomorphism ring R_n has the correct order of magnitude. The main obstruction to obtaining any sort of upper bound is the difficulty in estimating the number of orders containing R_n. We make the following conjecture:

Conjecture 1. *Let $A/\mathbb{F}_q$ be a simple almost ordinary abelian variety. For a positive proportion of integers n, $\#I(A,q^n) = q^{n(\dim \mathcal{A}_g - 1)(1/2+o(1))}$. Further, the right hand side is an upper-bound for all n.*

This agrees with Conjecture 3.1 of [13]. Indeed, the quantity $\dim \mathcal{A}_g$ in [13] is replaced by $\dim \mathcal{A}_g - 1$ because the Newton stratum consisting of almost ordinary abelian varieties has codimension 1 in $\mathcal{A}_g$, (as opposed to being of codimension 0, as in the ordinary case). Using these lower bounds, and the heuristics of [13], we have the following conjecture pertaining to abelian varieties isogenous to Jacobians:

Conjecture 2. *If $g \leq 9$, every g-dimensional almost ordinary abelian variety over $\overline{\mathbb{F}}_p$ is isogenous to the Jacobian of some curve. If $g \geq 10$, there exists an almost ordinary abelian variety over $\overline{\mathbb{F}}_p$ which is not isogenous to the Jacobian of any curve.*

In private communication, we have been informed that Edgar Costa, Taylor Dupuy, Stefano Marseglia, David Roe, Christelle Vincent, and Mckenzie West have forthcoming work where they will give algorithms to enumerate g-dimensional simple almost ordinary abelian varieties over $\mathbb{F}_q$ for small values of g and q, and that one of the inputs they use is the polarized version of Theorem 1.1. Therefore, our results have applications to both counting almost ordinary points in $\mathcal{A}_g(\mathbb{F}_q)$ contained within an isogeny class, as well as to more computational aspects of abelian varieties over finite fields.

Method of proof

One of the key steps in proving Theorem 1.1 is to construct an analogue of the "canonical lift" for a simple almost ordinary abelian variety A. Deuring in [4] proved that given any endomorphism of a supersingular elliptic curve, there exists a lift to characteristic zero of this endomorphism.

[2] For a definition of the Frobenius torus associated to an abelian variety, see [2, Section 3a].

The $\mathbb{F}_q$-structure on the supersingular part of $A[p^\infty]$ isolates a unique rank two subalgebra of $\mathrm{End}(A[p^\infty]_{\mathrm{ss}} \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q)$, and hence a choice of lift of $A[p^\infty]_{\mathrm{ss}}$ to mixed characterisic (see §2 for details). Using Grothendieck-Messing theory, we show that there is a canonical choice of lift in the inert case, and two equally canonical choices of lift in the ramified case.

Unlike the case of ordinary abelian varieties, there is no unique canonical functor between $\mathcal{C}_h$ and $\mathcal{L}_h$. This is because there are two different (and equally canonical) choices for a CM type on $K = \mathbb{Q}[x]/(h(x))$. Indeed, (after fixing an embedding of the algebraic closure of $\mathbb{Q}_p$ in $\mathbb{C}$) there are $g-1$ complex embeddings of K, say $\sigma_1^0, \dots, \sigma_{g-1}^0$, corresponding to the slope 0, $g-1$ embeddings, say $\sigma_1^1, \dots, \sigma_{g-1}^1$, corresponding to the slope 1 and 2 embeddings, say τ, τ', corresponding to the slope 1/2. The two different CM types are $\{\sigma_1^0, \dots, \sigma_{g-1}^0, \tau\} \coprod \{\sigma_1^1, \dots, \sigma_{g-1}^1, \tau'\}$ and $\{\sigma_1^0, \dots, \sigma_{g-1}^0, \tau'\} \coprod \{\sigma_1^1, \dots, \sigma_{g-1}^1, \tau\}$. This ambiguity in CM type affects functoriality in one of two possible ways, depending on whether the isogeny class is inert or ramified:

The inert case. In the inert case, even though there is a canonical choice of lifting, the association of the canonical lift to A is *not* functorial in A. Indeed, there is a distinguished order p subgroup of $A[p^\infty]_{\mathrm{ss}}$ which does not lift to a subgroup of the canonical lift, and it is using this subgroup that we define the subcategories of $\mathcal{C}_h$ — see Section 3.1 for more details. Once we restrict to one of the subcategories mentioned in the statement of Theorem 1.1, the association of the canonical lift to A becomes functorial. The above paragraph can be interpreted by saying that choosing a CM type on K is equivalent to choosing one of the two subcategories.

The ramified case. We prove that a choice of canonical lift for A fixes a natural choice of canonical lift for every other abelian variety isogenous to A, in a way that is functorial. That there are two different choices of compatible lifts in the ramified case corresponds to the ambiguity in picking a CM type on K.

Plan for the rest of the paper

We construct the canonical lift(s) in Section 2. We prove Theorem 1.1 in Section 3, and address the matter of polarizations in section 4. We apply the results of Sections 3 and 4 to establish lower bounds in Section 5.

Acknowledgements

It is a pleasure to thank Stefano Marseglia, Bjorn Poonen, David Roe, Yunqing Tang and Jacob Tsimerman for helpful discussions. We are also very grateful to Steven Kleiman and Rahul Singh for answering our questions pertaining to Gorenstein rings. Finally, we thank the referee for useful comments and for helping to improve the exposition of this paper.

2 The canonical lift

Throughout this section (and the paper), p will denote an odd prime. In this section, we will construct the "canonical lift", characterized by property that every endomorphism lifts. Further, this will be the unique (or the two unique) lift(s) to a slightly ramified extension[3] of $W := W(\overline{\mathbb{F}}_p)$. We will first need some preliminary results about the endomorphism rings of almost ordinary abelian varieties.

2.1 Endomorphism rings

Let A denote a simple almost ordinary abelian variety over $\mathbb{F}_q$, and let $\mathscr{G}$ denote its p-divisible group. Let $R = \mathrm{End}(A)$, and let $S = \mathrm{End}(\mathscr{G})$ (note that S is the endomorphism ring of $\mathscr{G}$ over $\mathbb{F}_q$, and not $\overline{\mathbb{F}}_p$). Tate's theorem states that $S = R \otimes_{\mathbb{Z}} \mathbb{Z}_p$. We have the following result:

Proposition 2.1. *The $\mathbb{Z}_p$-algebra S is of the form $S_{\mathrm{et}} \oplus S_{\mathrm{tor}} \oplus S_{\mathrm{ss}}$ according to the decomposition of $\mathscr{G} = \mathscr{G}_{\mathrm{et}} \times \mathscr{G}_{\mathrm{tor}} \times \mathscr{G}_{\mathrm{ss}}$. We have that R is an order inside a CM field of degree $2g$. Consequently, S_{ss} is a 2-dimensional $\mathbb{Z}_p$-algebra. Further, S_{ss} is the maximal order in its field of fractions.*

Proof. As $\mathbb{F}_q$ is a perfect field, every p-divisible group is a product of its étale, toric and local-local components, and so the first assertion follows.

Let π_A denote the Frobenius endomorphism of A. Let $K = \mathbb{Q}(\pi_A)$ and $L = R \otimes \mathbb{Q}$. We will prove that $K = L$ in order to show that S_{ss} is a rank 2 $\mathbb{Z}_p$-algebra. Let $h(x)$ and $f(x)$ denote the characteristic polynomial and minimal polynomial of π_A respectively. As A is simple and almost ordinary, $h(x)$ is either $f(x)$, or $f(x)^2$ according to whether R is commutative or not.

We now show that $f(x) = h(x)$. Indeed, let $f(x) = f_{\mathrm{et}}(x) \cdot f_{\mathrm{tor}}(x) \cdot f_{\mathrm{ss}}(x)$ over $\mathbb{Q}_p$ according to the slope decomposition of A, and similarly let $h = h_{\mathrm{et}} \cdot h_{\mathrm{tor}} \cdot h_{\mathrm{ss}}$ over $\mathbb{Q}_p$. If $h(x) = f(x)^2$, then f_{ss} is a degree one polynomial, and so let π denote its root. This implies that $h_{\mathrm{ss}} = (x - \pi)^2$. On the other hand, the product of the roots of h_{ss} is q, and so $\pi = q/\pi$, which implies that $\pi = \pm q^{1/2}$. However, this implies that the minimal polynomial of the Frobenius of $A \times_{\mathbb{F}_q} \mathbb{F}_{q^2}$ is reducible over $\mathbb{Q}$, which contradicts the assumption that A is geometrically simple. It follows that $h(x) = f(x)$, and therefore that R and S_{ss} are commutative.

It remains to prove that S_{ss} is the maximal order in its field of fractions. Let A' denote an abelian variety over $\mathbb{F}_q$ isogenous to A such that $\mathrm{End}(A')$ is the maximal order in its quotient algebra and denote by $\mathscr{G}'$ its p-divisible group. Let S'_{ss} be the endomorphism ring of $\mathscr{G}'_{\mathrm{ss}}$. Let $i \colon A_0 \to A$ be an isogeny, and let j denote the associated map from $\mathscr{G}_0$ and $\mathscr{G}$. Clearly, j breaks up as $j_{ord} \times j_{\mathrm{ss}}$. It suffices to show that S'_{ss} preserves the kernel of j_{ss}. Indeed, $\mathscr{G}'_{\mathrm{ss}}$ is a connected one-dimensional group, and hence $\mathscr{G}'_{\mathrm{ss}}$ has a unique subgroup of order p^m for every positive integer m. Therefore, it follows that S'_{ss} preserves the kernel of j_{ss} and the result follows. □

[3] See Definition 2.2 for the definition of slightly ramified

2.2 Deuring's theorem

We will now use Grothendieck–Messing theory to prove Deuring's lifting theorem. We note that Deuring's theorem does not generalize to arbitrary p-divisible groups. Indeed, there are many examples of p-divisible groups over $\overline{\mathbb{F}}_p$, which admit endomorphisms which cannot be lifted to characteristic zero (see [12] for examples of abelian varieties over $\overline{\mathbb{F}}_p$ which admit no CM lifts to characteristic zero). Indeed, we believe that given any Newton stratum of $\mathcal{A}_g$ which is neither ordinary nor almost ordinary, there exists a p-divisible group belonging to that Newton stratum which admits an endomorphism which cannot be lifted to characteristic zero. We now define the notion of a "slightly ramified" extension, as Grothendieck–Messing theory does not apply when the degree of ramification is large.

Definition 2.2. *Let L denote a finite extension of $W[1/p]$. We say that L and $\mathcal{O}_L$ are slightly ramified if the degree $[L : W[1/p]]$ is at most $p-1$.*

Proposition 2.3. *Let $\mathscr{G}_{\mathrm{ss}}$ denote a one-dimensional supersingular p-divisible group over $\overline{\mathbb{F}}_p$. Suppose that $\mathcal{O} \subset \mathrm{End}(\mathscr{G}_{\mathrm{ss}})$ is an integrally closed rank two $\mathbb{Z}_p$ algebra. Then:*

1. *If $\mathcal{O}$ is unramified, there exists a unique lift of $\mathscr{G}_{\mathrm{ss}}$ to W such that the action of $\mathcal{O}$ lifts.*
2. *If $\mathcal{O}$ is ramified, then there exist two lifts of $\mathscr{G}_{\mathrm{ss}}$ to $W[\sqrt{p}]$ such that the action of $\mathcal{O}$ lifts.*

In either of the above cases, the lifts described are the only ones to a slightly ramified extension of W such that the action of $\mathcal{O}$ lifts.

Proof. Let $\mathbb{D}$ denote the Dieudonne module of $\mathscr{G}_{\mathrm{ss}}$; $\mathbb{D}$ is a free rank 2 W-module, equipped with a Frobenius-semilinear endomorphism which we denote by F. The module $\mathbb{D}$ has a basis e_1, e_2 such that $Fe_1 = e_2, Fe_2 = pe_1$.

The endomorphisms of $\mathscr{G}_{\mathrm{ss}}$ consist of the W-linear endomorphisms of $\mathbb{D}$ which σ-commute with F. Every such endomorphism is easily seen to be of the form

$$M_{a,b} = \begin{bmatrix} a & p\sigma(b) \\ b & \sigma(a) \end{bmatrix}$$

where $a, b \in W(\mathbb{F}_{p^2})$. For ease of notation, we will identify the matrix $M_{a,b}$ with the endomorphism of $\mathscr{G}_{\mathrm{ss}}$ that it represents. Note that the characteristic polynomial of $M_{a,b}$ is $x^2 - (a + \sigma(a))x + (a\sigma(a) - pb\sigma(b))$.

As $\mathcal{O}$ is a rank-two $\mathbb{Z}_p$ module, it is monogenic as a $\mathbb{Z}_p$-algebra, and so we may assume that $\mathcal{O}$ is generated by a single trace-zero endomorphism. Therefore, there exist a, b such that $\mathcal{O} = \mathbb{Z}_p[M_{a,b}]$, such that $\sigma(a) = -a$. Further, $\mathcal{O}$ is the maximal order in its field of fractions, which is equivalent to $\mathcal{O}$ having square-free discriminant. The discriminant of $\mathcal{O}$ equals the discriminant of the characteristic polynomial of $M_{a,b}$, which is $-4(a\sigma(a) - pb\sigma(b))$ which is squarefree if and only if at least one among a, b is a p-adic unit. Further, $\mathcal{O}$ is unramified if and only if a is a p-adic unit.

Let R denote the ring of integers of some slightly ramified extension of W, and let π denote some choice of uniformizer. As the extension is slightly ramified, the maximal ideal (π) of R is closed under divided powers. The content of Grothendieck–Messing theory (see [10, Section 5, Theorem 1.6]) is: Deformations of $\mathscr{G}_{\mathrm{ss}}$ to R are in bijection with filtrations $\mathrm{Fil} \subset \mathbb{D} \otimes_W R$, which are co-torsion free, and such that Fil mod π equals the kernel of Frobenius on $\mathbb{D}$ mod π. In our setting, the kernel of Frobenius on $\mathbb{D}$ mod p is spanned by e_2. Further, an endomorphism of $\mathscr{G}_{\mathrm{ss}}$ lifts to a deformation if and only if it preserves the filtration associated to the deformation.

We summarize the above discussion. Deformations to R of $\mathscr{G}_{\mathrm{ss}}$ such that the action of $M_{a,b}$ lifts are in bijection with Fil, an R-submodule of $\mathbb{D} \otimes R$ satisfying the following conditions:

- Fil is rank one, and is co-torsion free.
- Fil mod π equals the span of e_2.
- the action of $M_{a,b}$ on $\mathbb{D}$ preserves Fil.

We will now show that there is a unique choice of Fil if a is a p-adic unit, and that there are exactly two choices of Fil otherwise. Indeed, the data of Fil is the same as the data of an eigenvector of $M_{a,b}$ of the form $e_2 + \lambda e_1$, where λ is in the maximal ideal of R.

Having fixed a, b, a vector of the form $e_2 + e_1\lambda$ is an eigen vector of $M_{a,b}$ if and only if λ satisfies the quadratic equation

$$b\lambda^2 + (\sigma(a) - a)\lambda - p\sigma(b) = 0. \tag{1}$$

Note that this already proves for us the statement that there are at most two deformations of $\mathscr{G}_{\mathrm{ss}}$ to a slightly ramified extension of W, such that the action of $M_{a,b}$ also lifts. We will now treat the following two cases to finish the proof of this lemma:

Case 1: a is a p-adic unit. We must prove that there is a unique λ with positive p-adic valuation that satisfies (1), and that this solution lies in W. Indeed, the newton polygon of (1) has a breakpoint, and so equals a product of linear factors, thereby proving that any λ is an element of W. Further, the product of the two roots has p-adic valuation 1, and the sum of the two roots (which equals $\frac{a-\sigma(a)}{b}$) has p-adic valuation non-positive. This is because $\sigma(a) = -a$, and a is a unit. Therefore, exactly one of the two solutions to (1) has positive p-adic valuation, as required.

Case 2: a is not a p-adic unit. Recall that b has to be a p-adic unit in this case. It follows that the discriminant of (1) has p-adic valuation one, and so must be an irreducible polynomial over W, and thus the two roots have the same p-adic valuation. As the product of the roots has p-adic valuation 1, each of the two roots must have p-adic valuation 1/2, and so must be defined over $W[\sqrt{p}]$. The lemma follows. □

2.3 Definition of the canonical lift(s)

We will now define the canonical lift(s) of our abelian variety.

Definition 2.4. *Let $\tilde{\mathscr{G}}_{\text{ss}}$ denote the lift(s) of $\mathscr{G}_{\text{ss}}$ constructed in Proposition 2.3. We define the canonical lift(s) $\mathscr{G}_{can}$ of $\mathscr{G}$ to be $\tilde{\mathscr{G}}_{\text{ss}} \times \tilde{\mathscr{G}}_{\text{et}} \times \tilde{\mathscr{G}}_{\text{tor}}$. We define the canonical lift(s) of A to be the abelian variety corresponding to $\mathscr{G}_{can}$ via the Serre-Tate lifting equivalence* [4].

Proposition 2.5. *The canonical lift has the property that all the endomorphisms of A lift.*

Proof. It suffices to show that all the $\mathbb{F}_q$-endomorphisms of $\mathscr{G}$ lift to $\mathscr{G}_{can}$. Recall that $\text{End}_{\mathbb{F}_q}(\mathscr{G}) = S_{\text{et}} \oplus S_{\text{tor}} \oplus S_{\text{ss}}$. By construction, the action of S_{ss} lifts to $\mathscr{G}_{can}$. It suffices to show that the actions of S_{et} and S_{tor} also lift. This follows, because $\tilde{\mathscr{G}}_{\text{et}} \times \tilde{\mathscr{G}}_{\text{tor}}$ is the canonical lift of $\mathscr{G}_{\text{et}} \times \mathscr{G}_{\text{tor}}$, and the canonical lift of an ordinary p-divisible group is characterized by the property that every endomorphism lifts. □

3 Classification

For this section, fix an odd prime p and $q = p^a$.

A remarkable application of the Serre-Tate canonical lift for ordinary abelian varieties was given by Deligne where he provides a classification of ordinary abelian varieties over finite fields in terms of a certain category of $\mathbb{Z}$-modules. More precisely, if $A/\mathbb{F}_q$ is an ordinary abelian variety, let $\tilde{A}/W(\mathbb{F}_q)$ denote its canonical lift. Fixing an embedding $\iota \colon W(\mathbb{F}_q) \hookrightarrow \mathbb{C}$, Deligne considers the integral homology $T := H_1(\tilde{A} \otimes_\iota \mathbb{C}, \mathbb{Z})$. The Frobenius endomorphism of A over $\mathbb{F}_q$ lifts to an endomorphism of $\tilde{A}$ and thus defines an endomorphism $F \in \text{End}_{\mathbb{Z}}(T)$. Deligne then shows that the association that takes $A/\mathbb{F}_q$ to the pair (T, F) gives an equivalence of categories between ordinary abelian varieties over $\mathbb{F}_q$ of dimension g and the category of pairs (T, F) where T is a free $\mathbb{Z}$-module of rank $2g$ and $F \in \text{End}_{\mathbb{Z}}(T)$ satisfies the following three conditions:

1. $F \otimes \mathbb{Q}$ acts semisimply on $T \otimes \mathbb{Q}$.
2. There exists $V \in \text{End}_{\mathbb{Z}}(T)$ such that $F \circ V = q = V \circ F$.
3. The characteristic polynomial $h(x) \in \mathbb{Z}[x]$ of F is a Weil q-polynomial (i.e. all its roots are Weil q-integers) such that $h(x)$ has at least g roots (counting multiplicities) in $\overline{\mathbb{Q}}_p$ that are p-adic units.

Our goal in this section is to provide a similar classification for simple almost ordinary abelian varieties over $\mathbb{F}_q$ using our canonical lift(s) defined above.

Suppose $A/\mathbb{F}_q$ is a *simple* almost ordinary abelian variety of dimension g. Fix an embedding $\epsilon \colon W(\overline{\mathbb{F}}_q)[\sqrt{p}] \hookrightarrow \mathbb{C}$. Let $\tilde{A}$ be one of the possibly two canonical lifts of A over a ramified quadratic extension of $W(\mathbb{F}_q)$ and consider $T(A) := H_1(\tilde{A} \otimes_\epsilon \mathbb{C}, \mathbb{Z})$, a free $\mathbb{Z}$-module of rank $2g$. The Frobenius endomorphism of A over $\mathbb{F}_q$ lifts to an endomorphism of $\tilde{A}$ and thus defines an $F(A) \in \text{End}_{\mathbb{Z}}(T(A))$. We associate the pair $(T(A), F(A))$ to A. Note that if $\mathcal{G}$ is the p-divisible group of A and if $\text{End}(\mathcal{G}_{\text{ss}})$ is ramified over $\mathbb{Z}_p$, then A has two canonical lifts over $W(\overline{\mathbb{F}}_q)[\sqrt{p}]$ and to each such canonical lift

[4] See [5] for a proof of the lifting equivalence due to Drinfel'd

we associate a pair (T, F). As in the ordinary case, 1. and 2. above are satisfied. However, we shall see that 3. is replaced by

3* The characteristic polynomial $h(x) \in \mathbb{Z}[x]$ of F is a Weil q-polynomial which is irreducible over $\mathbb{Q}$, and has $g-1$ roots in $\overline{\mathbb{Q}}_p$ that are p-adic units, $g-1$ roots with q-adic valuation 1 and 2 roots with q-adic valuation $1/2$. Thus, we have a factorisation in $\mathbb{Z}_p[x]$

$$h(x) = h_0(x) \cdot h_1(x) \cdot h_{1/2}(x)$$

where $h_i(x)$ has all its roots in $\overline{\mathbb{Q}}_p$ with q-adic valuation i. Moreover, $h_{1/2}(x)$ must be irreducible over $\mathbb{Q}_p$ and does not have $\pm\sqrt{q}$ as a root.

(Indeed, if $h_{1/2}(x)$ has two distinct roots in $\mathbb{Q}_p$ then the supersingular part of the p-divisible group of A has endomorphism algebra $\mathbb{Q}_p \times \mathbb{Q}_p$ which is not possible. If a is even, $\pm\sqrt{q}$ cannot be a root since otherwise A would have as an isogeny factor a supersingular elliptic curve with all its endomorphisms defined over $\mathbb{F}_q$. Similarly, if a is odd and if $\pm\sqrt{q}$ is a root of $h(x)$ then this would imply that $(x^2-q)^2$ divides $h(x)$ contradicting that A is almost ordinary.

The assumption that A is almost ordinary and simple implies that $h(x)$ is irreducible over $\mathbb{Q}$. Indeed, the simplicity of A yields that $h(x)$ is a power of a $\mathbb{Q}$-irreducible polynomial P, say $h(x) = P(x)^e$. We may compute e as in [14, p. 527]. Factor $P(x) = \prod P_\nu(x)$ into irreducible factors in $\mathbb{Q}_p[x]$. Since P has no real roots, e is the least common denominator of the $i_\nu := \frac{\mathrm{ord}_p P_\nu(0)}{a}$. Note that $h_{1/2}$ occurs as one of the P_ν, and $\frac{\mathrm{ord}_p(h_{1/2}(0))}{a} = 1$. The other P_ν, divide either h_0 or h_1. If P_ν divides h_0 then all the roots of P_ν are p-adic units and hence $i_\nu = 0$, and if P_ν divides h_1 then all the roots of P_ν have p-adic valuation a. In all cases, i_ν is an integer and hence $e = 1$, implying the irreducibility of $h(x)$ over $\mathbb{Q}$.)

Note that under the assumptions 1, 2 and 3* on the pair $(T(A), F(A))$ we have a decomposition

$$T(A) \otimes \mathbb{Z}_p = T_0 \oplus T_1 \oplus T_{1/2}$$

where $T_i := \mathrm{Ker}(h_i(F))$. Thus, $T_{1/2}$ is a rank 1 module over $\mathbb{Z}_p[x]/h_{1/2}(x)$. In fact, it follows from Proposition 2.1 that

4* $T_{1/2}$ has endomorphisms by the *maximal* order $\mathcal{O}_{\mathrm{ss}}$ of $K_{\mathrm{ss}} := \mathbb{Q}_p[x]/\langle h_{1/2}(x)\rangle$.

Definition 3.1.

1. *A pair (T, F) satisfying the four conditions 1, 2, 3* and 4* is said to be an almost ordinary Deligne module with Frobenius polynomial h.*

2. *A morphism of almost ordinary Deligne modules $\phi\colon (T, F) \to (T', F')$ is simply a morphism $\phi\colon T \to T'$ of $\mathbb{Z}$-modules such that $\phi \circ F = F' \circ \phi$*

3. *An isogeny of almost ordinary Deligne modules is a morphism $\phi\colon (T, F) \to (T', F')$ such that $\phi \otimes \mathbb{Q}\colon T \otimes \mathbb{Q} \to T' \otimes \mathbb{Q}$ is an isomorphism. Since we primarily deal with* simple *abelian varieties and Deligne modules, an isogeny is then just a non-zero morphism.*

4. *For a polynomial $h(x) \in \mathbb{Z}[x]$ satisfying 3*, we denote by $\mathcal{L}_h$ the category of almost ordinary Deligne modules with Frobenius polynomial h. Similarly, we define $\mathcal{C}_h$ as the category of simple almost ordinary abelian varieties over $\mathbb{F}_q$ with Frobenius polynomial h.*

5. *We say that $\mathcal{L}_h$ or $\mathcal{C}_h$ (or an object of either category) is ramified (resp. inert) when K_{ss} is a ramified (resp. unramified) quadratic extension of $\mathbb{Q}_p$.*

Thus, in case that $A \in \mathcal{C}_h$ is ramified, we obtain two almost ordinary Deligne modules $\mathfrak{T}_1(A), \mathfrak{T}_2(A)$ in $\mathcal{L}_h$ using the two possible canonical lifts of A.

Proposition 3.2. *Every almost ordinary Deligne module $(T, F) \in \mathcal{L}_h$ arises (up to isomorphism) from a simple almost ordinary abelian variety over $\mathbb{F}_q$*

Proof. By Honda–Tate theory we may find a simple almost ordinary abelian variety A over $\mathbb{F}_q$ such that the characteristic polynomial of the Frobenius π_A (relative to $\mathbb{F}_q$) is $h(x)$. Thus, we see that $(T(A) \otimes \mathbb{Q}, \pi_A) \cong (T \otimes \mathbb{Q}, F)$.

By making the above identification we have that $T \subset (T(A) \otimes \mathbb{Q}, \pi_A)$ is a π_A-stable lattice of full rank. We aim to find an almost abelian variety B isogenous to A, such that $(T(B), \pi_B) \cong (T, \pi_A)$. For this, we may assume that $T(A) \subseteq T$. Then $T/T(A)$ defines a finite subgroup $H \subseteq \tilde{A} \otimes_\epsilon \mathbb{C}$, stable under the lift to characteristic 0 of the Frobenius π_A of A. If the order of H is coprime to p then H defines a subgroup scheme of $\tilde{A}$. If $\overline{H} \subset A$ denotes the subgroup scheme obtained by reducing modulo p we see that $\tilde{A}/H$ is a canonical lift of $A/\overline{H}$ and moreover, $H_1(\tilde{A}/H \otimes_\epsilon \mathbb{C}, \mathbb{Z}) = T$. On the other hand, let $H = T/T(A)$ be a p-group. Then, corresponding to the decomposition $T \otimes \mathbb{Z}_p = T_0 \oplus T_1 \oplus T_{1/2}$ we have a decomposition of $H \otimes \mathbb{Z}_p = H_0 \oplus H_1 \oplus H_{1/2}$. Moreover, H_0 lifts uniquely an étale subgroup $\overline{H}_0 \subset A$, and similarly H_1 lifts $\overline{H}_1$ in the toric part of the p-divisible group of A. For the group $H_{1/2} = T_{1/2}/T(A)_{1/2}$, we note that since both $T_{1/2}$ and $T(A)_{1/2}$ admit endomorphisms by the maximal order $\mathcal{O}_{\mathrm{ss}} \subseteq \mathbb{Q}_p[x]/h_{1/2}(x)$, we must have that $T(A)_{1/2} = \varpi^n T_{1/2}$ where $\varpi \in \mathcal{O}_{\mathrm{ss}}$ is a uniformizer. Thus, $H_{1/2}$ lifts the supersingular part of the kernel of the isogeny given by ϖ^n on A. Hence, H lifts a unique subgroup $\overline{H} \subset A$, such that $\tilde{A}/H$ is a canonical lift of $B := A/\overline{H}$. Moreover, it is clear that $(T(B), \pi_B) = (T, \pi_A)$. □

3.1 Inert isogeny classes

Let $\alpha \in \mathrm{End}(A)$, where A is some inert simple almost ordinary abelian variety. Let $\alpha_{\mathrm{ss}} \in \mathcal{O}_{\mathrm{ss}}$ denote the restriction of α to the local-local part of $A[p^\infty]$. It is easy to see that the order of $\ker(\alpha_{\mathrm{ss}})$ equals $\mathrm{Norm}(\alpha_{\mathrm{ss}})$, and as $\mathcal{O}_{\mathrm{ss}}[1/p]$ is an unramified extension of $\mathbb{Q}_p$, it follows that the order has to be an *even* power of p. Motivated by this, given an inert isogeny class $\mathcal{C}_h$, we define the following equivalence relation on its set of objects $\mathrm{Ob}(\mathcal{C}_h)$. For $A, B \in \mathrm{Ob}(\mathcal{C}_h)$ we say that $A \sim B$ when some (hence *every*) $\mathbb{F}_q$-isogeny $f \colon A \to B$ is such that if $f[p^\infty] \colon A[p^\infty] \to B[p^\infty]$ denotes the induced map of p-divisible groups then $\ker(f[p^\infty])_{\mathrm{ss}}$ has order p^r for an *even* integer r. The equivalence relation partitions the objects of $\mathcal{C}_h$ into two equivalence classes and we let $\mathcal{C}_{1,h}$ and $\mathcal{C}_{2,h}$ denote the two full subcategories of $\mathcal{C}_h$ having objects of each equivalence class. Thus $\mathrm{Ob}(\mathcal{C}_h) = \mathrm{Ob}(\mathcal{C}_{1,h}) \cup \mathrm{Ob}(\mathcal{C}_{2,h})$. We claim that:

Proposition 3.3. *Restricted to each equivalence class $\mathcal{C}_{i,h}$ the association $A \mapsto \mathfrak{T}_i(A) \colon = (T(A), F(A))$ is functorial for $A \in \mathcal{C}_{i,h}$ and moreover induces an equivalence of categories*

$$\mathfrak{T}_i \colon \mathcal{C}_{i,h} \to \mathcal{L}_h.$$

Proof. The p-divisible group $A[p^\infty]_{\text{ss}}$ has a unique subgroup of order p^n for every n. Therefore, any subgroup of order p^{2m} must necessarily be the p^m-torsion of $A[p^\infty]_{\text{ss}}$. Let $f\colon A \to B$ be an $\mathbb{F}_q$-isogeny for $A, B \in \mathcal{C}_{i,h}$. Since $\ker(f[p^\infty])_{\text{ss}}$ is of order p^{2m} for $m \in \mathbb{Z}$, $f[p^\infty]$ lifts uniquely to a morphism of the lifts of the p-divisible groups $\widetilde{f[p^\infty]}\colon \widetilde{A}[p^\infty] \to \widetilde{B}[p^\infty]$ and hence to a morphism between the canonical lifts $\widetilde{f}\colon \widetilde{A} \to \widetilde{B}$. Thus, we obtain a morphism of integral homologies $\mathfrak{T}_i(A) \to \mathfrak{T}_i(B)$. It follows easily that $\mathfrak{T}_i$ is a functor.

The fact that each $\mathfrak{T}_i$ is essentially surjective follows from the proof of Proposition 3.2. We simply note that in the proof we may as well have started with an $A \in \mathcal{C}_{i,h}$ such that $(T(A) \otimes \mathbb{Q}, \pi_A) \cong (T \otimes \mathbb{Q}, F)$. Then it suffices to see that the $B = A/\overline{H}$ obtained at the end of the earlier proof belongs to the same equivalence class as A, since the order of $\overline{H}[p^\infty]_{\text{ss}}$ is indeed a square when p is inert in $\mathcal{O}_{\text{ss}}$.

It remains to show that $\mathfrak{T}_i$ is fully-faithful, i.e. for $A, B \in \mathcal{C}_{i,h}$ we show that the natural map $\operatorname{Hom}_{\mathbb{F}_q}(A, B) \to \operatorname{Hom}_{\mathcal{L}_h}(\mathfrak{T}_i(A), \mathfrak{T}_i(B))$ is a bijection. The injectivity of this map is clear. Indeed, different isogenies between A and B lift to different isogenies between $\tilde{A}$ and $\tilde{B}$, and different maps between $\tilde{A}$ and $\tilde{B}$ induce different maps between $T(B)$ and $T(C)$.

To show that an isogeny $g\colon T(A) \to T(B)$ is in the image, it suffices to show that $n \cdot g$ is in the image, for some integer n. Indeed, if $u\colon A \to B$ is an $\mathbb{F}_q$-isogeny such that $\mathfrak{T}_i(u)$ is divisible by n, then this means that $\tilde{u} \otimes_\epsilon \mathbb{C}$ is divisible by n, and hence $\tilde{u}$ is divisible by n over the generic point of $W(\mathbb{F}_q)$. Since the kernel of n is flat over W we get that $\tilde{u}$ and hence u is divisible by n.

Let $\phi\colon A \to B$ be an $\mathbb{F}_q$-isogeny. Note that $\mathfrak{T}_i(\phi)$ and g being isogenies give rise to isomorphisms $\mathfrak{T}_i(\phi)\colon T(A) \otimes \mathbb{Q} \xrightarrow{\cong} T(B) \otimes \mathbb{Q}$ and $g\colon T(A) \otimes \mathbb{Q} \xrightarrow{\cong} T(B) \otimes \mathbb{Q}$. Since we're free to replace g with $n \cdot g$, we may assume that $\mathfrak{T}_i(\phi)^{-1} \circ g\,(T(A)) \subseteq T(A)$. However, we recall that as A is assumed to be simple, $T(A) \otimes \mathbb{Q}$ is a dimension 1 vector space over the field $K\colon = \operatorname{End}^0(A)$, and thus $\mathfrak{T}_i(\phi)^{-1} \circ g$ is an element of $\lambda \in K$. By scaling g further by an integer n we may even assume $\lambda \in \operatorname{End}_{\mathbb{F}_q}(A)$. Thus, $g = \mathfrak{T}_i(\phi) \circ \mathfrak{T}_i(\lambda) = \mathfrak{T}_i(\phi \circ \lambda)$ as desired. □

Proposition 3.3 implies that there is a 2-1 map from $\mathcal{C}_h$ to $\mathcal{L}_h$. In particular, given any Deligne module, there exist two almost ordinary abelian varieties corresponding to it, and also two complex Abelian varieties with the same H_1 corresponding to the Deligne module. This non-uniqueness is explained by the fact that there are two different CM types on the algebra of endomorphisms associated to $\mathcal{C}_h$, and choosing one of these two different CM types is the same as choosing one of the two different equivalence classes in $\mathcal{C}_h$.

3.2 Ramified isogeny classes

In the case of ramified isogeny classes, there is no canonical way to associate to A a module T, because of the existence of two canonical lifts. However, as we will show, fixing a choice of canonical lift of some one almost ordinary abelian variety fixes a choice of canonical lift for every other abelian variety in the same isogeny class. Indeed, choosing one canonical lift over the other is equivalent to choosing one amongst the two possible CM types on the endomorphism algebra of the ramified isogeny class. To that end, fix a ramified $\mathbb{F}_q$-isogeny class $\mathcal{C}_h$, along with an abelian variety $A \in \mathcal{C}_h$ defined over $\mathbb{F}_q$. We define $\tilde{A}$ to be one of the two canonical lifts of A. For the rest of this section, we will call $\tilde{A}$ *the* canonical lift of A.

Proposition 3.4. *Let $G \subset A$ denote any finite flat subgroup defined over $\mathbb{F}_q$. There is then a canonical subgroup $\tilde{G} \subset \tilde{A}$ lifting G.*

Proof. If G is of the form $G_1 \times G_2$, it suffices to prove this result for both G_1 and G_2. Further, this result is tautologically true for prime-to-p subgroups of A. Therefore, we may assume that G has order a power of p. Further, we may assume that G is either étale, or multiplicative, or local-local. By the definition of the canonical lift, étale and multiplicative subgroups lift uniquely so it suffices to prove that every local-local finite flat subgroup of A lifts uniquely to $\tilde{A}$.

Therefore, let $G \subset A$ be a finite flat subgroup which is local-local. Further, let $A[p^\infty] = \mathscr{G}_{\text{et}} \times \mathscr{G}_{\text{tor}} \times \mathscr{G}_{\text{ss}}$. Then, $G \subset \mathscr{G}_{\text{ss}}$. Further, we defined the canonical lift of A to correspond to the product of the canonical lifts $\tilde{\mathscr{G}}_?$ of $\mathscr{G}_?$ where ? stands for either et, tor or s. Therefore, it suffices to prove that $G \subset \mathscr{G}_{\text{ss}}$ lifts to a subgroup $\tilde{G} \subset \tilde{\mathscr{G}}_{\text{ss}}$.

It is easy to see that $\mathscr{G}_{\text{ss}}$ has a unique order p^n subgroup for each n. In fact, as we are dealing with the ramified case, this subgroup equals the ϖ^n-torsion of $\mathscr{G}_{\text{ss}}$, where ϖ is the uniformizing parameter for $\operatorname{End}_{\mathbb{F}_q}(\mathscr{G}_{\text{ss}})$. Therefore, we may assume that $G = \mathscr{G}_{\text{ss}}[\varpi^n]$. As our canonical lift $\tilde{\mathscr{G}}_{\text{ss}}$ has the property that every endomorphism of $\mathscr{G}_{\text{ss}}$ lifts of $\tilde{\mathscr{G}}_{\text{ss}}$, it follows that the action of $\mathbb{Z}_p[\varpi]$ also lifts to $\tilde{\mathscr{G}}_{\text{ss}}$. It now follows that the ϖ^n torsion of $\tilde{\mathscr{G}}_{\text{ss}}$ is the required lift of G. □

Definition 3.5.

1. *Let $G \subset A$ be some finite flat subgroup. We define $\tilde{G} \subset \tilde{A}$ to be the (canonical) lift of G defined in Proposition 3.4.*
2. *Let B be an abelian variety isogenous to A, with $\phi\colon A \to B$ an isogeny with kernel G. Define $\tilde{B}$ to be the lift of B given by $\tilde{A}/\tilde{G}$.*

Proposition 3.6. *The lift $\tilde{B}$ is a canonical lift of B, and doesn't depend on the choice of the isogeny ϕ.*

Proof. That the lift is a canonical lift can be checked on the level of p-divisible groups. By construction, the p-divisible group $\tilde{B}[p^\infty]$ is a product of the lifts of the étale, multiplicative, and local-local parts of the p-divisible group $B[p^\infty]$. Further, the action of $\mathbb{Z}_p[\varpi]$ preserves $\tilde{G}$ by construction, and so continues to act on $\tilde{B}[p^\infty]$. This proves that $\tilde{B}$ is a canonical lift of B.

In order to prove that this lift is independent of ϕ and G, suppose that ϕ_1, ϕ_2 are two isogenies between A and B, whose kernels are G_1 and G_2. Define $\tilde{B}_i$ to be the lifts of B which equal $\tilde{A}/\tilde{G}_i$ for $i = 1, 2$. By replacing ϕ_2 with an integer scalar multiple, we may assume that ϕ_2 factors through ϕ_1. Therefore, there exists an endomorphism $\alpha \in \operatorname{End}(B)$ such that $\phi_2 = \alpha \circ \phi_1$. But now, the proposition follows from the fact that every endomorphism of B lifts to an endomorphism of $\tilde{B}_1$. □

Proposition 3.7. *Every $\mathbb{F}_q$-isogeny $\phi\colon B \to C$ lifts uniquely to an isogeny $\tilde{\phi}\colon \tilde{B} \to \tilde{C}$ where $\tilde{B}, \tilde{C}$ are the lifts provided by Proposition 3.6. Thus, the association of $B \mapsto \tilde{B}$ defines a functor from the $\mathbb{F}_q$-isogeny class $\mathcal{C}_h$ of A to the collection of lifts.*

Proof. Let $\psi\colon A \to B$ be an $\mathbb{F}_q$-isogeny. Let $G\colon = \ker(\psi)$ and $H\colon = \ker(\phi \circ \psi) \supseteq G$. Clearly, $\tilde{G} \subseteq \tilde{H}$ and moreover the lift $\tilde{\phi}$ corresponds to the natural isogeny $\tilde{B} = \tilde{A}/\tilde{G} \to \tilde{A}/\tilde{H} = \tilde{C}$. The fact that this is functorial is also clear. □

Therefore, given an $\mathbb{F}_q$-isogeny $\phi\colon B \to C$ (where B, C are abelian varieties in the isogeny class $\mathcal{C}_h$ of A) we get a map $\mathfrak{T}(\phi)\colon (T(B), \pi_B) \to (T(C), \pi_C)$. (Here $T(B)$ refers to $H_1(\tilde{B} \otimes_\epsilon \mathbb{C}, \mathbb{Z})$ for $\tilde{B}$ being the particular lift defined above.) This defines a functor $\mathfrak{T}\colon \mathcal{C}_h \to \mathcal{L}_h$.

Proposition 3.8. *The functor*

$$\mathfrak{T}\colon \mathcal{C}_h \to \mathcal{L}_h$$

is an equivalence of categories.

Proof. By Proposition 3.2, this functor is essentially surjective. That $\mathfrak{T}$ is fully-faithful follows from an argument almost identical to that of Proposition 3.3. □

This completes the proof of the classification Theorem 1.1 stated in the Introduction.

4 Polarizations

Throughout this section, we fix an isogeny class $\mathcal{C}_h$ of almost ordinary abelian varieties over $\mathbb{F}_q$ with Frobenius polynomial h. In the case that $\mathcal{C}_h$ is ramified we also fix at once a compatible choice of canonical lifts for all the varieties in $\mathcal{C}_h$ as was done in Section 3.2. Henceforth, we will refer to this choice of canonical lift as *the* canonical lift for any $A \in \mathcal{C}_h$. We note that an $\mathbb{F}_q$-isogeny $\phi\colon A \to B$ induces an isomorphism of fields $\mathrm{End}^0(A) \cong \mathrm{End}^0(B)$. After identifying these fields we denote the common endomorphism algebra by K. Finally, as we have fixed an embedding of $W(\overline{\mathbb{F}}_p)[\sqrt{p}]$ in $\mathbb{C}$, every $A \in \mathcal{C}_h$ gives rise to a complex abelian variety with CM by the field K, and in the ramified case the compatible choice of lifts amounts to a compatible CM type Φ of the common endomorphism algebra K.

Proposition 4.1. *Let A be an inert almost ordinary abelian variety over $\mathbb{F}_q$, and let $A^\vee$ denote its dual. Then $A^\vee$ is in the same equivalence class as A.*

Proof. Whether or not two isogenous abelian varieties are in the same equivalence class doesn't depend on the field of definition. Therefore we may replace $\mathbb{F}_q$ with a finite extension, and assume the existence of a principally polarized B isogenous to A. Let $\lambda B \to B^\vee$ denote a principal polarization. Let $\phi\colon A \to B$ denote an isogeny, and let $\phi^\vee\colon B^\vee \to A^\vee$ denote its dual. Then, the map $\lambda' = \phi^\vee \circ \lambda \circ \phi\colon A \to A^\vee$ is an isogeny from A to its dual (in fact, a polarization). Further, the finite flat group schemes $\ker(\phi) \cap A[p^\infty]_{\mathrm{ss}}$ and $\ker(\phi^\vee) \cap A^\vee[p^\infty]_{\mathrm{ss}}$ have the same cardinality, and so $\ker(\lambda') \cap A[p^\infty]_{\mathrm{ss}}$ has cardinality a perfect square. Therefore, A and $A^\vee$ are in the same equivalence class. □

We now no longer assume that A is inert.

Proposition 4.2. *The canonical lift of $A^\vee$ is the dual of the canonical lift of A.*

Proof. Let $\tilde{A}$ denote the canonical lift of A. Consider $(\tilde{A})^\vee$, the dual of $\tilde{A}$ – its special fiber is the dual of A, and hence $(\tilde{A})^\vee$ is a lift of $A^\vee$. $(\tilde{A})^\vee$ has the same endomorphism ring as the canonical lift of $\tilde{A}$, and hence $A^\vee$. Therefore it follows that $\tilde{A}^\vee$ is the canonical lift of $A^\vee$ as required. □

Definition 4.3. *Suppose $(T, F) \in \mathcal{L}_h$ is an almost ordinary Deligne module. Then we define the* dual *module following [6] as $(T, F)^\vee = (T^\vee, F^\vee)$ where $T^\vee$ is the $\mathbb{Z}$-module* $\mathrm{Hom}_{\mathbb{Z}}(T, \mathbb{Z})$ *and $F^\vee$ is the endomorphism of $T^\vee$ such that $(F^\vee \psi)(t) = \psi(Vt)$, for all $\psi \in T^\vee$ and $t \in T$.*

It is easy to see that the dual pair $(T, F)^\vee$ is indeed an almost ordinary Deligne module with the same Frobenius polynomial h, and that $^\vee\colon \mathcal{L}_h \to \mathcal{L}_h$ defines a functor. We also remark that a complex structure on $T \otimes \mathbb{R}$ determines the natural complex structure on $T^\vee \otimes \mathbb{R} = \mathrm{Hom}_{\mathbb{R}}(T \otimes \mathbb{R}, \mathbb{R})$ given by $(z \cdot f)(t) = f(\overline{z} \cdot t)$ for $f \in T^\vee \otimes \mathbb{R}$, $t \in T \otimes \mathbb{R}$ and $z \in \mathbb{C}$. In this manner, the g-many complex eigenvalues of $F \otimes \mathbb{R}$ and $F^\vee \otimes \mathbb{R}$ are the same.

Proposition 4.4. *Suppose $A^\vee$ denotes the (almost ordinary) abelian variety over $\mathbb{F}_q$ dual to A. Then, $(T(A^\vee), \pi_{A^\vee})$ is the dual of the pair $(T(A), \pi_A)$ defined above.*

Proof. The same argument as in [6, Proposition 4.5]. □

Let $\pi \in K$ denote the Frobenius of the isogeny class $\mathcal{C}_h$, and let $R \subseteq K$ be the smallest order containing $\mathbb{Z}[\pi, q/\pi]$ such that $R \otimes \mathbb{Z}_p$ contains $\mathcal{O}_{\mathrm{ss}}$. For an almost ordinary Deligne module $(T, F) \in \mathcal{L}_h$ we may view the isomorphism class of T as an R-fractional ideal $I \subset K$. In fact, it is clear that the isomorphism classes of objects of $\mathcal{L}_h$ are in bijection with the ideal class monoid $\mathrm{ICM}(R)$ of the order R. As in [9, §4, 5] we rephrase our results in these terms:

Theorem 4.5. *For a simple almost ordinary abelian variety $A \in \mathcal{C}_h$, let $I_A \subset K$ denote the associated fractional ideal. Then:*

1. *the dual variety $A^\vee$ corresponds to the fractional ideal $\overline{I}_A^t$ - the CM-conjugate of the trace-dual to I_A.*
2. $\mathrm{End}_{\mathbb{F}_q}(A)$ *is the ring $[I_A : I_A] = \{\lambda \in K : \lambda \cdot I_A \subseteq I_A\}$.*
3. (a) *There is a bijection between the $\mathbb{F}_q$-isomorphism classes of varieties in $\mathcal{C}_h$ ($\mathcal{C}_{i,h}$ in the inert case) and the ideal class monoid ICM(R)*
   (b) *R is a Gorenstein order*[5] *and thus there is a bijection between the $\mathbb{F}_q$-isomorphism classes of varieties in $\mathcal{C}_h$ ($\mathcal{C}_{i,h}$ in the inert case) having endomorphism ring exactly R and the ideal class group $\mathcal{C}\ell(R)$.*
4. *The data of a polarization on A is the same as a $\lambda \in K^\times$ such that:*
   - *the bilinear form on K defined by $(x, y)_\lambda := \mathrm{Trace}_{K/\mathbb{Q}}(\lambda x \bar{y})$ is integral on I_A.*

[5] By [7], it suffices to check that $R \otimes \mathbb{Z}_\ell$ is Gorenstein for every prime ℓ. For every $\ell \neq p$, the order is monogenic and hence Gorenstein. For $\ell = p$, it is easy to see that the local order is a direct sum of monogenic rings, and hence is Gorenstein.

- *λ is purely imaginary*
- *$\phi(\lambda)/i$ is a positive real number, for $\phi \in \Phi$*

The polarization corresponding to such a λ is principal if and only if the lattice I_A is self-dual for the bilinear form $(\ ,\ )_\lambda$.

5. *Two pairs (I, λ) and (I', λ') give rise to isomorphic polarized varieties if and only if there exists $\nu \in K^\times$ such that $I' = \nu I$ and $\lambda = \nu\bar{\nu}\lambda'$.*

Proof. It only remains to prove the last facts regarding polarizations. We will prove that the set of all polarizations on $\tilde{A}$ is the same as the set of all polarizations on A. The proposition follows from this statement. Indeed, a polarization on $\tilde{A}_{\mathbb{C}}$ is the same as a Riemann form on $T(A) = H_1(\tilde{A}_{\mathbb{C}}(\mathbb{C}), \mathbb{Z})$, and is principal if and only if the associated form is self-dual on $T(A)$. A Riemann form on $T(A)$ is the same data as in the statement of this proposition (see [11, Example 2.9]).

Therefore, it suffices to prove that the set of all polarizations on $\tilde{A}$ is the same as the set of all polarizations on A. By Proposition 4.2, $\widetilde{A^\vee} = (\tilde{A})^\vee$, and we further have that $\mathrm{Hom}(\tilde{A}, \widetilde{A^\vee}) = \mathrm{Hom}(A, A^\vee)$ (this follows from Proposition 3.7 in the ramified case, and Proposition 4.1 in the inert case). Finally, an element $\alpha \in \mathrm{Hom}(A, A^\vee)$ is a polarization on A if and only if it is a polarization of $\tilde{A}$. □

5 Size of isogeny classes

Let A denote a simple g-dimensional almost ordinary abelian variety over $\mathbb{F}_q$, where $g \geq 2$. We recall the following definition:

Definition 5.1. *Define $I(A, q^n)$ to be the set of principally polarized abelian varieties over $\mathbb{F}_{q^n}$ isogenous to A.*

The goal of this section is to prove Theorem 1.2, which we recall for the convenience of the reader.

Theorem 5.2. *Suppose that the Frobenius torus of A has full rank. Then we have the lower bound $I(A, q^n) \geq q^{n[g(g+1)/2-1+o(1)]/2}$ for a positive density set of n.*

We expect that the Frobenius torus condition is unnecessary, and also that the lower bound is actually an equality. Further, this condition is equivalent to the same multiplicative independence condition that appears in the statement of [13, Proposition 3.6]. We thank Yunqing Tang for pointing this out to us. As remarked earlier, proving that the lower bound is an equality would involve estimating the number of orders containing R_n, something which appears out of reach.

Let α denote a Weil q integer corresponding to the isogeny class containing A. Let R_n denote the smallest order inside $K = \mathbb{Q}(\alpha)$ containing $\alpha^n, q^n/\alpha^n$ and such that $R_n \otimes \mathbb{Z}_p$ contains $\mathcal{O}_{\mathrm{ss}}$. We have proved that the set of abelian varieties over $\mathbb{F}_{q^n}$ isogenous to A is in bijection with (or admits a 2-1 map onto) the set of equivalence classes of finitely generated R_n submodules of $\mathbb{Q}(\alpha)$.

Let R_n^+ denote the ring $\mathbb{Z}[\alpha^n + q^n/\alpha^n]$. The following proposition is the analogue of Proposition 3.4 in [13]:

Proposition 5.3. *The subset of $I(A, q^n)$ with endomorphism ring exactly equal to R_n is either empty, or admits a bijective[6] / two-one[7] map onto the kernel of the norm map*

$$N \colon \mathcal{C}\ell(R_n) \to \mathcal{C}\ell^+(R_n^+).$$

Here, $\mathcal{C}\ell^+(R_n^+)$ is the narrow class group of the totally real order R_n^+.

The proof follows directly from Theorem 4.5. For more details, see [13, Proposition 3.5].

We will also need the analogue of Lemma 3.7 in [13]:

Lemma 5.4. *For a density-one set of positive integers n, we have $\frac{\#\mathcal{C}\ell(R_n)}{\#\mathcal{C}\ell^+(R_n^+)} = (q^{n/2})^{\frac{g(g+1)}{2}-1+o(1)}$.*

Proof. As n tends to infinity, the class groups of both rings are well approximated by their root-discriminants.

We first compute the index of $\mathbb{Z}[\alpha^n]$ inside R_n. As in [13], this index is a power of p, therefore it suffices to compute the corresponding index after tensoring both rings with $\mathbb{Z}_p$. Let $f(x)$ denote the minimal polynomial of α^n, and let $f(x) = f_{\mathrm{et}}(x) f_{\mathrm{tor}}(x) f_{\mathrm{ss}}(x)$ over $\mathbb{Z}_p$ correspond to the slope decomposition of $\mathscr{G}$. As A is almost ordinary, f_{et} and f_{tor} have degree $g-1$, and f_{ss} has degree two. Let $\beta_1, \ldots, \beta_{g-1}$ denote the roots of f_{et}, $\gamma_1, \ldots, \gamma_{g-1}$ denote the roots of f_{tor} and δ_1, δ_2 denote the roots of f_{ss}. It follows that the β_i are p-adic units, that $\frac{v_p(\gamma_i)}{v_p(q^n)} = 1$ and $\frac{v_p(\delta_i)}{v_p(q^n)} = 1/2$.

Let g_{tor} denote the polynomial with roots γ_i/q and g_{ss} denote the polynomial with roots $\delta_i/q^{1/2}$. The index of $\mathbb{Z}_p[\alpha]$ inside $R_n \otimes \mathbb{Z}_p$ equals the index of $\mathbb{Z}_p[x]/f_{\mathrm{tor}}(x) f_{\mathrm{ss}}(x)$ inside $\mathbb{Z}_p[x]/g_{\mathrm{tor}}(x) g_{\mathrm{ss}}(x)$. This index equals the square-root of $\dfrac{(\delta_1 - \delta_2)^2 \cdot \prod_{ij} (\gamma_i - \gamma_j)^2 \cdot \prod_{ij} (\gamma_i - \delta_j)^2}{(\delta_1/q^{1/2} - \delta_2/q^{1/2})^2 \cdot \prod_{ij} (\gamma_i/q - \gamma_j/q)^2 \cdot \prod_{ij} (\gamma_i/q - \delta_j/q^{1/2})^2}$. It is easy to see that the square root of this quotient equals $q^{(g-1)(g-2)/2+g-1+1}$.

Therefore, it suffices to bound the quotient $\frac{d(\mathbb{Z}[\alpha^n])}{d(R_n^+)}$. The same argument as in the last paragraph of [13, Lemma 3.8] goes through verbatim to finish the proof of this result. □

We now prove Theorem 1.2. By Lemma 5.4 and Proposition 5.3, it suffices to prove that there is some principally polarized abelian variety with endomorphism ring equal to R_n for a positive density set of n.

Proof of Theorem 1.2. Let h_n be the minimal polynomial of $\alpha^n + (q/\alpha)^n$, and let $\lambda_n = [(\alpha^n - (q/\alpha)^n) h_n'(\alpha^n + (q/\alpha)^n)]^{-}1$. Note that λ_n is a purely imaginary algebraic number. Let $I \subset K$ denote any fractional ideal, and let Φ denote one of the two CM type on K. The pairing

$$(x, y) \mapsto \mathrm{Trace}_{K/\mathbb{Q}}(\lambda_n x \bar{y}) \tag{2}$$

[6] If the isogeny class is ramified.

[7] If the isogeny class is inert.

induces a polarization on I precisely when $\phi(\lambda_n)/i$ is a positive real number for every $\phi \in \Phi$. An argument identical to the one in [13, Proposition 3.6] proves that when the conjugates of α_n satisfy the multiplicative independence conditions in *loc. cit.*, the numbers $\phi(\lambda_n)/i$ are all positive for a positive proporition of n (namely, a proportion of $\frac{1}{2^g}$). Therefore, we will assume that n is an integer for which λ_n satisfies these polarization conditions, and prove that there exists an abelian variety A with endomorphism ring R_n, which is principally polarized. The theorem would follow from this, Proposition 5.3 and Lemma 5.4.

We will treat the case when $n = 1$; the same proof goes through verbatim for general n. Let $\mathfrak{b} \subset \mathcal{O}_K$ be the unique maximal ideal corresponding to the slope-half part of A. Let $R = R_1$. As R is locally the maximal order at $\mathfrak{b}$, it follows that the R-ideal $\mathfrak{b} \cap R$ is invertible. Further, both R and the ideal $\mathfrak{b}$ are stable under the action of complex conjugation on K.

Let $R' = \mathbb{Z}[\alpha, q/\alpha]$. The dual of R' with respect to the pairing (2) is R' (see [6, Proposition 9.5]). As the orders R and R' agree away from the prime $\mathfrak{b}$, it follows that the dual of R is a power of $\mathfrak{b}$, say $\mathfrak{b}^n$. As $\mathfrak{b}$ is stable under the action of conplex conjugation, the dual of $\mathfrak{b}$ with respect to (2) is $\mathfrak{b}^{n-1}$, the dual of $\mathfrak{b}^2$ is $\mathfrak{b}^{n-2}$, etc. If n was an even integer, then the ideal $\mathfrak{b}^{n/2}$ is self dual, thereby yielding a principally polarized abelian variety, as required. We will now prove that if the isogeny class is ramified, then n necessarily has to be even, and if the isogeny class is inert, we will produce an abelian variety which is principally polarized.

The ramified case

Suppose that n were odd. Without loss of generality, we assume that $n = 1$. Therefore, there exists a polarization with degree equal to the size of $R/\mathfrak{b}$. However, $R/\mathfrak{b}$ has size p, and the degree of a polarization is necessarily a square, yielding a contradiction. Therefore, n had to have been even, yielding the required result in the ramified case.

The inert case

Again, we assume that $n = 1$. Let A denote an abelian variety (in either equivalence class) corresponding to the ideal R. The polarization constructed is of the form $\lambda\colon A \to A^\vee$, and has kernel equal to the p-torsion of the supersingular part of $A[p^\infty]$. Let B be the abelian variety such that $B/G = A$, where $G \subset B[p]$ is the p-torsion of the étale part of $B[p^\infty]$. Then, the dual isogeny from $A^\vee$ to $B^\vee$ has kernel equal to the p-torsion of the multiplicative part of $A^\vee[p^\infty]$. Therefore, the composite map from B to $B^\vee$ has kernel $B[p]$, and thus $B^\vee = B/B[p] = B$. We have produced a principally polarized abelian variety B, isogenous to A! It is also clear that the endomorphism ring of B equals that of A, whence the theorem follows. □

References

[1] T.G. Centeleghe, J. Stix. Categories of abelian varieties over finite fields, I: Abelian varieties over $\mathbb{F}_p$. *Algebra Number Theory* 9 (2015), no. 1, 225265.

[2] W.C. Chi. ℓ-adic and λ-adic representations associated to abelian varieties defined over number fields. *Amer. J. Math.* 114 (1992), no. 2, 315353.

[3] P. Deligne. Variétés abéliennes ordinaires sur un corps fini. *Invent. Math.* 8 (1969) 238243.

[4] M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkrper. *Abh. Math. Sem. Univ. Hamburg* 14 (1941), no. 1, 197272.

[5] V.G. Drinfel'd. Coverings of p-adic symmetric domains. *Funkcional. Anal. i Priloen.* 10 (1976), no. 2, 2940.

[6] E. Howe. Principally polarized ordinary abelian varieties over finite fields. *Trans. Amer. Math. Soc.* 347 (1995), no. 7, 23612401.

[7] S.L. Kleiman, J.O. Kleppe. Macaulay duality over any base. *Preliminary preprint dated 26th December 2018.*

[8] H.W. Lenstra, Y.G. Zarhin. The Tate conjecture for almost ordinary abelian varieties over finite fields. *Advances in Number Theory: The Proceedings of the Third Conference of the Canadian Number Theory Association, August 18-24, 1991, the Queen's University at Kingston* (Vol. 3, p. 179). Oxford University Press on Demand (1993).

[9] S. Marseglia. Computing square-free polarized abelian varieties over finite fields. Arxiv:1805.10223, 2018.

[10] W. Messing. The crystals associated to Barsotti-Tate groups: with applications to abelian schemes. Lecture Notes in Mathematics, Vol. 264. *Springer-Verlag*, Berlin-New York, 1972.

[11] J.S. Milne. Complex Multiplication. www.jmilne.org/math/CourseNotes/CM.pdf

[12] F. Oort. CM-liftings of abelian varieties. *J. Algebraic Geom.* 1 (1992), no. 1, 131146.

[13] A.N. Shankar, J. Tsimerman. (2018). Unlikely Intersections in finite characteristic. *Forum of Mathematics, Sigma*, 6, E13.

[14] W.C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. cole Norm. Sup.* (4) 2 1969 521560.

Abhishek Oswal, Department of Mathematics, University of Toronto.
45 St. George Street, Toronto, ON M5S 2E5, Canada.
abhishek@math.toronto.edu

Ananth N. Shankar, Department of Mathematics, MIT.
182 Memorial Drive, Cambridge, MA 02142, USA.
ananths@mit.edu