Functiones et Approximatio
51.2 (2014), 415–436
doi: 10.7169/facm/2014.51.2.11

CLASSIFICATION OF CHARACTERISTIC POLYNOMIALS OF SIMPLE SUPERSINGULAR ABELIAN VARIETIES OVER FINITE FIELDS

Vijaykumar Singh, Gary McGuire, Alexey Zaytsev

Abstract: In this article, we give a complete description of the characteristic polynomials of simple supersingular abelian varieties over finite fields. We list them for the dimensions up to 7.

Keywords: abelian varieties over finite fields, Weil polynomials.

1. Introduction

An important isogeny invariant of an abelian variety over a finite field is the characteristic polynomial of its Frobenius endomorphism, sometimes called the Weil polynomial of the abelian variety. In this paper we give a complete description of the Weil polynomials of supersingular abelian varieties over finite fields. We list them for the dimensions up to 7. The results for dimensions $\leqslant 4$ were previously known; we give the details and references in Section 12. For any dimension, similiar results were obtained in [17] and [16], but our results are more explicit and algorithmic in nature.

The paper is organized as follows. In Section 2 we recall the necessary background for the paper. Section 3 proves our result in the case q is a nonsquare, and Section 4 deals with the case q is a square. Section 5 to 11 deal with dimensions 1 to 7 explicitly, deriving the possible polynomials from our general results. This can be done for dimensions larger than 7 also; we omit the details. Section 12 summarizes these results. Section 13 applies our general results to give some partial results on general existence questions.

2010 Mathematics Subject Classification: primary: 14G15; secondary: 11C08, 11G10, 11G25

2. Background

Let k denote the finite field $\mathbb{F}_q$, where $q = p^n$ and p is prime. Let A be an abelian variety of dimension g over k. Let $P_A(X)$ be the Weil polynomial of A. Using the Riemann Hypothesis over finite fields, due to Weil, $P_A(X)$ can be written

$$P_A(X) = X^{2g} + a_1 X^{2g-1} + \cdots + a_g X^g + q a_{g-1} X^{g-1} + \cdots + q^{g-1} a_1 X + q^g \quad (1)$$

for some $a_i \in \mathbb{Z}$. We will see that there are strong restrictions on the possibilities for the a_i when A is supersingular.

A *Weil-q-number* π is defined to be an algebraic number such that, for every embedding $\sigma : \mathbb{Q}[\pi] \hookrightarrow \mathbb{C}$, $|\sigma(\pi)| = q^{\frac{1}{2}}$ holds. The set of roots of $P_A(X)$ has the form $\{\omega_1, \overline{\omega}_1, \ldots, \omega_g, \overline{\omega}_g\}$, where the ω_i's are Weil-q-numbers. A monic polynomial with integer coefficients which satisfies this condition is called a *Weil polynomial*. Thus, every Weil polynomial of degree $2g$ has the form (1) for certain integers $a_i \in \mathbb{Z}$.

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, $P_A(X)$ is either irreducible over $\mathbb{Z}$ or $P_A(X) = h(X)^e$, where $h(X) \in \mathbb{Z}[X]$ is an irreducible, monic polynomial over $\mathbb{Z}$; see Milne and Waterhouse in [14]. We have the following result from Tate [12].

Theorem 2.1. *Let A and B be abelian varieties defined over $\mathbb{F}_q$. Then A is $\mathbb{F}_q$-isogenous to an abelian subvariety of B if and only if $P_A(X)$ divides $P_B(X)$ in $\mathbb{Q}[X]$. In particular, $P_A(X) = P_B(X)$ if and only if A and B are $\mathbb{F}_q$-isogenous.*

Let $W(q)$ be the set of Weil-q-numbers in $\mathbb{C}$. We say that elements π and π' are *conjugate*, if π and π' have the same minimum polynomial over $\mathbb{Q}$.

The conjugacy class of π_A depends only on the isogeny class of A. More precisely, we have the following theorem from [13].

Theorem 2.2 (Honda-Tate theorem). *The map $A \to \pi_A$ defines a bijection*

$$\{\textit{simple abelian varieties}/\mathbb{F}_q\}/(\textit{isogeny}) \mapsto W(q)/(\textit{conjugacy}).$$

In other words, given an irreducible Weil polynomial $P(X)$, there exist a unique abelian variety A up to isogeny and natural number e such that $P_A(X) = P(X)^e$.

A Weil-q number π is called a *supersingular Weil-q-number* if $\pi = \sqrt{q}\zeta$, where ζ is some root of unity.

Definition 2.3. An abelian variety A over k is called *supersingular* if any one of the following (equivalent) conditions holds: (see [8, Theorem 4.2])

1. the eigenvalues of the Frobenius π_A are supersingular Weil-q-numbers;
2. the Newton polygon of A is a straight line of slope $1/2$;
3. A is $\overline{k}$-isogenous to a power of a supersingular elliptic curve.

We will use the following useful theorem from [13].

Theorem 2.4. *Let A be a simple abelian variety over $k = \mathbb{F}_q$, then*

1. *$End_k(A) \otimes \mathbb{Q}$ is a division algebra with center $\mathbb{Q}(\pi_A)$ and*

$$2\,dim A = [End_k(A) \otimes \mathbb{Q} : \mathbb{Q}(\pi_A)]^{\frac{1}{2}}\,[\mathbb{Q}(\pi_A) : \mathbb{Q}].$$

2. *The division algebra $End_k(A) \otimes \mathbb{Q}$ over $\mathbb{Q}$ has the following splitting behaviour:*
   (a) *it splits at each divisor $\mathfrak{l}$ of l in $\mathbb{Q}(\pi_A)$, if $l \neq p$,*
   (b) *the invariants at the divisors $\mathfrak{p}$ of p in $\mathbb{Q}(\pi_A)$ can be evaluated with*

$$\mathrm{inv}_{\mathfrak{p}}(End_k(A) \otimes \mathbb{Q}) \equiv \frac{v_{\mathfrak{p}}(\pi_A)}{v_{\mathfrak{p}}(q)}[\mathbb{Q}(\pi_A)_{\mathfrak{p}} : \mathbb{Q}_p] \mod \mathbb{Z},$$

   where $\mathbb{Q}(\pi_A)_{\mathfrak{p}}$ denotes the completion of $\mathbb{Q}(\pi_A)$ at $\mathfrak{p}$ and $v_{\mathfrak{p}}$ denotes the $\mathfrak{p}$-adic valuation.
   (c) *it does not split at the real places of $\mathbb{Q}(\pi_A)$.*

If A is a supersingular abelian variety, then $\pi_A = \sqrt{q}\zeta$, where ζ is some root of unity. If A is also simple, then it follows from above theorem that $\mathrm{inv}_{\mathfrak{p}}(End_k(A) \otimes \mathbb{Q}) \equiv \frac{1}{2} e_{\mathfrak{p}} f_{\mathfrak{p}} \mod \mathbb{Z}$, where $e_{\mathfrak{p}}$ is the ramification index of $\mathfrak{p}$ over p and $f_{\mathfrak{p}}$ is the residue class degree.

Also, $\pi \in \overline{\mathbb{Q}}$ be the supersingular Weil-q-number and $P(X)$ be the corresponding minimal Weil polynomial. The invariants of $End_k(A) \otimes \mathbb{Q}$ lie in $\mathbb{Q}/\mathbb{Z}$. They can be evaluated from the minimal polynomial $P(X)$ of π_A as follows. The only real Weil numbers are $q^{1/2}$ and $-q^{1/2}$, so there are hardly any real places of $\mathbb{Q}(\pi_A)$. We consider the polynomial $P(X)$ in $\mathbb{Q}_p[X]$, i.e. over the p-adic numbers. Let

$$P(X) = \prod_i f_i(X)$$

be the decomposition in irreducible factors in $\mathbb{Q}_p[X]$. The factors $f_i(X)$ correspond uniquely to the divisors $\mathfrak{p}_i$ of p in $\mathbb{Q}(\pi_A)$. So to get the invariants, we have to factor $P(X)$ over $\mathbb{Q}_p$. Indeed,

$$\mathrm{inv}_{\mathfrak{p}_i}(End_k(A) \otimes \mathbb{Q}) \equiv \frac{v_p(f_i(0))}{v_p(q)} \mod \mathbb{Z}.$$

If $P(X)$ is a supersingular Weil polynomial, then $f_i(0) = \prod_{j=1}^{\deg f_i} \sqrt{q}\zeta_j$, where ζ_j is some root of unity. In that case,

$$\mathrm{inv}_{\mathfrak{p}_i}(End_k(A) \otimes \mathbb{Q}) = \frac{n^{\frac{\deg f_i}{2}}}{n} = \frac{\deg f_i}{2} \mod \mathbb{Z}.$$

Therefore the order of invariants is either 1 or 2 in $\mathbb{Q}/\mathbb{Z}$ depending on whether $\deg f_i$ is even or odd respectively. We use the invariants in order to evaluate the dimension of A as follows.

Since $End_k(A) \otimes \mathbb{Q}$ is a division algebra and $\mathbb{Q}(\pi_A)$ is a number field, the number $[End_k(A) \otimes \mathbb{Q} : \mathbb{Q}(\pi_A)]^{\frac{1}{2}}$ is equal to the order of $End_k(A) \otimes \mathbb{Q}$ in the Brauer group of $\mathbb{Q}(\pi_A)$ see theorem 18.6, [9], which is equal to the least common multiple of the orders of all the local invariants in $\mathbb{Q}/\mathbb{Z}$; see theorem 18.5, [9]. This fact, along with the Theorem 2.4, gives the dimension of A.

The rest of section is dedicated to elementary background on cyclotomic polynomials that is useful for computing supersingular Weil polynomials.

Let $U(\mathbb{Z}/m\mathbb{Z})$ denote the multiplicative group of integers modulo m and ζ_m be a primitive m-th root of unity and Φ_m denote the m-th cyclotomic polynomial. Then there exist a natural isomorphism of groups

$$U(\mathbb{Z}/m\mathbb{Z}) \to Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q}), \qquad a \to \sigma_a$$

where $\sigma_a(\zeta_m) = \zeta_m^a$. There is a unique nontrivial homomorphism $U(\mathbb{Z}/p\mathbb{Z}) \to \{\pm 1\}$ (p an odd prime), the Legendre symbol $a \to (\frac{a}{p})$. The group $U(\mathbb{Z}/8\mathbb{Z}) = \{\pm 1, \pm 3\}$ admits three nontrivial quadratic characters (homomorphisms to $\{\pm 1\}$):

1. ε, defined by $\varepsilon(a) \equiv a \mod 4$.
2. χ_2, given by $\chi_2(\pm 1) = 1,\ \chi_2(\pm 3) = -1$.
3. χ_{-2}, given by $\chi_{-2}(1) = \chi_{-2}(3) = 1, \chi_2(-1) = \ \chi_2(-3) = -1$.

For any odd prime p, $\sqrt{\pm p} \in \mathbb{Q}(\zeta_{4p})$ and

$$\sigma_a(\sqrt{\pm p}) = \begin{cases} (\frac{a}{p})\sqrt{\pm p} & \text{if } \pm p \equiv 1 \mod 4; \\ \varepsilon(a)(\frac{a}{p})\sqrt{\pm p} & \text{if } \pm p \equiv 3 \mod 4. \end{cases}$$

Note also that $\sqrt{\pm 2} \in \mathbb{Q}(\zeta_8)$ and for $a \in U(\mathbb{Z}/8\mathbb{Z})$, $\sigma_a(\sqrt{2}) = \chi_2(a)\sqrt{2}$, $\sigma_a(\sqrt{-2}) = \chi_{-2}(a)\sqrt{-2}$.

For an odd prime p we let

$$p^* = \left(\frac{-1}{p}\right) p = \begin{cases} p & \text{if } p \equiv 1 \mod 4; \\ -p & \text{if } p \equiv 3 \mod 4. \end{cases}$$

For p an odd prime and t any odd number let

$$\Psi_{p,t}(X) := \prod_{a \in U(\mathbb{Z}/pt\mathbb{Z})} (X - \left(\frac{a}{p}\right)\zeta_{pt}^a).$$

Let

$$\Psi_{2,t}(X) := \prod_{a \in U(\mathbb{Z}/t\mathbb{Z})} (X - \zeta_8\zeta_t^a)(X - \zeta_8^{-1}\zeta_t^a)$$

$$\Psi_{-2,t}(X) := \prod_{a \in U(\mathbb{Z}/t\mathbb{Z})} (X - \zeta_8\zeta_t^a)(X - \zeta_8^3\zeta_t^a).$$

The polynomial $\Psi_{p,t}(X) \in \mathbb{Q}(\sqrt{p^*})[X]$ as the coefficients of even powers of X are rational (even integers) and the coefficients of odd powers are integer multiples of

$\sqrt{p^*}$. The $\Psi_{p,t}$ is a reciprocal polynomial when $p \equiv 1 \mod 4$ and anti-reciprocal (i.e; $X^{\deg \Psi_{p,t}} \Psi_{p,t}(-\frac{1}{X})) = \Psi_{p,t}(X)$) when $p \equiv 3 \mod 4$. Note that $\Psi_{p,t}(X)$ actually depends on the choice of ζ_{pt}. If we replace it with ζ_{pt}^a where $(\frac{a}{p}) = -1$ then we get $\Psi_{p,t}(-X)$. Also we have

$$\Psi_{p,t}(X)\Psi_{p,t}(-X) = \Phi_{pt}(X^2).$$

A similar statement holds for $\Psi_{\pm 2,t}(X)$. Moreover polynomials

$$\Psi_{p,t}(X) \in \mathbb{Q}(\sqrt{p^*})[X]$$

$$\Psi_{2,t}(X) \in \mathbb{Q}(\sqrt{2})[X]$$

$$\Psi_{-2,t}(X) \in \mathbb{Q}(\sqrt{-2})[X]$$

factor as a product of two irreducibles over $\mathbb{Q}(\sqrt{p^*})[X]$, $\mathbb{Q}(\sqrt{2})[X]$, $\mathbb{Q}(\sqrt{-2})[X]$ respectively, which corresponds to the Aurifeuillian factorisation[1]. For example, the group $Gal(\mathbb{Q}(\zeta_{2pt})/\mathbb{Q}(\sqrt{p*}))$ fixes the polynomial $\Psi_{p,t}$ and $\Psi_{p,t}(X) = \Psi_{p,t}^1(X)\Psi_{p,t}^{-1}(X)$ where

$$\Psi_{p,t}^1(X) := \prod_{(\frac{a}{p})=1} \left(X - \left(\frac{a}{p}\right)\zeta_{pt}^a\right)$$

and

$$\Psi_{p,t}^{-1}(X) := \prod_{(\frac{a}{p})=-1} \left(X + \left(\frac{a}{p}\right)\zeta_{pt}^a\right)$$

and each of these factors are irreducible as the Galois group is clearly transitive on the roots. If K is a field, $f(X) \in K[X]$ and $a \in K^\times$, then let $f^{[a]}(X) := a^{\deg f} f(\frac{X}{a})$. Then $\Psi_{p,t}^{[\sqrt{p^*}]}(X)$, $\Psi_{2,t}^{[\sqrt{2}]}(X)$, $\Psi_{-2,t}^{[\sqrt{-2}]}(X) \in \mathbb{Q}[X]$ and are all irreducible over $\mathbb{Q}$. For example, for p, t odd, it follows from

$$\Psi_{p,t}^{[\sqrt{p^*}]}(X)\Psi_{p,t}^{[\sqrt{p^*}]}(-X) = \Phi_{pt}((\sqrt{p^*})^2X^2)$$

that $\Psi_{p,t}^{[\sqrt{p^*}]}(X)$ is irreducible over $\mathbb{Q}$.

3. When q is a nonsquare

Theorem 3.1. *Let A be a supersingular simple abelian variety over $\mathbb{F}_q$ with $q = p^n$ with n odd. If $P_A(X)$ has no real root, then $P_A(X)$ is irreducible over $\mathbb{Q}$.*

Proof. If A is a supersingular abelian variety then it follows from Theorem 2.4 that, $\mathrm{inv}_{\mathfrak{p}}(End_k(A) \otimes \mathbb{Q}) \equiv \frac{1}{2} e_i f_i \mod \mathbb{Z}$, where e_i is the ramification index of $\mathfrak{p}$ over p and f_i is the residue class degree. If $P_A(X)$ has no real root then $e_i = e = v_{\mathfrak{p}}(p) = 2v_{\mathfrak{p}}(\sqrt{p})$, and so the ramification index is always even. This implies $\mathrm{inv}_{\mathfrak{p}}(End_k(A) \otimes \mathbb{Q}) = 0 \mod \mathbb{Z}$. In other words, the order of the invariants is zero and $2 \dim A$ is equal to the degree of the Weil polynomial. This along with the definition of the characteristic polynomial implies $P_A(X)$ is irreducible. ∎

Remark 3.2. If $P(X)$ is a supersingular Weil polynomial with all real roots, over $\mathbb{F}_q$ with $q = p^n$, n odd, then $P(X) = X^2 - q$, then we have that the least common multiple of the local invariants is 2, hence $P(X)^2$ is a characteristic polynomial of a simple supersingular abelian variety of dimension 2, see [3].

The treatment is more uniform if we allow q to be both a positive and a negative prime power. Let p be a prime and $q = (\pm p)^n$ with n odd. We wish to calculate the minimal polynomial over $\mathbb{Q}$ of $\sqrt{q}\zeta_m$. From Theorem 3.1, it follows that the following theorem also gives characteristic polynomial in these cases. Without loss of generality we assume that $m = 4t$ for some t since $\sqrt{q}\zeta_m = \sqrt{-q}\zeta_4\zeta_m = \sqrt{-q}\zeta_{m'}$.

Theorem 3.3. *Let $\theta = \sqrt{q}\zeta_{4t}$. We distinguish two cases.*

1. *Full degree case: If either*
   (a) *q is odd and*
      (i) *t is even or*
      (ii) *$p \nmid t$ or*
      (iii) *$q \equiv 1 \mod 4$*

      or
   (b) *q is even and $t \not\equiv 2 \mod 4$.*

   then the minimal polynomial of θ over $\mathbb{Q}$ is $\Phi_{4t}^{[\sqrt{q}]}(X)$.
2. *Half degree case:*
   (a) *If $q \equiv 3 \mod 4$ and $p|t$ and t is odd, then the minimal polynomial of θ is $\Psi_{p,\frac{t}{p}}^{[\sqrt{q^*}]}(X)$.*
   (b) *If $q > 0$ is even and $t = 2s \equiv 2 \mod 4$, then the minimal polynomial of θ is $\Psi_{2,s}^{[\sqrt{q}]}(X)$.*
   (c) *If $q < 0$ is even and $t = 2s \equiv 2 \mod 4$, then the minimal polynomial of θ is $\Psi_{-2,s}^{[\sqrt{q}]}(X)$.*

Proof. First suppose $p \nmid t$. Then $\sqrt{q} \notin \mathbb{Q}(\zeta_{4t})$ and $\Gamma := Gal(\mathbb{Q}(\sqrt{q}, \zeta_{4t})/\mathbb{Q}) = \langle\sigma\rangle \times Gal(\mathbb{Q}(\zeta_{4t})/\mathbb{Q})$ where $\sigma(\sqrt{q}) = -\sqrt{q}$, $\sigma(\zeta_{4t}) = \zeta_{4t}$.

Let $\tau \in \Gamma$ and suppose $\tau(\theta) = \theta$. If $\tau = \sigma_a$ then $a \in U(\mathbb{Z}/4t\mathbb{Z})$ implies $\sqrt{q}\zeta_{4t} = \sqrt{q}\zeta_{4t}^a$ which implies $a = 1$ which implies $\tau = 1$. And if $\tau = \sigma\sigma_a$ then $\sqrt{q}\zeta_{4t} = -\sqrt{q}\zeta_{4t}^a$ which implies $\zeta_{4t}^a = -\zeta_{4t} = \zeta_{4t}^{1+2t}$ which implies $a = 2t + 1$. So the subgroup of Γ fixing θ is $\{1, \sigma\sigma_{1+2t}\}$ and $Gal(\mathbb{Q}(\theta)/\mathbb{Q}) \cong Gal(\mathbb{Q}(\zeta_{4t})/\mathbb{Q})$. In particular, the conjugates of θ over $\mathbb{Q}$ are $\sigma_a(\theta) = \sqrt{q}\zeta_{4t}^a$, and the minimal polynomial of θ over $\mathbb{Q}$ is $\prod_{a \in U(\mathbb{Z}/4t\mathbb{Z})}(X - \sqrt{q}\zeta_{4t}^a) = \Phi_{4t}^{[\sqrt{q}]}(X)$.

Next suppose p is odd and $p|t$. Then $\sqrt{q} \in \mathbb{Q}(\zeta_{4t})$ and if $a \in U(\mathbb{Z}/4t\mathbb{Z})$ we have

$$\sigma_a(\theta) = \sigma_a(\sqrt{q}\zeta_{4t}) = \begin{cases} (\frac{a}{p})\sqrt{q}\zeta_{4t}^a & \text{if } q \equiv 1 \mod 4; \\ \varepsilon(a)(\frac{a}{p})\sqrt{q}\zeta_{4t}^a & \text{if } q \equiv 3 \mod 4. \end{cases}$$

Suppose $q \equiv 1 \mod 4$ and $\sigma_a(\theta) = \theta$. Then $(\frac{a}{p})\zeta_{4t}^a = \zeta_{4t}$. If $(\frac{a}{p}) = 1$ then $a = 1$ in $U(\mathbb{Z}/4t\mathbb{Z})$ implies $\sigma_a = 1$. However $(\frac{a}{p}) = -1$ implies $\zeta_{4t}^a = \zeta_{4t}^{1+2t}$ which implies $a = 1 + 2t$ or $a \equiv 1 \mod p$. This implies $(\frac{a}{p}) = 1$ which is a contradiction. So $\sigma_a = 1$ and $Gal(\mathbb{Q}(\theta)/\mathbb{Q}) = Gal(\mathbb{Q}(\zeta_{4t})/\mathbb{Q})$ whence the minimal polynomial of θ is $\Phi_{4t}^{[\sqrt{q}]}(X)$.

Now suppose $q \equiv 3 \mod 4$ and $\sigma_a(\theta) = \theta$. Then $\zeta_{4t} = \varepsilon(a)(\frac{a}{p})\sqrt{q}\zeta_{4t}^a$. Since $\varepsilon(a)(\frac{a}{p}) \in \{1, -1\}$ we have $a \in \{1, 1 + 2t\}$. If $a = 1 + 2t$ then $(\frac{a}{p}) = 1$ and $\varepsilon(a) = 1 + 2t \mod 4 = -1$ if and only if t is odd. Thus if t is even, the minimal polynomial of θ is $\Phi_{4t}^{[\sqrt{q}]}(X)$. However, if t is odd, then θ is fixed by σ_{1+2t} and hence the degree of its minimal polynomial over $\mathbb{Q}$ is $\frac{1}{2}\phi(4t) = \phi(t)$. However, in this case $\sqrt{q}\zeta_{4t} = \pm\sqrt{-q}\zeta_t = \pm\sqrt{q^*}\zeta_t \in \mathbb{Q}(\zeta_t)$ and thus its minimal polynomial is $\prod_{a\in U(\mathbb{Z}/t\mathbb{Z})}(X - (\frac{a}{p})\zeta_t^a) = \Psi_{p,\frac{t}{p}}^{[\sqrt{q^*}]}(X)$.

We now consider the case q is even and $2|t$. So $4t = 8s$ for some $s > 0$. Let $\zeta = \zeta_{4t} = \zeta_{8s}$. Then $\theta \in \mathbb{Q}(\zeta)$ and

$$\sigma_a(\theta) = \sigma_a(\sqrt{q}\zeta) = \begin{cases} (\chi_2(a)\sqrt{q}\zeta^a & \text{if } q > 0; \\ \chi_{-2}(a)\sqrt{q}\zeta^a & \text{if } q < 0. \end{cases}$$

Suppose $\sigma_a(\theta) = \theta$. Then $\chi_{\pm 2}(a) = -1$ and $a = 1 + 4s \in U(\mathbb{Z}/8s\mathbb{Z})$. If s is even then $a \equiv 1 \mod 8$ which implies $\chi_{\pm 2}(a) = 1$ which a contradiction. Thus if s is even, the minimal polynomial of θ is $\Phi_{4t}^{[\sqrt{q}]}(X)$. We can suppose that $4t = 8s$ with s odd. Then $1 + 4s = -3 \in U(\mathbb{Z}/8s\mathbb{Z})$. It follows that θ is fixed by the $\{1, \sigma_{1+4s}\}$ and so its minimal polynomial has degree $\frac{1}{2}\phi(4t)$. We can write ζ as a product $\zeta_8\zeta_s$. So $\theta = \sqrt{q}\zeta_8\zeta_s$. If $q > 0$, the conjugates of θ are $\sqrt{q}\zeta_8\zeta_s^a$ and $\sqrt{q}\zeta_8^{-1}\zeta_s^a$ as a ranges over $U(\mathbb{Z}/s\mathbb{Z})$. Thus the minimal polynomial is

$$\prod_{a\in U(\mathbb{Z}/s\mathbb{Z})}(X - \sqrt{q}\zeta_8\zeta_s^a)(X - \sqrt{q}\zeta_8^{-1}\zeta_s^a) = \Psi_{2,s}^{[\sqrt{q}]}(X).$$

Similarly, if $q < 0$, the minimal polynomial of θ is $\Psi_{-2,s}^{[\sqrt{q}]}(X)$. This proves the theorem. ∎

Remark 3.4.

1. As the name suggests in full degree case, the degree of the minimal polynomial of θ is $\phi(4t)$ and in the half degree case the degree is $\frac{1}{2}\phi(4t)$.
2. It easily follows that the polynomials $\Psi_{p,t}$ can be calculated recursively in the same way as cyclotomic polynomials:

$$\Psi_{p,tp^k}(X) = \Psi_{p,t}(X^{p^{k-1}}).$$

If l is a prime not dividing t then

$$\Psi_{p,l^k}(X) = \frac{\Psi_{p,t}(X^{l^k})}{\Psi_{p,t}(X^{l^{k-1}})}.$$

4. When q is a square

If $P(X)$ is a supersingular Weil polynomial with all real roots, over $\mathbb{F}_q$ with $q = p^n$, n even, then $P(X) = X \pm \sqrt{q}$ and the least common multiple of the local invariants is 2, hence $P(X)^2$ is the characteristic polynomial of a simple supersingular abelian variety of dimension 1.

We prove the following theorem which characterizes all the possible characteristic polynomials of abelian varieties over $\mathbb{F}_q$.

Theorem 4.1. *Let $q = p^n$ where n is even. Let A be a simple supersingular abelian variety over $\mathbb{F}_q$ of dimension g. Then the Weil polynomial of A has the form $(\Phi_m^{[\sqrt{q}]}(X))^e$. Conversely, if $\phi(m) = 2g$ then $(\Phi_m^{[\sqrt{q}]}(X))^e$ is the characteristic polynomial of the Frobenius endomorphism of a simple supersingular abelian variety of dimension ge over $\mathbb{F}_q$, $q = p^n$, n even, where*

$$r = \begin{cases} \text{order of } p \text{ in the multiplicative group } U(\mathbb{Z}/m\mathbb{Z}), & \text{if } (p,m) = 1; \\ f(p^k - p^{k-1}),\ f \text{ is order of } p & \\ \text{in the multiplicative group } U(\mathbb{Z}/s\mathbb{Z}) & \text{if } m = p^k s. \end{cases}$$

and

$$e = \begin{cases} 1, & \text{if } r \text{ is even;} \\ 2, & \text{if } r \text{ is odd.} \end{cases}$$

Proof. Let $P_A(X)$ be the Weil polynomial of a simple supersingular abelian variety A of dimension g. Then $P_A(X) = P(X)^e$ where $P(X)$ is an irreducible supersingular Weil polynomial of degree $\frac{2g}{e}$ with $e = 1$ or 2. Since q is an even power of prime, $\sqrt{q} \in \mathbb{Z}$. Using Honda-Tate (Theorem 2.2) we get $\frac{1}{q^{\frac{g}{e}}}(P(\sqrt{q}X))$ is an irreducible cyclotomic polynomial $\Phi_m(X)$ over $\mathbb{Z}$ of degree $\frac{2g}{e}$, i.e. $\phi(m) = \frac{2g}{e}$. Therefore $P(X) = \Phi_m^{[\sqrt{q}]}(X)$.

Conversely, let $\phi(m) = 2g$, then $P(X) = \Phi_m^{[\sqrt{q}]}(X)$ is an irreducible supersingular Weil polynomial of degree $2g$. Therefore by Honda-Tate (Theorem 2.2) $P(X)^e$ is a Weil polynomial for some supersingular simple abelian variety. To determine the dimension of the corresponding abelian variety to $P(X)$, we will need to factorise $P(X)$ over $\mathbb{Q}_p$. If $P(X) = \prod_i f_i(X)$ is the factorisation over $\mathbb{Q}_p[X]$, then

$$\text{inv}_{\mathfrak{p}_i}(End_k(A) \otimes \mathbb{Q}) \equiv \frac{v_p(f_i(0))}{v_p(q)} \mod \mathbb{Z} \equiv \frac{\deg f_i}{2} \mod \mathbb{Z}.$$

Since $P(X) = \Phi_m^{[\sqrt{q}]}(X)$, $\text{inv}_{\mathfrak{p}_i}(End_k(A) \otimes \mathbb{Q}) = \frac{\deg r_i}{2} \mod \mathbb{Z}$, where $\Phi_m(X) = \prod_i r_i(X)$ over $\mathbb{Q}_p$. But it follows from the chapter IV.4 in [11] that $\deg r_i = r$, where

$$r = \begin{cases} \text{order of } p \text{ in the multiplicative group } U(\mathbb{Z}/m\mathbb{Z}), & \text{if } (p,m) = 1; \\ f(p^k - p^{k-1}), & \text{if } m = p^k s. \end{cases}$$

where f is order of p in the multiplicative group $U(\mathbb{Z}/s\mathbb{Z})$.

Hence

$$e = \mathrm{inv}_{\mathfrak{p}_i}(End_k(A) \otimes \mathbb{Q}) = \begin{cases} 1 & \text{if } r \text{ is even;} \\ 2 & \text{if } r \text{ is odd.} \end{cases}$$

From Theorem 2.4, $2 \dim A = e \deg P(X)$ or $\dim A = eg$. ■

In the following sections we treat each dimension separately, up to dimension 7 for $q = p^n$, n odd. We use theorem 3.3 all the time, without mentioning it explicitly. Let θ be a root of the characteristic polynomial of Frobenius endomorphism.

5. Dimension 1

5.1. Full degree case

In this case $\phi(4t) = 2g = 2$ which implies $t = 1$. Therefore $X^2 \pm q$ is a Weil polynomial.

5.2. Half degree case

In this case $\frac{1}{2}\phi(4t) = 2g = 2$. That implies $4t \in \{8, 12\}$ or $t \in \{2, 3\}$. In case $t = 2$ then $q = (\pm 2)^n$ with n odd. Then,

1. If $q > 0$ then the minimal polynomial of θ is $\Psi_{2,1}^{[\sqrt{q}]}(X)$.
   But, $\Psi_{2,1}(X) = (X - \zeta_8)(X - \zeta_8^{-1}) = X^2 \pm (\zeta_8 + \zeta_8^{-1})X + 1 = X^2 \pm \sqrt{2}X + 1$.
   Therefore $\Psi_{2,1}^{[\sqrt{q}]}(X) = X^2 \pm \sqrt{2q}X + q$.
2. If $q < 0$, then the minimal polynomial of θ is $\Psi_{-2,1}^{[\sqrt{q}]}(X)$.
   But, $\Psi_{2,1}(X) = (X - \zeta_8)(X - \zeta_8^3) = X^2 \pm (\zeta_8 + \zeta_8^3)X - 1 = X^2 \pm \sqrt{-2}X - 1$.
   Therefore $\Psi_{-2,1}^{[\sqrt{q}]}(X) = X^2 \pm \sqrt{-2q}X - q$.

In case $t = 3$, then $p = 3$ and $q = 3^n$ with n odd. In that case, the minimal polynomial of θ is $\Psi_{3,1}^{[\sqrt{q}]}(X)$.
But, $\Psi_{3,1}(X) = \prod_{a \in U(\mathbb{Z}/3\mathbb{Z})}(X - (\frac{a}{3})\zeta_3^a) = X^2 - \sum_{a=1}^{2}(\frac{a}{p})X + 1 = X^2 \pm \sqrt{-3}X - 1$.
Therefore $\Psi_{3,1}^{[\sqrt{q^*}]}(X) = X^2 \pm \sqrt{3q}X + q$.

6. Dimension 2

6.1. Full degree case

In this case $\phi(4t) = 2g = 4$. That implies $4t \in \{8, 12\}$ or $t \in \{2, 3\}$. Therefore either $t = 2$, p odd and the minimal polynomial is

$$\Phi_8^{[\sqrt{q}]}(X) = X^4 + q^2,$$

or $t = 3$, $q \neq 3^n$, n odd and the minimal polynomial is

$$\Phi_{12}^{[\sqrt{q}]}(X) = X^4 - qX^2 + q^2.$$

6.2. Half degree case

In this case $\frac{1}{2}\phi(4t) = 2g = 4$. That implies $4t \in \{16, 20, 24\}$ or $t \in \{4, 5, 6\}$.

1. Either p is odd, t is odd, p divides t, $q \equiv 3 \mod 4$.
   In that case, $t = p = 5$, $q = (-5)^n$ with n odd and $\Psi_{5,1}^{[\sqrt{q^*}]}(X)$ is the minimal polynomial of θ. We have $\Psi_{5,1}(X)\Psi_{5,1}(-X) = \Phi_5(X^2)$. Therefore, $\Psi_{5,1}(X) = X^4 \pm \sqrt{5}X^3 + 3X^2 \pm \sqrt{5}X + 1$ and

$$\Psi_{5,1}^{[\sqrt{q^*}]}(X) = X^4 \pm \sqrt{-5q}X^3 - 3qX^2 \mp q\sqrt{-5q}X + q^2.$$

2. $t \equiv 2 \mod 4$, $q = (\pm 2)^n$ with n odd. In that case, $t = 6 = 2 \cdot 3 \mod 4$. Then

   (a) If $q > 0$ then the minimal polynomial of θ is $\Psi_{2,3}^{[\sqrt{q}]}(X)$.
   But,

$$\Psi_{2,3}(X) = \frac{\Psi_{2,1}(X^3)}{\Psi_{2,1}(X)} = X^4 \pm \sqrt{2}X^3 + X^2 \pm \sqrt{2}X + 1$$

   and hence

$$\Psi_{2,3}^{[\sqrt{q}]}(X) = X^4 \pm \sqrt{2q}X^3 + qX^2 \pm q\sqrt{2q}X + q^2.$$

   (b) If $q < 0$, then the minimal polynomial of θ is $\Psi_{-2,3}^{[\sqrt{q}]}(X)$.
   But,

$$\Psi_{-2,3}(X) = X^4 \pm \sqrt{-2}X^3 - X^2 \mp \sqrt{-2}X + 1$$

   and hence

$$\Psi_{-2,3}^{[\sqrt{q}]}(X) = X^4 \pm \sqrt{-2q}X^3 - qX^2 \mp q\sqrt{-2q}X + q^2.$$

7. Dimension 3

7.1. Full degree case

In this case $\phi(4t) = 2g = 6$ and there is no such t. Therefore there are no possible polynomials.

7.2. Half degree case

In this case $\frac{1}{2}\phi(4t) = 2g = 6$. That implies $4t \in \{28, 36\}$ or $t \in \{7, 9\}$. In that case, p is odd, t is odd, p divides t, $q \equiv 3 \mod 4$.

1. $t = 7,\ p = 7,\ q = 7^n$ with n odd, then $\Psi_{7,1}^{[\sqrt{q^*}]}(X)$ is the minimal polynomial of θ.
   But $\Psi_{7,1}(X)\Psi_{7,1}(-X) = \Phi_7(X^2)$ and therefore,
   $$\Psi_{7,1}(X) = X^6 \pm \sqrt{-7}X^5 - 3X^4 \mp \sqrt{-7}X^3 + 3X^2 \pm \sqrt{-7}X - 1.$$
   This gives,
   $$\Psi_{7,1}^{[\sqrt{q^*}]}(X) = X^6 \pm \sqrt{7q}X^5 + 3qX^4 \pm q\sqrt{7q}X^3 + 3q^2X^2 \pm q^2\sqrt{7q}X + q^3$$
2. $t = 9,\ p = 3,\ q = 3^n$ with n odd, then $\Psi_{3,3}^{[\sqrt{q^*}]}(X)$ is the minimal polynomial of θ.
   But,
   $$\Psi_{3,3}(X) = \Psi_{3,1}(X^3) = X^6 \pm \sqrt{-3}X^3 - 1$$
   and hence,
   $$\Psi_{3,3}^{[\sqrt{q^*}]}(X) = X^6 \pm q\sqrt{3q}X^3 + q^3.$$

8. Dimension 4

8.1. Full degree case

In this case $\phi(4t) = 2g = 8$. That implies $4t \in \{16, 20, 24\}$ or $t \in \{4, 5, 6\}$. We have the following possibilities.

1. If $t = 4$ then,
   (a) q is odd and t is even,
   (b) q is even and $t \not\equiv 2 \mod 4$.
   Therefore the minimal polynomial is
   $$\Phi_{16}^{[\sqrt{q}]}(X) = X^8 + q^4$$
   for all primes p.
2. If $t = 5$ then,
   (a) q is odd and $p \nmid t$ but $p \equiv 1 \mod 4$, this implies $q \neq (-5)^n$, n odd.
   (b) q is even and $t \not\equiv 2 \mod 4$.
   Therefore the minimal polynomial is
   $$\Phi_{20}^{[\sqrt{q}]}(X) = X^8 - qX^6 + q^2X^4 - q^3X^2 + q^4$$
   for all $q \neq (-5)^n,\ n$ odd.
3. If $t = 6$ then,
   (a) q is odd and t is even,
   Therefore the minimal polynomial is
   $$\Phi_{24}^{[\sqrt{q}]}(X) = X^8 - q^2X^4 + q^4$$
   for all primes $p \neq 2$.

8.2. Half degree case

In this case $\frac{1}{2}\phi(4t) = 2g = 8$. That implies $4t \in \{32, 40, 48, 60\}$ or $t \in \{8, 10, 12, 15\}$. We have the following possibilities.

1. Either p is odd, t is odd, p divides t, $q \equiv 3 \mod 4$. In that case $t = 15$ then
   (a) either $p = 3,\ q = 3^n$ with n odd and $\Psi_{3,5}^{[\sqrt{q^*}]}(X)$ is the minimal polynomial of θ.
   Since
   $$\Psi_{3,5}(X) = \frac{\Psi_{3,1}(X^5)}{\Psi_{3,1}(X)},$$
   we have
   $$\Psi_{3,5}^{[\sqrt{q^*}]}(X) = X^8 \mp \sqrt{3q}X^7 + 2qX^6 \mp q\sqrt{3q}X^5 + q^2X^4 \mp \sqrt{3q}X^3 + 2X^2 \pm q^3\sqrt{3q}X + q^4$$
   or
   (b) $p = 5,\ q = (-5)^n$ with n odd and $\Psi_{5,3}^{[\sqrt{q^*}]}(X)$ is the minimal polynomial of θ.
   We have,
   $$\Psi_{5,3}(X) = \frac{\Psi_{5,1}(X^3)}{\Psi_{5,1}(X)} = X^8 \pm \sqrt{5}X^7 + 2X^6 \pm \sqrt{5}X^5 + 3X^4 \pm \sqrt{5}X^3 + 2X^2 \pm \sqrt{5}X + 1$$
   and hence
   $$\Psi_{5,3}^{[\sqrt{q^*}]}(X) = X^8 \pm \sqrt{-5q}X^7 - 2qX^6 \mp q\sqrt{-5q}X^5 + 3q^2X^4 \pm q^2\sqrt{-5q}X^3 - 2q^3X^2 \mp q^3\sqrt{-5q}X + q^4.$$
2. $t \equiv 2 \mod 4,\ q = (\pm 2)^n$ with n odd. In that case $t = 10 = 2 \cdot 5 \mod 4$.
   (a) If $q > 0$ then the minimal polynomial of θ is $\Psi_{2,5}^{[\sqrt{q}]}(X)$.
   But,
   $$\Psi_{2,5}(X) = \frac{\Psi_{2,1}(X^5)}{\Psi_{2,1}(X)} = X^8 \pm \sqrt{2}X^7 + X^6 - X^4 + X^2 \pm \sqrt{2}X + 1$$
   and hence
   $$\Psi_{2,5}^{[\sqrt{q}]}(X) = X^8 \pm \sqrt{2q}X^7 + qX^6 - q^2X^4 + q^3X^2 \pm q^3\sqrt{2q}X + q^4.$$
   (b) If $q < 0$, then the minimal polynomial of θ is $\Psi_{-2,5}^{[\sqrt{q}]}(X)$.
   But,
   $$\Psi_{-2,5}(X) = X^8 \pm \sqrt{-2}X^7 - X^6 - X^4 - X^2 \mp \sqrt{-2}X + 1.$$
   Therefore
   $$\Psi_{-2,5}^{[\sqrt{q}]}(X) = X^8 \pm \sqrt{-2q}X^7 - qX^6 - q^2X^4 - q^3X^2 \mp q^3\sqrt{-2q}X + q^4.$$

9. Dimension 5

9.1. Full degree case

In this case $\phi(4t) = 2g = 10$ and there is no such t. Therefore there are no possible polynomials.

9.2. Half degree case

In this case $\frac{1}{2}\phi(4t) = 2g = 10$. That implies $4t = 44$ or $t = 11$. In that case, $p = 11$, $q = 11^n$, then $\Psi_{11,1}^{[\sqrt{q^*}]}(X)$ is the minimal polynomial of θ. But $\Psi_{11,1}(X)\Psi_{11,1}(-X) = \Phi_{11}(X^2)$ which implies

$$\begin{aligned}\Psi_{11,1}(X) = X^{10} \mp \sqrt{-11}X^9 - 5X^8 \pm \sqrt{-11}X^7 - X^6 \pm \sqrt{-11}X^5 \\ + X^4 \pm \sqrt{-11}X^3 + 5X^2 \mp \sqrt{-11}X - 1.\end{aligned}$$

Hence,

$$\begin{aligned}\Psi_{11,1}^{[\sqrt{q^*}]}(X) = X^{10} \mp \sqrt{11q}X^9 + 5qX^8 \mp q\sqrt{11q}X^7 - q^2X^6 \pm q^2\sqrt{11q}X^5 \\ - q^3X^4 \mp q^3\sqrt{11q}X^3 + 5q^4X^2 \mp q^4\sqrt{11q}X + q^5.\end{aligned}$$

10. Dimension 6

10.1. Full degree case

In this case $\phi(4t) = 2g = 12$. That implies $4t \in \{28, 36\}$ or $t \in \{7, 9\}$. We have the following possibilities

1. If $t = 7$ then,
   (a) q is odd and $p \nmid t$ but $-7 \equiv 1 \mod 4$ i.e; $q \neq 7^n$, n odd.
   (b) q is even and $t \not\equiv 2 \mod 4$.
   Therefore the minimal polynomial is
   $$\Phi_{28}^{[\sqrt{q}]}(X) = X^{12} - qX^{10} + q^2X^8 - q^3X^6 + q^4X^4 - q^5X^2 + q^6$$
   for $q \neq 7^n$, n odd.
2. If $t = 9$ then,
   (a) q is odd and $p \nmid t$ but $-3 \equiv 1 \mod 4$ i.e; $q \neq 3^n$, n odd.
   (b) q is even and $t \not\equiv 2 \mod 4$.
   Therefore the minimal polynomial is
   $$\Phi_{36}^{[\sqrt{q}]}(X) = X^{12} - q^3X^6 + q^6$$
   for $q \neq 3^n$, n odd.

10.2. Half degree case

In this case $\frac{1}{2}\phi(4t) = 2g = 12$. That implies $4t \in \{52, 56, 72, 84\}$ or $t \in \{13, 14, 18, 21\}$.

1. Either p is odd, t is odd, p divides t, $q \equiv 3 \mod 4$

   (a) $t = p = 13$, $q = (-13)^n$ and $\Psi_{13,1}^{[\sqrt{q^*}]}(X)$ is the minimal polynomial of θ. But $\Psi_{13,1}(X)\Psi_{13,1}(-X) = \Phi_{13}(X^2)$ which implies

   $$\Psi_{13,1}(X) = X^{12} \pm \sqrt{13}X^{11} + 7X^{10} \pm 3\sqrt{13}X^9 + 15X^8 \pm 5\sqrt{13}X^7 + 19X^6 \pm 5\sqrt{13}X^5 + 15X^4 \pm 3\sqrt{13}X^3 + 7X^2 \pm \sqrt{13}X + 1$$

   and therefore

   $$\Psi_{13,1}^{[\sqrt{q^*}]}(X) = X^{12} \pm \sqrt{-13q}X^{11} - 7qX^{10} \mp 3q\sqrt{-13q}X^9 + 15q^2X^8 \pm 5q^2\sqrt{-13q}X^7 - 19q^3X^6 \mp 5q^3\sqrt{-13q}X^5 + 15q^4X^4 \pm 3q^4\sqrt{-13q}X^3 - 7q^5X^2 \mp q^5\sqrt{-13q}X + q^6.$$

   (b) $t = 21$, then

   (i) $p = 3$, $q = 3^n$ with n odd and $\Psi_{3,7}^{[\sqrt{q^*}]}(X)$ is the minimal polynomial of θ.
   But

   $$\Psi_{3,7}(X) = \frac{\Psi_{3,1}(X^7)}{\Psi_{3,1}(X)} = X^{12} \pm \sqrt{-3}X^{11} - 2X^{10} \mp \sqrt{-3}X^9 + X^8 + X^6 + X^4 \pm \sqrt{-3}X^3 - 2X^2 \mp \sqrt{-3}X + 1$$

   and hence

   $$\Psi_{3,7}^{[\sqrt{q^*}]}(X) = X^{12} \pm \sqrt{3q}X^{11} + 2qX^{10} \pm q\sqrt{3q}X^9 + q^2X^8 - q^3X^6 + q^4X^4 \pm q^4\sqrt{3q}X^3 + 2q^5X^2 \pm q^5\sqrt{3q}X + q^6$$

   or

   (ii) $p = 7$, $q = 7^n$ with n odd and $\Psi_{7,3}^{[\sqrt{q^*}]}(X)$ is the minimal polynomial of θ.

   $$\Psi_{7,3}(X) = \frac{\Psi_{7,1}(X^3)}{\Psi_{7,1}(X)} = X^{12} \pm \sqrt{-7}X^{11} - 4X^{10} \mp \sqrt{-7}X^9 - X^8 \mp 2\sqrt{-7}X^7 + 7X^6 \pm 2\sqrt{-7}X^5 - X^4 \pm \sqrt{-7}X^3 - 4X^2 \mp \sqrt{-7}X + 1.$$

   Hence,

   $$\Psi_{7,3}^{[\sqrt{q^*}]}(X) = X^{12} \pm \sqrt{7q}X^{11} + 4qX^{10} \pm q\sqrt{7q}X^9 - q^2X^8 \mp 2q^2\sqrt{7q}X^7 - 7q^3X^6 \mp 2q^3\sqrt{7q}X^5 - q^4X^4 \pm q^4\sqrt{7q}X^3 + 4q^5X^2 \pm q^5\sqrt{7q}X + q^6.$$

2. $t \equiv 2 \mod 4$, q even.
   (a) $t = 14 = 2 \cdot 7 \mod 4$.
      (i) If $q > 0$ then the minimal polynomial of θ is $\Psi_{2,7}^{[\sqrt{q}]}(X)$. But

$$\Psi_{2,7}(X) = \frac{\Psi_{2,1}(X^7)}{\Psi_{2,1}(X)} = X^{12} \mp \sqrt{2}X^{11} + X^{10} - X^8 \pm \sqrt{2}X^7 - X^6 \pm \sqrt{2}X^5 - X^4 + X^2 \mp \sqrt{2}X + 1$$

and hence,

$$\Psi_{2,7}^{[\sqrt{q}]}(X) = X^{12} \mp \sqrt{2q}X^{11} + qX^{10} - q^2X^8 \pm q^2\sqrt{2q}X^7 - q^3X^6 \pm q^3\sqrt{2q}X^5 - q^4X^4 + q^5X^2 \mp q^5\sqrt{2q}X + q^6.$$

      (ii) If $q < 0$, then the minimal polynomial of θ is $\Psi_{-2,7}^{[\sqrt{q}]}(X)$. But,

$$\Psi_{-2,7}(X) = X^{12} \pm \sqrt{-2}X^{11} - X^{10} - X^8 \mp \sqrt{-2}X^7 + X^6 \pm \sqrt{-2}X^5 - X^4 - X^2 \mp \sqrt{-2}X + 1$$

$$\Psi_{-2,7}^{[\sqrt{q}]}(X) = X^{12} \pm \sqrt{-2q}X^{11} - qX^{10} - q^2X^8 \mp q^2\sqrt{-2q}X^7 + q^3X^6 \pm q^3\sqrt{-2q}X^5 - q^4X^4 - q^5X^2 \mp q^5\sqrt{-2q}X + q^6.$$

   (b) $t = 18 = 2 \cdot 9 \mod 4$ with q even. In that case,
      (i) If $q > 0$ then the minimal polynomial of θ is $\Psi_{2,9}^{[\sqrt{q}]}(X)$. But,

$$\Psi_{2,9}(X) = \frac{\Psi_{2,1}(X^{3^2})}{\Psi_{2,1}(X^3)} = X^{12} \pm \sqrt{2}X^9 + X^6 \pm \sqrt{2}X^3 + 1.$$

and hence,

$$\Psi_{2,9}^{[\sqrt{q}]}(X) = X^{12} \pm q\sqrt{2q}X^9 + q^3X^6 \pm q^4\sqrt{2q}X^3 + q^6.$$

      (ii) If $q < 0$, then the minimal polynomial of θ is $\Psi_{-2,9}^{[\sqrt{q}]}(X)$. But, $\Psi_{-2,9}(X) = X^{12} \pm \sqrt{-2}X^9 - X^6 \mp \sqrt{-2}X^3 + 1$. Therefore $\Psi_{-2,9}^{[\sqrt{q}]}(X) = X^{12} \pm q\sqrt{-2q}X^9 - q^3X^6 \pm q^4\sqrt{-2q}X^3 + q^6$.

11. Dimension 7

11.1. Full degree case

In this case $\phi(4t) = 2g = 14$ and there is no such t. Therefore there are no possible polynomials.

11.2. Half degree case

In this case $\frac{1}{2}\phi(4t) = 2g = 14$ and there is no such t. Therefore there are no possible polynomials.

12. Summary of results for dimensions 1 to 7

We gather the list of characteristic polynomials, from dimensions 1 to 7, with references for the previously known cases.

Theorem 12.1. *Let A be an supersingular simple abelian variety over $\mathbb{F}_q$, where $q = p^n$, n odd. Then the characteristic polynomial of A must be one of the following:*

1. *Dimension 1* (Deuring and Waterhouse[2, 14])
   (a) $p = 2 : X^2 \pm \sqrt{2q}X + q$,
   (b) $p = 3 : X^2 \pm \sqrt{3q}X + q$,
   (c) $X^2 + q$.
2. *Dimension 2* (C.Xing, D.Maisner and E.Nart[15, 6])
   (a) $p \neq 3 : X^4 - qX^2 + q^2$,
   (b) $X^4 + qX^2 + q^2$,
   (c) $p = 2 : X^4 \pm \sqrt{pq}X^3 + qX^2 \pm q\sqrt{pq}X + q^2$,
   (d) $p = 5 : X^4 \pm \sqrt{pq}X^3 + 3qX^2 \pm q\sqrt{pq}X + q^2$,
   (e) $(X^2 - q)^2$,
   (f) $p \neq 2 : X^4 + q^2$.
3. *Dimension 3* (E.Nart, C.Ritzenthaler and S.Haloui [4, 7])
   (a) $p = 3 : X^6 \pm q\sqrt{pq}X^3 + q^3$, *or*
   (b) $p = 7 : X^6 \pm \sqrt{pq}X^5 + 3qX^4 \pm q\sqrt{pq}X^3 + 3q^2X^2 \pm q^2\sqrt{pq}X + q^3$.
4. *Dimension 4* (S.Haloui, V.Singh [5])
   (a) $X^8 + q^4$,
   (b) $X^8 - qX^6 + q^2X^4 - q^3X^2 + q^4$,
   (c) $p \neq 5 : X^8 + qX^6 + q^2X^4 + q^3X^2 + q^4$,
   (d) $p \neq 2 : X^8 - q^2X^4 + q^4$,
   (e) $p = 3 : X^8 \pm \sqrt{3q}X^7 + 2qX^6 \pm q\sqrt{3q}X^5 + q^2X^4 \pm q^2\sqrt{3q}X^3 + 2q^3X^2 \pm q^3\sqrt{3q}X + q^4$,
   (f) $p = 5 : X^8 \pm \sqrt{5q}X^7 + 2qX^6 \pm q\sqrt{5q}X^5 + 3q^2X^4 \pm q^2\sqrt{5q}X^3 + 2q^3X^2 \pm q^3\sqrt{5q}X + q^4$,
   (g) $p = 2 : X^8 \pm \sqrt{2q}X^7 + qX^6 - q^2X^4 + q^3X^2 \pm q^3\sqrt{2q}X + q^4$.

5. *Dimension 5*
   (a) $p = 11 : X^{10} \mp \sqrt{11q}X^9 + 5qX^8 \mp q\sqrt{11q}X^7 - q^2X^6 \pm q^2\sqrt{11q}X^5 - q^3X^4 \mp q^3\sqrt{11q}X^3 + 5q^4X^2 \mp q^4\sqrt{11q}X + q^5$.
6. *Dimension 6*
   (a) $X^{12} + qX^{10} + q^2X^8 + q^3X^6 + q^4X^4 + q^5X^2 + q^6$,
   (b) $p \neq 7 : X^{12} - qX^{10} + q^2X^8 - q^3X^6 + q^4X^4 - q^5X^2 + q^6$,
   (c) $X^{12} + q^3X^6 + q^6$,
   (d) $p \neq 3 : X^{12} - q^3X^6 + q^6$,
   (e) $X^{12} \pm \sqrt{13q}X^{11} + 7qX^{10} \pm 3q\sqrt{13q}X^9 + 15q^2X^8 \pm 5q^2\sqrt{13q}X^7 + 19q^3X^6 \pm 5q^3\sqrt{13q}X^5 + 15q^4X^4 \pm 3q^4\sqrt{13q}X^3 + 7q^5X^2 \pm q^5\sqrt{13q}X + q^6$
   (f) $X^{12} \pm \sqrt{3q}X^{11} + 2qX^{10} \pm q\sqrt{3q}X^9 + q^2X^8 - q^3X^6 + q^4X^4 \pm q^4\sqrt{3q}X^3 + 2q^5X^2 \pm q^5\sqrt{3q}X + q^6$.
   (g) $X^{12} \pm \sqrt{7q}X^{11} + 4qX^{10} \pm q\sqrt{7q}X^9 - q^2X^8 \mp 2q^2\sqrt{7q}X^7 - 7q^3X^6 \mp 2q^3\sqrt{7q}X^5 - q^4X^4 \pm q^4\sqrt{7q}X^3 + 4q^5X^2 \pm q^5\sqrt{7q}X + q^6$,
   (h) $X^{12} \mp \sqrt{2q}X^{11} + qX^{10} - q^2X^8 \pm q^2\sqrt{2q}X^7 - q^3X^6 \pm q^3\sqrt{2q}X^5 - q^4X^4 + q^5X^2 \mp q^5\sqrt{2q}X + q^6$,
   (i) $X^{12} \pm q\sqrt{2q}X^9 + q^3X^6 \pm q^4\sqrt{2q}X^3 + q^6$.
7. *Dimension 7* (K.Rubin, A.Silverberg [10])
   There is no supersingular simple abelian variety of dimension 7.

Furthermore, for each of these polynomials, there exists a simple abelian variety of the given dimension having that polynomial as its Weil polynomial.

The proof of this theorem follows from Section 3.

Theorem 12.2. *Let A be an supersingular simple abelian variety over $\mathbb{F}_q$, where $q = p^n$, n even. Then the characteristic polynomial of A must be one of the following:*

1. *Dimension 1* (Deuring and Waterhouse[2, 14])
   (a) $X^2 + X\sqrt{q} + q$, $p \not\equiv 1 \mod 3$,
   (b) $X^2 + q$, $p \not\equiv 1 \mod 4$,
   (c) $X^2 - X\sqrt{q} + q$, $p \not\equiv 1 \mod 6$,
   (d) $(X \pm \sqrt{q})^2$.
2. *Dimension 2* (C.Xing, D.Maisner and E.Nart[15, 6])
   (a) $(X^2 + X\sqrt{q} + q)^2$, $p \equiv 1 \mod 3$,
   (b) $(X^2 + q)^2$, $p \equiv 1 \mod 4$,
   (c) $(X^2 - X\sqrt{q} + q)^2$, $p \equiv 1 \mod 6$,
   (d) $X^4 + \sqrt{q}X^3 + qX^2 + q^{3/2}X + q^2$, $p \not\equiv 1 \mod 5$,
   (e) $X^4 + q^2$, $p \not\equiv 1 \mod 8$,

(f) $X^4 - \sqrt{q}X^3 + qX^2 - q^{3/2}X + q^2$, $p \not\equiv 1v \mod 10$,

(g) $X^4 - qX^2 + q^2$, $p \not\equiv 1 \mod 12$.

3. *Dimension 3* (E.Nart, C.Ritzenthaler and S.Haloui [4, 7])

(a) $X^6 + \sqrt{q}X^5 + qX^4 + q^{3/2}X^3 + q^2X^2 + q^{5/2}X + q^3$, $p \not\equiv 1, 2, 4 \mod 7$,

(b) $X^6 + q^{3/2}X^3 + q^3$, $p \not\equiv 1\ ,\ 4,\ 7 \mod 9$,

(c) $X^6 - \sqrt{q}X^5 + qX^4 - q^{3/2}X^3 + q^2X^2 - q^{5/2}X + q^3$, $p \not\equiv 1, 9, 11 \mod 14$,

(d) $X^6 - q^{3/2}X^3 + q^3$, $p \not\equiv 1, 7, 13 \mod 18$.

4. *Dimension 4* (S.Haloui, V.Singh [5])

(a) $(X^4 + \sqrt{q}X^3 + qX^2 + q^{3/2}X + q^2)^2$, $p \equiv 1 \mod 5$,

(b) $(X^4 + q^2)^2$, $p \equiv 1 \mod 8$,

(c) $(X^4 - \sqrt{q}X^3 + qX^2 - q^{3/2}X + q^2)^2$, $p \equiv 1 \mod 10$,

(d) $(X^4 - qX^2 + q^2)^2$, $p \equiv 1 \mod 12$,

(e) $X^8 - \sqrt{q}X^7 + q^{3/2}X^5 - q^2X^4 + q^{5/2}X^3 - q^{7/2}X + q^4$, $p \not\equiv 1 \mod 15$,

(f) $X^8 + q^4$, $p \not\equiv 1 \mod 16$,

(g) $X^8 - qX^6 + q^2X^4 - q^3X^2 + q^4$, $p \not\equiv 1 \mod 20$,

(h) $X^8 - q^2X^4 + q^4$, $p \not\equiv 1 \mod 24$,

(i) $X^8 + \sqrt{q}X^7 - q^{3/2}X^5 - q^2X^4 - q^{5/2}X^3 + q^{7/2}X + q^4$, $p \not\equiv 1 \mod 30$.

5. *Dimension 5*

(a) $X^{10} + \sqrt{q}X^9 + qX^8 + q^{3/2}X^7 + q^2X^6 + q^{5/2}X^5 + q^3X^4 + q^{7/2}X^3 + q^4X^2 + q^{9/2}X + q^5$, $p \not\equiv 1, 3, 4, 5, 9 \mod 11$,

(b) $X^{10} - \sqrt{q}X^9 + qX^8 - q^{3/2}X^7 + q^2X^6 - q^{5/2}X^5 + q^3X^4 - q^{7/2}X^3 + q^4X^2 - q^{9/2}X + q^5$, $p \not\equiv 1, 3, 5, 9, 15 \mod 22$.

6. *Dimension 6*

(a) $(X^6 + \sqrt{q}X^5 + qX^4 + q^{3/2}X^3 + q^2X^2 + q^{5/2}X + q^3)^2$, $p \equiv 1, 2, 4 \mod 7$,

(b) $(X^6 + q^{3/2}X^3 + q^3)^2$, $p \equiv 1\ ,\ 4,\ 7 \mod 9$,

(c) $(X^6 - \sqrt{q}X^5 + qX^4 - q^{3/2}X^3 + q^2X^2 - q^{5/2}X + q^3)^2$, $p \equiv 1, 9, 11 \mod 14$,

(d) $(X^6 - q^{3/2}X^3 + q^3)^2$, $p \equiv 1, 7, 13 \mod 18$,

(e) $X^{12} + \sqrt{q}X^{11} + qX^{10} + q^{3/2}X^9 + q^2X^8 + q^{5/2}X^7 + q^3X^6 + q^{7/2}X^5 + q^4X^4 + q^{9/2}X^3 + q^5X^2 + q^{11/2}X + q^6$, $p \not\equiv 1, 3, 9 \mod 13$,

(f) $X^{12} - \sqrt{q}X^{11} + q^{3/2}X^9 - q^2X^8 + q^3X^6 - q^4X^4 + q^{9/2}X^3 - q^{11/2}X + q^6$, $p \not\equiv 1, 4, 16 \mod 21$,

(g) $X^{12} - \sqrt{q}X^{11} + qX^{10} - q^{3/2}X^9 + q^2X^8 - q^{5/2}X^7 + q^3X^6 - q^{7/2}X^5 + q^4X^4 - q^{9/2}X^3 + q^5X^2 - q^{11/2}X + q^6$, $p \not\equiv 1, 3, 9 \mod 26$,

(h) $X^{12} - qX^{10} + q^2X^8 - q^3X^6 + q^4X^4 - q^5X^2 + q^6$, $p \not\equiv 1, 9, 25 \mod 28$,

(i) $X^{12} - q^3X^6 + q^6$,$p \not\equiv 1, 13, 25 \mod 36$,

(j) $X^{12} + \sqrt{q}X^{11} - q^{3/2}X^9 - q^2X^8 + q^3X^6 - q^4X^4 - q^{9/2}X^3 + q^{11/2}X + q^6$, $p \not\equiv 1, 25, 37 \mod 42$.

7. *Dimension 7*
   There is no supersingular simple abelian variety of dimension 7.

Furthermore, for each of these polynomials, there exists a simple abelian variety of the given dimension having that polynomial as its Weil polynomial.

Proof. The proof of this theorem, follows from straightforward calculations using Theorem 4.1. ■

13. Existence of supersingular abelian varieties

There are two important existential questions.

1. Given a positive integer d and $q = p^n$, does there exist a simple supersingular abelian variety of dimension d over $\mathbb{F}_q$?
2. How many isogeny classes of simple supersingular abelian varieties are there over $\mathbb{F}_q$ for a given dimension?

In this section, we will give partial answers to these questions.

Theorem 13.1. *Let $g > 2$ be an odd positive integer and $q = p^n$, n even. Then the characteristic polynomial of a supersingular simple abelian variety over $\mathbb{F}_q$ dimension g is irreducible.*

Proof. The characteristic polynomials of supersingular simple abelian variety of dimension g are $P(X)^e$, where $e = 1$ or $e = 2$. When $e = 1$, $P(X)$ is a supersingular Weil polynomial of degree $2g$ and when $e = 2$, $P(X)$ is a supersingular Weil polynomial of degree g. Also all non linear Weil polynomials have even degree. Since $g > 2$ and g is odd, $e = 2$ is not possible and hence the theorem follows. ■

Theorem 13.2. *Let $g > 2$. Then there is no simple supersingular abelian variety over $\mathbb{F}_q$, with $q = p^n$, n even, of dimension g if and only if $\phi^{-1}(g)$ and $\phi^{-1}(2g)$ are empty sets.*

Proof. A supersingular irreducible Weil polynomial of degree $2g$ is given by $\Phi_m^{[\sqrt{q}]}(X)$, where $\phi(m) = 2g$. The characteristic polynomials of supersingular simple abelian variety of dimension g are either irreducible supersingular Weil polynomials of degree $2g$ or the square of an irreducible supersingular Weil polynomials of degree g. There are no supersingular irreducible Weil polynomials of degree g and $2g$ if $\phi^{-1}(g)$ and $\phi^{-1}(2g)$ are empty sets, respectively. Conversely let $\phi^{-1}(g)$ or $\phi^{-1}(2g)$ be non empty set. If $\phi^{-1}(g)$ is not empty and $g > 2$ this implies g is even. If $\phi(m) = g$, then then by Theorem 4.1 $(\Phi_m^{[\sqrt{q}]}(X))^e$ is a characteristic polynomial of simple supersingular abelian variety over $\mathbb{F}_q$ of dimension $\frac{ge}{2}$, where e the order of $p \mod m + 1$ i.e; where $e = 1$ or $e = 2$. For p such that order of p modulo m is odd, $(\Phi_m^{[\sqrt{q}]}(X))^2$ is a characteristic polynomial of simple supersingular abelian variety over $\mathbb{F}_q$ of dimension g. Similarly if $\phi^{-1}(2g)$ is non empty,

for all primes p such that order of p modulo m is even, and repeating the argument above, we get $\Phi_m^{[\sqrt{q}]}(X)$ is characteristic polynomial of a simple supersingular abelian variety of dimension g. Hence the theorem follows. ■

Remark 13.3. Given an integer $m > 2$, there are infinitely many primes which have an even order modulo m and there are infinitely many primes which have an odd order modulo m.

Theorem 13.4. *Let $g > 2$. Then there is no simple supersingular abelian variety over $\mathbb{F}_q$, with $q = p^n$, n odd, of dimension g if $\phi^{-1}(g)$ and $\phi^{-1}(2g)$ are all empty sets.*

Proof. Let $q = p^n$, n odd. By Theorem 3.3 and Remark 3.4, there are no irreducible supersingular Weil polynomial of degree $2g$ if $\phi(4t) = 2g$ with and $\frac{1}{2}\phi(4t) = 2g$ has no solution for t. If $2|m$ then we have $\phi(2m) = 2\phi(m)$. Therefore, $\phi(4t) = 2g$ and $\phi(4t) = 4g$ has solutions for t if and only if $\phi(2t) = g$ $\phi(2t) = 2g$ has solutions for t. Therefore there is no irreducible supersingular Weil polynomial of degree $2g$ if $\phi^{-1}(2g)$ and $\phi^{-1}(g)$ has no solution. Since the characteristic polynomial of a simple supersingular abelian variety of dimension $g > 2$ is irreducible, the result follows. ■

Though the complete characterization of values of inverse of Euler function is a difficult problem, the above two theorems provide the following partial result.

Corollary 13.5. *If p is prime greater than 2 such that $2p + 1$ is not prime (i.e. p is not a Sophie Germain prime) then is no simple supersingular abelian variety of dimension p over finite fields.*

Therefore it follows from Theorems 13.2 and 13.4, that for the following dimensions $g \leqslant 100$ there are no simple supersingular abelian varieties.

$$\text{prime: } 7, 13, 17, 19, 31, 37, 43, 47, 61, 67, 71, 73, 79, 97.$$
$$\text{composite: } 25, 27, 34, 38, 45, 57, 62, 63, 76, 77, 85, 87, 91, 93, 94, 95.$$

Corollary 13.6. *There are infinitely many positive integers g such that there is no simple supersingular abelian variety of dimension g over finite fields.*

Proof. We will show the Theorem using the fact that by there are infinitely many primes satisfying Corollary 13.5. It is well known that there are infinitely many primes congruent to 5 mod 6 which implies $2p + 1 \equiv 4 \mod 6$. Hence $2p + 1$ in this family is not prime and the Theorem follows. ■

The following result is in contrast to Theorem 13.6.

Corollary 13.7. *There are infinitely many positive integers g such that there are simple supersingular abelian varieties of dimension g.*

Proof. There are infinitely many positive integers g such that $\phi^{-1}(g)$ or $\phi^{-1}(2g)$ are not all empty sets. From Theorem 13.2 and Remark 13.3, there is a supersingular simple abelian variety of dimension g over $\mathbb{F}_q$, where q is a square for infinitely many primes p and hence this result follows. ■

Let $G_{q,g}$ denote the number of isogeny classes of supersingular simple abelian varieties of dimension g over $\mathbb{F}_q$ and $A(m) := \#\{x|\phi(x) = m\}$.

Corollary 13.8. *If $g > 1$ and $q = p^n$, n even, then*

$$G_{q,g} = A(2g)(o(p, 2g) + 1) + A(g)(o(p, g)),$$

where $o(p, k) =$ the order of $p \mod k$, taken $\mod 2$.

Proof. It follows easily from Theorem 4.1. ■

Corollary 13.9. *If $g > 2$, $q = p^n$, n odd, then*

$$G_{q,g} \leqslant ((-1)^{g+1} + 1)A(2g) + 2 \sum_{n \in A(2g)} \omega(n),$$

where $\omega(n)$ is the number of distinct prime factors of n.

Proof. The proof follows from counting the supersingular irreducible Weil polynomial of degree $2g$ both in half degree and full degree case from the Theorem 3.3. ■

Acknowledgements

We would like to thank Kevin Hutchison, Hans-Georg Rück and Christophe Ritzenthaler for very helpful suggestions. This work forms part of the PhD thesis of the first author.

References

[1] R.P. Brent, *On computing factors of cyclotomic polynomials*, Mathematics of Computation, pages 131–149, 1993.

[2] M. Deuring, *Die typen der multiplikatorenringe elliptischer funktionenkörper*, in *Abhandlungen aus dem mathematischen Seminar der Universität Hamburg*, volume 14, pages 197–272. Springer, 1941.

[3] K. Eisenträger, *The theorem of Honda and Tate*, 2004.

[4] S. Haloui, *The characteristic polynomials of abelian varieties of dimensions* 3 *over finite fields*, Journal of Number Theory **130**(12) (2010), 2745–2752.

[5] S. Haloui and V. Singh, *The characteristic polynomials of abelian varieties of dimension* 4 *over finite fields*, in *Arithmetic, Geometry, Cryptography and Coding Theory: 13th Conference [on] Arithmetic, Geometry, Cryptography and Coding Theory, CIRM, Marseille, France, March 14-18, 2011: Geocrypt 2011, Bastia, France, June 19-24, 2011*, volume 574, page 59. American Mathematical Soc., 2012.

[6] D. Maisner and E. Nart, *Abelian surfaces over finite fields as Jacobians*, Experimental mathematics **11**(3) (2002), 321–337.
[7] E. Nart and C. Ritzenthaler, *Jacobians in isogeny classes of supersingular abelian threefolds in characteristic 2*, Finite Fields and their applications **14**(3) (2008), 676–702.
[8] F. Oort, *Subvarieties of moduli spaces*, Inventiones mathematicae **24**(2) (1974), 95–119.
[9] R.S. Pierce, *Associative algebras*, Springer Verlag, 1982.
[10] K. Rubin and A. Silverberg, *Supersingular abelian varieties in cryptology*, in Advances in Cryptology – CRYPTO 2002, pages 336–353, Springer, 2002.
[11] J.P. Serre, *Local fields*, Springer, 1979.
[12] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Inventiones mathematicae **2**(2) (1966), 134–144.
[13] J. Tate, *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)*, Séminaire Bourbaki vol. 1968/69 Exposés 347-363, pages 95–110, 1971.
[14] W.C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. Ecole Norm. Sup.(4) **2** (1969), 521–560.
[15] C. Xing, *On supersingular abelian varieties of dimension two over finite fields*, Finite Fields and Their Applications **2**(4) (1996), 407–421.
[16] H.J. Zhu, *Supersingular abelian varieties over finite fields*, Journal of Number Theory **86**(1) (2001), 61–77.
[17] H.J. Zhu, *Group structures of elementary supersingular abelian varieties over finite fields*, J. Number Theory **81** (2000), 292–309.

Addresses: Vijaykumar Singh: Department of Mathematics, Simon Fraser University, Canada;
Gary McGuire: Department of Mathematics, University College Dublin, Ireland;
Alexey Zaytsev: Immanuel Kant Baltic Federal University, Russia.

E-mail: vhsingh@sfu.ca, gary.mcguire@ucd.ie, alzaytsev@kantiana.ru

Received: 12 February 2014