Canad. Math. Bull. Vol. 58 (4), 2015 pp. 673–691
http://dx.doi.org/10.4153/CMB-2015-050-8

Local Heuristics and an Exact Formula for Abelian Surfaces Over Finite Fields

Jeffrey Achter and Cassandra Williams

Abstract. Consider a quartic q-Weil polynomial f. Motivated by equidistribution considerations, we define, for each prime ℓ, a local factor that measures the relative frequency with which f mod ℓ occurs as the characteristic polynomial of a symplectic similitude over $\mathbb{F}_\ell$. For a certain class of polynomials, we show that the resulting infinite product calculates the number of principally polarized abelian surfaces over $\mathbb{F}_q$ with Weil polynomial f.

1 Introduction

Consider abelian varieties over a finite field. With each such $X/\mathbb{F}_q$ one may associate a characteristic polynomial of Frobenius, $f_{X/\mathbb{F}_q}(T) \in \mathbb{Z}[T]$, and two abelian varieties X and Y are isogenous if and only if $f_{X/\mathbb{F}_q}(T) = f_{Y/\mathbb{F}_q}(T)$. In this way, isogeny classes of abelian varieties over $\mathbb{F}_q$ are parametrized by suitable q-Weil polynomials $f(T)$.

Conversely, given such a polynomial f, it is of intrinsic interest to calculate how many abelian varieties are in the corresponding isogeny class. In fact, a polarized variant of this problem seems even more natural. Let $\mathcal{A}_g$ be the moduli space of principally polarized abelian varieties of dimension g, and let

$$\mathcal{A}_g(\mathbb{F}_q; f) = \left\{ (X, \lambda) \in \mathcal{A}_g(\mathbb{F}_q) : f_{X/\mathbb{F}_q}(T) = f(T) \right\}.$$

Armed with an (overly optimistic) equidistribution philosophy, one might attempt to estimate $\#\mathcal{A}_g(\mathbb{F}_q; f)$ in the following fashion. To the extent possible, Frobenius elements of abelian varieties are equidistributed in $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$. By somehow multiplying together, over all ℓ, the frequency with which $f(T)$ mod ℓ occurs as the characteristic polynomial of a symplectic similitude, one might try to apprehend $\#\mathcal{A}_g(\mathbb{F}_q; f)$.

As written, this strategy is nonsense; for given g and ℓ, mod ℓ Frobenius elements are equidistributed only if $q \gg_g \ell$. Nonetheless, such congruence considerations apparently control the sizes of isogeny classes.

Our main result is as follows. For f in a certain class of simple, ordinary q-Weil polynomials of degree 4 (see Section 2), we define for each prime ℓ a quantity $\nu_\ell(f)$ (see (4.1)) that measures its relative frequency as the characteristic polynomial of an

Received by the editors November 28, 2014; revised May 17, 2015.
Published electronically July 24, 2015.
JDA was partially supported by grants from the Simons Foundation (204164) and the NSA (H98230-14-1-0161).
AMS subject classification: **14K02**.
Keywords: abelian surfaces, finite fields, random matrices.

element of $\mathrm{GSp}_4(\mathbb{F}_\ell)$. After defining a Sato–Tate term $\nu_\infty(f)$, we show that

$$\nu_\infty(f)\prod_\ell \nu_\ell(f) = \#\mathcal{A}_2(\mathbb{F}_q;f) \tag{1.1}$$

(where a principally polarized abelian surface is given mass inversely proportional to the size of its automorphism group).

This work is inspired by work of Gekeler [5], who derived a version of (1.1) for elliptic curves over a finite prime field. Our perspective was influenced by Katz's analysis [8] of Gekeler's product formula.

2 Abelian Varieties and Weil Polynomials

Let $X/\mathbb{F}_q$ be an abelian variety of dimension g over a finite field with $q = p^e$ elements, and let $f_{X/\mathbb{F}_q}(T) \in \mathbb{Z}[T]$ be the characteristic polynomial of its Frobenius endomorphism (acting on, say, any of the Tate modules $T_\ell X$ with $\ell \neq p$). Then $f_{X/\mathbb{F}_q}(T)$ is a q-Weil polynomial, *i.e.,* the complex roots $\alpha_1, \dots, \alpha_{2g}$ of $f_{X/\mathbb{F}_q}(T)$ may be ordered so that $\alpha_j\alpha_{g+j} = q$ for $1 \le j \le g$, and in fact $|\alpha_j| = \sqrt{q}$ for each j.

Now assume that $f(T)$ is a q-Weil polynomial of degree 4; such a polynomial corresponds to a (possibly empty) isogeny class $\mathcal{I}_f$ of abelian surfaces over $\mathbb{F}_q$. In the sequel, we will assume that f has the following properties:

(W.1) (*ordinary*) Its middle coefficient is relatively prime to p.
(W.2) (*principally polarizable*) There exists a principally polarized abelian surface with characteristic polynomial f.
(W.3) (*Galois*) The polynomial $f(T)$ is irreducible over $\mathbb{Q}$, and $K_f := \mathbb{Q}(T)/f(T)$ is Galois and unramified at p.
(W.4) (*maximal*) Let ϖ_f be a (complex) root of $f(T)$, with complex conjugate $\overline{\varpi}_f$. Then $\mathcal{O}_f := \mathbb{Z}[\varpi_f, \overline{\varpi}_f]$, *a priori* an order in K_f, is actually the maximal order $\mathcal{O}_{K_f}$.

Conditions (W.1) and (W.3) imply that any abelian surface in $\mathcal{A}_2(\mathbb{F}_q;f)$ is ordinary and simple. Condition (W.2) is explicitly characterized, in terms of the coefficients of f, in [7, Thm. 1.3]. Condition (W.4) is indeed an extra hypothesis, which we hope to relax in a future work. The isomorphism class of $\mathcal{O}_f$, as an abstract order, is independent of the choice of ϖ_f.

Note that $\mathrm{Gal}(K_f/\mathbb{Q})$ is abelian, since $[K_f:\mathbb{Q}] = 4$, and there is an intrinsically defined complex conjugation $\iota \in \mathrm{Gal}(K_f/\mathbb{Q})$, since K_f is a CM field. As in the description of Condition (W.4), we will often denote the action of ι on an element $\alpha \in K_f$ by $\overline{\alpha} = \iota(\alpha)$. If R is any ring, then ι acts on $\mathcal{O}_{K_f} \otimes R$ via the first component.

Example 2.1 The polynomial $f(T) = T^4 + 29T^3 + 331T^2 + 1769T + 3721$ is a 61-Weil polynomial that is ordinary, principally polarizable, Galois, and maximal. In fact, $\mathcal{O}_f$ is the ring of integers in $\mathbb{Q}(\zeta_5)$, and f is the characteristic polynomial of Frobenius of the Jacobian of the curve with affine equation $y^2 = x^5 - 2$.

Define the conductor of f, $\mathrm{cond}(f)$, as the index of $\mathbb{Z}[\varpi_f] \cong \mathbb{Z}[T]/f(T)$ in $\mathcal{O}_f$. If $f(T) = T^4 - aT^3 + bT^2 - aTq + q^2$, let $f^+(T) = T^2 - aT + (b - 2q)$; then $f^+(T)$ is

https://doi.org/10.4153/CMB-2015-050-8 Published online by Cambridge University Press

the minimal polynomial of $\omega_f + \overline{\omega}_f$, and $K_f^+ := \mathbb{Q}[T]/f^+(T)$ is the maximal totally real subfield of K_f. Denote the discriminants of $f(T)$ and $f^+(T)$ by Δ_f and Δ_{f^+}, respectively. Similarly, let $\Delta_{\mathcal{O}}$ represent the discriminant of an order $\mathcal{O}$; notice that $\Delta_{\mathbb{Z}[\omega_f]} = \Delta_f$ and $\Delta_{\mathcal{O}_{K^+}} = \Delta_{f^+}$.

Lemma 2.2 *The index of $\mathbb{Z}[\omega_f]$ in $\mathcal{O}_f$ is q.*

Proof Using the above definition of f and [7, Propositions 9.4 and 9.5],

$$\Delta_{\mathcal{O}_f} = \Delta_{f^+}^2 \cdot N_{K_f/\mathbb{Q}}(\omega_f - \overline{\omega}_f) = (a^2 - 4b + 8q)^2(b^2 + 4bq + 4q^2 - 4a^2q).$$

The discriminant of $\mathbb{Z}[\omega_f]$ is given by

$$\Delta_{\mathbb{Z}[\omega_f]} = \Delta_f = q^2(a^2 - 4b + 8q)^2(b^2 + 4bq + 4q^2 - 4a^2q) = q^2\Delta_{\mathcal{O}_f}$$

and $\Delta_f = [\mathcal{O}_f : \mathbb{Z}[\omega_f]]^2\Delta_{\mathcal{O}_f}$. Then the desired index is q. ∎

Corollary 2.3 *If $\ell \nmid p$, then $\mathcal{O}_{K_f} \otimes \mathbb{Z}_{(\ell)} \cong \mathbb{Z}_{(\ell)}[T]/f(T)$.*

Similarly, $\mathbb{Z}[T]/f^+(T)$ is maximal.

Lemma 2.4 *The order $\mathbb{Z}[T]/f^+(T)$ is the maximal order $\mathcal{O}_{K_f^+}$.*

Proof Condition (W.4) implies that $\mathcal{O}_f \cap K_f^+ = \mathcal{O}_{K_f} \cap K_f^+ = \mathcal{O}_{K_f^+}$. Certainly

$$\mathbb{Z}[T]/f^+(T) = \mathbb{Z}[\omega_f + \overline{\omega}_f] \subseteq \mathcal{O}_f \cap K_f^+.$$

Consider $a \in \mathcal{O}_f$; then $a = a_0 + a_1\omega_f + a_2\overline{\omega}_f + a_3\omega_f\overline{\omega}_f$ for some integers a_i. We have $\omega_f\overline{\omega}_f = q$ as f is a q-Weil polynomial, and $a \in K_f^+$ if and only if $a_1 = a_2$. Then $a \in \mathcal{O}_f \cap K_f^+$ has the form $a = (a_0 + a_3q) + a_1(\omega_f + \overline{\omega}_f)$ and $\mathcal{O}_f \cap K_f^+ \subseteq \mathbb{Z}[\omega_f + \overline{\omega}_f]$. Thus, $\mathbb{Z}[\omega_f + \overline{\omega}_f] = \mathcal{O}_{K_f^+}$. ∎

3 Conjugacy Classes in Symplectic Groups

If $X/\mathbb{F}_q$ is a principally polarized abelian surface, then the four-dimensional $\mathbb{F}_\ell$-vector space $X_\ell := X[\ell](\overline{\mathbb{F}}_q)$ is naturally equipped with a symplectic form. We collect some notation concerning symplectic (similitude) groups.

3.1 Symplectic Groups

Let V be a vector space of dimension $2g$ over a field k, equipped with a perfect, skew-symmetric form $\langle \cdot, \cdot \rangle$. The symplectic similitude group of V is the group of automorphisms that preserve this form up to a multiple. Concretely,

$$\mathrm{GSp}\big(V, \langle \cdot, \cdot \rangle\big) = \big\{ \gamma \in \mathrm{GL}(V) : \exists m(\gamma) \in k^\times, \forall u, v \in V, \langle \gamma u, \gamma v \rangle = m(\gamma)\langle u, v \rangle \big\}.$$

https://doi.org/10.4153/CMB-2015-050-8 Published online by Cambridge University Press

The group of automorphisms of the symplectic space is the symplectic group, $\mathrm{Sp}(V, \langle \cdot, \cdot \rangle)$, and these groups sit in an exact sequence

$$1 \longrightarrow \mathrm{Sp}(V, \langle \cdot, \cdot \rangle) \longrightarrow \mathrm{GSp}(V, \langle \cdot, \cdot \rangle) \xrightarrow{\text{mult}} k^\times \longrightarrow 1\,. \tag{3.1}$$
$$\gamma \longmapsto m(\gamma)$$

For $m \in k^\times$, we let $\mathrm{GSp}(V, \langle \cdot, \cdot \rangle)^{(m)} = \mathrm{mult}^{-1}(m)$.

Call a decomposition $V = W_1 \oplus W_2$ *symplectic* if, for each i, $\langle \cdot, \cdot \rangle|_{W_i}$ is a perfect pairing; and isotropic if, for some i, $\langle \cdot, \cdot \rangle|_{W_i} = 0$.

In fact, any symplectic space V of dimension $2g$ is isomorphic to $k^{\oplus 2g}$, equipped with the pairing described by the $2g \times 2g$ matrix

$$J = \begin{pmatrix} 0 & 1_g \\ -1_g & 0 \end{pmatrix};$$

the associated similitude and symplectic groups are $\mathrm{GSp}_{2g}(k)$ and $\mathrm{Sp}_{2g}(k)$, respectively.

3.2 Shapes of Conjugacy Classes

In a general linear group $\mathrm{GL}(V)$, semisimple conjugacy classes are parametrized by the theory of rational canonical form (RCF), which gives a decomposition of any automorphism of a vector space into a direct sum of cyclic automorphisms over invariant subspaces. (An automorphism is cyclic if and only if its minimal and characteristic polynomials coincide.) Specifically, we factor the characteristic polynomial of γ into a product of irreducible polynomials

$$f_\gamma(T) = \prod_i (\phi_i(T))^{\lambda_i}$$

and then associate with each factor ϕ_i a partition of its multiplicity λ_i. Denote the partition by $[\lambda_{i,1}, \lambda_{i,2}, \ldots, \lambda_{i,n}]$, where $\lambda_{i,1} \geq \lambda_{i,2} \geq \cdots \geq \lambda_{i,n}$. Then V has a γ-invariant subspace with characteristic polynomial $\phi_i^{\lambda_{i,j}}$ for each $1 \leq j \leq n$, and γ restricted to each of these subspaces is cyclic. Note that the minimal polynomial of γ is the product of $\phi_i^{\lambda_{i,1}}$, so γ is cyclic if and only if the partition of λ_i consists of a single part for each ϕ_i. Thus, arbitrary conjugacy classes in $\mathrm{GL}_{2g}(k)$ are determined by their characteristic polynomial and additional partition data.

The classification of conjugacy classes in $\mathrm{GSp}_{2g}(k)$ is more intricate for two reasons. First, for elements with repeated eigenvalues, the presence of the symplectic form places nontrivial restrictions on allowable partition data. Second, elements of $\mathrm{GSp}_{2g}(k)$ that are conjugate in $\mathrm{GL}_{2g}(k)$ need not be conjugate in the symplectic similitude group; certain GL_{2g}-conjugacy classes decompose into classes indexed by $k^\times/(k^\times)^2$. (For details of this decomposition, see, for example, [4] or [10]. Alternatively, compare our results to those of [1] or [9].)

In the sequel, we will only need the case where $g = 2$ and $k = \mathbb{F}_\ell$ is a finite field. Let $\mathcal{C}(\gamma)$ denote the conjugacy class of γ. We distinguish conjugacy classes by the factorization pattern of their characteristic polynomials $f_\gamma(T)$ into irreducible polynomials over $\mathbb{F}_\ell$, and then refine this with additional combinatorial data, if necessary.

https://doi.org/10.4153/CMB-2015-050-8 Published online by Cambridge University Press

The resulting collection of data associated with $\mathcal{C}(\gamma)$ will be called the *shape* of γ, or of its conjugacy class.

Our enumeration of conjugacy classes in $\mathrm{GSp}_4(\mathbb{F}_\ell)$ is purposefully incomplete; we only include those that arise in our subsequent study of abelian surfaces. First, we only consider those classes for which all irreducible factors of the characteristic polynomial have the same degree. (Briefly call such a class "relevant".) Second, we only list those conjugacy classes corresponding to regular or cyclic elements. In general, an element of an algebraic group $\gamma \in G(k)$ is called regular if the dimension of its centralizer, $\dim \mathcal{Z}_G(\gamma)$, is minimal, *i.e.,* equal to the rank of G. In the case of $G = \mathrm{GSp}_4$, it is equivalent to insisting that γ be cyclic in the standard representation, *i.e.,* that there exists $v \in V$ such that $\{\gamma^i v : i \geq 0\}$ spans V. As usual, a semisimple element is regular if and only if its eigenvalues are distinct.

Let $f_\gamma(T) = \prod_j g_j(T)^{e_j}$ be the factorization of $f_\gamma(T)$ into powers of distinct, irreducible monic polynomials of equal degree. To this factorization of $f_\gamma(T)$ there is an associated factorization $V \cong \bigoplus W_j$, where $\gamma|_{W_j}$ has characteristic polynomial $g_j(T)^{e_j}$. For each j, either $\langle \cdot, \cdot \rangle|_{W_j}$ is zero or it is perfect; call these factorizations isotropic and symplectic, respectively.

Case 1: Regular semisimple elements

A regular semisimple conjugacy class is one for which the elements have a squarefree characteristic polynomial. We classify such conjugacy classes by the factorization of $f_\gamma(T)$ (over $\mathbb{F}_\ell$) and by $m(\gamma)$; let $a_i \in \mathbb{F}_\ell$ be distinct and $g_1 \neq g_2$. Then Table 3.1 is a complete classification of relevant regular semisimple conjugacy class shapes. (In each of these cases, all $e_j = 1$ and so we omit the trivial partition data from RCF.)

Class shape	$f_\gamma(T)$	$m(\gamma)$	
Split	$\prod_{j=1}^4 (T - a_j)$	$m = a_1 a_3 = a_2 a_4$	
DQ-S	$g_1(T)g_2(T)$	$m = g_j(0)$	(symplectic)
DQ-I	$g_1(T)g_2(T)$	$m \neq g_j(0), m^2 = g_1(0)g_2(0)$	(isotropic)
Quartic	$g(T)$	$m^2 = g(0)$	

Table 3.1: Regular semisimple conjugacy class shapes

Case 2: Non-semisimple elements

As stated above, if $f_\gamma(T)$ is not squarefree, then γ is cyclic if and only if all of the associated partitions are maximal (consist of a single part). In fact, such a conjugacy class is determined by a signed partition (the sign corresponds to a choice of coset in $\mathbb{F}_\ell^\times/(\mathbb{F}_\ell^\times)^2$ as discussed above) and Table 3.2 completes our list of relevant cyclic conjugacy class shapes. (As in Table 3.1, the $a_i \in \mathbb{F}_\ell$ are distinct.)

https://doi.org/10.4153/CMB-2015-050-8 Published online by Cambridge University Press

Class shape	$f_\gamma(T)$	$m(\gamma)$		Partition
QRL	$(T-a)^4$	$m = a^2$		$[4]$
DRL-S	$(T-a)^2(T+a)^2$	$m = a^2$	(symplectic)	$\{[2],[2]\}\pm$
DRL-I	$(T-a_1)^2(T-a_2)^2$	$m = a_1a_2$	(isotropic)	$[2]$
RQ-1	$[g(T)]^2$	$m = g(0)$		$[2]$
RQ-2	$(T^2-m)^2$	$m \neq \square$		$[2]\pm$

Table 3.2: Non-semisimple cyclic conjugacy class shapes

(For the conjugacy class shape **DRL-I**, the partition $[2]$ corresponds to the factor $(T-a_1)(T-a_2)$ in $f_\gamma(T)$, and thus to a subspace with characteristic polynomial $(T-a_1)(T-a_2)$.)

Note that, for a fixed characteristic polynomial f of shape **DRL-S** or **RQ-2**, the set of cyclic elements with characteristic polynomial f forms *two* conjugacy classes. For example, for a nonsquare $x \in \mathbb{F}_\ell^\times$,

$$\gamma_1 = \begin{pmatrix} a & & 1 & \\ & -a & & 1 \\ & & a & \\ & & & -a \end{pmatrix} \quad \text{and} \quad \gamma_2 = \begin{pmatrix} a & & 1 & \\ & -a & & x \\ & & a & \\ & & & -a \end{pmatrix}$$

are both elements of shape **DRL-S**. (Verification of this fact is discussed in the proof of Lemma 3.2.) The matrix

$$Z = \begin{pmatrix} z_1 & & z_3 & \\ & z_2 & & z_4 \\ & & z_1 & \\ & & & z_2x \end{pmatrix}$$

conjugates γ_1 to γ_2 over $\mathrm{GL}_4(\mathbb{F}_\ell)$, but is an element of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ if and only if $z_1^2 = z_2^2x$. Since x is nonsquare, γ_1 and γ_2 are not conjugate in $\mathrm{GSp}_4(\mathbb{F}_\ell)$, although they are conjugate in $\mathrm{GSp}_4(\mathbb{F}_{\ell^2})$. (A similar argument shows that we also have two classes of shape **RQ-2**.)

3.3 Centralizer Orders

We determine the size of each of the conjugacy classes $\mathcal{C}(\gamma)$ listed in Tables 3.1 and 3.2 by computing the order of the centralizer of the representative γ. Let $\mathcal{Z}_{\mathrm{GSp}_4(\mathbb{F}_\ell)}(\gamma)$ denote the centralizer of γ in $\mathrm{GSp}_4(\mathbb{F}_\ell)$.

A representative of a regular semisimple conjugacy class is an element of a unique maximal torus of $\mathrm{GSp}_4(\mathbb{F}_\ell)$, and the centralizer of such a γ is that maximal torus [3]. We use the structure of these maximal tori to compute the sizes of the centralizers of the regular semisimple class shapes.

https://doi.org/10.4153/CMB-2015-050-8 Published online by Cambridge University Press

Lemma 3.1 *Let $\mathcal{C}(\gamma)$ have one of the conjugacy class shapes listed in Table 3.1. Then*

$$\#\mathcal{Z}_{\mathrm{GSp}_4(\mathbb{F}_\ell)}(\gamma) = \begin{cases} (\ell-1)^3 & \text{if } \mathcal{C}(\gamma) \text{ is } \textbf{Split}, \\ (\ell+1)^2(\ell-1) & \text{if } \mathcal{C}(\gamma) \text{ is } \textbf{DQ-S}, \\ (\ell+1)(\ell-1)^2 & \text{if } \mathcal{C}(\gamma) \text{ is } \textbf{DQ-I}, \\ (\ell^2+1)(\ell-1) & \text{if } \mathcal{C}(\gamma) \text{ is } \textbf{Quartic}. \end{cases}$$

Proof In each case, we determine the size of the appropriate torus. For example, if $\mathcal{C}(\gamma)$ is **Quartic**, the polynomial $f_\gamma(T)$ has roots t, t^ℓ, t^{ℓ^2}, and t^{ℓ^3} in $\mathbb{F}_{\ell^4}^\times$ in one orbit under the action of Galois. Two pairs of roots have product $m(\gamma) \in \mathbb{F}_\ell^\times$ since $\gamma \in \mathrm{GSp}_4(\mathbb{F}_\ell)$. The element tt^ℓ cannot lie in $\mathbb{F}_\ell^\times$ when $t \in \mathbb{F}_{\ell^4} \smallsetminus \mathbb{F}_{\ell^2}$, thus $tt^{\ell^2} = m(\gamma)$. The map $t \mapsto tt^{\ell^2}$ is the norm map of $\mathbb{F}_{\ell^4}$ over $\mathbb{F}_{\ell^2}$. There are $\frac{\ell^4-1}{\ell^2-1}\cdot(\ell-1) = (\ell^2+1)(\ell-1)$ elements of $\mathbb{F}_{\ell^4}^\times$ whose $\mathbb{F}_{\ell^2}$-norm lies in $\mathbb{F}_\ell^\times$, which is the size of the torus and thus the centralizer. The other centralizer orders are computed analogously. ∎

Determining the centralizer orders of the non-semisimple class shapes requires more effort.

Lemma 3.2 *Suppose $\mathcal{C}(\gamma)$ has one of the conjugacy class shapes listed in Table 3.2. Then*

$$\#\mathcal{Z}_{\mathrm{GSp}_4(\mathbb{F}_\ell)}(\gamma) = \begin{cases} \ell^2(\ell-1) & \text{if } \mathcal{C}(\gamma) \text{ is } \textbf{QRL}, \\ 2\ell^2(\ell-1) & \text{if } \mathcal{C}(\gamma) \text{ is } \textbf{DRL-S}, \\ \ell(\ell-1)^2 & \text{if } \mathcal{C}(\gamma) \text{ is } \textbf{DRL-I}, \\ \ell(\ell^2-1) & \text{if } \mathcal{C}(\gamma) \text{ is } \textbf{RQ-1}, \\ 2\ell^2(\ell-1) & \text{if } \mathcal{C}(\gamma) \text{ is } \textbf{RQ-2}. \end{cases}$$

Proof For each conjugacy class shape, find an explicit cyclic representative $\gamma \in \mathrm{GSp}_4(\mathbb{F}_\ell)$ such that f_γ and $m(\gamma)$ are as given in Table 3.2. Then find a generic member C of the centralizer of γ and use it to find the size of $\mathcal{Z}_{\mathrm{GSp}_4(\mathbb{F}_\ell)}(\gamma)$. (For the **DRL-S** and **RQ-2** shapes, two distinct non-conjugate representatives are needed for the + and − classes.)

As an example, reconsider our previous example where $\mathcal{C}(\gamma)$ is **DRL-S**. It is easy to verify that the representatives γ_1 and γ_2 given earlier are cyclic elements of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ with characteristic polynomial $(T-a)^2(T+a)^2$ and $m(\gamma) = a^2$. The matrix

$$C = \begin{pmatrix} c_1 & & c_3 & \\ & c_2 & & c_4 \\ & & c_1 & \\ & & & c_2 \end{pmatrix}$$

centralizes both γ_1 and γ_2 with the conditions that $c_1 \in \mathbb{F}_\ell^\times$, $c_2 = \pm c_1$, and $c_3, c_4 \in \mathbb{F}_\ell$. Then each class has a centralizer of order $2\ell^2(\ell-1)$.

The rest of the computations are similar and are omitted here. ∎

https://doi.org/10.4153/CMB-2015-050-8 Published online by Cambridge University Press

4 Local Factors for f

Given f, we will define terms $v_\ell(f)$ for each finite prime of ℓ, as well as an archimedean term $v_\infty(f)$. For finite primes $\ell \neq p$, we let $v_\ell(f)$ be the probability that a random element of $\mathrm{GSp}_4(\mathbb{F}_\ell)^{(q)}$ has characteristic polynomial f, and compare this probability to the corresponding probability for a "typical" polynomial. (This is a higher-dimensional analogue of Gekeler's philosophy and concomitant definition for elliptic curves [5, Sec. 3]; see Section 6.4 for a brief discussion of why, in the presence of Condition (W.4), it suffices to work with a simpler definition than that of [5].) The definitions of $v_p(f)$ and $v_\infty(f)$ are more intricate, but guided by a similar philosophy.

4.1 $v_\ell(f)$

First, suppose $\ell \neq p$ is a finite rational prime. The Frobenius endomorphism $\varpi_{X/\mathbb{F}_q}$ of a principally polarized abelian variety $X/\mathbb{F}_q$ acts as an automorphism of X_ℓ. The polarization induces a symplectic pairing on X_ℓ; $\varpi_{X/\mathbb{F}_q}$ scales this pairing by a factor of q, and we may think of $\varpi_{X/\mathbb{F}_q}$ as an element of $\mathrm{GSp}(X_\ell)^{(q)} \cong \mathrm{GSp}_4(\mathbb{F}_\ell)^{(q)}$ (recall the notation surrounding (3.1)).

(Briefly) setting aside abelian varieties, there are ℓ^2 polynomials that occur as characteristic polynomials of elements of $\mathrm{GSp}_4(\mathbb{F}_\ell)^{(q)}$. The average frequency (over all such polynomials) with which a given polynomial occurs as the characteristic polynomial of an element of $\mathrm{GSp}_4(\mathbb{F}_\ell)^{(q)}$ is $\#\mathrm{GSp}_4(\mathbb{F}_\ell)^{(q)}/\ell^2$.

Consequently, at least for ℓ unramified in K_f, we measure the departure of the frequency of occurrence of f from the average such frequency by

$$v_\ell(f) = \frac{\#\{\gamma \in \mathrm{GSp}_4(\mathbb{F}_\ell)^{(q)} : f_\gamma \equiv f \bmod \ell\}}{\#\mathrm{GSp}_4(\mathbb{F}_\ell)^{(q)}/\ell^2}. \tag{4.1}$$

(An extension of this definition to all $\ell \neq p$ is given below in (5.1).)

4.2 $v_p(f)$

By way of motivation, suppose that $X/\mathbb{F}_q$ is an ordinary abelian surface, with characteristic polynomial of Frobenius $f_{X/\mathbb{F}_q}(T) = T^4 - a_X T^3 + b_X T^2 - q a_X T + q^2$. Since X is ordinary (and $\mathbb{F}_q$ is perfect), there is a canonical decomposition $X[p] \cong X[p]^{\mathrm{et}} \oplus X[p]^{\mathrm{tor}}$ of the p-torsion group scheme into étale and toric components. Note that $X_p := X[p](\overline{\mathbb{F}}_q)$ is actually $X[p]^{\mathrm{et}}(\overline{\mathbb{F}}_q) \cong (\mathbb{Z}/p)^2$. The $\mathbb{F}_q$-rational structure of $X[p]^{\mathrm{et}}$ is captured by the action of the q-power Frobenius on X_p. In fact, $\varpi_{X/\mathbb{F}_q}$ acts invertibly on X_p, with characteristic polynomial $g_{X/\mathbb{F}_q}(T) := T^2 - a_X T + b_X \bmod p$.

Now, $X[p]^{\mathrm{tor}}$ is connected, and specifically $X[p]^{\mathrm{tor}}(\overline{\mathbb{F}}_q)$ is a single point, but its Cartier dual is étale. In particular $(X[p]^{\mathrm{tor}})^*(\overline{\mathbb{F}}_q) \cong (\mathbb{Z}/p)^2$, and the action of Frobenius on this Galois module (again) has characteristic polynomial $g_{X/\mathbb{F}_q}(T)$.

Finally, recall that the Frobenius operator must preserve the canonical decomposition of $X[p]$ into its étale and toric parts.

https://doi.org/10.4153/CMB-2015-050-8 Published online by Cambridge University Press

Because of these considerations, we set

$$v_p(f) = \frac{\#\{\gamma \in \mathrm{GSp}_4(\mathbb{F}_p)^{(b^2)} : f_\gamma \equiv (T^2 - aT + b)^2 \bmod p \text{ and } \gamma \text{ semisimple}\}}{\#\,\mathrm{GSp}_4(\mathbb{F}_p)^{(b^2)}/p^2}.$$

4.3 $v_\infty(f)$

It remains to define an archimedean term; our choice comes from the Sato–Tate measure, which (conjecturally) explains the distribution of Frobenius elements of abelian surfaces.

Recall that semisimple conjugacy classes in the compact group USp_4 are parametrized by ("Frobenius angles") $0 \le \theta_1 \le \theta_2 \le \pi$. The Sato–Tate measure on the space of Frobenius angles is simply the pushforward of Haar measure. Explicitly, the Weyl integration formula [11, p. 218, 7.8B] shows that this measure is

$$\mu_{\mathrm{ST}}(\theta_1, \theta_2) = \frac{16}{\pi^2}\big(\cos(\theta_2) - \cos(\theta_1)\big)^2 \sin^2(\theta_1)\sin^2(\theta_2)\, d\theta_1\, d\theta_2.$$

Once q is fixed, a pair of angles $\{\theta_1, \theta_2\}$ gives rise to a q-Weil polynomial

$$\prod_{j=1,2}\big(T - \sqrt{q}\exp(i\theta_j)\big)\big(T - \sqrt{q}\exp(-i\theta_j)\big);$$

the induced measure on the space of q-Weil polynomials is

$$\mu_{\mathrm{ST}}(a, b) = \frac{1}{4q^3\pi^2}\sqrt{(a^2 - 4b + 8q)(b^2 + 4bq + 4q^2 - 4a^2q)}\, da\, db.$$

Note that, since there are approximately $q^{\dim \mathcal{A}_2} = q^3$ principally polarized abelian surfaces over $\mathbb{F}_q$, abelian varieties, $q^3\mu_{\mathrm{ST}}(a, b)$ is a sort of archimedean prediction for $\#\mathcal{A}_2(\mathbb{F}_q; f)$. Guided by this and the calculations of Lemma 2.2, we set

$$v_\infty(f) = \frac{1}{\mathrm{cond}(f)\,4\pi^2}\sqrt{\left|\frac{\Delta_f}{\Delta_{f^+}}\right|}. \tag{4.2}$$

5 The Shape of Frobenius

Fix a q-Weil polynomial satisfying Conditions (W.1)–(W.4). To ease notation slightly, we will write K for K_f and, given Condition (W.4), write $\mathcal{O}_K$ for $\mathcal{O}_f$. Suppose $X/\mathbb{F}_q$ is a principally polarized abelian variety such that $\mathcal{O}_K \subseteq \mathrm{End}(X)$; we choose the polarization so that the Rosati involution on $\mathrm{End}(X)$ induces complex conjugation on $\mathcal{O}_K$. On ℓ-torsion, the principal polarization induces a symplectic pairing on X_ℓ; complex conjugation on $\mathcal{O}_K \otimes \mathbb{F}_\ell$ is adjoint with respect to this pairing, and we obtain $\rho_\ell(\varpi_f) \in \mathrm{GSp}(X_\ell)$. Our goal in this section is to relate the shape of $\rho_\ell(\varpi_f)$ (in the sense of Section 3.2) to the structure of $f(T) \bmod \ell$.

Of course, all of this can be formulated without recourse to abelian varieties. Let $\kappa(\ell) = \mathcal{O}_K \otimes \mathbb{F}_\ell$; it is a four-dimensional vector space over $\mathbb{F}_\ell$. Choose a symplectic pairing $\langle\cdot,\cdot\rangle$ on $\kappa(\ell)$ for which complex conjugation on $\mathcal{O}_K \otimes \mathbb{F}_\ell$ is the adjoint with respect to $\langle\cdot,\cdot\rangle$. (If $\ell \nmid \Delta_K$, one can explicitly construct such a pairing as follows.

https://doi.org/10.4153/CMB-2015-050-8 Published online by Cambridge University Press

Choose $\alpha \in \mathcal{O}_K$ relatively prime to ℓ such that $\overline{\alpha} = -\alpha$. Then the reduction modulo ℓ of the pairing

$$\begin{aligned} \mathcal{O}_K \times \mathcal{O}_K &\longrightarrow \mathbb{Z} \\ (x, y) &\longmapsto \operatorname{tr}_{K/\mathbb{Q}}(\alpha x \overline{y}) \end{aligned}$$

is a suitable form.) Such a form is canonically defined up to scaling, and in particular its group of symplectic similitudes is independent of the choice of form.

Then $\bar{\omega}_f$ acts on $\kappa(\ell)$. Let γ_ℓ be the image of $\bar{\omega}_f$ in $\mathrm{GSp}(\kappa(\ell))$; our goal is to use the splitting behavior of $f(T)$ mod ℓ to compute the *cyclic shape* of γ_ℓ, *i.e.,* the shape of any cyclic element whose semisimplification is conjugate to γ_ℓ.

In fact, we define

$$\nu_\ell(f) = \frac{\#\{\gamma \in \mathrm{GSp}_4(\mathbb{F}_\ell) : \gamma \text{ is cyclic, with semisimplification } \gamma_\ell\}}{\#\,\mathrm{GSp}_4(\mathbb{F}_\ell)^{(q)}/\ell^2}. \tag{5.1}$$

Lemma 5.1 *If $\ell \nmid p\Delta_K$, then definitions* (4.1) *and* (5.1) *coincide.*

Proof If $\ell \nmid p\Delta_K$, then $\ell \nmid \Delta_f$. Therefore, $f(T)$ mod ℓ has distinct roots, and γ_ℓ is regular semisimple. The classification in Table 3.1 shows that if $f(T)$ mod ℓ is either irreducible or a product of linear factors, then any element with characteristic polynomial $f(T)$ mod ℓ is actually conjugate to γ_ℓ. If $f(T)$ mod ℓ is a product of distinct irreducible quadratic polynomials, then the possible shapes of γ_ℓ are distinguished by their multiplier, but one knows that the multiplier of γ_ℓ is q. The claim now follows once one recalls that a regular semisimple element is cyclic. ∎

Note that, tautologically, the characteristic polynomial of γ_ℓ is exactly the reduction of $f(T)$. If, for instance, $f(T)$ mod ℓ is irreducible, then a moment's reflection (or a glance at Tables 3.1 and 3.2) reveals that γ_ℓ is **Quartic**.

However, it sometimes happens (*e.g.,* with **DQ-S** and **DQ-I**) that the factorization pattern of f alone does not determine the shape of γ.

Since $\kappa(\ell) = \mathcal{O}_K/\ell \cong \mathbb{F}_\ell[T]/f(T)$ (Corollary 2.3), the factorization of $f(T)$ mod ℓ is precisely determined by the splitting of ℓ in $\mathcal{O}_K$. We have

$$\kappa(\ell) \cong \bigoplus_{\lambda \mid \ell} \kappa(\ell)_\lambda,$$

where λ ranges over all primes of K which lie over ℓ. (In fact, the dimension of $\kappa(\ell)_\lambda$ over the residue field $\mathcal{O}_K/\lambda$ is $e(\lambda/\ell)$, the ramification index of λ.)

For the sequel, it is worth singling out the following immediate observation.

Lemma 5.2 *The symplectic pairing induces a perfect duality between $\kappa(\ell)_\lambda$ and $\kappa(\ell)_{\overline{\lambda}}$.*

Proof We have chosen $\langle \cdot, \cdot \rangle$ such that the involution induced by complex conjugation is the adjoint with respect to $\langle \cdot, \cdot \rangle$. ∎

Consider a finite Galois extension $L/\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) = G$. If ℓ is a rational prime and λ is a prime of $\mathcal{O}_L$ lying over ℓ, the decomposition group and inertia group of λ

https://doi.org/10.4153/CMB-2015-050-8 Published online by Cambridge University Press

are, respectively,

$$D(\lambda/\ell) = \{\sigma \in G : \sigma(\lambda) = \lambda\}$$
$$I(\lambda/\ell) = \{\sigma \in G : \forall \beta \in \mathcal{O}_L, \sigma(\beta) \equiv \beta \bmod \lambda\}.$$

Then $I(\lambda/\ell)$ is normal in $D(\lambda/\ell)$. In fact, we will only use these notions for the abelian extension $K/\mathbb{Q}$, and thus the inertia and decomposition groups depend only on ℓ, and not on the choice of λ. Hence we write $I(\ell)$ and $D(\ell)$ for $I(\lambda/\ell)$ and $D(\lambda/\ell)$.

Let $f(T) \equiv \prod_{1\le j\le r} g_j(T)^{e_j} \bmod \ell$ be the factorization of $f(T)$ mod ℓ into irreducible monic polynomials. Since $\mathcal{O}_K/\ell \cong \mathbb{F}_\ell[T]/f(T)$, there are r primes, $\lambda_1, \dots, \lambda_r$ of K lying over ℓ; $\mathcal{O}_K/\lambda_i$ has degree $\deg g_i$ over $\mathbb{F}_\ell$; and the ramification index of λ_i is e_i. Note that the quantities $\deg g_i$ and e_i are independent of i as $K/\mathbb{Q}$ is Galois. (This is why we restricted to relevant conjugacy classes in Section 3.2.)

Finally, if $\ell \nmid \Delta_f$ then there exists an element of $\mathrm{Gal}(K/\mathbb{Q})$ which induces the canonical generator of $\mathrm{Gal}(\kappa(\lambda)/\mathbb{F}_\ell)$. Let $\mathrm{Frob}_K(\ell) \in \mathrm{Gal}(K/\mathbb{Q})$ be this element, called the *Frobenius endomorphism* of λ over ℓ.

5.1 K Cyclic

Suppose that $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic, with generator σ. Note that complex conjugation is given by $\iota = \sigma^2$. We classify the splitting behavior of rational primes ℓ in K by enumerating the possibilities for $D(\ell)$ and $I(\ell)$.

Lemma 5.3 *Suppose f satisfies Conditions* (W.1)–(W.4) *with cyclic Galois group generated by σ. Let $\ell \neq p$ be a rational prime. The cyclic shape of γ_ℓ is determined by the decomposition and inertia groups $D(\ell)$ and $I(\ell)$ as in Table* 5.1.

Thus, for instance, Lemma 5.3 asserts that if $D(\ell) = \langle\sigma^2\rangle$ and $I(\ell) = \langle 1\rangle$, then γ_ℓ has cyclic shape **DQ-S**. Note that if γ_ℓ has cyclic shape **RQ-2**, then there are two conjugacy classes with cyclic shape γ_ℓ. Otherwise, the cyclic shape of γ_ℓ determines a unique conjugacy class.

Proof In Table 5.1, we have enumerated all of the possibilities for pairs of subgroups $I(\ell) \subseteq D(\ell) \subseteq \mathrm{Gal}(K/\mathbb{Q})$. For each such pair, in the prime factorization of $f(T)$ mod ℓ, there are $r = \#\mathrm{Gal}(K/\mathbb{Q})/\#D(\ell)$ distinct irreducible factors. Each has degree $f = \#D(\ell)/\#I(\ell)$ and multiplicity $e = \#I(\ell)$. When $I(\ell) \subseteq D(\ell)$ is either $\{1\} \subseteq \{1\}$, $\{1\} \subset \langle\sigma\rangle$, or $\langle\sigma\rangle \subseteq \langle\sigma\rangle$, this factorization pattern already determines the cyclic shape of γ_ℓ.

Of the remaining cases, we first consider those in which $D(\ell) = \langle\sigma^2\rangle$. Let λ be one of the two primes of K lying over ℓ. Lemma 5.2 shows that $\kappa(\ell)_\lambda$ is symplectic if and only if complex conjugation stabilizes λ, *i.e.,* if and only if $\iota = \sigma^2 \in D(\ell)$. Since this happens in the two cases under consideration, the induced decomposition is symplectic and the cyclic shape of γ_ℓ is the **S** variant.

Finally, we analyze the situation in which $I(\ell) = \langle\sigma^2\rangle \subset D(\ell) = \langle\sigma\rangle$; we must decide whether the cyclic shape is **RQ-1** or **RQ-2**. Let λ be the prime of K lying over ℓ.

https://doi.org/10.4153/CMB-2015-050-8 Published online by Cambridge University Press

Consider the Frobenius element ϖ_f as an element of $\mathcal{O}_K$. Then

$$f(T) = \prod_{0 \le j \le 3} (T - \sigma^j(\varpi_f)).$$

The ramification hypothesis implies that $\sigma^2(\varpi_f) \equiv \varpi_f \bmod \lambda$, and we have the factorization $f(T) \equiv g(T)^2 \bmod \lambda$ where

$$g(T) \equiv (T - \varpi_f)\big(T - \sigma(\varpi_f)\big) \bmod \lambda.$$

By comparing constant terms, we find that $(\varpi_f \sigma(\varpi_f))^2 \equiv q^2 \bmod \lambda$, and in particular $\varpi_f \sigma(\varpi_f) \equiv \pm q \bmod \lambda$. However, if we had $\varpi_f \sigma(\varpi_f) \equiv q \bmod \lambda$, then we would know that $\sigma(\varpi_f) \equiv \sigma^2(\varpi_f) \bmod \lambda$, which contradicts the hypothesis that $\sigma \notin I(\ell)$.

Therefore, the constant term of the irreducible factor $g(T)$ is $-q \bmod \lambda$, and the cyclic shape of γ_ℓ is **RQ-2**. ∎

$D(\ell)$	$I(\ell)$	$\mathrm{Frob}_K(\ell)$	(e, f, r)	Class shape
$\{1\}$	$\{1\}$	1	(1,1,4)	**Split**
$\langle\sigma^2\rangle$	$\{1\}$	σ^2	(1,2,2)	**DQ-S**
$\langle\sigma^2\rangle$	$\langle\sigma^2\rangle$	-	(2,1,2)	**DRL-S**
$\langle\sigma\rangle$	$\{1\}$	σ or σ^3	(1,4,1)	**Quartic**
$\langle\sigma\rangle$	$\langle\sigma^2\rangle$	-	(2,2,1)	**RQ-2**
$\langle\sigma\rangle$	$\langle\sigma\rangle$	-	(4,1,1)	**QRL**

Table 5.1: Prime factorizations and conjugacy class shapes for $K/\mathbb{Q}$ cyclic

5.2 K Biquadratic

Suppose instead that $K = \mathrm{Split}(f)$ is biquadratic. Then K is the compositum of quadratic imaginary fields K_1 and K_2, and we have

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(K_1/\mathbb{Q}) \oplus \mathrm{Gal}(K_2/\mathbb{Q}) \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2.$$

Let τ_i generate $\mathrm{Gal}(K/K_i)$. Then complex conjugation is given by $\iota = \tau_1\tau_2$; its fixed field is the real quadratic subfield K^+. We again classify the splitting behavior of primes ℓ by considering pairs $D(\ell)$ and $I(\ell)$.

Lemma 5.4 *Suppose f satisfies Conditions* (W.1)–(W.4) *with $K = K_f$ biquadratic. Let $\ell \neq p$ be a rational prime. The cyclic shape of γ_ℓ is determined by the decomposition and inertia groups $D(\ell)$ and $I(\ell)$ as in Table* 5.2.

As before, the cyclic shape of γ_ℓ determines a unique conjugacy class except when that shape is either **DRL-S** or **RQ-2**. In these cases, there are two conjugacy classes with the cyclic shape given by γ_ℓ.

https://doi.org/10.4153/CMB-2015-050-8 Published online by Cambridge University Press

Proof Proceed as in the proof of Lemma 5.3. Note that, by Lemma 5.2, $\kappa(\ell)_\lambda$ is isotropic if and only if complex conjugation acts nontrivially on λ, *i.e.,* if and only if $\iota = \tau_1\tau_2 \notin D(\ell)$. In these cases the induced decomposition is isotropic and the cyclic shape of γ_ℓ is the **I** variant. All ambiguous cases where $r > 1$ can be identified by the action of the pairing on the induced decomposition.

Now (without loss of generality) suppose that $I(\ell) = \langle\tau_1\rangle \subset D(\ell) = \langle\tau_1, \tau_2\rangle$, and let λ be the prime lying over ℓ. As in Lemma 5.3, we recall that

$$f(T) \equiv (T - \varpi_f)(T - \tau_1(\varpi_f))(T - \tau_2(\varpi_f))(T - \tau_1\tau_2(\varpi_f)) \bmod \lambda.$$

The assumption on ramification implies that $\varpi_f \equiv \tau_1(\varpi_f) \bmod \lambda$, and thus that $\tau_2(\varpi_f) \equiv \tau_1\tau_2(\varpi_f) \bmod \lambda$. Therefore, $f(T)$ factors as

$$f(T) \equiv \big((T - \varpi_f)(T - \tau_2(\varpi_f))\big)^2 \bmod \lambda.$$

Moreover, $\varpi_f\tau_2(\varpi_f) \equiv \varpi_f\tau_1\tau_2(\varpi_f) \equiv q \bmod \lambda$. Therefore, $f(T) \equiv g(T)^2 \bmod \lambda$ where $g(0) = q$, and the cyclic shape of γ_ℓ is **RQ-1**.

The remaining cases follow in an analogous fashion. ∎

$D(\ell)$	$I(\ell)$	$\mathrm{Frob}_K(\ell)$	(e, f, r)	Class shape
$\{1\}$	$\{1\}$	1	(1,1,4)	**Split**
$\langle\tau_i\rangle$	$\{1\}$	τ_i	(1,2,2)	**DQ-I**
$\langle\tau_i\rangle$	$\langle\tau_i\rangle$	-	(2,1,2)	**DRL-I**
$\langle\tau_1\tau_2\rangle$	$\{1\}$	$\tau_1\tau_2$	(1,2,2)	**DQ-S**
$\langle\tau_1\tau_2\rangle$	$\langle\tau_1\tau_2\rangle$	-	(2,1,2)	**DRL-S**
$\langle\tau_1, \tau_2\rangle$	$\langle\tau_i\rangle$	-	(2,2,1)	**RQ-1**
$\langle\tau_1, \tau_2\rangle$	$\langle\tau_1\tau_2\rangle$	-	(2,2,1)	**RQ-2**

Table 5.2: Prime factorizations and conjugacy class shapes for $K/\mathbb{Q}$ biquadratic

6 Local Terms for K

Let $\mathrm{Gal}(K/\mathbb{Q})^*$ be the character group of the Galois group of K. For $\chi \in \mathrm{Gal}(K/\mathbb{Q})^*$, let K^χ be the subfield of K fixed by $\ker\chi$. For a rational prime ℓ, let

$$\chi(\ell) = \chi(\mathrm{Frob}_{K^\chi}(\ell))$$

if ℓ is unramified in K^χ, and let $\chi(\ell) = 0$ otherwise.

Since K^+ is a subextension of K, $\mathrm{Gal}(K^+/\mathbb{Q})^*$ is naturally a subgroup of $\mathrm{Gal}(K/\mathbb{Q})^*$, and we define

$$v_\ell(K) = \prod_{\chi \in S(K)} \frac{1}{1 - \chi(\ell)/\ell}, \tag{6.1}$$

where

$$S(K) = \mathrm{Gal}(K/\mathbb{Q})^* \smallsetminus \mathrm{Gal}(K^+/\mathbb{Q})^*.$$

https://doi.org/10.4153/CMB-2015-050-8 Published online by Cambridge University Press

6.1 K Cyclic

As in Section 5.1, let $\mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma\rangle$. Let χ be a faithful character of $\mathrm{Gal}(K/\mathbb{Q})$, so that $\overline{\chi} := \chi \circ \iota$ is the other faithful character of $\mathrm{Gal}(K/\mathbb{Q})$ and $S(K) = \{\chi, \overline{\chi}\}$.

Lemma 6.1 *Let ℓ be a rational prime. The multiset of values $\{\chi(\ell), \overline{\chi}(\ell)\}$ is determined by the decomposition and inertia groups $D(\ell)$ and $I(\ell)$ as in Table 6.1.*

Proof This follows from the definition of $\{\chi, \overline{\chi}\}$ and the calculation of Frobenius elements in Lemma 5.3. In particular, $\{\chi(\ell), \overline{\chi}(\ell)\}$ depends only on the order of $D(\ell)$ and $I(\ell)$, and not on their canonical generators. It is also independent of the choice of generator of $\mathrm{Gal}(K/\mathbb{Q})^*$. ■

$D(\ell)$	$I(\ell)$	$\{\chi(\ell), \overline{\chi}(\ell)\}$	Class shape
$\{1\}$	$\{1\}$	$\{1,1\}$	**Split**
$\langle\sigma^2\rangle$	$\{1\}$	$\{-1,-1\}$	**DQ-S**
$\langle\sigma^2\rangle$	$\langle\sigma^2\rangle$	$\{0,0\}$	**DRL-S**
$\langle\sigma\rangle$	$\{1\}$	$\{-i,i\}$	**Quartic**
$\langle\sigma\rangle$	$\langle\sigma^2\rangle$	$\{0,0\}$	**RQ-2**
$\langle\sigma\rangle$	$\langle\sigma\rangle$	$\{0,0\}$	**QRL**

Table 6.1: Values of imaginary characters on Frobenius elements for $K/\mathbb{Q}$ cyclic.

6.2 K Biquadratic

As in Section 5.2, let $\mathrm{Gal}(K/\mathbb{Q}) = \langle\tau_1, \tau_2\rangle$. Denote the quadratic imaginary subfields of K by K_1 and K_2 and let $\mathrm{Gal}(K/K_i) = \langle\tau_i\rangle$. For $i \in \{1,2\}$, define the character

$$\phi_i(\tau_j) := \begin{cases} -1 & i = j, \\ 1 & i \neq j. \end{cases}$$

Then $S(K) = \{\phi_1, \phi_2\}$.

Lemma 6.2 *Let ℓ be a rational prime. The multiset of values $\{\phi_1(\ell), \phi_2(\ell)\}$ is determined by the decomposition and inertia groups $D(\ell)$ and $I(\ell)$ as in Table 6.2.*

6.3 Matching

In this section, we show that each of the local factors naïvely assigned to f matches a factor intrinsic to the splitting field $K = K_f$.

Proposition 6.3 *If $\ell \neq p$, then $v_\ell(f) = v_\ell(K)$.*

https://doi.org/10.4153/CMB-2015-050-8 Published online by Cambridge University Press

$D(\ell)$	$I(\ell)$	$\{\phi_1(\ell), \phi_2(\ell)\}$	Class shape
$\{1\}$	$\{1\}$	$\{1,1\}$	**Split**
$\langle\tau_i\rangle$	$\{1\}$	$\{-1,1\}$	**DQ-I**
$\langle\tau_i\rangle$	$\langle\tau_i\rangle$	$\{0,1\}$	**DRL-I**
$\langle\tau_1\tau_2\rangle$	$\{1\}$	$\{-1,-1\}$	**DQ-S**
$\langle\tau_1\tau_2\rangle$	$\langle\tau_1\tau_2\rangle$	$\{0,0\}$	**DRL-S**
$\langle\tau_1,\tau_2\rangle$	$\langle\tau_i\rangle$	$\{0,-1\}$	**RQ-1**
$\langle\tau_1,\tau_2\rangle$	$\langle\tau_1\tau_2\rangle$	$\{0,0\}$	**RQ-2**

Table 6.2: Values of imaginary characters on Frobenius elements for $K/\mathbb{Q}$ biquadratic.

Proof Let γ_ℓ be as in Section 5. We first assume that the cyclic shape of γ_ℓ determines a unique conjugacy class in $\mathrm{GSp}_4(\mathbb{F}_\ell)$, and then indicate what must be changed to accommodate the remaining cases.

Thus, let γ be any cyclic element whose semisimplification is γ_ℓ, and assume the shape of γ is neither **DRL-S** nor **RQ-2**. By Lemmas 6.1 and 6.2, the set of character values $\{\chi(\ell)\colon \chi \in S(K)\}$ depends only on the shape of γ; and tautologically, the size of the conjugacy class $\mathcal{C}(\gamma)$ only depends on the shape of γ, as well.

On one hand, by (5.1) we have

$$\nu_\ell(f) = \frac{\#\mathcal{C}(\gamma)}{\#\,\mathrm{GSp}_4(\mathbb{F}_\ell)^{(q)}/\ell^2} = \frac{\#\,\mathrm{GSp}_4(\mathbb{F}_\ell)/\#\mathcal{Z}(\gamma)}{\#\,\mathrm{GSp}_4(\mathbb{F}_\ell)^{(q)}/\ell^2} = \frac{\ell^2(\ell-1)}{\#\mathcal{Z}(\gamma)}.$$

Lemmas 3.1 and 3.2 supply column 2 of Table 6.3, and applying this simple calculation provides column 3.

On the other hand, recall that (6.1) gives

$$\nu_\ell(K) = \prod_{\chi\in S(K)} \frac{1}{1-\chi(\ell)/\ell}.$$

Lemmas 6.1 and 6.2 provide column 4 of Table 6.3, and we compute column 5 using (6.1).

If γ_ℓ has cyclic shape of type **DRL-S** or **RQ-2**, then there are two cyclic conjugacy classes with semisimplification γ_ℓ. For a representative γ of each class,

$$\#\mathcal{C}(\gamma)/\left(\#\,\mathrm{GSp}_4(\mathbb{F}_\ell)^{(q)}/\ell^2\right) = \frac{1}{2},$$

and thus $\nu_\ell(f) = \frac{1}{2} + \frac{1}{2}$.

As columns 3 and 5 are equal, the theorem is proven. ∎

Similarly, we have the following lemma.

Lemma 6.4 *We have* $\nu_p(f) = \nu_p(K)$.

https://doi.org/10.4153/CMB-2015-050-8 Published online by Cambridge University Press

Class shape	$\#\mathcal{Z}(\gamma)$	$\nu_\ell(f)$	$\{\chi(\ell) : \chi \in S(K)\}$	$\nu_\ell(K)$
Split	$(\ell-1)^3$	$\frac{\ell^2}{(\ell-1)^2}$	$\{1,1\}$	$\frac{\ell}{\ell-1}\cdot\frac{\ell}{\ell-1}$
DQ-S	$(\ell+1)^2(\ell-1)$	$\frac{\ell^2}{(\ell+1)^2}$	$\{-1,-1\}$	$\frac{\ell}{\ell+1}\cdot\frac{\ell}{\ell+1}$
DQ-I	$(\ell+1)(\ell-1)^2$	$\frac{\ell^2}{\ell^2-1}$	$\{-1,1\}$	$\frac{\ell}{\ell+1}\cdot\frac{\ell}{\ell-1}$
Quartic	$(\ell^2+1)(\ell-1)$	$\frac{\ell^2}{\ell^2+1}$	$\{-i,i\}$	$\frac{\ell}{\ell-i}\cdot\frac{\ell}{\ell+i}$
QRL	$\ell^2(\ell-1)$	1	$\{0,0\}$	$1\cdot 1$
DRL-S	$2\ell^2(\ell-1)$	1	$\{0,0\}$	$1\cdot 1$
DRL-I	$\ell(\ell-1)^2$	$\frac{\ell}{\ell-1}$	$\{0,1\}$	$\frac{\ell}{\ell-1}\cdot 1$
RQ-1	$\ell(\ell^2-1)$	$\frac{\ell}{\ell+1}$	$\{-1,0\}$	$\frac{\ell}{\ell+1}\cdot 1$
RQ-2	$2\ell^2(\ell-1)$	1	$\{0,0\}$	$1\cdot 1$

Table 6.3: $\nu_\ell(f)$ and $\nu_\ell(K)$

Proof Since we have assumed p unramified in K (W.3), $g(T) := T^2 - aT + b$ is not a square. For convenience, we recall the definition

$$\nu_p(f) = \frac{\#\{\gamma \in \mathrm{GSp}_4(\mathbb{F}_p)^{(b^2)} : f_\gamma(T) \equiv g(T)^2 \bmod p \text{ and } \gamma \text{ semisimple}\}}{\#\,\mathrm{GSp}_4(\mathbb{F}_p)^{(b^2)}/p^2}.$$

First suppose that $K/\mathbb{Q}$ is cyclic. Then p splits completely in K (*e.g.*, [6, Table 3]), and $g(T)$ factors (in $\mathbb{F}_p$). The set of *semisimple* elements with characteristic polynomial $g(T)^2$ has the same cardinality as a conjugacy class of type **Split**. From (the first line of) Table 6.3, we see that $\nu_p(f) = \nu_p(K)$.

Now instead suppose that $K/\mathbb{Q}$ is biquadratic. Then either p splits completely in K, or p splits in exactly one of the K_i ([6, Table 4]). The former case has already been addressed. For the latter case, the set of semisimple elements with characteristic polynomial $g(T)^2$ has the same cardinality as a conjugacy class of type **DQ-I**. Again we conclude from Table 6.3 that $\nu_p(f) = \nu_p(K)$. ∎

Finally, we compute the following lemma.

Lemma 6.5 *We have*

$$\nu_\infty(f) = \frac{1}{4\pi^2}\sqrt{\left|\frac{\Delta_K}{\Delta_{K^+}}\right|}.$$

Proof From Lemma 2.2 we have $\mathrm{cond}(f) = q$ and $\Delta_f = q^2\Delta_K$. Also, Lemma 2.4 implies that $\Delta_{f^+} = \Delta_{K^+}$. Then (4.2) gives the result. ∎

https://doi.org/10.4153/CMB-2015-050-8 Published online by Cambridge University Press

6.4 Comparison with [5]

As we mentioned in the introduction, this work is inspired by Gekeler's work [5] with ordinary isogeny classes of elliptic curves over $\mathbb{F}_p$. He starts with an ordinary quadratic p-Weil polynomial $g(T)$; defines

$$v_\ell^{\mathrm{G}}(g) = \lim_{r\to\infty} \frac{\#\{\gamma \in \mathrm{GL}_2(\mathbb{Z}/\ell^r)^{(q)} : f_\gamma \equiv g \bmod \ell^r\}}{\#\,\mathrm{GL}_2(\mathbb{Z}/\ell^r)^{(q)}/\ell^r}; \tag{6.2}$$

and among other results shows ([5, Cor. 4.8]) that if $\ell^2 \nmid \Delta_g$, then

$$v_\ell^{\mathrm{G}}(g) = \frac{1}{1-\chi(\ell)/\ell},$$

where χ is the quadratic character of the splitting field of g.

If $\ell \nmid \Delta_g$, then the centralizer of an element with characteristic polynomial g is smooth over $\mathbb{Z}_\ell$, and thus setting $r = 1$ in the right-hand side of (6.2) already calculates the limiting value. If ℓ, but not its square, divides Δ_g, then (6.2) does not stabilize at $r = 1$. However, if instead we ask for the proportion of *cyclic* elements of $\mathrm{GL}_2(\mathbb{F}_\ell)$ with characteristic polynomial $f_\gamma \equiv g \bmod \ell$, then we again have a finite expression that computes $v_\ell^{\mathrm{G}}(g)$.

Returning to the context of abelian surfaces, the same "smoothness of centralizers" argument shows that if $\ell \nmid \Delta_f$, then the proportion in (4.1) calculates the GSp_4-analogue of the limit in (6.2). Condition (W.4), which corresponds to the local condition $\ell^2 \nmid \Delta_g$, is why passing to the cyclic shape in (5.1) again allows us to compute in $\mathbb{F}_\ell$, as opposed to $\mathbb{Z}_\ell$.

7 Main Result

In the following, we will have several occasions to consider conditionally convergent infinite products. For a sequence of numbers $\{a_\ell\}$ indexed by finite primes, let

$$\prod_\ell a_\ell = \lim_{X\to\infty} \prod_{\ell<X} a_\ell. \tag{7.1}$$

With this convention, we have $\left(\prod_\ell a_\ell\right)\cdot\left(\prod_\ell b_\ell\right) = \prod_\ell (a_\ell b_\ell)$.

For a number field L, let $h(L)$, ω_L and R_L denote, respectively, the class number, number of roots of unity, and regulator of L.

Theorem 7.1 *Let f be a degree 4 q-Weil polynomial that is ordinary, principally polarizable, Galois, and maximal. Let K_f be the splitting field of f, and let K_f^+ be its maximal totally real subfield. Then*

$$v_\infty(f)\prod_\ell v_\ell(f) = \frac{1}{\omega_K}\frac{h(K_f)}{h(K_f^+)}. \tag{7.2}$$

Proof We write K and K^+ for K_f and K_f^+. By the analytic class number formula, the ratio of class numbers on the right-hand side of (7.2) is

$$\frac{h(K)}{h(K^+)} = \lim_{s\to 1}\frac{(s-1)\zeta_K(s)}{(s-1)\zeta_{K^+}(s)}\frac{\sqrt{|\Delta_K|}2^2\omega_K R_{K^+}}{\sqrt{|\Delta_{K^+}|}(2\pi)^2\omega_{K^+}R_K}.$$

https://doi.org/10.4153/CMB-2015-050-8 Published online by Cambridge University Press

For a finite abelian extension $L/\mathbb{Q}$, we have

$$\lim_{s\to 1}(s-1)\zeta_L(s) = \prod_{\chi\in \mathrm{Gal}(L/\mathbb{Q})^*\smallsetminus \mathrm{id}} L(1,\chi),$$

where the product is over nontrivial characters of $\mathrm{Gal}(L/\mathbb{Q})$, and, as in (7.1), we interpret $L(1,\chi)$ as the conditionally convergent product

$$L(1,\chi) = \lim_{X\to\infty} \prod_{\ell<X} \frac{1}{1-\chi(\ell)/\ell}.$$

With our convention on conditionally convergent products,

$$\prod_{\chi\in \mathrm{Gal}(L/\mathbb{Q})^*\smallsetminus \mathrm{id}} L(1,\chi) = \prod_{\ell}\Big(\prod_{\chi\in \mathrm{Gal}(L/\mathbb{Q})^*\smallsetminus \mathrm{id}} \frac{1}{1-\chi(\ell)/\ell}\Big).$$

By hypothesis K and K^+ are abelian, as they are Galois over $\mathbb{Q}$ of degrees 4 and 2, respectively. By definition (6.1), for each ℓ,

$$\frac{\prod_{\chi\in \mathrm{Gal}(K/\mathbb{Q})^*\smallsetminus \mathrm{id}} \frac{1}{1-\chi(\ell)/\ell}}{\prod_{\chi\in \mathrm{Gal}(K^+/\mathbb{Q})^*\smallsetminus \mathrm{id}} \frac{1}{1-\chi(\ell)/\ell}} = v_\ell(K).$$

Finally, $\mathcal{O}_K^\times$ and $\mathcal{O}_{K^+}^\times$ agree up to torsion, so $R_K = 2R_{K^+}$, and K^+ is a real field, so $\omega_{K^+} = 2$. Consequently,

$$\frac{h(K)}{h(K^+)} = \omega_K \frac{1}{4\pi^2}\sqrt{\frac{|\Delta_K|}{|\Delta_{K^+}|}} \prod_\ell v_\ell(K) = \omega_K v_\infty(f)\prod_\ell v_\ell(f)$$

by Proposition 6.3 and Lemmas 6.4 and 6.5. ∎

In fact, (7.2) has a natural interpretation in terms of abelian varieties.

Corollary 7.2 *For f as in Theorem 7.1, suppose further that $\mathrm{Gal}(K_f/\mathbb{Q})$ is cyclic. Then*

$$v_\infty(f)\prod_\ell v_\ell(f) = \#\mathcal{A}_2(\mathbb{F}_q; f), \tag{7.3}$$

the number of isomorphism classes of principally polarized abelian surfaces over $\mathbb{F}_q$ with characteristic polynomial of Frobenius f, weighted by (inverse) size of automorphism group.

Proof If $(X,\lambda)\in \mathcal{A}_2(\mathbb{F}_q; f)$, then $\#\operatorname{Aut}(X,\lambda) = \omega_K$. By [2], $h(K)/h(K^+)$ is the (unweighted) size of $\mathcal{A}_2(\mathbb{F}_q; f)$. Indeed, under the hypothesis that $\mathrm{Gal}(K_f/\mathbb{Q})$ is cyclic of order 4 and the maximality Condition (W.4), [2, Thm. 3.1 and Cor. 3.2] show that the size of the isogeny class parametrized by f is (in their notation)

$$\#\mathfrak{C}(K) = \frac{h(K)}{h^+(K^+)}\big[(\mathcal{O}_{K^+}^\times)^+ : \mathrm{N}_{K/K^+}(\mathcal{O}_K^\times)\big],$$

where $h^+(K^+)$ denotes the narrow class group of K^+, and $(\mathcal{O}_{K^+}^\times)^+$ denotes the totally positive units of $\mathcal{O}_{K^+}$. Since

$$\big[(\mathcal{O}_{K^+}^\times)^+ : \mathrm{N}_{K/K^+}(\mathcal{O}_K^\times)\big] = \frac{h^+(K^+)}{h(K^+)},$$

https://doi.org/10.4153/CMB-2015-050-8 Published online by Cambridge University Press

we find that $\#\mathfrak{C}(K) = h(K)/h(K^+)$.

Now invoke Theorem 7.1. ∎

In fact, unpublished work of Howe shows that in much greater generality, $h(K)/h(K^+)$ computes the size of a suitable isogeny class. Thus, we expect (7.3) to also hold when K_f is biquadratic.

Acknowledgments We thank Everett Howe for sharing with us his work on principally polarized abelian varieties within a given isogeny class. We further thank the referee for helpful suggestions.

References

[1] J. Breeding II, *Irreducible characters of* $\mathrm{GSp}(4, q)$ *and dimensions of spaces of fixed vectors*. Ramanujan J. **36**(2015), no. 3, 305–354. http://dx.doi.org/10.1007/s11139-014-9622-3

[2] R. Bröker,D. Gruenewald, and K. Lauter, *Explicit CM theory for level 2-structures on abelian surfaces*. Algebra Number Theory **5**(2011), no. 4, 495–528. http://dx.doi.org/10.2140/ant.2011.5.495

[3] R. W. Carter, *Finite groups of Lie type*. Wiley Classics Library John Wiley & Sons Ltd., Chichester, 1993.

[4] J. Fulman, *A probabilistic approach to conjugacy classes in the finite symplectic and orthogonal groups*. J. Algebra **234**(2000), no. 1, 207–224. http://dx.doi.org/10.1006/jabr.2000.8455

[5] E.-U. Gekeler, *Frobenius distributions of elliptic curves over finite prime fields*. Int. Math. Res. Not. **37**(2003), 1999–2018.

[6] E. Z. Goren and K. E. Lauter, *Genus 2 curves with complex multiplication*. Int. Math. Res. Not. IMRN **5**(2012), 1068–1142.

[7] E. W. Howe, *Principally polarized ordinary abelian varieties over finite fields*. Trans. Amer. Math. Soc. **347**(1995), no. 7, 2361–2401. http://dx.doi.org/10.2307/2154828

[8] N. M. Katz, *Lang-Trotter revisited*. Bull. Amer. Math. Soc. (N.S.) **46**,(2009), no. 3, 413–457. http://dx.doi.org/10.1090/S0273-0979-09-01257-9

[9] K.-i. Shinoda, *The characters of the finite conformal symplectic group,* $\mathrm{CSp}(4, q)$. Comm. Algebra **10**(1982), no. 13, 1369–1419. http://dx.doi.org/10.1080/00927878208822782

[10] G. E. Wall, *On the conjugacy classes in the unitary, symplectic and orthogonal groups*. J. Austral. Math. Soc. **3**(1963), 1–62. http://dx.doi.org/10.1017/S1446788700027622

[11] H. Weyl, *The classical groups*. Princeton Landmarks in Mathematics, Princeton University Press, Princeton, NJ, 1997.

Colorado State University, Fort Collins, CO 80523-1874, USA
e-mail: achter@math.colostate.edu

James Madison University, Harrisonburg, VA 22807, USA
e-mail: willi5cl@jmu.edu