GROUP STRUCTURE OF ABELIAN VARIETIES

PATRICK MEISNER

Abstract. Let $A$ be an abelian variety over $\mathbb{F}_q$. Let $h_A(t)$ be the characteristic polynomial of $A$. Rybakov (in [Ryb]) showed that if $h_A(t)$ is squarefree and $G$ is any finite group with $|G| = h_A(1)$, then $G = A'(\mathbb{F}_q)$ for some $A'$ isogenous to $A$ if and only if the $\ell$-th Hodge polygon of $G$ is under the $\ell$-th Newton polygon of $h_A(1-t)$ for all primes $\ell$. In this paper, we will extend this result to get a classification theorem for the group structure of all abelian varieties.

1. Introduction

Let $0 \leq m_1 \leq \cdots \leq m_r$ be nonnegative integers and let $H = \oplus_{i=1}^r \mathbb{Z}/\ell^{m_i}\mathbb{Z}$ be an abelian group of order $\ell^m$, where $\ell$ is a prime. The Hodge polygon, $H_p(H)$, of $H$ is the convex polygon with vertices $(i, \sum_{j=1}^{i-1} m_j)$, $i = 0, \ldots, r$. It has $(0,m)$ and $(r,0)$ as its endpoints and its slopes are $-m_r, \ldots, -m_1$.

If $H = \oplus_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}$ where $n_{i-1} | n_i$ then define $H_\ell = \oplus_{i=1}^r \mathbb{Z}/\ell^{e_i(n_i)}\mathbb{Z}$, the $\ell$-th primary part of $H$. Then the $\ell$-th Hodge polygon of $H$ is $H_p(H) = H_p(H_\ell)$.

Let $f(t) = t^n + a_1 t^{n-1} + \cdots + a_n$ be a polynomial. We define the $\ell$-th Newton Polygon of $f(T)$, $N_p(f(t))$, to be the convex hull of the points $(i, v_\ell(a_{i-n}))$, $i = 0, \ldots, n$. It has $(0, v_\ell(0))$ and $(n,0)$ as its endpoints.

Remark. In this paper, our groups will be $A(k)_\ell$, the $\ell$-th torsion of the $k = \mathbb{F}_q$ points of an Abelian variety, and $f(t) = h_A(1-t)$, where $h_A$ is the characteristic polynomial. Thus the Hodge polygons and the Newton polygons will have the same endpoint $(0, h_A(1))$ and $(2g,0)$, where $g$ is the genus of $A$.

Rybakov (in [Ryb]) first proved that if an abelian variety, $A$, defined over a finite field, $k = \mathbb{F}_q$, has a square-free characteristic polynomial, $h_A(t)$, then $H_\ell(A(k))$ must lie under $N_p(h_A(1-t))$. Furthermore, he showed that all groups whose $\ell$-th Hodge polygon lies under $N_p(h_A(1-t))$ can occur in the isogeny class of $A$.

To prove that $H_\ell(A(k))$ lies under $N_p(h_A(1-t))$, Rybakov uses the fact that $A(k)_\ell \cong T_\ell(A)/(1-F)T_\ell(A)$, where $T_\ell(A)$ is the Tate-module, and a result by Weyl that says that the Hodge polygon of the cokernel of a function of a $\mathbb{Z}_\ell$-module lies under the $\ell$-th Newton polygon of its characteristic polynomial. To show that all groups such that $H_\ell(G)$ lies under $N_p(h_A(1-t))$ can occur, he constructed a basis, $\beta$, for $T_\ell(A) \otimes \mathbb{Q}_\ell$ and let $T = \text{span}_{\mathbb{Z}_\ell}(\beta)$ such that $T/(1-F)T = G$ and then use the following well-known lemma to say that $T \cong T_\ell(A')$ for some $A' \sim A$ (Lemma 1 from [Ryb]).

Lemma 1.1. If $T$ is a $\mathbb{Z}_\ell$ module such that $T \otimes \mathbb{Q}_\ell \cong T_\ell(A) \otimes \mathbb{Q}_\ell$ and $F_A(T) \subset T$ where $F_A$ is the Frobenius map for $A$, then $T \cong T_\ell(A')$ for some $A' \sim A$.

1
Remark. In Rybakov’s proof, he used the fact the characteristic polynomial was squarefree only to prove that all groups occur, and he proves that the Hodge polygon of \( A(k)_\ell \) lies under the \( \ell^{th} \) Newton polygon of \( h_A(1-t) \) for all abelian varieties.

In the Section 2, we will extend Rybakov’s result to the case where the characteristic polynomial is a power of a squarefree. In particular we will prove

**Theorem 1.2.** Let \( A \) be an abelian variety such that \( h_A(t) = f_A(t)^r \), \( f_A \) squarefree. Then,

\[
A(k)_\ell \cong G_1 \oplus \cdots \oplus G_e
\]

where \( H_p(G_i) \) lies under \( N_p(f_A(1-t)) \). Furthermore, all such groups may occur as the \( \ell^{th} \) torsion of an abelian variety in the isogeny class. Hence

\[
A(k) \cong G'_1 \oplus \cdots \oplus G'_e
\]

such that \( H_p(G_i) \) lies under \( N_p(h_A(1-t)) \) for all \( i \) and all primes \( \ell \). Furthermore all such groups may occur.

To state the next Theorem which applies to all \( h_A(t) \) not necessarily squarefree, we first need a definition. We say that an abelian group \( B \), is an extension of \( C \) by \( A \) if there exists an exact sequence

\[
0 \to A \to B \to C \to 0.
\]

We will write this as \( B \in \text{Ext}(C, A) \).

In Section 3 we will use Theorem 1.2 and an induction argument to determine all possible group structures of abelian varieties. In particular we will prove

**Theorem 1.3.** Let \( A \) be an abelian variety with characteristic polynomial \( h_A(t) = P_1^{e_1}(t) \cdots P_n^{e_n}(t) \) where the \( P_i(t) \) are squarefree and coprime. If \( n = 1 \), then the groups that appear are classified in Theorem 1.2. If \( n \geq 2 \) then \( G = A'(k) \) for some \( A \sim A' \) if and only if

\[
G = \text{Ext}(G_1, \text{Ext}(G_2, \ldots \text{Ext}(G_{n-1}, G_n)))
\]

where \( G_i = G_{i,1} \oplus \cdots \oplus G_{i,e_i} \), such that \( H_p(G_{i,j}) \) is under \( N_p(P_i(1-t)) \) for all \( i,j \).

Remark. The \( G_{i,j} \) appearing in Theorem 1.3 are \( \ell \)-groups. Thus when we write \( H_p(G_{i,j}) \), it is implied that it is the \( \ell^{th} \) Hodge polygon.

2. Power of a Squarefree

In this section we will prove Theorem 1.2. But first, we will generalize Rybakov’s proof to prove a more general result.

**Theorem 2.1.** Let \( A \) be an abelian variety over \( k \) with characteristic polynomial \( h_A(t) \). Write \( h_A(t) = P_1(t)^{e_1} \cdots P_n(t)^{e_n} \), such that all the \( P_i \) are squarefree and coprime. Let \( G \) be a group such that \( |G| = h_A(1) \) and

\[
G = G_{1,1} \oplus \cdots \oplus G_{1,e_1} \oplus \cdots \oplus G_{n,1} \oplus \cdots \oplus G_{n,e_n}
\]

where the Hodge-polygon of \( G_{i,j} \) lies under the \( \ell^{th} \) Newton polygon of \( P_i(1-t) \) for all \( j \). Then there exists an \( A' \sim A \), such that \( A'(k)_\ell \cong G_\ell \) for all \( \ell \).

The idea for this proof is to use the basis constructed by Rybakov in the case of a squarefree characteristic polynomial for each component of the vector space \( V_\ell(A) = T_\ell(A) \otimes \mathbb{Q}_\ell \).
Proof of Theorem 2.1. Since $F$ acts semisimply on $V_{\ell}(A) = T_{\ell}(A) \otimes \mathbb{Q}_\ell$, we have that $1 - F$ acts semisimply with characteristic polynomial $h_A(1 - t) = P_1(1 - t)^{e_1} \cdots P_n(1 - t)^{e_n}$, and therefore,

$$V_{\ell}(A) \cong (\mathbb{Q}_\ell[t]/(P_1(1 - t)))^{e_1} \oplus \cdots \oplus (\mathbb{Q}_\ell[t]/(P_n(1 - t)))^{e_n}$$

where $1 - F$ acts by multiplication by $t$ on each component.

We restrict our attention to just the first component $\mathbb{Q}_\ell[t]/(P_1(1 - t))$. Let $P_1(1 - t) = t^d + b_1 t^{d-1} + \cdots + b_{d-1} t + P_1(1)$. Suppose we have numbers $m_1, \ldots, m_d$ such that, for each $i$, $m_1 + \cdots + m_i \leq \text{ord}_e(b_i)$ and $m_1 + \cdots + m_d = \text{ord}_e(P_1(1))$.

We construct these $m_i$ specifically so that the Hodge polygon associated to the $m_i$ lies under the Newton polygon $P_1(1 - t)$ with the same endpoints. Then we can construct an ordered basis of $\mathbb{Q}_\ell[t]/(P_1(1 - t))$

$$\{v_1, \ldots, v_d\} = \{e^{m_2 + \cdots + m_d}, e^{m_2 + \cdots + m_{d-1}} \ell t, \ldots, e^{m_2 \ell^2 - 2} - \ell^d - 1\}.$$

Now, since $1 - F$ acts like $t$, we get for $i \neq d$

$$(1 - F)v_i = e^{m_2 + \cdots + m_{d-1} + 1} t^{i+2} = e^{m_d - i+1} v_{i+1}.$$

Further,

$$(1 - F)v_d = -t^d = b_1 t^{d-1} + b_2 t^{d-2} + \cdots + b_{d-1} t + P_1(1)$$

$$= -b_1 v_d + \frac{b_2}{\ell m_2} v_{d-1} + \cdots + \frac{b_{d-1}}{\ell m_2 \cdots + m_{d-1}} v_2 + e^{m_1} v_1. $$

Now, by our choices of $m_i$, we get that $(1 - F)v_d \in \mathbb{Q}_\ell \text{ span}_{\mathbb{Z}}(v_1, \ldots, v_d)$

Thus, if we let $T_{i,1} = \text{span}_{\mathbb{Z}}(v_1, \ldots, v_d)$, we get

$$(1 - F)v_{d-i+1} \in \mathbb{Q}_\ell T_{i,1}^{m_i} \text{ for } i \neq 1 \text{ and } (1 - F)v_d \in \mathbb{Q}_\ell T_1^{m_1}.$$

If we do this for all the components and let $T_\ell$ be $\bigoplus T_{i,j}$. Then there exists an isogenous abelian variety $A'$ such that $T_\ell(A') \cong T_\ell$ by lemma 1.1. Thus there exists a surjective map from $T_\ell(A')/(1 - F)T_\ell(A')$ to

$$G = G_{1,1} \oplus \cdots \oplus G_{i,e_i} \oplus \cdots \oplus G_{n,1} \oplus \cdots \oplus G_{n,e_n}$$

where $G$ satisfies the statement of the theorem. Since they have the same size, these groups must be isomorphic. Further, our choice of $m_i$ was arbitrary so any group satisfying those conditions can occur.

\[ \square \]

In [Ryb], Rybakov showed that these are all the groups occurring in the special case $n = 1 = e_1$. We now prove Theorem 1.2 which shows that these are all the groups occurring when $n = 1$ and $P_1(t)$ is squarefree.

Proof of Theorem 1.2. Theorem 2.1 shows that if we have a group satisfying the conditions of the theorem then there exists an $A' \sim A$ such that $A'(k) \cong G$. So it remains to show that if $A$ is an abelian variety then $A(k)$ satisfies the conditions of the theorem.

If we write $f_A = \prod_{i=1}^n f_i$, with $f_i$ irreducible over $\mathbb{Q}_\ell$, and we let $\pi_i$ be a root of $f_i$, then, by a paper by Waterhouse and Milne ([WM]), we get

$$\text{End}(T_\ell(A)) \otimes \mathbb{Q}_\ell \cong \bigoplus M_{e_i}(\mathbb{Q}_\ell(\pi_i)).$$
and under this isomorphism, \( F \) gets mapped to
\[
\begin{bmatrix}
\pi_1 & & \\
& \ddots & \\
& & \pi_1
\end{bmatrix},
\]
\[
\begin{bmatrix}
1 & & \\
& \ddots & \\
& & 1
\end{bmatrix},
\]
\[
\begin{bmatrix}
1 & & \\
& \ddots & \\
& & 1
\end{bmatrix},
\]
i.e the inverse image of the matrices with 1 \(-\pi_j \) in the \( i^{th} \) diagonal, 1 on the other diagonals and 0 everywhere else.

Then \( 1 - F = \prod_{i=1}^e E_i \). The idea is to use a Chinese Remainder Theorem argument to show that \( A(k) \cong T_k(A)/(1 - F)T_k(A) \cong \bigoplus_{i=1}^e T_k(A)/E_iT_k(A) \).

To do this we must show two things: that \( E_i \in \text{End}(T_k(A)) \) (so that the quotient actually makes sense), and that the \( E_i \)'s are ”coprime”.

We know that \( E_i \in \text{End}(T_k(A)) \otimes \mathbb{Q}_\ell \), but we would like to show that \( E_i \in \text{End}(T_k(A)) \). Write \( E_i = M_i \otimes \ell^{n_i} \), where \( M_i \in \text{End}(T_k(A)) \) but \( M_i/\ell \notin \text{End}(T_k(A)) \) so that \( E_i \in \text{End}(T_k(A)) \) if and only if \( n_i \geq 0 \). Further we know
\[
1 - F = \prod E_i = (\prod M_i) \otimes \ell^{\sum n_i} \in \text{End}(T_k(A)).
\]

Now, suppose that \( n_i < 0 \) for all \( i \). Then we have that \( \sum n_i \leq -e \). However, by our choice of \( M_i \), we have \( (\prod M_i)/\ell^e \notin \text{End}(T_k(A)) \). That is, \( (\prod M_i) \otimes \ell^{\sum n_i} \notin \text{End}(T_k(A)) \), a contradiction. Hence, WLOG, \( n_1 \geq 0 \), and therefore \( E_1 \in \text{End}(T_k(A)) \).

The idea here is to then say that \( (1 - F)/E_1 \in \text{End}(T_k(A)) \) and then use an induction argument to show that all the \( E_i \in \text{End}(T_k(A)) \) for all \( i \). Now, \( E_1 \in \text{End}(T_k(A)) = \text{End}(A) \otimes \mathbb{Z}_\ell \), so there must an \( M \in \text{End}(A) \) and a \( \ell \in \mathbb{Z}_\ell \) such that \( E_1 = M \otimes \ell \). Now, \( \ker(M) \subset \ker(E_1) \subset \ker(1 - F) \), hence \( M \) is separable and we get that \( (1 - F)/M \in \text{End}(T_k(A)) \). Therefore, \( \prod_{i=2}^e E_i = (1 - F)/E_1 = (1 - F)/M \otimes 1/\ell \in \text{End}(T_k(A)) \otimes \mathbb{Q}_\ell \), and by induction then, \( E_i \in \text{End}(T_k(A)) \) for all \( i \).

Consider the map
\[
\psi : T_k(A)/(\prod_{i=1}^e E_i)T_k(A) \rightarrow \bigoplus_{i=1}^e T_k(A)/E_iT_k(A)
\]
\[
v \mapsto \left( v \mod E_1T_k(A), \ldots, v \mod E_eT_k(A) \right).
\]

Suppose that \( v \in \ker(\psi) \), then \( v \in E_iT_k(A) \) for all \( i \). But by the construction of the \( E_i \)'s, we can see that this means that \( v \in (\prod_{i=1}^e E_i)T_k(A) \), that is \( v \equiv 0 \). Thus \( \psi \) is injective. Now, we know that \( |T_k(A)/(\prod_{i=1}^e E_i)T_k(A)| = h_A(1) = f_A(1)^e \).

Further, the characteristic polynomial of each of the \( E_i \) is \( f_A(1 - t)(1 - t)^{2g - d} \),
(d = \text{deg}(f_A), g the genus of A) so \(|T_\ell(A)/E_iT_\ell(A)| = f_A(1)\) and so

\[|T_\ell(A)/(\prod_{i=1}^c E_iT_\ell(A))| = |\oplus_{i=1}^c T_\ell(A)/E_iT_\ell(A)|.\]

Therefore, \(\psi\) must be surjective and hence an isomorphism.

Finally, since the characteristic polynomial of \(E_i\) is \(f_A(1-t)(1-t)^{2g-d}\), then the Hodge polygon of \(T_\ell(A)/E_iT_\ell(A)\) lies under the Newton polygon of \(f_A(1-t)(1-t)^{2g-d}\) which is the same as the Newton polygon of \(f_A(1-t)\). This completes the proof of Theorem 1.2.

\[\square\]

**Remark.** We could have defined some other functions, \(F_i\), to be the inverse image of

\[\begin{pmatrix} 1 & \cdots & \pi_1 \\ \vdots & \ddots & \vdots \\ \pi_n & \cdots & 1 \end{pmatrix}\]

with \(\pi_j\) in the \(i\)th diagonal. Then we would have \(\prod_{i=1}^c F_i = F\). Further we could also define for \(I \subset \{1, \ldots, e\}\), \(F_I = \prod_{i \in I} F_i\) (likewise \(E_I\)). Then if \(I, J \subset \{1, \ldots, e\}\) such that \(I \cap J = \emptyset\) and \(I \cup J = \{1, \ldots, e\}\), then we get \(E_I F_J = F_{I+J} = \text{id}\). Using this we could have constructed an inverse map to the \(\psi\) function above in the same manner of the Chinese Remainder Theorem. However, we would need \(F_i \in \text{End}(T_\ell(A))\) but the argument we used for the \(E_i\) wouldn’t work as if we write \(F_i = M_i \otimes u_\ell\) for some \(M_i \in \text{End}(A)\) and \(u_\ell \in \mathbb{Z}_\ell^*\), then \(M_i\) is almost guaranteed to not be separable when \(\ell = p\).

With some condition on \(h_A\) (\(h_A(1)\) squarefree in [Ry], \(h_A(t) = f_A(t)^r\) here) only those groups described in Theorem 2.1 can occur, but this is not true in general as show in [Ry]. We reproduce his nice counterexample here for completeness.

Let \(h_A(t) = (t^2 - 2t + 9)(t + 3)^2\) be the characteristic polynomial of an abelian variety over \(\mathbb{F}_9\) that is isogenous to the product of two non-isogenous elliptic curves. Then \(h_A(1-t) = (t^2 + 8)(t - 4)^2\) and, if the construction in Theorem 2.1 were all the possible cases, then all such abelian varieties would have the group structure \(\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}\) such that \(n = 1\) or \(2\) and \(m = 8/n\). We will show that this is not true by constructing a module that gives rise to a group structure not of this form.

By the construction in Theorem 2.1, we get that we can find a basis for \(V_\ell(A)\), \(v_1, v_2, v_3, v_4\) such that \((1 - F)v_1 = 2v_2, (1 - F)v_2 = -4v_1, (1 - F)v_3 = 4v_3, (1 - F)v_4 = 4v_4\). Thus if we let \(T\) be the module over \(\mathbb{Z}_\ell\) spanned by this basis we get that \(T\) corresponds to an abelian variety whose groups structure is

\[\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}\]

Now, if we take the new basis \(u_1 = v_1 + v_3, u_2 = -4v_2 + 4v_3, u_3 = v_2 + v_4, u_4 = 4v_1 + 2v_4\). Then a quick calculation gives

\[(1 - F)u_1 = 4u_1 + 2u_3 - u_4\]

\[(1 - F)u_2 = 16u_1\]

\[\text{GROUP STRUCTURE OF ABELIAN VARIETIES} 5\]
(1 - F)u_3 = 4u_1 - u_2 + 4u_3
(1 - F)u_4 = 8u_3

Then if $T'$ is the module spanned over $\mathbb{Z}_\ell$ over this new basis, we get it corresponds to a new abelian variety whose group structure is

$$Z/8Z \oplus Z/16Z,$$

which clearly does not come from the construction of Theorem 2.1. Instead we need a more general description of the groups of abelian varieties with more general characteristic polynomials.

We will generalize this later and find all possible groups that can occur as an abelian variety over $\mathbb{F}_9$ with characteristic polynomial $h_A(t) = (t^2 - 2t + 9)(t + 3)^2$.

3. Proof of Theorem 1.3

To prove Theorem 1.3, we will need this theorem which is the content of section 2 of a paper by Fulton ($[Ful]$).

\textbf{Theorem 3.1.} Let $T_1, T_2, T_3$ be $\mathbb{Z}_\ell$-modules such that

$$0 \to T_1 \to T_2 \to T_3 \to 0$$

Let $V_i = T_i \otimes \mathbb{Q}_\ell$. Then $V_2 \cong V_1 \oplus V_3$ and let $E_i$ be endomorphisms on $T_i$ such that when viewed as endomorphism of $V_i$, $E_2 = E_1 \oplus E_3$. By the snake lemma, we get an exact sequence of cokernels

$$0 \to T_1/E_1T_1 \to T_2/E_2T_2 \to T_3/E_3T_3 \to 0.$$  

Conversely suppose $A, B, C$ are finite groups with an exact sequence

$$0 \to A \to B \to C \to 0$$

and such that there exists $T_1, T_3 \mathbb{Z}_\ell$-modules and $E_1, E_3$ endomorphism such that

$$T_1/E_1T_1 \cong A \quad \text{and} \quad T_3/E_3T_3 \cong C.$$  

Then there exists $T_2$ and an endomorphism $E_2$ such that

$$0 \to T_1 \to T_2 \to T_3 \to 0,$$

and $E_2 = E_1 \oplus E_3$ as viewed as an endomorphism of $V_2 = T_2 \otimes \mathbb{Q}_\ell$ and $T_2/E_2T_2 \cong B$.

Before we begin the proof of Theorem 1.3, we define, for any abelian variety $A$, $V_t(A) = T_t(A) \otimes \mathbb{Q}_\ell$

\textbf{Proof of Theorem 1.3.} We will prove Theorem 1.3 by induction on $n$ (the number of squarefree coprime polynomial appearing in the characteristic polynomial).

When $n = 1$, the work is done by Theorem 1.2. So we can continue with the proof by induction.

Assume that if $h_A = P_{n}^{e_1} \cdots P_{n-1}^{e_{n-1}}$ then $G = A(k)$ if and only if $G_{\ell} \in Ext(G_1, \ldots, Ext(G_{n-2}, G_{n-1}))$ where $G_i = G_{i,1} \oplus \cdots \oplus G_{i,e_i}$ such that $H_p(G_{i,j})$ lies under $N_{p}(P_l(1-t))$ for all $i, j$.

Let $h_A = P_{n}^{e_1} \cdots P_{n}^{e_n}$. Let $F_A$ be the Frobenius endomorphism on $A$, and let $E = P_1(1 - F_A) \cdots P_{n-1}(1 - F_A)$. Define $T_1 := \ker(E)$ and $T_2 := \im(E)$. Then we get an exact sequence

$$0 \to T_1 \to T_2 \to T_2 \to 0.$$. 
Further $1 - F_A$ acts semisimply on $T_1$ and $T_2$ with characteristic polynomials $P_1 \ldots P_{n-1}$, respectively. Thus we get that
\begin{align*}
T_1 \otimes \mathbb{Q}_\ell &\cong (\mathbb{Q}_\ell[t]/P_1(t)\mathbb{Q}_\ell[t])^{e_1} \oplus \cdots \oplus (\mathbb{Q}_\ell[t]/P_{n-1}(t)\mathbb{Q}_\ell[t])^{e_{n-1}} \cong V_\ell(B) \\
T_2 \otimes \mathbb{Q}_\ell &\cong (\mathbb{Q}_\ell[t]/P_n(t)\mathbb{Q}_\ell[t])^{e_n} \cong V_\ell(C)
\end{align*}
for some abelian varieties $B$ and $C$ with characteristic polynomials $P_1^{e_1} \ldots P_{n-1}^{e_{n-1}}$ and $P_n^{e_n}$, respectively. Further, $V_\ell(A) \cong V_\ell(B) \oplus V_\ell(C)$, with $1 - F_A = (1 - F_B, 1 - F_C)$. That is $1 - F_A$ acts on $T_1$ (respectively $T_2$) by $1 - F_B$ (respectively $1 - F_C$). Therefore $(1 - F_B)(T_1) \subset T_1$ and since $T_1 \otimes \mathbb{Q}_\ell \cong V_\ell(B)$, we get that $T_1 \cong T_\ell(B')$ for some $B' \sim B$. Likewise $T_2 \cong T_\ell(C')$ for some $C' \sim C$. (WLOG assume $B' = B$ and $C' = C$).

Hence $T_1/(1 - F_A)(T_1) = T_1/(1 - F_B)(T_1) = B(k)_\ell$ and $T_2/(1 - F_A)(T_2) = T_2/(1 - F_C)(T_2) = C(k)_\ell$ and we have the exact sequence
\[ 0 \to B(k)_\ell \to A(k)_\ell \to C(k)_\ell \to 0. \]

By induction we know that
\[ C(k)_\ell \cong G_1 \]
\[ B(k)_\ell \in \text{Ext}(G_2, \text{Ext}(G_3, \ldots \text{Ext}(G_{n-1}, G_n))). \]
where the $G_i$ have the required property. Hence
\[ A(k)_\ell \in \text{Ext}(G_1, \text{Ext}(G_2, \ldots \text{Ext}(G_{n-1}, G_n))). \]

Conversely, suppose we have a group $G \in \text{Ext}(G_1, \text{Ext}(G_2, \ldots \text{Ext}(G_{n-1}, G_n)))$ we want to show there exists an $A'$ such that $A' \sim A$ with $A'(k)_\ell \cong G$. Then there exists an $H \in \text{Ext}(G_2, \text{Ext}(G_3, \ldots \text{Ext}(G_{n-1}, G_n)))$ such that we have the exact sequence
\[ 0 \to H \to G \to G_1 \to 0. \]

We know by induction that there exists abelian varieties $B, C$ such that
\[ B(k)_\ell \cong T_\ell(B)/(1 - F_B)T_\ell(B) \cong H \]
\[ C(k)_\ell \cong T_\ell(C)/(1 - F_C)T_\ell(C) \cong G_1. \]

Hence by Theorem 3.1 we can find a module $T$ such that $E = (1 - F_B)(1 - F_C)$ is an endomorphism, $T/ET \cong G$ and
\[ 0 \to T_\ell(B) \to T \to T_\ell(C) \to 0. \]

So it remains to show that $T \cong T_\ell(A)$ for some abelian variety $A$. If we tensor the above exact sequence with $\mathbb{Q}_\ell$, we get
\[ 0 \to V_\ell(B) \to T \otimes \mathbb{Q}_\ell \to V_\ell(C) \to 0. \]

Thus $T \otimes \mathbb{Q}_\ell \cong V_\ell(B) \oplus V_\ell(C) \cong V_\ell(A)$. Further from here we can see the $(1 - F_A) = (1 - F_B, 1 - F_C) = (1 - F_B)(1 - F_C) = E$. That is $(1 - F_A)(T) \subset T$. Hence $T \cong T_\ell(A')$ for some abelian variety $A' \sim A$ by Lemma 1.1, completing Theorem 1.3.

\[ \square \]

Remark. We could have stated the Theorem 1.3 without the extra condition for when $n = 1$. For when $n = 1$, there is no $(n - 1)^{st}$ polynomial and thus, vacuously, $G_{n-1}$ must be the constant monic polynomial (i.e. 1). Thus the Theorem states that if $G$ appears as a group of the isogeny class then $G \in \text{Ext}(0, G_1)$, but the extensions of $G_1$ by 0 would just be $G_1$ itself. That is it says that if $h_A = P^e$ is a
power of a squarefree polynomial then $G$ appears as group of the isogeny class if and only if

$$G \cong G_1 \oplus \cdots \oplus G_e$$

where the Hodge polygon of $G_i$ lies under the $\ell^\text{th}$ Newton polygon of $P$, which is exactly Theorem 1.2.

4. Comments on Ext

We have shown that we can classify the groups appearing as abelian varieties over finite fields in terms of extensions of some specific groups. So it remains to understand, given two groups, what groups may appear as the extension of them. Clearly, $A \oplus C \in \text{Ext}(A,C)$. Thus we get that all the groups from Theorem 2.1 do occur in the classification in Theorem 1.3. However, we can get more groups and we describe here the classification theorem of groups occurring as extensions of two given groups. We refer the reader to Fulton’s paper ([Ful]) for the details.

Define the set

$$U^n_r = \{(I,J,K) | \sum_{i \in I} i + \sum_{j \in J} j = \sum_{k \in K} k + r(r+1)/2\},$$

where $(I,J,K)$ run over all subsets of $\{1, \ldots, n\}$ of the same size, $r \geq 1$. Note that these sets need not be disjoint, nor must their union be all of $\{1, \ldots, n\}$.

Now we use this set to recursively on $r$ define

$$T^n_p = \{(I,J,K) \in U^n_p | \text{for all } p < r \text{ and all } (F,G,H) \in T^n_p, \sum_{f \in F} i_f + \sum_{g \in G} j_g \leq \sum_{h \in H} k_h + p(p+1)/2\}.$$

We now explain the notation used in the definition of $T^n_p$. Since $(I,J,K) \in U^n_p$ we have that they are subsets of $\{1, \ldots, n\}$ of size $r$. Write them as $I = \{i_1, \ldots, i_r\}$, $J = \{j_1, \ldots, j_r\}$, $K = \{k_1, \ldots, k_r\}$. Then we can view $F,G,H \subset \{1, \ldots, r\}$ as subsets of the indices of $I, J, K$ respectively. Thus for $f \in F$, $i_f$ would be the $f^\text{th}$ element of $i$.

Now suppose we have two groups $A, B, C$ such that

$$A = \mathbb{Z}/\ell^{\alpha_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/\ell^{\alpha_n}\mathbb{Z}$$

$$B = \mathbb{Z}/\ell^{\beta_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/\ell^{\beta_n}\mathbb{Z}$$

$$C = \mathbb{Z}/\ell^{\gamma_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/\ell^{\gamma_n}\mathbb{Z}$$

where $\alpha_1 \geq \cdots \geq \alpha_n$, $\beta_1 \geq \cdots \geq \beta_n$, $\gamma_1 \geq \cdots \geq \gamma_n$ and some are allowed to be 0.

Define the relationship

$$\sum_{k \in K} \gamma_k \leq \sum_{i \in I} \alpha_i + \sum_{j \in J} \beta_j$$

for subsets $I, J, K$ of $\{1, \ldots, n\}$ of the same size. Then $C$ is an extension of $B$ by $A$ (that is there exists an exact sequence $0 \to A \to C \to B \to 0$) if and only if $\sum \gamma_i = \sum \alpha_i + \sum \beta_i$ and (4.1) holds for all $(I,J,K) \in T^n_r$ for all $r < n$.

Remark. This classification of extensions tell us that $\text{Ext}(A,B) = \text{Ext}(B,A)$ as all the conditions are symmetric among the values appearing in $A$ and the values appearing in $B$. Thus if we want to determine all the groups that can occur for a certain isogeny class is does not matter in which order we factor the characteristic polynomial.
Now let us use this classification to determine what groups may appear in Rybakov’s counterexample. Recall he let $h_A(t) = (t^2 - 2t + 9)(t + 3)^2$, so $h_A(1 - t) = (t^2 + 8)(t - 4)^2$. Thus by our theorem we know that all such groups will appear satisfy one of two exact sequences:

$$0 \to \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \to G \to \mathbb{Z}/8\mathbb{Z} \to 0$$

$$0 \to \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \to G \to \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \to 0$$

Thus we need to determine what $T_r^n$ is for all $r < 4$. First we need to determine $U_r^n$ for all $r \leq n \leq 4$. We note that if $(I, J, K) \in U_r^n$ then $(J, I, K) \in U_r^n$ and so to save space we will only write one.

$$U_1^1 = \left\{ \left( \{1\}, \{1\}, \{1\} \right) \right\}$$

$$U_2^1 = U_1^1 \cup \left\{ \left( \{1\}, \{2\}, \{2\} \right) \right\}$$

$$U_2^2 = \left\{ \left( \{1,2\}, \{1,2\}, \{1,2\} \right) \right\}$$

$$U_3^2 = U_2^2 \cup \left\{ \left( \{1,2\}, \{3,3\}, \{2,2\}, \{3\} \right) \right\}$$

$$U_3^1 = \left\{ \left( \{1,2,3\}, \{1,2,3\}, \{1,2,3\} \right) \right\}$$

$$U_4^1 = U_3^1 \cup \left\{ \left( \{1\}, \{4\}, \{4\} \right) \right\}$$

$$U_2^3 = U_2^2 \cup \left\{ \left( \{1,2\}, \{1,4\}, \{2,3\} \right) \right\}$$

$$U_3^3 = U_3^2 \cup \left\{ \left( \{1,2,3\}, \{1,2,3\}, \{1,2,3\} \right) \right\}$$

$$U_4^3 = U_4^2 \cup \left\{ \left( \{1,2,3\}, \{2,3,4\}, \{2,3,4\} \right) \right\}$$

Now for the $T_r^n$ we can see also that if $(I, J, K) \in T_r^n$ then $(J, I, K) \in T_r^n$ so, again, we will only list one. Further, it is trivially true that $T_1^n = U_1^n$ and $T_2^n = U_2^n$ for all $n$.

$$T_2^3 = T_2^2 \cup \left\{ \left( \{1,2\}, \{1,3\}, \{1,3\} \right) \right\}$$

$$T_2^4 = T_2^3 \cup \left\{ \left( \{1,2\}, \{1,4\}, \{1,4\} \right) \right\}$$

$$T_3^4 = T_3^3 \cup \left\{ \left( \{1,2,3\}, \{1,2,4\} \right) \right\}$$
Now let $G = \mathbb{Z}/2^\gamma \mathbb{Z} \oplus \mathbb{Z}/2^\gamma \mathbb{Z} \oplus \mathbb{Z}/2^\gamma \mathbb{Z} \oplus \mathbb{Z}/2^\gamma \mathbb{Z}$ and consider the first exact sequence

$$0 \to \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \to G \to \mathbb{Z}/8\mathbb{Z} \to 0.$$ 

Thus we get that $\alpha_1 = 2, \alpha_2 = 2, \alpha_3 = 0, \alpha_4 = 0, \beta_1 = 3, \beta_2 = 0, \beta_3 = 0, \beta_4 = 0$. Looking at the conditions imposed by $T_1^4$ we get that $\gamma_1 \leq 5$ and $\gamma_2 \leq 2$. The conditions imposed by $T_2^4$ are $\gamma_1 + \gamma_3 \leq 5, \gamma_2 + \gamma_3 \leq 4, \gamma_1 + \gamma_4 \leq 5, \gamma_2 + \gamma_4 \leq 2, \gamma_3 + \gamma_4 \leq 2$. The conditions imposed by $T_3^4$ are $\gamma_1 + \gamma_3 + \gamma_4 \leq 5$ and $\gamma_2 + \gamma_3 + \gamma_4 \leq 4$. Also, we need $\gamma_1 + \gamma_2 + \gamma_3 + \gamma_4 = 7$. Thus we get

$$(\gamma_1, \gamma_2, \gamma_3, \gamma_4) = (5, 2, 0, 0), (4, 2, 1, 0) \text{ or } (3, 2, 2, 0)$$

Now consider the second exact sequence

$$0 \to \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \to G \to \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \to 0.$$ 

Then we have $\alpha_1 = 2, \alpha_2 = 2, \alpha_3 = 0, \alpha_4 = 0, \beta_1 = 2, \beta_2 = 1, \beta_3 = 0, \beta_4 = 0$. The conditions imposed by $T_1^2$ are $\gamma_1 \leq 4, \gamma_2 \leq 3, \gamma_3 \leq 2$. The conditions imposed by $T_2^2$ are $\gamma_1 + \gamma_3 \leq 5, \gamma_2 + \gamma_3 \leq 4, \gamma_1 + \gamma_4 \leq 4, \gamma_2 + \gamma_4 \leq 3, \gamma_3 + \gamma_4 \leq 3$. The conditions imposed by $T_3^2$ are $\gamma_1 + \gamma_3 + \gamma_4 \leq 5, \gamma_2 + \gamma_3 + \gamma_4 \leq 5$. Thus we get

$$(\gamma_1, \gamma_2, \gamma_3, \gamma_4) = (4, 3, 0, 0), (4, 2, 1, 0), (3, 2, 2, 0), (3, 2, 1, 1), (3, 3, 1, 0) \text{ or } (2, 2, 2, 1)$$

Hence all the groups that may appear as an abelian variety with characteristic polynomial $h_4(t) = (t^2 - 2t + 9)(t + 3)^2$ are

$$\mathbb{Z}/32\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \quad \mathbb{Z}/16\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \quad \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$$

$$\mathbb{Z}/16\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \quad \mathbb{Z}/16\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \quad \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

$$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \quad \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

Notice that we do get Rybakov’s counterexample of $\mathbb{Z}/16\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. Further we do get the two direct sums as well $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

References

[FM] William Fulton. Eigenvalues, invariant factors, highest weights, and schubert calculus. Bulletin of the American Mathematical Society, 37(3):209–249, 2000

[Ryb] Sergey Rybakov. The groups of point on abelian varieties over finite fields. Central European Journal of Mathematics, 8(2):282–288, 2010

[WM] William C Waterhous, JS Milne. Abelian varieties over finite fields. Ann. Sci. École Norm. Sup. (4), 2:521–560, 1969.