ABELIAN VARIETIES OVER FINITE FIELDS: AN INTRODUCTION

STEFANO MARSEGLIA

1. Abelian Varieties

1.1. **Basic definitions.** Let k be a field.

Definition 1.1. A *group variety* over a field k is a variety V together with morphisms

$$+ : V \times V \to V \text{ and } - : V \to V,$$

and a point $\varepsilon \in V(k)$ such that the structure on $V(\bar{k})$ defined by $+$ and $-$ is that of a group with multiplication induced by $+$, inverse by $-$ and identity element ε.

Equivalently, we can say that the quadruple $(V, +, -, \varepsilon)$ is a group object in the category of varieties over k.

Example 1.2. The requirement that $V(\bar{k})$ is a group with multiplication $+$, inverse $-$ and neutral element ε can be equivalently expressed using diagrams. For example, the diagrams

$$\begin{array}{ccccc} V \times V & & \xrightarrow{id \times -} & & V \times V \\ {\scriptstyle \text{diag}}\uparrow & & & & \downarrow{\scriptstyle +} \\ V & \longrightarrow & \text{Spec}(k) & \xrightarrow{\varepsilon} & V \end{array} \qquad \begin{array}{ccccc} V \times V & & \xrightarrow{- \times id} & & V \times V \\ {\scriptstyle \text{diag}}\uparrow & & & & \downarrow{\scriptstyle +} \\ V & \longrightarrow & \text{Spec}(k) & \xrightarrow{\varepsilon} & V \end{array}$$

encode the property for $- : V \to V$ to be the inverse.

For every geometric point $a \in V(\bar{k})$, the projection $V_{\bar{k}} \times V_{\bar{k}} \to V_{\bar{k}}$ induces an isomorphism $V_{\bar{k}} \times \{a\} \simeq V_{\bar{k}}$. We define the *translation t_a by a* as the composition

$$V_{\bar{k}} \simeq V_{\bar{k}} \times \{a\} \subset V_{\bar{k}} \times V_{\bar{k}} \xrightarrow{+} V_{\bar{k}}.$$

On points t_a acts as $P \mapsto m(P, a)$. In particular if $a \in V(k)$ then t_a maps V into V.

For any variety the non-singular locus U is open and non-empty. For a group variety V the translates of $U_{\bar{k}}$ cover $V_{\bar{k}}$, hence every group variety is non-singular.

Definition 1.3. A connected and complete group variety is called an *abelian variety.*

Definition 1.4. A *homomorphism* of abelian varieties is a morphism of varieties which is compatible with the group variety operation.

In the next proposition we will sum up some interesting properties of abelian varieties.

Proposition 1.5. *Let A be any abelian variety. Then*

- *every morphism $f : A \to B$ of abelian varieties is the composite of a homomorphism $h : A \to B$ with a translation t_b, where $b = -f(\varepsilon_A) \in B(k)$;*
- *the group law on A is commutative;*
- *A is projective.*

Date: January 21, 2025.

Example 1.6. An abelian variety of dimension one is the same as an *elliptic curve* E, that is, a smooth projective plane curve of degree 3 together with a chosen point. It is easy to describe elliptic curves embedded in a projective space in terms of equations. For example, if the characteristic of k is not 2 or 3 then E inside $\mathbb{P}^2 = \mathrm{Proj}(k[x,y])$ is given by an equation of the form

$$zy^2 = x^3 + axz^2 + bz^3,$$

for some $a, b \in k$ such that $4a^3 + 27b^2 \neq 0$ with marked point $(0:1:0)$. In this case it is possible to give explicit formulas for the addition of two points. The theory of elliptic curves is very rich and many results about them can be generalized to the higher dimensional case, but they will have a much more abstract flavor, since in general it is hard to find equations describing an abelian variety.

Exercise 1.7. Can you give an example of an abelian variety of dimension > 1?

Abelian varieties of dimension 1 can be described by one single equation in 3 projective variables. The situation is dramatically different in higher dimension. Already in dimension 2, in general, over an algebraically closed field, one needs 72 equations in 16 projective variables! If you want to see the actual eqautions, check out [CF96].

1.2. **Isogenies.** Among all morphisms between abelian varieties, the so-called isogenies play a special role since they allow us to split each abelian variety into a product of simple objects, see Corollary 1.18. In particular, over a finite field, we can classify and enumerate up to isogeny all abelian varieties of a given dimension, as we explain in Section 2.

Proposition 1.8. *Let $f : A \to B$ be a homomorphism of abelian varieties. The following are equivalent:*

(1) f is surjective and $\dim(A) = \dim(B)$;
(2) $\ker(f)$ is a finite group scheme and $\dim(A) = \dim(B)$;
(3) f is finite, flat and surjective.

Definition 1.9. A homomorphism $f : A \to B$ satisfying the conditions of 1.8 is called an *isogeny*. The *degree* of an isogeny is the degree of the function field extension $[k(A) : f^*k(B)]$.

Equivalently we can define the degree of an isogeny as the rank of its kernel as a group scheme. Observe that the composition of two isogenies is an isogeny and the degree is multiplicative with respect to composition.

Let n be a non-zero integer and consider the homomorphism multiplication by n, $[n]_A : A \to A$. Write $A[n] := \ker([n]_A)$.

Proposition 1.10. *The homomorphism $[n]_A$ is an isogeny. If $g = \dim(A)$ then $\deg([n]_A) = n^{2g}$.*

Proposition 1.11. *If $f : A \to B$ is an isogeny of degree d, then there exists an isogeny $g : B \to A$ such that $g \circ f = [d]_A$ and $f \circ g = [d]_B$.*

Corollary 1.12. *Being isogenous is an equivalence relation.*

When we one has an equivalence relation, the irresistible thing to do is to try to describe the equivalence classes! In order to so, we first show that an abelian variety is isogenous to a product of "simple" ones.

Let A and B be abelian variety over the field k. If f and g are homomorphisms from A to B then we can define a morphism

$$f + g = +_B \circ (f,g) : A \xrightarrow{(f,g)} B \times_k B \xrightarrow{+_B} B.$$

This shows that $\mathrm{Hom}_k(A,B)$ has the structure of an abelian group and that $\mathrm{End}_k(A)$ has a ring structure with composition as multiplication.

If $n \neq 0$ then $[n]_A$ is an isogeny and it is in particular surjective. This implies that $\mathrm{Hom}_k(A,B)$ is torsion-free. We define

$$\mathrm{Hom}_k^0(A,B) = \mathrm{Hom}_k(A,B) \otimes_{\mathbb{Z}} \mathbb{Q} \text{ and } \mathrm{End}_k^0(A) = \mathrm{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

The $\mathbb{Q}$-algebra $\mathrm{End}_k^0(A)$ is called the *endomorphism algebra* of A. Observe that every isogeny $f : A \to B$ becomes invertible in $\mathrm{Hom}_k^0(A,B)$.

Theorem 1.13 (Poincaré Splitting Theorem)**.** *Let A be an abelian variety over a field k. If $B \subset A$ is an abelian sub-variety then there exists an abelian sub-variety $C \subset A$ such that the homomorphism $f : B \times C \to A$ given by $(x,y) \mapsto x + y$ is an isogeny.*

Definition 1.14. An abelian variety A over the field k is *simple* if it does not have non-trivial sub-varieties, that is, if $B \subset A$ is a sub-variety, then $B = 0$ or $B = A$.

Exercise 1.15. Can you produce an example of a simple abelian variety? And a non-simple one?

Exercise 1.16. Let $f : A \to B$ be a homomorphism between abelian varieties. If A and B are simple then f is either zero or an isogeny.

Let k' be a field extension of k. An abelian variety defined over k and which is simple over k need not be simple also over k'.

Example 1.17. Let q be a power of a prime number and let a be an integer such that $|a| < 2\sqrt{q}$ and coprime with q. Take an elliptic curve E over $\mathbb{F}_{q^2}$ in the isogeny class determined by the polynomial $x^2 + ax + q^2$, see Section 2 for the definition. Let A be the Weil restriction $\mathrm{Res}(\mathbb{F}_{q^2}/\mathbb{F}_q, E)$ of E to $\mathbb{F}_q$. By our assumptions on a, we see that the characteristic polynomial of Frobenius $x^4 + ax^2 + q$ of A is irreducible. Hence A is simple over $\mathbb{F}_q$, but it is isogenous to $E \times E^{(q)}$ over $\mathbb{F}_{q^2}$, where $E^{(q)}$ is the $\mathbb{F}_q$-conjugate of E.

Corollary 1.18. *Every non-zero abelian variety A over k is isogenous to a product of simple abelian varieties over k. More precisely, there exist k-simple abelian varieties $B_1, \ldots, B_r$, pairwise non-isogenous, and positive integers m_i, such that*

$$A \sim_k B_1^{m_1} \times \ldots \times B_r^{m_r}.$$

This decomposition is unique up to permutation of the indices.

2. Abelian varieties in positive characteristic

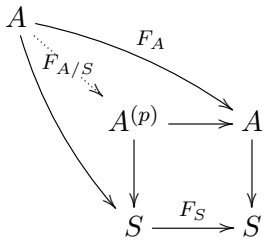
Assume from now on that k is a field of positive characteristic p (eg. $k = \mathbb{F}_{p^r}$, $k\bar{\mathbb{F}_p}$ or $\mathbb{F}_p(t)$)..

Exercise 2.1.
- Show that $\sigma : k \to k$, $x \mapsto x^p$ is a field homomorphism.
- What are the fixed elements of σ?
- What are the fixed elements of σ^r?

The morphism described in the exercise induces a map on geometric objects defined over k.

More precisely, if S is a scheme (eg. an abelian variety) over $\mathbb{F}_p$ we define the *absolute Frobenius* of S to be the morphism $F_S : S \to S$ induced by the ring homomorphism $\mathcal{O}_S \to$

$\mathcal{O}_S : x \to x^p$. Let A be a scheme over S. Define $A^{(p)}$ to be the fibered product $A \times_S S$ induced by the absolute Frobenius F_S. We define the *relative Frobenius* $F_{A/S}$ of A by



where F_A is the relative Frobenius induced by the $\mathbb{F}_p$-scheme structure of A and the vertical arrows are the projection $A^{(p)} \to S$ and the S-scheme structure map of A, respectively.

Example 2.2. Let A be the variety over $\mathbb{F}_q$ defined by a polynomial $\sum_I a_I X^I$, where I is a multi-index. Then $A^{(p)}$ is defined by $\sum_I a_I^p X^I$ and the relative Frobenius $F_{A/S}$ is the map $X_i \mapsto X_i^p$.

If A is an abelian variety over a finite field $\mathbb{F}_{p^n}$ then the relative Frobenius sends zero to zero and so it is a homomorphism of group schemes. Moreover, we can identify $A^{(p^n)} \simeq A$ and we can define the *Frobenius* of A over $\mathbb{F}_{p^n}$ as

$$\pi_A = \left(A \xrightarrow{F_{A/S}} A^{(p)} \xrightarrow{F_{A^{(p)}/S}} A^{(p^2)} \xrightarrow{F_{A^{(p^2)}/S}} \dots \to A^{(p^{n-1})} \xrightarrow{F_{A^{(p^{n-1})}/S}} A^{(p^n)} \simeq A. \right).$$

Proposition 2.3. *Let A be an abelian variety over k of dimension g, where k is field of characteristic $p > 0$. Then the relative Frobenius $F_{A/k}$ is an isogeny of degree p^g.*

3. The Tate module of an abelian variety

Before giving the definition of the Tate module, we introduce the ℓ-adic numbers, where ℓ is a prime number.

Exercise 3.1. Consider the sequence of ring homomorphisms

$$\frac{\mathbb{Z}}{\ell\mathbb{Z}} \leftarrow \frac{\mathbb{Z}}{\ell^2\mathbb{Z}} \leftarrow \frac{\mathbb{Z}}{\ell^3\mathbb{Z}} \leftarrow \dots$$

given by reductions. Define the ℓ-adic integers $\mathbb{Z}_\ell$ as the inverse limit $\varprojlim \mathbb{Z}/\ell^m\mathbb{Z}$, that is,

$$\mathbb{Z}_\ell = \left\{ (x_1, x_2, \dots) \in \prod_{m \geq 1} \frac{\mathbb{Z}}{\ell^m\mathbb{Z}} \mid x_i = x_{i+1} \bmod \ell^i \right\}.$$

Show that $\mathbb{Z}_\ell$ is a commutative ring that contains $\mathbb{Z}$.

Now, let A be an abelian variety over a perfect field k and let ℓ be a prime distinct from the characteristic of k. Then the multiplication by ℓ^m is a group homomorphism whose kernel $A[\ell^m]$ is a finite group scheme of rank $(\ell^m)^{2g}$, where g is the dimension of A. This implies that $A[\ell^m]$ is étale and hence it is completely described by its $\overline{k}$-points and the action of the absolute Galois group $\mathcal{G} = \mathrm{Gal}(\overline{k}/k)$. The torsion groups $A[\ell^m]$ form an inverse system under the multiplication by $\ell : A[\ell^{m+1}] \to A[\ell^m]$.

Definition 3.2. The *ℓ-Tate module* of A by

$$T_\ell A = \varprojlim A[\ell^m](\overline{k}).$$

Exercise 3.3. Describe $T_\ell(A)$ as a subset of a direct product and show that $T_\ell(A)$ has a natural structure as a $\mathbb{Z}_\ell$-module.

Proposition 3.4. *The Tate module of A is a free $\mathbb{Z}_\ell$-module of rank $2\dim(A)$ and $\mathcal{G}$ acts on it by $\mathbb{Z}_\ell$-linear maps.*

Moreover, we have an isomorphism of $\mathcal{G}$-modules $A[\ell^m](\overline{k}) \simeq T_\ell A/\ell^m T_\ell A$.

Consider a homomorphism of abelian varieties $\varphi : A \to B$. For every $m \geq 1$, it sends $A[\ell^m]$ to $B[\ell^m]$. Hence φ induces a morphism $\varphi_\ell : T_\ell A \to T_\ell B$. In particular, this makes T_ℓ a functor from the category of abelian varieties over k to the category of $\mathbb{Z}_\ell[\mathcal{G}]$-modules.

Observe that $\mathrm{Hom}_{\mathbb{Z}_\ell[\mathcal{G}]}(T_\ell A, T_\ell B)$ has finite rank.

Theorem 3.5 (Weil)**.** *Let A and B be two abelian varieties over a perfect field k and let ℓ be prime number distinct from the characteristic of k. The natural morphism*

$$\varphi : \mathrm{Hom}(A, B) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to \mathrm{Hom}_{\mathbb{Z}_\ell[\mathcal{G}]}(T_\ell A, T_\ell B)$$

is injective. In particular, $\mathrm{Hom}(A, B)$ *is a free $\mathbb{Z}$-module of finite rank.*

Let A be an abelian variety over a finite field $\mathbb{F}_q$. The Frobenius π_A of A induces an endomorphism $T_\ell(\pi_A)$ of $T_\ell A$. After choosing a basis of $T_\ell A$, that is, fixing a $\mathbb{Z}_\ell$-linear isomorphism

$$T_\ell(A) \simeq \mathbb{Z}_\ell^{2g},$$

where $g = \dim(A)$, one can represent $T_\ell(\pi_A)$ with a $2g \times 2g$-matrix with coefficients in $\mathbb{Z}_\ell$. Let $h_A(x)$ be the characteristic polynomial of this matrix.

Lemma 3.6. *The polynomial $h_A(x)$ has integer coefficients and it is independent of the choice of $\ell \neq p$.*

The polynomial h_A will be called the *characteristic polynomial* of Frobenius π_A, or simply the characteristic polynomial of A.

4. Isogeny classification: Honda-Tate theorems

This section is dedicated at showing how the isogeny class of an abelian variety A defined over a finite field $\mathbb{F}_q$ is completely determined by its characteristic polynomial, and how they can be used to enumerate the isogeny classes (for a fixed dimension g).

Definition 4.1. Let $q = p^n$ be a prime power. A *q-Weil number* π is an algebraic integer such that for every embedding $\psi : \mathbb{Q}(\pi) \to \mathbb{C}$ we have $|\psi(\pi)| = \sqrt{q}$. We say that two q-Weil numbers π and π' are conjugate if there exists a field isomorphism $\mathbb{Q}(\pi) \simeq \mathbb{Q}(\pi')$ (sending π to π'). Observe that this is equivalent to saying that the minimal polynomials over $\mathbb{Q}$ of π and π' are the same.

Theorem 4.2 (Weil)**.** *If A is a simple abelian variety over $\mathbb{F}_q$ then $h_A(x) = (m(x))^e$ for some $\mathbb{Q}$-irreducible polynomial $m(x) \in \mathbb{Z}[x]$ and some strictly positive integer e. Moreover, the Frobenius endomorphism π_A of $A/\mathbb{F}_q$ can be identified with a conjugacy class of q-Weil numbers.*

Theorem 4.3 (Tate isogeny Theorem)**.** *Let A and B be two abelian varieties over the finite field $\mathbb{F}_q$, where q is a prime power, with characteristic polynomials h_A and h_B, respectively. Then B is $\mathbb{F}_q$-isogenous to a subvariety of A if and only if h_B divides h_A. Moreover, the following are equivalent:*

- *A is $\mathbb{F}_q$-isogenous to B*

- $h_A = h_B$
- *A and B have the same number of points over $\mathbb{F}_{q^m}$ for every $m > 0$.*

Proof. See [Tat66, Theorem 3]. □

Consider the map Φ that sends a simple abelian variety A defined over $\mathbb{F}_q$ to its Frobenius π_A, considered as an algebraic integer. Observe that the characteristic polynomial h_A of π_A is a power of an irreducible polynomial, which will be the minimal polynomial of π_A over $\mathbb{Q}$. In view of Theorem 4.3, Φ induces an injective map between the isogeny classes of simple abelian varieties over $\mathbb{F}_q$ and the conjugacy classes of q-Weil numbers. Honda in [Hon68] proved that this is also surjective.

Theorem 4.4 (Honda-Tate)**.** *The map that sends a simple abelian variety A defined over $\mathbb{F}_q$ to the algebraic integer π_A defined by its Frobenius endomorphism induces a bijection between the isogeny classes of simple abelian varieties over $\mathbb{F}_q$ and conjugacy classes of q-Weil numbers.*

Proof. See [Tat66] and [Hon68]. □

Corollary 4.5. *Let A be an abelian variety over $\mathbb{F}_q$. Let $m_1, \dots, m_r$ be positive integers and let $B_1, \dots B_r$ be simple pairwise non-$\mathbb{F}_q$-isogenous abelian varieties over $\mathbb{F}_q$ such that*

$$A \sim_{\mathbb{F}_q} B_1^{m_1} \times \dots \times B_r^{m_r}.$$

Then the $\mathbb{F}_q$-isogeny class of A is uniquely determined by the pairs

$$(\pi_{B_1}, m_1), \dots, (\pi_{B_r}, m_r).$$

The set $\{\pi_{B_1}, \dots, \pi_{B_r}\}$ is called the *Weil support* of A.

Exercise 4.6. Prove Corollary 4.5 using the previous results we have seen.

5. q-Weil polynomials

Let $\mathbb{F}_q$ be a finite field of positive characteristic p with $q = p^n$ elements.

Definition 5.1. A q-Weil polynomial is a monic polynomial in $\mathbb{Z}[x]$ of even positive degree $2g$ whose set of complex roots has the form $\{w_1, \bar{w}_1, \dots, w_g, \bar{w}_g\}$ and each w_i has absolute value $\sqrt{q}$, that is, is a q-Weil number. We denote the set of q-Weil polynomials of degree $2g$ by $\mathcal{W}_q(g)$.

Proposition 5.2. *Let A be an abelian variety over $\mathbb{F}_q$ with characteristic polynomial $h_A(x)$. Then $h_A(x)$ is a q-Weil polynomial.*

Proof. It follows from the results in Section 4. □

It is natural to wonder if the converse of Proposition 5.2 is true: is every polynomial in $\mathcal{W}_q(g)$ the characteristic polynomial of some abelian variety defined over $\mathbb{F}_q$ of dimension g? The answer is: no. But the subset of $\mathcal{W}_q(g)$ consisting of characteristic polynomials can be completely understood using Corollary 4.5 and the following remark.

Remark 5.3. By Theorem 4.2, the characteristic polynomial of a simple abelian variety B over $\mathbb{F}_q$ is of the form

$$h_B(x) = m(x)^e$$

for some $\mathbb{Q}$-irreducible polynomial $m(x) \in \mathbb{Z}[x]$ whose roots are q-Weil numbers and some strictly positive integer e. The exponent e is the least common denominator of the rational numbers

$$\left\{ \frac{v_p(g_1(0))}{d}, \dots, \frac{v_p(g_s(0))}{d} \right\}, \tag{1}$$

where v_p is the valuation of $\mathbb{Q}_p$, $g_1(x), \ldots, g_s(x)$ are the irreducible factors of $m(x)$ over $\mathbb{Q}_p[x]$ and we add $1/2$ to the set (1) if $m(x)$ has a root in $\mathbb{R}$.

Example 5.4. The isogeny class over $\mathbb{F}_4$ with LMFDB-label 4.4.ai_bk_aei_ka has 4-Weil polynomial $h(x) = m(x)^2$, where $m(x)$ is the irreducible polynomial

$$m(x) = x^4 - 4x^3 + 10x^2 - 16x + 16.$$

One can verify that $m(x)$ is a 4-Weil polynomial, but it is not the characteristic polynomial of an abelian variety over $\mathbb{F}_4$.

The following lemma contains easy but important observations about q-Weil polynomials. These will be (often implicitly) used throughout the rest of the text.

Lemma 5.5. *Let $h(x)$ be a q-Weil polynomial. Then the following statements hold:*

(1) all real roots of $h(x)$, if any, occur with even multiplicities;
(2) $h(x) = (x^{2g}/q^g)h(q/x)$;
(3) there are integers $a_1, \ldots, a_g$ such that

$$h(x) = x^{2g} + a_1 x^{2g-1} + \cdots + a_{g-1}x^{g+1} + a_g x^g + a_{g-1}qx^{g-1} + \cdots + a_1 q^{g-1}x + q^g$$

Proof. Statement (1) follows immediately from the definition. Let w be a complex root of $h(x)$. We have $\bar{w} = q/w$. Then $h(x)$ and $(x^{2g}/q^g)h(q/x)$ are both monic polynomials with the same set of roots. Hence they are equal as in statement (2). Finally, statement (3) follows from (2), by comparing the coefficients. □

Exercise 5.6. Is this a characterization? That is, if $h(x)$ is a polynomial in $\mathbb{Z}[x]$ satisfying (1), (2) and (3), is then $h(x)$ a q-Weil polynomial ?

Example 5.7. Together with our definition of q-Weil number, which is used for example in [Hal10] and [HS12], there is (at least) another definition in the literature in which a q-Weil polynomial is a monic integer polynomial whose complex roots have absolute value $\sqrt{q}$. To avoid confusion, we will call polynomials satisfying this second more general convention, which is used for example in [DKRV21], generalized q-Weil polynomials. We will not use this more general notion outside of this example.

A generalized q-Weil polynomial can have odd degree. For example, if $q = p^n$ with n odd then the minimal polynomial $m_1(x) = x^2 - q$ of $\sqrt{q}$ over $\mathbb{Q}$ is a generalized q-Weil polynomial but not a q-Weil polynomial. Also, if n is even then $m_2(x) = x - \sqrt{q}$ and $m_3(x) = (x - \sqrt{q})(x + \sqrt{q})$ are generalized q-Weil polynomials but not q-Weil polynomial.

Nevertheless, under the same assumptions on n as above, $m_1(x)^2$, $m_2(x)^2$ and $m_3(x)^2$ are q-Weil polynomials. In fact, they are characteristic polynomials of abelian varieties over $\mathbb{F}_q$ of dimensions 2, 1 and 2, respectively.

In the following two well-known propositions, we compute the sets $\mathcal{W}_q(1)$ and $\mathcal{W}_q(2)$.

Proposition 5.8 ($g = 1$)**.** *Consider the polynomial $h(x) = x^2 + ax + q$ in $\mathbb{Z}[x]$. Then $h(x) \in \mathcal{W}_q(1)$ if and only if $|a| \leq 2\sqrt{q}$.*

Proof. The result follows immediately from the quadratic formula. □

Proposition 5.9 ($g = 2$)**.** *Let a and b be integers. Consider the polynomial $h(x) = x^4 + ax^3 + bx^2 + aqx + q^2$ in $\mathbb{Z}[x]$.*

If $h(x)$ is irreducible over $\mathbb{Q}$ then $h(x)$ is in $\mathcal{W}_q(2)$ if and only if the following conditions holds:

- $|a| < 4\sqrt{q}$,

- $2\,|a|\,\sqrt{q} - 2q < b < a^2/4 + 2q$, *and*
- $a^2 - 4b + 8q$ *is not a square in* $\mathbb{Z}$.

If $h(x)$ *is reducible over* $\mathbb{Q}$ *then* $h(x) \in \mathcal{W}_q(2)$ *if and only if*

(1) either $h(x) = h_1(x)h_2(x)$ *with* $h_1(x), h_2(x) \in \mathcal{W}_q(1)$,

(2) or q *is not a square and* $h(x) = (x^2 - q)^2$.

Proof. The case when $h(x)$ is irreducible is [R$\ddot{\text{9}}$0, Lemma 3.1]. So we assume for the rest of the proof that $h(x)$ is reducible over $\mathbb{Q}$. It is clear if (1) or (2) hold then $h(x)$ is in $\mathcal{W}_q(2)$. Also, if q is a square, then $(x - \sqrt{q})^2$ and $(x - \sqrt{q})^2$ are in $\mathcal{W}_q(1)$. So (1) and (2) are mutually exclusive. We are left to show that if $h(x) \in \mathcal{W}_q(2)$ is reducible over $\mathbb{Q}$ then (1) or (2) hold.

Assume first that $h(x)$ has a linear divisor over $\mathbb{Q}$, say $(x - \alpha)$. Then $\alpha = \pm\sqrt{q}$ and q is a square. By Lemma 5.5.(1), we have that $h(x) = (x - \alpha)^2 h_2(x)$ for some $h_2(x) \in \mathbb{Z}[x]$. By looking at the roots of $h(x)$, we see that $h_2(x) \in \mathcal{W}_q(1)$. So, (1) holds.

Assume for the rest of the proof that $h(x)$ factors as the product of 2 irreducible quadratic polynomials in $\mathbb{Q}[x]$. If $\sqrt{q}$ or $-\sqrt{q}$ is a root, it must have a quadratic minimal polynomial. Hence q is not a square and $(x^2 - q)$ divides $h(x)$. By Lemma 5.5.(1), we $(x^2 - q)^2$ divides $h(x)$ and (2) holds. Finally, assume that $h(x) = h_1(x)h_2(x)$ over $\mathbb{Q}$, with $h_1(x)$ and $h_2(x)$ irreducible over $\mathbb{Q}$ and with no real roots. Then we are in case (1). □

The next well-known proposition allows us to describe $\mathcal{W}_q(g)$, which consists of integer polynomials of degree $2g$, in terms of there roots of real polynomials of degree g.

Proposition 5.10. *Let* $h(x)$ *be a polynomial in* $\mathbb{Z}[x]$ *of the form*

$$h(x) = x^{2g} + a_1 x^{2g-1} + \cdots + a_{g-1}x^{g+1} + a_g x^g + a_{g-1}q x^{g-1} + \cdots + a_1 q^{g-1}x + q^g.$$

Then $h(x)$ *is in* $\mathcal{W}_q(g)$ *if and only if there exists* $\omega_1, \ldots, \omega_g \in \mathbb{C}$ *such that*

$$h(x) = \prod_{i=1}^{g}(x^2 + \omega_i x + q) \tag{2}$$

and the complex roots of the polynomials

$$h^+(x) = \prod_{i=1}^{g}(x - (2\sqrt{q} - \omega_i)),$$

$$h^-(x) = \prod_{i=1}^{g}(x - (2\sqrt{q} + \omega_i)),$$

are all in $\mathbb{R}_{\geq 0}$. *Moreover,* $h(x)$ *has no real roots if and only if the roots of* $h^+(x)$ *and* $h^-(x)$ *are all positive.*

Proof. Assume that $h(x)$ is a q-Weil polynomial with complex roots $w_1, \bar{w}_1, \ldots, w_g, \bar{w}_g$. For $i = 1, \ldots, g$, set $\omega_i = -w_i - \bar{w}_i$. Then $h(x)$ can be written as in Equation (2) and the complex roots of $h^+(x)$ and $h^-(x)$ are in $\mathbb{R}_{\geq 0}$. If $h(x)$ has a real root, say $w_i = \pm\sqrt{q}$, then $\omega_i = \mp 2\sqrt{q}$. Hence $h^+(0) = 0$ or $h^-(0) = 0$. This proves one direction. Now, we prove the converse statement. Since the complex roots of $h^+(x)$ and $h^-(x)$ are in $\mathbb{R}_{\geq 0}$, each ω_i is a real number satisfying $|\omega_i| \leq 2\sqrt{q}$. Hence, $x^2 + \omega_i x + q$ is a real polynomial with roots over the complex numbers of the form α_i and $\bar{\alpha}_i$. Then $\alpha_i\bar{\alpha}_i = q$, that is the absolute value of α_i is $\sqrt{q}$. It follows by Equation (2) that each α_i is an algebraic integer. Hence, $h(x)$ is a q-Weil polynomial. Assume in addition that $h^+(0) = 0$. Then there exists an index i such that $\omega_i = 2\sqrt{q}$. Then $x^2 + \omega_i x + q$, and hence also $h(x)$, has a real root. In a similar fashion, we see that if $h^-(0) = 0$ then $h(x)$ has a real root, concluding the proof. □

6. Computing and describing q-Weil polynomials of a fixed degree

In this section we give a brief overview of the known results about describing $\mathcal{W}_q(g)$ for fixed g and q.

- An algorithm to compute $\mathcal{W}_q(g)$ is described in [Ked08]. An implementation is included in SageMath. This algorithm has been used to enumerate and study isogeny classes in [DKRV21].
- The sets $\mathcal{W}_q(1)$ and $\mathcal{W}_q(2)$ are well known. They complete description is given in Propositions 5.8 and 5.9 above.
- The sets $\mathcal{W}_q(3)$, $\mathcal{W}_q(4)$ and $\mathcal{W}_q(5)$ are described in [Hal10], [HS12] and [Soh13], respectively. They all contain mistakes of various severity. In [Bra12] there is an attempt to fix the result of [HS12]. But it contains a typo as well.
- Jun Jie Lin's master thesis at Utrecht University fixed the issues `https://studenttheses.uu.nl/handle/20.500.12932/44249`. The author of this note, who was the supervisor of Lin, is slowly turning the thesis into an article, which should hopefully see the light soon.
- The results cited above use Proposition 5.10 to reduce the problem of computing $\mathcal{W}_q(g)$ for $g = 3, 4, 5$ to the study of the real roots of a real polynomial of degree ≤ 4. A key ingredient is that for such a polynomial, we have explicit formulas for the roots in terms of radicals. In particular, this method does not carry over to $g \geq 6$.

Exercise 6.1. Provide an independent implementation of Jun Jie Lin's result in SageMath. Check the output against the built-in algorithm. Do the output match?

Exercise 6.2. Can one use Sturm's theorem to determine $\mathcal{W}_q(g)$? The statement of Sturm's theorem can be found in several texts. A version valid also for polynomials with multiple roots is in [Tho41].

Further reading material about abelian varieties

- Milne - online notes on Abelian Varieties,
  available at `https://jmilne.org/math/CourseNotes/AV.pdf`
- Chapter 2 of [Wat69], available at `http://www.numdam.org/article/ASENS_1969_4_2_4_521_0.pdf`
- (draft of the) book on abelian varieties by Moonen, Edixhoven, van der Geer
  see `https://www.math.ru.nl/~bmoonen/research.html#bookabvar`
  and `http://van-der-geer.nl/~gerard/AV.pdf`

References

[Bra12] Jeremy Bradford, *Commutative endomorphism rings of simple abelian varieties over finite fields*, ProQuest LLC, Ann Arbor, MI, 2012, Thesis (Ph.D.)–University of Maryland, College Park. MR 3153176

[CF96] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2, London Mathematical Society Lecture Note Series, vol. 230, Cambridge University Press, Cambridge, 1996. MR 1406090

[DKRV21] Taylor Dupuy, Kiran Kedlaya, David Roe, and Christelle Vincent, *Isogeny classes of abelian varieties over finite fields in the LMFDB*, Arithmetic geometry, number theory, and computation, Simons Symp., Springer, Cham, [2021] ©2021, pp. 375–448. MR 4427971

[Hal10] Safia Haloui, *The characteristic polynomials of abelian varieties of dimensions 3 over finite fields*, Journal of 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), 83–95. MR 229642

[HS12] Safia Haloui and Vijaykumar Singh, *The characteristic polynomials of abelian varieties of dimension 4 over finite fields*, Arithmetic, geometry, cryptography and coding theory, Contemp. Math., vol. 574, Amer. Math. Soc., Providence, RI, 2012, pp. 59–68. MR 2961400

[Ked08] Kiran S. Kedlaya, *Search techniques for root-unitary polynomials*, Computational arithmetic geometry, Contemp. Math., vol. 463, Amer. Math. Soc., Providence, RI, 2008, pp. 71–81. MR 2459990

[RÖ90] Hans-Georg Rück, *Abelian surfaces and Jacobian varieties over finite fields*, Compositio Mathematica **76** (1990), no. 3, 351–366. MR 1080007

[Soh13] Gyoyong Sohn, *The bounds of the coefficients of the characteristic polynomials for abelian varieties of dimension 5 over finite fields*, Advanced Studies in Contemporary Mathematics (Kyungshang). Memoirs of the Jangjeon Mathematical Society **23** (2013), no. 3, 415–421. MR 3100101

[Tat66] John Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144. MR 206004

[Tho41] Joseph Miller Thomas, *Sturm's theorem for multiple roots*, Natl. Math. Mag. **15** (1941), 391–394. MR 5945

[Wat69] William C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560. MR 265369

Stefano Marseglia, Laboratoire Jean Alexandre Dieudonné, Université Côte Azur, 06108 Nice Cedex 2, France

Email address: stefano.marseglia@univ-cotedazur.fr

URL: https://stmar89.github.io