FROBENIUS DISTRIBUTIONS OF LOW DIMENSIONAL ABELIAN VARIETIES OVER FINITE FIELDS

SANTIAGO ARANGO-PIÑEROS, DEEWANG BHAMIDIPATI, AND SOUMYA SANKAR

ABSTRACT. Given a g-dimensional abelian variety A over a finite field $\mathbf{F}_q$, the Weil conjectures imply that the normalized Frobenius eigenvalues generate a multiplicative group of rank at most g. The Pontryagin dual of this group is a compact abelian Lie group that controls the distribution of high powers of the Frobenius endomorphism. This group, which we call the Serre–Frobenius group, encodes the possible multiplicative relations between the Frobenius eigenvalues. In this article, we classify all possible Serre–Frobenius groups that occur for $g \leq 3$. We also give a partial classification for simple ordinary abelian varieties of prime dimension $g > 3$.

1. INTRODUCTION

Let E be an elliptic curve over a finite field $\mathbf{F}_q$ of characteristic $p > 0$. The zeros $\alpha_1, \overline{\alpha}_1$ of the characteristic polynomial of Frobenius acting on the Tate module of E are complex numbers of absolute value $\sqrt{q}$. Consider $u_1 := \alpha_1/\sqrt{q}$ and $\overline{u}_1$ the normalized zeros in the unit circle $\mathsf{U}(1)$. The curve E is *ordinary* if and only if u_1 is not a root of unity, and in this case, the sequence $(u_1^r)_{r=1}^{\infty}$ is equidistributed in $\mathsf{U}(1)$. Further, the normalized Frobenius traces $x_r := u_1^r + \overline{u}_1^r$ are equidistributed on the interval $[-2, 2]$ with respect to the pushforward of the probability Haar measure on $\mathsf{U}(1)$ via $u \mapsto u + \overline{u}$, namely

$$\lambda_1(x) := \frac{\mathrm{d}x}{\pi\sqrt{4 - x^2}}, \tag{1.1}$$

where $\mathrm{d}x$ is the restriction of the Lebesgue measure to $[-2, 2]$ (see [Fit15, Proposition 2.2]).

In contrast, if E is supersingular, the sequence $(u_1^r)_{r=1}^{\infty}$ generates a finite cyclic subgroup of order m, $C_m \subset \mathsf{U}(1)$. In this case, the normalized Frobenius traces are equidistributed with respect to the pushforward of the uniform measure on C_m.

This dichotomy branches out in an interesting way for abelian varieties of higher dimension $g > 1$: potential non-trivial multiplicative relations between the Frobenius eigenvalues $\alpha_1, \overline{\alpha}_1, \ldots, \alpha_g, \overline{\alpha}_g$ increase the complexity of the problem of classifying the distribution of normalized traces of high powers of Frobenius,

$$x_r := (\alpha_1^r + \overline{\alpha}_1^r + \cdots + \alpha_g^r + \overline{\alpha}_g^r)/q^{r/2} \in [-2g, 2g], \text{ for } r \geq 1. \tag{1.2}$$

In analogy with the case of elliptic curves, we identify a compact abelian subgroup of $\mathsf{U}(1)^g$ controlling the distribution of Sequence (1.2) via pushforward of the Haar measure. In this article, we provide a complete classification of this subgroup, which we call the *Serre–Frobenius group*, for abelian varieties of dimension up to 3. We do this by classifying the possible multiplicative relations between the Frobenius eigenvalues. This classification provides a description of all the possible distributions of Frobenius traces in these cases (see Corollary 1.1.1). We also provide a partial classification for simple ordinary abelian varieties of odd prime dimension.

Definition 1.0.1 (Serre–Frobenius group). Let A be an abelian variety of dimension g over $\mathbf{F}_q$. Let $\alpha_1, \alpha_2 \ldots, \alpha_g, \overline{\alpha}_1, \overline{\alpha}_2 \ldots \overline{\alpha}_g$ denote the eigenvalues of Frobenius, ordered such that $\arg(\alpha_i) \geq \arg(\alpha_j)$ if $g \geq i > j \geq 1$. Let $u_i = \alpha_i/\sqrt{q}$ denote the normalized Frobenius eigenvalues. The Serre–Frobenius group of A, denoted by $\mathsf{SF}(A)$, is the closure of the subgroup of $\mathsf{U}(1)^g$ generated by the vector $\mathbf{u} := (u_1, \ldots, u_g)$.

We classify the Serre–Frobenius groups of abelian varieties of dimension $g \leq 3$.

Theorem A (Elliptic curves). *Let E be an elliptic curve defined over $\mathbf{F}_q$. Then*

2020 *Mathematics Subject Classification.* 11G10, 11G25, 11M38, 14K02, 14K15.

Key words and phrases. Abelian varieties over finite fields, Frobenius traces, Equidistribution.

(1) E is ordinary if and only if $\mathsf{SF}(E) = \mathsf{U}(1)$.
(2) E is supersingular if and only if $\mathsf{SF}(E) \in \{C_1, C_3, C_4, C_6, C_8, C_{12}\}$.

Moreover, each one of these groups is realized for some prime power q.

We note that the classification of supersingular Serre–Frobenius groups of elliptic curves follows from Deuring [Deu41] and Waterhouse's [Wat69] classification of Frobenius traces (see also [Oor07, Section 14.6] and [SHOR20, Theorem 2.6.1]).

Theorem B (Abelian surfaces)**.** *Let S be an abelian surface over $\mathbf{F}_q$. Then, S has Serre–Frobenius group according to Figure 4. The possible options for the connected component of the identity, $\mathsf{SF}(S)^\circ$, and the size of the cyclic component group $\mathsf{SF}(S)/\mathsf{SF}(S)^\circ$ are given below. Further, each one of these groups is realized for some prime power q.*

$\mathsf{SF}(S)^\circ$	$\#\mathsf{SF}(S)/\mathsf{SF}(S)^\circ$
1	1,2,3,4,5,6,8,10,12,24
$\mathsf{U}(1)$	1,2,3,4,6,8,12
$\mathsf{U}(1)^2$	1

Theorem C (Abelian threefolds)**.** *Let X be an abelian threefold over $\mathbf{F}_q$. Then, X has Serre–Frobenius group according to Figure 10. The possible options for the connected component of the identity, $\mathsf{SF}(X)^\circ$, and the size of the cyclic component group $\mathsf{SF}(X)/\mathsf{SF}(X)^\circ$ are given below. Further, each one of these groups is realized for some prime power q.*

$\mathsf{SF}(X)^\circ$	$\#\mathsf{SF}(X)/\mathsf{SF}(X)^\circ$
1	1,2,3,4,5,6,7,8,9,10,12,14,15,18,20,24,28,30,36
$\mathsf{U}(1)$	1,2,3,4,5,6,7,8,10,12,24
$\mathsf{U}(1)^2$	1,2,3,4,6,8,12,24
$\mathsf{U}(1)^3$	1

If g is an odd prime, we have the following classification for simple ordinary abelian varieties. In the following theorem, we say that an abelian variety A splits over a field extension $\mathbf{F}_{q^m}$ if A is isogenous over $\mathbf{F}_{q^m}$ to a product of proper abelian subvarieties.

Theorem D (Prime dimension)**.** *Let A be a simple ordinary abelian variety defined over $\mathbf{F}_q$ of prime dimension $g > 2$. Then, exactly one of the following conditions holds.*
(1) A is absolutely simple.
(2) A splits over a degree g extension of $\mathbf{F}_q$ as a power of an elliptic curve, and $\mathsf{SF}(A) \cong \mathsf{U}(1) \times C_g$.
(3) $2g+1$ is prime (i.e., g is a Sophie Germain prime) and A splits over a degree $2g+1$ extension of $\mathbf{F}_q$ as a power of an elliptic curve, and $\mathsf{SF}(A) \cong \mathsf{U}(1) \times C_{2g+1}$.

Key to our results is the relation between the Serre–Frobenius group and the multiplicative subgroup of $U_A \subset \mathbf{C}^\times$ generated by the normalized eigenvalues $u_1, \dots, u_g$. Indeed, an equivalent definition of the former is via the Pontryagin dual of the latter (see Lemma 2.3.1). The rank of the group U_A is called the angle rank of the abelian variety and the order of the torsion subgroup is called the angle torsion order. The relation between $\mathsf{SF}(A)$ and the group generated by the normalized eigenvalues gives us the following structure theorem.

Theorem E. *Let A be an abelian variety defined over $\mathbf{F}_q$. Then*

$$\mathsf{SF}(A) \cong \mathsf{U}(1)^\delta \times C_m,$$

where $\delta = \delta_A$ is the angle rank and $m = m_A$ is the angle torsion order. Furthermore, the connected component of the identity is

$$\mathsf{SF}(A)^\circ = \mathsf{SF}(A_{\mathbf{F}_{q^m}}).$$

1.1. **Application to distributions of Frobenius traces.** Our results can be applied to understanding the distribution of Frobenius traces of an abelian variety over $\mathbf{F}_q$ as we range over finite extensions of the base field. Indeed, for each integer $r \geq 1$, we may rewrite Equation (1.2) as

$$x_r = u_1^r + \overline{u}_1^r + \cdots + u_g^r + \overline{u}_g^r \in [-2g, 2g]$$

denote the normalized Frobenius trace of the base change of an abelian variety A to $\mathbf{F}_{q^r}$.

In [AS10], the authors study Jacobians of smooth projective genus g curves with maximal angle rank[1] and show that the sequence $(x_r/2g)_{r=1}^\infty$ is equidistributed on $[-1,1]$ with respect to an explicit measure. The Serre–Frobenius group enables us to remove the assumption of maximal angle rank.

Corollary 1.1.1. *Let A be a g-dimensional abelian variety defined over $\mathbf{F}_q$. Then, the sequence $(x_r)_{r=1}^\infty$ of normalized traces of Frobenius is equidistributed in $[-2g, 2g]$ with respect to the pushforward of the Haar measure on $\mathsf{SF}(A) \subseteq \mathsf{U}(1)^g$ via*

$$\mathsf{SF}(A) \subseteq \mathsf{U}(1)^g \to [-2g, 2g], \quad (z_1, \ldots, z_g) \mapsto z_1 + \overline{z}_1 + \cdots + z_g + \overline{z}_g. \tag{1.3}$$

The classification of the Serre–Frobenius groups in our theorems can be used to distinguish between the different Frobenius trace distributions occurring in each dimension.

Example 1.1.2. Let S be a simple abelian surface over $\mathbf{F}_q$ with Frobenius eigenvalues $R_S = \{\alpha_1, \alpha_2, \overline{\alpha}_1, \overline{\alpha}_2\}$ and suppose that $S_{(2)} := S \times_{\mathbf{F}_q} \mathbf{F}_{q^2}$ is isogenous to E^2 for some ordinary elliptic curve $E/\mathbf{F}_{q^2}$. In this case, $\left\{\alpha_1^2, \overline{\alpha}_1^2\right\} = R_E = \left\{\alpha_2^2, \overline{\alpha}_2^2\right\}$. Normalizing, and using the fact the S is simple, we see that either (1) $u_2 = -u_1$, or (2) $u_2 = -\overline{u}_1$. The Serre–Frobenius groups in these cases can be calculated as follows.

(1) When $u_2 = -u_1$, the vector of normalized eigenvalues $\mathbf{u} = (u_1, u_2) = (u_1, -u_1)$ generates the group

$$\mathsf{SF}(S) = \overline{\{(u_1^m, -u_1^m) \colon m \in \mathbf{Z}\}} = \{(u, -u) : u \in \mathsf{U}(1)\} \subset \mathsf{U}(1)^2.$$

Extending scalars to $\mathbf{F}_{q^2}$, we get:

$$\mathsf{SF}(S_{(2)}) = \overline{\{(u_1^{2m}, (-u_1)^{2m}) : m \in \mathbf{Z}\}} = \{(u, u) \colon u \in \mathsf{U}(1)\} \subset \mathsf{U}(1)^2.$$

(2) When $u_2 = -\overline{u}_1$, the vector of normalized eigenvalues $\mathbf{u} = (u_1, u_2) = (u_1, -u_1^{-1})$ generates the group $\mathsf{SF}(S) = \left\{(u, -u^{-1}) : u \in \mathsf{U}(1)\right\} \subset \mathsf{U}(1)^2$. Similar to the case above, $\mathsf{SF}(S_{(2)}) = \left\{(u, u^{-1}) : u \in \mathsf{U}(1)\right\}$.

In both cases, the sequence of normalized traces is given by

$$x_r = u_1^r + \overline{u}_1^r + (-1)^r \overline{u}_1^r + (-1)^r u_1^r \in [-4, 4].$$

In particular, $x_r = 0$ when r is odd, and $x_r = 2u_1^r + 2\overline{u}_1^r$ when r is even. Extending the base field to $\mathbf{F}_{q^2}$ yields the sequence of normalized traces $x_r(S_{(2)}) = x_{2r}(S) = 2x_r(E)$. The equality of the trace distributions is a consequence of the fact the $\mathsf{SF}(S)$ in both cases is isomorphic to $\mathsf{U}(1) \times C_2$. The data of the embedding $\mathsf{SF}(S) \subseteq \mathsf{U}(1)^2$ precisely captures the (non-trivial) multiplicative relations between the Frobenius eigenvalues.

In both cases (1) and (2), the normalized traces $x_r(S)$ are equidistributed with respect to the pushforward of the Haar measure under the map $\mathsf{SF}(S) \subseteq \mathsf{U}(1)^2 \to [-4, 4]$ given by $(z_1, z_2) \mapsto z_1 + \overline{z}_1 + z_2 + \overline{z}_2$. This can be computed explicitly as

$$\tfrac{1}{2}\delta_0 + \frac{\mathrm{d}x}{2\pi\sqrt{16 - x^2}} \quad \text{and} \quad \frac{\mathrm{d}x}{\pi\sqrt{16 - x^2}} \tag{1.4}$$

for S and $S_{(2)}$ respectively, where $\mathrm{d}x$ is the restriction of the Haar measure to $[-4, 4]$, and δ_0 is the Dirac measure supported at 0.

For instance, choose the surface S to be in the isogeny class with LMFDB label[2] `2.5.a_ab` and Weil polynomial $P(T) = T^4 - T^2 + 25$. This isogeny class is ordinary and simple, but not geometrically simple. Indeed, $S_{(2)}$ is in the isogeny class `1.25.ab`^{2} = `2.25.ac_bz` corresponding to the square of an ordinary elliptic curve. The corresponding a_1-histograms describing the frequency of the sequence $(x_r)_{r=1}^\infty$ are depicted in Figure 1. Each graph represents a histogram of $16^6 = 16777216$ samples placed into $4^6 = 4096$ buckets

[1] In their notation, this is the condition that the Frobenius angles are linearly independent modulo 1.

[2] Recall the labelling convention for isogeny classes of abelian varieties over finite fields in the LMFDB: `g.q.iso` where `g` is the dimension, `q` is the cardinality of the base field, and `iso` specifies the isogeny class by writing the coefficients of the Frobenius polynomial in base 26.

partitioning the interval $[-2g, 2g]$. The vertical axis has been suitably scaled, with the height of the uniform distribution, $1/4g$, indicated by a gray line.

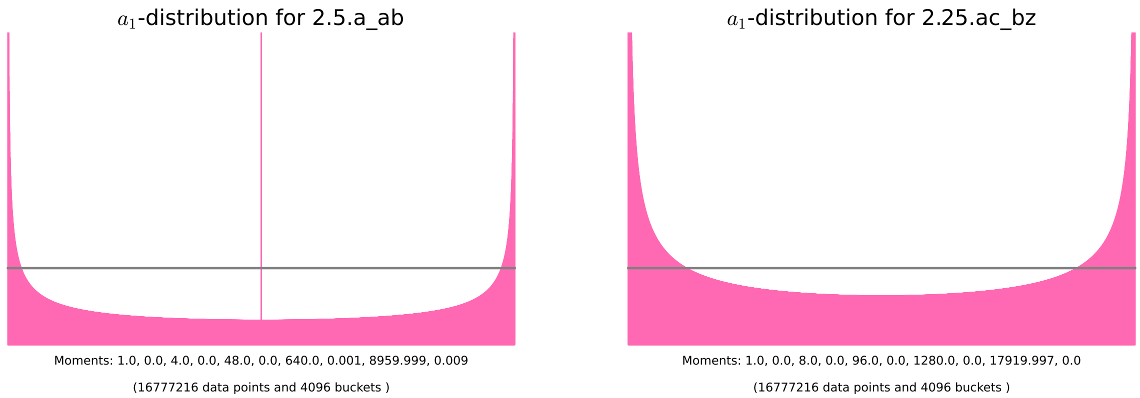


FIGURE 1. a_1-histograms for 2.5.a_ab and 2.25.ac_bz.

1.2. **Relation to other work.** The reason for adopting the name "Serre-Frobenius group" is that the Lie group $\mathsf{SF}(A)$ is closely related to Serre's Frobenius torus [Ser13], as explained in Remark 2.3.3.

1.2.1. *Angle rank.* In this article, we study multiplicative relations between Frobenius eigenvalues, a subject studied extensively by Zarhin [Zar91, Zar93, LZ93, Zar94, Zar15]. Our classification relies heavily on being able to understand multiplicative relations in low dimension, and we use results of Zarhin in completing parts of it. The number of multiplicative relations is quantified by the angle rank, an invariant studied in [DKZB21], [DKRV21b] for absolutely simple abelian varieties by elucidating its interactions with the Galois group and Newton polygon of the Frobenius polynomial. We study the angle rank as a stepping stone to classifying the full Serre–Frobenius group. While our perspective differs from that in [DKZB21], the same theme is continued here: the Serre–Frobenius groups depend heavily on the Galois group of the Frobenius polynomial. It is worth noting that here that the results about the angle rank in the non-absolutely simple case cannot be pieced together by knowing the results in the absolutely simple cases (see for instance, see Zywina's exposition of Shioda's example [Zyw22, Remark 1.16]).

1.2.2. *Sato–Tate groups.* The Sato–Tate group of an abelian variety defined over a number field controls the distribution of the Frobenius of the reduction modulo prime ideals, and it is defined via its ℓ-adic Galois representation (see [Sut16, Section 3.2]). The Serre–Frobenius group can also be defined via ℓ-adic representations in an analogous way: it is conjugate to a maximal compact subgroup of the image of Galois representation $\rho_{A,\ell}\colon \mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q) \to \mathrm{Aut}(V_\ell A) \otimes \mathbf{C}$, where $V_\ell A$ is the ℓ-adic Tate vector space. Therefore it is natural to expect that the Sato–Tate and the Serre–Frobenius group are related to each other. The following observations support this claim:

- Assuming standard conjectures, the connected component of the identity of the Sato–Tate group can be recovered from knowing the Frobenius polynomial at two suitably chosen primes ([Zyw22, Theorem 1.6]).
- Several abelian Sato–Tate groups (see [FKRS12, FKS23]) appear as Serre–Frobenius groups of abelian varieties over finite fields. The ones with maximal angle rank are:
  - $\mathsf{U}(1)$ is the Sato–Tate group of an elliptic curve with complex multiplication over any number field that contains the CM field (see 1.2.B.1.1a). It is also the Serre–Frobenius group of any ordinary elliptic curve (see Figure 2), and the a_1-moments coincide.
  - $\mathsf{U}(1)^2$ is the Sato–Tate group of weight 1 and degree 4 (see 1.4.D.1.1a). It is also the Serre–Frobenius group of an abelian surface with maximal angle rank (see Figure 7), and the a_1-moments coincide.
  - $\mathsf{U}(1)^3$ is the Sato–Tate group of weight 1 and degree 6 (see 1.6.H.1.1a). It is also the Serre-Frobenius group of abelian threefolds with maximal angle rank (see Figure 11), and the a_1-moments coincide.

This is not unexpected, since $\mathsf{U}(1)^g$ embeds into $\mathrm{USp}_{2g}(\mathbf{C})$ and composition with the trace map gives the normalized traces $(x_r)_{r=1}^{\infty}$.

1.3. **Outline.** In Section 2, we give some background on abelian varieties over finite fields, expand on the definition of the Serre–Frobenius group, and describe how it controls the distribution of traces of high powers of Frobenius. In Section 3, we prove some preliminary results on the geometric isogeny types of abelian varieties of dimension $g \leq 3$ and g odd prime. We also recall some results about Weil polynomials of supersingular abelian varieties, and Zarhin's notion of neatness. In Sections 4, 5, and 6, we give a complete classification of the Serre–Frobenius group for dimensions 1, 2, and 3 respectively. In Section 7, we discuss the case of simple ordinary abelian varieties of odd prime dimension. A list of tables containing different pieces of the classification follows this section.

1.4. **Notation.** Throughout this paper, A will denote a g-dimensional abelian variety over a finite field $\mathbf{F}_q$ of characteristic p. The polynomial $P_A(T) = \sum_{i=1}^{2g} a_i T^{2g-i}$ will denote the characteristic polynomial of Frobenius acting on the Tate module of A, and $h_A(T)$ its minimal polynomial. The set of roots of $P_A(T)$ is denoted by R_A. We usually write $\alpha_1, \overline{\alpha}_1 \ldots, \alpha_g, \overline{\alpha}_g \in R_A$ for the Frobenius eigenvalues. In the case that $P_A(T)$ is a power of $h_A(T)$, we will denote by e_A this power (See 2.1). The subscript $(\cdot)_{(r)}$ will denote the base change of any object or map to $\mathbf{F}_{q^r}$. The group U_A will denote the multiplicative group generated by the normalized eigenvalues of Frobenius, δ_A its rank and m_A the order of its torsion subgroup. The group Γ_A will denote the multiplicative group generated by $\{\alpha_1, \alpha_2 \ldots \alpha_g, q\}$. In Section 5, S will be used to denote an abelian surface, while in Section 6, X will be used to denote a threefold.

1.5. **Acknowledgements.** We would like to thank David Zureick-Brown, Kiran Kedlaya, Francesc Fité, Brandon Alberts, Edgar Costa and Andrew Sutherland for useful conversations about this paper. We thank Yuri Zarhin for providing us with useful references. We would also like to thank Everett Howe for helping us with a missing piece of the puzzle in Theorem 3.1.1. This project started as part of the Rethinking Number Theory workshop in 2021. We would like to thank the organizers of the workshop for giving us the opportunity and space to collaborate, and the funding sources for the workshop, AIM, the Number Theory Foundation, and the University of Wisconsin-Eau Claire Department of Mathematics. We would also like to thank Rachel Pries for her guidance at the beginning of the workshop, which helped launch this project.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

2. Frobenius multiplicative groups

In this section we introduce the Serre–Frobenius group of A and explain how it is related to Serre's theory of Frobenius tori [Ser13]. We do this from the perspective of the theory of algebraic groups of multiplicative type, as in [Mil17, Chapter 12]. We start by recalling some facts about abelian varieties over finite fields.

2.1. **Background on Abelian varieties over finite fields.** Fix A a g dimensional abelian variety over $\mathbf{F}_q$. A q-Weil number is an algebraic integer α such that $|\phi(\alpha)| = \sqrt{q}$ for every embedding $\phi\colon \mathbf{Q}(\alpha) \to \mathbf{C}$. Let $P_A(T)$ denote the characteristic polynomial of the Frobenius endomorphism acting on the ℓ-adic Tate module of A. The polynomial $P_A(T)$ is monic of degree $2g$, and Weil [Wei49] showed that its roots are q-Weil numbers; we denote the set of roots of $P_A(T)$ by $R_A := \{\alpha_1, \alpha_2 \ldots, \alpha_g, \alpha_{g+1}, \ldots, \alpha_{2g}\}$ with $\alpha_{g+j} = q/\alpha_j$ for $j \in \{1, \ldots, g\}$. We index the first g roots according to non-decreasing angles; that is $\arg(\alpha_j) \leq \arg(\alpha_i)$ if $j < i$. The seminal work of Honda [Hon68] and Tate [Tat66] [Tat71] classifies the isogeny decomposition type of A in terms of the factorization of $P_A(T)$. In particular, if A is simple, we have that $P_A(T) = h_A(T)^{e_A}$ where $h_A(T)$ is the minimal polynomial of the Frobenius endomorphism and e_A is the degree, i.e., the square root of the dimension, of the central simple algebra $\mathrm{End}^0(A) := \mathrm{End}(A) \otimes \mathbf{Q}$ over its center. The Honda–Tate theorem gives a bijective correspondence between isogeny classes of simple abelian varieties over $\mathbf{F}_q$ and conjugacy classes of q-Weil numbers, sending the isogeny class determined by A to the set of roots R_A. Further, if $A \sim A_1 \times A_2 \ldots \times A_k$, then $P_A(T) = \prod_{i=1}^{k} P_{A_i}(T)$.

Writing $P_A(T) = \sum_{i=0}^{2g} a_i T^{2g-i}$, the q-Newton polygon of A is the lower convex hull of the set of points $\{(i, \nu(a_i)) \in \mathbf{R}^2 : a_i \neq 0\}$ where ν is the p-adic valuation normalized so that $\nu(q) = 1$. The Newton polygon is isogeny invariant. Define the p-rank of A as the number of slope 0 segments of the Newton polygon. An abelian variety is called ordinary if it has maximal p-rank, i.e. its p-rank is equal to g. It is called supersingular if all the slopes of the Newton polygon are equal to $1/2$. The field $L = L_A := \mathbf{Q}(\alpha_1, \ldots, \alpha_g)$ is the splitting field of the Frobenius polynomial. By definition, the Galois group $\mathrm{Gal}(L/\mathbf{Q})$ acts on the roots R_A by permuting them.

Notation. Whenever A is fixed or clear from context, we will omit the subscript corresponding to it from the notation described above. In particular, we will use $P(T), h(T)$ and e instead of $P_A(T), h_A(T)$ and e_A.

2.2. **Angle groups.** Denote by $\Gamma := \Gamma_A$ the multiplicative subgroup of $\mathbf{C}^\times$ generated by the set of Frobenius eigenvalues R_A, and let $\Gamma_{(r)} := \Gamma_{A_{(r)}}$ for every $r \geq 1$. Since $\alpha \mapsto q/\alpha$ is a permutation of R_A, the set $\{\alpha_1, \ldots, \alpha_g, q\}$ is a set of generators for Γ; that is, every $\gamma \in \Gamma$ can be written as

$$\gamma = q^k \prod_{j=1}^{g} \alpha_j^{k_j} \tag{2.1}$$

for a some $(k, k_1, \ldots, k_g) \in \mathbf{Z}^{g+1}$.

Since Γ is a subgroup of $\overline{\mathbf{Q}}^\times$, it is naturally a $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-module. However, this perspective is not necessary for our applications. This group is denoted as Φ_A in [Zyw22].

Definition 2.2.1. We define the angle group of A to be $U := U_A$, the multiplicative subgroup of $\mathsf{U}(1)$ generated by the unitarized eigenvalues $\{u_j := \alpha_j/\sqrt{q} : j = 1, \ldots, g\}$. When A is fixed, for every $r \geq 1$ we abbreviate $U_{(r)} := U_{A_{(r)}}$.

Definition 2.2.2. The angle rank of an abelian variety $A/\mathbf{F}_q$ is the rank of the finitely generated abelian group U_A. It is denoted by $\delta_A := \mathrm{rk}\, U_A$. The angle torsion order m_A is the order of the torsion subgroup of U_A, so that $U_A \cong \mathbf{Z}^{\delta_A} \oplus \mathbf{Z}/m_A\mathbf{Z}$.

The angle rank δ is by definition an integer between 0 and g. When $\delta = g$, there are no multiplicative relations among the normalized eigenvalues. In other words, there are no additional relations among the generators of Γ_A apart from the ones imposed by the Weil conjectures. If A is absolutely simple, the maximal angle rank condition also implies that the Tate conjecture holds for all powers of A (see Remark 1.3 in [DKZB21]). On the other extreme, $\delta = 0$ if and only if A is supersingular (See Example 5.1 [DKRV21b]).

Remark 2.2.3. The angle rank is invariant under base extension: $\delta(A) = \delta(A_{(r)})$ for every $r \geq 1$. Indeed, any multiplicative relation between $\{u_1^r, \ldots, u_g^r\}$ is a multiplicative relation between $\{u_1, \ldots, u_g\}$. We have that $U_A/\mathrm{Tors}(U_A) \cong U_{A_{(r)}}/\mathrm{Tors}(U_{A_{(r)}})$ for every positive integer r. In particular, $U_A/\mathrm{Tors}(U_A) \cong U_{A_{(m)}}$ where $m = m_A$ is the angle torsion order of A.

Example 2.2.4 (Extension and restriction of scalars)**.** Let $A/\mathbf{F}_q$ be an abelian variety with Frobenius polynomial $P_A(T) = \prod(T-\alpha) \in \mathbf{C}[T]$ and circle group $U_A = \langle u_1, \ldots, u_g\rangle$. Then, the extension of scalars $A_{(r)}$ has Frobenius polynomial $P_{(r)}(T) = \prod(T-\alpha^r)$ and circle group $U_{A_{(r)}} = \langle u_1^r, \ldots, u_g^r\rangle \subset U_A$. On the other hand, if $B/\mathbf{F}_{q^r}$ is an abelian variety for some $r \geq 1$, and $A/\mathbf{F}_q$ is the Weil restriction of B to $\mathbf{F}_q$, then $P_A(T) = P_B(T^r)$ and $U_A = \langle U_B, \zeta_r\rangle \supset U_B$. See [DN03].

2.3. **The Serre–Frobenius group.** For every locally compact abelian group G, denote by $\widehat{G}$ its Pontryagin dual; this is the topological group of continuous group homomorphisms $G \to \mathsf{U}(1)$. It is well known that $G \mapsto \widehat{G}$ gives an anti-equivalence of categories from the category of locally compact abelian groups to itself. Moreover, this equivalence preserves exact sequences, and every such G is canonically isomorphic to its double dual via the evaluation isomorphism. See [Pon34] for the original reference and [Mor77] for a gentle introduction.

Recall that we defined the Serre–Frobenius group of A as the topological group generated by the vector $\mathbf{u} = (u_1, \ldots, u_g)$ of normalized eigenvalues (see Definition 1.0.1). This explicit description of the group is practical for calculating examples, but the following equivalent definition is conceptually advantageous.

Lemma 2.3.1. *The Serre–Frobenius group of an abelian variety A has character group U_A. In particular, $\mathsf{SF}(A) \cong \widehat{U}_A$ canonically via the evaluation isomorphism.*

Proof. We have an injection $U_A \to \widehat{\mathsf{SF}(A)}$ given by mapping γ to the character ϕ_γ that maps $\mathbf{u}$ to γ. To see that this map is surjective, observe that by the exactness of Pontryagin duality, the inclusion $\mathsf{SF}(A) \hookrightarrow \mathsf{U}(1)^g$ induces a surjection $\mathbf{Z}^g = \widehat{\mathsf{U}(1)}^g \to \widehat{\mathsf{SF}(A)}$. Explicitly, this tells us that every character of $\mathsf{SF}(A)$ is given by $\phi(z_1, \ldots, z_g) = z_1^{m_1} \ldots z_g^{m_g}$ for some $(m_1, \cdots, m_g) \in \mathbf{Z}^g$. By continuity, every character ϕ of $\mathsf{SF}(A)$ is completely determined by $\phi(\mathbf{u})$. In particular, we have that $\phi(\mathbf{u}) = u_1^{m_1} \ldots u_g^{m_g} \in U_A$. □

The following theorem should be compared to [Sut16, Theorem 3.12]

Theorem 2.3.2 (Theorem E)**.** *Let A be an abelian variety defined over $\mathbf{F}_q$. Then*

$$\mathsf{SF}(A) \cong \mathsf{U}(1)^\delta \times C_m,$$

where $\delta = \delta_A$ is the angle rank and $m = m_A$ is the angle torsion order. Furthermore, the connected component of the identity is

$$\mathsf{SF}(A)^\circ = \mathsf{SF}(A_{(m)}).$$

Proof. Since every finite subgroup of $\mathsf{U}(1)$ is cyclic, the torsion part of the finitely generated group U_A is generated by some primitive m-th root of unity ζ_m. The group $U_{(m)}$ is torsion free by Remark 2.2.3. We thus have the split short exact sequence

$$1 \longrightarrow \langle\zeta_m\rangle \longrightarrow U_A \xrightarrow{u \mapsto u^m} U_{(m)} \longrightarrow 1. \tag{2.2}$$

After dualizing, we get:

$$1 \longrightarrow \mathsf{SF}(A_{(m)}) \longrightarrow \mathsf{SF}(A) \longrightarrow \langle\zeta_m\rangle \longrightarrow 1. \tag{2.3}$$

We conclude that $\mathsf{SF}(A)^\circ = \mathsf{SF}(A_{(m)})$ and $\mathsf{SF}(A)/\mathsf{SF}(A)^\circ \cong \langle\zeta_m\rangle$. □

Remark 2.3.3. By definition, U_A is the image of Γ_A under the radial projection $\psi\colon \mathbf{C}^\times \to \mathsf{U}(1), z \mapsto z/|z|$. Thus, we have a short exact sequence

$$1 \longrightarrow \Gamma_A \cap \mathbf{R}_{>0} \longrightarrow \Gamma_A \xrightarrow{\psi|_\Gamma} U_A \longrightarrow 1, \tag{2.4}$$

which is split by the section $u_j \mapsto \alpha_j$. The kernel $\Gamma \cap \mathbf{R}_{>0}$ is free of rank 1 and contains the group $q^{\mathbf{Z}}$. The relation between the Serre–Frobenius group $\mathsf{SF}(A)$ and Serre's Frobenius Torus (see [Ser13], [Chi92, Section 3]) can be understood via their character groups.

- The (Pontryagin) character group of $\mathsf{SF}(A)$ is U_A.
- The (algebraic) character group of the Frobenius torus of A is the torsion free part of Γ_A.

2.4. **Equidistribution results.** Let (Y, μ) be a measure space in the sense of Serre (see Appendix A.1 in [Ser68]). Recall that a sequence $(y_r)_{r=1}^{\infty} \subset Y$ is μ-equidistributed if for every continuous function $f\colon Y \to \mathbf{C}$ we have that

$$\int_Y f\mu = \lim_{n\to\infty} \frac{1}{n} \sum_{r=1}^{n} f(y_r). \tag{2.5}$$

In our setting, Y will be a compact abelian Lie group with probability Haar measure μ. We have the following lemma.

Lemma 2.4.1. *Let G be a compact group, and $h \in G$. Let H be the closure of the group generated by h. Then, the sequence $(h^r)_{r=1}^{\infty}$ is equidistributed in H with respect to the Haar measure μ_H.*

Proof. For a non-trivial character $\phi\colon H \to \mathbf{C}^{\times}$, the image of the generator $\phi(h) = u \in \mathsf{U}(1)$ is not trivial. We see that

$$\lim_{n\to\infty} \frac{1}{n} \sum_{r=1}^{n} \phi(h^r) = \lim_{n\to\infty} \frac{1}{n} \sum_{r=1}^{n} u^r = 0, \tag{2.6}$$

both when u has finite or infinite order. The latter case follows from Weyl's equidistribution theorem in $\mathsf{U}(1)$. The result follows from Lemma 1 in [Ser68, I-19] and the Peter–Weyl theorem. ☐

Corollary 2.4.2 (Corollary 1.1.1)**.** *Let A be a g-dimensional abelian variety defined over $\mathbf{F}_q$. Then, the sequence $(x_r)_{r=1}^{\infty}$ of normalized traces of Frobenius is equidistributed in $[-2g, 2g]$ with respect to the pushforward of the Haar measure on $\mathsf{SF}(A) \subseteq \mathsf{U}(1)^g$ via*

$$\mathsf{SF}(A) \subseteq \mathsf{U}(1)^g \to [-2g, 2g], \quad (z_1, \ldots, z_g) \mapsto z_1 + \overline{z}_1 + \cdots + z_g + \overline{z}_g.$$

Proof. By Lemma 2.4.1, the sequence $(\mathbf{u}^r)_{r=1}^{\infty}$ is equidistributed in $\mathsf{SF}(A)$ with respect to the Haar measure $\mu_{\mathsf{SF}(A)}$. By definition, the sequence $(x_r)_{r=1}^{\infty}$ is equidistributed with respect to the pushforward measure. ☐

Remark 2.4.3 (Maximal angle rank). When A has maximal angle rank $\delta = g$, the Serre–Frobenius group is the full torus $\mathsf{U}(1)^g$, and the sequence of normalized traces of Frobenius is equidistributed with respect to the pushforward of the measure $\mu_{\mathsf{U}(1)^g}$; which we denote by $\lambda_g(x)$ following the notation[3] in [AS10].

3. Preliminary Results

For this entire section, we let A be an abelian variety over $\mathbf{F}_q$, where $q = p^d$ for some prime p.

3.1. **Splitting of simple ordinary abelian varieties of odd prime dimension.** Recall from Section 1 that an abelian variety A splits over a field extension $\mathbf{F}_{q^m}$ if $A \sim_{(m)} A_1 \times A_2$ and $\dim A_1, \dim A_2 < \dim A$, i.e., if A obtains at least one isogeny factor when base-changed to $\mathbf{F}_{q^m}$. We say that A splits completely over $\mathbf{F}_{q^m}$ if $A_{(m)} \sim A_1 \times A_2 \times \ldots \times A_k$, where each A_i is an absolutely simple abelian variety defined over $\mathbf{F}_{q^m}$. In other words, A acquires its geometric isogeny decomposition over $\mathbf{F}_{q^m}$.

In this section, we analyze the splitting behavior of simple ordinary abelian varieties of *prime dimension* $g > 2$. Our first result is analogous to [HZ02, Theorem 6] for odd primes.

Theorem 3.1.1 (Theorem D)**.** *Let A be a simple ordinary abelian variety defined over $\mathbf{F}_q$ of prime dimension $g > 2$. Then, exactly one of the following conditions holds.*

1. *A is absolutely simple.*
2. *A splits over a degree g extension of $\mathbf{F}_q$ as a power of an elliptic curve, and $\mathsf{SF}(A) \cong \mathsf{U}(1) \times C_g$.*
3. *$2g+1$ is prime (i.e., g is a Sophie Germain prime) and A splits over a degree $2g+1$ extension of $\mathbf{F}_q$ as a power of an elliptic curve, and $\mathsf{SF}(A) \cong \mathsf{U}(1) \times C_{2g+1}$.*

[3]Beware of the different choice of normalization. We chose to use the interval $[-2g, 2g]$ instead of $[-1, 1]$ to be able to compare our distributions with the Sato–Tate distributions of abelian varieties defined over number fields.

Proof. Let $\alpha = \alpha_1$ be a Frobenius eigenvalue of A, and denote by $K = \mathbf{Q}(\alpha) \cong \mathbf{Q}[T]/P(T)$ the number field generated by α. Since A is ordinary, $\mathbf{Q}(\alpha^n) \neq \mathbf{Q}$ is a CM-field over $\mathbf{Q}$ for every positive integer n, and $P(T)$ is irreducible and therefore $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 2g$. Suppose that A is not absolutely simple, and let m be the smallest positive integer such that $A_{(m)}$ splits; by [HZ02, Lemma 4] this is also the smallest m such that $\mathbf{Q}(\alpha^m) \subsetneq \mathbf{Q}(\alpha)$. Since $\mathbf{Q}(\alpha^m)$ is also a CM field, it is necessarily a quadratic imaginary number field.

Observe first that m must be odd. Indeed, if m was even, then $\mathbf{Q}(\alpha^{m/2}) = \mathbf{Q}(\alpha)$ and $[\mathbf{Q}(\alpha^{m/2}) : \mathbf{Q}(\alpha^m)] = 2$. This contradicts the fact that $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 2g$, since g is an odd prime. By [HZ02, Lemma 5], there are two possibilities:

(i) $P(T) \in \mathbf{Q}[T^m]$,
(ii) $K = \mathbf{Q}(\alpha^m, \zeta_m)$.

If (i) holds and $P(T) = T^{2m} + bT^m + q^g$, we conclude that $m = g$ and $b = a_g$. In this case, the minimal polynomial of α^g has degree 2 and is of the form $h_{(g)}(T) = (T - \alpha^g)(T - \overline{\alpha}^g)$. Note that α^g and $\overline{\alpha}^g$ are distinct, since A is ordinary. Thus, $P_g(T) = h_{(g)}(T)^g$ and A must split over a degree g extension.

If (ii) holds, we have that $\varphi(m) \mid 2g$. Since $m > 1$ is odd and $\varphi(m)$ takes even values, we have two possible options: either $\varphi(m) = 2$ or $\varphi(m) = 2g$. If $\varphi(m) = 2$, then $[K : \mathbf{Q}(\alpha^m)] \leq 2$ which contradicts the fact that $\mathbf{Q}(\alpha)$ is a degree $2g$ extension of $\mathbf{Q}$. Therefore, necessarily, $\varphi(m) = 2g$, and $\mathbf{Q}(\alpha) = \mathbf{Q}(\zeta_m)$. Recall from elementary number theory that the solutions to this equation are $(m, g) = (9, 3)$ or $(m, g) = (2g + 1, g)$ for g a Sophie Germain prime.

- ($g > 3$) In this case, (ii) only occurs when $2g + 1$ is prime.
- ($g = 3$) In this case, either $m = 7$ or $m = 9$. To conclude the proof, we show that $m = 9$ does not occur. More precisely, we will show that if A splits over a degree 9 extension, it splits over a degree 3 extension as well. In fact, suppose that $K = \mathbf{Q}(\zeta) = \mathbf{Q}(\alpha)$ for some primitive 9th root of unity. The subfield $F = \mathbf{Q}(\zeta^3)$ is the only quadratic imaginary subfield of K, so if a power of α does not generate K, it must lie in F. Suppose α^9 lies in F. Let σ be the generator of $\mathrm{Gal}(K/F)$ sending ζ to ζ^4. The minimal polynomial of α over F divides $T^9 - \alpha^9$, so $\sigma(\alpha) = \alpha \cdot \zeta^j$ for some j, and $\sigma^2(\alpha) = \alpha\zeta^{5j}$. Since the product of three conjugates of α over F must lie in F, we have that $\alpha^3 \cdot \zeta^{6j} = (\alpha)(\alpha \cdot \zeta^j)(\alpha \cdot \zeta^{5j}) \in F$, which implies that $\alpha^3 \in F$ and we conclude that A splits over a degree-3 extension of the base field.

□

We thank Everett Howe for explaining to us why the case $m = 9$ above does not occur.

3.2. **Zarhin's notion of neatness.** In this section we discuss Zarhin's notion of *neatness*, a useful technical definition closely related to the angle rank. Define

$$R'_A := \{u_j^2 : \alpha_j \in R_A\}. \tag{3.1}$$

Note that according to our numbering convention, we have that $u_j^{-1} = \overline{u}_j = u_{j+g}$ for every $j \in \{1, \dots, g\}$.

Definition 3.2.1 (Zarhin)**.** Let A be an abelian variety defined over $\mathbf{F}_q$. We say that A is neat if it satisfies the following conditions:

(Na) Γ_A is torsion free.
(Nb) For every function $e\colon R'_A \to \mathbf{Z}$ satisfying

$$\prod_{\beta \in R'_A} \beta^{e(\beta)} = 1,$$

then $e(\beta) = e(\beta^{-1})$ for every $\beta \in R'_A$.

Remarks 3.2.2.

(3.2.2.a) If A is supersingular and Γ_A is torsion free, then A is neat. Indeed, in this case we have that $R'_A = \{1\}$ and condition (Nb) is trivially satisfied.
(3.2.2.b) Suppose that the Frobenius eigenvalues of A are distinct and not supersingular. Some base extension of A is neat if and only if A has maximal angle rank.
(3.2.2.c) In general, maximal angle rank always implies neatness.

3.3. **Behavior of Serre–Frobenius groups in products.** We begin by stating an important lemma, attributed to Bjorn Poonen in [KS00].

Lemma 3.3.1 (Poonen)**.** *If $E_1, \dots, E_n$ are n pairwise absolutely non-isogenous elliptic curves over $\mathbf{F}_q$, then their eigenvalues of Frobenius $\alpha_1, \dots, \alpha_n$ are multiplicatively independent.*

In fact, for abelian varieties that split completely as products of elliptic curves, we can give an explicit description of the Serre–Frobenius group.

Proposition 3.3.2. *Let A be a g-dimensional abelian variety over $\mathbf{F}_q$ that splits completely as a product of elliptic curves. Let r be the degree of the smallest extension such that $A \sim_{(r)} A_1 \times B_1 \times B_2 \ldots \times B_s$, satisfying*

- *(i) A_1 is supersingular or trivial,*
- *(ii) each B_j splits over $\mathbf{F}_{q^{rm_j}}$ as the power of an ordinary elliptic curve $E_j/\mathbf{F}_{q^{rm_j}}$, and*
- *(iii) E_j is not geometrically isogenous to E_i for $i \neq j$.*

Let $n_1 \geq 1$ be the smallest integer such that A_1 is isogenous to a power of an elliptic curve E over $\mathbf{F}_{q^{rn_1}}$. Then, $\mathsf{SF}(A) = \mathsf{U}(1)^s \times C_{m_A}$, where

$$m_A = r\,\mathrm{lcm}(n_1 m_E, m_1, m_2, \dots, m_s).$$

The proof of this proposition follows from the following lemmas.

Lemma 3.3.3. *Let $B/\mathbf{F}_q$ be an abelian variety such that B splits completely over $\mathbf{F}_{q^m}$ as a power of an ordinary elliptic curve, for some $m \geq 1$. Then, $\mathsf{SF}(B) = \mathsf{U}(1) \times C_m$.*

Proof. Angle rank is invariant under base change, so $\delta_B = \delta_{E^g} = 1$. It remains to show that the angle torsion order m_B is equal to m. Since $B_{(m)} \sim E^g$, we have that $P_{B,(m)}(T) = P_E(T)^g$. If we denote by $\gamma_1, \overline{\gamma}_1, \dots \gamma_g, \overline{\gamma}_g$ and $\pi_1, \overline{\pi}_1$ the Frobenius eigenvalues of B and E respectively, we have that $\left\{\gamma_1^m, \overline{\gamma}_1^m, \dots, \gamma_g^m, \overline{\gamma}_g^m\right\} = \{\pi_1, \overline{\pi}_1\}$. Possibly after relabelling, we have that $\gamma_j = \zeta_m^{\nu_j}\gamma_1$ for $j = 1, \dots, g$ and at least one $\zeta_m^{\nu_j}$ is a primitive m-th root. This shows that $C_m \subset U_B$, so that $m \mid m_B$. On the other hand, we have that $\mathsf{SF}(B_{(m)}) = \mathsf{SF}(E^g) \cong \mathsf{U}(1)$ is connected. This implies that $m_B \mid m$ and the result follows. $\square$

Lemma 3.3.4. *Let $A = A_1 \times B$ be an abelian variety over $\mathbf{F}_q$ such that A_1 is supersingular with angle torsion order $m_{A_1} = m_1$ and B is simple and splits completely over $\mathbf{F}_{q^m}$ as the power of an ordinary elliptic curve. Then, $\mathsf{SF}(A)^\circ \cong \mathsf{U}(1)$ and $m_A = \mathrm{lcm}(m_1, m)$.*

Proof. From the discussion above, we see that $U_A = \langle \zeta_{m_1}, \zeta_m, v_1 \rangle$, where $v_1 = \gamma_1/\sqrt{q}$ and all the other roots γ_j can be written as $\zeta_m^{\nu_j}\gamma_1$ with at least one $\zeta_m^{\nu_j}$ primitive. It follows that $U_A = C_{\mathrm{lcm}(m_1,m)} \oplus \langle v_1 \rangle$ so that $\delta_A = 1$ and $m_A = \mathrm{lcm}(m_1, m)$. $\square$

Lemma 3.3.5. *If $B/\mathbf{F}_q$ is an ordinary abelian variety such that $B \sim_{(r)} B_1 \times \cdots \times B_s$ and satisfying*

- *(i) each B_j splits over $\mathbf{F}_{q^{m_j}}$ the power of an ordinary elliptic curve $E_j/\mathbf{F}_{q^{m_j}}$, and*
- *(ii) E_j is not geometrically isogenous to E_i for $i \neq j$.*

then $\mathsf{SF}(B) \cong \mathsf{U}(1)^s \times C_{m_B}$ with $m_B = r\,\mathrm{lcm}(m_1, \dots, m_s)$.

Proof. This follows from combining Lemma 3.3.1 with the fact that the Serre–Frobenius group of B is connected over an extension of degree $\mathrm{lcm}(m_1, m_2, \dots, m_s)$. The proof then proceeds as in Lemma 3.3.3. $\square$

3.4. **Supersingular Serre–Frobenius groups.** Recall that a q-Weil number α is called supersingular if $\alpha/\sqrt{q}$ is a root of unity. In [Zhu01, Proposition 3.1], Zhu classified the minimal polynomials $h(T)$ of supersingular q-Weil numbers. Let $\Phi_r(T)$ denote the rth cyclotomic polynomial, $\varphi(r) := \deg \Phi_r(T)$ the Euler totient function, and $\left(\frac{a}{b}\right)$ the Jacobi symbol. Then the possibilities for the minimal polynomials of supersingular q-Weil numbers are given in Table 1.

Table 1. Minimal polynomial of a supersingular q-Weil number α.

Type	d		$h(T)$	Roots
Z-1	Even	-	$\Phi_m^{[\sqrt{q}]}(T) := \sqrt{q}^{\varphi(m)}\Phi_m(T/\sqrt{q})$	$\zeta_m^j\sqrt{q}$ for $j \in (\mathbf{Z}/m\mathbf{Z})^\times$
Z-2	Odd	$\mathbf{Q}(\alpha) \neq \mathbf{Q}(\alpha^2)$	$\Phi_n^{[q]}(T^2) := q^{\varphi(n)}\Phi_n(T^2/q)$	$\pm\zeta_{2n}^j\sqrt{q}$ for $j \in (\mathbf{Z}/n\mathbf{Z})^\times$
Z-3	Odd	$\mathbf{Q}(\alpha) = \mathbf{Q}(\alpha^2)$	$\prod_{\substack{1\leq j\leq n \\ \gcd(j,n)=1}} \left(T - \left(\frac{q}{j}\right)\zeta_m^{\nu j}\sqrt{q}\right)$	$\left(\frac{q}{j}\right)\zeta_m^{\nu j}\sqrt{q}$ for $j \in (\mathbf{Z}/n\mathbf{Z})^\times$

Notation (Table 1). In case (Z-1), m is any positive integer. In cases (Z-2) and (Z-3), m additionally satisfies $m \not\equiv 2 \bmod 4$, and $n := m/\gcd(2,m)$. The symbol ζ_m denotes the primitive m-th root of unity given by $e^{\frac{2\pi i}{m}}$, and ζ_m^ν is also primitive. Note that in this case, $\varphi(n) = \varphi(m)/\gcd(2,m)$. Following the notation in [SMZ14], given a polynomial $f(T) \in K[T]$ for some field K, and a constant $a \in K^\times$, let

$$f^{[a]}(T) := a^{\deg f} f(T/a).$$

Given any supersingular abelian variety A defined over $\mathbf{F}_q$, the Frobenius polynomial $P_A(T)$ is a power of the minimal polynomial $h_A(T)$, and this minimal polynomial is of type (Z-1), (Z-2), or (Z-3) as above. We say that A is of type Z-i if the minimal polynomial $h_A(T)$ is of type (Z-i) for $i = 1, 2, 3$.

Since U_A is finite in the supersingular case, we have that $\mathsf{SF}(A) \cong U_A$. In particular, we can read off the character group U_A from the fourth column in Table 1. For instance, if $m = 3$ and d is even, then we have a polynomial of type Z-1, and the Serre–Frobenius group is isomorphic to C_3. On the other hand, if $m = 3$ and we have a polynomial of type Z-2, then the Serre–Frobenius group is isomorphic to C_6. Given a q-Weil polynomial $f(T) \in \mathbf{Q}[T]$ with roots $\alpha_1, \cdots, \alpha_{2n}$, the associated normalized polynomial $\tilde{f}(T) \in \mathbf{R}[T]$ is the monic polynomial with roots $u_1 = \alpha_1/\sqrt{q}, \ldots, u_{2n} = \alpha_{2n}/\sqrt{q}$. Table 1 allows us to go back and forth between q-Weil polynomials $f(T)$ and the normalized polynomials $\tilde{f}(T)$.

- If $h(T)$ is the minimal polynomial of a supersingular q-Weil number of type Z-1, the normalized polynomial $\tilde{h}(T)$ is the cyclotomic polynomial $\Phi_m(T)$. Conversely, we have that $h(T) = \tilde{h}^{[\sqrt{q}]}(T)$.
- If $h(T)$ is the minimal polynomial of a supersingular q-Weil number of type Z-2, the normalized polynomial $\tilde{h}(T)$ is the polynomial $\Phi_n(T^2)$. Conversely, $h(T) = \tilde{h}^{[q]}(T)$.

4. Elliptic Curves

The goal of this section is to prove Theorem A. Furthermore, we give a thorough description of the set of possible orders m for the supersingular Serre–Frobenius groups $\mathsf{SF}(E) = C_m$ in terms of p and $q = p^d$.

The isogeny classes of elliptic curves over $\mathbf{F}_q$ were classified by Deuring [Deu41] and Waterhouse [Wat69, Theorem 4.1]. Writing the characteristic polynomial of Frobenius as $P(T) = T^2 + a_1T + q$, the Weil bounds give $|a_1| \leq 2\sqrt{q}$. Conversely, the integers a in the interval $|a| \leq 2\sqrt{q}$ corresponding to the isogeny class of an elliptic curve are the following.

Theorem 4.0.1 ([SHOR20, Theorem 2.6.1])**.** *Let p be a prime and $q = p^d$. Let $a \in \mathbf{Z}$ satisfy $|a| \leq 2\sqrt{q}$.*

(1) If $p \nmid a$, then a is the trace of Frobenius of an elliptic curve over $\mathbf{F}_q$. This is the ordinary case.

(2) If $p \mid a$, then a is the trace of Frobenius of an elliptic curve over $\mathbf{F}_q$ if and only if one of the following holds:

(i) d is even and $a = \pm 2\sqrt{q}$,

(ii) d is even and $a = \sqrt{q}$ with $p \not\equiv 1 \bmod 3$,

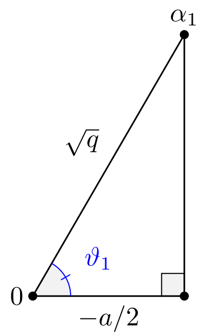
(iii) d is even and $a = -\sqrt{q}$ with $p \not\equiv 1 \bmod 3$,

(iv) d is even and $a = 0$ with $p \not\equiv 1 \bmod 4$,

(v) d is odd and $a = 0$,

(vi) d is odd, $a = \pm\sqrt{2q}$ with $p = 2$.

(vii) d is odd, $a = \pm\sqrt{3q}$ with $p = 3$.
This is the supersingular case.



In the ordinary case, the normalized Frobenius eigenvalue u_1 is not a root of unity, and thus $\mathsf{SF}(E) = \mathsf{U}(1)$. In the supersingular case, the normalized Frobenius eigenvalue u_1 is a root of unity, and thus $\mathsf{SF}(E) = C_m$ is cyclic, with m equal to the order of u_1. For each value of q and a in Theorem 4.0.1 part (2), we get a right triangle of hypotenuse of length $\sqrt{q}$ and base $-a/2$, from which we can deduce the angle ϑ_1 and thus the order m of the corresponding root of unity u_1. We thus obtain the following restatement of Theorem 4.0.1 in terms of the classification of Serre–Frobenius groups for elliptic curves.

TABLE 2. Serre–Frobenius groups of elliptic curves.

Thm. 4.0.1	p	d	a	$\mathsf{SF}(E)$
(1)	-	-	$\gcd(a, p) = 1$	$\mathsf{U}(1)$
2-(i)	-	Even	$\pm 2\sqrt{q}$	C_1
2-(iii)	$p \not\equiv 1 \bmod 3$	Even	$-\sqrt{q}$	C_3
2-(iv)	$p \not\equiv 1 \bmod 4$	Even	0	C_4
2-(v)	-	Odd	0	C_4
2-(ii)	$p \not\equiv 1 \bmod 3$	Even	$\sqrt{q}$	C_6
2-(vi)	2	Odd	$\pm\sqrt{2q}$	C_8
2-(vii)	3	Odd	$\pm\sqrt{3q}$	C_{12}

There are seven Serre–Frobenius groups for elliptic curves, and they correspond to seven possible Frobenius distributions of elliptic curves over finite fields. For ordinary elliptic curves (as explained in Section 1), the sequence of normalized traces $(x_r)_{r=1}^{\infty}$ is equidistributed in the interval $[-2, 2]$ with respect to the measure $\lambda_1(x)$ (Equation 1.1) obtained as the pushforward of the Haar measure $\mu_{\mathsf{U}(1)}$ under $z \mapsto z + \overline{z}$. See Figure 2.

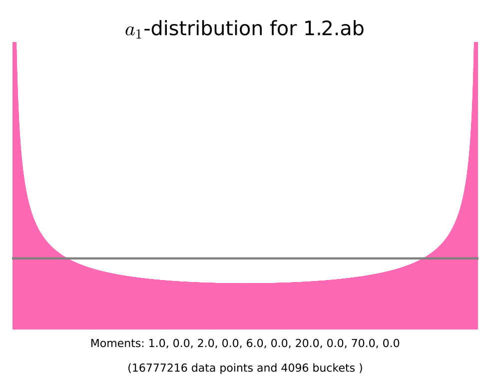
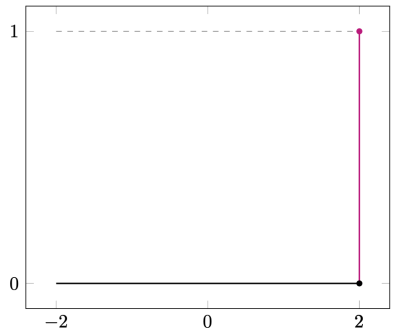


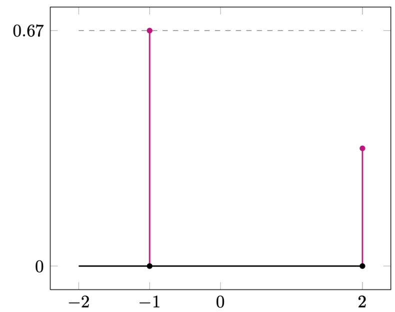
FIGURE 2. a_1-distribution for ordinary elliptic curves.

The remaining six Serre–Frobenius groups are finite and cyclic; they correspond to supersingular elliptic curves. For a given $C_m = \langle \zeta_m \rangle \subset \mathsf{U}(1)$, denote by δ_m the measure obtained by pushforward along $z \mapsto z + \overline{z}$ of the normalized counting measure,

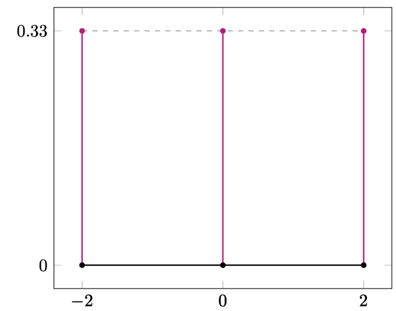
$$\mu_{C_m}(f) := \int f \, \mu_{C_m} := \frac{1}{m} \sum_{j=1}^{m} f(\zeta_m^j). \tag{4.1}$$



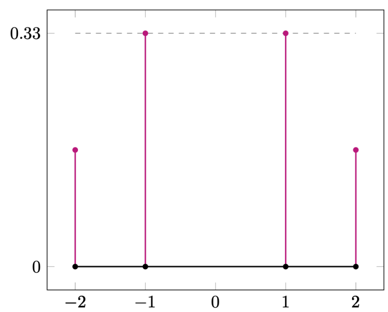
(A) $\mathsf{SF}(E) = C_1$.



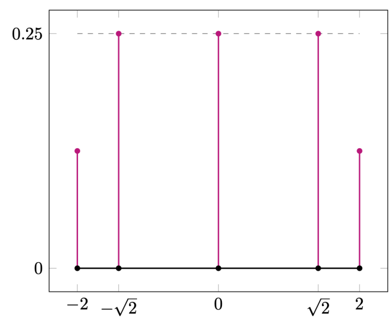
(B) $\mathsf{SF}(E) = C_3$.



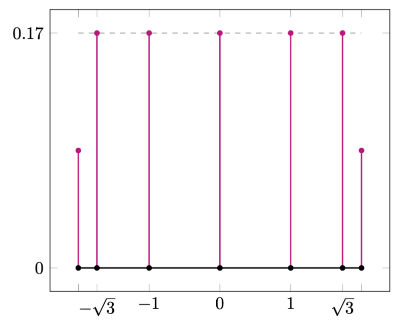
(C) $\mathsf{SF}(E) = C_4$



(D) $\mathsf{SF}(E) = C_6$



(E) $\mathsf{SF}(E) = C_8$



(F) $\mathsf{SF}(E) = C_{12}$.

FIGURE 3. a_1-histograms of supersingular elliptic curves $E/\mathbf{F}_q$.

5. Abelian Surfaces

The goal of this section is to classify the possible Serre–Frobenius groups of abelian surfaces (Theorem B). The proof is a careful case-by-case analysis, described by Flowchart 4.

We separate our cases first according to p-rank, and then according to simplicity. In the supersingular and almost ordinary cases this stratification is enough. In the ordinary case, we have to further consider the geometric isogeny type of the surface.

5.1. Simple ordinary surfaces.

We restate a theorem of Howe and Zhu in our notation.

Theorem 5.1.1 ([HZ02, Theorem 6]). *Suppose that $P(T) = T^4 + a_1T^3 + a_2T^2 + qa_1T + q^2$ is the Frobenius polynomial of a simple ordinary abelian surface S defined over $\mathbf{F}_q$. Then, exactly one of the following conditions holds:*

(a) S is absolutely simple.
(b) $a_1 = 0$ and S splits over a quadratic extension.
(c) $a_1^2 = q + a_2$ and S splits over a cubic extension.
(d) $a_1^2 = 2a_2$ and S splits over a quartic extension.
(e) $a_1^2 = 3a_2 - 3q$ and S splits over a sextic extension.

Lemma 5.1.2 (Node S-A in Figure 4). *Let S be a simple ordinary abelian surface over $\mathbf{F}_q$. Then, exactly one of the following conditions holds:*

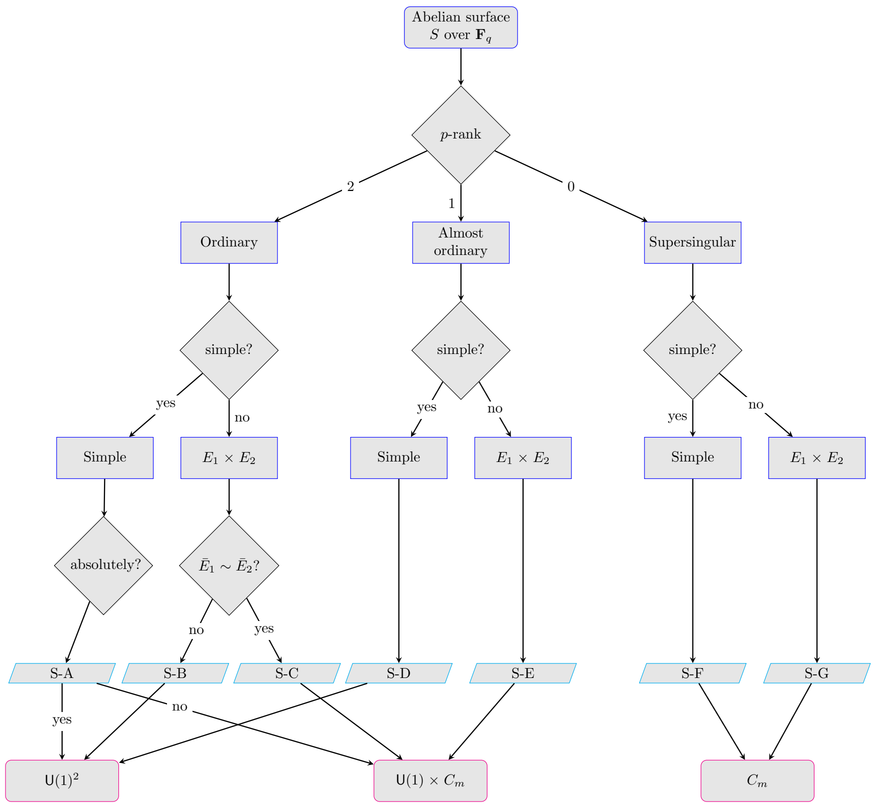


FIGURE 4. Theorem B: Classification in dimension 2.

(a) S is absolutely simple and $\mathsf{SF}(S) \cong \mathsf{U}(1)^2$.
(b) S splits over a quadratic extension and $\mathsf{SF}(S) \cong \mathsf{U}(1) \times C_2$.
(c) S splits over a cubic extension and $\mathsf{SF}(S) \cong \mathsf{U}(1) \times C_3$.
(d) S splits over a quartic extension and $\mathsf{SF}(S) \cong \mathsf{U}(1) \times C_4$.
(e) S splits over a sextic extension and $\mathsf{SF}(S) \cong \mathsf{U}(1) \times C_6$.

TABLE 3. Serre–Frobenius groups of simple ordinary surfaces.

Splitting type	$\mathsf{SF}(S)$	Example
Absolutely simple	$\mathsf{U}(1)^2$	`2.2.ab_b`
Splits over quadratic extension	$\mathsf{U}(1) \times C_2$	`2.2.a_ad`
Splits over cubic extension	$\mathsf{U}(1) \times C_3$	`2.2.ab_ab`
Splits over quartic extension	$\mathsf{U}(1) \times C_4$	`2.3.ac_c`
Splits over sextic extension	$\mathsf{U}(1) \times C_6$	`2.2.ad_f`

Proof.

(a) From [Zar15, Theorem 1.1], we conclude that some finite base extension of an absolutely simple abelian surface is neat and therefore has maximal angle rank by Remark (3.2.2.c). Alternatively, this also follows from the proof of [AS10, Theorem 2] for Jacobians of genus 2 curves, which generalizes to any abelian surface. Theorem E then implies that $\mathsf{SF}(S) = \mathsf{U}(1)^2$.

(b,c,d,e) Denote by m the smallest degree of the extension $\mathbf{F}_{q^m} \supset \mathbf{F}_q$ over which S splits. By Theorem 5.1.1 we know that $m \in \{2,3,4,6\}$. Let $\alpha \in \{\alpha_1, \overline{\alpha}_1, \alpha_2, \overline{\alpha}_2\}$ be a Frobenius eigenvalue of S. From [HZ02, Lemma 4] and since S is ordinary, we have that $[\mathbf{Q}(\alpha) : \mathbf{Q}(\alpha^m)] = [\mathbf{Q}(\alpha^m) : \mathbf{Q}] = 2$. In particular, the minimal polynomial $h_{(m)}(T)$ of α^m is quadratic, and $P_{(m)}(T) = h_{(m)}(T)^2$. This implies that $\{\alpha_1^m, \overline{\alpha}_1^m\} = \{\alpha_2^m, \overline{\alpha}_2^m\}$, so that there is a primitive m-th root of unity ζ giving one of the following multiplicative relations:

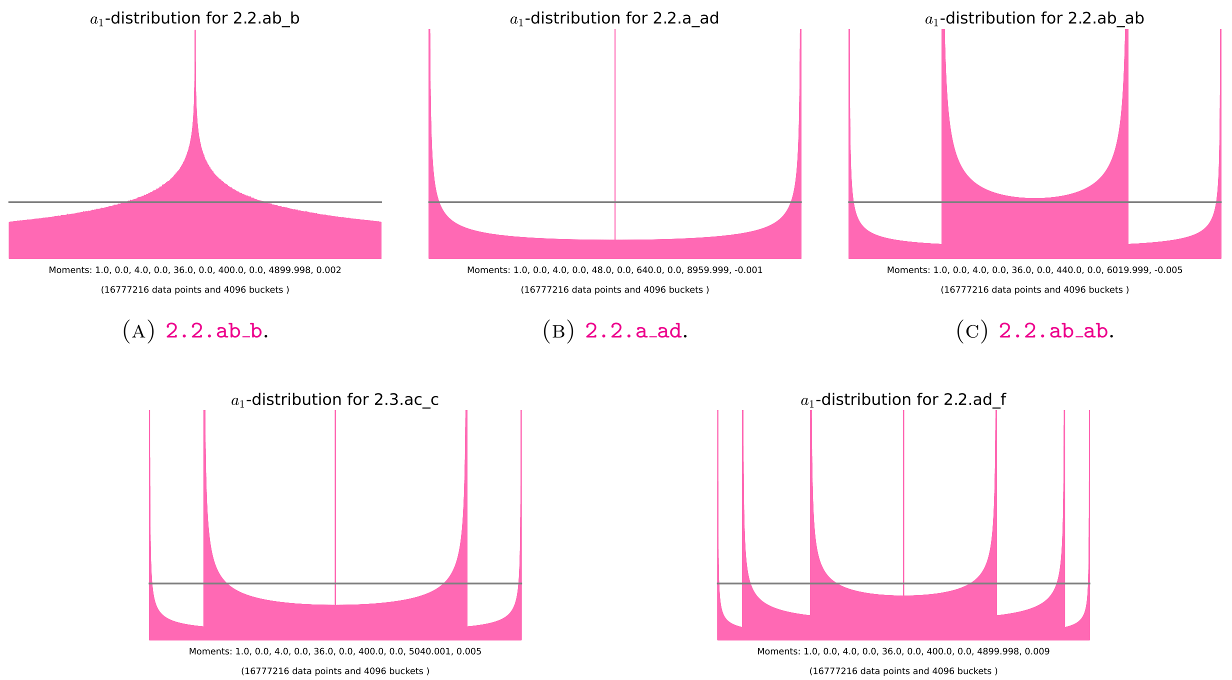
$$\alpha_2 = \zeta\alpha_1, \qquad \alpha_2 = \zeta\overline{\alpha}_1.$$

We note here that ζ must be a primitive m-th root, since otherwise, $P_n(T)$ would split for some $n \leq m$, contradicting the minimality of m. If $\alpha_2 = \zeta\alpha_1$, then

$$\mathsf{SF}(S) = \overline{\langle (u_1, \zeta u_1) \rangle} = \left\{ (u, \zeta^k u) : u \in \mathsf{U}(1), k \in \mathbf{Z}/m\mathbf{Z} \right\} \cong \mathsf{U}(1) \times C_m$$

and $\mathsf{SF}(S)^\circ$ embeds diagonally in $\mathsf{U}(1)^2$. Similarly, if $\alpha_2 = \zeta\overline{\alpha}_1$, then $\mathsf{SF}(S) \cong \mathsf{U}(1) \times C_m$ with embedding $\mathsf{SF}(S) = \left\{ (u, \zeta^k u^{-1}) : u \in \mathsf{U}(1), k \in \mathbf{Z}/m\mathbf{Z} \right\} \subset \mathsf{U}(1)^2$.

□



(A) `2.2.ab_b`. (B) `2.2.a_ad`. (C) `2.2.ab_ab`.

(D) `2.3.ac_c`. (E) `2.2.ad_f`.

FIGURE 5. a_1-histograms for simple ordinary abelian surfaces.

5.2. **Non-simple ordinary surfaces.** Let S be a non-simple ordinary abelian surface defined over $\mathbf{F}_q$. Then, S is isogenous to a product of two ordinary elliptic curves $E_1 \times E_2$. As depicted in Figure 4, we consider two cases:

(S-B) E_1 and E_2 are not isogenous over $\overline{\mathbf{F}}_q$.
(S-C) E_1 and E_2 become isogenous over some base extension $\mathbf{F}_{q^{m_1}} \supseteq \mathbf{F}_q$, for $m_1 \geq 1$.

Lemma 5.2.1 (Node S-B in Figure 4)**.** *Let S be an abelian surface defined over $\mathbf{F}_q$ such that S is isogenous to $E_1 \times E_2$, for E_1 and E_2 absolutely non-isogenous ordinary elliptic curves. Then S has maximal angle rank $\delta = 2$ and $\mathsf{SF}(S) = \mathsf{U}(1)^2$.*

The proof is a straightforward application of Lemma 3.3.1.

Table 4. Serre–Frobenius groups of non-simple ordinary surfaces.

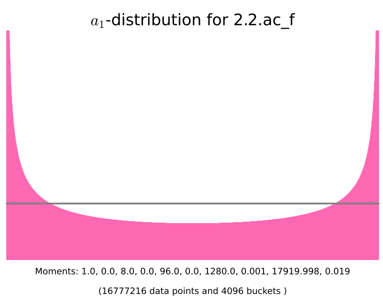
m such that $E_1 \sim_{(m)} E_2$	$\mathsf{SF}(E_1 \times E_2)$	Example
1	$\mathsf{U}(1)$	2.2.ac_f
2	$\mathsf{U}(1) \times C_2$	2.2.a_d
3	$\mathsf{U}(1) \times C_3$	2.7.af_s
4	$\mathsf{U}(1) \times C_4$	2.5.ag_s
6	$\mathsf{U}(1) \times C_6$	2.7.aj_bi

Lemma 5.2.2 (Node S-C in Figure 4)**.** *Let S be an abelian surface defined over $\mathbf{F}_q$ such that S is isogenous to $E_1 \times E_2$, for E_1 and E_2 absolutely isogenous ordinary elliptic curves. Then S has angle rank $\delta = 1$ and $\mathsf{SF}(S) = \mathsf{U}(1) \times C_m$ for $m \in \{1, 2, 3, 4, 6\}$. Furthermore, m is precisely the degree of the extension of $\mathbf{F}_q$ over which E_1 and E_2 become isogenous.*

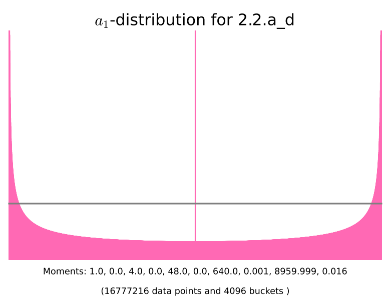
Proof. Let $\alpha_1, \overline{\alpha}_1$ and $\alpha_2, \overline{\alpha}_2$ denote the Frobenius eigenvalues of E_1 and E_2 respectively. Let m_1 be the smallest positive integer such that $E_1 \sim_{(m_1)} E_2$. From Proposition 3.3.2, we immediately have that $\mathsf{SF}(S) \cong \mathsf{U}(1) \times C_m$, where $m = m_1$. In order to find the value of m, observe that $\{\alpha_1^m, \overline{\alpha}_1^m\} = \{\alpha_2^m, \overline{\alpha}_2^m\}$, from which we get one of the following multiplicative relations:

$$\alpha_2 = \zeta\alpha_1, \qquad \alpha_2 = \zeta\overline{\alpha}_1, \tag{5.1}$$

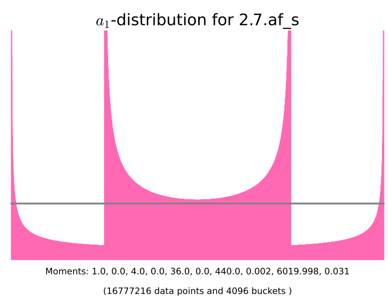
for some primitive m-th root of unity ζ. Since the curves E_1 and E_2 are ordinary, the number fields $\mathbf{Q}(\alpha_1)$ and $\mathbf{Q}(\alpha_2)$ are imaginary quadratic and $\mathbf{Q}(\alpha_1) = \mathbf{Q}(\alpha_1^m) = \mathbf{Q}(\alpha_2^m) = \mathbf{Q}(\alpha_2)$. Hence, $\zeta \in \mathbf{Q}(\alpha_1)$ and thus $\varphi(m) = [\mathbf{Q}(\zeta) : \mathbf{Q}] \in \{1, 2\}$; therefore $m \in \{1, 2, 3, 4, 6\}$. Depending on whether $\alpha_2 = \zeta\alpha_1$ or $\alpha_2 = \zeta\overline{\alpha}_1$, the group $\mathsf{SF}(S) = \mathsf{U}(1) \times C_m$ embeds in $\mathsf{U}(1)^2$ as $(u, \zeta^r) \mapsto (u, \zeta^r u)$ or $(u, \zeta^r) \mapsto (u, \zeta^r u^{-1})$. $\square$



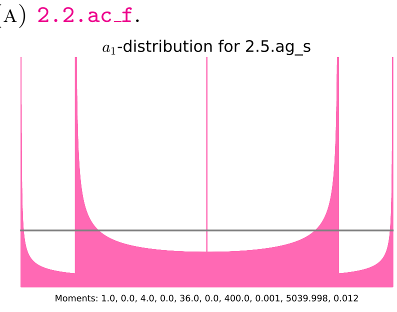
(A) 2.2.ac_f.



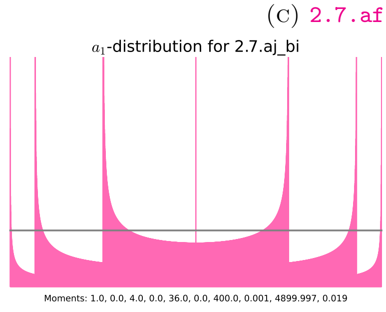
(B) 2.2.a_d.



(C) 2.7.af_s



(D) 2.5.ag_s



(E) 2.7.aj_bi.

Figure 6. a_1-histograms of non-simple ordinary abelian surfaces.

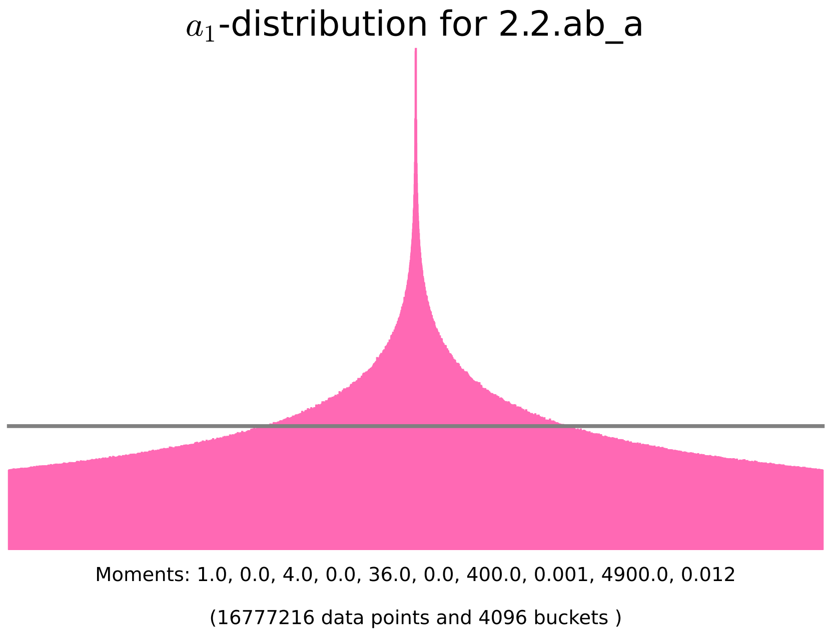


FIGURE 7. a_1-histogram of simple almost ordinary abelian surface 2.2.ab_a.

5.3. **Simple almost ordinary surfaces.** An abelian variety is called almost ordinary if the set of slopes of the Newton polygon is $\{0, 1/2, 1\}$ and the slope $1/2$ has length 2. In [LZ93] Lenstra and Zarhin carried out a careful study of the multiplicative relations of Frobenius eigenvalues of simple almost ordinary varieties, which was later generalized in [DKZB21]. In particular, they prove that even-dimensional simple almost ordinary abelian varieties have maximal angle rank ([LZ93, Theorem 5.8]). Since every abelian surface of p-rank 1 is almost ordinary, their result allows us to deduce the following:

Lemma 5.3.1 (Node S-D in Figure 4)**.** *Let S be a simple and almost ordinary abelian surface defined over $\mathbf{F}_q$. Then, S has maximal angle rank $\delta = 2$ and $\mathsf{SF}(S) = \mathsf{U}(1)^2$.*

5.4. **Non-simple almost ordinary surfaces.** If S is almost ordinary and not simple, then S is isogenous to the product of an ordinary elliptic curve E_1 and a supersingular elliptic curve E_2.

Lemma 5.4.1 (Node S-E in Figure 4)**.** *Let S be a non-simple almost ordinary abelian surface defined over $\mathbf{F}_q$. Then, S has angle rank $\delta = 1$ and $\mathsf{SF}(S) \cong \mathsf{U}(1) \times C_m$ for some $m \in \{1, 3, 4, 6, 8, 12\}$.*

Proof. Let E_1 be an ordinary elliptic curve and E_2 a supersingular elliptic curve such that $S \sim E_1 \times E_2$. By Proposition 3.3.2, $\mathsf{SF}(S) = \mathsf{SF}(E_1) \times \mathsf{SF}(E_2) \cong \mathsf{U}(1) \times C_m$ with m in the list of possible orders of Serre–Frobenius groups of supersingular elliptic curves. $\square$

5.5. **Simple supersingular surfaces.** Since every supersingular abelian variety is geometrically isogenous to a power of an elliptic curve, the Serre–Frobenius group only depends on the extension over which this occurs (Proposition 3.3.2). We separate our analysis into the simple and non-simple cases.

The classification of Frobenius polynomials of supersingular abelian surfaces over finite fields was completed by Maisner and Nart [MN02, Theorem 2.9] building on work of Xing [Xin96] and Rück [R9̈0]. Denoting by (a_1, a_2) the isogeny class of abelian surfaces over $\mathbf{F}_q$ with Frobenius polynomial $P_S(T) = T^4 + a_1T^3 + a_2T^2 + qa_1T + q^2$, the following lemma gives the classification of Serre–Frobenius groups of simple supersingular surfaces.

Lemma 5.5.1 (Node S-F in Table 4)**.** *Let S be a simple supersingular abelian surface defined over $\mathbf{F}_q$. The Serre–Frobenius group of S is classified according to Table 5.*

TABLE 5. Serre–Frobenius groups of simple supersingular surfaces.

(a_1, a_2)	p	d	e	Type	$\tilde{h}(T)$	$\mathsf{SF}(S)$
$(0,0)$	$\not\equiv 1 \bmod 8$	even	1	Z-1	$\Phi_8(T)$	C_8
$(0,0)$	$\neq 2$	odd	1	Z-2	$\Phi_8(T)$	C_8
$(0,q)$	-	odd	1	Z-2	$\Phi_3(T^2)$	C_6
$(0,-q)$	$\not\equiv 1 \bmod 12$	even	1	Z-1	$\Phi_{12}(T)$	C_{12}
$(0,-q)$	$\neq 3$	odd	1	Z-2	$\Phi_6(T^2) = \Phi_{12}(T)$	C_{12}
$(\sqrt{q}, q)$	$\not\equiv 1 \bmod 5$	even	1	Z-1	$\Phi_5(T)$	C_5
$(-\sqrt{q}, q)$	$\not\equiv 1 \bmod 5$	even	1	Z-1	$\Phi_{10}(T) = \Phi_5(-T)$	C_{10}
$(\sqrt{5q}, 3q)$	$= 5$	odd	1	Z-3	$\Psi_{5,1}(T)$	C_{10}
$(-\sqrt{5q}, 3q)$	$= 5$	odd	1	Z-3	$\Psi_{5,1}(-T)$	C_{10}
$(\sqrt{2q}, q)$	$= 2$	odd	1	Z-3	$\Psi_{2,3}(T)$	C_{24}
$(-\sqrt{2q}, q)$	$= 2$	odd	1	Z-3	$\Psi_{2,3}(-T)$	C_{24}
$(0,-2q)$	-	odd	2	Z-2	$\Phi_1(T^2)$	C_2
$(0,2q)$	$\equiv 1 \bmod 4$	even	2	Z-1	$\Phi_4(T)$	C_4
$(2\sqrt{q}, 3q)$	$\equiv 1 \bmod 3$	even	2	Z-1	$\Phi_3(T)$	C_3
$(-2\sqrt{q}, 3q)$	$\equiv 1 \bmod 3$	even	2	Z-1	$\Phi_6(T) = \Phi_3(-T)$	C_6

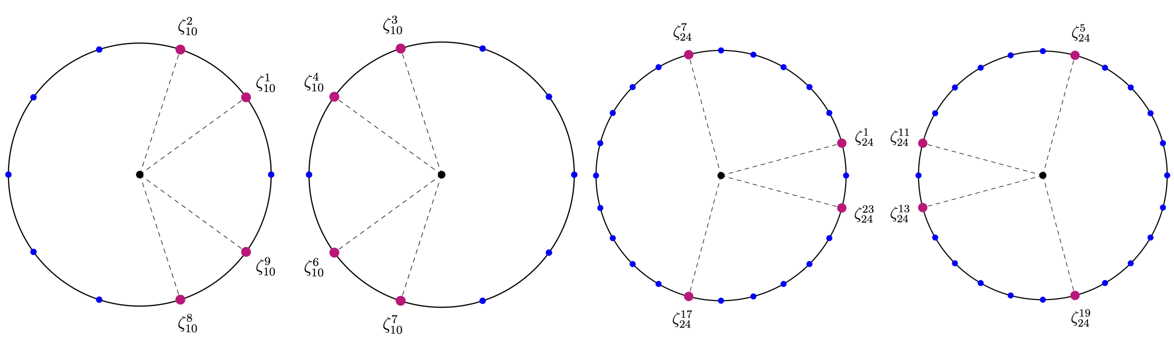
The notation for polynomials of type Z-3 is taken from [SMZ14], where the authors classify simple supersingular Frobenius polynomials for $g \leq 7$. We have

$$\Psi_{5,1}(T) := \prod_{a \in (\mathbf{Z}/5)^\times} \left(T - \left(\tfrac{a}{5}\right)\zeta_5^a\right) = T^4 + \sqrt{5}T^3 + 3T^2 + \sqrt{5}T + 1, \tag{5.2}$$

and

$$\Psi_{2,3}(T) := \prod_{a \in (\mathbf{Z}/3)^\times} \left(T - \zeta_8\zeta_3^a\right)\left(T - \overline{\zeta}_8\zeta_3^a\right) = T^4 + \sqrt{2}T^3 + T^2 + \sqrt{2}T + 1. \tag{5.3}$$

We exhibit the proof of the second line in Table 5 for exposition. The remaining cases can be checked similarly. If $(a_1, a_2) = (0,0)$, $p \neq 2$ and q is an odd power of p: then, $P(T) = T^4 + q^2 = \sqrt{q}^4\Phi_8(T/\sqrt{q}) = q^2\Phi_4(T^2/q)$ and $\tilde{h}(T) = \Phi_8(T)$. Thus U_S is generated by a primitive 8th root of unity.

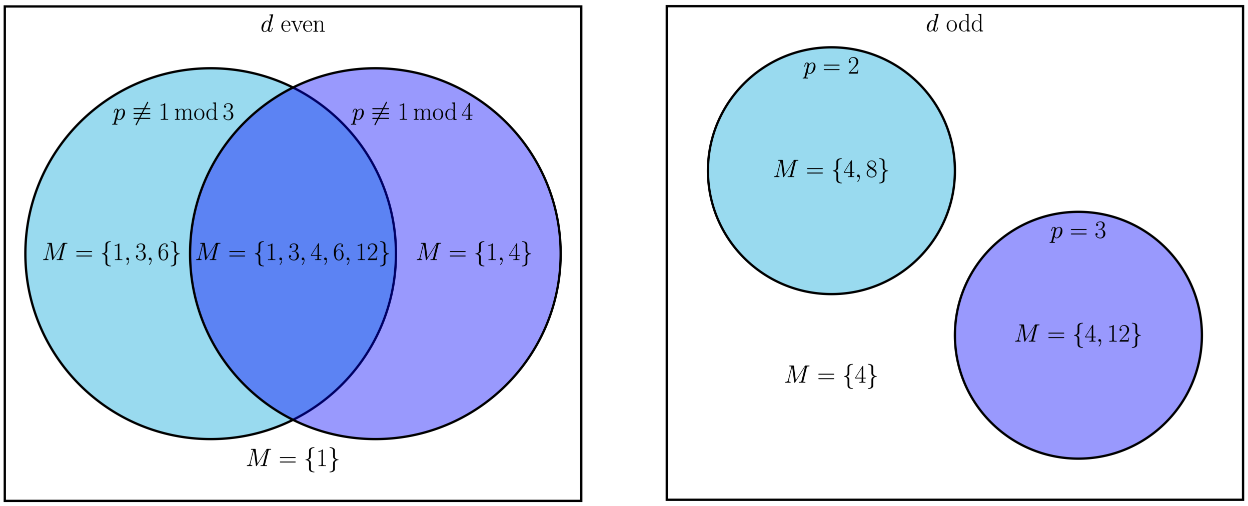


(A) $\Psi_{5,1}(T)$. (B) $\Psi_{5,1}(-T)$. (C) $\Psi_{2,3}(T)$. (D) $\Psi_{2,3}(-T)$.

FIGURE 8. Roots of Z-3 type normalized Frobenius polynomials in Table 5.

5.6. **Non-simple supersingular surfaces.** If S is a non-simple supersingular surface, then S is isogenous to a product of two supersingular elliptic curves E_1 and E_2. If m_{E_1} and m_{E_2} denote the torsion orders of E_1 and E_2 respectively, then the extension over which E_1 and E_2 become isogenous is precisely $\mathrm{lcm}(m_{E_1}, m_{E_2})$. Thus, by Proposition 3.3.2, we have the following result, depending on the values of $q = p^d$ as in Table 2.

Lemma 5.6.1 (Node S-G in Figure 4)**.** *Let S be a non-simple supersingular abelian surface defined over $\mathbf{F}_q$. Then, S has angle rank $\delta = 0$ and $\mathsf{SF}(S) = C_m$ for m in the set $M = M(p,d)$ described in Figure 9.*



(A) When q is a square.

(B) When q is not a square.

Figure 9. Sets M of possible orders of the Serre–Frobenius groups of non-simple supersingular surfaces as a function of p and $q = p^d$.

6. Abelian Threefolds

In this section, we classify the Serre–Frobenius groups of abelian threefolds (see Figure 10). Let X be an abelian variety of dimension 3 defined over $\mathbf{F}_q$. For our analysis, we will first stratify the cases by p-rank and then by simplicity. Before we proceed, we make some observations about simple threefolds that will be useful later.

6.1. **Simple abelian threefolds.** If X is a simple abelian threefold, there are only two possibilities for the Frobenius polynomial $P_X(T) = h_X(T)^e$:

$$P_X(T) = h_X(T) \tag{6.1}$$

$$P_X(T) = h_X(T)^3. \tag{6.2}$$

Indeed, if $h_X(T)$ were a linear or cubic polynomial, it would have a real root, $\pm\sqrt{q}$. By an argument of Waterhouse ([Wat69, Chapter 2]), the q-Weil numbers $\pm\sqrt{q}$ must come from simple abelian varieties of dimension 1 or 2. Further, Xing [Xin94] showed that 6.2 can only happen in very special cases (see also [Hal10, Proposition 1.2]).

Theorem 6.1.1 ([Xin94], [Hal10, Prop 1.2])**.** *Let X be a simple abelian threefold over $\mathbf{F}_q$. Then, $P_X(T) = h_X(T)^3$ if and only if 3 divides $\log_p(q)$ and $h_X(T) = T^2 + aq^{1/3}T + q$ with $\gcd(a,p) = 1$.*

Note that in this case, X is non-supersingular and has Newton Polygon as in Figure 16.

Further, putting these observations together gives us that every simple abelian threefold is either absolutely simple or is isogenous over an extension to the cube of an elliptic curve. Thus, we have the following fact.

Fact 6.1.2. If X is an abelian threefold defined over $\mathbf{F}_q$ that is not ordinary or supersingular, then X is simple if and only if it is absolutely simple.

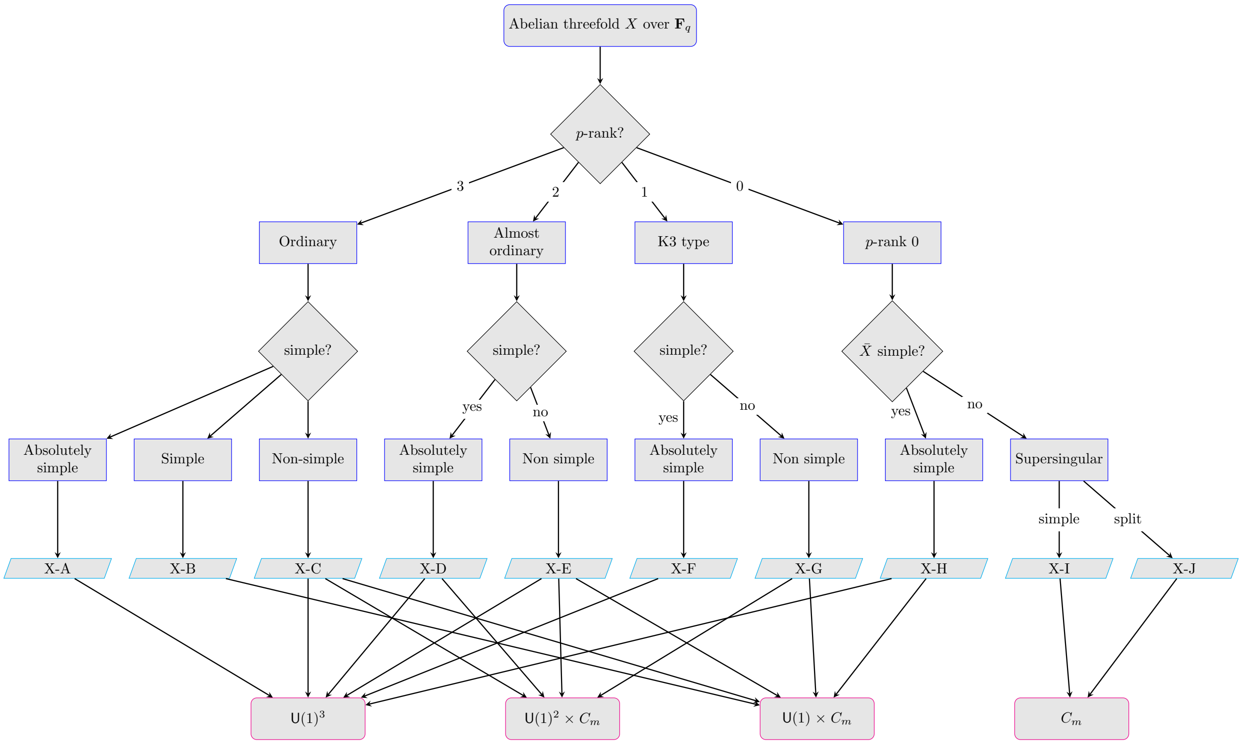


FIGURE 10. Theorem C: Classification in dimension 3

6.2. **Simple ordinary threefolds.** In this section, X will denote a simple ordinary threefold defined over $\mathbf{F}_q$. As a corollary to Theorem 3.1.1, we have the following.

Proposition 6.2.1. *Let X be a simple ordinary abelian threefold defined over $\mathbf{F}_q$. Then, exactly one of the following conditions is satisfied.*

(1) X is absolutely simple.
(2) X splits over a degree 3 extension and $P_X(T) = T^6 + a_3T^3 + q^3$.
(3) X splits over a degree 7 extension and the number field of $P_X(T)$ is $\mathbf{Q}(\zeta_7)$.

Lemma 6.2.2 (Node X-A in Figure 10)**.** *Let X be an absolutely simple abelian threefold defined over $\mathbf{F}_q$. Then X has maximal angle rank $\delta = 3$ and $\mathsf{SF}(X) = \mathsf{U}(1)^3$.*

Proof. Let $m = m_X$ be the order of the torsion subgroup of Γ_X. By [Zar15, Theorem 1.1], we have that $X_{(m)}$ is neat. Since $X_{(m)}$ is ordinary and simple, its Frobenius eigenvalues are distinct and non-real. Remark (3.2.2.b) implies that $X_{(m)}$ has maximal angle rank. Since angle rank is invariant under base extension (Remark 2.2.3) we have that $\delta(X) = \delta(X_{(m)}) = 3$ as we wanted to show. □

Lemma 6.2.3. *Let X be a simple ordinary abelian threefold over $\mathbf{F}_q$ that is not absolutely simple. Then X has angle rank 1 and*

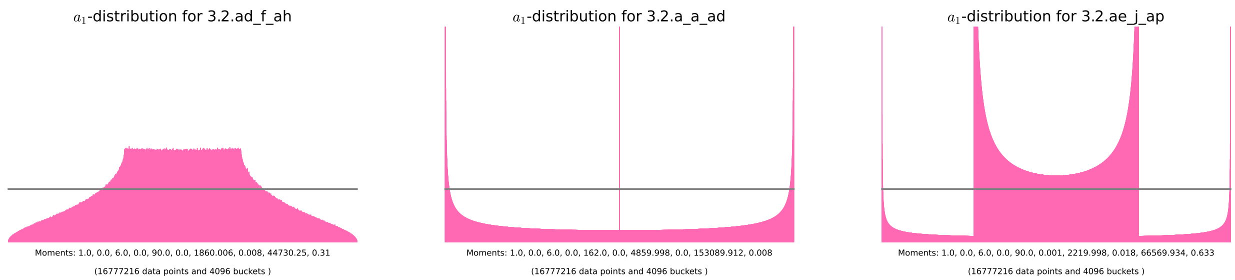
(a) $\mathsf{SF}(X) = \mathsf{U}(1) \times C_3$ if X splits over a degree 3 extension, or
(b) $\mathsf{SF}(X) = \mathsf{U}(1) \times C_7$ if X splits over a degree 7 extension.

Proof. From the proof of Theorem 3.1.1, we have that the torsion free part of U_X is generated by a fixed normalized root $u_1 = \alpha_1/\sqrt{q}$, and all other roots u_j for $1 < j \leq g$ are related to u_1 by a primitive root of unity of order 3 or 7 respectively. □

Example 6.2.4. The isogeny class 3.2.ad_f_ah is ordinary and absolutely simple. According to Lemma 6.2.3, its Serre–Frobenius group is the full torus $\mathsf{U}(1)^3$ and the following histogram approximates the distribution corresponding to the measure λ_3.

Example 6.2.5. The isogeny class 3.2.a_a_ad is ordinary and simple, but it splits over a degree 3 extension as $\texttt{1.8.ad}^3$. According to Lemma 6.2.3, its Serre–Frobenius group is $\mathsf{U}(1) \times C_3$, and the histogram corresponding to this group is the following.

Example 6.2.6. The isogeny class 3.2.ae_j_ap is ordinary and simple, but it splits over a degree 7 extension as $\texttt{1.128.an}^3$. According to Lemma 6.2.3, its Serre–Frobenius group is $\mathsf{U}(1) \times C_7$, and the histogram corresponding to this group is the following.



(A) a_1-histogram of 3.2.ad_f_ah. (B) a_1-histogram of 3.2.a_a_ad. (C) a_1 histogram of 3.2.ae_j_ap.

FIGURE 11. a_1-distributions for simple ordinary threefolds.

6.3. **Non-simple ordinary threefolds.** Let X be a non-simple ordinary threefold defined over $\mathbf{F}_q$. Then X is isogenous to a product $S \times E$, for some ordinary surface S and some ordinary elliptic curve E.

The Frobenius polynomial of X is the product of the Frobenius polynomials of S and E. Further, exactly one of the following is true for S: either it is absolutely simple, or it is simple and geometrically isogenous to the power of a single elliptic curve, or it is not simple (see observation after 5.1.2). The Serre–Frobenius group of X depends on its geometric isogeny decomposition, of which there are four possibilities:

(6.3-a) X is geometrically isogenous to E^3.

(6.3-b) X is geometrically isogenous to $E_1^2 \times E$, for some ordinary elliptic curve E_1, with $E_1 \not\sim_{\overline{\mathbf{F}}_q} E$.

(6.3-c) X is geometrically isogenous to $E_1 \times E_2 \times E$, for ordinary and pairwise geometrically non-isogenous elliptic curves E_1, E_2 and E.

(6.3-d) X is geometrically isogenous to $S \times E$ for an absolutely simple ordinary surface S and an ordinary elliptic curve E.

Lemma 6.3.1. *Let X be a non-simple ordinary abelian threefold over $\mathbf{F}_q$. The Serre–Frobenius group of X is given by Table 6.*

TABLE 6. Serre–Frobenius groups of non-simple ordinary threefolds.

Geometric isogeny type	δ_X	M
(6.3-a)	1	$\{1, 2, 3, 4, 6\}$
(6.3-b)	2	$\{1, 2, 3, 4, 6\}$
(6.3-c)	3	$\{1\}$
(6.3-d)	3	$\{1\}$

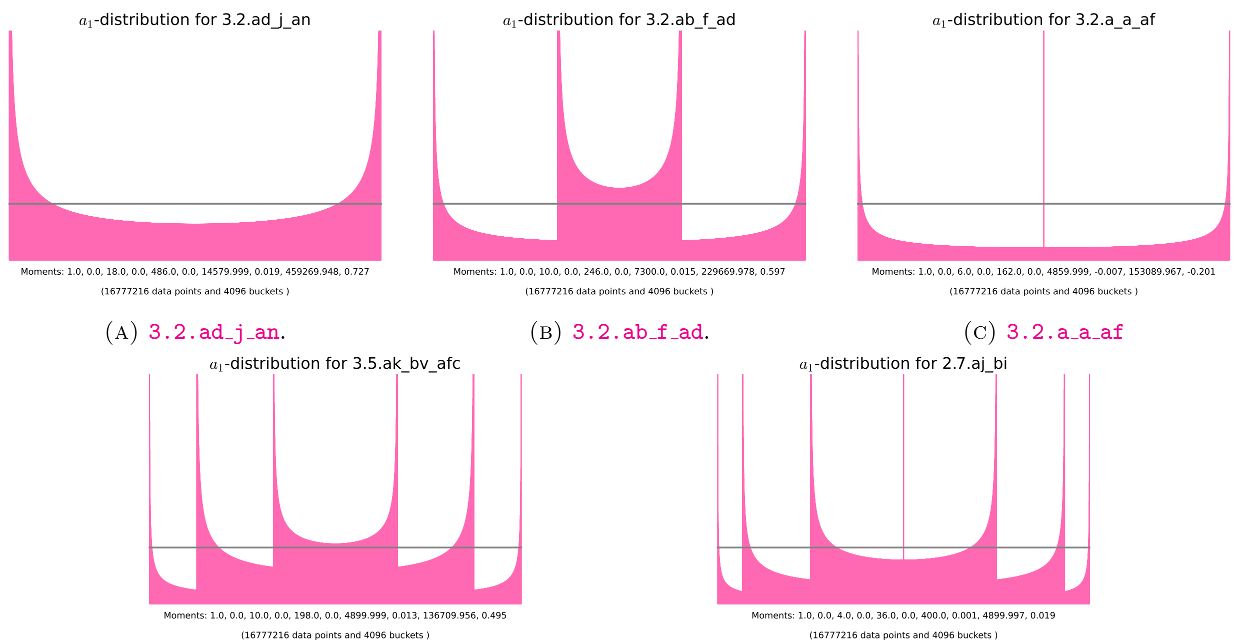
Proof. Recall that $X \sim S \times E$ over $\mathbf{F}_q$.
(6.3-a) If X is geometrically isogenous to E^3, then S is geometrically isogenous to E^2. By Proposition 3.3.2 $\mathsf{SF}(X) = \mathsf{U}(1) \times C_m$, where m is the smallest extension over which $S \sim_{(m)} E^2$. By [HZ02, Theorem 6], we have that $m \in \{1, 2, 3, 4, 6\}$.
(6.3-b)

In this case, by Proposition 3.3.2, $\mathsf{SF}(X) = \mathsf{U}(1)^2 \times C_m$, where m is the smallest extension over which $S \sim_{(m)} E_1^2$. As in the previous case, $m \in \{1, 2, 3, 4, 6\}$.

(6.3-c) In this case $S \sim E_1 \times E_2$ over the base field. By Lemma 3.3.1 we conclude that $\delta_X = 3$.
(6.3-d) In this case, $X \sim S \times E$ with S absolutely simple. By [Zar15, Theorem 1.1], we know that X is neat. Since X is ordinary and S is simple, all Frobenius eigenvalues are distinct and not supersingular. By Remark (3.2.2.b), we conclude that $\delta_X = 3$. $\square$

Example 6.3.2 (Non-simple ordinary threefolds of splitting type (6.3-a)).

($m = 1$) The isogeny class `3.2.ad_j_an` is isogenous over the field of definition to `1.2.ab`^{3}.
($m = 2$) The base change of `3.2.ab_f_ad` over a quadratic extension is `1.4.d`^{3}.
($m = 3$) The base change of `3.2.a_a_af` over a cubic extension is `1.8.af`^{3}.
($m = 4$) The base change of `3.5.ak_bv_afc` over a quartic extension is `1.625.o`^{3}.
($m = 6$) The base change of `3.7.ao_di_alk` over a degree 6 extension is `1.117649.la`^{3}.



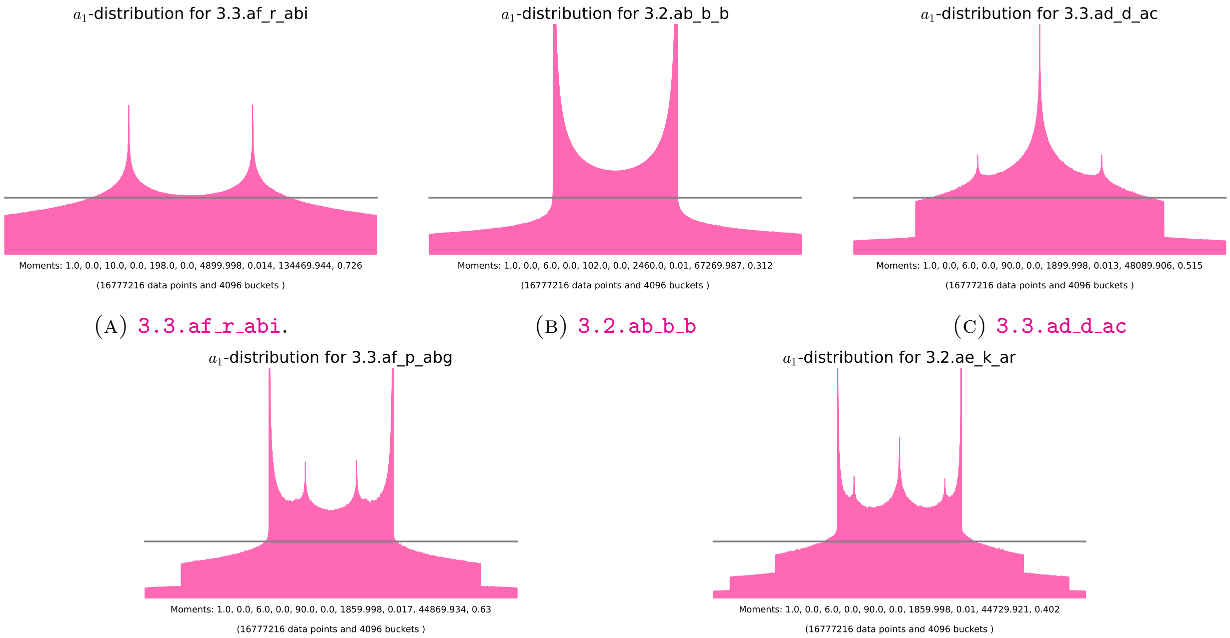
(A) `3.2.ad_j_an`. (B) `3.2.ab_f_ad`. (C) `3.2.a_a_af`

(D) `3.5.ak_bv_afc` (E) `3.7.ao_di_alk`.

FIGURE 12. a_1-distributions for non-simple ordinary abelian threefolds of splitting (6.3-a).

Example 6.3.3 (Non-simple ordinary threefolds of splitting type (6.3-b)).

($m = 1$) The isogeny class `3.3.af_r_abi` is isogenous to `1.3.ac`$^2 \times$ `1.3.ab`.
($m = 2$) The base change of `3.2.ab_b_b` over a quadratic extension is `1.4.ab`$^2 \times$ `1.4.d`.
($m = 3$) The base change of `3.3.ad_d_ac` over a cubic extension is `1.27.ai`$^2 \times$ `1.27.k`.
($m = 4$) The base change of `3.3.af_p_abg` over a quartic extension is `1.81.ao`$^2 \times$ `1.81.ah`.
($m = 6$) The base change of `3.2.ae_k_ar` over a sextic extension is `1.64.l`$^2 \times$ `1.64.aj`.



(A) `3.3.af_r_abi`. (B) `3.2.ab_b_b` (C) `3.3.ad_d_ac`

(D) `3.3.af_p_abg` (E) `3.2.ae_k_ar`

FIGURE 13. a_1-distributions for non-simple ordinary abelian threefolds of splitting (6.3-b).

6.4. **Simple almost ordinary threefolds.** Let X be a simple and almost ordinary abelian threefold over $\mathbf{F}_q$. Recall that X is in fact absolutely simple, so that the Frobenius polynomial $P_{(r)}(T)$ is irreducible for every positive integer r.

TABLE 7. Serre–Frobenius groups of simple almost ordinary threefolds.

Neat	$\sqrt{q} \in \mathbf{Q}(\alpha)$	δ_X	M
Yes	-	3	$\{1\}$
No	Yes	2	$\{1, 2, 3, 4, 6\}$
No	No	2	$\{1, 2, 3, 4, 6, 8, 12\}$

Lemma 6.4.1. *Let X be a simple almost ordinary abelian threefold over $\mathbf{F}_q$. The Serre–Frobenius group of X can be read from Table 7.*

Proof. Let $m := m_X$ be the torsion order of U_X, and consider the base extension $Y := X_{(m)}$. By [LZ93, Theorem 5.7], we know that $\delta_X = \delta_Y \geq 2$. Furthermore, since Y is absolutely simple, by the discussion in Section 6.1, the roots of $P_Y(T) = P_{(m)}(T)$ are distinct and non-supersingular. If Y is neat, Remark (3.2.2.b) implies that $\delta_X = \delta_Y = 3$. Assume then that Y is not neat, so that $\delta_X = 2$. Let $\alpha = \alpha_1$ be a Frobenius eigenvalue of X. By [Zar15, Theorem 1.1] and the discussion thereafter, we have that the sextic CM-field $\mathbf{Q}(\alpha) = \mathbf{Q}(\alpha^m)$ contains a quadratic imaginary field B, and $(u_1u_2u_3)^{2m} = \mathrm{Norm}_{\mathbf{Q}(\alpha)/B}(u_1^{2m}) = 1$. Since U_Y has no torsion, this implies that $(u_1u_2u_3)^m = 1$. Moreover, this means that $u_1u_2u_3 = \zeta$ for some primitive[4] m-th root of unity ζ. Therefore,

$$\zeta^2 = \mathrm{Norm}_{\mathbf{Q}(\alpha)/B}(u_1^2) \in B. \tag{6.3}$$

[4]The primitivity of ζ follows from the fact that m is the minimal positive integer such that $U_{(m)}$ is torsion free.

If m is odd, ζ^2 is also primitive, so that $\varphi(m) \leq 2$ and $m \in \{1,3\}$. If m is even, then we may distinguish between two cases. If $\sqrt{q} \in \mathbf{Q}(\alpha)$, we know that $u_1 \in \mathbf{Q}(\alpha)$ so that in fact $\pm\zeta = \mathrm{Norm}_{\mathbf{Q}(\alpha)/B}(u_1) \in B$ and $\varphi(m) \leq 2$ implies that $m \in \{2,4,6\}$. If $\sqrt{q} \notin \mathbf{Q}(\alpha)$, then ζ^2 is a primitive $m/2$-root of unity and $m/2 \in \{1,2,3,4,6\}$. ☐

6.5. **Non-simple almost ordinary threefolds.** Since X is not simple, we have that $X \sim S \times E$ for some surface S and some elliptic curve E. For this section, we let $\pi_1, \overline{\pi}_1, \pi_2, \overline{\pi}_2$ and $\alpha, \overline{\alpha}$ be the Frobenius eigenvalues of S and E respectively. The normalized eigenvalues will be denoted by $u_1 := \pi_1/\sqrt{q}, u_2 = \pi_2/\sqrt{q}$ and $u := \alpha/\sqrt{q}$. Instead of paragraph below: if X has a geometric supersingular factor, by Honda–Tate theory, it must have a supersingular factor over the base field; and without loss of generality we may assume that this factor is E.

Lemma 6.5.1. *Let $X \sim S \times E$ be a non-simple almost ordinary abelian threefold over $\mathbf{F}_q$. The Serre–Frobenius group of X can be read from Flowchart 14. In particular, if X has no supersingular factor, then $\delta_X = 3$. If E is supersingular, then $\delta_X \in \{1,2\}$ and $m_X = \mathrm{lcm}(m_S, m_E)$. The list of possible torsion orders m_X in this case is given by:*

(1) $\delta_X = 1$, d even: $M(p,d) = \{1,2,3,4,6,12\}$.
(2) $\delta_X = 1$, d odd: $M(p,d) = \{4,12,24\}$.
(3) $\delta_X = 2$: All possible orders in Table 2.

Proof. First, suppose that X has no supersingular factor. Thus E is ordinary and S is almost ordinary and absolutely simple. This implies that $\mathbf{Q}(\pi_1^r)$ and $\mathbf{Q}(\alpha^r)$ are CM-fields of degrees 4 and 2 respectively, for every positive integer r. In particular, $\#\{\pi_1^r, \overline{\pi}_1^r, \pi_2^r, \overline{\pi}_2^r, \alpha^r, \overline{\alpha}^r\} = 6$ for every r. Let $m = m_X$ and consider the base extension $X_{(m)}$. Since $X_{(m)}$ is not simple, [Zar15, Theorem 1.1] implies that $X_{(m)}$ is neat. The eigenvalues of $X_{(m)}$ are all distinct and not supersingular, so that $\delta(X) = \delta(X_{(m)}) = 3$ by Remark (3.2.2.b).

Now, suppose that X does have a supersingular factor, namely E. This implies that $\delta_X \leq 2$ since $u = \alpha/\sqrt{q} = \zeta_{m_E}$ is a root of unity. Since S is ordinary in this case, we have that the sets $\{u_1, u\}$ and $\{u_2, u\}$ are multiplicatively independent, so that $\delta_X = 1$ or 2 depending on the rank of the subgroup $U_S \subset U_X$. Similarly, we see that $U_X[\mathrm{tors}] = \langle \zeta_{m_S}, \zeta_{m_E} \rangle$ and $m_X = \mathrm{lcm}(m_S, m_E)$. If S is simple, the result follows from Lemma 5.1.2. If S is not simple, the result follows from 5.2.1. ☐

6.6. **Abelian threefolds of K3-type.** In this section X will be an abelian threefold defined over $\mathbf{F}_q$ of p-rank 1. The q-Newton polygon of such a variety is give in Figure 15. This is the three-dimensional instance of abelian varieties of K3 type, which were studied by Zarhin in [Zar93] and [Zar91].

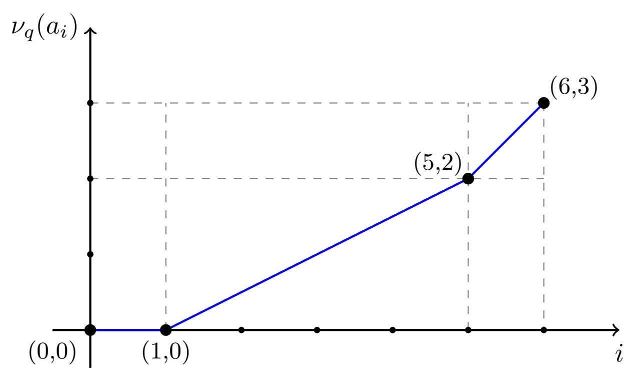


FIGURE 15. q-Newton polygon of p-rank 1 abelian threefolds.

Definition 6.6.1. An abelian variety A defined over $\mathbf{F}_q$ is said to be of K3-type if the set of slopes is either $\{0,1\}$ or $\{0,1/2,1\}$, and the segments of slope 0 and 1 have length one.

By [Zar91, Theorem 5.9], simple abelian varieties of K3-type have maximal angle rank. As a corollary, we have another piece of the classification.

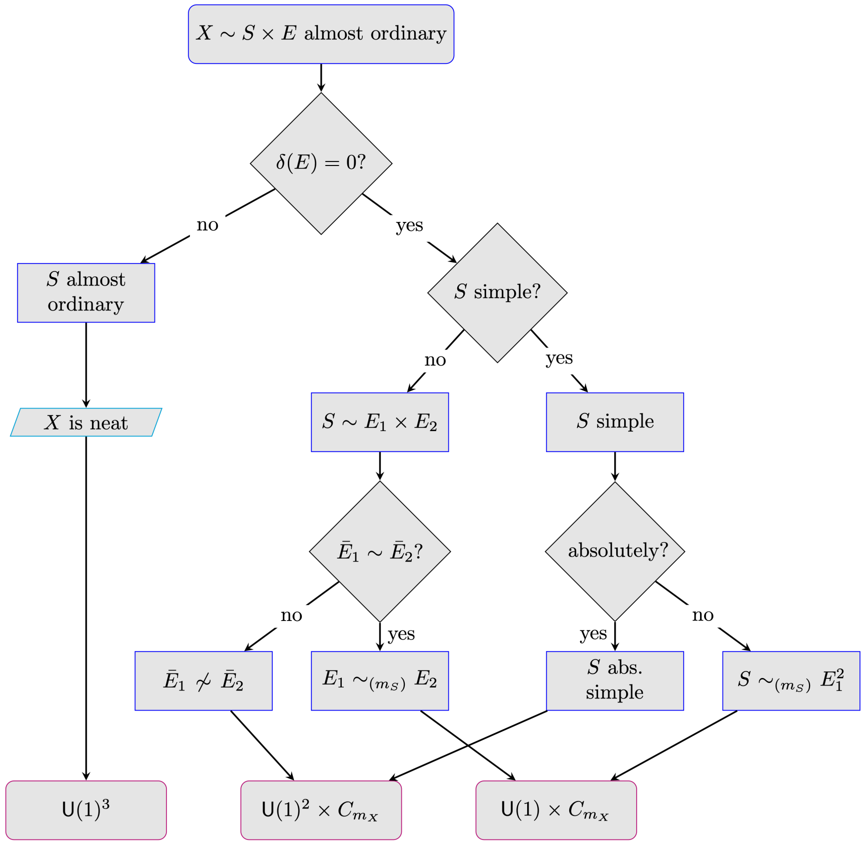


FIGURE 14. Serre–Frobenius groups of non-simple almost ordinary threefolds.

Lemma 6.6.2 (Node X-F in Figure 10)**.** *Let X be a simple abelian threefold over $\mathbf{F}_q$ of p-rank 1. Then X has maximal angle rank and $\mathsf{SF}(X) \cong \mathsf{U}(1)^3$.*

Now assume that X is not simple, so that $X \sim S \times E$ for some surface S and elliptic curve E.

Lemma 6.6.3 (Node X-G in Figure 10)**.** *Let $X \sim S \times E$ be a non-simple abelian threefold over $\mathbf{F}_q$ of p-rank 1. The Serre–Frobenius group of X is given by Table 8.*

Proof. As in Section 6.3, we let $\pi_1, \overline{\pi}_1, \pi_2, \overline{\pi}_2$ and $\alpha, \overline{\alpha}$ be the Frobenius eigenvalues of S and E respectively. Denote the normalized eigenvalues by $u_1 := \pi_1/\sqrt{q}, u_2 = \pi_2/\sqrt{q}$ and $u := \alpha/\sqrt{q}$. We consider three cases:

(6.6.3-a) S is simple and almost ordinary, and E is supersingular.
(6.6.3-b) S is non-simple and almost ordinary, and E is supersingular.
(6.6.3-c) S is supersingular and E is ordinary.

Type	δ_X	M
(6.6.3-a)	2	$\{1, 3, 4, 6, 8, 12\}$
(6.6.3-b)	1	Diagram 9.
(6.6.3-c)	1	$\{1, 2, 3, 4, 5, 6, 8, 10, 12, 24\}$

TABLE 8. Serre–Frobenius groups of abelian threefolds of p-rank 1.

Suppose first that X is of type (6.6.3-a). By Lemma 5.3.1, the set $\{u_1, u_2\}$ is multiplicatively independent. Since u is a root of unity, $U_X = \langle u_1, u_2, u\rangle = U_S \oplus U_E \cong \mathbf{Z}^2 \oplus C_m$ for $m \in M = \{1, 3, 4, 6, 8, 12\}$ the set of possible torsion orders for supersingular elliptic curves. Thus, $\mathsf{SF}(X) \cong \mathsf{U}(1)^2 \times C_m$ in this case.

If X is of type (6.6.3-b), then $S \sim E_1 \times E_2$ with E_1 ordinary and E_2 supersingular. By Proposition 3.3.2, $\mathsf{SF}(X) \cong \mathsf{U}(1) \times C_m$, with m in the set of possible torsion orders of non-simple supersingular surfaces.

If X is of type (6.6.3-c), we have $U_X = U_E \oplus U_S \cong \mathbf{Z} \oplus C_m$ for m in the set $M = \{1, 2, 3, 4, 5, 6, 8, 10, 12, 24\}$ of possible torsion orders of supersingular surfaces from Lemmas 5.5.1 and 5.6.1. □

6.7. **Absolutely simple p-rank 0 threefolds.** In this section, X will be a non-supersingular p-rank 0 abelian threefold over $\mathbf{F}_q$. From the q-Newton polygon of the Frobenius polynomial $P(T) = P_X(T)$ (see Figure 16) we see that X is absolutely simple, since the slope $1/3$ does not occur for abelian varieties of smaller dimension. Let e_r^2 denote the dimension of $\mathrm{End}^0(X_{(r)})$ over its center. We consider two cases:

(6.7-a) There exists $r \geq 1$ such that $e_r = 3$. In this case we have $P_{(r)}(T) = h_{(r)}(T)^3$ and $h_{(r)}(T)$ is as in Theorem 6.1.1, so that 3 divides $r \cdot \log_p(q)$.

(6.7-b) $e_r = 1$ for every positive integer r.

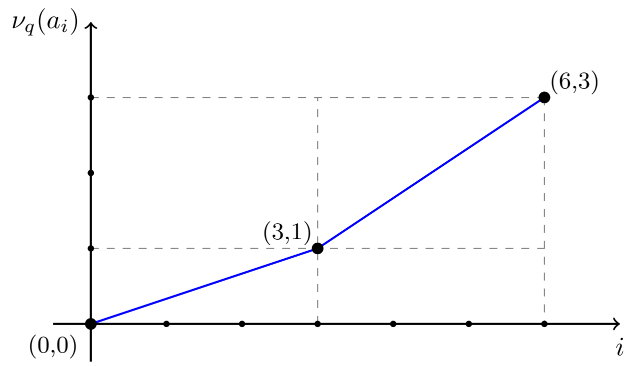


FIGURE 16. q-Newton polygon of p-rank 0 non-supersingular abelian threefolds.

Lemma 6.7.1. *Let X be an absolutely simple abelian threefold of p-rank 0 defined over $\mathbf{F}_q$. Then, the Serre–Frobenius group of X is classified according to Table 9. Furthermore, X is of type (6.7-a), m_X is the smallest positive integer r such that $e_r = 3$.*

TABLE 9. Serre–Frobenius groups of absolutely simple abelian threefolds of p-rank 0.

Type	$q = p^d$	δ_X	M
(6.7-a)	$3 \mid m_X \cdot d$	1	$\{1, 3, 7\}$
(6.7-b)	-	3	$\{1\}$

Remark 6.7.2. The techniques for proving the Generalized Lenstra–Zarhin result in [DKZB21, Theorem 1.5], cannot be applied to this case. Thus, even the angle rank analysis in this case is particularly interesting.

Proof. Suppose first that X is of type (6.7-a), and let m be the minimal positive integer such that $e_m = 3$. Maintaining previous notation, $P_{(m)}(T) = h_{(m)}(T)^3$ implies that $\alpha_2 = \zeta \cdot \alpha_1$ and $\alpha_3 = \xi \cdot \alpha_1$ for primitive m-th roots of unity ζ and ξ. By Proposition 2.3.1, this implies that $\mathsf{SF}(X) \cong \mathsf{U}(1) \times C_m$. We conclude that $\delta_X = 1$ and $m = m_X$. To calculate the set M of possible torsion orders, assume that $m_X = m > 1$. Then $\mathbf{Q}(\alpha_1^m)$ is a quadratic imaginary subextension of $\mathbf{Q}(\alpha_1) \supset \mathbf{Q}$, and we can argue as in the proof of Theorem 3.1.1 (with $\ell = 3$) to conclude that $m \in \{3, 7\}$.

Assume now that X is of type (6.7-b). This implies that $\mathbf{Q}(\alpha_1^r)$ is a degree 6 CM-field for every positive integer r. If $m := m_X$, the base extension $X_{(m)}$ is neat and the Frobenius eigenvalues are distinct and not supersingular. By Remark (3.2.2.b) we have that $\delta_X = 3$ and $m = 1$. $\square$

Example 6.7.3 (Histograms for X of type (6.7-a))**.**

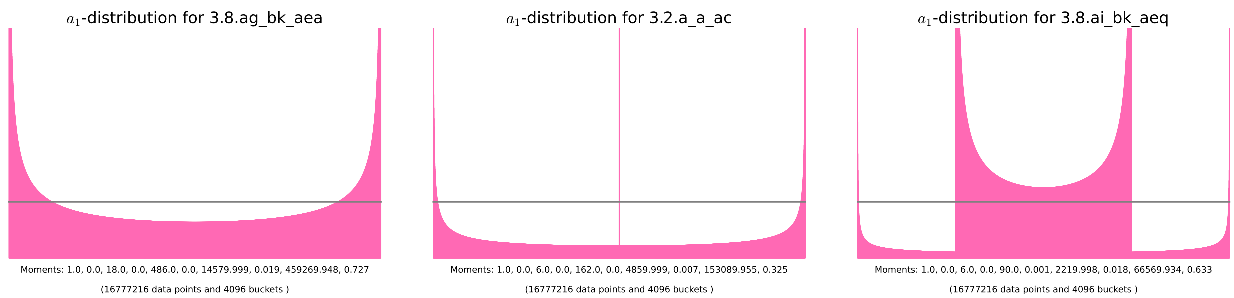
($m_X = 1$) The isogeny class 3.8.ag_bk_aea satisfies $m_X = 1$. Note that 3 divides $m_X \cdot \log_2(8)$.

($m_X = 3$) The isogeny class 3.2.a_a_ac has angle rank 1 and irreducible Frobenius polynomial $P(T) = T^6 - 2T^3 + 8$. The cubic base extension gives the isogeny class 3.8.ag_bk_aea with reducible Frobenius polynomial $P_{(3)}(T) = (T^6 - 2T^3 + 8)^3$. Note that 3 divides $m_X \cdot \log_2(2)$.

($m_X = 7$) The isogeny class 3.8.ai_bk_aeq has angle rank 1 and irreducible Frobenius polynomial $P(T) = T^6 - 8T^5 + 36T^4 - 120T^3 + 288T^2 - 512T + 512$. It's base change over a degree $m_X = 7$ extension is the isogeny class 3.2097152.ahka_bfyoxc_adesazpwa with Frobenius polynomial

$$P_{(7)}(T) = (T^2 - 1664T + 2097152)^3.$$

In this example, $q = 8$, so that 3 divides $m_X \cdot \log_2(8)$.



(A) 3.8.ag_bk_aea. (B) 3.2.a_a_ac. (C) 3.8.ai_bk_aeq.

FIGURE 17. a_1-distribution for p-rank 0 non-supersingular threefolds of type (6.7-a).

6.8. **Simple supersingular threefolds.** Nart and Ritzenthaler [NR08] showed that the only degree 6 supersingular q-Weil numbers are the conjugates of:

$$\begin{aligned} &\pm\sqrt{q}\zeta_7, \pm\sqrt{q}\zeta_9, && \text{when } q \text{ is a square, and} \\ &7^{d/2}\zeta_{28}, 3^{d/2}\zeta_{36}, && \text{when } q \text{ is not a square.} \end{aligned}$$

Building on their work, Haloui [Hal10, Proposition 1.5] completed the classification of simple supersingular threefolds. This classification is also discussed in [SMZ14]; and we adapt their notation for the polynomials of Z-3 type. Denoting by (a_1, a_2, a_3) the isogeny class of abelian threefolds over $\mathbf{F}_q$ with Frobenius polynomial $P_X(T) = T^6 + a_1T^5 + a_2T^4 + a_3T^3 + qa_2T^2 + q^2a_1T + q^3$, the following lemma gives the classification of Serre–Frobenius groups of simple supersingular threefolds, which is a corollary of Haloui's result.

Lemma 6.8.1 (Node X-F in Figure 10)**.** *Let X be a simple supersingular abelian threefold defined over $\mathbf{F}_q$. The Serre–Frobenius group of X is classified according to Table 10.*

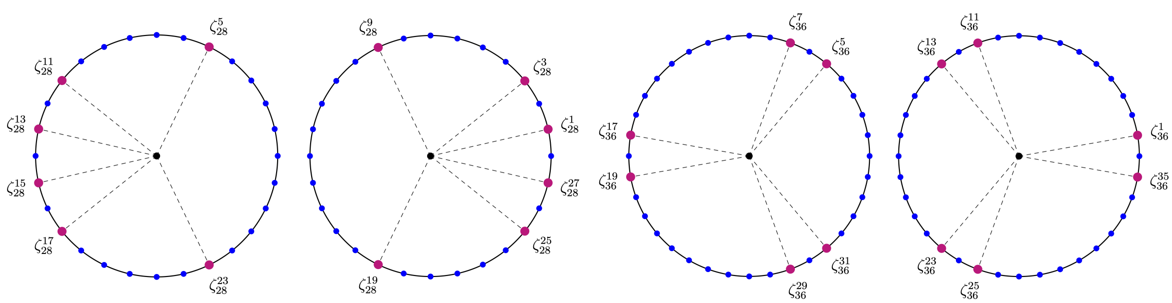
TABLE 10. Serre–Frobenius groups of simple supersingular threefolds.

(a_1, a_2, a_3)	p	d	Type	$\tilde{h}(T)$	$\mathsf{SF}(X)$
$(\sqrt{q}, q, q\sqrt{q})$	$7 \nmid (p^3 - 1)$	even	Z-1	$\Phi_7(T)$	C_7
$(-\sqrt{q}, q, -q\sqrt{q})$	$7 \nmid (p^3 - 1)$	even	Z-1	$\Phi_{14}(T)$	C_{14}
$(0, 0, q\sqrt{q})$	$\not\equiv 1 \bmod 3$	even	Z-1	$\Phi_9(T)$	C_9
$(0, 0, -q\sqrt{q})$	$\not\equiv 1 \bmod 3$	even	Z-1	$\Phi_{18}(T)$	C_{18}
$(\sqrt{7q}, 3q, q\sqrt{7q})$	$= 7$	odd	Z-3	$h_{7,1}(T)$	C_{28}
$(-\sqrt{7q}, 3q, -q\sqrt{7q})$	$= 7$	odd	Z-3	$h_{7,1}(-T)$	C_{28}
$(0, 0, q\sqrt{3q})$	$= 3$	odd	Z-3	$h_{3,3}(T)$	C_{36}
$(0, 0, -q\sqrt{3q})$	$= 3$	odd	Z-3	$h_{3,3}(-T)$	C_{36}

Proof. By Xing's theorem 6.1.1, we know that the Frobenius polynomial of all supersingular threefolds $P_X(T)$ coincides with the minimal polynomial $h_X(T)$ and $e = 1$ in every row of the table.

The first four rows of Table 10 correspond to isogeny classes of type (Z-1). By the discussion in Section 3.4, the minimal polynomials are of the form[5] $\Phi_m^{[\sqrt{q}]}(T)$ and the normalized polynomials are just the cyclotomic polynomials $\Phi_m(T)$.

The last four rows of Table 10 correspond to isogeny classes of type (Z-3). The normalized Frobenius polynomials are $h_{7,1}(\pm T) = T^6 \pm \sqrt{7}T^5 + 3T^4 \pm \sqrt{7}T^3 + 3T^2 \pm \sqrt{7}T + 1$, and $h_{3,3}(\pm T) = T^6 \pm \sqrt{3}T^3 + 1$. Noting that $h_{7,1}(T)h_{7,1}(-T) = \Phi_{28}(T)$ and $h_{3,3}(T)h_{3,3}(-T) = \Phi_{36}(T)$ we conclude that the unit groups U_X are generated by ζ_{28} and ζ_{36} respectively. $\square$



(A) $h_{7,1}(T)$. (B) $h_{7,1}(-T)$. (C) $h_{3,3}(T)$. (D) $h_{3,3}(-T)$.

FIGURE 18. Roots of Z-3 type normalized Frobenius polynomials in Table 10.

6.9. **Non-simple supersingular threefolds.** If X is a non-simple supersingular threefold over $\mathbf{F}_q$, then there are two cases:

(6.9.0-a) $X \sim S \times E$, with S a simple supersingular surface over $\mathbf{F}_q$ and E a supersingular elliptic curve.
(6.9.0-b) $X \sim E_1 \times E_2 \times E_3$, where each E_i is a supersingular elliptic curve.

The classification of the Serre–Frobenius group in these cases can be summarized in the following lemma.

Lemma 6.9.1 (Node X-J in 10)**.** *If X is a non-simple supersingular threefold as in Case (6.9.0-a), then $\mathsf{SF}(X) \cong C_m$, for $m \in M(p, d)$, where*

[5]Recall that $f^{[a]}(T) := a^{\deg f} f(T/a)$.

- *If d is even, $M(p,d) = \{3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30\}$,*
- *If d is odd, $M(p,d) = \{4, 8, 12, 20, 24\}$.*

Proof. In this case, $m = \operatorname{lcm}(m_S, m_E)$, since this is the degree of the smallest extension over which the Serre–Frobenius group becomes connected. The list of values for m_E and m_S come from Tables 2 and 5. □

Lemma 6.9.2 (Node X-J in 10)**.** *If X is a non-simple supersingular threefold as in Case (6.9.0-b), then $\mathsf{SF}(X) \cong C_m$, for $m \in M(p,d)$, where*

- *If d is even, $M(p,d) = \{1, 3, 4, 6, 12\}$,*
- *If d is odd, $M(p,d) = \{4, 8, 12\}$.*

Proof. By Proposition 3.3.2, m is the degree of the extension over which all the elliptic curve factors E_i become isogenous. This is precisely the least common multiple of the m_{E_i}'s. From Table 2, we can calculate the various possibilities for the lcm's depending on the parity of d. □

7. Simple ordinary abelian varieties of odd dimension

We conclude this article with a corollary of Theorem 3.1.1.

Theorem 7.0.1 (Restatement of Theorem 3.1.1)**.** *Let $g > 2$ be prime, and let A be a simple ordinary abelian variety of dimension g over $\mathbf{F}_q$ that is not absolutely simple. Then A has angle rank 1 and*

(a) A splits over a degree g extension and $\mathsf{SF}(A)/\mathsf{SF}(A)^\circ \cong C_g$, or
(b) $2g + 1$ is prime, A splits over a degree $2g + 1$ extension and $\mathsf{SF}(A)/\mathsf{SF}(A)^\circ \cong C_{2g+1}$.

The proof of this lemma is the same as the proof of Lemma 6.2.3, so we do not repeat it here. However, it would be interesting to have a more complete result for simple ordinary abelian varieties of prime dimension; that is, whether every ordinary absolutely simple abelian variety of prime dimension $g > 3$ has maximal angle rank. Tankeev [Tan84] showed that the angle rank of any absolutely simple abelian variety of prime dimension lies in $\{1, g-1, g\}$. We also know from [DKZB21] that a necessary condition for $\delta_A = g$ is that the *code* is trivial. Furthermore, the answer is negative when the dimension is not prime (see [DKRV21a]).

References

[AS10] Omran Ahmadi and Igor E. Shparlinski, *On the distribution of the number of points on algebraic curves in extensions of finite fields*, Math. Res. Lett. **17** (2010), no. 4, 689–699. MR 2661173

[Chi92] Wenchen Chi, *ℓ-adic and λ-adic representations associated to abelian varieties defined over number fields*, American Journal of Mathematics **114** (1992), no. 2, 315–353.

[Deu41] Max Deuring, *Die typen der multiplikatorenringe elliptischer funktionenkörper*, Abhandlungen aus dem mathematischen Seminar der Universität Hamburg, vol. 14, Springer, 1941, pp. 197–272.

[DKRV21a] Taylor Dupuy, Kiran Kedlaya, David Roe, and Christelle Vincent, *Counterexamples to a conjecture of Ahmadi and Shparlinski*, Experimental Mathematics (2021), 1–5.

[DKRV21b] ______, *Isogeny classes of abelian varieties over finite fields in the LMFDB*, Arithmetic Geometry, Number Theory, and Computation (Cham) (Jennifer S. Balakrishnan, Noam Elkies, Brendan Hassett, Bjorn Poonen, Andrew V. Sutherland, and John Voight, eds.), Springer International Publishing, 2021, pp. 375–448.

[DKZB21] Taylor Dupuy, Kiran S. Kedlaya, and David Zureick-Brown, *Angle ranks of abelian varieties*, arXiv preprint arXiv:2112.02455 (2021), 1–15.

[DN03] Claus Diem and Niko Naumann, *On the structure of Weil restrictions of abelian varieties*, J. Ramanujan Math. Soc. **18** (2003), no. 2, 153–174. MR 1995864

[Fit15] Francesc Fité, *Equidistribution, L-functions, and Sato–Tate groups*, Contemporary Mathematics **649** (2015), 63–88.

[FKRS12] Francesc Fité, Kiran S. Kedlaya, Víctor Rotger, and Andrew V. Sutherland, *Sato–Tate distributions and Galois endomorphism modules in genus 2*, Compositio Mathematica **148** (2012), no. 5, 1390–1442.

[FKS23] Francesc Fité, Kiran S. Kedlaya, and Andrew V. Sutherland, *Sato-Tate groups of abelian threefolds*, 2023.

[Hal10] Safia Haloui, *The characteristic polynomials of abelian varieties of dimensions 3 over finite fields*, J. Number Theory **130** (2010), no. 12, 2745–2752. MR 2684495

[Hon68] Taira Honda, *Isogeny classes of abelian varieties over finite fields*, Journal of the Mathematical Society of Japan **20** (1968), no. 1-2, 83–95.

[HZ02] Everett W. Howe and Hui June Zhu, *On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field*, Journal of Number Theory **92** (2002), no. 1, 139–163.

[KS00] Jan Krajíček and Thomas Scanlon, *Combinatorics with definable sets: Euler characteristics and Grothendieck rings*, Bull. Symbolic Logic **6** (2000), no. 3, 311–330. MR 1803636

[LZ93] Hendrik W. Lenstra, Jr. and Yuri G. Zarhin, *The Tate conjecture for almost ordinary abelian varieties over finite fields*, Advances in number theory (Kingston, ON, 1991), Oxford Sci. Publ., Oxford Univ. Press, New York, 1993, pp. 179–194. MR 1368419

[Mil17] James S. Milne, *Algebraic groups: the theory of group schemes of finite type over a field*, vol. 170, Cambridge University Press, 2017.

[MN02] Daniel Maisner and Enric Nart, *Abelian surfaces over finite fields as Jacobians*, Experiment. Math. **11** (2002), no. 3, 321–337, With an appendix by Everett W. Howe. MR 1959745

[Mor77] Sidney A. Morris, *Pontryagin duality and the structure of locally compact abelian groups*, London Mathematical Society Lecture Note Series, No. 29, Cambridge University Press, Cambridge-New York-Melbourne, 1977. MR 0442141

[NR08] Enric Nart and Christophe Ritzenthaler, *Jacobians in isogeny classes of supersingular abelian threefolds in characteristic 2*, Finite Fields Appl. **14** (2008), no. 3, 676–702. MR 2435055

[Oor07] Frans Oort, *Abelian varieties over finite fields*, https://math.nyu.edu/~tschinke/books/finite-fields/final/05_oort.pdf, 2007.

[Pon34] L. Pontrjagin, *The theory of topological commutative groups*, Ann. of Math. (2) **35** (1934), no. 2, 361–388. MR 1503168

[R9̈0] Hans-Georg Rück, *Abelian surfaces and Jacobian varieties over finite fields*, Compositio Math. **76** (1990), no. 3, 351–366. MR 1080007

[Ser68] Jean-Pierre Serre, *Abelian ℓ-adic representations and elliptic curves*, Research notes in Mathematics ; v. 7, A.K. Peters, Wellesley, Mass, 1998 - 1968 (eng).

[Ser13] ———, *Oeuvres/Collected papers. IV. 1985–1998*, Springer Collected Works in Mathematics, Springer, Heidelberg, 2013, Reprint of the 2000 edition [MR1730973]. MR 3185222

[SHOR20] Jean-Pierre Serre, Everett W Howe, Joseph Oesterle, and Christophe Ritzenthaler, *Rational points on curves over finite fields*, Société mathématique de France, 2020.

[SMZ14] Vijaykumar Singh, Gary McGuire, and Alexey Zaytsev, *Classification of characteristic polynomials of simple supersingular abelian varieties over finite fields*, Funct. Approx. Comment. Math. **51** (2014), no. 2, 415–436. MR 3282636

[Sut16] Andrew V. Sutherland, *Sato–Tate distributions*, Analytic methods in arithmetic geometry **740** (2016), 197–248.

[Tan84] Sergei G Tankeev, *On cycles on abelian varieties of prime dimension over finite or number fields*, Mathematics of the USSR-Izvestiya **22** (1984), no. 2, 329.

[Tat66] John Tate, *Endomorphisms of abelian varieties over finite fields*, Inventiones mathematicae **2** (1966), no. 2, 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. MR 3077121

[Wat69] William C. Waterhouse, *Abelian varieties over finite fields*, Annales scientifiques de l'École normale supérieure, vol. 2, 1969, pp. 521–560.

[Wei49] André Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508. MR 29393

[Xin94] Chaoping Xing, *The characteristic polynomials of abelian varieties of dimensions three and four over finite fields*, Sci. China Ser. A **37** (1994), no. 2, 147–150. MR 1275799

[Xin96] ———, *On supersingular abelian varieties of dimension two over finite fields*, Finite Fields Appl. **2** (1996), no. 4, 407–421. MR 1409453

[Zar91] Yuri G. Zarhin, *Abelian varieties of $K3$ type and ℓ-adic representations*, ICM-90 Satellite Conference Proceedings (Tokyo) (Akira Fujiki, Kazuya Kato, Yujiro Kawamata, Toshiyuki Katsura, and Yoichi Miyaoka, eds.), Springer Japan, 1991, pp. 231–255.

[Zar93] ———, *Abelian varieties of $K3$ type*, Séminaire de Théorie des Nombres, Paris, 1990–91, Progr. Math., vol. 108, Birkhäuser Boston, Boston, MA, 1993, pp. 263–279. MR 1263531

[Zar94] Yuri G. Zarhin, *The Tate conjecture for non-simple abelian varieties over finite fields*, pp. 267–298, De Gruyter, Berlin, New York, 1994.

[Zar15] ———, *Eigenvalues of Frobenius endomorphisms of abelian varieties of low dimension*, Journal of Pure and Applied Algebra **219** (2015), no. 6, 2076–2098.

[Zhu01] Hui June Zhu, *Supersingular abelian varieties over finite fields*, Journal of Number Theory **86** (2001), no. 1, 61–77.

[Zyw22] David Zywina, *Determining monodromy groups of abelian varieties*, Res. Number Theory **8** (2022), no. 4, Paper No. 89, 53. MR 4496693

Department of Mathematics, Emory University, Atlanta, GA 30322, USA
Email address: santiago.arango@emory.edu
URL: https://sarangop1728.github.io/

Mathematics Department, University of California, Santa Cruz, CA 95064, USA
Email address: dbhamidi@ucsc.edu
URL: https://bdeewang.com/

542 Math Tower, 231 West 18th Avenue, Columbus, OH 43210-1174, USA
Email address: sankar.40@osu.edu
URL: https://sites.google.com/site/soumya3sankar/