Characteristic polynomials of abelian varieties over $\mathbb{F}_p$

Chantal David, CICMA and Concordia University

February 22, 1999

1 Introduction

Let A be an abelian variety of dimension g over the finite field $\mathbb{F}_p$, and let ϕ be the Frobenius endomorphism of A over $\mathbb{F}_p$. Let $P_A(x)$ be the characteristic polynomial of ϕ acting on the Tate module $T_\ell(A)$ for any $\ell \neq p$. Then, $P_A(x)$ is a monic polynomial of degree $2g$ with coefficients in $\mathbb{Z}$. It was shown by Tate [4] that $P_A(x)$ characterizes A up to $\mathbb{F}_p$-isogeny, i.e. that two abelian varieties A and B over $\mathbb{F}_p$ are $\mathbb{F}_p$-isogenous if and only if $P_A(x) = P_B(x)$.

We write

$$P_A(x) = \prod_{i=1,\ldots,2g} (x - \pi_i).$$

By the Weil's Riemann hypothesis, $|\pi_i| = \sqrt{p}$ for $i = 1, \ldots, 2g$. We then call a Weil number over $\mathbb{F}_p$ an algebraic integer π such that $|\sigma(\pi)| = \sqrt{p}$ for all conjugates of π. Also, the roots of $P_A(x)$ come in pairs $(\pi, p/\pi)$, and $P_A(x)$ writes as

$$P_A(x) = x^{2g} + a_1 x^{2g-1} + \ldots + a_g x^g + p a_{g-1} x^{g+1} + \ldots + p^{g-1} a_1 x + p^g. \tag{1}$$

We also say that the polynomial $P_A(x)$ is the isogeny class of A.

By the triangle inequality,

$$|a_n| \leq \binom{2g}{n} p^{n/2} \quad \text{for } n = 1, \ldots, g. \tag{2}$$

If A is an elliptic curve, i.e. $g = 1$, then $a_1 = a_p(E)$ and the triangle inequality is the Hasse inequality

$$|a_p(E)| \leq 2\sqrt{p}.$$

Moreover, the triangle inequality is effective in this case, as it was shown by Deuring [1] that for any integer $|a| \leq 2\sqrt{p}$, there is an elliptic curve $E/\mathbb{F}_p$ such that $P_E(x) = x^2 - ax + p$. This is not true for $g > 1$. For example, let $P(x) = x^4 + 3px^2 + p^2$. This is a polynomial of the form (1) satisfying (2), but the roots of $P(x)$ are not Weil numbers over $\mathbb{F}_p$, and then $P(x)$ is not the isogeny class of any abelian variety over $\mathbb{F}_p$.

We show in this paper that there exists contants such that the triangle inequality is effective for all dimensions g. This result also gives a lower bound for the number of isogeny classes of abelian varieties of dimension g over $\mathbb{F}_p$.

Theorem 1.1 *Fix any integer $g \geq 1$. For any integers $a_1, \ldots, a_g$ and any prime p, let $P(x)$ be the polynomial*

$$P(x) = x^{2g} + a_1 x^{2g-1} + \ldots + a_g x^g + p a_{g-1} x^{g+1} + \ldots + p^{g-1} a_1 x + p^g.$$

Then, there exists positive constants $C_g(n)$ (not depending on p) such

$$|a_n| \leq C_g(n)\, p^{n/2} \quad \text{for } n = 1, \ldots, g$$

implies that $P(x)$ is the isogeny class of an abelian variety over $\mathbb{F}_p$.

Corollary 1.2 *Let g be a positive integer. For any prime p, let $I_g(p)$ be the number of $\mathbb{F}_p$-isogeny classes of abelian varieties of dimension g over $\mathbb{F}_p$. Then, there exists positive constants A_g and B_g depending only on g such that*

$$A_g\, p^{g(g+1)/4} \leq I_g(p) \leq B_g\, p^{g(g+1)/4}.$$

Proof: The lower bound is from Theorem 1.1, and the upper bound from the triangle inequality. QED.

2 Honda's Theorem

Theorem 2.1 (Honda [2]) *Let $q = p^a$ for some positive integer a, and let π be a Weil number over $\mathbb{F}_q$ with minimal polynomial $m(x)$. Then, there exists an elementary abelian variety A over $\mathbb{F}_q$ such that $P_A(x) = m(x)^e$, where e is the least common denominator of the invariants i_v for each place v above p in $E = End_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ and*

$$i_v = \begin{cases} \frac{1}{2} & \text{if } v \text{ is real;} \\ \frac{f_v\, ord_v(\pi)}{a} & \text{otherwise} \end{cases}$$

where f_v is the residual degree at v.

This version of Honda's Theorem is from [5, Theorem 1]. Then, over $\mathbb{F}_p$, the correspondence between Weil numbers and abelian varieties can be stated as a correspondance between polynomials and abelian varieties. More precisely, we have the following corollary.

Corollary 2.2 *Let $P(x) \in \mathbb{Z}[x]$ a polynomial of degree $2g$ of the form*

$$P(x) = x^{2g} + a_1 x^{2g-1} + \ldots + a_g x^g + p a_{g-1} x^{g+1} + \ldots + p^{g-1} a_1 x + p^g$$

such that the roots of $P(x)$ are Weil numbers over $\mathbb{F}_p$. Then, $P(x) = P_A(x)$ for some abelian variety of dimension g over $\mathbb{F}_p$.

Proof: Write $P(x) = (x^2 - p)^{2n_0} P_1(x)^{n_1} \ldots P_r(x)^{n_r}$ where $n_0 \in \mathbb{N}$ and for $i = 1, \ldots, r$, $P_i(x)$ is an irreducible polynomial with no real root, and n_i a positive integer. By Honda's Theorem, there are elementary abelian varieties $A_1, \ldots, A_r$ over $\mathbb{F}_p$ such that $P_{A_i}(x) = P_i(x)^{e_i}$ for $i = 1, \ldots, r$. As $a = 1$ and $P_i(x)$ has no real roots, $e_i = 1$ for $i = 1, \ldots, r$. Similary, there is an abelian variety A_0 over $\mathbb{F}_p$ such that $P_{A_0}(x) = (x^2 - p)^2$. Then, $P(x) = P_A(x)$ for

$$A = A_0^{n_0} \times A_1^{n_1} \times \ldots \times A_r^{n_r}.$$

QED.

It then suffices to prove the following proposition to obtain Theorem 1.1.

Proposition 2.3 *Fix any integer $g \geq 1$, and let $a_1, \ldots, a_g$ be any integers. For any prime p, let $P(x)$ be the polynomial*

$$P(x) = x^{2g} + a_1 x^{2g-1} + \ldots + a_g x^g + p a_{g-1} x^{g+1} + \ldots + p^{g-1} a_1 x + p^g.$$

There exists constants $C_g(n)$, $n = 1, \ldots, g$, (not depending on p) such that

$$|a_n| \leq C_g(n)\, p^{n/2} \quad \text{for } n = 1, \ldots, g \tag{3}$$

implies that the roots of $P(x)$ are Weil numbers for $\mathbb{F}_p$.

3 Proof of Proposition 2.3

We number the roots $\pi_1, \ldots, \pi_{2g}$ of $P(x)$ such that $\pi_{g+i} = p/\pi_i$ for $i = 1, \ldots, g$.

Let $Q(x)$ be the monic polynomial

$$Q(x) = \prod_{i=1,\ldots,g} (x - (\pi_i + p/\pi_i)) = \prod_{i=1,\ldots,g} (x - \beta_i).$$

Lemma 3.1 *Let $P(x)$ and $Q(x)$ be the polynomials defined above. Then, $|\pi_i| = \sqrt{p}$ for $i = 1, \ldots, 2g$ if and only if $Q(x)$ is totally real, and $|\beta_i| \leq 2\sqrt{p}$ for $i = 1, \ldots, g$.*

Proof: The proof is a standard observation, and can be found for example in [6]. If $|\pi_i| = \sqrt{p}$ for $i = 1, \ldots, 2g$, then clearly $|\beta_i| \le 2\sqrt{p}$ for $i = 1, \ldots, g$. Also, as $\pi_i = p/\pi_i$ if and only if $\pi_i = \pm\sqrt{p}$, it follows that $\beta_i = \pi_i + p/\pi_i$ is either the real part of the complex number π_i or $\pm 2\sqrt{p}$. Conversly, assume that all β_i are real and that $|\beta_i| \le 2\sqrt{p}$. Then, π_i and p/π_i are the roots of

$$x^2 - \beta_i x + p,$$

which has either complex conjugate roots, i.e. $|\pi| = |p/\pi| = \sqrt{p}$, or a double real root, i.e. $\pi = p/\pi = \pm\sqrt{p}$. QED.

It then suffices to prove that (3) implies that $Q(x)$ is totally real with roots β_i such that $|\beta_i| \le 2\sqrt{p}$ for $i = 1, \ldots, g$. We write

$$Q(x) = \prod_{i=1,\ldots,g} (x - \beta_i) = x^g + b_1 x^{g-1} + \ldots + b_{g-1} x + b_g.$$

We first need to express the coefficients $b_1, \ldots, b_n$ of $Q(x)$ in term of $a_1, \ldots, a_n$. We also define $a_0 = b_0 = 1$.

Lemma 3.2 *For $n = 1, \ldots, g$,*

$$a_n = b_n + \sum_{i=1}^{[n/2]} \binom{g-(n-2i)}{i} p^i \, b_{n-2i}$$

Proof: Let

$$A_n = (-1)^n a_n = \sum_{1 \le i_1 < \ldots < i_n \le 2g} \pi_{i_1} \ldots \pi_{i_n},$$

and

$$B_n = (-1)^n b_n = \sum_{1 \le i_1 < \ldots < i_n \le g} (\pi_{i_1} + p/\pi_{i_1}) \ldots (\pi_{i_n} + p/\pi_{i_n}) = \sum_{1 \le i_1 < \ldots < i_n \le 2g}^{(0)} \pi_{i_1} \ldots \pi_{i_n}$$

where $\displaystyle\sum_{1 \le i_1 < \ldots < i_n \le 2g}^{(r)}$ means that exactly r pairs $(i, g+i)$ occurs among $i_1, \ldots, i_n$. Then,

$$\begin{aligned} A_n &= B_n + \sum_{1 \le i_1 < \ldots < i_n \le 2g}^{(1)} \pi_{i_1} \ldots \pi_{i_n} + \sum_{1 \le i_1 < \ldots < i_n \le 2g}^{(2)} \pi_{i_1} \ldots \pi_{i_n} + \ldots \\ &= B_n + \sum_{i=1}^{[n/2]} \binom{g-(n-2i)}{i} p^i \, B_{n-2i}. \end{aligned}$$

This proves the result. QED.

Lemma 3.3 *For $n = 1, \ldots, g$,*

$$b_n = \sum_{i=0}^{[n/2]} d(n,i)\ p^i\ a_{n-2i}$$

where $d(n,i)$ are integers independant of p.

Proof: Use Lemma 3.2 and induction on n. QED.

To show Proposition 2.3, we show that the conditions (3) on the coefficients of $P(x)$ imply that the associated polynomial $Q(x)$ is "close enough" to a given polynomial $Q_0(x)$ which is totally real. Consider the polynomial

$$P_0(x) = x^{2g} + p^g,$$

i.e. $a_i = 0$ for $i = 1, \ldots, n$. The roots of $P_0(x)$ are

$$\pi_k = \zeta_{4g}^{2k-1}\sqrt{p} \quad \text{for } k = 1, \ldots, 2g,$$

where $\zeta_{4g} = \exp\left(\frac{2\pi i}{4g}\right)$. Then, by Honda's theorem, $P_0(x)$ is the isogeny class of some abelian variety A_0 over $\mathbb{F}_p$. (A_0 is a supersingular abelian variety, i.e. it becomes isogenous to a product of supersingular elliptic curves over some extension of $\mathbb{F}_p$).

Then

$$Q_0(x) = \prod_{k=1,\ldots,g} (x - (\pi_k + p/\pi_k))$$

have roots

$$\beta_k = (\pi_k + p/\pi_k) = 2\sqrt{p}\cos\left(\frac{2\pi(2k-1)}{4g}\right) \quad \text{for } k = 1, \ldots, g.$$

For $k = 1, \ldots, g-1$, let α_k be non-zero real numbers such that $\beta_{k+1} < \alpha_k < \beta_k$, and let $\alpha_0 = 2\sqrt{p}$ and $\alpha_g = -2\sqrt{p}$. For $k = 0, \ldots, g$, we also define γ_k by $\alpha_k = \gamma_k\sqrt{p}$. Then, $Q_0(\alpha_k)$ and $Q_0(\alpha_{k-1})$ have opposite signs for $k = 1, \ldots, g$, and if

$$|Q(\alpha_k) - Q_0(\alpha_k)| < |Q_0(\alpha_k)| \quad \text{for } k = 0, \ldots, g, \tag{4}$$

then $Q(x)$ also has g real roots of absolute value $\leq 2\sqrt{p}$.

We then have to prove that (3) implies (4). Using Lemma 3.3, we get

$$\begin{aligned} |Q_0(\alpha_k)| &= \left|\sum_{\substack{n=0 \\ n \text{ even}}}^{g} d(n,n/2)\ p^{n/2}\ \gamma_k^{g-n}\sqrt{p}^{g-n}\right| \\ &= p^{g/2}\left|\sum_{\substack{n=0 \\ n \text{ even}}}^{g} d(n,n/2)\ \gamma_k^{g-n}\right| = p^{g/2}K(g,k), \end{aligned} \tag{5}$$

where $K(g,k)$ is a non-zero constant independant of p. Similarly, if

$$|a_n| \leq C_g(n) p^{n/2} \quad \text{for } n = 1, \ldots, g,$$

then

$$\begin{aligned} |Q(\alpha_k) - Q_0(\alpha_k)| &= \left| \sum_{n=0}^{g} \left(\sum_{\substack{i=0 \\ 2i \neq n}}^{[n/2]} d(n,i)\, p^i \, a_{n-2i} \right) \gamma_k^{g-n} \sqrt{p}^{g-n} \right| \\ &\leq p^{g/2} \sum_{n=0}^{g} \left(\sum_{\substack{i=0 \\ 2i \neq n}}^{[n/2]} |d(n,i)| \, C_g(n-2i) \right) |\gamma_k|^{g-n}. \end{aligned} \tag{6}$$

Comparing (5) and (6), it suffices to choose constants $C_g(n)$ such that

$$\sum_{n=0}^{g} \left(\sum_{\substack{i=0 \\ 2i \neq n}}^{[n/2]} |d(n,i)| \, C_g(n-2i) \right) |\gamma_k|^{g-n} < K(g,k) \qquad \text{for } k = 0, \ldots, g.$$

Let $N(k,g)$ be the number of terms on the sum above. Then, it suffices to choose constants $C_g(n)$ such that for each i, n, k

$$|d(n,i)| \, C_g(n-2i) \, |\gamma_k|^{g-n} < \frac{K(g,k)}{N(k,g)}.$$

This completes the proof of Proposition 2.3. QED.

Acknowledgements: The author would like to thank Eyal Goren and Hershy Kisilevsky for many helpful discussions, and Francesco Pappalardi for a careful reading of the manuscript.

References

[1] M. Deuring, Die Typen de Multiplikatorenringe elliptischer Functionenkörper, *Abh. Math. Sem. Hamburg* **14** (1941), 197-272.

[2] T. Honda, Isogeny classes of abelian varieties over finite fields, *J. Math. Soc. Japan* **20** (1968), 83-95.

[3] J. S. Milne and W. C. Waterhouse, Abelian varieties over finite fields, *Proc. Sympos. Pure Math.* **20** (1971), 53–64.

[4] J. Tate, Endomorphisms of abelian varieties over finite fields, *Invent. Math.* **2** (1966), 134-144.

[5] J. Tate, Classes d'isogénie des variétés abéliennes sur un corps fini, Séminaire Bourbaki, *Lecture Notes in Math.* **179**, 1971.

[6] W. C. Waterhouse, Abelian varieties over finite fields, *Ann. scient. École Norm. Sup.* **2** (1969), 521-560.

Concordia University, Department of Mathematics, 1455 de Maisonneuve Blvd. West, Montréal, Quebec H3G 1M8, CANADA
E–mail: chantal@cicma.concordia.ca