The Characteristic Polynomials for Abelian Varieties of Dimension 6 Over Finite Fields

Gyoyong Sohn

Department of Mathematics Education
Daegu National University of Education
Daemyung 2-dong, Daegu, Republic of Korea

This article is distributed under the Creative Commons by-nc-nd Attribution License. Copyright © 2020 Hikari Ltd.

Abstract

We describe the characteristic polynomials of the Frobenious endomorphism of abelian varieties of dimension 6 over finite fields.

Mathematics Subject Classification: 14G15, 11C08, 11G10, 11G25

Keywords: Weil polynomials, Abelian varieties over finite fields

1 Basic Facts and Results

Let $A$ be an abelian variety of dimension $g$ over $\mathbb{F}_q$ where $q = p^n$. Let $T_l(A)$ be the $l$-th Tate module of $A$, and $V_l(A) = T_l(A) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ be the corresponding vector space over $\mathbb{Q}_l$. For $l \neq p$, the characteristic polynomial of the Frobenious endomorphism $\pi_A$ of $A$ is defined as,

$$P_A(t) = \det(\pi_A - tI_d|V_l(A)).$$

It is a monic polynomial of degree $2g$ with rational integer coefficients independent of the choice of prime $l$. In fact, $P_A(t)$ can be represented as

$$P_A(t) = t^{2g} + a_1t^{2g-1} + \cdots + a_g t^g + q a_{g-1} t^{g-1} + \cdots + q^{g-1}a_1 t + q^g,$$

for all $a_i \in \mathbb{Z}$ ($1 \leq i \leq g$). The set of roots $P_A(t)$ consist of couples of complex conjugated numbers of modulus $\sqrt{q}$. A monic polynomial with integer coefficients which satisfies this condition is called a Weil polynomial. Thus, the
characteristic polynomial of the Frobenius endomorphism of abelian varieties of dimension $g$ is a Weil polynomial of degree $2g$, but the converse is false.

An abelian variety $A$ is $k$-simple if it is not isogenous to a product of abelian varieties of lower dimensions over $k$. In that case, $P_A(t)$ is either irreducible over $\mathbb{Z}$ if $P_A(t) = h(t)^e$ where $h(t) \in \mathbb{Z}[t]$ is an irreducible over $\mathbb{Z}$, see [7]. We have the following result from Tate [6].

**Theorem 1.1** If $A$ and $B$ are the abelian varieties defined over $\mathbb{F}_q$. Then $A$ is $\mathbb{F}_q$-isogenous to abelian subvariety if and only if $P_A(t)$ divides $P_B(t)$ over $\mathbb{Q}[t]$. In particular, $P_A(t) = P_B(t)$ if and only if $A$ and $B$ are $\mathbb{F}_q$-isogenous.

The Tate theorem gives us a nice description of isogeny classes of abelian varieties over $\mathbb{F}_q$ in terms of Weil polynomials.

In this paper, we present a criterion to determine when a Weil polynomial of degree 12 is the characteristic polynomial of an abelian variety of dimension 6. Haloui gave the set of characteristic polynomial of abelian varieties of dimension 3 over finite fields[1]. Haloui and Singh gave the list of characteristic polynomials of abelian varieties of dimension 4 over finite field[2]. In [3], the characteristic polynomials of abelian varieties of dimension 5 over finite fields are described.

Throughout this paper, the Weil polynomial of degree 12 has the form

\[
P(t) = t^{12} + a_1 t^{11} + a_2 t^{10} + a_3 t^9 + a_4 t^8 + a_5 t^7 + a_6 t^6 + a_5 q t^5 + a_4 q^2 t^4 + a_3 q^3 t^3 + a_2 q^4 t^2 + a_1 q^5 t + q^6,
\]

for all $a_i \in \mathbb{Z}$ ($1 \leq i \leq 6$). The set of roots of $P(t)$ has complex numbers of the form \{\$\alpha_1, \bar{\alpha}_1, \ldots, \alpha_6, \bar{\alpha}_6$\} and the absolute value of each $\alpha_i$ is equal to $\sqrt{q}$. The following theorem gives us the set of the characteristic polynomials of the Frobenius endomorphism of abelian varieties of dimension 6 over finite fields. It determine the possible Newton polygons of $P(t)$ when $P(t)$ is irreducible ($e = 1$). Let $v_p$ denote the $p$-adic additive valuation normalized as $v_p(p) = 1$.

**Theorem 1.2** Let $P(t)$ be an irreducible Weil polynomial of the form (1). Then $P(t)$ is the characteristic polynomial of an abelian variety of dimension 6 if and only if one of the following conditions holds:

1. $v_p(a_6) = 0$,
2. $v_p(a_5) = 0$, $v_p(a_6) \geq n/2$ in $\mathbb{Q}_p$, and $P(t)$ has no root of valuation $n/2$ in $\mathbb{Q}_p$,
3. $v_p(a_4) = 0$, $v_p(a_5) \geq n/2$, $v_p(a_6) \geq n$ and $P(t)$ has no root of valuation $n/2$ in $\mathbb{Q}_p$,
4. $v_p(a_3) = 0$, $v_p(a_4) \geq n/2$, $v_p(a_5) \geq n$, $v_p(a_6) \geq 3n/2$ and $P(t)$ has no root of valuation $n/2$ and a factor of degree 3 in $\mathbb{Q}_p$,
5. \(v_p(a_2) = 0, v_p(a_3) \geq n/2, v_p(a_4) \geq n, v_p(a_5) \geq 3n/2, v_p(a_6) \geq 2n\) and \(P(t)\) has no root of valuation \(n/2\) nor factor of degree 3 in \(\mathbb{Q}_p\),

6. \(v_p(a_1) = 0, v_p(a_2) \geq n/2, v_p(a_3) \geq n, v_p(a_4) \geq 3n/2, v_p(a_5) \geq 2n, v_p(a_6) \geq 5n/2\) and \(P(t)\) has no root of valuation \(n/2\) nor a factor of degree 3 or 5 in \(\mathbb{Q}_p\),

7. \(v_p(a_1) \geq n/6, v_p(a_2) \geq n/3, v_p(a_3) \geq n/2, v_p(a_4) \geq 2n/3, v_p(a_5) \geq 5n/6, v_p(a_6) = n\) and \(P(t)\) has two irreducible factors of degree 6 in \(\mathbb{Q}_p\),

8. \(v_p(a_1) \geq n/3, v_p(a_2) \geq 2n/3, v_p(a_3) \geq n, v_p(a_4) \geq 4n/3, v_p(a_5) = 5n/3, v_p(a_6) = 2n\) and \(P(t)\) has two irreducible factors of degree 6 in \(\mathbb{Q}_p\),

9. \(v_p(a_3) = 0, v_p(a_4) \geq n/3, v_p(a_5) \geq 2n/3, v_p(a_6) = n\) and \(P(t)\) has no root of valuation \(n/3\) or \(2n/3\) in \(\mathbb{Q}_p\),

10. \(v_p(a_2) = 0, v_p(a_3) \geq n/4, v_p(a_4) \geq n/2, v_p(a_5) \geq 3n/4, v_p(a_6) = n\) and \(P(t)\) has no root of valuation \(n/4\) or \(3n/4\) nor an irreducible factor of degree 2 in \(\mathbb{Q}_p\),

11. \(v_p(a_1) = 0, v_p(a_2) \geq n/5, v_p(a_3) \geq 2n/5, v_p(a_4) \geq 3n/5, v_p(a_5) \geq 4n/5, v_p(a_6) = n\) and \(P(t)\) has no root of valuation \(n/5\) or \(4n/5\) in \(\mathbb{Q}_p\),

12. \(v_p(a_1) = 0, v_p(a_2) \geq 2n/5, v_p(a_3) \geq 4n/5, v_p(a_4) \geq 6n/5, v_p(a_5) \geq 8n/5, v_p(a_6) = 2n\) and \(P(t)\) has no root of valuation \(2n/5\) or \(8n/5\) in \(\mathbb{Q}_p\),

13. \(v_p(a_1) \geq n/5, v_p(a_2) \geq 2n/5, v_p(a_3) \geq 3n/5, v_p(a_4) \geq 4n/5, v_p(a_5) = n, v_p(a_6) \geq 3n/2\) and \(P(t)\) has no root of valuation \(n/5, n/2\) and \(4n/5\) in \(\mathbb{Q}_p\),

14. \(v_p(a_1) \geq 2n/5, v_p(a_2) \geq 4n/5, v_p(a_3) \geq 6n/5, v_p(a_4) \geq 8n/5, v_p(a_5) = 2n, v_p(a_6) \geq 5n/2\) and \(P(t)\) has no root of valuation \(2n/5, n/2\) and \(8n/5\) in \(\mathbb{Q}_p\),

15. \(v_p(a_1) \geq n/4, v_p(a_2) \geq n/2, v_p(a_3) \geq 3n/4, v_p(a_4) = n, v_p(a_5) = 3n/2, v_p(a_6) = 2n\) and \(P(t)\) has no root of valuation \(n/4, n/2\) and \(3n/4\) in \(\mathbb{Q}_p\),

16. \(v_p(a_1) \geq n/3, v_p(a_2) \geq 2n/3, v_p(a_3) = n, v_p(a_4) \geq 3n/2, v_p(a_5) = 2n, v_p(a_6) \geq 5n/2\) and \(P(t)\) has no root of valuation \(n/3, n/2\) and \(2n/3\) in \(\mathbb{Q}_p\),

17. \(v_p(a_1) \geq n/2, v_p(a_2) \geq n, v_p(a_3) \geq 3n/2, v_p(a_4) \geq 2n, v_p(a_5) \geq 5n/2, v_p(a_6) \geq 3n\) and \(P(t)\) has no root nor factor of degree 3 or 5 in \(\mathbb{Q}_p\).

2 Newton Polygons

Let \(P(t)\) be an irreducible Weil polynomial of degree 12. By [4], \(P(t)\) is the characteristic polynomial of an abelian variety of dimension 6 if and only if \(e = 1\) for \(P(t)^e\), where \(e\) the least common denominator of \(v_p(f(0))/n\) where \(f(t)\) runs through the irreducible factors of \(P(t)\) over \(\mathbb{Q}_p\). Thus, we consider the Newton polygons of \(P(t)\) over \(\mathbb{Q}_p\) in order to determine when this condition is satisfied. It means the lower envelope of the set of points \(\{(i, v_p(a_i))|0 \leq i \leq 2g\}\)
Gyeyong Sohn

in $\mathbb{R} \times \mathbb{R}$, where $v_p$ is the $p$-adic valuation of $\mathbb{Q}_p$. Its shape leads to a decomposition of $P(t)$ over $\mathbb{Q}_p$. We denote by $\nu_p$ the unique extension of the $p$-adic valuation $v_p$ to the algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$, normalized so that $\nu_p(p) = 1$. Then we can be divided into six cases of the Newton polygons of $P(t)$ with regard to decomposition form of $P(t)$ over $\mathbb{Q}_p$. There are called ordinary, supersingular, symmetry, Mixed I, Mixed II, and Mixed III. The obtained results are summarized in Theorem 1.2.

**Case 1: Ordinary**

In this case, the Newton polygon of $P(t)$ is represented in Figure 1. The Newton polygon has a segment of length 6 and with slope 0. This is the Newton polygon of $P(t)$ if and only if $v_p(a_6) = 0$. Then we have $\nu_p(\alpha_i) = 0$ for $\alpha_i$ roots of $P(t)$, $1 \leq i \leq 6$, and we have always $e = 1$.

![Figure 1: Ordinary case](image)

**Case 2: Symmetry**

In this case, there are two Newton polygons as in Figure 2. There is an integer $\lambda$ satisfying $0 < \lambda < 1/2$. We have $\nu_p(\alpha_i) = \lambda n$ for $1 \leq i \leq 6$. First, we consider the upper polygon in Figure 2. The Newton polygon of $P(t)$ has two segments from the right with slopes $-n/3$ and $-2n/3$, respectively. This is the Newton polygon of $P(t)$ if and only if $v_p(a_1) \geq n/3$, $v_p(a_2) \geq 2n/3$, $v_p(a_3) \geq n$, $v_p(a_4) \geq 4n/3$, $v_p(a_5) \geq 5n/3$, $v_p(a_6) = 2n$. If this condition hold, $P(t)$ has two factors of degree 6 in $\mathbb{Q}_p$, one with roots of valuation $1/3$ and the other with roots of valuation $2/3$. Then $e = 1$ if and only if $P(t)$ has two irreducible factors of degree 6 in $\mathbb{Q}_p$.

Second, we consider the lower polygon in Figure 2. The Newton polygon has two segments from the right with slopes $-n/6$ and $-5n/6$, respectively. This is the Newton polygon of $P(t)$ if and only if $v_p(a_1) \geq n/6$, $v_p(a_2) \geq n/3$, $v_p(a_3) \geq n/2$, $v_p(a_4) \geq 2n/3$, $v_p(a_5) \geq 5n/6$, $v_p(a_6) = n$. Hence $e = 1$ if and only if $P(t)$ has two irreducible factors of degree 6 in $\mathbb{Q}_p$ with roots of valuation $1/6$ and $5/6$, respectively.

**Case 3. Mixed I**

In this case, there are five Newton polygons as in Figure 3. The Newton
The characteristic polynomials for abelian varieties of dimension 6 over ...

Figure 2: Symmetry case

polygon of $P(t)$ has the segments from the right with slope $0, -n/2$ and $-n$, respectively. Then we have $\nu_p(\alpha_i) = 0$ and $\nu_p(\alpha_j) = n/2$ for some $i, j$.

Figure 3: Mixed I case

First, we consider $p$-rank 5. This is the Newton polygon of $P(t)$ if and only if $v_p(a_5) = 0, v_p(a_6) \geq n/2$. If this conditions holds, $P(t)$ has a factor in $\mathbb{Q}_p$ of degree 2 with roots of valuation $n/2$ and thus $e = 1$ if and only if this factor is irreducible, that is, if and only if $P(t)$ has no root of valuation $n/2$ in $\mathbb{Q}_p$.

Second, we consider $p$-rank 4. This is the Newton polygon of $P(t)$ if and only if $v_p(a_4) = 0, v_p(a_5) \geq n/2, v_p(a_6) \geq n$. If this conditions holds, $e = 1$ if and only if $P(t)$ has no root of valuation $n/2$ in $\mathbb{Q}_p$. 
Third, we consider $p$-rank 3. This is the Newton polygon of $P(t)$ if and only if $v_p(a_3) = 0$, $v_p(a_4) \geq n/2$, $v_p(a_5) \geq n$, $v_p(a_6) \geq 3n/2$. If this conditions hold, $e = 1$ if and only if $P(t)$ has no root of valuation $n/2$ nor a factor of degree 3 in $\mathbb{Q}_p$.

Fourth, we consider $p$-rank 2. This is the Newton polygon of $P(t)$ if and only if $v_p(a_2) = 0$, $v_p(a_3) \geq n/2$, $v_p(a_4) \geq n$, $v_p(a_5) \geq 3n/2$, $v_p(a_6) \geq 2n$. If this conditions hold, $e = 1$ if and only if $P(t)$ has no root of valuation $n/2$ nor a factor of degree 3 in $\mathbb{Q}_p$.

Fifth, we consider $p$-rank 1. This is the Newton polygon of $P(t)$ if and only if $v_p(a_1) = 0$, $v_p(a_2) \geq n/2$, $v_p(a_3) \geq n$, $v_p(a_4) \geq 3n/2$, $v_p(a_5) \geq 2n$, $v_p(a_6) \geq 5n/2$. If these conditions holds, $e = 1$ if and only if $P(t)$ has no root of valuation $n/2$ nor a factor of degree 3 or 5 in $\mathbb{Q}_p$.

**Case 4 : Mixed II**

In this case, there are four Newton polygons as in Figure 4. The Newton polygon has the segments from the right with slopes $0$, $-\lambda n$, $-(1-\lambda)n$, and $-n$ for $\lambda \in \mathbb{Z}$, $1 < \lambda < 1/2$. Then we have the valuation $\nu_p(\alpha_i) = 0$ and $\nu_p(\alpha_j) = n/2$ for some $i$, $j$.

![Figure 4: Mixed II case](image)

First, we consider $p$-rank 3. This is the Newton polygon of $P(t)$ if and only if $v_p(a_3) = 0$, $v_p(a_4) \geq n/3$, $v_p(a_5) \geq 2n/3$, $v_p(a_6) = n$. If this conditions hold, $e = 1$ if and only if $P(t)$ has no root of valuation $n/3$ or $2n/3$ in $\mathbb{Q}_p$.

Second, we have $p$-rank 2. This is the Newton polygon of $P(t)$ if and only if $v_p(a_2) = 0$, $v_p(a_3) \geq n/4$, $v_p(a_4) \geq n/2$, $v_p(a_5) \geq 3n/4$, $v_p(a_6) = n$. If this conditions hold, $e = 1$ if and only if $P(t)$ has no root of valuation $n/4$ or $3n/4$ nor an irreducible factor of degree 2 in $\mathbb{Q}_p$.

Third, we consider the upper polygon in $p$-rank 1. This is the Newton
polygon of $P(t)$ if and only if $v_p(a_1) = 0$, $v_p(a_2) \geq 2n/5$, $v_p(a_3) \geq 4n/5$, $v_p(a_4) \geq 6n/5$, $v_p(a_5) \geq 8n/5$, $v_p(a_6) = 2n$. If these conditions holds, $e = 1$ if and only if $P(t)$ has no root of valuation $2n/5$ or $8n/5$ in $\mathbb{Q}_p$.

Fourth, we consider the lower polygon in $p$-rank 1. This is the Newton polygon of $P(t)$ if and only if $v_p(a_1) = 0$, $v_p(a_2) \geq n/5$, $v_p(a_3) \geq 2n/5$, $v_p(a_4) \geq 3n/5$, $v_p(a_5) \geq 4n/5$, $v_p(a_6) = n$. If these conditions holds, $e = 1$ if and only if $P(t)$ has no root of valuation $n/5$ or $4n/5$ in $\mathbb{Q}_p$.

**Case 5 : Mixed III**

In this case, there are four Newton polygons of Figure 5. The Newton polygon has the segments from the right with slopes $0$, $-\lambda n$, $-(1-\lambda)n$, and $-n$ for $\lambda \in \mathbb{Z}$, $1 < \lambda < 1/2$. Then we have the valuation $v_p(\alpha_i) = 0$ and $v_p(\alpha_j) = n/2$ for some $i, j$.

![Figure 5: Mixed III case](image)

First, we consider the upper polygon in the upper left side of Figure 5. This is the Newton polygon of $P(t)$ has $v_p(a_1) \geq n/5$, $v_p(a_2) \geq 2n/5$, $v_p(a_3) \geq 3n/5$, $v_p(a_4) \geq 4n/5$, $v_p(a_5) = n$, $v_p(a_6) \geq 3n/2$. If these conditions hold, $e = 1$ if and only if $P(t)$ has no root of valuation $n/5$, $n/2$ and $4n/5$ in $\mathbb{Q}_p$.

Second, we consider the lower polygon in the upper left side of Figure 5. This is the Newton polygon of $P(t)$ has $v_p(a_1) \geq 2n/5$, $v_p(a_2) \geq 4n/5$, $v_p(a_3) \geq 6n/5$, $v_p(a_4) \geq 8n/5$, $v_p(a_5) = 2n$, $v_p(a_6) \geq 5n/2$. If these conditions hold, $e = 1$ if and only if $P(t)$ has no root of valuation $2n/5$, $n/2$ and $8n/5$ in $\mathbb{Q}_p$.

Third, we consider the polygon of the upper right side. This is the Newton polygon of $P(t)$ if and only if $v_p(a_1) \geq n/4$, $v_p(a_2) \geq n/2$, $v_p(a_3) \geq 3n/4$, $v_p(a_4) = n$, $v_p(a_5) = 3n/2$, $v_p(a_6) = 2n$. If these conditions hold, $e = 1$ if and only if $P(t)$ has no root of valuation $n/4$, $n/2$ and $3n/4$ in $\mathbb{Q}_p$.

Fourth, we consider the polygon of the lower position of Figure 5. This is the
Newton polygon of \( P(t) \) if and only if \( v_p(a_1) \geq n/3, v_p(a_2) \geq 2n/3, v_p(a_3) = n, v_p(a_4) \geq 3n/2, v_p(a_5) = 2n, v_p(a_6) \geq 5n/2 \). If this conditions hold, \( e = 1 \) if and only if \( P(t) \) has no root of valuation \( n/3, n/2 \) and \( 2n/3 \) in \( \mathbb{Q}_p \).

**Case 6. Supersingular**

In this case, there is one Newton polygon of \( P(t) \) as in Figure 6.

This is the Newton polygon of \( P(t) \) if and only if \( v_p(a_1) \geq \frac{n}{2}, v_p(a_2) \geq n, v_p(a_3) \geq \frac{3}{2}n, v_p(a_4) \geq 2n, v_p(a_5) \geq \frac{5}{2}n, v_p(a_6) \geq 3n \). If this condition holds, \( e = 1 \) if and only if \( P(t) \) has no root nor factor of degree 3 or 5 in \( \mathbb{Q}_p \).

![Figure 6: Supersingular case](image)

**References**


Received: March 25, 2020; Published: April 7, 2020