Utrecht University

Isogeny Classes of Abelian Varieties over Finite Fields

Master thesis Mathematical Sciences

Author: Jun Jie Lin

Supervisor: Dr. S. (Stefano) Marseglia
Second reader: Prof. dr. G.L.M. (Gunther) Cornelissen

Utrecht University, The Netherlands,
Faculty of Science
June 29, 2023

Abstract

The aim of this thesis is to determine the isogeny classification of abelian varieties over a finite field $\mathbb{F}_q$ with $q = p^n$, particularly for dimensions 3, 4 and 5. For a given dimension g, each isogeny class has a distinguished characteristic polynomial, which is a q-Weil polynomial of degree $2g$ satisfying certain conditions regarding its factorisation over the p-adic integers $\mathbb{Z}_p$. A q-Weil polynomial is a polynomial with integer coefficients such that all of its roots have absolute value $q^{1/2}$. Enumerating all isogeny classes is a two-steps procedure. The first step is determining all q-Weil polynomials of degree $2g$ and the second step is determining the conditions for which a given q-Weil polynomial is the characteristic polynomial of some abelian variety over $\mathbb{F}_q$. This process has been carried out for a fixed dimension up to $g = 5$ in recent articles by various authors. However, a few of these results contained some mistakes, particularly in the first step for $g = 3$, 4 and 5. This thesis contains a correction of these specific results and also explains the second step for these dimensions.

Acknowledgements

First of all, words cannot express my gratitude to my supervisor, Stefano Marseglia, who was also the supervisor of my bachelor thesis. Thanks to that, we were able to agree very easily on this topic. At the start of the project, Stefano provided me with a general overview of the necessary background knowledge on abelian varieties and some ideas for the project. This is invaluable to me as it helped me greatly with understanding the basic concepts and deciding on the goals of my thesis. Additionally, Stefano always responded timely and provided many insightful suggestions, which I also appreciate very much. Furthermore, I am grateful for his patience with me. During the process, I encountered multiple problems with the computations and substitutions that always took me quite a long time to solve despite the fact that in the end, the problems were fairly easy to understand. I also arrived sometimes too late to our meetings. However, Stefano never seemed to be upset by either of these two things.
I also wish to thank my second reader, Gunther Cornelissen, for helpful suggestions and words of encouragement at the end of the project. Moreover, I would like to sincerely thank both my tutor, Valentijn Karemaker, and my study adivsor, Yo-Yi Pat, to whom I could talk to when I went through a difficult period regarding my home environment. Another person I would like to acknowledge is Carel Faber, who sent me the lecture notes for the course *Algebraic Geometry 2*, which I did not take. The notes provided me with sufficient background knowledge that I was lacking during the initial stage of the project.
Lastly, special thanks to my colleagues Puck te Rietmole and Jaap Nieuwenhuizen, who were in my thesis study group despite their field of study being far more towards the applied side of mathematics. Their support and weekly meetings helped me stay motivated during the project.

Contents

Introduction **4**

1 Abelian varieties **7**

2 Isogenies **12**

3 Tate-ℓ-module **15**

4 Frobenius endomorphism **18**

5 Isogeny classification **21**

6 Classification of q-Weil polynomials **23**

6.1 Characteristic polynomial 23

6.2 Newton polygon 24

7 Robinson's method **27**

7.1 Explanation of the method 27

7.2 Application to low degrees 30

8 Dimension 3 **38**

8.1 Weil polynomials of degree 6 38

8.1.1 Real root 38

8.1.2 No real roots 39

8.2 Irreducibility 41

8.3 Newton polygons 43

9 Dimension 4 **46**

9.1 Weil polynomials of degree 8 46

9.1.1 Real roots 46

9.1.2 No real roots 46

9.2 Newton polygons 50

9.2.1 Square polynomial 50

9.2.2 Irreducible polynomial 51

10 Dimension 5 **54**

10.1 Weil polynomials of degree 10 54

10.1.1 Real roots 54

10.1.2 No real roots 54

10.2 Newton polygons 59

Bibliography **63**

Introduction

Abelian varieties over a field k are complete connected algebraic varieties whose k-rational points form a group. Maps between two abelian varieties X and Y over k are called k-homomorphisms, which are k-morphisms of algebraic varieties that respect the group structures of X and Y. If X and Y have the same dimension over k, a surjective homomorphism from X to Y is called a k-isogeny. We will be mostly working with a fixed field k, so we often leave out the k except when working over a different field. One can show that the existence of an isogeny between two abelian varieties over k is an equivalence relation. Furthermore, by John Tate [23, Theorem 1], the abelian varieties X and Y over a finite field $k = \mathbb{F}_q = \mathbb{F}_{p^n}$ are k-isogenous if and only if their respective characteristic polynomials $P_{\pi_X}(x)$ and $P_{\pi_Y}(x)$ are the same, which are defined in the following way. The characteristic polynomial of an abelian variety X over a finite field k is the characteristic polynomial of the endomorphism π_X acting on the Tate-ℓ-module of X, with ℓ any prime different from p, induced by the Frobenius endomorphism π on X. In particular, $P_{\pi_X}(x)$ is a polynomial with integer coefficients. Hence, in order to determine all the isogeny classes for given k and dimension g, one can compute all the possible characteristic polynomials.

A simple abelian variety is an abelian variety which has no proper abelian subvariety. Each abelian variety X can be decomposed into a product of powers of simple abelian varieties $X_1^{m_1} \times \ldots \times X_t^{m_t}$, with $X_1, \ldots, X_t$ pairwise not isogenous. This decomposition is unique up to isogeny and permutation. Accordingly, the characteristic polynomial $P_{\pi_X}(x)$ of X factors into the product $P_{\pi_{X_1}}(x)^{m_1} \cdot \ldots \cdot P_{\pi_{X_t}}(x)^{m_t}$ of characteristic polynomials of the X_i's. Hence, to determine the isogeny classification of abelian varieties of a given dimension it is sufficient to restrict to simple abelian varieties, as the results from lower dimensions can be used for non-simple abelian varieties. By the Tate-Honda Theorem [10] [23], there is a bijection between isogeny classes of simple abelian varieties over $\mathbb{F}_q$ and conjugacy classes of q-Weil numbers, which are defined as follows. A q-Weil number ϖ is an algebraic number such that $|\sigma(\varpi)| = q^{1/2}$ for every embedding $\sigma : \mathbb{Q}[\varpi] \to \mathbb{C}$ and two q-Weil numbers are conjugate if and only if they have the same minimal polynomial. A q-Weil polynomial is a polynomial with integer coefficients that only has q-Weil numbers as roots. In this thesis, $y^{1/m}$ and $\sqrt[m]{y}$ will denote the real root for any real number y. If m is even, that is if there are two real roots, then $y^{1/m}$ and $\sqrt[m]{y}$ denotes the positive real root.

The characteristic polynomial of an abelian variety over $\mathbb{F}_q$ of dimension g is a q-Weil polynomial of degree $2g$. Hence, the first step to determine the isogeny classification of abelian varieties over finite fields is to determine all possible q-Weil polynomials of degree $2g$. However, the converse is not necessarily true. Hence, the second step is to determine the conditions for which a given q-Weil polynomial of degree $2g$ corresponds to an abelian variety over $\mathbb{F}_q$ of dimension g.

If X is a simple abelian variety over $\mathbb{F}_q$, then its characteristic polynomial is equal to $(P(x))^d$, where $P(x)$ is some q-Weil polynomial, irreducible over $\mathbb{Q}$, and d is some positive integer. In particular, d divides $2g$ and $\deg(P(x)) = \frac{2g}{d}$. Therefore, the second step to determine the isogeny classification is equivalent to finding all possible irreducible q-Weil polynomials $P(x)$ of degree $\frac{2g}{d}$ for each divisor d of $2g$ such that $(P(x))^d$ is the characteristic polynomial of some simple abelian variety of dimension g over $\mathbb{F}_q$. These problems have been studied in-depth for up to dimension $g = 5$. Daiki Hayashida in [9] has made an overview of the recent results, see Table 1.

Dimension Conditions for	$g = 1$	$g = 2$	$g = 3$	$g = 4$	$g = 5$
a polynomial being a q-Weil polynomial of degree $2g$	clear	[17], [14]	[6]	[7]	[22]
a q-Weil polynomial of degree $2g$ being the characteristic polynomial of a simple abelian variety of dimension g over $\mathbb{F}_q$	[25]	[17], [14]	[6], [28]	[7], [28]	[8]

Table 1: Recent results [9, Table 1]

An abelian variety of dimension 1 is called an elliptic curve. One can easily verify that a polynomial

$x^2 + ax + b$ with integer coefficients is a q-Weil polynomial if and only if $b = q$ and $|a| \leq 2\sqrt{q}$, as b is the product of the roots and a is equal to minus the sum of the roots. William C. Waterhouse [25, Chapter 4] determined the correspondence between isogeny classes of elliptic curves over $\mathbb{F}_q$ and q-Weil numbers. Both the bounds of the coefficients of q-Weil polynomials of degree 4 as well as the conditions of such a q-Weil polynomial being the characteristic polynomial of an abelian variety over $\mathbb{F}_q$ of dimension 2, i.e. an abelian surface, has been found by Hans-Georg Rück [17, Lemma 3.1 and Theorem 1.1] as well as Daniel Maisner and Enric Nart [14, Lemma 2.1 and Theorem 2.9]. The bounds of the coefficients of q-Weil polynomials of degree 6 and determination of irreducible characteristic polynomials of simple abelian varieties of dimension 3 over $\mathbb{F}_q$ have been computed by Safia Haloui [6, Theorems 1.1 and 1.4]. The case where $d = 2$ for dimension 3 has been determined by Chao Ping Xing [28, Proposition 2], who also provided the case where $d = 2$ for dimension 4 [28, Proposition 4]. The bounds of the coefficients of q-Weil polynomials of degree 8 were determined by Safia Haloui and Vijaykumar Singh [7, Theorem 1.1] and they found which irreducible q-Weil polynomials of degree 8 are characteristic polynomials of simple abelian varieties of dimension 4 over $\mathbb{F}_q$, see [7, Theorem 1.2]. Lastly, for dimension 5, Gyoyong Sohn computed the bounds for the coefficients of q-Weil polynomials of degree 10 [22, Theorem 2.1] and Daiki Hayashida determined the characteristic polynomials of simple abelian varieties of dimension 5 over $\mathbb{F}_q$ [8, Theorem 1.3].

This work covers the results regarding the isogeny classification of simple abelian varieties of dimensions $3, 4$ and 5 over finite fields $\mathbb{F}_q$ in Chapters 8, 9 and 10, respectively. We can limit ourselves to the simple isogeny classes, since results for non-simple isogeny classes can be found by combining results from lower dimensions. Recall that the factorisation of a characteristic polynomial into a product of powers of irreducible q-Weil polynomials corresponds to the decomposition of the abelian variety into a product of powers of simple abelian varieties. The reason we work with these dimensions specifically is due to an article by Dupuy, Kedlaya, Roe and Vincent, [3, Chapter 3.1]. While computing the q-Weil polynomials to populate the LMFDB [LMFDB], the authors have found some errors in previous results by Haloui [6], Haloui-Singh [7] and Sohn [22] regarding the bounds on the coefficients of q-Weil polynomials. Higher dimensions are not covered due to the inability of applying the used method to higher degree polynomials.
All of the results from Haloui, Haloui-Singh and Sohn had in common that they were computed using Robinson's method, described in Chapter 7. The main goal is to determine these errors and correct them. The corresponding result for $g = 3, 4, 5$ are respectively Theorems 8.2, 9.2 and 10.2. The main differences lie in the q-Weil polynomials with real roots which were omitted in the original articles by Haloui, Haloui-Singh and Sohn. Furthermore, for $g = 4$ and $g = 5$, there were mistakes in some of the bounds and the bound for the coefficient of x^4 specifically required more attention regarding the ordering of a cube root.
Results about determining when a given irreducible q-Weil polynomial corresponds to a simple abelian variety of dimension $3, 4$ and 5 over $\mathbb{F}_q$ will also be included to provide a full overview of the isogeny classifications for the respective dimension, see Theorems 8.6, 9.4 and 10.4. These results can be obtained from looking at the Newton polygons of the characteristic polynomials.

Chapters 1, 2, 3, 4 and 5 provide necessary background knowledge on abelian varieties over finite fields in order to be able to understand the correspondence between isogeny classes and q-Weil numbers. In Chapter 1, abelian varieties are defined together with homomorphisms, which are morphisms between abelian varieties that respect the group structures. Surjective homomorphisms with finite kernel are called isogenies, which are introduced in Chapter 2. In particular, it is shown that given two abelian varieties X and Y over a field k, there exists an isogeny from X to Y if and only if there exists an isogeny from Y to X. In Chapter 3, the Tate-ℓ-module $T_\ell X$ of an abelian variety X is constructed for $\ell \neq \mathrm{char}(k)$ from the ℓ^n-torsion points for $n \geq 1$, similar as to how the ℓ-adic integers $\mathbb{Z}_\ell$ are constructed from $\mathbb{Z}/\ell^n\mathbb{Z}$, that is the integers modulo ℓ^n. A relation between isogenies from X to Y and maps from $T_\ell X$ to $T_\ell Y$ is shown. This leads to the definition of the characteristic polynomial of an endomorphism of an abelian variety, which is explicitly explained for the Frobenius endomorphism in Chapter 4. The characteristic polynomial of the Frobenius endomorphism corresponding to an abelian variety X over a finite field is called the characteristic polynomial of X. In Chapter 5, a key theorem by Tate [24] is mentioned, which states that two abelian varieties are isogenous if and only if their characteristic polynomials are the same. Furthermore, the characteristic polynomials of abelian varieties are always q-Weil polynomials.

A method to determine whether a given q-Weil polynomial is the characteristic polynomial of a simple abelian variety over $\mathbb{F}_q$ is described in Chapter 6 using Newton polygons, which due to the discussion above is sufficient to give the complete isogeny classification. In Chapter 7, we explain an application of Robinson's method that was used by Haloui, Haloui-Singh and Sohn to determine q-Weil polynomials. The idea, described in Chapter 6, is that a q-Weil polynomial can be factored into a product of quadratic polynomials of the form $x^2 + \omega_i x + q$, where $\omega_i \in \mathbb{R}$ and $|\omega_i| \leq 2\sqrt{q}$. Furthermore, $|\omega_i| = 2\sqrt{q}$ implies that $x^2 + \omega_i x + q$ has two real roots. These can be handled separately, hence the emphasis lies on $|\omega_i| < 2\sqrt{q}$. One can construct the polynomials $\prod(x - (2\sqrt{q} + \omega_i))$ and $\prod(x - (2\sqrt{q} - \omega_i))$ and determine the conditions for which these polynomials have all roots real and positive, which can be found exactly using Robinson's method, see the second part of Chapter 7. These results can be substituted back in the original polynomial $\prod(x^2 + \omega_i x + q)$ to find the bounds on its coefficients. The original article explaining Robinson's method by Christopher Smyth [20] only mentioned the method for the case where all roots are distinct. An explanation will be given in 7 for why the method can still be used for our goals when there is a multiple root. Results from Chapters 6 and 7 are used to determine q-Weil polynomials of degree $6, 8$ and 10 and characteristic polynomials of simple abelian varieties over $\mathbb{F}_q$ of dimension 3, 4 and 5 in Chapter 8, 9 and 10 respectively.

Results are implemented in SageMath 9.3 [18], which has an in-built function `weil_polynomials` written by Kiran Kedlaya, see [11]. The built-in function uses a similar idea as our approach, namely looking at polynomials of the form $\prod(x + \omega_i)$, where the ω_i's are real numbers such that $\prod(x^2 + \omega_i x + q)$ is a q-Weil polynomial, i.e. it looks for polynomials with roots in the interval $[-2\sqrt{q}, 2\sqrt{q}]$. These are found by determining the derivatives which have roots in the interval. A tree exhaustion is applied to obtain all possible polynomials satisfying certain conditions, such as Rolle's theorem and Sturm's theorem. The q-Weil polynomials without real roots would have $\omega_i \in (-2\sqrt{q}, 2\sqrt{q})$, the open interval. The implementation of Theorems 8.6, 9.4 and especially 10.4 were in general a fair bit slower than the in-built function, partly due to my code being fairly unoptimised and due to Kedlaya's function using Cython for some of its calculations. However, one advantage our result has over the built-in function is that the obtained list with q-Weil polynomials are immediately separated into a part with real roots and a part without real roots.

The results from Theorems 8.6, 9.4 and 10.4 about which q-Weil polynomials are characteristic polynomials of simple abelian varieties for dimension 3, 4 and 5 respectively, were compared with the results in the LMFDB [LMFDB] for small q. The implementation of the bounds and the comparisons can be found in my repository [13]. The results for the values of q that were tested, omitting the q-Weil polynomials with real roots, matched completely with the in-built function and the LMFDB-data. However, precision errors may occur in my code when trying higher values of q.

1 Abelian varieties

This section will serve as an introduction to the basic definitions of abelian varieties and give some useful properties. This part will be largely based on the preliminary notes by Edixhoven, Van der Geer and Moonen, [4, Chapter 1]. Intuitively, an abelian variety over a field k is a complete algebraic variety over the field k such that its k-rational points form a group. Here, with the term (algebraic) variety, we mean a separated k-scheme of finite type that is geometrically integral. In fact, one can show that abelian varieties are projective varieties, see [15, Section I.6].

Formally, one defines abelian varieties as follows.

Definition 1.1. Let X be a variety over a field k. Let $j_1 : \mathrm{Spec}(k) \times X \to X$ and $j_2 : X \times \mathrm{Spec}(k) \to X$ be canonical isomorphisms, $\Delta_{X/k} : X \to X \times X$ be the diagonal morphism and $\pi : X \to \mathrm{Spec}(k)$ be the structure morphism. Let

$$\begin{aligned} m: &\quad X \times X &\longrightarrow X \\ i: &\quad X &\longrightarrow X \end{aligned}$$

be morphisms and $e \in X(k)$ a k-rational point. We call (X, m, i, e) a *group variety* if the following diagrams commute:

1. Associativity:

$$\begin{tikzcd} X \times X \times X \arrow[r, "\mathrm{id}_X \times m"] \arrow[d, "m \times \mathrm{id}_X"] & X \times X \arrow[d, "m"] \\ X \times X \arrow[r, "m"] & X \end{tikzcd} .$$

2. Identity element:

$$\begin{tikzcd} \mathrm{Spec}(k) \times X \arrow[r, "e \times \mathrm{id}_X"] \arrow[dr, "j_1"] & X \times X \arrow[d, "m"] \\ & X \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} X \times \mathrm{Spec}(k) \arrow[r, "\mathrm{id}_X \times e"] \arrow[dr, "j_2"] & X \times X \arrow[d, "m"] \\ & X \end{tikzcd} .$$

3. Two-sided inverse:

$$\begin{tikzcd} X \times X \arrow[rr, "\mathrm{id}_X \times i"] & & X \times X \arrow[d, "m"] \\ X \arrow[u, "\Delta"] \arrow[r, "\pi"] & \mathrm{Spec}(k) \arrow[r, "e"] & X \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} X \times X \arrow[rr, "i \times \mathrm{id}_X"] & & X \times X \arrow[d, "m"] \\ X \arrow[u, "\Delta"] \arrow[r, "\pi"] & \mathrm{Spec}(k) \arrow[r, "e"] & X \end{tikzcd} .$$

If the above holds, then we say that m defines the *group law*, i defines the *inverse* and e defines the *identity element.*

Remark 1.2. One can generalise Definition 1.1 to schemes to obtain the definition of *group schemes.* Some of the results below can also be generalised to group schemes. See [4, Chapter 3] for more details.

Definition 1.3. An *abelian variety* is a group variety that is also a complete variety.

We will often simply write X for the abelian variety (X, m_X, i_X, e_X). Note that $i^2 = \mathrm{id}_X$.

Example 1.4. Abelian varieties over a field k of dimension 1 are called *elliptic curves*, which are non-singular curves of genus 1 together with a rational k-point. See [19, Sections II and III] for more details. Using the theory of divisors and the Riemann-Roch theorem, one can deduce that every elliptic curve over k can be given by a cubic equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.1}$$

for some $a_i \in k$ such that the discriminant of the equation is invertible in k. This equation is called a *(general) Weierstrass equation.* If the characteristic of the field k is not equal to 2 or 3, then a change of coordinates makes the equation in (1.1) into the much simpler equation

$$y^2 = x^3 + Ax + B$$

with $A, B \in k$ with $4A^3 + 27B^2$ invertible. Such an equation is called a *short Weierstrass equation.*
The group law on such an elliptic curve has a nice geometric interpretation. Firstly, assume we are working with an elliptic curve defined by a short Weierstrass equation. The point $O = (0 : 1 : 0)$ at infinity, which lies on every vertical line, corresponds to the identity element. For any points P, Q on the curve, $m(P, Q)$ is the result of reflecting the unique third intersection point of the curve with the line through P and Q (counting with multiplicity) across the x-axis. In particular, the inverse map is given by the reflection across the x-axis. For a curve given by a general Weierstrass equation, one still has that if P, Q, R lie on the curve and are collinear, then $m(P, m(Q, R)) = O$ and that $i(P)$ is the intersection point (other than O) of the vertical line through P with the curve. However, in this case the curve might not be symmetric, so that the general formulas are longer.

Explicitly in coordinates assuming the curve is given in generalised Weierstrass form, the maps m and i can be given using the following rational functions

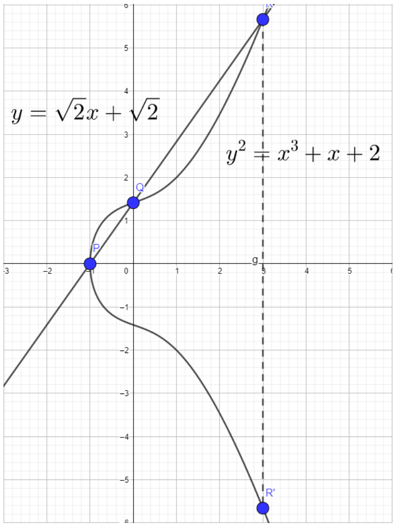


Figure 1: An elliptic curve in $\mathbb{R}$, $m(P, Q) = R'$

$$i(x, y) = (x, -y - a_1x - a_3)$$
$$m((x_1, y_1), (x_2, y_2)) = \begin{cases} O & \text{if } x_1 = x_2 \text{ and } y_1 = -y_2 - a_1x_2 - a_3, \\ (x_3, y_3) & \text{else,} \end{cases}$$

where

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$
$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3,$$

with

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } x_1 \neq x_2, \\ \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & \text{if } x_1 = x_2, \end{cases} \qquad \nu = \begin{cases} \frac{y_1x_2 - x_1y_2}{x_2 - x_1} & \text{if } x_1 \neq x_2, \\ \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} & \text{if } x_1 = x_2. \end{cases}$$

One can compute that $y = \lambda x + \nu$ defines the line through (x_1, y_1) and (x_2, y_2) or the tangent line of the curve at (x_1, y_1) if $x_1 = x_2$ and $y_1 = y_2$.

The next step is to define maps between abelian varieties X and Y. Maps between algebraic varieties that preserve the algebraic structure are morphisms of algebraic varieties. Naturally, we want morphisms in the category of abelian varieties to be morphisms of algebraic varieties that respect the group structures on the abelian varieties.

Definition 1.5. Let (X, m_X, i_X, e_X) and (Y, m_Y, i_Y, e_Y) be group varieties and $f : X \to Y$ a morphism of algebraic varieties. We say that f is a *homomorphism* if the following diagram commutes:

$$\begin{tikzcd}
X \times X \arrow[r, "m_X"] \arrow[d, "f \times f"] & X \arrow[d, "f"] \\
Y \times Y \arrow[r, "m_Y"] & Y
\end{tikzcd} .$$

Remark 1.6. If the above conditions holds, then $f(e_X) = e_Y$ and $f \circ i_X = i_Y \circ f$ follow from combining Definitions 1.1 and 1.5.

Any group can be thought of as acting transitively on itself via either left or right multiplication. The same can be stated for abelian varieties.

Definition 1.7. Let X be a group variety over a field k and let $x \in X(k)$ be a k-rational point. Let $t_x : X \to X$ and $t'_x : X \to X$ be maps such that the following diagrams commute:

$$\begin{tikzcd}
X \times \mathrm{Spec}(k) \arrow[r, "\mathrm{id}_X \times x"] & X \times X \arrow[d, "m"] \\
X \arrow[u, "j_2^{-1}"] \arrow[r, "t_x"] & X
\end{tikzcd} \quad \text{and} \quad \begin{tikzcd}
\mathrm{Spec}(k) \times X \arrow[r, "x \times \mathrm{id}_X"] & X \times X \arrow[d, "m"] \\
X \arrow[u, "j_1^{-1}"] \arrow[r, "t'_x"] & X
\end{tikzcd} .$$

We call t_x the *right translation* and t'_x the *left translation.*

These indeed define a group action, since if we take $x = e$, then the commutative diagrams simply become extensions of the ones we have given in Definition 1.1 for the identity element. Furthermore, extending the diagrams with themself gives that indeed

$$t_{m(x,y)} = t_y \circ t_x \quad \text{and} \quad t'_{m(x,y)} = t'_y \circ t'_x$$

for points $x, y \in X(k)$. One can also deduce that

$$t_{i(x)} = t_x^{-1} \quad \text{and} \quad t'_{i(x)} = (t'_x)^{-1}.$$

For a given point x, these can be simply stated as $t_x(y) = m(y, x)$ and $t'_x(y) = m(x, y)$. Note that t_x and t'_x are generally not homomorphisms, since if $x \neq e$, then

$$t_x(e) = m(e, x) = x \neq e,$$
$$t'_x(e) = m(x, e) = x \neq e.$$

Let X and Y be abelian varieties. We will relate any morphism of algebraic varieties from X to Y with a homomorphism from X to Y and a translation map, which then tells us something about the number of possible group structures on an algebraic variety. To do that, we first need the following lemma.

Lemma 1.8 (Rigidity)**.** *Let X, Y and Z be algebraic varieties over a field k. Suppose that X is complete. A morphism $f : X \times Y \to Z$ of algebraic varieties such that for some $y \in Y(k)$, the fibre $X \times \{y\}$ is mapped to a point $z \in Z(k)$ factors through the projection $pr_Y : X \times Y \to Y$.*

Proof. Some parts of this proof were paraphrased from [4, Lemma 1.12].

If k is not algebraically closed, we may apply a base change to the morphism to get a morphism $X \times Y \times_k \overline{k} \to Z \times_k \overline{k}$ and if this factors through the projection $Y \times k$, we can get a projection $X \times Y \to Y$. Hence, we may assume $k = \overline{k}$. Any algebraic variety X over $\overline{k}$ has a k-rational point, hence choose $x_0 \in X(k)$. Then define a morphism $g : Y \to Z$ by $g(y) = f(x_0, y)$. We will show that $f = g \circ \mathrm{pr}_Y$ on k-rational points, which is sufficient as $X \times Y$ is an algebraic variety, hence reduced.

For $z \in Z$, let $U \subseteq Z$ be an open affine neighbourhood of z. By the definition of completeness, pr_Y is a closed map. This means that the set V defined by $V = \mathrm{pr}_Y(f^{-1}(Z - U))$ is closed in Y. If $P \in V$, then by construction $f(X \times \{P\}) \subseteq U$. Any morphism from a complete irreducible variety to an affine variety is constant. Furthermore, the algebraic variety $X \times \{P\}$ is canonically isomorphic to X, hence complete. It follows that f is constant on $X \times \{P\}$, so $f = g \circ \mathrm{pr}_Y$ on $X \times (Y - V)$, which is a non-empty open subset of $X \times Y$. By irreducibility of $X \times Y$, it follows that $f = g \circ \mathrm{pr}_Y$ everywhere. □

Proposition 1.9. *Let X and Y be abelian varieties and let $f : X \to Y$ be a morphism of algebraic varieties. Then, there exists a homomorphism $h : X \to Y$, such that the morphism f is equal to $f = t_{f(e_X)} \circ h$, where $t_{f(e_X)}$ is the translation over $f(e_X)$ on Y.*

Proof. Let $y \in Y$ be the inverse of $f(e_X)$, that is $y = i_Y(f(e_X))$. Define $h : X \to Y$ by $h(x) = (t_y \circ f)(x)$, so that $h(e_X) = e_Y$ by construction. We want h to be a homomorphism, since then we have that

$$f = t_{i_Y(i_Y(f(e_X)))} \circ h = t_{f(e_X)} \circ h.$$

Then, the composite morphism $g : X \times X \to Y$ defined by

$$g = m_Y \circ ((h \circ m_X) \times (i_Y \circ m_Y \circ (h \times h)))$$

has the property that

$$\begin{aligned} g(\{e_X\} \times X) &= m_Y(h(X) \times i_Y(m_Y(e_Y \times h(X)))) \\ &= m_Y(h(X) \times i_Y(h(X))) \\ &= \{e_Y\}, \end{aligned}$$

by definition of the maps m_X, i_Y and m_Y. Hence, by Lemma 1.8, g factors through the projection $\mathrm{pr}_2 : X \times X \to X$ onto the second part and by symmetry also through the projection $\mathrm{pr}_1 : X \times X \to X$. Therefore, g is the constant map sending every element to e_Y. It follows that

$$h \circ m_X = i_Y \circ i_Y \circ m_Y \circ (h \times h) = m_Y \circ (h \times h).$$

This shows that h is indeed a homomorphism. □

Corollary 1.10. *Let (X, m, i, e) be an abelian variety over a field k*

1. *If (X, n, j, e) is an abelian variety, then $m = n$ and $i = j$. That is, the morphisms m and i making an algebraic variety X into a abelian variety with identity element e are necessarily unique.*
2. *Let $s : X \times X \to X \times X$ be defined by $(x, y) \mapsto (y, x)$. Then, the equality $m = m \circ s$ holds, i.e. the group structure is commutative.*

Proof. 1. Suppose (X, m, i, e) and (X, n, j, e) are abelian varieties. By Definition 1.1, for any $x \in X(k)$, we have

$$\begin{aligned} m(e, x) &= x = n(e, x), \\ m(x, e) &= x = n(x, e). \end{aligned}$$

It follows that m and n are the same on the fibers $X \times \{e\}$ and $\{e\} \times X$. Define the morphism $h : X \times X \to X$ by $h = m \circ (m, i \circ n)$. Since m and n agree on the fibers $X \times \{e\}$ and $\{e\} \times X$, it follows that h is constant on these fibers by definition of i, sending everything to e. Then, Lemma 1.8 tells us that h factors through the projection $X \times X \to X$. Similar as in the proof of Proposition 1.9, due to symmetry, it follows that h is constant with value e everywhere. Combining this with the same morphism but with m and n swapped and j instead of i then gives $m = n$ and $i = j$.

2. Since $i : X \to X$ is a morphism mapping e to itself, it follows that i is actually a homomorphism by Proposition 1.9. This implies that the group is abelian.

$\square$

2 Isogenies

We are now interested in a specific type of homomorphisms, namely isogenies. In this part, we will discuss some notions and properties of isogenies. We will always assume that the isogenies are defined over the base field k unless stated otherwise.

Definition 2.1. Let $f : X \to Y$ be a homomorphism of abelian varieties. The *kernel* of f is defined as the subscheme $\mathrm{Ker}(f) = f^{-1}(e_Y)$ of X.

The kernel $\mathrm{Ker}(f)$ is a closed subscheme of X that inherits the group structure of X. This leads into the definition of an isogeny.

Definition 2.2. We call a homomorphism $f : X \to Y$ of abelian varieties an *isogeny* if it is surjective, and $\mathrm{Ker}(f)$ is finite.

However, one can use other equivalent definitions.

Proposition 2.3. *Let $f : X \to Y$ be a homomorphism of abelian varieties. Then the following are equivalent:*

1. *f is an isogeny;*
2. *f is surjective and* $\dim(X) = \dim(Y)$*;*
3. *Ker(f) is finite and* $\dim(X) = \dim(Y)$*;*
4. *f is a finite, flat and surjective morphism.*

Proof. The image $f(X)$ is a closed subvariety of Y, since X is a complete variety and Y is a separated variety. In particular, every point $b \in f(X)$ induces the translation map t_b which gives an isomorphism of $f^{-1}(0) \to f^{-1}(b)$. It follows that all fibers of f over points of $f(X)$ are isomorphic up to extension of scalars, so that they have the same dimension. It follows that

$$\dim f^{-1}(b) = \dim X - \dim f(X),$$

which immediately shows the equivalence of the first three statements. The last statement clearly implies that f is a isogeny, as fibers of finite morphisms are finite sets, in particular the kernel. Now suppose f is an isogeny. Then, by the above, f is quasi-finite. As $\dim X = \dim Y$ and both X, Y are irreducible regular noetherian schemes, then f must be flat, see [1, Chapter V]. □

Definition 2.4. Let $f : X \to Y$ be an isogeny. The *degree* of f is equal to the degree of the function field extension $[k(X) : f^*k(Y)]$, where $f^* : k(Y) \to k(X)$ is the pull-back.

As mentioned in the proof of Proposition 2.3, the fibres of f are translates of $\mathrm{Ker}(f)$. Hence, the sheaf $f_*\mathcal{O}_X$ is a locally free $\mathcal{O}_Y$-module of finite rank. One can compute this rank to be equal to the degree of f. Similar as to (homo)morphisms, if $f : X \to Y$ and $g : Y \to Z$ are isogenies, then so is $g \circ f$ and furthermore, $\deg(g \circ f) = \deg(g) \cdot \deg(f)$.

One important isogeny is the multiplication map by a non-zero integer, which intuitively is the group law applied multiple times to the same element. We will use the notation $x + x$ for $m(x, x)$. Note that for $m(x, m(x, x)) = x + x + x = m(m(x, x), x)$ there is no confusion due to associativity, so we can use this notation for multiple iterative operations.

Definition 2.5. For an abelian variety X over a field k, the *multiplication by n* map given by

$$\begin{aligned}[n]_X &: X \to X \\ x &\mapsto n \cdot x = \underbrace{x + x + \cdots + x}_{n \text{ times}},\end{aligned}$$

where $n \neq 0$ (for negative n, it maps x to $n \cdot i(x)$). We write $X[n] := \mathrm{Ker}([n]_X)$ for the kernel of the map, which is the *n-torsion of the abelian variety.*

One can show that the degree of the map $[n]_X$ is exactly n^{2g}, where $g = \dim X$. Furthermore, given an isogeny $f : X \to Y$ of degree d, we can find a nice way to relate it to $[d]_X$.

Proposition 2.6. *Let $f : X \to Y$ be an isogeny of abelian varieties of degree d. There exists an isogeny $g : Y \to X$ such that $g \circ f = [d]_X$ and $f \circ g = [d]_Y$.*

Proof. Since f is of degree d, we know that $\operatorname{Ker}(f)$ is a finite group scheme of rank d. It follows that $\operatorname{Ker}(f)$ is annihilated by $[d]_X$, so $[d]_X$ factors as

$$[d]_X = \left(X \xrightarrow{f} Y \xrightarrow{g} X\right)$$

for some isogeny $g : Y \to X$. Then, we as isogenies must respect the group structure, we deduce that

$$g \circ [d]_Y = [d]_X \circ g = g \circ f \circ g.$$

In general, if f, g_1, g_2, h are isogenies of abelian varieties such that $h \circ g_1 \circ f = h \circ g_2 \circ f$, then $g_1 = g_2$. Thus from the above, we find that $[d]_Y = f \circ g$ if we compose both sides with the identity on Y. □

With the above, we can state an important result for the goal of this thesis.

Corollary 2.7. *Define the relation $\sim$ on abelian varieties over k by*

$$X \sim_k Y \iff \text{there exists an isogeny } f : X \to Y.$$

Then, $\sim_k$ is an equivalence relation.

Example 2.8. This example is from [19, Chapter III, Example 4.5]. Let k be a field with $\operatorname{char}(k) \neq 2$ and $A, B \in k$ such that $B \neq 0$ and $A^2 - 4B \neq 0$. Consider the elliptic curves given by

$$\begin{aligned} E_1 &: y^2 = x^3 + Ax^2 + Bx, \\ E_2 &: Y^2 = X^3 - 2AX^2 + (A^2 - 4B)X \end{aligned}$$

over k. Then, one can verify that the maps

$$\begin{aligned} \phi &: E_1 \to E_2, & \hat{\phi} &: E_2 \to E_1, \\ (x, y) &\mapsto \left(\frac{y^2}{x^2}, \frac{y(B - x^2)}{x^2}\right), & (X, Y) &\mapsto \left(\frac{Y^2}{4X^2}, \frac{Y(A^2 - 4B - X^2)}{8X^2}\right). \end{aligned}$$

define isogenies. The kernels of these maps are

$$\begin{aligned} \operatorname{Ker}(\phi) &= \{O_{E_1}, (0, 0)\}, \\ \operatorname{Ker}(\hat{\phi}) &= \{O_{E_2}, (0, 0)\}. \end{aligned}$$

The map ϕ is unramified at both those points and similarly for $\hat{\phi}$. This shows that both maps are of degree 2. Note that on both elliptic curves, the point $(0, 0)$ has order 2, which can be deduced from the formulas in Example 1.4. Furthermore, a direct computation shows $\phi \circ \hat{\phi} = [2]_{E_2}$ and $\hat{\phi} \circ \phi = [2]_{E_1}$.

Any isogeny can be factorised in a helpful way. For that, we will first make the following definition regarding separability and inseparability of an isogeny. See [4, Chapter 5] for more details.

Definition 2.9. Let $f : X \to Y$ be an isogeny of abelian varieties. We call f *separable* if the function field $k(X)$ is a separable field extension of $f^*k(Y)$ and *purely inseparable* if $k(X)$ is a purely separable extension of $f^*k(Y)$.

Again, we have multiple equivalent definitions for the above, using the *étale* property.

Proposition 2.10. *Let $f : X \to Y$ be an isogeny of abelian varieties.*

1. *Then the following are equivalent:*
   - *(a) f is a separable isogeny;*
   - *(b) f is an étale morphism, i.e. the induced map df of tangent spaces at any point is an isomorphism;*
   - *(c) $Ker(f)$ is an étale group scheme.*
2. *Furthermore, the following are equivalent:*
   - *(a) f is a purely inseparable isogeny;*
   - *(b) f is a purely inseparable morphism;*
   - *(c) $Ker(f)$ is a connected group scheme.*

See [16] to learn more about étale morphisms and schemes and [4, Proposition 5.6] for the proof.

Each isogeny can therefore be broken up into a separable part and an inseparable part.

Corollary 2.11. *Let $f : X \to Y$ be an isogeny of abelian varieties. Then f can be factorised into a composition $f = h \circ g$ with $g : X \to Z$ a purely inseparable and $h : Z \to Y$ a separable isogeny of abelian varieties. Furthermore, if $f = h' \circ g' : X \to Z' \to Y$, then there is an isomorphism $\alpha : Z \to Z'$ with $g' = \alpha \circ g$ and $h' = \alpha \circ h$.*

3 Tate-ℓ-module

Recalling the map given in Definition 2.5, one can prove that $[n]_X$ is separable if $\gcd(n, \mathrm{char}(k)) = 1$. In particular, this lets us deduce the structure of the n-torsion subgroup, see [4, Corollary 5.11].

Proposition 3.1. *Let X be an abelian variety over a field k. Let k_s be the separable closure of k. If $gcd(char(k), n) = 1$, then $X[n](k_s) \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$.*

Let ℓ be a prime different from $\mathrm{char}(k)$. Since $[\ell^n]_X$ is in this case separable, it can be shown that $X[\ell^n]$ is completely determined by the ℓ^n-torsion points $X[\ell^n](k_s)$ in $X(k_s)$ and the natural action of the Galois group $\mathrm{Gal}(k_s/k)$. Furthermore, by Proposition 3.1, we find that $X[\ell^n](k_s) \simeq (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$ and note that multiplication by ℓ induces a group homomorphism

$$X[\ell^{n+1}](k_s) \xrightarrow{[\ell]_X} X[\ell^n](k_s)$$

and so a homomorphism $X[\ell^{n+1}] \to X[\ell^n]$ of group schemes as well. Taking the inverse limit of n, one finds a construction similar to that of the ℓ-adic integers $\mathbb{Z}_\ell$ from the finite groups $\mathbb{Z}/\ell^n\mathbb{Z}$.

Definition 3.2. Let X be an abelian variety over a field k. The *Tate-ℓ-module* of X is the inverse limit

$$T_\ell X := \varprojlim_n X[\ell^n](k_s),$$

where the inverse limit is taken with respect to the natural maps

$$X[\ell^{n+1}](k_s) \xrightarrow{[\ell]_X} X[\ell^n](k_s).$$

Using Proposition 3.1, we determine that the structure of $T_\ell X$ is that of a free $\mathbb{Z}_\ell$-module of rank $2g$, where $g = \dim X$. Explicitly, an element x of $T_\ell X$ is the limit of an infinite sequence $(x_1, x_2, \ldots)$ in $X(k_s)$ such that $\ell \cdot x_1 = 0$ in $X(k_s)$ and $\ell \cdot x_j = x_{j-1}$ for each $j > 1$. In particular, it follows that $x_j \in X[\ell^n](k_s)$ for each $1 \leq j \leq n$.

As $\mathrm{Gal}(k_s/k)$ has a natural action on each $X[\ell^n](k_s)$, we obtain a natural action of $\mathrm{Gal}(k_s/k)$ on $T_\ell X$, namely the ℓ-adic representation

$$\rho : \mathrm{Gal}(k_s/k) \to \mathrm{Aut}(T_\ell X).$$

We will now describe a useful property of the Tate module. Let $f : X \to Y$ be a homomorphism of abelian varieties over a field k. As f is a homomorphism, it must map ℓ^n-torsion points of X to ℓ^n-torsion points of Y, i.e. for each integer n, f induces a map

$$f : X[\ell^n](k_s) \to Y[\ell^n](k_s).$$

In particular, it induces a map

$$T_\ell f : T_\ell X \to T_\ell Y,$$

which is $\mathbb{Z}_\ell$-linear and $\mathrm{Gal}(k_s/k)$-equivariant. This leads to the following result, see [15, Theorem I.10.15]

Lemma 3.3. *Let X and Y be abelian varieties over a field k. For any prime $\ell \neq char(k)$, the natural map*

$$\mathrm{Hom}(X, Y) \otimes \mathbb{Z}_\ell \to \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell X, T_\ell Y)$$

given by $f \otimes c \mapsto c \cdot T_\ell f$ is injective and has finite cokernel.

Tate [24] showed an even stronger result in the case where k is a finite field.

Theorem 3.4. *Let k be a finite field, X and Y abelian varieties over k. Then*

$$\mathrm{Hom}(X,Y)\otimes\mathbb{Z}_\ell\to\mathrm{Hom}_{\mathbb{Z}_\ell[Gal(k_s/k)]}(T_\ell X,T_\ell Y)$$

is an isomorphism, where on the right-hand side we mean $\mathbb{Z}_\ell$-linear homomorphisms $T_\ell X\to T_\ell Y$ that commute with $Gal(k_s/k)$.

Since $T_\ell X$ is a free $\mathbb{Z}_\ell$-module of rank $2\dim X$ and similarly for Y, we get the structure of $\mathrm{Hom}(X,Y)$.

Corollary 3.5. *Let X and Y abelian varieties over a field k. Then $\mathrm{Hom}(X,Y)$ is a free $\mathbb{Z}$-module of rank $\leq 4\cdot\dim(X)\cdot\dim(Y)$.*

As $T_\ell X$ is a free $\mathbb{Z}_\ell$-module, it can be embedded into the vector space $V_\ell X:=T_\ell X\otimes_{\mathbb{Z}_\ell}\mathbb{Q}_\ell$. As an isogeny $f:X\to Y$ of abelian varieties over k induces a map $T_\ell f:T_\ell X\to T_\ell Y$, we also get an induced map $V_\ell f:V_\ell X\to V_\ell Y$. The map $V_\ell f$ is an isomorphism, as X and Y have the same dimension and f is surjective by Proposition 2.3. Similar as $T_\ell f$, it behaves well under the Galois group action $\mathrm{Gal}(k_s/k)$.

In particular, if $f:X\to X$ is an endomorphism, then we obtain a linear transformation $V_\ell f$ on $V_\ell X$.

Definition 3.6. Let X be an abelian variety over a field k. Let ℓ be a prime such that $\ell\neq\mathrm{char}(k)$. The *characteristic polynomial* $P_f(x)$ of the endomorphism $f:X\to X$ is the characteristic polynomial of the matrix induced by $V_\ell f:V_\ell X\to V_\ell X$, i.e. $P_f(x)=\det(x\cdot\mathrm{id}_{2g}-V_\ell f)$.

It can be shown that this definition does not depend on the choice of the prime ℓ, for example in [4, Theorem 12.18]. Note that $V_\ell X$ is a vector space over $\mathbb{Q}_\ell$ of dimension $2g$. Hence, the matrix induced by $V_\ell f$ is a $2g\times 2g$-matrix with coefficients in $\mathbb{Q}_\ell$ and so $P_f(x)$ is a degree $2g$ monic polynomial in $\mathbb{Q}_\ell$ by linear algebra. In particular, we know that the coefficient of x^{2g-1} is minus the trace of the matrix, which we will call the *trace* $\mathrm{Tr}(f)$ *of* f.

Moreover, an alternative way to define the characteristic polynomial is due to the following property, see [4, Chapter 12]:

Proposition 3.7. *Let X be an abelian variety over a field k. Let $f:X\to X$ be an endomorphism. Then there is a unique monic polynomial $P_f(x)\in\mathbb{Q}[x]$ which has degree $2g$ and satisfies $P_f(n)=\deg(f-[n]_X)$ for all $n\in\mathbb{Z}$.*

An important consequence of this correspondence is that there is a factorisation of the characteristic polynomial of the endomorphism f in accordance to how the abelian variety X can be decomposed.

Definition 3.8. An abelian variety X is called *simple* if there is no abelian subvariety $Y\subsetneq X$ such that $Y\neq 0$. We call X *elementary* if it is isogenous to a power of a simple abelian variety.

One can show that every abelian variety X can be decomposed into a product of elementary abelian varieties such that none of the simple abelian varieties are isogenous, see [4, Corollary 12.5]. In other words, there are simple abelian varieties $X_1,\dots,X_t$ with no two of them isogenous and positive integers $m_1,\dots,m_t$ with

$$X\sim_k X_1^{m_1}\times\cdots\times X_t^{m_t}. \tag{3.1}$$

This decomposition then also tells us something about the $\mathbb{Q}$-algebra $\mathrm{End}^0(X):=\mathrm{End}(X)\otimes\mathbb{Q}$. Note that any homomorphism between simple abelian varieties must be either 0 or an isogeny. Therefore, for simple abelian varieties X, we have that $\mathrm{End}^0(X)$ must be a division algebra, as we have seen that for any endomorphism f there exists an endomorphism g with $g\circ f=[\deg(f)]_X$ and in $\mathrm{End}^0(X)$, this has an inverse, namely as $\deg(f)$ is an integer, so it has an inverse in $\mathbb{Q}$. Furthermore, one can deduce that then $\mathrm{End}^0(X^n)$ is then isomorphic to $M_n(\mathrm{End}^0(X))$, which consists of all $n\times n$-matrices with coefficients in $\mathrm{End}^0(X)$. From this, it can be determined that if X is of the form as in (3.1), then the following result holds.

Lemma 3.9. *Let X be an abelian variety over a field k such that it is isogenous to*

$$X\sim_k X_1^{m_1}\times\cdots\times X_t^{m_t}$$

where each $X_1, \dots, X_t$ is simple and no two of them are isogenous. Then,

$$End^0(X) \simeq M_{m_1}(End^0(X_1)) \times \cdots \times M_{m_t}(End^0(X_t)),$$

where $End^0(X) = End(X) \otimes \mathbb{Q}$ and $M_m(End^0(X_j))$ is the $m \times m$ matrix ring with indices in $End^0(X_j)$.

4 Frobenius endomorphism

An important isogeny is the *Frobenius endomorphism* when working with an abelian variety X over a finite field $\mathbb{F}_q$, where q is a prime power. On $\overline{\mathbb{F}}_q$, there exists an automorphism given by $x \mapsto x^q$, of which the fixed points are exactly $\mathbb{F}_q$. If we have an algebraic variety X over $\overline{\mathbb{F}}_q$, then this map induces a morphism $X \to X$, which fixes $X(\mathbb{F}_q)$.

Definition 4.1. For an algebraic variety X over $\mathbb{F}_q$, the *Frobenius endomorphism* $\pi_X : X \to X$ is defined to be the identity on the underlying topological space X and $f \mapsto f^q$ on the sections f of the sheaf O_X.

Note that if $f : X \to Y$ is a morphism, then $f \circ \pi_X = \pi_Y \circ f$. In particular, for any projective embedding $X \to \mathbb{P}^n$, the Frobenius endomorphism induces the map $(x_0 : \ldots : x_n) \mapsto (x_0^q : \ldots : x_n^q)$ on $X(\overline{\mathbb{F}}_q)$ and the fixed points are given by $X(\mathbb{F}_q)$. In other words, $\mathrm{Ker}(\pi_X - \mathrm{id}) = X(\mathbb{F}_q)$ if we view the Frobenius endomorphism as $\pi_X : X(\overline{\mathbb{F}}_q) \to X(\overline{\mathbb{F}}_q)$. One can show that the map $\pi_X - \mathrm{id}$ is a separable map, which can be deduced from observing that the map $(d\pi)_0$ is equal to 0 for any variety over a field of characteristic p. If restricted to an affine open $U \subseteq X$, which can be embedded into $\mathbb{A}^n$, the map π is given by $X_i \mapsto X_i^q$, which has differential $d(X_i^q) = qX_i^{q-1} = 0$ in characteristic p. Hence, it follows that

$$d(\pi - \mathrm{id})_0 = (d\pi)_0 - d(\mathrm{id})_0 = 0 - 1 = -1,$$

which implies $\pi - \mathrm{id}$ is separable at the origin by Proposition 2.10. In particular due to the structure of abelian varieties, it follows that it is separable at every point.
Hence, if X is an abelian variety over $\mathbb{F}_q$, then the identity element is fixed under the Frobenius. It follows that π_X is an endomorphism. Moreover, one can show that its degree is q^g and that it is a purely inseparable map, refer to [4, Theorem 5.15]. Furthermore, we can consider its characteristic polynomial $P_{\pi_X}(x)$ and deduce some properties, as explained in [15, Theorem II.1.1].

Definition 4.2. Let X be an abelian variety over a finite field $\mathbb{F}_q$ and π_X the Frobenius endomorphism. The *characteristic polynomial of* X is the characteristic polynomial $P_{\pi_X}(x) \in \mathbb{Z}[x]$ of the Frobenius endomorphism.

Theorem 4.3. *Let X be an abelian variety over a finite field $k = \mathbb{F}_q$. Let $P_{\pi_X}(x)$ be its characteristic polynomial. Write $P_{\pi_X}(x) = \prod_{i=1}^{2g}(x - \alpha_i)$ for some $\alpha_1, \ldots, \alpha_{2g} \in \mathbb{C}$. Then*

(a) $|X(\mathbb{F}_{q^m})| = \prod_{i=1}^{2g}(1 - \alpha_i^m)$,

(b) $|\alpha_i| = q^{\frac{1}{2}}$.

Example 4.4. Let E be an elliptic curve over $\mathbb{F}_q$. Then the characteristic polynomial of the Frobenius endomorphism on E is given by the polynomial $x^2 - tx + q$, where t is the *trace of Frobenius* and $|E(\mathbb{F}_q)| = q + 1 - t$.

To see why Theorem 4.3 (a) holds, note that we explained above that $\pi_X - \mathrm{id}_X$ is a separable map. This implies

$$|X(\mathbb{F}_q)| = \deg(\pi_X - \mathrm{id}),$$

as the kernel of $\pi_X - \mathrm{id}_X$ is exactly $X(\mathbb{F}_q)$. Then by Proposition 3.7, it follows that $P_{\pi_X}(1) = \deg(\pi_X - \mathrm{id}_X)$ as $[1]_X = \mathrm{id}_X$. If we replace q with q^m and π_X with π_X^m, we get a similar result. Note that by linear algebra, if $\alpha_1, \alpha_2, \ldots, \alpha_{2g}$ are the eigenvalues of π_X, then $\alpha_1^m, \alpha_2^m, \ldots, \alpha_{2g}^m$ are those of π_X^m. For (b), one uses the *Rosati involution* on $\mathrm{End}(X) \otimes \mathbb{Q}$, see [15, Section I.14, Lemmas II.1.2 and II.1.3].

Theorem 4.3 is closely related to the *Weil conjectures* for abelian varieties.

Definition 4.5. Let X be a projective variety over $\mathbb{F}_q$. Let $N_1, N_2, \ldots$ be the sequence such that $N_m = |X(\mathbb{F}_{q^m})|$. The *zeta function* of X is defined as the power series

$$Z(X;t) = \exp\left(\sum_{m=1}^{\infty} N_m \frac{t^m}{m}\right) \in \mathbb{Q}[\![t]\!].$$

Example 4.6. Let $X = \mathbb{P}^1$ be the projective line over $\mathbb{F}_q$. We know that $\mathbb{P}^1$ over any field k is the union $\mathbb{P}^1(j) = \{(x:1) \mid x \in j\} \cup \{(1:0)\}$. Thus, $N_m = |X(\mathbb{F}_{q^m})| = q^m + 1$ and we deduce

$$Z(X;t) = \exp\left(\sum_{m=1}^{\infty}(q^m+1)\frac{t^m}{m}\right).$$

Moreover, due to the power series expansion of the logarithm we find

$$\log Z(\mathbb{P}^1;t) = \sum_{m=1}^{\infty}(q^m+1)\frac{t^m}{m} = -\log(1-t) - \log(1-qt) = \log\left(\frac{1}{(1-t)(1-qt)}\right).$$

In particular, we have determined that

$$Z(\mathbb{P}^1;t) = \frac{1}{(1-t)(1-qt)}.$$

Theorem 4.7. *Let X be an abelian variety over $\mathbb{F}_q$ of dimension g. Then the following holds:*

1. *Rationality*

$$Z(X;t) \in \mathbb{Q}(t),$$

i.e. $Z(t)$ is a rational function.

2. *Functional equation*

$$Z\left(X;\frac{1}{q^g t}\right) = \pm q^{g\epsilon/2}t^{\epsilon}Z(X;t),$$

where ϵ is the Euler characteristic of X.

3. *Riemann hypothesis*

$$Z(X;t) = \frac{P_1(t)P_3(t)\cdots P_{2g-1}(t)}{P_0(t)P_2(t)\cdots P_{2g}(t)},$$

where $P_i(t) \in \mathbb{Z}[t]$ for each i such that $P_0(t) = 1-t$ and $P_{2g}(t) = 1 - q^g t$ and for each $1 \leq i \leq 2g-1$, the polynomial $P_i(t)$ factors over $\mathbb{C}$ as

$$P_i(t) = \prod(1-\alpha_{ij}t),$$

with $|\alpha_{ij}| = q^{1/2}$. The degree of $P_i(t)$ is called the i^{th} Betti number of X.

See Weil's article [27] for more details.

From Theorem 4.3 and the fact that the characteristic polynomial has real coefficients, we can deduce some properties regarding multiplicities of roots, as described in [4, Theorem 16.4].

Corollary 4.8. *Let X be an abelian variety over $\mathbb{F}_q$ and $P_{\pi_X}(x)$ its characteristic polynomial. If α is a non-real root of $P_{\pi_X}(x)$, then its conjugate $\overline{\alpha} = q/\alpha$ is as well and they both have the same multiplicity. Furthermore, if $\alpha = \sqrt{q}$ or $\alpha = -\sqrt{q}$ is a root of $P_{\pi_X}(x)$ is a root, then it has an even multiplicity.*

Proof. As $|\alpha| = \sqrt{q}$ due to Theorem 4.3, we have $\overline{\alpha} = q/\alpha$. Furthermore, because $P_{\pi_X}(x)$ is a real polynomial, it is clear that α and $\overline{\alpha}$ must have the same multiplicity. It follows that we can pair the non-real roots with their complex conjugates to factor $P_{\pi_X}(x)$ over $\mathbb{R}$ into

$$P_{\pi_X}(x) = (x-\sqrt{q})^k(x+\sqrt{q})^{\ell}\prod_{\substack{P_{\pi_X}(\alpha)=0\\ \mathrm{Im}(\alpha)>0}}(x^2-(\alpha+\overline{\alpha})x+q), \tag{4.1}$$

where the product is taken over all non-real roots with positive imaginary part to ensure conjugate roots are not counted twice. Since P_{π_X} is a polynomial of degree $2g$ and all non-real roots occur in pairs with their complex conjugate, we must have that $k+\ell$ is even. Suppose k and ℓ are both odd and that without loss of generality $k \leq \ell$. Then

$$(x-\sqrt{q})^k(x+\sqrt{q})^\ell = (x^2-q)^k(x+\sqrt{q})^{\ell-k}.$$

As $\ell-k$ is even, the constant term of $(x+\sqrt{q})^{\ell-k}$ is $q^{(\ell-k)/2}$. As k is odd, the constant coefficient of $(x^2-q)^k$ is $-q^k$ and so we would get that the right-hand side of (4.1) will be equal to $-q^g$. However, from linear algebra, we know that $P_{\pi_X}(0) = \deg(\pi_X(x)) = q^g$, which is a contradiction. Hence, the multiplicities of the even roots are even. □

Hence, we can factor the characteristic polynomial into quadratic polynomials in $\mathbb{R}$, of the form

$$P_{\pi_X}(x) = \prod_{i=1}^{g}(x^2-(\alpha_i+\overline{\alpha_i})x+q),$$

with $|\alpha_i+\overline{\alpha_i}| \leq 2\sqrt{q}$. From this, we can deduce that the characteristic polynomial is of the form

$$\begin{aligned} P_{\pi_X}(x) &= x^{2g}+a_1x^{2g-1}+\cdots+a_{g-1}x^{g+1}+a_gx^g+a_{g-1}qx^{g-1}+\cdots+a_1q^{g-1}x+q^g \\ &= x^{2g}+a_gx^g+q^g+\sum_{i=1}^{g-1}a_i\left(x^{2g-i}+q^{g-i}x^i\right). \end{aligned}$$

5 Isogeny classification

The importance of the characteristic polynomial of the Frobenius endomorphism of abelian varieties over finite fields is due to the following result by Tate [24, Theorem 1].

Theorem 5.1. *Let X and Y be abelian varieties over a finite field k and let π_X and π_Y be the characteristic polynomials of their respective Frobenius endomorphisms. Then the following are equivalent:*

1. *X and Y are k-isogenous.*
2. *$P_{\pi_X}(x) = P_{\pi_Y}(x)$.*
3. *$Z(X;t) = Z(Y;t)$.*
4. *$|X(k')| = |Y(k')|$ for any finite extension k' of k.*

By Theorem 4.3 and Definition 4.5 it is very clear why the last three statements are equivalent. For the equivalence of the first two statements, one uses Theorem 3.4. Namely, one shows that $P_{\pi_X}(x)$ divides $P_{\pi_Y}(x)$ if and only if $V_\ell(X)$ is isomorphic to a subspace of $V_\ell(Y)$ for some ℓ, which follows from the semisimple actions of the Frobenius endomorphisms on the Tate modules and that the latter statement equivalent is to X being isogenous to an abelian subvariety of Y using Theorem 3.4.

Furthermore, if we decompose any abelian variety X over a finite field k into a product of elementary abelian varieties, say

$$X \sim_k X_1^{m_1} \times \cdots \times X_n^{m_n},$$

then by Lemma 3.9, if $P_{\pi_X}(x)$ denotes the characteristic polynomial of X and $P_{\pi_{X_1}}(x), \ldots, P_{\pi_{X_n}}(x)$ of $X_1, \ldots, X_n$ respectively, we get

$$P_{\pi_X}(x) = \prod_{i=1}^{n} (P_{\pi_{X_i}}(x))^{m_n}.$$

Therefore, we will assume that X is a simple abelian variety until the end of this chapter. By Tate [24, Theorem 2], we know that the center $\mathbb{Q}[\pi_X]$ of $\mathrm{End}(X) \otimes \mathbb{Q}$ is a field and that $P_{\pi_X}(x)$ is a power of a polynomial $P(x) \in \mathbb{Q}[x]$ that is irreducible over $\mathbb{Q}$, say $P_{\pi_X}(x) = P(x)^d$. More precisely, the polynomial $P(x)$ is the minimal polynomial of π_X over $\mathbb{Q}$, where we identify the Frobenius endomorphism with a root of the characteristic polynomial and consider the embedding $\mathbb{Q}[\pi_X] \to \mathbb{C}$. Moreover, it holds that $\deg(P) = [\mathbb{Q}(\pi_X) : \mathbb{Q}]$ and $d = [\mathrm{End}^0(X) : \mathbb{Q}(\pi_X)]^{1/2}$, consequently $2\dim(X) = d \cdot \deg(P)$.

Definition 5.2. Let q be a prime power. A *q-Weil number* π is an algebraic integer such that $|\sigma(\pi)| = \sqrt{q}$ for every embedding $\sigma : \mathbb{Q}[\pi] \to \mathbb{C}$. The set of all q-Weil numbers is denoted by $W(q)$. We say that two q-Weil numbers are *conjugate* if they have the same minimal polynomial over $\mathbb{Q}$. A monic polynomial $P(x)$ with integer coefficients is called a *q-Weil polynomial* if every root of $P(x)$ is a q-Weil number.

By Theorem 4.3, we see that the Frobenius endomorphism represents a conjugacy class of q-Weil numbers, so we can indeed identify the Frobenius endomorphism with an algebraic integer $\pi \in \overline{\mathbb{Q}}$. Let π be any algebraic integer. Due to the restrictions on q-Weil numbers and its conjugates, one can show that π must be either one of the following forms, see [3, Lemma 2.2].

Lemma 5.3. *π is a q-Weil number if and only if either*

1. *$\pi = \sqrt{q}$ or $\pi = -\sqrt{q}$, or*
2. *π is a (complex) root of $x^2 - (\pi + q/\pi)x + q$ with $\mathbb{Q}(\pi + q/\pi)$ a totally real field in which $(\pi + q/\pi)^2 - 4q$ is totally negative.*

Firstly, if $\pi = \sqrt{q}$ (or $\pi = -\sqrt{q}$), then its minimum polynomial is given by $x - \sqrt{q}$ (or $x + \sqrt{q}$) if $\sqrt{q} \in \mathbb{Z}$ and $x^2 - q$ if $\sqrt{q} \notin \mathbb{Z}$. If π does not have a real embedding note that the complex conjugate of π is $\overline{\pi} = q/\pi$, so that $\mathbb{Q}(\pi + q/\pi)$ is totally real and $\mathbb{Q}(\pi)$ is a quadratic extension of it. Furthermore, $|\pi + q/\pi| < 2\sqrt{q}$. Conversely, for any algebraic number $\beta \in \mathbb{R}$ with $|\beta| < 2\sqrt{q}$, the solutions of the equation $\pi^2 - \beta\pi + q = 0$ give q-Weil numbers π with $\mathbb{Q}(\pi)$ quadratic over $\mathbb{Q}(\beta)$, since the polynomial $x^2 - \beta x + q$ has a negative discriminant for $\beta < 2\sqrt{q}$ and so its roots are complex conjugates with absolute value $\sqrt{q}$.

With the definition of q-Weil numbers, one can now make a classification of simple abelian varieties up to isogeny, as we have seen in Theorem 4.3 that isogenous abelian varieties have the same characteristic polynomial, hence the same q-Weil numbers up to conjugacy. The following result has been proven by Honda [10] and Tate [23].

Theorem 5.4. *Let q be a prime power. There exists a bijection between isogeny classes of simple abelian varieties over $\mathbb{F}_q$ and conjugacy classes of q-Weil numbers given by associating a simple abelian variety X over $\mathbb{F}_q$ to a root of its characteristic polynomial.*

We can distinguish the cases between real q-Weil numbers, which are $\sqrt{q}$ and $-\sqrt{q}$, and non-real q-Weil numbers. A useful result from [8, Lemma 2.4] states that the simple abelian variety corresponding to a real q-Weil numbers is either of dimension 1 or 2, which can be deduced from the fact that the minimal polynomials of $\sqrt{q}$ and $-\sqrt{q}$ have degree 1 if q is a square or degree 2 if q is not a square.

Lemma 5.5. *Let X be a simple abelian variety over $\mathbb{F}_q = \mathbb{F}_{p^n}$ and $P_{\pi_X}(x)$ its characteristic polynomial. If $P_{\pi_X}(x)$ has a real root, then either*

1. $\dim(X) = 1$ *if n is even, or*
2. $\dim(X) = 2$ *if n is odd.*

6 Classification of q-Weil polynomials

We know that the characteristic polynomial of an abelian variety is a Weil polynomial. However, the converse is not necessarily true. Hence, in order to determine the isogeny classes of simple abelian varieties over a given finite field $\mathbb{F}_q$ as described in [8, Chapter 2], we will first have to determine a criterion for which a polynomial with integer coefficients of the form

$$x^{2g} + a_1 x^{2g-1} + \cdots + a_{g-1}x^{g+1} + a_g x^g + a_{g-1}qx^{g-1} + \cdots + a_1 q^{g-1}x + q^g \tag{6.1}$$

is a q-Weil polynomial. Furthermore, as X is simple and thus $P_{\pi_X}(x) = (P(x))^d$ where $P(x)$ is an irreducible q-Weil polynomial and d is a positive integer, we would also need to determine all possible d. Lastly for each of these d, we need to find the criteria for which a q-Weil polynomial of the form (6.1) is the characteristic polynomial of some simple abelian variety of dimension g over $\mathbb{F}_q$.

For isogeny classes of abelian varieties that are not simple, we can use and combine the results from lower dimensions, as the decomposition of an abelian variety into simple abelian varieties corresponds one-to-one with the factorisation of the characteristic polynomial into the characteristic polynomials of the simple abelian varieties.

6.1 Characteristic polynomial

Again, assuming we only consider simple abelian varieties over $\mathbb{F}_q = \mathbb{F}_{p^n}$, the characteristic polynomials will be of the form $P_{\pi_X}(x) = (P(x))^d$, where $P(x)$ is an irreducible q-Weil polynomial over $\mathbb{Q}$, i.e. $P(x)$ is the minimal polynomial of a q-Weil number.

For a polynomial of the form

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

we note that $h(x) = \frac{x^{2g}}{q^g} h\left(\frac{q}{x}\right)$ for $x \neq 0$, so we can rearrange the roots of h into $\alpha_1, q/\alpha_1, \alpha_2, q/\alpha_2, \ldots, \alpha_g, q/\alpha_g$. Pairing the root α_i with q/α_i gives

$$h(x) = \prod_{i=1}^{g}(x^2 - (\alpha_i + q/\alpha_i)x + q).$$

By Lemma 5.3, we must have $\alpha_i + q/\alpha_i \in \mathbb{R}$ and $|\alpha_i + q/\alpha_i| \leq 2\sqrt{q}$ for all i in order to get a q-Weil polynomial by the abc-formula. Equivalently, the polynomials

$$\begin{aligned} h^+(x) &= \prod_{i=1}^{g}(x - (2\sqrt{q} - (\alpha_i + q/\alpha_i))), \\ h^-(x) &= \prod_{i=1}^{g}(x - (2\sqrt{q} + (\alpha_i + q/\alpha_i))), \end{aligned}$$

only have non-negative roots. This results in the following statement.

Proposition 6.1. *Let $h(x)$ be an integer polynomial of degree $2g$ of the form*

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

Then, $h(x)$ is a q-Weil polynomial if and only if there exists $\omega_1, \ldots, \omega_g \in \mathbb{C}$ such that $h(x)$ can be factored into

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

over $\mathbb{C}$ and the polynomials

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

only have real roots that are all non-negative. Moreover, $h(x)$ has no real roots if and only if the roots of $h^+(x)$ and $h^-(x)$ are all positive.

The coefficients of $h^+(x)$ and $h^-(x)$ are related to those of $h(x)$ and can be described using the degree and coefficients of $h(x)$ without knowing the values of the ω_i's. The reason we formulate Proposition 6.1 in this way is because the degrees of $h^+(x)$ and $h^-(x)$ are equal to a half of the degree of $h(x)$. This means we can more easily determine conditions on the coefficients of $h^+(x)$ and $h^-(x)$ with unknown ω_i's using formulas for their roots.

If $P(x)$ does not have a real root, then by [26, Theorem 8] one can make a criterion on which d can occur given $P(x)$.

Lemma 6.2. *Let $P(x)$ be a q-Weil polynomial without real roots that is irreducible over $\mathbb{Q}$, where $q = p^n$. Let $f_1(x), \dots, f_t(x)$ be its irreducible factors over $\mathbb{Q}_p$. Then, $(P(x))^d$ is the characteristic polynomial of a simple abelian variety of dimension $\frac{1}{2} \cdot d \cdot \deg(P)$ over $\mathbb{F}_q$, where d is the least common denominator of*

$$\frac{v_p(f_1(0))}{n}, \dots, \frac{v_p(f_t(0))}{n},$$

where $v_p(f_i(0))$ is the p-adic valuation of $f_i(0)$.

If $P(x)$ does have a real root, we can simply apply Lemma 5.5.

In general, it is difficult to consider all possible powers d such that $(P(x))^d$ is the characteristic polynomial of an abelian variety of dimension $g = \frac{1}{2} \cdot d \cdot \deg(P)$, as g could have many divisors. The following result by Hayashida [8, Theorem 1.2] gives a clear criterion for the case where $d = g > 2$, i.e. characteristic polynomials of simple abelian varieties of dimension g that are of the form $(x^2 + ax + b)^g$, where $x^2 + ax + b$ is irreducible.

Theorem 6.3. *Let $a, b \in \mathbb{Z}$ and $2 < g \in \mathbb{Z}$. Set $h(x) = (x^2 + ax + b)^g \in \mathbb{Z}[x]$. Then the polynomial $h(x)$ is the characteristic polynomial of a simple abelian variety of dimension g over $\mathbb{F}_q = \mathbb{F}_{p^n}$ if and only if g divides n, $b = q$, $|a| < 2\sqrt{q}$ and $a = kq^{s/g}$, where $k, s \in \mathbb{Z}$ satisfying $gcd(k, p) = 1$, $gcd(g, s) = 1$ and $1 \leq s < g/2$.*

Example 6.4. Suppose $g = \ell$ is an odd prime. We want to find the d such that $(P(x))^d$ is the characteristic polynomial of a simple abelian variety, where $P(x)$ is an irreducible q-Weil polynomial. Clearly, d has to divide $2\ell = \deg((P(x))^d)$, so $d \in \{1, 2, \ell, 2\ell\}$. Suppose $d = 2\ell$ or $d = 2$, which means $\deg(P)$ is odd, so it must have a real root. However, this contradicts Lemma 5.5 as real q-Weil numbers correspond to simple abelian varieties of dimension 1 or 2. Therefore, the only characteristic polynomials of simple abelian varieties of dimension ℓ are those from Theorem 6.3 or irreducible q-Weil polynomials of degree 2ℓ satisfying Lemma 6.2 with $d = 1$.

6.2 Newton polygon

To check if an irreducible q-Weil polynomial without real roots satisfies Lemma 6.2 for a given d, one can look at its Newton polygon.

Definition 6.5. Let $P(x) = b_0 + b_1 x + \cdots + b_{d-1}x^{d-1} + b_e x^e$ be a polynomial with integer coefficients and p a prime integer. The *Newton polygon* of $P(x)$ with respect to p is the lower convex hull of the following set of points in the real coordinate plane:

$$S_p(P) = \{(0, v_p(b_0)), (1, v_p(b_1)), \dots, (d, v_p(b_e))\}.$$

A Newton polygon can be constructed from $S_p(P)$ by rotating a vertical line counterclockwise about $(0, v_p(b_0))$ and $(0, v_p(b_0))$ until it hits a point $(i, v_p(b_i))$ and taking the line segment from $(0, v_p(b_0))$ to the greatest i_1 such that $(i_1, v_p(b_{i_1}))$ is on the line. Afterwards, rotating the line counterclockwise about $(i_1, v_p(b_{i_1}))$ until it hits another point in S_P gives another edge by taking the line segment from $(i_1, v_p(b_{i_1}))$ to $(i_2, v_p(b_{i_2}))$, where i_2 is the largest index such that $(i_2, v_p(b_{i_2}))$ is on the line. Then continuing by rotating the line about $(i_2, v_p(b_{i_2}))$ and so on until the point $(e, v_p(b_e))$ is reached.

Example 6.6. Let $p = 2$ and

$$P(x) = x^{14}+3x^{13}+30x^{12}+28x^{11}+10x^{10}+16x^9+160x^8+224x^7+320x^6+64x^5+80x^4+448x^3+960x^2+192x+128.$$

Then the set $S_2(P)$ is

$$S_2(P) = \{(0,7),(1,6),(2,6),(3,6),(4,5),(5,6),(6,6),(7,5),(8,5),(9,4),(10,2),(11,2),(12,1),(13,0),(14,0)\}.$$

The Newton polygon of $P(x)$ is therefore as in Figure 2.

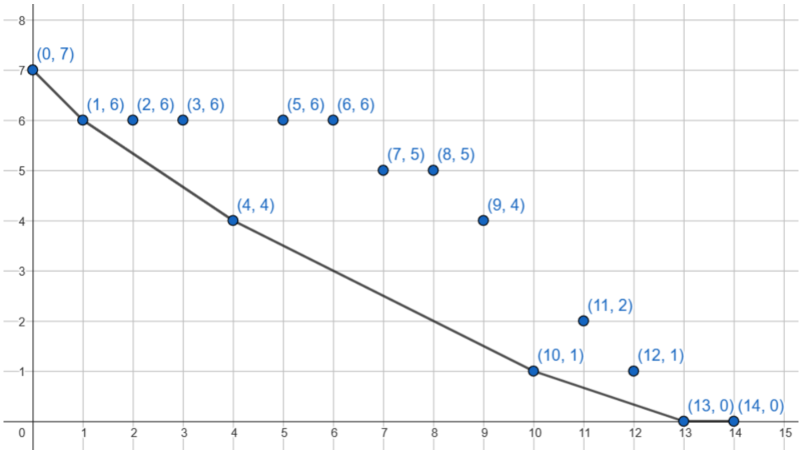


Figure 2: The Newton polygon for Example 6.6

Clearly, the initial point and endpoint of the Newton polygon with respect to p of a polynomial of the form

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

with $q = p^n$ are $(0, n \cdot g)$ and $(2g, 0)$ respectively. Furthermore, as $b_i = q^{g-i}b_{2g-i}$ for $1 \leq i \leq g-1$, we have $v_p(b_i) = n(g-i) + v_p(b_{2g-i})$ for $1 \leq i \leq g-1$. If α is a root of a q-Weil polynomial, then q/α is a root of the same multiplicity. This gives us a lot of information about the Newton polygon due to the following lemma [12, IV, Lemma 4].

Lemma 6.7. *Let $P(x)$ be a polynomial of degree $2g$ and L_P its splitting field in $\mathbb{C}$. Let $P(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{2g})$ be the factorisation of $P(x)$ in L_P. Denote by v_p the extension of the p-adic valuation from $\mathbb{Q}_p$ to L_P. Let $\lambda_i = -v_p(\alpha_i)$. If λ is the slope of a segment of the Newton polygon of $P(x)$ with respect to p with horizontal length m, then precisely m of the λ_i's are equal to λ.*

Corollary 6.8. *Let $P(x)$ be an irreducible q-Weil polynomial of degree $2g$, where $q = p^n$. Then $P(x)$ is the characteristic polynomial of a simple abelian variety of dimension g over $\mathbb{F}_q$ if and only if its Newton polygon satisfies the following conditions.*

1. *The initial point is $(0, gn)$ and the end point is $(2g, 0)$.*
2. *Every vertex is contained in the lattice $\mathbb{Z} \times n\mathbb{Z}$.*
3. *If the Newton polygon has an edge with slope $-\lambda$, then it has another edge with slope $-(n-\lambda)$ with the same horizontal length.*

Proof. The first statement is clear. Assuming the second statement holds, the third statement follows from Lemma 6.7 and

$$v_p(q/\alpha) = v_p(q) - v_p(\alpha) = n - v_p(\alpha).$$

By Lemma 6.2, we must have that $v_p(f_j(0)) \in n\mathbb{Z}$ for each irreducible factor $f_j(x)$ of $P(x)$ in $\mathbb{Q}_p[x]$. Furthermore, for each segment of the Newton polygon of $P(x)$, the length ℓ_j of its projection onto the horizontal axis is exactly the degree of a factor $f_j(x)$ of $P(x)$ in $\mathbb{Q}_p$ and all of the roots of $f_j(x)$ have valuation equal to $-s_j$, where s_j is the slope of the edge. Hence, we have that $v_p(f_j(0)) = l_j \cdot s_j$, i.e. the condition that $v_p(f_j)/n$ is an integer is equivalent to $l_j \cdot s_j$ being a multiple of n. This, in combination with the first statement, gives us that every vertex must have a multiple of n as y-coordinate. □

Constructing all possible Newton polygons satisfying these conditions and considering the possibilities for the coefficients gives us a classification of all possible characteristic polynomials.

Remark 6.9. Recall that if $P(x)$ is a q-Weil polynomial, we can write

$$\begin{aligned} P(x) &= x^{2g} + a_1x^{2g-1} + \cdots + a_{g-1}x^{g+1} + a_gx^g + a_{g-1}qx^{g-1} + \cdots + a_1q^{g-1}x + q^g \\ &= x^{2g} + a_gx^g + q^g + \sum_{i=1}^{g-1} a_i \left(x^{2g-i} + q^{g-i}x^i\right). \end{aligned}$$

As $v_p(q^{g-i}) = (g-i)n$, we have that the Newton polygon of $P(x)$ is uniquely determined by the values of $v_p(a_1), v_p(a_2), \ldots, v_p(a_g)$. Since the endpoints of the Newton polygon are $(0, gn)$ and $(2g, 0)$, we can determine all possible Newton polygons by looking at all lattice points with x-coordinate corresponding to $a_1, \ldots, a_g$ that are below the line between $(0, gn)$ and $(2g, 0)$ and on or above the x-axis.

The Newton polygons can be partially distinguished by the length of the segment with horizontal horizontal, which shows a property of the corresponding isogeny class.

Definition 6.10. Let X be an abelian variety over $\mathbb{F}_q = \mathbb{F}_{p^n}$. The p-rank of X is the integer $0 \leq r(X) \leq g$ such that $X[p](\overline{k}) \simeq (\mathbb{Z}/p\mathbb{Z})^{r(X)}$.

By Gonzalez [5, Proposition 3.1], we have the following proposition.

Proposition 6.11. *Let X be an abelian variety of dimension g over a finite field $k = \mathbb{F}_q = \mathbb{F}_{p^n}$ with characteristic polynomial $P_{\pi_X}(x)$. Let $r(X)$ be the p-rank of X. Then $r(X)$ is equal to the sum of the multiplicities of the non-zero roots of the* $\pmod p$*-reduced polynomial $P_{\pi_X}(x)$ in $\mathbb{C}$.*

If the characteristic polynomial is reduced modulo p, then it will be of the form

$$x^{2g} + a_1x^{2g-1} + \ldots + a_gx^g \equiv x^g(x^g + a_1x^{g-1} + \ldots + a_g) \pmod p.$$

The number of non-zero roots of this polynomial in $\mathbb{C}$ counted with multiplicity is equal to the largest index $0 \leq i \leq g$ such that $a_i \not\equiv 0 \pmod p$, equivalently the highest index i such that $v_p(a_i) = 0$, since the a_i's are all integers, so $v_p(a_i) \geq 0$. Hence, we immediately obtain the following result.

Corollary 6.12. *The p-rank of an abelian variety over $\mathbb{F}_q = \mathbb{F}_{p^n}$ with characteristic polynomial $P_{\pi_X}(x)$ is equal to the length of the horizontal slope of the Newton polygon of $P_{\pi_X}(x)$.*

7 Robinson's method

7.1 Explanation of the method

The method Haloui [6, Chapter 2] and Sohn [21] use to determine bounds on the coefficients of q-Weil polynomials is called Robinson's method, originally explained in [20, Chapter 2]. The method relies on two results. The first result is Rolle's theorem which implies that if a polynomial has only real roots that are all positive, then so does all its derivatives. The second result is the following lemma.

Lemma 7.1. *Let $k \geq 2$ and $h(x)$ be a monic polynomial of degree $k-1$ with real roots $\beta_1 > \beta_2 > \ldots > \beta_{k-1} > 0$. Consider the monic polynomial $H(x) = k\int_0^x h(t)dt$. Let $c \in \mathbb{R}$. Then every root of $H(x) - c$ is real and positive if and only if $(-1)^k c < 0$ and*

$$\max_{i=1}^{\lfloor k/2 \rfloor} H(\beta_{2i-1}) \leq c \leq \min_{i=1}^{\lfloor (k-1)/2 \rfloor} H(\beta_{2i}). \tag{7.1}$$

Proof. The statement can be deduced from looking at the graph of $H(x)$ which can be determined using the graph of $h(x)$. Namely, since $h(x)$ is a (multiple) of the derivative of $H(x)$, we know that $\beta_1, \ldots, \beta_{k-1}$ are the critical points of the graph of $H(x)$, i.e. the local minima and local maxima, since all roots are distinct. Since $H(x)$ is monic, there is some $x_0 \in \mathbb{R}$ such that $H(x)$ is only increasing for $x > x_0$. In particular, $H(x)$ attains a local minimum at $x = \beta_1$. Subsequently, as all roots are distinct and functions defined by polynomials are continuous, $H(x)$ attains a local maximum at $x = \beta_2$. Inductively, $H(\beta_{2_{i-1}})$ are all local minima and $H(\beta_{2i})$ are all local maxima. In order for all roots of $H(x) - c$ to be real, i.e. for the graph to have k distinct values of x for which $H(x) = c$, we must have that c is a value between all those local minima and maxima. In other words, c is a value greater than or equal to the highest local minimum and less than or equal to the lowest local maximum. Conversely, if c satisfies (7.1), then by looking at the graph we can determine that $H(x) - c$ has k real roots $\alpha_1 \geq \alpha_2 \geq \ldots \geq \alpha_k$ satisfying $\alpha_i \geq \beta_i$ for $1 \leq i \leq k-1$ and $\alpha_j \leq \beta_{j-1}$ for $2 \leq j \leq k$.

In particular, $\alpha_1, \ldots, \alpha_{k-1}$ are positive roots. The condition $(-1)^k c < 0$ follows from Descartes' rule of sign change, which states that the number of positive roots (counted with multiplicity) of a polynomial is either equal to the number of sign changes between consecutive coefficients of the polynomial or an even number less than that. Since $h(x)$ is a monic polynomial with all roots real and positive, it follows that the coefficients of $h(x)$ and subsequently $H(x)$ changes $k-1$ times, i.e. the sign of the coefficient of x^n in $H(x)$ is $(-1)^{k-n}$. In order for α_1 to be a positive root, we must have that the coefficients of $H(x) - c$ changes k times, as we know it has already at least $k-1$ positive roots. Hence, the condition $(-1)^k c < 0$ follows. □

Remark 7.2. The condition that $h(x)$ and $H(x)$ are monic polynomials is not strictly necessary, if we scale c appropriately, since the roots of $h(x)$ do not change if we multiply $h(x)$ by some real constant. Hence, the extrema of the primitives of $h(x)$ remain also at the same values of x. However, one should be careful when $h(x)$ has a negative leading coefficient. If that is the case, the primitives of $h(x)$ will have local maxima at the even-numbered roots of $h(x)$, while the local minima are at the odd-numbered roots of $h(x)$.

Corollary 7.3. *Let $H(x)$ be a polynomial with a derivative that has only real roots that are all positive. Let $c \in \mathbb{R}$. Then every root of $H(x) - c$ is real and positive, one of which being a multiple root, if and only if*

$$\max_{i=1}^{\lfloor k/2 \rfloor} H(\beta_{2i-1}) = c \leq \min_{i=1}^{\lfloor (k-1)/2 \rfloor} H(\beta_{2i}) \quad or \quad \max_{i=1}^{\lfloor k/2 \rfloor} H(\beta_{2i-1}) \leq c = \min_{i=1}^{\lfloor (k-1)/2 \rfloor} H(\beta_{2i}).$$

Proof. We will use the same notation as in Lemma 7.1. If $H(x) - c$ has a multiple root at some $x = \alpha$ if and only if α is also a root of its derivative, i.e. $h(\alpha) = 0$. This means $\alpha = \beta_i$ for some $1 \leq i \leq k-1$. Due to the restrictions on c in Lemma 7.1, the result follows. □

Example 7.4. Let

$$h(x) = x^4 - 10x^3 + 35x^2 - 50x + 24 = (x-1)(x-2)(x-3)(x-4),$$

so that $\beta_i = 5 - i$ for $1 \leq i \leq 4$. Then, we easily compute

$$\int_0^x h(t)dt = \frac{1}{5}x^5 - \frac{5}{2}x^4 + \frac{35}{3}x^3 - 25x^2 + 24x. \tag{7.2}$$

We will simply define $H(x)$ as the integral in (7.2) and make the graph of $H(x)$, see Figure 3. Since $h(x)$ is a polynomial of degree 4, we know $H(x) - c$ is a polynomial of degree 5 and hence has exactly 5 roots in $\mathbb{C}$, counted with multiplicity. We can see from the graph that $H(x) - c$ has exactly 5 real roots that are all positive if and only if

$$7 + \frac{11}{15} = \max\{H(4), H(2)\} \leq c \leq \min\{H(3), H(1)\} = 8 + \frac{1}{10}.$$

The condition that $(-1)^5 c < 0$ is in this case automatically satisfied.

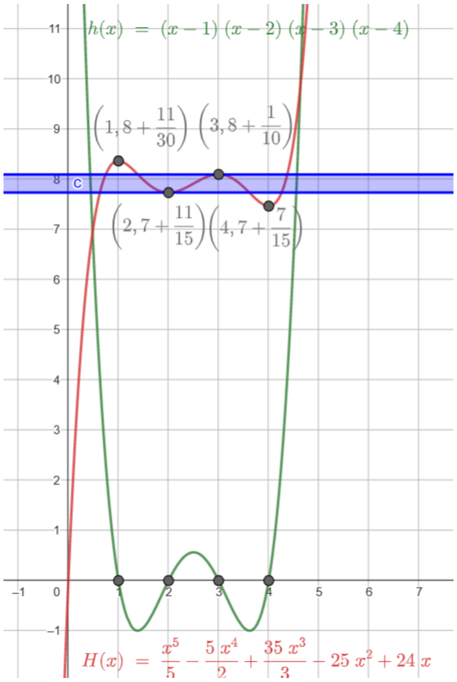


Figure 3: The values of c for which every root of $H(x) - c$ is real and positive

Henceforth, we will simply assume that the leading coefficient of $h(x)$ is positive and that $H(x) = \int_0^x h(t)dt$, i.e. $H(x)$ is the primitive of $h(x)$ with a root at $x = 0$.

Lemma 7.1 is still valid if $\beta_1 \geq \beta_2 \geq \ldots \geq \beta_{k-1} > 0$ instead of $\beta_1 > \beta_2 > \ldots > \beta_{k-1} > 0$, at least for the degrees k we will work with, which we will now explain. In particular, if $x = \beta_i$ is a multiple root, then either we must have $c = H(\beta_i)$ or such c does not exist. This is due to the following arguments.

Note that if β_i is a root of $h(x)$ with odd multiplicity, then it is a local minimum or maximum of $H(x)$, while if it is a root of $h(x)$ with even multiplicity, it is an inflection point of $H(x)$. Hence, it does not change the fact that in the labelling, the values for which $H(x)$ attains a local minima are all contained in $\{\beta_{2j-1} : 1 \leq j \leq \lfloor k/2 \rfloor\}$, while the values for which $H(x)$ attains a local maxima are all contained in $\{\beta_{2j} : 1 \leq j \leq \lfloor (k-1)/2 \rfloor\}$.

In the case that $h(x)$ has a multiple root at $x = \beta_i > 0$, say $h(x) = (x - \beta_i)^n \tilde{h}(x)$, where $\tilde{h}$ is a polynomial of degree $k - 1 - n$ with $\tilde{h}(\beta_i) \neq 0$, note that $h(x)$ has at most $k - n$ distinct roots and so $H(x) = k \int_0^x h(t)dt$ has at most $k - n$ critical points, as it is a primitive of $h(x)$. Therefore, the number of peaks and valleys in the graph of $H(x)$ is at most $k - n$. Hence, the number of distinct roots of $H(x) - c$ will be at most $k - n + 1$. In order for all the roots of $H(x) - c$ to be real, it must have a root of higher multiplicity, i.e. one of its critical points must be a root.

Lemma 7.5. *Let $h(x) = (x-\beta_i)^n \tilde{h}(x)$ be a polynomial, where $\tilde{h}(\beta_i) \neq 0$. Let $H(x)$ be a primitive of $h(x)$. If $H(\beta_i) = 0$, then $H(x) = (x-\beta_i)^{n+1}G(x)$ for some polynomial $G(x)$ with $G(\beta_i) \neq 0$, otherwise, $H(x) = (x-\beta_i)^{n+1}G(x) + c$ for some constant c. In particular, if $H(x) = \int_0^x h(t)dt$ and $c = H(\beta_i)$, then $H(x) - c$ has a root at $x = \beta_i$ of multiplicity $n+1$.*

Proof. We know that $H(x)$ is a primitive of $h(x)$ if and only if $H(x) + c$ is for any $c \in \mathbb{R}$. Furthermore, we also have that if $H(\beta_i) = 0$, then it is of the form $H(x) = (x-\beta_i)^\ell g(x)$ for some $\ell \in \mathbb{Z}_{>0}$ and polynomial $g(x)$ with $g(\beta_i) \neq 0$. Then computing its derivative gives

$$\begin{aligned}\frac{\mathrm{d}}{\mathrm{d}x}H(x) &= \ell(x-\beta_i)^{\ell-1}g(x) + (x-\beta_i)^\ell g'(x)\\ &= (x-\beta_i)^{\ell-1}\left(\ell \cdot g(x) + (x-\beta_i)g'(x)\right).\end{aligned}$$

Note that since $g(\beta_i) \neq 0$, we have

$$\left(\ell \cdot g(x) + (x-\beta_i)g'(x)\right)\big|_{x=\beta_i} = \ell \cdot g(\beta_i) \neq 0.$$

Hence, as $h(x)$ is equal to the derivative of $H(x)$, we find that $\ell - 1 = n$ and $\ell \cdot g(x) + (x-\beta_i)g'(x) = \tilde{h}(x)$. □

Corollary 7.6. *Let k be an integer with $2 \leq k \leq 5$. Let $h(x)$ be a polynomial of degree $k-1$ such that all of its roots are real and positive and at least one of which is a multiple root. Let β_i be a multiple root of $h(x)$ of multiplicity n. Suppose there exists a primitive $H(x) - c$ of $h(x)$ with all roots real and positive. Then β_i is necessarily a root of $H(x) - c$.*

Proof. Write $h(x) = (x-\beta_i)^n \tilde{h}(x)$ with $\tilde{h}(\beta_i) \neq 0$. If β_i is not a root of $H(x) - c$, the sum of the multiplicities of the real roots of $H(x) - c$ is equal to the number of distinct real roots plus their multiplicities as roots of $\tilde{h}(x)$. The number of distinct real roots of $H(x) - c$ at most the number of local maxima and local minima plus 1, i.e. the number of distinct roots of $h(x)$ plus 1, so $k - n + 1$. The polynomial $\tilde{h}(x)$ is of degree $k - 1 - n$, so the sum of the roots of the roots of $H(x) - c$ as roots of $\tilde{h}(x)$ is at most $k - 1 - n$.

If there is a critical point before a local minimum, the last such has to be a local maximum or a strictly decreasing point of inflection. Similarly, if there is a critical point before a local maximum, the last such has to be a local minimum or a strictly increasing point of inflection. This means that $H(x)$ does not attain the same value at all the different critical points. More precisely, if $H(x) - c$ has the same value at a local maximum x_1 as at a local minimum x_2, the graph must attain another local minimum and local maximum in the interval (x_1, x_2) and vice versa. Furthermore, $H(x) - c$ can only have the same value at an inflection point x_1 as at another critical point x_2 if $H(x) - c$ attains local maximum and/or local minimum in the interval (x_1, x_2). Therefore, the number of distinct real roots of $H(x) - c$ that are also roots of $\tilde{h}(x)$ is actually at most $\frac{1}{2}(k - 1 - n)$.

Computing the possible variations of the number of possible distinct roots and their multiplicities as roots of $\tilde{h}(x)$ for each n will always result in either β_i being a root of $H(x) - c$ or $H(x) - c$ having a complex root. □

Example 7.7. Take $k = 5$. If $h(x)$ has a triple root β_i, it can have at most 2 distinct real roots, so that its primitive $H(x)$ has at most two local extrema (exactly two to be precise). Hence, the number of distinct real roots that $H(x) - c$ can have is at most 3. If it has exactly 3 distinct real roots, then one of them has to be a triple root or two of them have to be double roots. However, neither can happen, since its derivative $h(x)$ has a triple root β_i and one simple real root. Hence, the number of distinct real roots is at most 2, which means there must be a real root of multiplicity at least 3. That is, the only possibility is a root of multiplicity 4 at β_i.

If $h(x)$ instead has two distinct double real roots β_i, β_j, then they are both inflection points of $H(x)$. Thus, $H(x)$ has no local minima or local maxima, so that $H(x) - c$ is increasing for all c, which shows it is not possible to have 5 real roots for $H(x) - c$.

Lastly, suppose $h(x)$ has one double root β_i and two simple roots β_{j_1}, β_{j_2}. A double root corresponds to an inflection point on $H(x)$. Therefore, $H(x)$ has exactly one local maxima and one local minima, namely at the simple roots $x = \beta_{j_1}$ and $x = \beta_{j_2}$ of $h(x)$. The number of distinct real roots of $H(x) - c$ is hence at most 3. Again, one of them must be a triple real root, which would correspond to $x = \beta_i$ or two of them have to be double real roots, which would correspond to β_{j_1} and β_{j_2}. However, since $H(x)$ has no other local minima or local maxima, the function is strictly decreasing (or increasing) between β_{j_1} and β_{j_2}, which shows it cannot happen that the values $H(\beta_{j_1})$ and $H(\beta_{j_2})$ are equal.

7.2 Application to low degrees

Lemma 7.8. *Let $g(x) := a_2x^2 + a_1x + a_0$ be a real polynomial with $a_2 > 0$ such that its derivative $g'(x) = 2a_2x + a_1$ has a positive root. Then, all roots of $g(x)$ are real and positive if and only if*

$$0 < a_0 \leq \frac{a_1^2}{4a_2}.$$

Proof. Note that the root of $g'(x)$ is at $x = -\frac{a_1}{2a_2}$, so in particular $a_1 < 0$. By Lemma 7.1, we compute that every root of $g(x)$ is real and positive if and only if $a_0 > 0$ and

$$-\frac{a_1^2}{4a_2} = a_2\left(-\frac{a_1}{2a_2}\right)^2 + a_1\left(-\frac{a_1}{2a_2}\right) \leq -a_0.$$

Hence, we obtain the bounds $0 < a_0 \leq \frac{a_1^2}{4a_2}$. □

Lemma 7.9. *Let $g(x) := a_3x^3 + a_2x^2 + a_1x + a_0$ be a real polynomial with $a_3 > 0$ such that all roots of its derivative are real and positive. Then every root of $g(x)$ is real and positive if and only if*

$$\frac{-2a_2^3 + 9a_1a_2a_3 - 2(a_2^2 - 3a_1a_3)^{3/2}}{27a_3^2} \leq a_0 \leq \frac{-2a_2^3 + 9a_1a_2a_3 + 2(a_2^2 - 3a_1a_3)^{3/2}}{27a_3^2},$$

and $a_0 < 0$.

Proof. The derivative $g'(x) = 3a_3x^2 + 2a_2x + a_1$ has roots

$$\alpha_1 = \frac{-a_2 + \sqrt{a_2^2 - 3a_1a_3}}{3a_3},$$
$$\alpha_2 = \frac{-a_2 - \sqrt{a_2^2 - 3a_1a_3}}{3a_3},$$

by the *abc*-formula. Clearly $\alpha_1 \geq \alpha_2$. We compute

$$a_3\alpha_1^3 + a_2\alpha_1^2 + a_1\alpha_1 = \frac{2a_2^3 - 9a_1a_2a_3 - 2(a_2^2 - 3a_1a_3)^{3/2}}{27a_3^2},$$
$$a_3\alpha_2^3 + a_2\alpha_2^2 + a_1\alpha_2 = \frac{2a_2^3 - 9a_1a_2a_3 + 2(a_2^2 - 3a_1a_3)^{3/2}}{27a_3^2}.$$

Hence by Lemma 7.1, the roots of $g(x)$ are real and positive if and only if

$$-\frac{2a_2^3 - 9a_1a_2a_3 + 2(a_2^2 - 3a_1a_3)^{3/2}}{27a_3^2} \leq a_0 \leq -\frac{2a_2^3 - 9a_1a_2a_3 - 2(a_2^2 - 3a_1a_3)^{3/2}}{27a_3^2},$$

and $a_0 < 0$. □

Lemma 7.10. *Let $g(x) := a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ be a real polynomial with $a_4 > 0$ such that its derivative only has real roots that are all positive. Define*

$$u_2 = \frac{8a_2a_4 - 3a_3^2}{16a_4^2},$$
$$u_3 = \frac{a_3^3 - 4a_2a_3a_4 + 8a_1a_4^2}{32a_4^3},$$
$$\zeta_3 = e^{\frac{2\pi i}{3}},$$
$$\eta = \left(-\frac{u_2^6}{27} - 5u_2^3u_3^2 + \frac{27}{2}u_3^4 + \frac{27|u_3|(u_3^2 + \frac{4}{27}u_2^3)^{3/2}}{2}\right)^{1/3}$$

and let S_η be the set

$$S_\eta := \left\{ \eta + \overline{\eta} + \frac{2u_2^2}{3}, \zeta_3 \eta + \zeta_3^2 \overline{\eta} + \frac{2u_2^2}{3}, \zeta_3^2 \eta + \zeta_3 \overline{\eta} + \frac{2u_2^2}{3} \right\}.$$

Observe that every element in S_η is real, since $\overline{\zeta_3^k \eta} = \zeta_3^{-k}\eta$ and $u_2 \in \mathbb{R}$. Let $\theta_1 \leq \theta_2 \leq \theta_3$ be the three elements in S_η ordered from least to greatest. Then every root of $g(x)$ is real and positive if and only if

$$\frac{3a_3^4}{256a_4^3} - \frac{a_3^2 a_2}{16a_4^2} + \frac{a_3 a_1}{4a_4} + a_4\theta_1 \leq a_0 \leq \frac{3a_3^4}{256a_4^3} - \frac{a_3^2 a_2}{16a_4^2} + \frac{a_3 a_1}{4a_4} + a_4\theta_2,$$

and $a_0 > 0$

Proof. Assume the derivative $g'(x) = 4a_4x^3 + 3a_3x^2 + 2a_2x + a_1$ only has real roots that are all positive. To obtain the roots of $g'(x)$, we will apply Cardano's method. Firstly, we make the substitution $f(y) = \frac{1}{4a_4} g'(y - \frac{a_3}{4a_4})$ to obtain the depressed cubic

$$f(y) = y^3 + u_2 y + u_3,$$

where

$$u_2 = \frac{8a_2a_4 - 3a_3^2}{16a_4^2},$$
$$u_3 = \frac{a_3^3 - 4a_2a_3a_4 + 8a_1a_4^2}{32a_4^3}.$$

Since by assumption the roots of $g'(x)$ are all real, we know that those of $f(y)$ are also all real. Hence, the discriminant $\Delta = u_3^2 + \frac{4}{27}u_2^3$ of f is non-positive and the roots of f are given by

$$S := \{\omega + \overline{\omega}, \zeta_3\omega + \zeta_3^2\overline{\omega}, \zeta_3^2\omega + \zeta_3\overline{\omega}\} \subseteq \mathbb{R},$$

where ζ_3 is a primitive third root of unity and $\omega = \left(\frac{-u_3 + \sqrt{\Delta}}{2}\right)^{1/3} \in \mathbb{C}$ is some third root. Note that no matter the choice of the third root you take, the set S will remain the same. Therefore, the roots of $g'(x)$ are given by

$$S' := \left\{ \omega + \overline{\omega} - \frac{a_3}{4a_4}, \zeta_3\omega + \zeta_3^2\overline{\omega} - \frac{a_3}{4a_4}, \zeta_3^2\omega + \zeta_3\overline{\omega} - \frac{a_3}{4a_4} \right\} \subseteq \mathbb{R}.$$

Suppose $\gamma_1 \geq \gamma_2 \geq \gamma_3$ are the three elements in S' ordered from least to greatest. In order for $g(x)$ to have only real roots, we must have

$$-\int_0^{\gamma_2} g'(t)dt \leq a_0 \leq -\max\left\{ \int_0^{\gamma_1} g'(t)dt, \int_0^{\gamma_3} g'(t)dt \right\},$$

by Lemma 7.1. Note that

$$-\max\left\{ \int_0^{\gamma_1} g'(t)dt, \int_0^{\gamma_3} g'(t)dt \right\} = \min\left\{ -\int_0^{\gamma_1} g'(t)dt, -\int_0^{\gamma_3} g'(t)dt \right\}.$$

As discussed in the proof of Lemma 7.1, assuming the roots are distinct, the primitives of $g'(x)$ (in particular $g(x)$) have a local maximum at $x = \gamma_2$ and local minima at $x = \gamma_1$ and $x = \gamma_3$. Therefore, the negative of the primitives of $g'(x)$ have a local minima at $x = \gamma_2$ and local maxima at $x = \gamma_1$ and $x = \gamma_3$. In the case in which some of the γ_i's are equal, we can describe the behaviour of the negative of the primitive analogously. Furthermore, since the negatives of the primitives have at most three distinct critical points, at most one of which is a local minimum, we automatically have that $\gamma_1 \geq \gamma_2 \geq \gamma_3$ implies

$$-\int_0^{\gamma_2} g'(t)dt \leq -\max\left\{ \int_0^{\gamma_1} g'(t)dt, \int_0^{\gamma_3} g'(t)dt \right\}.$$

Say $\gamma_i = \zeta_3^k\omega + \zeta_3^{-k}\overline{\omega} - \frac{a_3}{4a_4}$ for some k. A computation shows

$$\int_0^{\gamma_i} g'(t)dt = -\frac{3a_3^4}{256a_4^3} + \frac{a_3^2a_2}{16a_4^2} - \frac{a_3a_1}{4a_4} + a_4\left((\zeta_3^k\omega + \zeta_3^{-k}\overline{\omega})^4 + 2u_2(\zeta_3^k\omega + \zeta_3^{-k}\overline{\omega})^2 + 4u_3(\zeta_3^k\omega + \zeta_3^{-k}\overline{\omega})\right).$$

In particular, we find that the bounds for a_0 are

$$\frac{3a_3^4}{256a_4^3} - \frac{a_3^2a_2}{16a_4^2} + \frac{a_3a_1}{4a_4} + a_4\cdot\min_{0\le k\le 2}\left(-(\zeta_3^k\omega + \zeta_3^{-k}\overline{\omega})^4 - 2u_2(\zeta_3^k\omega + \zeta_3^{-k}\overline{\omega})^2 - 4u_3(\zeta_3^k\omega + \zeta_3^{-k}\overline{\omega})\right) \le a_0 \quad (7.3)$$

and

$$a_0 \le \frac{3a_3^4}{256a_4^3} - \frac{a_3^2a_2}{16a_4^2} + \frac{a_3a_1}{4a_4} + a_4\cdot\operatorname*{median}_{0\le k\le 2}\left(-(\zeta_3^k\omega + \zeta_3^{-k}\overline{\omega})^4 - 2u_2(\zeta_3^k\omega + \zeta_3^{-k}\overline{\omega})^2 - 4u_3(\zeta_3^k\omega + \zeta_3^{-k}\overline{\omega})\right). \quad (7.4)$$

We can further simplify the expression using the following observations:

$$\begin{aligned}(\zeta_3^k\omega)^3 &= \frac{-u_3+\sqrt{\Delta}}{2},\\ (\zeta_3^k\overline{\omega})^3 &= \frac{-u_3-\sqrt{\Delta}}{2},\\ \zeta_3^k\omega\cdot\zeta_3^{3-k}\overline{\omega} &= \left(\frac{u_3^2-\Delta}{4}\right)^{1/3} = \left(\frac{-\frac{4}{27}u_2^3}{4}\right)^{1/3} = -\frac{u_2}{3}.\end{aligned}$$

This gives us

$$\begin{aligned}2u_2(\zeta_3^k\omega + \zeta_3^{-k}\overline{\omega})^2 &= 2u_2(\zeta_3^{2k}\omega^2 + \zeta_3^{-2k}\overline{\omega}^2) - \frac{4u_2^2}{3}\\ &= -6\omega\overline{\omega}(\zeta_3^{2k}\omega^2 + \zeta_3^{-2k}\overline{\omega}^2) - \frac{4u_2^2}{3}\\ &= -6\left(\frac{-u_3+\sqrt{\Delta}}{2}\right)\zeta_3^{-k}\overline{\omega} - 6\left(\frac{-u_3-\sqrt{\Delta}}{2}\right)\zeta_3^k\omega - \frac{4u_2^2}{3}\\ &= 3u_3(\zeta_3^k\omega + \zeta_3^{-k}\overline{\omega}) + 3\sqrt{\Delta}(\zeta_3^k\omega - \zeta_3^{-k}\overline{\omega}) - \frac{4u_2^2}{3},\end{aligned}$$

and

$$(\zeta_3^k\omega + \zeta_3^{-k}\overline{\omega})^4 = -\frac{5u_3}{2}(\zeta_3^k\omega + \zeta_3^{-k}\overline{\omega}) - \frac{3\sqrt{\Delta}}{2}(\zeta_3^k\omega - \zeta_3^{-k}\overline{\omega}) + \frac{6u_2^2}{9}.$$

Hence,

$$\begin{aligned}(\zeta_3^k\omega + \zeta_3^{-k}\overline{\omega})^4 + 2u_2(\zeta_3^k\omega + \zeta_3^{-k}\overline{\omega})^2 + 4u_3(\zeta_3^k\omega + \zeta_3^{-k}\overline{\omega}) &= \frac{9u_3}{2}(\zeta_3^k\omega + \zeta_3^{-k}\overline{\omega}) + \frac{3\sqrt{\Delta}}{2}(\zeta_3^k\omega - \zeta_3^{-k}\overline{\omega}) - \frac{2u_2^2}{3}\\ &= \zeta_3^k\omega\left(\frac{9u_3}{2} + \frac{3\sqrt{\Delta}}{2}\right) + \zeta_3^{-k}\overline{\omega}\left(\frac{9u_3}{2} - \frac{3\sqrt{\Delta}}{2}\right) - \frac{2u_2^2}{3}.\end{aligned}$$

Observe that since $\Delta \le 0$, we have

$$\overline{\zeta_3^k\omega\left(\frac{9u_3}{2} + \frac{3\sqrt{\Delta}}{2}\right)} = \zeta_3^{-k}\overline{\omega}\left(\frac{9u_3}{2} - \frac{3\sqrt{\Delta}}{2}\right).$$

Computing and substituting $\Delta = u_3^2 + \frac{4}{27}u_2^3$ back gives us

$$\begin{aligned}\left(\frac{9u_3}{2} + \frac{3\sqrt{\Delta}}{2}\right)^3 \left(\frac{-u_3 + \sqrt{\Delta}}{2}\right) &= -\frac{729u_3^4}{16} + \frac{243u_3^2\Delta}{8} + \frac{27\Delta^2}{16} + \frac{27u_3\Delta^{3/2}}{2} \\ &= \frac{u_2^6}{27} + 5u_2^3u_3^2 - \frac{27}{2}u_3^4 + \frac{27u_3(u_3^2 + \frac{4}{27}u_2^3)^{3/2}}{2}.\end{aligned}$$

Define η to be

$$\eta := \left(-\frac{u_2^6}{27} - 5u_2^3u_3^2 + \frac{27}{2}u_3^4 + \frac{27|u_3|(u_3^2 + \frac{4}{27}u_2^3)^{3/2}}{2}\right)^{1/3},$$

and let S_η be the set

$$S_\eta := \left\{\eta + \overline{\eta} + \frac{2u_2^2}{3}, \zeta_3\eta + \zeta_3^2\overline{\eta} + \frac{2u_2^2}{3}, \zeta^2\eta + \zeta_3\overline{\eta} + \frac{2u_2^2}{3}\right\} \subseteq \mathbb{R}.$$

Note that the definition of the set S_η does not depend on the sign of u_3, since

$$\overline{\left(-\frac{u_2^6}{27} - 5u_2^3u_3^2 + \frac{27}{2}u_3^4 + \frac{27u_3(u_3^2 + \frac{4}{27}u_2^3)^{3/2}}{2}\right)^{1/3}} = \left(-\frac{u_2^6}{27} - 5u_2^3u_3^2 + \frac{27}{2}u_3^4 - \frac{27u_3(u_3^2 + \frac{4}{27}u_2^3)^{3/2}}{2}\right)^{1/3}.$$

Let $\theta_1 \leq \theta_2 \leq \theta_3$ be the three elements in S_η. Combining (7.3) and (7.4) we find the bounds

$$\frac{3a_3^4}{256a_4^3} - \frac{a_3^2a_2}{16a_4^2} + \frac{a_3a_1}{4a_4} + a_4\theta_1 \leq a_0 \leq \frac{3a_3^4}{256a_4^3} - \frac{a_3^2a_2}{16a_4^2} + \frac{a_3a_1}{4a_4} + a_4\theta_2.$$

□

Lemma 7.11. *Let $g(x) := x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ be a real polynomial such that the roots of its derivative are all real and positive. Define*

$$\begin{aligned}u_2 &= \frac{15a_3 - 6a_4^2}{50}, \\ u_3 &= \frac{4a_4^3 - 15a_3a_4 + 25a_2}{250}, \\ u_4 &= \frac{-3a_4^4 + 15a_4^2a_3 - 50a_4a_2 + 125a_1}{625}.\end{aligned}$$

If $u_3 = 0$, let x_{i_1,i_2} be

$$x_{i_1,i_2} = i_1\sqrt{-u_2 + i_2\sqrt{u_2^2 - u_4}},$$

for $i_1, i_2 \in \{+1, -1\}$. Otherwise, define

$$\begin{aligned}v_2 &= -\frac{u_2^2}{3} - u_4, \\ v_3 &= \frac{2u_2u_4}{3} - \frac{2u_2^3}{27} - 2u_3^2, \\ C &= \left(\frac{-v_3 + \sqrt{v_3^2 + \frac{4}{27}v_2^3}}{2}\right)^{1/3}, \\ y &= \begin{cases}\sqrt[3]{-v_3} - \frac{2u_2}{3} & \textit{if } v_2 = 0, \\ C - \frac{v_2}{3C} - \frac{2u_2}{3} & \textit{if } v_2 \neq 0,\end{cases}\end{aligned}$$

and let x_{i_1,i_2} for $i_1, i_2 \in \{+1, -1\}$ be defined by

$$x_{i_1,i_2} = \frac{i_1\sqrt{2y} + i_2\sqrt{-4u_2 - 2y - i_1\frac{8u_3}{\sqrt{2y}}}}{2},$$

in other words $x_{i_1,i_2} - \frac{a_4}{5}$ are the roots of the derivative $g'(x)$ of $g(x)$ and that by assumption, they are all real.
Let $\gamma_1 \geq \gamma_2 \geq \gamma_3 \geq \gamma_4$ be equal to x_{i_1,i_2} with each a distinct pair (i_1, i_2), so that they are ordered. Let $\tilde{g}(x)$ be the polynomial defined by

$$\tilde{g}(x) = -x^5 - \frac{10}{3}u_2x^3 - 10u_3x^2 - 5u_4x,$$

and define

$$\begin{aligned}\lambda_1 &= \max\{\tilde{g}(\gamma_2), \tilde{g}(\gamma_4)\},\\ \lambda_2 &= \min\{\tilde{g}(\gamma_1), \tilde{g}(\gamma_3)\}.\end{aligned}$$

Then every root of $g(x)$ is real and positive if and only if

$$-\frac{4a_4^5}{3125} + \frac{a_3a_4^3}{125} - \frac{a_2a_4^2}{25} + \frac{a_1a_4}{5} + \lambda_1 \leq a_0 \leq -\frac{4a_4^5}{3125} + \frac{a_3a_4^3}{125} - \frac{a_2a_4^2}{25} + \frac{a_1a_4}{5} + \lambda_2, \tag{7.5}$$

and $a_0 < 0$.

Proof. In order to determine the bounds on a_0, we need to determine the roots of $g'(x) = 5x^4 + 4a_4x^3 + 3a_3x^2 + 2a_2x + a_1$. Firstly, we make a substitution to obtain a depressed quartic

$$\frac{1}{5}g'\left(x - \frac{a_4}{5}\right) = x^4 + 2u_2x^2 + 4u_3x + u_4,$$

where

$$\begin{aligned}u_2 &= \frac{15a_3 - 6a_4^2}{50},\\ u_3 &= \frac{4a_4^3 - 15a_3a_4 + 25a_2}{250},\\ u_4 &= \frac{-3a_4^4 + 15a_4^2a_3 - 50a_4a_2 + 125a_1}{625}.\end{aligned}$$

First suppose $u_3 = 0$. Then, $x^4 + 2u_2x^2 + u_4 = 0$ has solutions

$$x_{i_1,i_2} = i_1\sqrt{\frac{-2u_2 + i_2\sqrt{4u_2^2 - 4u_4}}{2}} = i_1\sqrt{-u_2 + i_2\sqrt{u_2^2 - u_4}}, \tag{7.6}$$

where $i_1, i_2 \in \{+1, -1\}$. Hence, if $u_3 = 0$, then the roots of $g'(x)$ are

$$\left\{\pm\sqrt{-u_2 + \sqrt{u_2^2 - u_4}} - \frac{a_4}{5}, \pm\sqrt{-u_2 - \sqrt{u_2^2 - u_4}} - \frac{a_4}{5}\right\}.$$

Now suppose $u_3 \neq 0$. The equation $x^4 + 2u_2x^2 + 4u_3x + u_4 = 0$ is equivalent to

$$(x^2 + u_2)^2 = -4u_3x - u_4 + u_2^2.$$

This is equivalent to

$$(x^2 + u_2 + y)^2 = 2yx^2 - 4u_3x + y^2 + 2yu_2 + u_2^2 - u_4, \tag{7.7}$$

for any number y. Choose y such that the right-hand side of (7.7) is a square. In other words, y is chosen such that the discriminant of the quadratic polynomial in x on the right-hand side of (7.7) is zero, that is

$$16u_3^2 - 4 \cdot 2y \cdot (y^2 + 2yu_2 + u_2^2 - u_4) = 0.$$

Equivalently, y satisfies the equation $f(y) = 0$ with

$$f(y) = y^3 + 2u_2y^2 + (u_2^2 - u_4)y - 2u_3^2,$$

and y is non-zero due to the assumption that $u_3 \neq 0$. To solve the cubic, we first apply the substitution $f(y - \frac{2u_2}{3}) = h(y)$ to get a depressed cubic

$$h(y) = y^3 + v_2y + v_3,$$

where

$$\begin{aligned} v_2 &= -\frac{u_2^2}{3} - u_4, \\ v_3 &= \frac{2u_2u_4}{3} - \frac{2u_2^3}{27} - 2u_3^2. \end{aligned}$$

If $v_2 = 0$, then a solution to $y^3+v_3 = 0$ is simply $\sqrt[3]{-v_3}$. Hence, substituting backwards gives $f(\sqrt[3]{-v_3} - \frac{2u_2}{3}) = 0$. Else, a solution of $h(y) = 0$ is $y = C - \frac{v_2}{3C}$, where

$$C = \left(\frac{-v_3 + \sqrt{v_3^2 + \frac{4}{27}v_2^3}}{2} \right)^{1/3}$$

is some third root in $\mathbb{C}$. The choice of C does not matter. Hence, a solution of $f(y) = 0$ is $y = \sqrt[3]{-v_3} - \frac{2u_2}{3}$ if $v_2 = 0$ and $y = C - \frac{v_2}{3C} - \frac{2u_2}{3}$ if $v_2 \neq 0$, which in particular implies $C \neq 0$.

By assumption, we have that y is non-zero. Consider the expression

$$\left(x\sqrt{2y} - \frac{2u_3}{\sqrt{2y}} \right)^2 = 2yx^2 - 4u_3x + \frac{4u_3^2}{2y}.$$

We can substitute $f(y) = 0$ in $\frac{4u_3^2}{2y}$ and combine this with (7.7) to get

$$(x^2 + u_2 + y)^2 = \left(x\sqrt{2y} - \frac{2u_3}{\sqrt{2y}} \right)^2.$$

Hence,

$$\left(x^2 + u_2 + y + x\sqrt{2y} - \frac{2u_3}{\sqrt{2y}} \right) \left(x^2 + u_2 + y - x\sqrt{2y} + \frac{2u_3}{\sqrt{2y}} \right) = 0.$$

Therefore, by the quadratic formula, the solutions of $x^4 + 2u_2x^2 + 4u_3x + u_4 = 0$ are given by

$$x_{i_1,i_2} = \frac{i_1\sqrt{2y} + i_2\sqrt{-4u_2 - 2y - i_1\frac{8u_3}{\sqrt{2y}}}}{2}, \tag{7.8}$$

where $i_1, i_2 \in \{+1, -1\}$. It follows that if $u_3 \neq 0$ the roots of $g'(x)$ are given by

$$\left\{ \frac{\sqrt{2y} \pm \sqrt{-4u_2 - 2y - \frac{8u_3}{\sqrt{2y}}}}{2} - \frac{a_4}{5}, \frac{-\sqrt{2y} \pm \sqrt{-4u_2 - 2y + \frac{8u_3}{\sqrt{2y}}}}{2} - \frac{a_4}{5} \right\}.$$

Let $\gamma_1 \geq \gamma_2 \geq \gamma_3 \geq \gamma_4$ be equal to x_{i_1,i_2} with each a distinct pair (i_1, i_2), where x_{i_1,i_2} is as in (7.6) or (7.8) if $u_3 = 0$ respectively $u_3 \neq 0$. The bounds of a_0 are

$$-\min\left\{\int_0^{\gamma_1+\frac{a_4}{5}} g'(t)dt, \int_0^{\gamma_3+\frac{a_4}{5}} g'(t)dt\right\} \leq a_0 \leq -\max\left\{\int_0^{\gamma_2+\frac{a_4}{5}} g'(t)dt, \int_0^{\gamma_4+\frac{a_4}{5}} g'(t)dt\right\},$$

by Lemma 7.1. Equivalently,

$$\max\left\{-\int_0^{\gamma_1+\frac{a_4}{5}} g'(t)dt, -\int_0^{\gamma_3+\frac{a_4}{5}} g'(t)dt\right\} \leq a_0 \leq \min\left\{-\int_0^{\gamma_2+\frac{a_4}{5}} g'(t)dt, -\int_0^{\gamma_4+\frac{a_4}{5}} g'(t)dt\right\}. \tag{7.9}$$

As discussed in the proof of Lemma 7.1, assuming the roots are distinct, the primitives of $g'(x)$ (in particular $g(x)$) have a local maximum at $x = \gamma_2 + \frac{a_4}{5}$ and $x = \gamma_4 + \frac{a_4}{5}$, and a local minimum at $x = \gamma_1 + \frac{a_4}{5}$ and $x = \gamma_3 + \frac{a_4}{5}$. Therefore, the negative of the primitives of $g'(x)$ have a local minimum at $x = \gamma_2 + \frac{a_4}{5}$ and $x = \gamma_4 + \frac{a_4}{5}$, and a local maximum at $x = \gamma_1 + \frac{a_4}{5}$ and $x = \gamma_3 + \frac{a_4}{5}$. In the case in which some of the γ_i's are equal, we can describe the behaviour of the negative of the primitive analogously. Note that since the primitives can have multiple local minima and local maxima, it may happen that the value of the primitive at a local minimum is higher than at one of the local maxima, in which case no value of a_0 suffices the bounds in (7.5), see Example 7.13.
A computation shows that for $1 \leq j \leq 4$

$$\int_0^{\gamma_j+\frac{a_4}{5}} g'(t)dt = \frac{4a_4^5}{3125} - \frac{a_3a_4^3}{125} + \frac{a_2a_4^2}{25} - \frac{a_1a_4}{5} + \gamma_j^5 + \frac{10}{3}u_2\gamma_j^3 + 10u_3\gamma_j^2 + 5u_4\gamma_j. \tag{7.10}$$

Let $\tilde{g}(x) = -x^5 - \frac{10}{3}u_2x^3 - 10u_3x^2 - 5u_4x$. Observe that

$$-\min\left\{\int_0^{\gamma_1+\frac{a_4}{5}} g'(t)dt, \int_0^{\gamma_3+\frac{a_4}{5}} g'(t)dt\right\} \leq -\max\left\{\int_0^{\gamma_2+\frac{a_4}{5}} g'(t)dt, \int_0^{\gamma_4+\frac{a_4}{5}} g'(t)dt\right\},$$

is equivalent to

$$\lambda_1 := \max_{i=2,4} \tilde{g}(\gamma_i) \leq \min_{j=1,3} \tilde{g}(\gamma_j) =: \lambda_2.$$

Hence, by (7.9) and (7.10), every root of $g(x)$ is real and positive if and only if

$$-\frac{4a_4^5}{3125} + \frac{a_3a_4^3}{125} - \frac{a_2a_4^2}{25} + \frac{a_1a_4}{5} + \lambda_1 \leq a_0 \leq -\frac{4a_4^5}{3125} + \frac{a_3a_4^3}{125} - \frac{a_2a_4^2}{25} + \frac{a_1a_4}{5} + \lambda_2.$$

□

Remark 7.12. Note that y satisfies a degree 3 polynomial, which always has a real root. Also, note that $\Delta = v_3^2 + \frac{4}{27}v_2^3$ is (a multiple of) the discriminant of $h(y)$. The discriminant is positive if and only if $h(y)$ has one real root and two complex roots, which in this case gives $C \in \mathbb{R}$. Hence, $\frac{v_2}{3C} \in \mathbb{R}$, which leads to $y \in \mathbb{R}$. Clearly, C is also real if $\Delta = 0$. Furthermore, $\Delta < 0$ happens if and only if $h(y)$ has three real roots. In this case, one can compute $-\frac{v_2}{3C} = \overline{C}$. We know from Cardano's method that $y = C + \overline{C}$ is a root of $h(y)$. Thus, our construction always gives $y \in \mathbb{R}$.

Example 7.13. Let $g(x) = \frac{x^5}{5} - 3x^4 + \frac{49}{3}x^3 - 39x^2 + 40x - 15$. Its graph is given in Figure 4. The derivative of $g(x)$ is given by $g'(x) = (x-1)(x-2)(x-4)(x-5)$. Despite every root of the derivative of $g(x)$ being real and positive and $g(x)$ satisfying the Descartes' rule of sign change, there is no value $c \in \mathbb{R}$ for which every root of $g(x) - c$ is real and positive. This is because $g(x)$ attains a higher value at the local minimum at $x = 5$ than at the local maximum $x = 1$. Using the same notation as in Lemma 7.11, this would correspond to the case where $\lambda_1 > \lambda_2$.

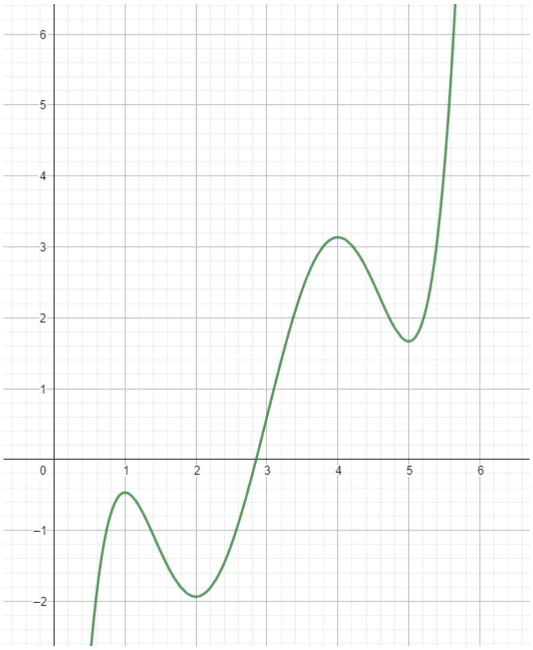


Figure 4: Graph of $g(x) = \frac{x^5}{5} - 3x^4 + \frac{49}{3}x^3 - 39x^2 + 40x - 15$

8 Dimension 3

For abelian varieties over any finite field $\mathbb{F}_q$ of dimension 3, the bounds for the coefficients of q-Weil polynomials of degree 6 has been computed by Haloui [6, Theorem 1.1]. In the same article, Haloui also determined the conditions for which a q-Weil polynomial of degree 6 is irreducible and the conditions for which irreducible q-Weil polynomial of degree 6 is the characteristic polynomial of a simple abelian variety of dimension 3. Xing [28, Proposition 2] determined when the cube of a quadratic polynomial is the characteristic polynomial of an abelian variety over $\mathbb{F}_q$ of dimension 3. This statement has been later generalised by Hayashida for arbitrary dimensions, see Theorem 6.3. These results combined give a complete classification for simple abelian varieties of degree 3. However, according to some contributors of the LMFDB [3, Chapter 3.1], the explicit description of the space of q-Weil polynomials of degree 6 by Haloui was missing some non-simple examples. After computing them myself, the missing q-Weil polynomials seem to be the ones with real roots arising from the case when q is a square. This chapter will serve as a summary and correction of the results stated by Haloui.

8.1 Weil polynomials of degree 6

Suppose we have a polynomial of the form

$$P(x) = x^6 + a_1x^5 + a_2x^4 + a_3x^3 + qa_2x^2 + q^2a_1x + q^3, \tag{8.1}$$

for some $a_1, a_2, a_3 \in \mathbb{Z}$. We want to consider the conditions for which $P(x)$ is a q-Weil polynomial. For this, we will first cover the cases where $P(x)$ has a real root and afterwards cover the case where $P(x)$ has no real roots. Recall from Corollary 4.8 that the real roots of the characteristic polynomial of an abelian variety must have even multiplicity. With a similar proof as the corollary due to the assumption of the constant coefficient of (8.1), we can conclude that real roots of $P(x)$ have even multiplicity.

8.1.1 Real root

Suppose $P(x)$ has a real root, so at $x = \pm\sqrt{q}$. If $P(x)$ has a root at both $x = \sqrt{q}$ and $x = -\sqrt{q}$ with the same multiplicities, then as the multiplicities at real roots of q-Weil polynomials have to be even, we get

$$P(x) = (x^2 - q)^2(x^2 - (\alpha + \overline{\alpha})x + q).$$

with α a complex root of $P(x)$ with $|\alpha| = \sqrt{q}$, so $|\alpha + \overline{\alpha}| < 2\sqrt{q}$. Then in particular, we determine that $\alpha + \overline{\alpha} \in \mathbb{Z}$ by comparing the coefficient of x^5, as $P(x)$ has integer coefficients.

In the case where $P(x)$ has a root at both $x = \sqrt{q}$ and $x = -\sqrt{q}$, but their multiplicities differ, we must have

$$P(x) = (x + \sqrt{q})^4(x - \sqrt{q})^2 = (x^2 - q)^2(x + \sqrt{q})^2 \quad \text{or} \quad P(x) = (x + \sqrt{q})^2(x - \sqrt{q})^4 = (x^2 - q)^2(x - \sqrt{q})^2,$$

which results in a polynomial with coefficients in $\mathbb{Z}[\sqrt{q}]$. Hence, $P(x)$ can be of this form only if $\sqrt{q} \in \mathbb{Z}$.

Now suppose $P(x)$ has a root at $x = -\sqrt{q}$ of multiplicity 4 but no root at $x = \sqrt{q}$. Then,

$$P(x) = (x + \sqrt{q})^4(x^2 - (\alpha + \overline{\alpha})x + q),$$

where $|\alpha| = \sqrt{q}$ and $P(\alpha) = 0$ a complex root, so $|\alpha + \overline{\alpha}| < 2\sqrt{q}$. As $P(x)$ is a polynomial with integer coefficients, we find by comparing the coefficients that

$$\begin{aligned} -(\alpha + \overline{\alpha}) + 4\sqrt{q}&, \\ 7q - 4(\alpha + \overline{\alpha})\sqrt{q}&, \quad \in \mathbb{Z} \\ -6q(\alpha + \overline{\alpha}) + 8q\sqrt{q}&. \end{aligned}$$

In particular, combining the first and the third restriction, we see again that $P(x)$ can have this form only if $\sqrt{q} \in \mathbb{Z}$, so that subsequently also $\alpha + \overline{\alpha} \in \mathbb{Z}$. The case with $x = \sqrt{q}$ instead of $x = -\sqrt{q}$ works analogously.

Lastly, if $P(x)$ has a root at $x = -\sqrt{q}$ of multiplicity 2 but not a root at $x = \sqrt{q}$, we have

$$P(x) = (x + \sqrt{q})^2(x^2 - (\alpha_1 + \overline{\alpha_1})x + q)(x^2 - (\alpha_2 + \overline{\alpha_2})x + q),$$

with α_1, α_2 complex roots of P of absolute value $\sqrt{q}$, so that $|\alpha_i + \overline{\alpha_i}| < 2\sqrt{q}$. Again comparing coefficients gives

$$\left.\begin{aligned} 2\sqrt{q} - (\alpha_1 + \overline{\alpha_1}) - (\alpha_2 + \overline{\alpha_2}), \\ -2(\alpha_1 + \overline{\alpha_1})\sqrt{q} - 2(\alpha_2 + \overline{\alpha_2})\sqrt{q} + (\alpha_1 + \overline{\alpha_1})(\alpha_2 + \overline{\alpha_2}), \\ 2(\alpha_1 + \overline{\alpha_1})(\alpha_2 + \overline{\alpha_2})\sqrt{q} - 2q(\alpha_1 + \overline{\alpha_1}) - 2q(\alpha_2 + \overline{\alpha_2}) + 4q\sqrt{q}. \end{aligned}\right. \quad \in \mathbb{Z}$$

Substituting $r = (\alpha_1 + \overline{\alpha_1}) + (\alpha_2 + \overline{\alpha_2})$ in the first restriction gives us an expression for $s = (\alpha_1 + \overline{\alpha_1})(\alpha_2 + \overline{\alpha_2})$ in terms of integers, $\sqrt{q}$ and r using the second restriction. Then combining this with the third restriction tells us that $\sqrt{q} \in \mathbb{Z}$. Then looking at the first two again, we see that both r and s must be integers.

8.1.2 No real roots

Now suppose $P(x)$ has no real roots. We will use Proposition 6.1 and apply the results from Lemma 7.1 to it. We may write

$$P(x) = \prod_{i=1}^{3}(x^2 + \omega_i x + q), \tag{8.2}$$

for some $\omega_1, \omega_2, \omega_3 \in \mathbb{C}$. The polynomial $P(x)$ is a q-Weil polynomial if and only if the polynomials

$$P^+(x) = \prod_{i=1}^{3}(x - (2\sqrt{q} + \omega_i)), \tag{8.3}$$

$$P^-(x) = \prod_{i=1}^{3}(x - (2\sqrt{q} - \omega_i)), \tag{8.4}$$

have only positive real roots.

Therefore, to determine conditions for which $P(x)$ is a q-Weil polynomial with only complex roots, we can simply determine the conditions for which $P^+(x)$ and $P^-(x)$ have only real positive roots and substitute the result to get conditions on the coefficients $P(x)$.

Let $P(x)$, $P^+(x)$ and $P^-(x)$ be polynomials as in (8.2), (8.3) and (8.4), expanded to

$$\begin{aligned} P(x) &= x^6 + a_1x^5 + a_2x^4 + a_3x^3 + qa_2x^2 + q^2a_1x + q^3, \\ P^+(x) &= x^3 + b_1^+x^2 + b_2^+x + b_3^+, \\ P^-(x) &= x^3 + b_1^-x^2 + b_2^-x + b_3^-. \end{aligned}$$

We can write the coefficients at each power of x in terms of the symmetric polynomials in ω_1, ω_2 and ω_3,

$$\begin{aligned} s_1 &= \omega_1 + \omega_2 + \omega_3, \\ s_2 &= \omega_1\omega_2 + \omega_2\omega_3 + \omega_1\omega_3, \\ s_3 &= \omega_1\omega_2\omega_3. \end{aligned}$$

Expanding (8.2) gives

$$\begin{aligned} a_1 &= s_1, \\ a_2 &= s_2 + 3q, \\ a_3 &= s_3 + 2qs_1. \end{aligned}$$

Hence, the symmetric polynomials in terms of a_1, a_2 and a_3 are

$$\begin{aligned} s_1 &= a_1, \\ s_2 &= a_2 - 3q, \\ s_3 &= a_3 - 2qa_1. \end{aligned}$$

Expanding (8.3) and (8.4) gives

$$\begin{aligned} b_1^+ &= -s_1 - 6\sqrt{q}, & b_1^- &= s_1 - 6\sqrt{q}, \\ b_2^+ &= s_2 + 4\sqrt{q}s_1 + 12q, & b_2^- &= s_2 - 4\sqrt{q}s_1 + 12q, \\ b_3^+ &= -s_3 - 2\sqrt{q}s_2 - 4qs_1 - 8q\sqrt{q}, & b_3^+ &= s_3 - 2\sqrt{q}s_2 + 4qs_1 + -8q\sqrt{q}. \end{aligned}$$

We can apply substitution so that the coefficients b_1^+, b_2^+, b_3^+ and b_1^-, b_2^-, b_3^- are in terms of a_1, a_2 and a_3,

$$\begin{aligned} b_1^+ &= -a_1 - 6\sqrt{q}, & b_1^- &= a_1 - 6\sqrt{q}, \\ b_2^+ &= a_2 + 4\sqrt{q}a_1 + 9q, & b_2^- &= a_2 - 4\sqrt{q}a_1 + 9q, \\ b_3^+ &= -a_3 - 2\sqrt{q}a_2 - 2qa_1 - 2q\sqrt{q}, & b_3^+ &= a_3 - 2\sqrt{q}a_2 + 2qa_1 - 2q\sqrt{q}. \end{aligned}$$

Lemma 8.1. *Let $h(x) = x^3 + r_1x^2 + r_2x + r_3$ be a monic polynomial of degree 3 with real coefficients. Then $h(x)$ has only real positive roots if and only if the following conditions hold:*

1. $r_1 < 0$,
2. $0 < r_2 \leq \frac{r_1^2}{3}$,
3. $\frac{r_1r_2}{3} - \frac{2r_1^3}{27} - \frac{2}{27}(r_1^2 - 3r_2)^{3/2} \leq r_3 \leq \frac{r_1r_2}{3} - \frac{2r_1^3}{27} + \frac{2}{27}(r_1^2 - 3r_2)^{3/2}$,
4. $r_3 < 0$.

Proof. Consider the derivatives of $h(x)$:

$$\begin{aligned} h'(x) &= 3x^2 + 2r_1x + r_2, \\ h''(x) &= 6x + 2r_1. \end{aligned}$$

The bound for r_1 follows from Descartes' rule of sign change. For the other bounds, we can apply Lemma 7.8 to $h'(x)$ to get the bounds for r_2 and afterwards Lemma 7.9 to $h(x)$ for r_3 to get the desired result. □

Now we can apply Lemma 8.1 to $b_1^+, b_1^-, b_2^+, b_2^-, b_3^+, b_3^-$ to get specific bounds for a_1, a_2, a_3.

Clearly $b_1^+, b_1^- < 0$ implies that $|a_1| < 6\sqrt{q}$. The second part of Lemma 8.1 gives

$$0 < 9q + a_2 + 4\sqrt{q}a_1 \leq \frac{(-6\sqrt{q} - a_1)^2}{3} \quad \text{and} \quad 0 < 9q + a_2 - 4\sqrt{q}a_1 \leq \frac{(-6\sqrt{q} + a_1)^2}{3}.$$

After a computation, we get

$$-9q + 4\sqrt{q}|a_1| < a_2 \leq 3q + \frac{a_1^2}{3}.$$

Lastly, for a_3, in both cases of the non-strict bounds for the third coefficient (b_3^+ and b_3^-) we obtain

$$-\frac{2a_1^3}{27} + \frac{a_1a_2}{3} + qa_1 - \frac{2}{27}(a_1^2 - 3a_2 + 9q)^{3/2} \leq a_3 \leq -\frac{2a_1^3}{27} + \frac{a_1a_2}{3} + qa_1 + \frac{2}{27}(a_1^2 - 3a_2 + 9q)^{3/2}.$$

The conditions $b_3^+, b_3^- < 0$ give

$$-2qa_1 - 2\sqrt{q}a_2 - 2q\sqrt{q} < a_3 < -2qa_1 + 2\sqrt{q}a_2 + 2q\sqrt{q}.$$

In short, we obtain the following theorem.

Theorem 8.2. *Let $P(x) = x^6 + a_1x^5 + a_2x^4 + a_3x^3 + a_2qx^2 + a_1q^2x + q^3$ be a polynomial with integer coefficients. The polynomial $P(x)$ is a q-Weil polynomial if and only if one of the following conditions hold:*

1. *q is a square and $P(x) = (x + \sqrt{q})^{2k}(x - \sqrt{q})^{2\ell}h(x)$, where $1 \leq k + \ell \leq 3$ and*

$$h(x) = \begin{cases} 1 & \text{if } k+\ell = 3, \\ x^2 + \omega x + q & \text{if } 1 < k+\ell < 3, \text{ where } \omega \in \mathbb{Z} \text{ and } |\omega| < 2\sqrt{q}, \\ (x^2 + \omega_1 x + q)(x^2 + \omega_2 x + q) & \text{if } k+\ell = 1, \text{ where } |\omega_1|, |\omega_2| < 2\sqrt{q} \text{ and } \omega_1 \cdot \omega_2, \omega_1 + \omega_2 \in \mathbb{Z} \end{cases}$$

2. *q is not a square and $P(x) = (x^2 - q)^2(x^2 + \omega x + q)$, where $\omega \in \mathbb{Z}$ and $|\omega| < 2\sqrt{q}$;*
3. *the following conditions hold:*
   - *(a) $|a_1| < 6\sqrt{q}$,*
   - *(b) $4\sqrt{q}|a_1| < a_2 \leq \frac{a_1^2}{3} + 3q$,*
   - *(c) $-\frac{2a_1^3}{27} + \frac{a_1a_2}{3} + qa_1 - \frac{2}{27}(a_1^2 - 3a_2 + 9q)^{3/2} \leq a_3 \leq -\frac{2a_1^3}{27} + \frac{a_1a_2}{3} + qa_1 + \frac{2}{27}(a_1^2 - 3a_2 + 9q)^{3/2}$,*
   - *(d) $-2qa_1 - 2\sqrt{q}a_2 - 2q\sqrt{q} < a_3 < -2qa_1 + 2\sqrt{q}a_2 + 2q\sqrt{q}$.*

Remark 8.3. One could simplify the first condition by saying that $h(x)$ must be a q-Weil polynomial of degree 2 if $1 < k + \ell < 3$ or of degree 4 if $k + \ell = 3$. See [14, Lemma 2.1] for the bounds of the coefficients of q-Weil polynomials of degree 4.
Comparing this result to [6, Theorem 1.1], the polynomials of the first case, where q is a square, is omitted in Haloui's paper, while the other statements are identical. After implementing the bounds in SageMath 9.3 [13] and comparing the result to built-in function in SageMath by Kedlaya [11], this indeed seems to be the case.

8.2 Irreducibility

Since Theorem 6.3 describes the q-Weil polynomials of the form $(x^2+\omega x+q)^3$ completely, the only remaining q-Weil polynomials of degree 6 corresponding to simple abelian varieties of dimension 3 are the irreducible q-Weil polynomials, see Example 6.4. We will determine when a given q-Weil polynomial of degree 6 is irreducible, which will be very similar to what is done by Haloui in [6, Chapter 3].

Let $P(x) = \prod_{i=1}^{g}(x^2 + \omega_i x + q)$ be a q-Weil polynomial, that is, $|\omega_i| \leq 2\sqrt{q}$. Define $f_P(x) = \prod_{i=1}^{g}(x + \omega_i)$. We can find conditions for irreducibility of $P(x)$ by determining the conditions for irreducibility of $f(x)$. First note that the coefficients of $f_P(x)$ are the symmetric polynomials $s_1, s_2, \ldots, s_g$ in $\omega_1, \ldots, \omega_g$. Since $P(x)$ has coefficients in $\mathbb{Z}$, we get that $s_1 \in \mathbb{Z}$ since it is the coefficient of x^{2g-1}. Similarly, $s_2 + gq$ is the coefficient of x^{2g-2} and so $s_2 \in \mathbb{Z}$. Inductively, one can determine that all symmetric polynomials in ω_i result in integers by looking at the coefficients of $P(x)$, which is a Weil polynomial and hence has integer coefficients.

Lemma 8.4. *Let $g \geq 2$ and $P(x)$ be a q-Weil polynomial of degree $2g$. If $\sqrt{q} \notin \mathbb{Z}$, then assume that $P(x) \neq (x - \sqrt{q})^2(x + \sqrt{q})^2$. The polynomial $P(x)$ is irreducible over $\mathbb{Q}$ if and only if $f_P(x)$ is irreducible over $\mathbb{Q}$.*

Proof. If $f_P(x)$ is reducible, we can assume without loss of generality by reordering that for some $1 \leq m \leq g-1$ we can factor f_P in $\mathbb{Q}[x]$ as

$$f_P(x) = \left(\prod_{i=1}^{m}(x + \omega_i)\right)\left(\prod_{j=m+1}^{g}(x + \omega_j)\right).$$

Since $f_P(x)$ is a monic polynomial with integer coefficients, the factors also have integer coefficients. In particular, the factors of $P(x)$ with integer coefficients are

$$P(x) = \left(\prod_{i=1}^{m}(x^2 + \omega_i x + q)\right)\left(\prod_{j=m+1}^{g}(x^2 + \omega_j x + q)\right).$$

Clearly, if $P(x)$ is reducible, then its factors are also q-Weil polynomials, say $P(x) = (x-\sqrt{q})^{2k}(x+\sqrt{q})^{2\ell}h(x)$, where $h(x)$ is a q-Weil polynomial without real roots. If $k \neq \ell$, or $k = \ell > 0$ and $h(x) \neq 1$, then since $P(x) \in \mathbb{Z}[x]$, we must have $\sqrt{q} \in \mathbb{Z}$. This means that in this case $f_P(x)$ can be factored into

$$f_P(x) = (x - 2\sqrt{q})^k(x + 2\sqrt{q})^\ell f_h(x).$$

If $k = \ell > 1$ and $h(x) = 1$, we can decompose

$$f_P(x) = (x^2 - 4q)(x^2 - 4q)^{k-1}.$$

Lastly, if $k = \ell = 0$, then by assumption $h(x)$ is reducible, say

$$h(x) = \left(\prod_{i=1}^{m}(x^2 + \omega_i x + q)\right)\left(\prod_{j=m+1}^{g}(x + \omega_j x + q)\right).$$

for some k. Inductively, one can deduce that the symmetric polynomials in $\omega_1, \ldots, \omega_m$ are integers. Similarly, the symmetric polynomials in $\omega_{m+1}, \ldots, \omega_g$ are integers as well. Hence, $f_h(x)$ factors into

$$\left(\prod_{i=1}^{m}(x + \omega_i)\right)\left(\prod_{j=m+1}^{g}(x + \omega_j)\right).$$

□

Haloui uses Cardano's method to determine the conditions for which $f_P(x)$ is irreducible. That is, the author makes a substitution to end up with a polynomial $F_P(x) = x^3 + rx + s$. Note that we can express $f_P(x)$ in terms of the coefficients of $P(x)$ as

$$f_P(x) = x^3 + a_1x^2 + (a_2 - 3q)x + (a_3 - 2qa_1)$$

using the symmetric functions in $\omega_1, \omega_2, \omega_3$ and the same substitutions we made in the previous section. Then, we end up with $f_P(x) = F_P(x + a_1/3)$ and clearly $f_P(x)$ has a root in $\mathbb{Q}$ if and only if $F_P(x)$ has. In other words, $f_P(x)$ is irreducible over $\mathbb{Q}$ if and only if $F_P(x)$ is. Explicitly, one can compute

$$r = -\frac{a_1^2}{3} + a_2 - 3q \quad \text{and} \quad s = \frac{2a_1^3}{27} - \frac{a_1a_2}{3} - qa_1 + a_3.$$

The discriminant Δ of $F_P(x)$ is equal to (a multiple of)

$$\Delta = s^2 + \frac{4}{27}r^3.$$

Note that due to the bounds we have on a_1, a_2, a_3, one can compute that

$$r \leq 0 \quad \text{and} \quad s^2 \leq -\frac{4}{27}r^3.$$

Hence, we always have $\Delta \leq 0$. Moreover, $\Delta = 0$ if and only if $F_P(x)$ has a root of multiplicity at least 2. If $r = 0$, then also $s = 0$, so then $F_P(x)$ has a triple root at $x = 0$. If $r \neq 0$, then its roots are $-\frac{3s}{r}$ and $\frac{3s}{2r}$, where the latter is a double root. In particular, the roots of $F_P(x)$ are in these cases in $\mathbb{Q}$, so that it is reducible over $\mathbb{Q}$.

If $\Delta < 0$, then all roots are distinct and real. Set $u = \frac{-s+\sqrt{\Delta}}{2}$. By Cardano's formula, the roots of $F_P(x)$ are of the form $v + \overline{v}$, where v is a cube root of u. If $v \in \mathbb{Q}(\sqrt{\Delta})$, then clearly $v + \overline{v} \in \mathbb{Q}$, so then $F_P(x)$ is reducible over $\mathbb{Q}$. Conversely, if $F_P(x)$ is reducible over $\mathbb{Q}$, meaning it has a root in $\mathbb{Q}$, then u has a cube root $v = a + bi$ with $a \in \mathbb{Q}$, as $v + \overline{v} = 2a \in \mathbb{Q}$. A computation shows

$$-\frac{s}{2} + i\frac{\sqrt{-\Delta}}{2} = u = v^3 = (a^3 - 3ab^2) + ib(3a^2 - b^2).$$

Suppose $a = 0$, then by comparing the real part on both sides of the equation, we must have that $s = 0$. In particular, $\Delta = \frac{4}{27}r^3 = (\frac{2}{3}r)^2\frac{r}{3}$ and so $u = (\sqrt{\frac{r}{3}})^3$, so u is a cube in $\mathbb{Q}(\Delta) = \mathbb{Q}(\sqrt{\frac{r}{3}})$. In the case where $a \neq 0$, again identifying the real parts on both sides, we determine that $b^2 \in \mathbb{Q}$. Using the imaginary parts, it follows that $b \in \mathbb{Q}(\sqrt{-\Delta})$, so that $v \in \mathbb{Q}(\sqrt{\Delta})$.

In conclusion, we get the following proposition:

Proposition 8.5. *Let $P(x) = x^6 + a_1x^5 + a_2x^4 + a_3x^3 + a_2qx^2 + a_1q^2x + q^3$ be a q-Weil polynomial. Set*

$$r = -\frac{a_1^2}{3} + a_2 - 3q \quad \text{and} \quad s = \frac{2a_1^3}{27} - \frac{a_1a_2}{3} - qa_1 + a_3$$

and define

$$\Delta = s^2 + \frac{4}{27}r^3 \quad \text{and} \quad u = \frac{-s + \sqrt{\Delta}}{2}.$$

Then $P(x)$ is irreducible over $\mathbb{Q}$ if and only if $\Delta \neq 0$ and u is not a cube in $\mathbb{Q}(\sqrt{\Delta})$.

8.3 Newton polygons

In order to determine conditions for which an irreducible q-Weil polynomial of degree 6 is the characteristic polynomial of a simple abelian variety of dimension 3, we consider the possible Newton polygons. These Newton polygons were first determined by Haloui [6].
The Newton polygons must satisfy the conditions stated in Corollary 6.8. Namely, the vertices must be in the lattice $\mathbb{Z} \times n\mathbb{Z}$ with initial point $(0, 3n)$ and endpoint $(6, 0)$. Furthermore, if the Newton polygon has an edge with slope $-\lambda$, then it has another edge with slope $-(n - \lambda)$ of the same horizontal length. The possible Newton polygons are shown in Figure 5.

This leads to the following classification by Haloui [6, Theorem 1.4], when combined with Theorem 6.3, which was first determined by Xing [28, Proposition 2] for dimension 3 specifically.

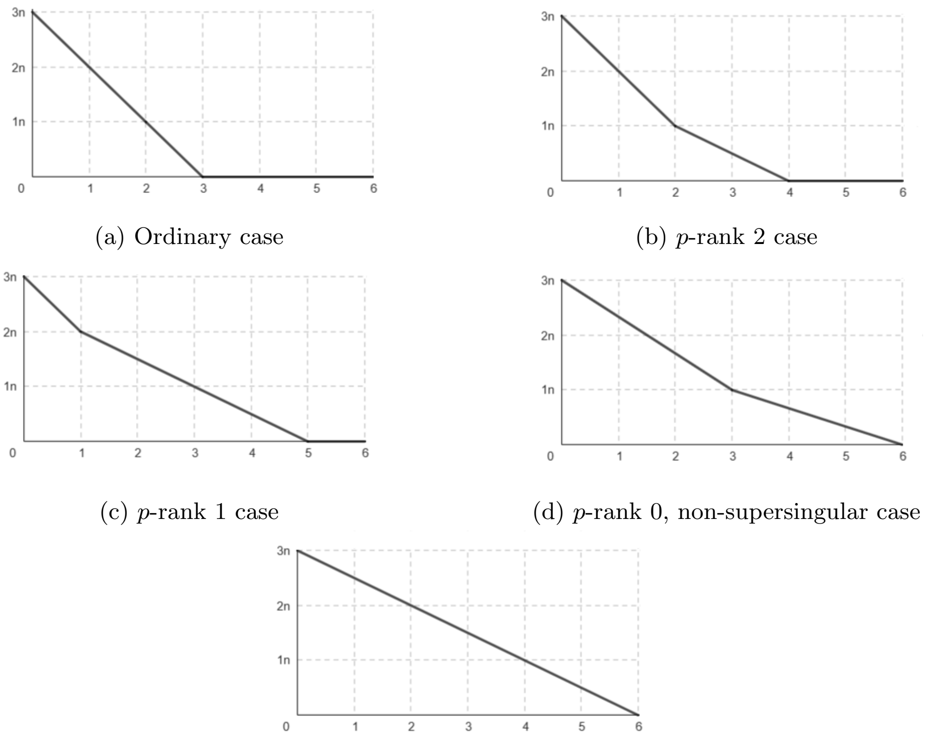
Theorem 8.6. *Let $P(x) = x^6 + a_1x^5 + a_2x^4 + a_3x^3 + a_2qx^3 + a_1q^2x + q^3$ be a q-Weil polynomial with $q = p^n$. Then $P(x)$ is the characteristic polynomial of a simple abelian variety of dimension 3 if and only if one of the following conditions holds:*

1. *n is a multiple of 3 and $P(x) = (x^2 + \omega x + q)^3$, where $|\omega| < 2\sqrt{q}$ and $\omega = kq^{1/3}$ with $k \in \mathbb{Z}$ not divisible by p,*
2. *the polynomial $P(x)$ is irreducible over $\mathbb{Q}$ and one of the following conditions holds:*
   - *(a) $v_p(a_3) = 0$,*
   - *(b) $v_p(a_3) \geq n/2, v_p(a_2) = 0$ and $P(x)$ has no root of valuation $n/2$ in $\mathbb{Q}_p$,*
   - *(c) $v_p(a_3) \geq n, v_p(a_2) \geq n/2, v_p(a_1) = 0$ and $P(x)$ has no root of valuation $n/2$ in $\mathbb{Q}_p$,*
   - *(d) $v_p(a_3) = n, v_p(a_2) \geq 2n/3, v_p(a_1) \geq n/3$ and $P(x)$ has no root $\mathbb{Q}_p$,*
   - *(e) $v_p(a_3) \geq 3n/2, v_p(a_2) \geq n, v_p(a_1) \geq n/2$ and $P(x)$ has no root nor a factor of degree 3 in $\mathbb{Q}_p$.*

The p-rank of abelian varieties in case (1) *is* 0*, while the p-ranks of abelian varieties in cases* (2a), (2b), (2c), (2d) *and* (2e) *are respectively* 3, 2, 1, 0 *and* 0*. Furthermore, the abelian varieties in case* (2e) *are supersingular.*

Proof. For case (1), we have that ω is divisible by p. This means that the $\pmod p$-reduced polynomials in this case are simply x^6. By Theorem 6.11, it follows that the p-rank of abelian varieties in this case is 0.

For the irreducible case, the conditions regarding the valuations of the coefficients follow immediately from their respective Newton polygons, since $v_p(a_3), v_p(a_2)$ and $v_p(a_1)$ correspond to the values at 3, 4 and 5 of the x-axis respectively, see Figure 5. The p-ranks also follow from the Newton polygons and Corollary 6.12.



(a) Ordinary case

(b) p-rank 2 case

(c) p-rank 1 case

(d) p-rank 0, non-supersingular case

(e) Supersingular case

Figure 5: Newton polygons of characteristic polynomials of simple abelian varieties of dimension 3. See [6].

The lattice points at $x = 3, 4, 5$ that are below the line between $(0, 3n)$ and $(6, 0)$ are $(3, 0)$, $(3, 1)$, $(4, 0)$ and $(5, 0)$, each determining a unique Newton polygon.

Suppose $(3, 0)$ is a vertex giving a p-rank of 3, which is equal to the dimension, see Figure 5a. This is called the ordinary case. We determine from the corresponding Newton polygon that the q-Weil polynomial factors into two polynomials in $\mathbb{Q}_p$, as there are two lines. Since these lines only pass lattice points at each integer value of the x-axis, anything regarding the reducibility of these two factors is allowed.

Now suppose $(4, 0)$ is the first vertex on the x-axis, corresponding to a p-rank of 2, see Figure 5b. In this case, we see that the Newton polygon has an edge that goes through $(3, n/2)$. Its slope is $-n/2$ and its horizontal length is 2. Hence, the q-Weil polynomial has a factor in $\mathbb{Q}_p$ of degree 2 which has two roots of valuation $n/2$. This factor must be irreducible, since $(3, n/2)$ is not a lattice point and hence, the q-Weil polynomial cannot have a root of valuation $n/2$ in $\mathbb{Q}_p$.

Now let $(5, 0)$ be the first vertex on the x-axis, resulting in a p-rank of 1, see Figure 5c. This Newton polygon has a segment with slope $-n/2$ of horizontal length 4 that goes through $(2, 3n/2)$, $(3, n)$ and $(4, n/2)$. This corresponds to a polynomial factor of degree 4 in $\mathbb{Q}_p$ that is allowed to be factored into a product of two degree 2 polynomials, since $(3, n)$ is a lattice point, but cannot be factored further. That is, the q-Weil polynomial cannot have a root of valuation $n/2$ in $\mathbb{Q}_p$ similar to the previous case.

Now let $(3, 1)$ be a vertex, see Figure 2d. In this case is the p-rank is 0, but the abelian variety is not supersingular. We can see that the polynomial factors into a product of two polynomials of degree 3. However, as the only lattice points on the lines are $(0, 3n), (3, n)$ and $(6, 0)$, the q-Weil polynomial cannot be factored further. In other words, those two polynomials of degree 3 must be irreducible in $\mathbb{Q}_p$. Equivalently, they have no root in $\mathbb{Q}_p$.

Lastly, if none of the above is a vertex, we have the supersingular case, see Figure 5e. The only lattice points on the line are $(0, 3n), (2, 2n), (4, n)$ and $(6, 0)$ and the slope is $-n/2$. Hence, it is possible that the q-Weil polynomial in $\mathbb{Q}_p$ is a product of three quadratic polynomials in $\mathbb{Q}_p$, but they have to be all irreducible, i.e.

they must have no root in $\mathbb{Q}_p$. Furthermore, we must have that the polynomial is not able to be factored into two degree 3 (irreducible) polynomials over $\mathbb{Q}_p$. $\square$

9 Dimension 4

The isogeny classification of simple abelian varieties over finite fields of dimension 4 has been done by Haloui and Singh [7] and Xing [28]. The former determines the bounds on the coefficients of q-Weil polynomials of degree 8 and the conditions for which such an irreducible polynomial is the characteristic polynomial of a simple abelian variety of dimension 4. The latter determines the cases when a power of an irreducible q-Weil polynomial of lower degree is the characteristic polynomial of a simple abelian variety of dimension 4. This chapter will summarise their results and provide some additional context for some statements.

As noted by some contributors of the LMFDB [3, Chapter 3.1], there is an error in the result regarding the bounds of the coefficients of Weil polynomials of degree 8 by Haloui and Singh. A correction has been stated in Bradford's PhD thesis [2, Theorem 2.22], which still contained a small mistake, see Remark 9.3. We will add some notes regarding the case where the q-Weil polynomial has a real root and compute the correct bounds for the q-Weil polynomials of degree 8.

9.1 Weil polynomials of degree 8

First, we will determine the conditions for which a polynomial of the form

$$P(x) = x^8 + a_1x^7 + a_2x^6 + a_3x^5 + a_4x^4 + qa_3x^3 + q^2a_2x^2 + q^3a_1x + q^4 \tag{9.1}$$

with $a_1, a_2, a_3, a_4 \in \mathbb{Z}$ is a q-Weil polynomial. Recall from Corollary 4.8 that the characteristic polynomial of an abelian variety must have even multiplicity at real roots. With a similar proof as the corollary due to the assumption of the constant coefficient of (9.1), we can conclude that real roots of $P(x)$ have even multiplicity.

9.1.1 Real roots

Suppose $P(x)$ has a real root, i.e. a root at $x = \sqrt{q}$ or $x = -\sqrt{q}$. First consider the case where q is a square. Because its multiplicity has to be at least 2, we can factor $P(x)$ into

$$P(x) = (x + \sqrt{q})^2\tilde{P}(x) \quad \text{or} \quad P(x) = (x - \sqrt{q})^2\tilde{P}(x),$$

where $\tilde{P}(x)$ is a polynomial in $\mathbb{Z}[x]$ of degree 6. Then, $P(x)$ is a q-Weil polynomial if and only if $\tilde{P}(x)$ is and we know from Chapter 8.1 under which conditions on the polynomial $\tilde{P}(x)$ is a q-Weil polynomial.

Now consider the case where q is not a square. We know the multiplicity of the roots of $P(x)$ at $x = \sqrt{q}$ or $x = -\sqrt{q}$ are even and that their sum is at most 8, since that is the degree of $P(x)$. Write

$$P(x) = (x + \sqrt{q})^{2k}(x - \sqrt{q})^{2\ell}h(x),$$

where $1 \leq k + \ell \leq 4$ and $h(x)$ some polynomial in $\mathbb{R}[x]$. First assume that the multiplicities are the same, i.e. $k = \ell$. The only possible ways to factor $P(x)$ in $\mathbb{R}[x]$ such that the result is a q-Weil polynomial, are as follows:

$$P(x) = \begin{cases} (x^2 - q)^4 & \text{if } k = \ell = 2 \\ (x^2 - q)^2(x^2 + \omega_1x + q)(x^2 + \omega_2x + q) & \text{if } k = \ell = 1, \end{cases}$$

with $\omega_1, \omega_2 \in \mathbb{R}$ such that $|\omega_1|, |\omega_2| \leq 2\sqrt{q}$ and $\omega_1 + \omega_2$, $\omega_1\omega_2 \in \mathbb{Z}$. If $\sqrt{q} \notin \mathbb{Z}$, then the minimal polynomial of $\sqrt{q}$ and $-\sqrt{q}$ is $x^2 - q$, which must divide $P(x)$ if either of them is a root of $P(x)$. Since the quotient is still a q-Weil polynomial, now of degree 6, we can deduce from Theorem 8.2 that we must have $k = \ell$.

9.1.2 No real roots

Similar to the case for dimension 3, we will apply results from Lemma 7.1 in order to determine when a degree 8 polynomial of the form

$$P(x) = x^8 + a_1x^7 + a_2x^6 + a_3x^5 + a_4x^4 + qa_3x^3 + q^2a_2x^2 + q^3a_1x + q^4, \tag{9.2}$$

without real roots, is a q-Weil polynomial. Namely, as in Proposition 6.1, one can factorise $P(x)$ over $\mathbb{C}$ into a product of quadratic polynomials

$$P(x) = \prod_{i=1}^{4}(x^2 + \omega_i x + q), \tag{9.3}$$

for some $\omega_1, \omega_2, \omega_3, \omega_4 \in \mathbb{C}$. Then $P(x)$ is a q-Weil polynomial if and only if the polynomials

$$P^+(x) = \prod_{i=1}^{4}(x - (2\sqrt{q} + \omega_i)), \tag{9.4}$$

$$P^-(x) = \prod_{i=1}^{4}(x - (2\sqrt{q} - \omega_i)), \tag{9.5}$$

only have real positive roots. Let s_1, s_2, s_3 and s_4 denote the symmetric polynomials in the ω_i's, that is

$$\prod_{i=1}^{4}(x + \omega_i) = x^4 + s_1x^3 + s_2x^2 + s_3x + s_4.$$

Explicitly,

$$\begin{aligned} s_1 &= \omega_1 + \omega_2 + \omega_3 + \omega_4, \\ s_2 &= \omega_1\omega_2 + \omega_1\omega_3 + \omega_1\omega_4 + \omega_2\omega_3 + \omega_2\omega_4 + \omega_3\omega_4, \\ s_3 &= \omega_1\omega_2\omega_3 + \omega_1\omega_2\omega_4 + \omega_1\omega_3\omega_4 + \omega_2\omega_3\omega_4, \\ s_4 &= \omega_1\omega_2\omega_3\omega_4. \end{aligned}$$

Expanding (9.3) and writing the coefficients in (9.2) in terms of the symmetric polynomials, we get

$$\begin{aligned} a_1 &= s_1, \\ a_2 &= s_2 + 4q, \\ a_3 &= s_3 + 3qs_1, \\ a_4 &= s_4 + 2qs_2 + 6q^2. \end{aligned}$$

Hence, writing the symmetric polynomials in terms of the coefficients of $P(x)$ we get

$$\begin{aligned} s_1 &= a_1, \\ s_2 &= a_2 - 4q, \\ s_3 &= a_3 - 3qa_1, \\ s_4 &= a_4 - 2qa_2 + 2q^2. \end{aligned}$$

We write

$$P^+(x) = x^4 + b_1^+x^3 + b_2^+x^2 + b_3^+x + b_4^+, \tag{9.6}$$

$$P^-(x) = x^4 + b_1^-x^3 + b_2^-x^2 + b_3^-x + b_4^-. \tag{9.7}$$

Then expanding (9.4) and (9.5) and comparing it to (9.6) and (9.7) respectively leads to

$$\begin{aligned} b_1^+ &= -s_1 - 8\sqrt{q}, & b_1^- &= s_1 - 8\sqrt{q}, \\ b_2^+ &= s_2 + 6\sqrt{q}s_1 + 24q, & b_2^- &= s_2 - 6\sqrt{q}s_1 + 24q, \\ b_3^+ &= -s_3 - 4\sqrt{q}s_2 - 12qs_1 - 32q\sqrt{q}, & b_3^- &= s_3 - 4\sqrt{q}s_2 + 12qs_1 - 32q\sqrt{q}, \\ b_4^+ &= s_4 + 2\sqrt{q}s_3 + 4qs_2 + 8q\sqrt{q}s_1 + 16q^2, & b_4^- &= s_4 - 2\sqrt{q}s_3 + 4qs_2 - 8q\sqrt{q}s_1 + 16q^2. \end{aligned}$$

Hence,

$$\begin{aligned} b_1^+ &= -a_1 - 8\sqrt{q}, & b_1^- &= a_1 - 8\sqrt{q}, \\ b_2^+ &= a_2 + 6\sqrt{q}a_1 + 20q, & b_2^- &= a_2 - 6\sqrt{q}a_1 + 20q, \\ b_3^+ &= -a_3 - 4\sqrt{q}a_2 - 9qa_1 - 16q\sqrt{q}, & b_3^- &= a_3 - 4\sqrt{q}a_2 + 9qa_1 - 16q\sqrt{q}, \\ b_4^+ &= a_4 + 2\sqrt{q}a_3 + 2qa_2 + 2q\sqrt{q}a_1 + 2q^2, & b_4^- &= a_4 - 2\sqrt{q}a_3 + 2qa_2 - 2q\sqrt{q}a_1 + 2q^2. \end{aligned}$$

Lemma 9.1. *Let $h(x) = x^4 + r_1x^3 + r_2x^2 + r_3x + r_4$ be a monic polynomial of degree 4 with real coefficients. Set*

$$\begin{aligned}
u_2 &:= \frac{r_2}{2} - \frac{3r_1^2}{16},\\
u_3 &:= \frac{r_1^3}{32} - \frac{r_1r_2}{8} + \frac{r_3}{4},\\
\zeta_3 &= e^{\frac{2\pi i}{3}},\\
\eta &:= \left(-\frac{u_2^6}{27} - 5u_2^3u_3^2 + \frac{27}{2}u_3^4 + i\frac{27|u_3|(-u_3^2 - \frac{4}{27}u_2^3)^{3/2}}{2}\right)^{1/3}.
\end{aligned}$$

Let $S_\eta := \{\eta + \overline{\eta} + \frac{2u_2^2}{3}, \zeta_3\eta + \zeta_3^2\overline{\eta} + \frac{2u_2^2}{3}, \zeta_3^2\eta + \zeta_3\overline{\eta} + \frac{2u_2^2}{3}\} \subseteq \mathbb{R}$. Let $\theta_1 \leq \theta_2 \leq \theta_3$ be the three elements in S_η. Then, $h(x)$ has only real roots that are all positive if and only if the following conditions hold:

1. $r_1 < 0$,
2. $0 < r_2 \leq \frac{3r_1^2}{8}$,
3. $\frac{r_1r_2}{2} - \frac{r_1^3}{8} - \frac{1}{216}(9r_1^2 - 24r_2)^{3/2} \leq r_3 \leq \frac{r_1r_2}{2} - \frac{r_1^3}{8} + \frac{1}{216}(9r_1^2 - 24r_2)^{3/2}$,
4. $r_3 < 0$,
5. $\frac{3r_1^4}{256} - \frac{r_1^2r_2}{16} + \frac{r_1r_3}{4} + \theta_1 \leq r_4 \leq \frac{3r_1^4}{256} - \frac{r_1^2r_2}{16} + \frac{r_1r_3}{4} + \theta_2$,
6. $0 < r_4$.

Proof. Consider derivatives of $h(x)$, which are

$$\begin{aligned}
h'(x) &= 4x^3 + 3r_1x^2 + 2r_2x + r_3,\\
h''(x) &= 12x^2 + 6r_1x + 2r_2,\\
h'''(x) &= 24x + 6r_1.
\end{aligned}$$

Clearly, $r_1 < 0$ due to Descartes' rule of sign change. We can conclude the result by applying Lemma 7.8 to $h''(x)$, afterwards applying Lemma 7.9 to $h'(x)$ and lastly applying Lemma 7.10 to $h(x)$. □

We will apply Lemma 9.1 to b_i^+ and b_i^- for $i = 1, 2, 3, 4$. First we compute u_2 and u_3 in terms of a_1, a_2, a_3 using the expressions we have for b_1^+, b_2^+, b_3^+ and b_1^-, b_2^-, b_3^-. We determine that

$$\begin{aligned}
u_2 &= -\frac{3a_1^2}{16} + \frac{a_2}{2} - 2q,\\
u_3 &= \begin{cases} -\frac{a_1^3}{32} + \frac{a_1a_2}{8} + \frac{a_1q}{4} - \frac{a_3}{4} & \text{with } b_1^+, b_2^+, b_3^+,\\ \frac{a_1^3}{32} - \frac{a_1a_2}{8} - \frac{a_1q}{4} + \frac{a_3}{4} & \text{with } b_1^-, b_2^-, b_3^-. \end{cases}
\end{aligned}$$

Note that, due to u_3 only appearing in the definition of η as an even power or absolute value $|u_3|$, we will the same result in Lemma 9.1 for both choices of $b_1^+, b_2^+, b_3^+, b_4^+$ and $b_1^-, b_2^-, b_3^-, b_4^-$.

Substituting $b_1^+, b_2^+, b_3^+, b_4^+$ and $b_1^-, b_2^-, b_3^-, b_4^-$ in Lemma 9.1 and combining the results with the results for the real root case, we obtain the following theorem.

Theorem 9.2. *Let $P(x) = x^8 + a_1x^7 + a_2x^6 + a_3x^5 + a_4x^4 + a_3qx^3 + a_2q^2x^2 + a_1q^3x + q^4$ be a polynomial with integer coefficients. Set*

$$\begin{aligned}
u_2 &= -\frac{3a_1^2}{16} + \frac{a_2}{2} - 2q,\\
u_3 &= -\frac{a_1^3}{32} + \frac{a_1a_2}{8} + \frac{a_1q}{4} - \frac{a_3}{4},\\
\zeta_3 &= e^{\frac{2\pi i}{3}},\\
\eta &= \left(-\frac{u_2^6}{27} - 5u_2^3u_3^2 + \frac{27}{2}u_3^4 + i\frac{27|u_3|(-u_3^2 - \frac{4}{27}u_2^3)^{3/2}}{2}\right)^{1/3}.
\end{aligned}$$

Let S_η be the set

$$S_\eta = \left\{\eta + \overline{\eta} + \frac{2u_2^2}{3}, \zeta_3\eta + \zeta_3^2\overline{\eta} + \frac{2u_2^2}{3}, \zeta_3^2\eta + \zeta_3\overline{\eta} + \frac{2u_2^2}{3}\right\} \subseteq \mathbb{R}.$$

Let $\theta_1 \le \theta_2 \le \theta_3$ be the three elements of S_η. Then $P(x)$ is a q-Weil polynomial if and only if one of the following conditions hold:

1. *q is a square and $P(x) = (x + \sqrt{q})^2\tilde{P}(x)$ or $P(x) = (x - \sqrt{q})^2\tilde{P}(x)$, where $\tilde{P}(x)$ is a q-Weil polynomial of degree 3, see Theorem 8.2;*
2. *q is not a square and $P(x) = (x^2 - q)^4$ or $P(x) = (x^2 - q)^2(x^2 + \omega_1x + q)(x^2 + \omega_2x + q)$, where $\omega_1, \omega_2 \in \mathbb{R}$ such that $|\omega_1|, |\omega_2| < 2\sqrt{q}$ and $\omega_1 \cdot \omega_2, \omega_1 + \omega_2 \in \mathbb{Z}$;*
3. *the following conditions hold:*
   (a) $|a_1| < 8\sqrt{q}$,
   (b) $6\sqrt{q}|a_1| - 20q < a_2 \le \frac{3a_1^2}{8} + 4q$,
   (c) $\frac{a_1a_2}{2} - \frac{a_1^3}{8} + a_1q - \frac{1}{216}(9a_1^2 - 24a_2 + 96q)^{3/2} \le a_3 \le \frac{a_1a_2}{2} - \frac{a_1^3}{8} + a_1q + \frac{1}{216}(9a_1^2 - 24a_2 + 96q)^{3/2}$,
   (d) $-4\sqrt{q}a_2 - 9qa_1 - 16q\sqrt{q} < a_3 < 4\sqrt{q}a_2 - 9qa_1 + 16q\sqrt{q}$,
   (e) $\frac{3a_1^4}{256} - \frac{a_1^2a_2}{16} - \frac{a_1^2q}{2} + \frac{a_1a_3}{4} + 2a_2q - 2q^2 + \theta_1 \le a_4 \le \frac{3a_1^4}{256} - \frac{a_1^2a_2}{16} - \frac{a_1^2q}{2} + \frac{a_1a_3}{4} + 2a_2q - 2q^2 + \theta_2$,
   (f) $2\sqrt{q}|a_1q + a_3| - 2qa_2 - 2q^2 < a_4$.

Remark 9.3. For the second condition, one can use [14, Lemma 2.1] for the bounds of the coefficients of q-Weil polynomials of degree 4 instead of the conditions in terms of ω_1, ω_2.
When comparing my bounds to the ones stated in Bradford's thesis [2, Theorem 2.22], there seems to be a typo in their statement, where ω should be

$$\omega = \frac{1}{24}\left(-8r_2^6 - 540r_2^3r_3^2 + 729r_3^4 + i729|r_3|\left(-r_3^2 - \frac{8}{27}r_2^3\right)^{3/2}\right)^{1/3}.$$

Furthermore, the original statement is missing the q-Weil polynomials that have a real root.
After implementing the corrected bounds in SageMath 9.3 [13] and comparing the result to the built-in function by [11], a few non-square-free q-Weil polynomials without real roots were determined by the in-built function in SageMath that did not satisfy my result due to precision errors, which we will now explain. Since they are non-square-free, they must have a multiple root. As explained in Corollary 7.6, a coefficient being equal to one of its (non-strict) bounds necessarily means that there is a multiple root. Due to these precision errors, some of the bounds were not correctly identified as integers. Increasing the precision of the code solved this problem for the values of q for which the tests were done, but may still cause an issue for higher values of q.

9.2 Newton polygons

We will now determine which q-Weil polynomials of degree 8 correspond to a simple abelian variety of dimension 4 over $\mathbb{F}_q = \mathbb{F}_{p^n}$ by combining results by Xing [28] and results by Haloui and Singh [7]. We know that a simple abelian variety has a characteristic polynomial of the form $P(x)^d$, where $P(x)$ is an irreducible q-Weil polynomial of degree $\frac{2g}{d}$. The divisors of 8 are $d = 1, 2, 4, 8$. However, if $d = 8$, we would get that $P(x)$ is a q-Weil polynomial of degree 1, which can only have a real root. Hence, this case cannot happen due to Lemma 5.5. For $d = 4, 2$, the result was determined by Xing [28, Propositions 3 and 4], while Haloui and Singh [7, Theorem 1.2] determined the case for $d = 1$. Combining these two results are as follows.

Theorem 9.4. *Let $P(x) = x^8 + a_1x^7 + a_2x^6 + a_3x^5 + a_4x^4 + a_3qx^3 + a_2q^2x^2 + a_1q^3x + q^4$ be a q-Weil polynomial with $q = p^n$. Then $P(x)$ is the characteristic polynomial of a simple abelian variety of dimension 4 over $\mathbb{F}_q$ if and only if one of the following conditions holds:*

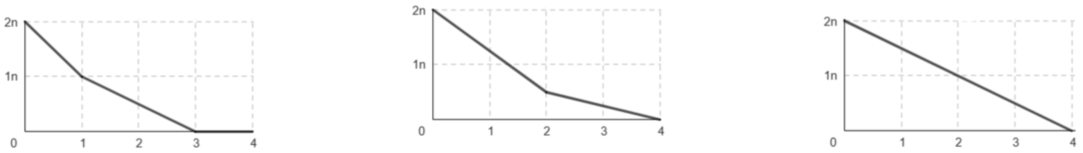
1. *n is a multiple of 4 and $P(x) = (x^2 + \omega x + q)^4$, where $|\omega| < 2\sqrt{q}$ and $\omega = kq^{1/4}$ with $k \in \mathbb{Z}$ not divisible by p,*
2. *$P(x) = m(x)^2$, with $m(x) = x^4 + b_1x^3 + b_2x^2 + b_1qx + q^2 \in \mathbb{Z}[x]$ an irreducible q-Weil polynomial and one of the following conditions hold:*
   - *(a) $v_p(b_2) \geq n/2$, $v_p(b_1) = 0$ and $m(x)$ has 4 roots in $\mathbb{Q}_p$ counted with multiplicity,*
   - *(b) $v_p(b_2) = n/2$, $v_p(b_1) \geq n/4$ and $m(x)$ has no root in $\mathbb{Q}_p$,*
   - *(c) $v_p(b_2) \geq n$, $v_p(b_1) \geq n/2$ and $m(x)$ has a root in $\mathbb{Q}_p$,*
3. *$P(x)$ is irreducible over $\mathbb{Q}$ and one of the following conditions hold:*
   - *(a) $v_p(a_4) = 0$,*
   - *(b) $v_p(a_4) \geq n/2$, $v_p(a_3) = 0$ and $P(x)$ has no root of valuation $n/2$ in $\mathbb{Q}_p$,*
   - *(c) $v_p(a_4) \geq n$, $v_p(a_3) \geq n/2$, $v_p(a_2) = 0$ and $P(x)$ has no root of valuation $n/2$ in $\mathbb{Q}_p$,*
   - *(d) $v_p(a_4) = n, v_p(a_3) \geq 2n/3$, $v_p(a_2) \geq n/3, v_p(a_1) = 0$ and $P(x)$ has no root of valuation $n/3$ or $2n/3$ in $\mathbb{Q}_p$,*
   - *(e) $v_p(a_4) \geq 3n/2, v_p(a_3) \geq n$, $v_p(a_2) \geq n/2, v_p(a_1) = 0$ and $P(x)$ has no root of valuation $n/2$ nor an irreducible factor of degree 3 in $\mathbb{Q}_p$,*
   - *(f) $v_p(a_4) = n, v_p(a_3) \geq 3n/4, v_p(a_2) \geq n/2, v_p(a_1) \geq n/4$ and $P(x)$ has no root nor a factor of degree 2 in $\mathbb{Q}_p$,*
   - *(g) $v_p(a_4) \geq 3n/2, v_p(a_3) = n, v_p(a_2) \geq 2n/3, v_p(a_1) \geq n/3$ and $P(x)$ has no root in $\mathbb{Q}_p$,*
   - *(h) $v_p(a_4) \geq 2n, v_p(a_3) \geq 3n/2, v_p(a_2) \geq n, v_p(a_1) \geq n/2$ and $P(x)$ has no root nor a factor of degree 3 in $\mathbb{Q}_p$.*

The abelian varieties corresponding to case (1) *have p-rank* 0*, while the p-ranks of abelian varieties in cases* (2a), (2b) *and* (2c) *are respectively* 2, 0 *and* 0*. The p-ranks of abelian varieties in cases* (3a), (3b), (3c), (3d), (3e), (3f), (3g) *and* (3h) *are respectively* 4, 3, 2, 1, 1, 0, 0 *and* 0*. Furthermore, case* (3h) *correspond to supersingular abelian varieties.*

Case (1) follows from Theorem 6.3, which was first determined by Xing [28, Propositions 3] for dimension 4 specifically. Note that these polynomials clearly have p-rank 0, since ω is divisible by p. We will explain cases (2a), (2b) and (2c) in Section 9.2.1. The others are explained in Section 9.2.2.

9.2.1 Square polynomial

For dimension 4, the case with $d = 2$ has been determined by Xing [28]. Let $m(x) = x^4+b_1x^3+b_2x^2+b_1qx+q^2$ be an irreducible q-Weil polynomial. An analogue to Corollary 6.8 can be made using Lemma 6.2 and Lemma 6.7, where the endpoints are $(0, 2n)$ and $(4, 0)$, and the vertices have to be contained in $\mathbb{Z} \times (n/2)\mathbb{Z}$ with at least one vertex not in $\mathbb{Z} \times n\mathbb{Z}$. We must have at least one vertex not in $\mathbb{Z} \times n\mathbb{Z}$, because otherwise $m(x)$ we would not get $d = 2$ in Lemma 6.2. This means we must have $v_p(b_1) = n/2$ or $v_p(b_2) = n/2$, since they would not appear as vertices on the Newton polygon otherwise. The resulting Newton polygons are given in Figure 6 and the conditions for $v_p(b_1)$ and $v_p(b_2)$ follow immediately.



(a) p-rank 2 case

(b) p-rank 0, first case

(c) p-rank 0, second case

Figure 6: Newton polygons of characteristic polynomials $m(x)^2$ of simple abelian varieties of dimension 4. See [28].

For the first case, suppose $v_p(b_2) = n/2$ and $v_p(b_1) = 0$, see Figure 6a. We can see from the Newton polygon that $m(x)$ can be factored into a product of two linear and one quadratic polynomial over $\mathbb{Q}_p$. However, since $(2, n/2)$ is a necessary vertex, the quadratic polynomial has to be a product of two linear polynomials over $\mathbb{Q}_p$. Hence, the polynomial $m(x)$ must have 4 roots in $\mathbb{Q}_p$. Equivalently, as determined by Xing in [28, Proposition 4], $(b_2^2 + 2q)^2 - 4qb_1^2$ is a square in $\mathbb{Z}_p$.

For the case where $(2, n/2)$ is a vertex, but $(3, 0)$ is not, see Figure 6b. We see from the Newton polygon that $m(x)$ can be factored into a product of two quadratic polynomials over $\mathbb{Q}_p$. However, as the values of the Newton polygon at $x = 1$ and $x = 3$ are not in $(n/2)\mathbb{Z}$, these quadratic polynomials must be irreducible. Equivalently, $m(x)$ has no root in $\mathbb{Q}_p$.

Lastly, if $(3, n/2)$ is a vertex, see Figure 6c. Since $(3, n/2)$ is a necessary vertex, $m(x)$ must be factorisable into a product of a linear and a cubic polynomial over $\mathbb{Q}_p$. Equivalently, $m(x)$ has a root in $\mathbb{Q}_p$.

Since these Newton polygons are of $m(x)$ and not of $P(x)$, we cannot immediately determine the p-rank of these cases. After observing that $m(x)^2 = P(x)$, we can express a_1, a_2, a_3 and a_4 in terms of b_1 and b_2 to find the p-ranks. We compute

$$\begin{aligned} a_1 &= 2b_1, \\ a_2 &= b_1^2 + 2b_2, \\ a_3 &= 2b_1b_2 + 2b_1q, \\ a_4 &= 2b_1^2q + b_2^2 + 2q^2. \end{aligned}$$

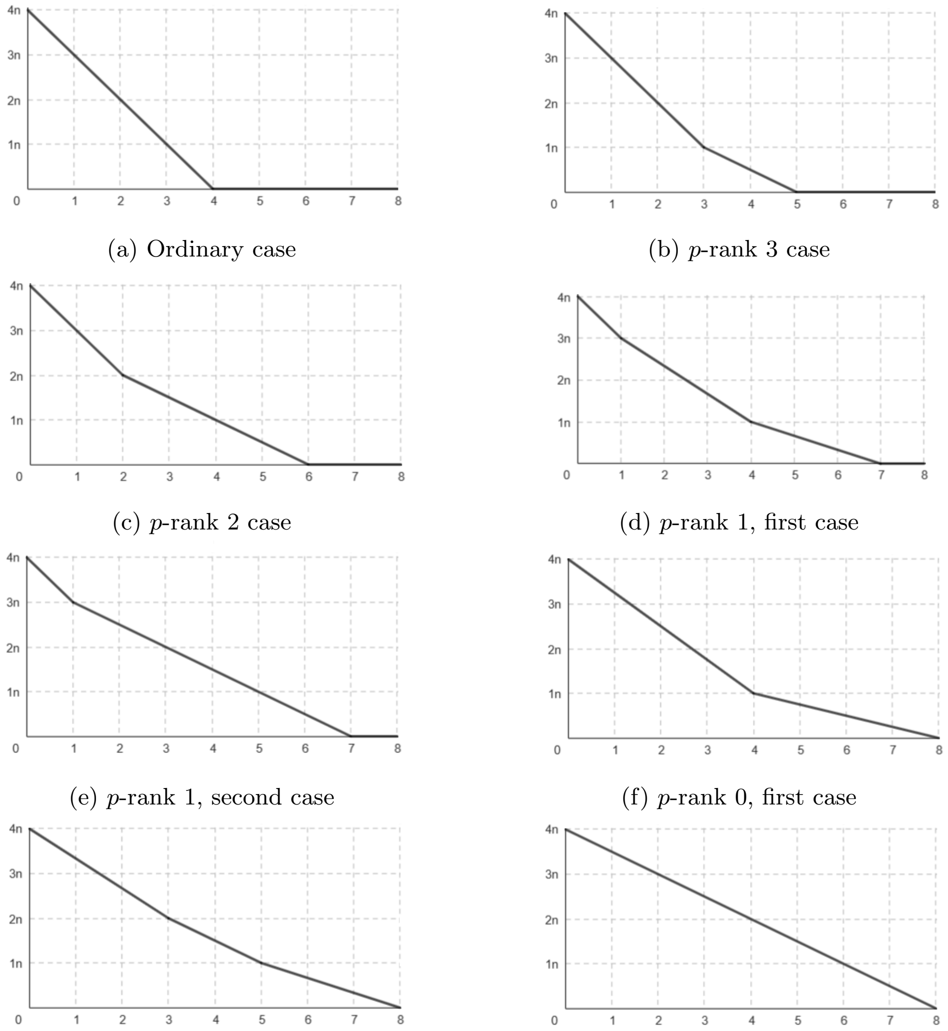
Since by Proposition 6.11 the p-rank is equal to the largest index i with $v_p(a_i) = 0$, we immediately have that the cases in Figures 6b and 6c have p-rank 0, as $v_p(b_1), v_p(b_2) > 0$, leading to $v_p(a_1), v_p(a_2), v_p(a_3), v_p(a_4) > 0$. For case in Figure 6a, we have $v_p(b_2) > 0$, but $v_p(b_1) = 0$. This leads to $v_p(a_2) = 0$ and $v_p(a_3), v_p(a_4) > 0$, so the p-rank is 2.

9.2.2 Irreducible polynomial

We now consider the case $d = 1$, that is, when $P(x)$ is an irreducible q-Weil polynomial of degree 8 of the form

$$P(x) = x^8 + a_1x^7 + a_2x^6 + a_3x^5 + a_4x^4 + a_3qx^3 + a_2q^2x^2 + a_1q^3x + q^4.$$

Using Corollary 6.8, we can determine all possible Newton polygons of $P(x)$ such that it is the characteristic polynomial of a simple abelian variety of dimension 4. The lattice points under the line through $(0, 4n)$ and $(8, 0)$ and on or above the x-axis with x-coordinate 4, 5, 6 or 7 are $(4, 0), (4, 1), (5, 0), (5, 1), (6, 0)$ and $(7, 0)$. They all give one Newton polygon with another possible construction having vertices $(4, 1)$ and $(7, 0)$ and the last construction being the line through $(0, 4n)$ and $(8, 0)$. This result was first determined by Haloui and Singh [7, Theorem 1.2]. The possible Newton polygons are given in Figure 7. The graphs immediately give the conditions regarding the valuations of a_1, a_2, a_3 and a_4 and the horizontal slope gives the p-rank of the respective case, see Corollary 6.12.



(a) Ordinary case

(b) p-rank 3 case

(c) p-rank 2 case

(d) p-rank 1, first case

(e) p-rank 1, second case

(f) p-rank 0, first case

(g) p-rank 0, second case

(h) Supersingular case

Figure 7: Newton polygons of irreducible characteristic polynomials of simple abelian varieties of dimension 4, c.f. [7].

First suppose $(4, 0)$ is a vertex, so the case in Figure 7a. The Newton polygon tells us that in $\mathbb{Q}_p[x]$, the polynomial $P(x)$ is a product of two degree 4 polynomials. Since the segments pass through a lattice point at each integer value of x, these two polynomials are allowed to be factored in any possible way over $\mathbb{Q}_p$.

Now suppose $(5, 0)$ is a vertex, but $(4, 0)$ is not, see Figure 7b. We determine that $P(x)$ is a product of two degree 3 polynomials and one degree 2 polynomial in $\mathbb{Q}_p[x]$. However, at $x = 4$, the Newton polygon does not pass through a lattice point. Hence, the degree 2 polynomial cannot be factored further, that is it cannot have a root in $\mathbb{Q}_p$. Since the slope of this line is $-n/2$, we can simply say that $P(x)$ cannot have a root of p-adic valuation $n/2$ in $\mathbb{Q}_p$.

If $(6, 0)$ is a vertex, but $(5, 0)$ is not, we have the p-rank 2 case, see Figure 7c. The Newton polygon shows that $P(x)$ can be factored over $\mathbb{Q}_p$ into a product of two degree 2 polynomials and one degree 4 polynomial. The former may have roots in $\mathbb{Q}_p$, since the corresponding segments only pass through lattice points at integer values of x. The latter may be factored into a product of two degree 2 polynomials, since the middle point

$(4, n)$ of the segment with horizontal length 4 is a lattice point, but cannot be further factored, which means it cannot have a root. The slope of this segment is $-n/2$, while the other segments have a different slope, so we can simply say that $P(x)$ does not have a root of p-adic valuation $n/2$ in $\mathbb{Q}_p$.

In the first case of p-rank 1 where $(4, 1)$ is a vertex, see Figure 7e, $P(x)$ has two linear factors and two factors of degree 3. Since the segments with horizontal length 3 do not go through any lattice point except for their endpoints, they must be irreducible. Equivalently, they have no root in $\mathbb{Q}_p$. As the slopes of these edges are $-n/3$ and $-2n/3$, the polynomial $P(x)$ does not have a root in $\mathbb{Q}_p$ of p-adic valuation $n/3$ or $2n/3$.

The second case of p-rank 1 is given in Figure 7d. Here, $P(x)$ has two linear factors and a factor of degree 6 in $\mathbb{Q}_p$. Since the edge with horizontal length 6 only passes through lattice points for every second integer value of x, the polynomial factor of degree 6 is allowed to be factored into three quadratic polynomials, but these cannot have roots. Furthermore, the degree 6 polynomial cannot be factored into two polynomials of degree 3. The slope of the corresponding edge is $-n/2$. Hence, $P(x)$ does not have a root of p-adic valuation $n/2$ nor an irreducible factor of degree 3 in $\mathbb{Q}_p$.

In the case with p-rank 0 where $(4, 1)$ is a vertex, see Figure 7f, we see that $P(x)$ must have two irreducible factors of degree 4 in $\mathbb{Q}_p$. This is because there are two segments of horizontal length 4 that do not go through any lattice points except their endpoints. Equivalently, $P(x)$ has no root nor a factor of degree 2 in $\mathbb{Q}_p$.

The second case with p-rank 0, see Figure 7g, has two edges of horizontal length 3 and one of length 2. These edges only pass through lattice points at their endpoints. Hence, the factorisation over $P(x)$ over $\mathbb{Q}_p$ consists of two irreducible polynomials of degree 3 and one irreducible polynomial of degree 2. Equivalently, $P(x)$ has no root in $\mathbb{Q}_p$.

Lastly, we have the supersingular case, see Figure 7h. Only at even values of x does the Newton polygon pass through lattice points. Hence, $P(x)$ is allowed to be factored into a product of polynomials over $\mathbb{Q}_p$, but none of them can have odd degree. Equivalently, $P(x)$ has no root nor a factor of degree 3 over $\mathbb{Q}_p$.

10 Dimension 5

The bounds on the coefficients of q-Weil polynomials of degree 10 have been determined by Sohn [22], while Hayashida [8] has determined conditions for which a q-Weil polynomial of degree 10 is the characteristic polynomial of an abelian variety of dimension 5 over a fixed finite field. However, according to some contributors of the LMFDB [3, Chapter 3.1], the bounds by Sohn are incorrect. We will add some notes regarding the case where the q-Weil polynomial has a real root and explain how to correctly compute the bounds. Afterwards, we summarise Hayashida's result on which q-Weil polynomials of degree 10 correspond to characteristic polynomials of simple abelian varieties of dimension 5 over $\mathbb{F}_q$.

10.1 Weil polynomials of degree 10

Let

$$P(x) = x^{10} + a_1x^9 + a_2x^8 + a_3x^7 + a_4x^6 + a_5x^5 + qa_4x^4 + q^2a_3x^3 + q^3a_2x^2 + q^4a_1x + q^5 \tag{10.1}$$

be an integer polynomial. In order to determine the conditions on the coefficients in order for it to be a q-Weil polynomial, we will again distinguish the cases with a real root and without a real root similar as our procedures in Chapters 8 and 9.

10.1.1 Real roots

Recall from Corollary 4.8 that the characteristic polynomial of an abelian variety must have even multiplicity at real roots. If $P(x)$ has a real root and $\sqrt{q} \in \mathbb{Z}$, then $P(x)$ is a q-Weil polynomial if and only if

$$P(x) = (x + \sqrt{q})^2\tilde{P}(x) \quad \text{or} \quad P(x) = (x + \sqrt{q})^2\tilde{P}(x),$$

where $\tilde{P}(x)$ is a q-Weil polynomial of degree 8, for which we refer to Theorem 9.2.

In the case where q is not a square, if the root at $x = \sqrt{q}$ is of the same multiplicity as the one at $x = -\sqrt{q}$, then the following cases occur:

$$P(x) = \begin{cases} (x^2 - q)^4(x^2 + \omega x + q) & \text{if } k = \ell = 2, \text{ where } \omega \in \mathbb{Z} \text{ with } |\omega| < 2\sqrt{q}, \\ (x^2 - q)^2 \prod_{i=1}^{3}(x^2 + \omega_i + q) & \text{if } k = \ell = 1, \text{ where } \omega_i \in \mathbb{R} \text{ such that } \prod_{i=1}^{3}(x + \omega_i) \in \mathbb{Z}[x]. \end{cases}$$

Moreover, if $\sqrt{q} \notin \mathbb{Z}$, the minimal polynomial of both $\sqrt{q}$ and $-\sqrt{q}$ is $x^2 - q$, so it must divide $P(x)$. The quotient is then a q-Weil polynomial, now of degree 8, so we conclude using Theorem 9.2 that $k \neq \ell$ does not happen if $\sqrt{q} \notin \mathbb{Z}$.

10.1.2 No real roots

Write

$$P(x) = \prod_{i=1}^{5}(x^2 + \omega_i x + q), \tag{10.2}$$

for some $\omega_1, \ldots, \omega_i \in \mathbb{C}$. As explained in Proposition 6.1, $P(x)$ is a q-Weil polynomial without real roots if and only if the polynomials

$$P^+(x) = \prod_{i=1}^{5}(x - (2\sqrt{q} + \omega_i)), \tag{10.3}$$

$$P^-(x) = \prod_{i=1}^{5}(x - (2\sqrt{q} - \omega_i)), \tag{10.4}$$

only have real positive roots. Let s_1, s_2, s_3, s_4 and s_5 denote the symmetric polynomials in ω_i, that is

$$\prod_{i=1}^{5}(x+\omega_i) = x^5 + s_1x^4 + s_2x^3 + s_3x^2 + s_4x + s_5.$$

Expanding (10.2) and comparing it with (10.1) gives

$$\begin{aligned}
a_1 &= s_1,\\
a_2 &= s_2 + 5q,\\
a_3 &= s_3 + 4qs_1,\\
a_4 &= s_4 + 3qs_2 + 10q^2,\\
a_5 &= s_5 + 2qs_3 + 6q^2s_1.
\end{aligned}$$

Hence, the symmetric polynomials in terms of the coefficients of $P(x)$ are

$$\begin{aligned}
s_1 &= a_1,\\
s_2 &= a_2 - 5q,\\
s_3 &= a_3 - 4qa_1,\\
s_4 &= a_4 - 3qa_2 + 5q^2,\\
s_5 &= a_5 - 2qa_3 + 2q^2a_1.
\end{aligned}$$

We write the coefficients of $P^+(x)$ and $P^-(x)$ as

$$P^+(x) = x^5 + b_1^+x^4 + b_2^+x^3 + b_3^+x^2 + b_4^+x + b_5^+, \tag{10.5}$$
$$P^-(x) = x^5 + b_1^-x^4 + b_2^-x^3 + b_3^-x^2 + b_4^-x + b_5^-. \tag{10.6}$$

Expanding (10.3) and (10.4) and comparing it to (10.5) and (10.6) respectively yields

$$\begin{aligned}
b_1^+ &= -s_1 - 10\sqrt{q}, & b_1^- &= s_1 - 10\sqrt{q},\\
b_2^+ &= s_2 + 8\sqrt{q}s_1 + 40q, & b_2^- &= s_2 - 8\sqrt{q}s_1 + 40q,\\
b_3^+ &= -s_3 - 6\sqrt{q}s_2 - 24qs_1 - 80q\sqrt{q}, & b_3^- &= s_3 - 6\sqrt{q}s_2 + 24qs_1 - 80q\sqrt{q},\\
b_4^+ &= s_4 + 4\sqrt{q}s_3 + 12qs_2 + 32q\sqrt{q}s_1 + 80q^2, & b_4^- &= s_4 - 4\sqrt{q}s_3 + 12qs_2 - 32q\sqrt{q}s_1 + 80q^2,\\
b_5^+ &= -s_5 - 2\sqrt{q}s_4 - 4qs_3 - 8q\sqrt{q}s_2 - 16q^2s_1 - 32q^2\sqrt{q}, & b_5^- &= s_5 - 2\sqrt{q}s_4 + 4qs_3 - 8q\sqrt{q}s_2 + 16q^2s_1 - 32q^2\sqrt{q}.
\end{aligned}$$

Substituting the values of $s_1, \ldots, s_5$ in terms of $a_1, \ldots, a_5$ then gives

$$\begin{aligned}
b_1^+ &= -a_1 - 10\sqrt{q}, & b_1^- &= a_1 - 10\sqrt{q},\\
b_2^+ &= a_2 + 8\sqrt{q}a_1 + 35q, & b_2^- &= a_2 - 8\sqrt{q}a_1 + 35q,\\
b_3^+ &= -a_3 - 6\sqrt{q}a_2 - 20qa_1 - 50q\sqrt{q}, & b_3^- &= a_3 - 6\sqrt{q}a_2 + 20qa_1 - 50q\sqrt{q},\\
b_4^+ &= a_4 + 4\sqrt{q}a_3 + 9qa_2 + 16q\sqrt{q}a_1 + 25q^2, & b_4^- &= a_4 - 4\sqrt{q}a_3 + 9qa_2 - 16q\sqrt{q}a_1 + 25q^2,\\
b_5^+ &= -a_5 - 2\sqrt{q}a_4 - 2qa_3 - 2q\sqrt{q}a_2 - 2q^2a_1 - 2q^2\sqrt{q}, & b_5^- &= a_5 - 2\sqrt{q}a_4 + 2qa_3 - 2q\sqrt{q}a_2 + 2q^2a_1 - 2q^2\sqrt{q}.
\end{aligned}$$

Lemma 10.1. *Let $h(x) = x^5 + r_1x^4 + r_2x^3 + r_3x^2 + r_4x + r_5$ be a monic polynomial of degree 5 with real coefficients. Set*

$$\begin{aligned}
u_2 &:= \frac{3r_2}{10} - \frac{3r_1^2}{25},\\
u_3 &:= \frac{2r_1^3}{125} - \frac{3r_1r_2}{50} + \frac{r_3}{10},\\
u_4 &= \frac{-3r_1^4}{625} + \frac{3r_1^2r_2}{125} - \frac{2r_1r_3}{25} + \frac{r_4}{5},\\
\zeta_3 &:= e^{\frac{2\pi i}{3}},\\
\eta &:= 5\left(-\frac{u_2^6}{27} - 5u_2^3u_3^2 + \frac{27u_3^4}{2} + i\frac{27|u_3|\left(-u_3^2 - \frac{4}{27}u_2^3\right)^{3/2}}{2}\right)^{1/3}.
\end{aligned}$$

Define $S_\eta := \left\{\eta + \overline{\eta} + \frac{10u_2^2}{3}, \zeta_3\eta + \zeta_3^2\overline{\eta} + \frac{10u_2^2}{3}, \zeta_3^2\eta + \zeta_3\overline{\eta} + \frac{10u_2^2}{3}\right\} \subseteq \mathbb{R}$ *and let* $\theta_1 \leq \theta_2 \leq \theta_3$ *be the three elements of* S_η *ordered from least to greatest. If* $u_3 = 0$*, let* x_{i_1,i_2} *be*

$$x_{i_1,i_2} = i_1\sqrt{-u_2 + i_2\sqrt{u_2^2 - u_4}},$$

for $i_1, i_2 \in \{+1, -1\}$*. Otherwise, define*

$$\begin{aligned} v_2 &= -\frac{u_2^2}{3} - u_4, \\ v_3 &= \frac{2u_2u_4}{3} - \frac{2u_2^3}{27} - 2u_3^2, \\ C &= \left(\frac{-v_3 + \sqrt{v_3^2 + \frac{4}{27}v_2^3}}{2}\right)^{1/3}, \\ y &= \begin{cases} \sqrt[3]{-v_3} - \frac{2u_2}{3} & \text{if } v_2 = 0, \\ C - \frac{v_2}{3C} - \frac{2u_2}{3} & \text{if } v_2 \neq 0, \end{cases} \end{aligned}$$

and let x_{i_1,i_2} *for* $i_1, i_2 \in \{+1, -1\}$ *be defined by*

$$x_{i_1,i_2} = \frac{i_1\sqrt{2y} + i_2\sqrt{-4u_2 - 2y - i_1\frac{8u_3}{\sqrt{2y}}}}{2}.$$

Note that under the conditions on r_1, r_2, r_3, r_4 *below, all* x_{i_1,i_2}*'s will be real. Let* $\gamma_1 \geq \gamma_2 \geq \gamma_3 \geq \gamma_4$ *be equal to* x_{i_1,i_2} *with each a distinct pair* (i_1, i_2)*, so that they are ordered. Let* $\tilde{g}(x)$ *be a polynomial defined by*

$$\tilde{g}(x) = -x^5 - \frac{10}{3}u_2x^3 - 10u_3x^2 - 5u_4x,$$

and define

$$\begin{aligned} \lambda_1 &= \max\{\tilde{g}(\gamma_2), \tilde{g}(\gamma_4)\}, \\ \lambda_2 &= \min\{\tilde{g}(\gamma_1), \tilde{g}(\gamma_3)\}. \end{aligned}$$

Then $h(x)$ *has only real roots that are all positive if and only if the following conditions hold:*

1. $r_1 < 0$,
2. $0 < r_2 \leq \frac{2r_1^2}{5}$,
3. $-\frac{4}{25}r_1^3 + \frac{3}{5}r_1r_2 - \frac{1}{50}(4r_1^2 - 10r_2)^{3/2} \leq r_3 \leq -\frac{4}{25}r_1^3 + \frac{3}{5}r_1r_2 + \frac{1}{50}(4r_1^2 - 10r_2)^{3/2}$,
4. $r_3 < 0$,
5. $\frac{3r_1^4}{125} - \frac{3r_1^2r_2}{25} + \frac{2r_1r_3}{5} + \theta_1 \leq r_4 \leq \frac{3r_1^4}{125} - \frac{3r_1^2r_2}{25} + \frac{2r_1r_3}{5} + \theta_2$,
6. $r_4 > 0$,
7. $-\frac{4r_1^5}{3125} + \frac{r_1^3r_2}{125} - \frac{r_1^2r_3}{25} + \frac{r_1r_4}{5} + \lambda_1 \leq r_5 \leq -\frac{4r_1^5}{3125} + \frac{r_1^3r_2}{125} - \frac{r_1^2r_3}{25} + \frac{r_1r_4}{5} + \lambda_1$,
8. $r_5 < 0$.

Proof. Once again, we will be applying the results obtained from Robinson's method, Lemma 7.1, in order to prove the statements. The derivatives of $h(x)$ are

$$\begin{aligned} h'(x) &= 5x^4 + 4r_1x^3 + 3r_2x^2 + 2r_3x + r_4, \\ h''(x) &= 20x^3 + 12r_1x^2 + 6r_2x + 2r_3, \\ h'''(x) &= 60x^2 + 24r_1x + 6r_2, \\ h''''(x) &= 120x + 24r_1. \end{aligned}$$

We obtain the bounds of r_2 by applying Lemma 7.8 to $h'''(x)$, then apply Lemma 7.9 to $h''(x)$ for the bounds of r_3, afterwards use Lemma 7.10 on $h'(x)$ for the bounds of r_4 and lastly the bounds for r_5 follow from Lemma 7.10 with $h(x)$. □

We will be applying the bounds described in Lemma 10.1 to $b_1^+, \dots, b_5^+$ and $b_1^-, \dots, b_5^-$. First we compute

$$\begin{aligned} u_2 &= -\frac{3a_1^2}{25} + \frac{3a_2}{10} - \frac{3q}{2}, \\ u_3 &= \begin{cases} -\frac{2a_1^3}{125} + \frac{3a_1a_2}{50} + \frac{a_1q}{10} - \frac{a_3}{10} & \text{with } b_1^+, \dots, b_5^+, \\ \frac{2a_1^3}{125} - \frac{3a_1a_2}{50} - \frac{a_1q}{10} + \frac{a_3}{10} & \text{with } b_1^-, \dots, b_5^- \end{cases}, \\ u_4 &= -\frac{3a_1^4}{625} + \frac{3a_1^2a_2}{125} + \frac{a_1^2q}{5} - \frac{2a_1a_3}{25} - \frac{3qa_2}{5} + \frac{a_4}{5} + q^2. \end{aligned}$$

We claim that the bounds for $P(x)$ do not depend on the sign of u_3. The only definitions in Lemma 10.1 with an odd power of u_3 are in η and x_{i_1,i_2}. For η, note that the definition of S_η does not change, since a sign change of u_3 in η gives the complex conjugate $\overline{\eta}$. For x_{i_1,i_2}, note that

$$\begin{aligned} \frac{i_1\sqrt{2y} + i_2\sqrt{-4u_2 - 2y - i_1\frac{8(-u_3)}{\sqrt{2y}}}}{2} &= \frac{i_1\sqrt{2y} + i_2\sqrt{-4u_2 - 2y + (-i_1)\frac{8u_3}{\sqrt{2y}}}}{2} \\ &= -\frac{(-i_1)\sqrt{2y} + (-i_2)\sqrt{-4u_2 - 2y + (-i_1)\frac{8u_3}{\sqrt{2y}}}}{2}. \end{aligned}$$

Hence, a sign change of u_3 applied to x_{i_1,i_2} gives $-x_{-i_1,-i_2}$ and so the elements of $\{x_{+1,+1}, x_{+1,-1}, x_{-1,+1}, x_{-1,-1}\}$ are re-ordered and change sign. However, we notice that the sign of a_5 in b_5^+ is different from a_5 in b_5^-. Hence, if we are careful with the signs in the definition of λ_1 and λ_2, the bounds for a_5 are the same in either case. Substituting $b_1^+, b_2^+, b_3^+, b_4^+, b_5^+$ and $b_1^-, b_2^-, b_3^-, b_4^-, b_5^-$ in Lemma 10.1 results in the following.

Theorem 10.2. *Let $P(x) = x^{10} + a_1x^9 + a_2x^8 + a_3x^7 + a_4x^6 + a_5x^5 + a_4qx^4 + a_3q^2x^3 + a_2q^3x^2 + a_1q^4x + q^5$ be an integer polynomial.*

$$\begin{aligned} u_2 &= -\frac{3a_1^2}{25} + \frac{3a_2}{10} - \frac{3q}{2}, \\ u_3 &= \frac{2a_1^3}{125} - \frac{3a_1a_2}{50} - \frac{a_1q}{10} + \frac{a_3}{10}, \\ u_4 &= -\frac{3a_1^4}{625} + \frac{3a_1^2a_2}{125} + \frac{a_1^2q}{5} - \frac{2a_1a_3}{25} - \frac{3qa_2}{5} + \frac{a_4}{5} + q^2, \\ \zeta_3 &:= e^{\frac{2\pi i}{3}}, \\ \eta &:= 5\left(-\frac{u_2^6}{27} - 5u_2^3u_3^2 + \frac{27u_3^4}{2} + i\frac{27|u_3|\left(-u_3^2 - \frac{4}{27}u_2^3\right)^{3/2}}{2}\right)^{1/3}. \end{aligned}$$

Define $S_\eta := \left\{\eta + \overline{\eta} + \frac{10u_2^2}{3}, \zeta_3\eta + \zeta_3^2\overline{\eta} + \frac{10u_2^2}{3}, \zeta_3^2\eta + \zeta_3\overline{\eta} + \frac{10u_2^2}{3}\right\} \subseteq \mathbb{R}$ and let $\theta_1 \le \theta_2 \le \theta_3$ be the three elements of S_η. If $u_3 = 0$, let x_{i_1,i_2} be

$$x_{i_1,i_2} = i_1\sqrt{-u_2 + i_2\sqrt{u_2^2 - u_4}},$$

for $i_1, i_2 \in \{+1, -1\}$. Otherwise, define

$$\begin{aligned} v_2 &= -\frac{u_2^2}{3} - u_4, \\ v_3 &= \frac{2u_2u_4}{3} - \frac{2u_2^3}{27} - 2u_3^2, \\ C &= \left(\frac{-v_3 + \sqrt{v_3^2 + \frac{4}{27}v_2^3}}{2} \right)^{1/3}, \\ y &= \begin{cases} \sqrt[3]{-v_3} - \frac{2u_2}{3} & \text{if } v_2 = 0, \\ C - \frac{v_2}{3C} - \frac{2u_2}{3} & \text{if } v_2 \neq 0, \end{cases} \end{aligned}$$

and let x_{i_1,i_2} for $i_1, i_2 \in \{+1, -1\}$ be defined by

$$x_{i_1,i_2} = \frac{i_1\sqrt{2y} + i_2\sqrt{-4u_2 - 2y - i_1\frac{8u_3}{\sqrt{2y}}}}{2}.$$

Note that under the conditions on a_1, a_2, a_3, a_4 below, all x_{i_1,i_2}'s will be real. Let $\gamma_1 \geq \gamma_2 \geq \gamma_3 \geq \gamma_4$ be equal to x_{i_1,i_2} with each a distinct pair (i_1, i_2), so that they are ordered. Let $\tilde{g}(x)$ be a polynomial defined by

$$\tilde{g}(x) = -x^5 - \frac{10}{3}u_2x^3 - 10u_3x^2 - 5u_4x,$$

and define

$$\begin{aligned} \lambda_1 &= \max\{\tilde{g}(\gamma_2), \tilde{g}(\gamma_4)\}, \\ \lambda_2 &= \min\{\tilde{g}(\gamma_1), \tilde{g}(\gamma_3)\}. \end{aligned}$$

Then $P(x)$ is q-Weil polynomial if and only if one of the following conditions holds:

1. *q is a square and $P(x) = (x + \sqrt{q})^2\tilde{P}(x)$ or $P(x) = (x - \sqrt{q})^2\tilde{P}(x)$, where $\tilde{P}(x)$ is a q-Weil polynomial of degree 8, see Theorem 9.2;*

2. *q is not a square and $P(x) = (x^2 - q)^4(x^2 + \omega x + \sqrt{q})$ with $\omega \in \mathbb{R}$, $|\omega| < 2\sqrt{q}$, or $P(x) = (x^2 - q)^2\tilde{P}(x)$, where $\tilde{P}(x)$ is a q-Weil polynomial of degree 6, see Theorem 8.2;*

3. *the following conditions hold:*

   (a) $|a_1| < 10\sqrt{q}$

   (b) $8\sqrt{q}|a_1| - 35\sqrt{q} < a_2 \leq \frac{2}{5}a_1^2 + 5q,$

   (c) $-\frac{4}{25}a_1^3 + \frac{3}{5}a_1a_2 + a_1q - \frac{1}{50}(4a_1^2 + 50q - 10a_2)^{3/2} \leq a_3 \leq -\frac{4}{25}a_1^3 + \frac{3}{5}a_1a_2 + a_1q + \frac{1}{50}(4a_1^2 + 50q - 10a_2)^{3/2},$

   (d) $-6\sqrt{q}a_2 - 20qa_1 - 50q\sqrt{q} < a_3 < 6a_2\sqrt{q} - 20qa_1 + 50q\sqrt{q},$

   (e) $\frac{3a_1^4}{125} - \frac{3a_1^2a_2}{25} - a_1^2q + \frac{2a_1a_3}{5} + 3qa_2 - 5q^2 + \theta_1 \leq a_4 \leq \frac{3a_1^4}{125} - \frac{3a_1^2a_2}{25} - a_1^2q + \frac{2a_1a_3}{5} + 3qa_2 - 5q^2 + \theta_2,$

   (f) $4\sqrt{q}|4qa_1 + a_3| - 9qa_2 - 25q^2 < a_4,$

   (g) $-\frac{4a_1^5}{3125} + a_1^3\left(\frac{15q+a_2}{125}\right) - \frac{a_1^2a_3}{25} + a_1\left(\frac{a_4-3qa_2-5q^2}{5}\right) + 2qa_3 + \lambda_1 \leq a_5 \leq -\frac{4a_1^5}{3125} + a_1^3\left(\frac{15q+a_2}{125}\right) - \frac{a_1^2a_3}{25} + a_1\left(\frac{a_4-3qa_2-5q^2}{5}\right) + 2qa_3 + \lambda_2,$

   (h) $-2\sqrt{q}a_4 - 2qa_3 - 2q\sqrt{q}a_2 - 2q^2a_1 - 2q^2\sqrt{q} < a_5 < 2\sqrt{q}a_4 - 2qa_3 + 2q\sqrt{q}a_2 - 2q^2a_1 + 2q^2\sqrt{q}.$

Remark 10.3. When comparing this result to the original result by Sohn [22, Theorem 2.1], one notable difference is in the non-strict bound for a_3, where Sohn was missing a term $50q$ inside the base with exponent $3/2$. Furthermore, similar to the original result for dimension 4 by Haloui and Singh [7], the q-Weil polynomials with real roots were missing and the bound for a_4 needed more attention to which of the cube

roots were chosen for the bounds of a_4. There also seems to be a typo in Sohn's result, where the strict and non-strict bounds for a_5 were merged and an extra bound for a_4 was written but nowhere explained.
After implementing my bounds [13] and comparing the resulting polynomials with the built-in SageMath 9.3 function by Kedlaya [11], my bounds missed some polynomials without real roots that contained a multiple root. These occurred due to precision errors, similar to the ones for degree 8, see Remark 9.3 and Corollary 7.6. Increasing the precision of the code solved this problem for the values of q for which the tests were done, but may still cause an issue for higher values of q.

10.2 Newton polygons

We want to determine the conditions for which a q-Weil polynomial of degree 10 corresponds to the characteristic polynomial of a simple abelian variety of dimension 5 over $\mathbb{F}_q$. This contents of this section was first determined by Hayashida [8]. Compared to the original result, the Newton polygons will be reordered based on p-rank and value of $v_p(a_5)$, similar to how Haloui and Haloui-Singh ordered their Newton polygons for dimension 3 and 4 respectively.
Firstly, since we only look at simple abelian varieties, the characteristic polynomial must be a power of an irreducible q-Weil polynomial. The positive divisors of 10 are $1, 2, 5$ and 10. Note that if the degree of a polynomial is odd, it will have a real root, which would not give a simple abelian variety of dimension 5, see Lemma 5.5. Hence, either the characteristic polynomial is of the form $(x^2 + ax + q)^5$, as in Theorem 6.3 or it is irreducible over $\mathbb{Q}$.

Let

$$P(x) = x^{10} + a_1x^9 + a_2x^8 + a_3x^7 + a_4x^6 + a_5x^5 + qa_4x^4 + q^2a_3x^3 + q^3a_2x^2 + q^4a_1x + q^5$$

be an irreducible q-Weil polynomial. We can use Corollary 6.8 to determine the conditions on the coefficients. The lattice points of $\mathbb{Z}\times n\mathbb{Z}$ that are under the line through $(0, 5n)$ and $(10, 0)$ with x-coordinate corresponding to the coefficients a_1, a_2, a_3, a_4 or a_5 are $(5, 0), (5, 1), (5, 2), (6, 0), (6, 1), (7, 0), (7, 1), (8, 0)$ and $(9, 0)$. These all give one construction of a possible Newton polygon. Constructions that can be made using multiple of these points are one with $(5, 1)$ and $(8, 0)$, another one with $(5, 1)$ and $(9, 0)$ and a third Newton polygon with $(6, 1)$ and $(9, 0)$. Together with the line through $(0, 5n)$ and $(10, 0)$, we get all possible Newton polygons, see Figure 8. This result was first determined by Hayashida [8, Theorem 1.3].

Theorem 10.4. *Let $P(x) = x^{10} + a_1x^9 + a_2x^8 + a_3x^7 + a_4x^6 + a_5x^5 + qa_4x^4 + q^2a_3x^3 + q^3a_2x^2 + q^4a_1x + q^5$ be a q-Weil polynomial. Then $P(x)$ is the characteristic polynomial of a simple abelian variety of dimension 5 over $\mathbb{F}_q = \mathbb{F}_{p^n}$ if and only if one of the following conditions holds:*

1. *n is a multiple of 5 and $P(x) = (x^2 + \omega x + q)^5$, where $|\omega| < 2\sqrt{q}$ and $\omega = kq^{1/5}$ or $\omega = kq^{2/5}$ with $k \in \mathbb{Z}$ not divisible by p,*

2. *the polynomial $P(x)$ is irreducible over $\mathbb{Q}$ and one of the following conditions holds:*

   (a) $v_p(a_5) = 0$,

   (b) $v_p(a_5) \geq n/2$, $v_p(a_4) = 0$ and $P(x)$ has no root of valuation $n/2$ in $\mathbb{Q}_p$,

   (c) $v_p(a_5) \geq n$, $v_p(a_4) \geq n/2$, $v_p(a_3) = 0$ and $P(x)$ has no root of valuation $n/2$ in $\mathbb{Q}_p$,

   (d) $v_p(a_5) = n$, $v_p(a_4) \geq 2n/3$, $v_p(a_3) \geq n/3$, $v_p(a_2) = 0$ and $P(x)$ has no root of valuation $n/3$ or $2n/3$ in $\mathbb{Q}_p$,

   (e) $v_p(a_5) \geq 3n/2$, $v_p(a_4) \geq n, v_p(a_3) \geq n/2, v_p(a_2) = 0$ and $P(x)$ has no root of valuation $n/2$ nor an irreducible factor of degree 3 in $\mathbb{Q}_p$,

   (f) $v_p(a_5) = n, v_p(a_4) \geq 3n/4, v_p(a_3) \geq n/2, v_p(a_2) \geq n/4, v_p(a_1) = 0$ and $P(x)$ has no root of valuation $n/4$ or $3n/4$ nor an irreducible factor of degree 2 in $\mathbb{Q}_p$,

   (g) $v_p(a_5) \geq 3n/2, v_p(a_4) = n, v_p(a_3) \geq 2n/3, v_p(a_2) \geq n/3, v_p(a_1) = 0$ and $P(x)$ has no root of valuation $n/3, n/2$ or $2n/3$ in $\mathbb{Q}_p$,

(h) $v_p(a_5) \geq 2n, v_p(a_4) \geq 3n/2, v_p(a_3) \geq n, v_p(a_2) \geq n/2, v_p(a_1) = 0$ *and* $P(x)$ *has no root of valuation* $n/2$ *nor an irreducible factor of degree* 3 *in* $\mathbb{Q}_p$*,*

(i) $v_p(a_5) = n, v_p(a_4) \geq 4n/5, v_p(a_3) \geq 3n/5, v_p(a_2) \geq 2n/5, v_p(a_1) \geq n/5$ *and* $P(x)$ *has no root nor a factor of degree* 2 *in* $\mathbb{Q}_p$*,*

(j) $v_p(a_5) \geq 3n/2, v_p(a_4) = n, v_p(a_3) \geq 3n/4, v_p(a_2) \geq n/2, v_p(a_1) \geq n/4$ *and* $P(x)$ *has no root and exactly one irreducible factor of degree* 2 *in* $\mathbb{Q}_p$*,*

(k) $v_p(a_5) \geq 2n, v_p(a_4) \geq 3n/2, v_p(a_3) = n, v_p(a_2) \geq 2n/3, v_p(a_1) \geq n/3$ *and* $P(x)$ *has no root in* $\mathbb{Q}_p$*,*

(l) $v_p(a_5) = 2n, v_p(a_4) \geq 8n/5, v_p(a_3) \geq 6n/5, v_p(a_2) \geq 4n/5, v_p(a_1) \geq 2n/5$ *and* $P(x)$ *has no root nor a factor of degree* 2 *in* $\mathbb{Q}_p$*,*

(m) $v_p(a_5) \geq 5n/2, v_p(a_4) \geq 2n, v_p(a_3) \geq 3n/2, v_p(a_2) \geq n, v_p(a_1) \geq n/2$ *and* $P(x)$ *has no root nor a factor of degree* 3 *or* 5 *in* $\mathbb{Q}_p$*.*

The abelian varieties corresponding to case (1) *have p-rank* 0*. Furthermore, the p-ranks of abelian varieties corresponding to cases* (2b), (2c), (2d), (2e), (2f), (2g), (2h), (2i), (2j), (2k), (2l), (2m) *are respectively* $5, 4, 3, 2, 2, 1, 1, 1, 0, 0, 0, 0, 0$*. The abelian varieties corresponding to* (2m) *are supersingular.*

Proof. The statements regarding the valuation of the coefficients follow immediately from the Newton polygons. Furthermore, by Corollary 6.12, we can also immediately see the p-ranks in each case.

Let $(5, 0)$ be a vertex, as in Figure 8a. Since the Newton polygon has two edges of horizontal length 5, we know $P(x)$ can be factored into two polynomials of degree 5 in $\mathbb{Q}_p$. These polynomials are allowed to be factored in any possible way in $\mathbb{Q}_p$, as every point on the Newton polygon with integer value x-coordinate is contained in the lattice.

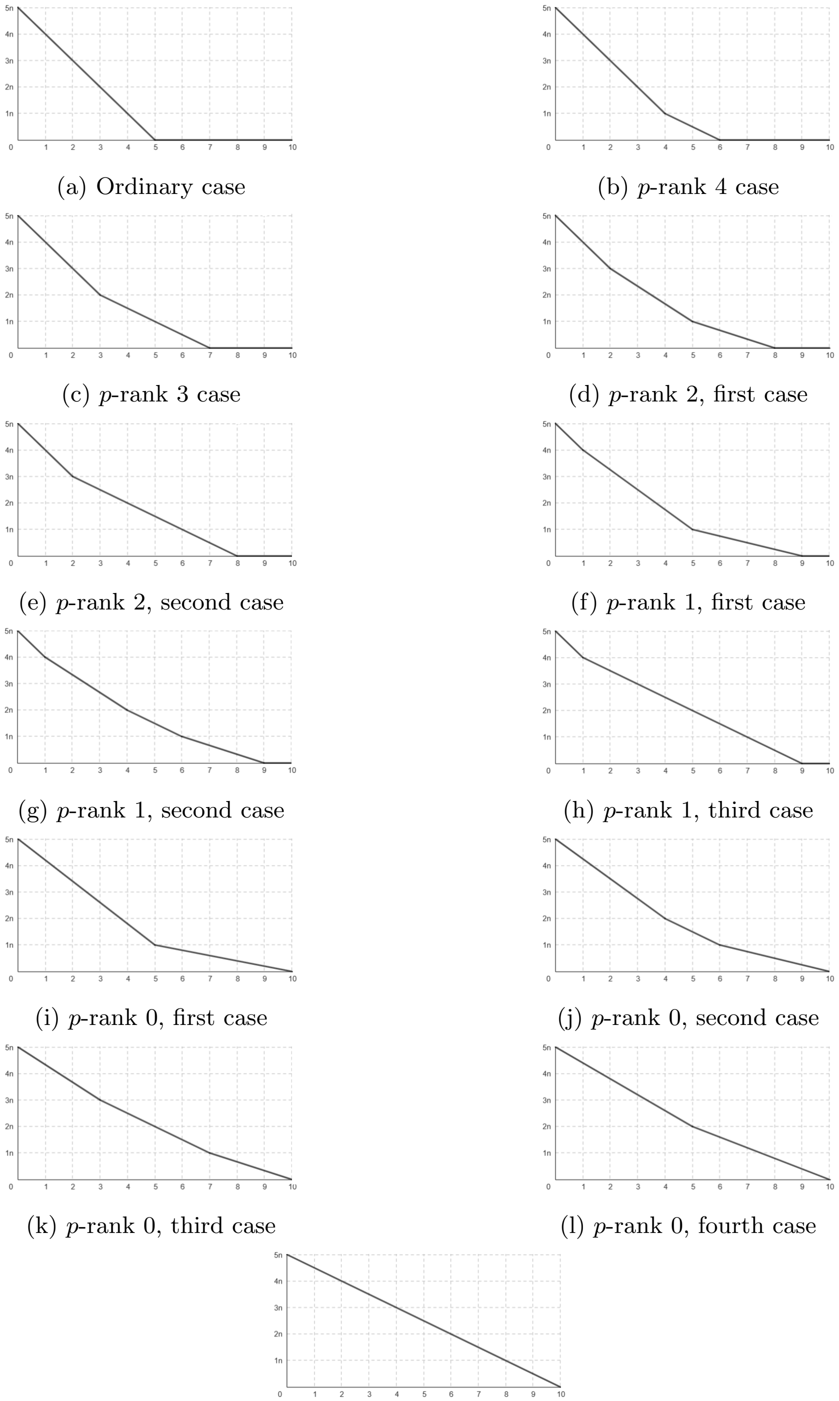
Now suppose $(6, 0)$ be a vertex, as in Figure 8b. The Newton polygon has two segments of horizontal length 4 and one of length 2, so $P(x)$ can be factored into a product of two degree 4 polynomials and one degree 2 polynomial in $\mathbb{Q}_p$. This Newton polygon passes through only lattice points at every integer value except for $x = 5$. The slope of this segment is $-n/2$ and it has horizontal length 2. Hence, anything regarding the factorisation of the degree 4 polynomials in $\mathbb{Q}_p$ is allowed, while the degree 2 polynomial must be irreducible in $\mathbb{Q}_p$. Equivalently, $P(x)$ has no root of valuation $n/2$ in $\mathbb{Q}_p$.

If $(7, 0)$ is a vertex, as in Figure 8c, the Newton polygon has two edges of horizontal length 3 and one of length 4. It follows that $P(x)$ is the product of two degree 3 polynomials and one degree 4 polynomial in $\mathbb{Q}_p$. Only the edge with horizontal length 4, which has slope $-n/2$, does not pass through lattice points, namely at $x = 4$ and $x = 6$. This means that the polynomial of degree 4 must not have a root. Equivalently, $P(x)$ has no root of valuation $n/2$ in $\mathbb{Q}_p$.

Now suppose $(5, 1)$ and $(8, 0)$ are both vertices as in Figure 8d. There are two edges of horizontal length 2 and two edges of length 3. The edges of length 2 only pass through lattice points at integer values of x, while the edges of length 3 only have their respective endpoints as lattice points. It follows that the degree 3 polynomials must be irreducible over $\mathbb{Q}_p$, while the polynomial of degree 2 is allowed to be reducible over $\mathbb{Q}_p$. The slope of the edges of length 3 are $-n/3$ and $-2n/3$, so equivalently $P(x)$ must not have a root of valuation $n/3$ or $2n/3$ in $\mathbb{Q}_p$.

Suppose that $(8, 0)$ is a vertex again, but not $(5, 1)$, as in Figure 8e. The two segments of horizontal length 2 only go through lattice points at integer values of x, while the segment of length 6 only passes through lattices points for even values of x. Hence, $P(x)$ is a product of two degree 2 polynomials and one degree 6 polynomial in $\mathbb{Q}_p$, where the degree 2 polynomials may be reducible and the degree 6 polynomial can only have factors of even degree. The edge of length 6 has slope $-n/2$, so equivalently $P(x)$ has no root of valuation $-n/2$ nor an irreducible factor of degree 3 in $\mathbb{Q}_p$.

Let $(5, 1)$ and $(9, 0)$ be vertices of the Newton polygon, see Figure 8f. Two segments of horizontal length 1 indicate two roots in $\mathbb{Q}_p$. Furthermore, the two segment of length 4 only go through lattice points at their respective endpoints. This indicates two irreducible polynomials of degree 4 of $P(x)$ in $\mathbb{Q}_p$. The slopes of these edges are $-n/4$ and $-3n/4$, so $P(x)$ cannot have a root of valuation $-n/4$ or $-3n/4$ nor can $P(x)$ have an irreducible factor of degree 2 in $\mathbb{Q}_p$.



(a) Ordinary case

(b) p-rank 4 case

(c) p-rank 3 case

(d) p-rank 2, first case

(e) p-rank 2, second case

(f) p-rank 1, first case

(g) p-rank 1, second case

(h) p-rank 1, third case

(i) p-rank 0, first case

(j) p-rank 0, second case

(k) p-rank 0, third case

(l) p-rank 0, fourth case

(m) Supersingular case

Figure 8: Newton polygons of irreducible characteristic polynomials of simple abelian varieties of dimension 5, c.f. [8].

Let both $(6,1)$ and $(9,0)$ be vertices of the Newton polygon, as in Figure 8g. Two edges of horizontal length 1 indicate two roots in $\mathbb{Q}_p$. Furthermore, the two edges of length 3 and the edge of length 2 only go through lattice points at their respective endpoints. This indicates two irreducible polynomials of degree 3 and one irreducible polynomial of degree 2 of $P(x)$ in $\mathbb{Q}_p$. The slopes of these edges are $-n/3, -n/2, -2n/3$, so $P(x)$

cannot have a root of valuation $n/3, n/2$ or $2n/3$ in $\mathbb{Q}_p$.

Now suppose $(9,0)$ is a vertex, but not $(5,1)$ or $(6,1)$, see Figure 8h. Again, two edges of horizontal length 1 indicate two roots in $\mathbb{Q}_p$. The edge of length 8 only passes through lattice points at every other integer value of x, which means that the corresponding polynomial factor of degree 8 of $P(x)$ in $\mathbb{Q}_p$ may only be factored into a product of polynomials of even degrees. The slope of this edge is $-n/2$. Hence, $P(x)$ cannot have a root of valuation $n/2$ nor an irreducible factor of degree 3 in $\mathbb{Q}_p$.

Let $(5,1)$ be a vertex, but $(8,0)$ and $(9,0)$ not, see Figure 8i. These two segments of length 5 only pass through lattice points at their respective endpoints. Hence, $P(x)$ factors in $\mathbb{Q}_p$ into a product of two irreducible degree 5 polynomials. Equivalently, $P(x)$ has no root nor an irreducible factor of degree 2 in $\mathbb{Q}_p$.

If $(6,1)$ is a vertex, but not $(9,0)$, as in Figure 8j, we have three segments which only pass through lattice points at their respective endpoints. The horizontal lengths are $4, 2$ and 4. Hence, $P(x)$ has two irreducible factors of degree 4 and one of degree 2 in $\mathbb{Q}_p$. Equivalently, $P(x)$ has exactly one factor of degree 2 and no roots in $\mathbb{Q}_p$.

If $(7,1)$ is a vertex, as in Figure 8k, there are two segments of horizontal length 3 and one of length 4 with the only lattice points being their endpoints and the middle point of the segment of length 4. Hence, the factorisation of $P(x)$ in $\mathbb{Q}_p$ consists of two irreducible polynomials of degree 3 and one of degree 4 or two of degree 2. Given the Newton polygon, it is equivalent to say that $P(x)$ has no roots in $\mathbb{Q}_p$.

Let $(5,2)$ be a vertex, see Figure 8l. There are two edges of length 5 and the only lattice points on the Newton polygon are the endpoints and the middle. Hence, $P(x)$ in $\mathbb{Q}_p$ must factor into a product of two irreducible polynomials of degree 5. Equivalently, given the Newton polygon, $P(x)$ has no roots nor a factor of degree 2 in $\mathbb{Q}_p$.

Lastly, suppose the Newton polygon is simply the line through $(0,5n)$ and $(10,0)$, as in Figure 8m. The line only passes through lattice points at even values of x. Hence, $P(x)$ may be factorisable in $\mathbb{Q}_p$ into a product of polynomials of even degrees, but not odd degrees. □

Bibliography

[1] Allen Altman and Steven Kleiman. *Introduction to Grothendieck duality theory.* Lecture Notes in Mathematics, Vol. 146. Springer-Verlag, Berlin-New York, 1970, pp. ii+185.

[2] Jeremy Bradford. *Commutative endomorphism rings of simple abelian varieties over finite fields.* Thesis (Ph.D.)–University of Maryland, College Park. ProQuest LLC, Ann Arbor, MI, 2012, p. 78. ISBN: 978-1303-01065-1.

[3] Taylor Dupuy et al. "Isogeny classes of abelian varieties over finite fields in the LMFDB". In: *Arithmetic geometry, number theory, and computation.* Simons Symp. Springer, Cham, 2021, pp. 375–448.

[4] Bart Edixhoven, Gerard v.d. Geer, and Ben Moonen. *Abelian Varieties (PRELIMINARY VERSION OF THE FIRST CHAPTERS).* [Online; accessed 5 November 2022]. URL: `http://van-der-geer.nl/~gerard/AV.pdf`.

[5] Josep González. "On the p-rank of an abelian variety and its endomorphism algebra". In: *Publicacions Matemàtiques* 42.1 (1998), pp. 119–130. ISSN: 0214-1493.

[6] Safia Haloui. "The characteristic polynomials of abelian varieties of dimensions 3 over finite fields". In: *Journal of Number Theory* 130.12 (2010), pp. 2745–2752. ISSN: 0022-314X.

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

[8] Daiki Hayashida. "The characteristic polynomials of abelian varieties of higher dimension over finite fields". In: *Journal of Number Theory* 196 (2019), pp. 205–222. ISSN: 0022-314X.

[9] Daiki Hayashida. "The characteristic polynomials of abelian varieties over finite fields". In: *Algebraic Number Theory and Related Topics 2018.* RIMS Kôkyûroku Bessatsu, B86. Res. Inst. Math. Sci. (RIMS), Kyoto, 2021, pp. 47–62.

[10] Taira Honda. "Isogeny classes of abelian varieties over finite fields". In: *Journal of the Mathematical Society of Japan* 20 (1968), pp. 83–95. ISSN: 0025-5645.

[11] Kiran S. Kedlaya. *root-unitary.* `https://github.com/kedlaya/root-unitary`. commit 4bcbb2a, [Online; accessed 20 March 2023]. 2019.

[12] Neal Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions.* Second. Vol. 58. Graduate Texts in Mathematics. Springer-Verlag, New York, 1984, pp. xii+150. ISBN: 0-387-96017-1.

[13] Jun Jie Lin. *Isogeny-Classes-of-Abelian-Varieties-over-Finite-Fields.* `https://github.com/Jun-Jie-Lin/Isogeny-Classes-of-Abelian-Varieties-over-Finite-Fields`. 2023.

[LMFDB] The LMFDB Collaboration. *The L-functions and modular forms database.* `https://www.lmfdb.org`. [Online; accessed 9 June 2023]. 2023.

[14] Daniel Maisner and Enric Nart. "Abelian surfaces over finite fields as Jacobians". In: *Experimental Mathematics* 11.3 (2002). With an appendix by Everett W. Howe, pp. 321–337. ISSN: 1058-6458.

[15] James S. Milne. *Abelian Varieties (v2.00).* [Online; accessed 5 November 2022]. 2008. URL: `https://www.jmilne.org/math/CourseNotes/av.html`.

[16] James S. Milne. *Étale cohomology.* Princeton University Press, Princeton, N.J.,, 1980, pp. xiii+323. ISBN: 0-691-08238-3.

[17] Hans-Georg Rück. "Abelian surfaces and Jacobian varieties over finite fields". In: *Compositio Mathematica* 76.3 (1990), pp. 351–366. ISSN: 0010-437X.

[18] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.3).* `https://www.sagemath.org`, [Online; downloaded 5 April 2022]. 2023.

[19] Joseph H. Silverman. *The arithmetic of elliptic curves.* Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009, pp. xx+513. ISBN: 978-0-387-09493-9.

[20] Christopher Smyth. “Totally positive algebraic integers of small trace”. In: *Université de Grenoble. Annales de l’Institut Fourier* 34.3 (1984), pp. 1–28. ISSN: 0373-0956.

[21] Gyoyong Sohn. “The bounds of the coefficients of the characteristic polynomials for abelian varieties of dimension 5 over finite fields”. In: *Advanced Studies in Contemporary Mathematics (Kyungshang). Memoirs of the Jangjeon Mathematical Society* 23.3 (2013), pp. 415–421. ISSN: 1229-3067.

[22] Gyoyong Sohn. “The Newton polygons of the characteristic polynomials for abelian varieties of dimension 5 over finite fields”. In: *Advanced Studies in Contemporary Mathematics (Kyungshang). Memoirs of the Jangjeon Mathematical Society* 23.4 (2013), pp. 655–660. ISSN: 1229-3067.

[23] John Tate. “Classes d’isogénie des variétés abéliennes sur un corps fini (d’après T. Honda)”. In: *Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363*. Vol. 175. Lecture Notes in Math. Springer, Berlin, 1971, Exp. No. 352, 95–110.

[24] John Tate. “Endomorphisms of abelian varieties over finite fields”. In: *Inventiones Mathematicae* 2 (1966), pp. 134–144. ISSN: 0020-9910.

[25] William C. Waterhouse. “Abelian varieties over finite fields”. In: *Annales Scientifiques de l’École Normale Supérieure. Quatrième Série* 2 (1969), pp. 521–560. ISSN: 0012-9593.

[26] William C. Waterhouse and James S. Milne. “Abelian varieties over finite fields”. In: *1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969)*. Amer. Math. Soc., Providence, R.I., 1971, pp. 53–64.

[27] André Weil. “Numbers of solutions of equations in finite fields”. In: *Bulletin of the American Mathematical Society* 55 (1949), pp. 497–508. ISSN: 0002-9904.

[28] Chao Ping Xing. “The characteristic polynomials of abelian varieties of dimensions three and four over finite fields”. In: *Science in China (Scientia Sinica). Series A. Mathematics, Physics, Astronomy* 37.2 (1994), pp. 147–150. ISSN: 1001-6511.