EXISTENCE OF GEOMETRICALLY SIMPLE ORDINARY ABELIAN VARIETIES OVER A FIXED FINITE FIELD

HUI ZHU

Abstract. Given a prime number p and a positive integer d, we prove that there exist geometrically simple d-dimensional ordinary abelian varieties defined over the finite field of p elements. We present an algorithm to determine whether an abelian variety over a finite field k, given with the characteristic polynomial of its Frobenius endomorphism relative to k, is geometrically simple.

1. Introduction

Fix a prime number p. Let $\mathbf{F}_p$ be the prime field of p elements. For any field k, denote by k^a an algebraic closure of k. Let A be an abelian variety over a field k. It is *simple* if has no proper subabelian varieties over k. It is *geometrically simple* if it is simple over k^a. (It is also called *absolutely simple.*) In [6], it is shown that every Newton polygon except the supersingular type (i.e., whose Newton polygon is a straight line of slope $1/2$) arises as that of a geometrically simple abelian variety over $\mathbf{F}_p^a$. In this paper we prove the following theorem.

Theorem . *Given a prime number p and any positive integer d, there exist geometrically simple d-dimensional ordinary abelian varieties defined over $\mathbf{F}_p$.*

We would like to remark on some related questions here: (Q1) Given a perfect field k and a positive integer d, does there exist a curve over k of genus d whose Jacobian is geometrically simple? In a recent preprint [1], Chai and Oort gave an affirmative answer when k is an algebraic closure of a finite field. We do not know the general answer in the case where k is a fixed finite field or a number field. In §3 we prove a special case: there exist geometrically simple ordinary Jacobian varieties of dimension 2 over $\mathbf{F}_p$. (Q2) Consider the types of Newton polygons for d-dimensional abelian varieties over $\mathbf{F}_p$. Our result shows that the ordinary type contains geometrically simple fibres defined over $\mathbf{F}_p$. We do not know whether every non-supersingular type contains (geometrically) simple fibres defined over $\mathbf{F}_p$.

The organization of the paper is as follows. In §2 we present an algorithm to determine whether an abelian variety over a finite field k is geometrically simple. The proof of the main theorem is reduced to the constructions of certain Weil p-polynomials. Our construction is divided into two parts: §3 deals with the case $d = 2$ and §4 handles that of $d \geq 3$. Of course when $d = 1$ the problem is trivial.

Here I thank Mike Zieve, who raised the original question which led to the research and results in this paper. I thank Robert Coleman for many conversations

Date: August 9, 1999.

Research supported by the Mathematical Science Research Institute (MSRI) at Berkeley by a postdoctoral fellowship.

and suggestions. Most of all, I am very grateful to Hendrik Lenstra for his contribution of Lemma 1, for fruitful conversations, and some valuable correspondences. Some computations in this paper used the PARI/GP package for computational number theory.

2. An algorithm

Let $q = p^c$ for some positive integer c. An algebraic integer whose absolute values at all infinite places are $\sqrt{q}$ is called a *Weil q-number.* Let $f = \sum_{i=0}^{n} a_i X^{n-i} \in \mathbf{Z}[X]$ be a monic polynomial. It is a *Weil q-polynomial* if its roots are Weil q-numbers and its real roots occur with even multiplicities. Clearly it is of even degree. Consider the following sequence of points in the real coordinate plane: $(0,0), (1, (\mathrm{ord}_p a_1)/c), (2, (\mathrm{ord}_p a_2)/c), \cdots, (n, (\mathrm{ord}_p a_n)/c)$. The *normalized p-adic Newton polygon* of f is the "lower convex hull" of the set of these points (see [7, IV, §3]). Let K be the number field generated by a root of f. Each slope s_j of the Newton polygon of f corresponds to a prime ideal $\wp_j$ in K lying over p. Let $e_f = 2$ if f has real roots, otherwise e_f is equal to the least common multiple of the denominators of $s_j[K_{\wp_j} : \mathbf{Q}_p]$ where s_j for all j.

Let k be a finite field of q elements. Let d be a positive integer. There is a 1-1 correspondence between the isogeny classes of simple d-dimensional abelian varieties A over k and the set of Weil q-polynomials f_A of degree $2d$ with $f_A = g_A^{e_{f_A}}$ for an irreducible $g_A \in \mathbf{Z}[X]$. In this *Honda-Tate-correspondence*, an abelian variety A over k corresponds to the characteristic polynomial f_A of its Frobenius endomorphism relative to k. (See [10, Théorèm 1].) Let k_n be a degree n extension of k. Let f_{A/k_n} and g_{A/k_n} be the characteristic polynomial of the Frobenius of A relative to k_n. The roots of f_{A/k_n} are equal to π^n for some root π of f_A. Applying the Honda-Tate theorem to k_n for all $n \geq 1$, we conclude that A is geometrically simple if and only if $f_{A/k_n} = g_{A/k_n}^{e_{f_{A/k_n}}}$ for all n. But $e_{f_{A/k_n}} \deg(g_{A/k_n}) = 2d$, where $e_{f_{A/k_n}} \leq e_{f_{A/k_m}}$ and $\deg(g_{A/k_n}) \leq \deg(g_{A/k_m})$ for any $m \mid n$. Thus A is geometrically simple if and only if $f_A = g_A^{e_{f_A}}$ for some irreducible polynomial $g_A \in \mathbf{Z}[X]$ and $\mathbf{Q}(\pi) = \mathbf{Q}(\pi^n)$ for all $n > 1$.

Algorithm . *We have the following algorithm of* 5 *steps to determine if a given monic polynomial $f \in \mathbf{Z}[X]$ Honda-Tate-corresponds to a geometrically simple abelian variety over $\mathbf{F}_q$.*

(A1) *Check that f is a Weil q-polynomial.*
(A2) *Check that $f = g^e$ for some irreducible $g \in \mathbf{Z}[X]$ and a positive integer e.*
(A3) *Compute e_f. Check that $e = e_f$.*
(A4) *Check that $g \notin \mathbf{Z}[X^m]$ for all integers $m > 1$.*
(A5) *Let t be the maximal integer such that $\zeta_t \in \mathbf{Q}(\pi)$, where π is a root of f in $\mathbf{Q}^a$. Check that $\mathbf{Q}(\pi) = \mathbf{Q}(\pi^t)$.*

Proof. It suffices to check that Steps (A4) and (A5) imply $\mathbf{Q}(\pi) = \mathbf{Q}(\pi^n)$ for every integer $n > 1$. This can be seen from the following lemma, due to Hendrik Lenstra. □

Lemma 1. *Let π be an algebraic number with irreducible polynomial $g \in \mathbf{Q}[X]$ such that $g \notin \mathbf{Q}[X^m]$ for any integer $m > 1$. If there exists $n > 1$ with $\mathbf{Q}(\pi) = \mathbf{Q}(\pi^2) = \cdots = \mathbf{Q}(\pi^{n-1}) \neq \mathbf{Q}(\pi^n)$, then $\mathbf{Q}(\pi) = \mathbf{Q}(\pi, \zeta_n) = \mathbf{Q}(\pi^n, \zeta_n)$, where ζ_n is the primitive n-th root of unity $\exp(\frac{2\pi\sqrt{-1}}{n})$ in $\mathbf{Q}^a$.*

Proof. Let σ be a $\mathbf{Q}(\pi^n)$-embedding of $\mathbf{Q}(\pi)$ in $\mathbf{Q}^a$. Obviously, $\pi^\sigma = \pi\zeta_n^l$ for some positive integer $l \le n$. Suppose $(\zeta_n^l)^s = 1$ for some positive integer $s < n$. By assumption $\pi \in \mathbf{Q}(\pi^s)$, and so $\pi = g_0(\pi^s)$ for some $g_0(X) \in \mathbf{Q}[X]$. Thus $\pi^\sigma = g_0(\pi^s)^\sigma = g_0((\pi^\sigma)^s)$ and so $\pi\zeta_n^l = g_0((\pi\zeta_n^l)^s) = g_0(\pi^s) = \pi$, which is absurd. Therefore, ζ_n^l is primitive. Write $K := \mathbf{Q}(\pi) \cap \mathbf{Q}(\zeta_n)$. Let g_1 and g_1^σ be the minimal polynomials of π and π^σ over K and K^σ, respectively. But K is Galois over $\mathbf{Q}$, so $K^\sigma = K$. Write $g_1 = \sum_{i=0}^e a_i X^{e-i}$, then $g_1^\sigma = \sum_{i=0}^e a_i(\zeta_n^l)^i X^{e-i}$, where $g_1, g_1^\sigma \in K[X]$. Let t be the least positive integer such that $(\zeta_n^l)^t \in K$. For any integer j, we note that $a_j \ne 0$ implies $t \mid j$. Thus $g_1(X) \in \mathbf{Q}[X^t]$. Since $\mathbf{Q}(\zeta_n)/\mathbf{Q}$ is abelian, $K/\mathbf{Q}$ is Galois and so $g = \prod_{\rho\in\mathrm{Gal}(K/\mathbf{Q})} g_1^\rho(X) \in \mathbf{Q}[X^t]$. Thus $t = 1$, and hence $\zeta_n^l \in K$ and hence $\mathbf{Q}(\pi) = \mathbf{Q}(\pi, \zeta_n)$. On the other hand, each $\mathbf{Q}(\pi^n)$-conjugate π^σ of π has its minimal polynomial $g_1^\sigma \ne g_1$ over $\mathbf{Q}(\pi^n, \zeta_n)$, which implies that π^σ is no longer conjugate to π over $\mathbf{Q}(\pi^n, \zeta_n)$. Thus $\mathbf{Q}(\pi, \zeta_n) = \mathbf{Q}(\pi^n, \zeta_n)$. □

3. Case $d = 2$

For any monic polynomial $H(X) = \sum_{i=0}^d c_i X^{d-i} \in \mathbf{Z}[X]$, define $H^*(X) := X^d H(X + \frac{p}{X})$. We can write

$$H^*(X) = X^{2d} + c_1^* X^{2d-1} + \cdots + c_d^* X^d + \cdots + c_1^* p^{d-1} X + p^d$$

for $c_i^* \in \mathbf{Z}$ satisfying the following relation:

$$c_i^* = c_i + p\binom{d-(i-2)}{1}c_{i-2} + p^2\binom{d-(i-4)}{2}c_{i-4} + \cdots + \begin{cases} p^{i/2}\binom{d}{i/2}c_0 & \text{if } d \text{ is even;} \\ p^{(i-1)/2}\binom{d-1}{(i-1)/2}c_1 & \text{if } d \text{ is odd.} \end{cases} \tag{1}$$

Lemma 2. *To check if $H^* \in \mathbf{Z}[X]$ Honda-Tate-corresponds to an ordinary geometrically simple abelian variety over $\mathbf{F}_p$, it suffices to apply to H^* the Algorithm where (A1), (A2) and (A3) are replaced by*

(A1') *Check that H is irreducible, $p \nmid c_d$ and H^* is a Weil p-polynomial.*

Proof. From (1) we have $c_d^* \equiv c_d \bmod p$. That $p \nmid c_d$ implies $e_{H^*} = 1$. We claim that (A1') implies H^* is irreducible. Every pair of complex roots $\pi, \overline{\pi}$ of H^* satisfy $X^2 - \alpha X + p$ where $\alpha = \pi + \overline{\pi}$ is a root of H. If $\pi \in \mathbf{Q}(\alpha)$, i.e., the above quadratic is reducible over $\mathbf{Q}(\alpha)$, then $\alpha = 2\pi = \pm 2\sqrt{p}$ and so $H = X^2 - 4p$. This contradicts our assumption that $p \nmid c_d$. Thus $[\mathbf{Q}(\pi) : \mathbf{Q}] = 2[\mathbf{Q}(\alpha) : \mathbf{Q}] = 2d$ and H^* is irreducible since $\deg(H^*) = 2d$. Then H^* corresponds to some ordinary abelian variety over $\mathbf{F}_p$ by [2, § 2]. □

Below we apply Lemma 2 to H^*. Let $H = X^2 + c_1 X + c_2 \in \mathbf{Z}[X]$ be such that $c_1 \ne 0$ and (A1') is satisfied. So (A4) is satisfied and $\mathbf{Q}(\pi) = \mathbf{Q}(\pi^2)$. Let α denote a root of H in $\mathbf{Q}^a$ and let π denote a root of H^* in $\mathbf{Q}^a$ which satisfies $X^2 - \alpha X + p$. We claim that $N := (c_2 + 4p)^2 - 4pc_1^2 \notin \mathbf{Q}(\alpha)^2$ implies (A5) is satisfied. To show ζ_2 is the largest root of unity in $\mathbf{Q}(\pi)$, it suffices to show that $\mathbf{Q}(\pi)$ is not Galois since $\mathbf{Q}(\pi)$ is a CM field with totally real subfield $\mathbf{Q}(\alpha)$. If $\mathbf{Q}(\pi) = \mathbf{Q}(\alpha, \sqrt{\alpha^2 - 4p})$ is Galois, then $\mathbf{Q}(\pi) = \mathbf{Q}(\alpha, \sqrt{-r})$ for some $r \in \mathbf{Q}_{>0}$. Then $N_{\mathbf{Q}(\alpha)/\mathbf{Q}}(\alpha^2 - 4p) \in \mathbf{Q}(\alpha)^2$. This implies $N \in \mathbf{Q}(\alpha)^2$, which leads to a contradiction. Thus we proved our claim. If additionally $\mathbf{Z}[\alpha]$ is the ring of integers in $\mathbf{Q}(\alpha)$, then H^* Honda-Tate-corresponds to a geometrically simple ordinary Jacobian variety over $\mathbf{F}_p$ (see [9, Theorem 1.2]).

$\boxed{\text{Case } p = 2, d = 2.}$ Let $H = X^2 - X - 3$. Note that $N = 17 \notin \mathbf{Q}(\alpha)^2$, since 17 is a prime number which does not ramify in $\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{13})$.

$\boxed{\text{Case } p \geq 3, p \not\equiv 1 \bmod 5, d = 2.}$ Let $H = X^2 + X - 1$. Since $|\alpha| \leq 2\sqrt{p}$, the roots of $X^2 - \alpha X + p$ are totally imaginary of absolute value $\sqrt{p}$. Hence H^* is a Weil p-polynomial. Suppose $N = (4p-1)^2 - 4p \in \mathbf{Q}(\sqrt{5})^2$. Then exist integers x, y such that $16p^2 - 12p + 1 = (x + \frac{-1+\sqrt{5}}{2}y)^2$. Comparing both sides, we have $16p^2 - 12p + 1 = x^2$ or $5x^2$. In the first possibility, we reduce modulo 3 both sides and get a contradiction. In the second possibility, we reduce modulo 5 both sides then get $p \equiv 1 \bmod 5$, which contradicts our assumption.

$\boxed{\text{Case } p \geq 3, p \equiv 1 \bmod 5, d = 2.}$ Let $H = X^2 + 3X + 1$. Then $\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{5})$. It remains to check that $N = 16p^2 - 28p + 1 \notin \mathbf{Q}(\sqrt{5})^2$. We use an analogous argument as the above case to lead a contradiction.

4. Case $d \geq 3$

Denote by $\mathrm{Gal}(\cdot)$ the Galois group of a polynomial or a Galois extension. Let $f \in \mathbf{Q}[X]$ be an irreducible polynomial Let $G = \mathrm{Gal}(f)$ operate on the set Σ_f of roots of f in $\mathbf{Q}^a$. If, for every $\beta \in \Sigma_f$, the isotropy subgroup G_β in G is a maximal subgroup, then G is called a *primitive group*. (See also [8, Chapter I, Ex. 46]). In such a case, $\mathbf{Q}(\beta)$ is the field fixed by G_β, and there is no intermediate subfield in $\mathbf{Q}(\beta)/\mathbf{Q}$.

Lemma 3. *To prove the main theorem for $d \geq 3$, it suffices to construct a monic polynomial $H(X) = \sum_{i=0}^{d} c_i X^{d-i} \in \mathbf{Z}[X]$ with*

(C1) *H is irreducible and $p \nmid c_d$; $c^*_{d-1} \neq 0$ and $\mathrm{Gal}(H)$ contains a $(d-1)$-cycle;*
(C2) *H^* is a Weil p-polynomial.*

Proof. By Lemma 2 it suffices to show that $\mathbf{Q}(\pi) = \mathbf{Q}(\pi^n)$ for all $n \geq 1$. Suppose not then there exists an integer $n > 1$ such that $\mathbf{Q}(\pi) = \mathbf{Q}(\pi^2) = \cdots = \mathbf{Q}(\pi^{n-1}) \neq \mathbf{Q}(\pi^n)$. Suppose $\alpha \in \Sigma_H$ is fixed by the given $(d-1)$-cycle. The $(d-1)$-cycle acts transitively on the complement of α in Σ_H, and so $\mathrm{Gal}(H)$ is 2-transitive by [8, Chapter I, Ex. 47(a)]. Hence $\mathrm{Gal}(H)$ is primitive by [8, Chapter I, Ex. 47(c)]. So there is no intermediate field in the extension $\mathbf{Q}(\pi+\overline{\pi})/\mathbf{Q}$. If $\mathbf{Q}(\pi^n+\overline{\pi}^n) = \mathbf{Q}(\pi+\overline{\pi})$ then $\mathbf{Q}(\pi) = \mathbf{Q}(\pi^n)$ which contradicts our assumption. So we are forced to have $\mathbf{Q}(\pi^n + \overline{\pi}^n) = \mathbf{Q}$. Write L for the Galois closure of $\mathbf{Q}(\pi + \overline{\pi})/\mathbf{Q}$ in $\mathbf{Q}^a$. It is totally real since $\mathbf{Q}(\pi+\overline{\pi})$ is. Thus $\mathbf{Q}(\pi+\overline{\pi}) = \mathbf{Q}(\pi) \cap L$ and $\mathbf{Q} = \mathbf{Q}(\pi^n) \cap L$. The compositum $L.\mathbf{Q}(\pi^n)$ is imaginary quadratic over the totally real field L, so it is the Galois closure of $\mathbf{Q}(\pi^n)$ in $\mathbf{Q}^a$ with $\mathrm{Gal}(L.\mathbf{Q}(\pi^n)/\mathbf{Q}(\pi^n)) = \mathrm{Gal}(H)$. On the other hand, (C1) implies that $H^*(X) \notin \mathbf{Z}[X^m]$ for any integer $m > 1$, so $\mathbf{Q}(\pi)/\mathbf{Q}(\pi^n)$ is abelian by Lemma 1. Thus $\mathrm{Gal}(H)$ is abelian of order d containing a cyclic subgroup of order $d-1$, so $d \leq 2$, which contradicts our assumption. □

Let $a = 1$ if $p \neq 2, 3$ and $a = 3/2$ if $p = 2, 3$. Define a function $F(X, d, m) := X^{d+1} - X^d - 3X^{d-m} - 3(X^2 - aX - (2-a)) \in \mathbf{Q}[X]$ with domain $X \geq \sqrt{2}, m \geq 1$, and $d \geq 3$.

Lemma 4. *Let $d \geq 3$. If for some non-negative integer m and two distinct primes p_1, p_2 there is a monic $H = \sum_{i=0}^{d} c_i X^{d-i} \in \mathbf{Z}[X]$ such that*

(C1') *$H_1 := H \bmod p_1 \in \mathbf{F}_{p_1}[X]$ and $H_2 := H \bmod p_2 \in \mathbf{F}_{p_2}[X]$ are polynomials with one being irreducible and the other a product of a linear polynomial and an irreducible. For all $i = 1, \cdots, m$ we have*

$$\begin{aligned} c_i \;\; &\equiv \;\; -p\binom{d-(i-2)}{1}c_{i-2} - p^2\binom{d-(i-4)}{2}c_{i-4} - \cdots \\ &\quad - \begin{cases} p^{i/2}\binom{d}{i/2}c_0 \bmod p_1p_2 & \text{if } d \text{ is even;} \\ p^{(i-1)/2}\binom{d-1}{(i-1)/2}c_1 \bmod p_1p_2 & \text{if } d \text{ is odd.} \end{cases} \end{aligned}$$

(C2') *If $p_1 = 2, p_2 = 3$, we have $b := \sum_{i=m+1}^{d-1} \frac{|c_i^*|}{\sqrt{p}^i} + \frac{|c_d^*|}{2\sqrt{p}^d} \leq 1$ or $F(\sqrt{p}, d, m) \geq 0$.*

Then there exists H with (C1) and (C2) satisfied.

Proof. Obviously (C1') implies (C1). Now suppose $p_1 = 2, p_2 = 3$. While (C1') determines $H \bmod 6$, we may choose H in the following way: By (1) we can construct c_i^* from $c_i \bmod 6$ inductively for $i = 1, 2, \cdots, d$. It is easy to see that given a $c_i \bmod 6$ we may choose c_i so that $|c_i^*| \leq 3$ for all $1 \leq i \leq d$. If $c_{d-1}^* = 0$ then we replace c_{d-1}^* by 6; If $p \neq 2, 3$ and $p \mid c_d^*$ then we replace c_d^* by $c_d^* + 6$ or $c_d^* - 6$ so that $|c_d^*| \leq 6$. If $p = 2$ (resp., 3) we let the d-th coefficients of H_1 (resp., H_2) be non-zero. Thus $p \nmid c_d$. We get

$$\begin{aligned} &|c_i^*| \leq 3 \text{ for } 1 \leq i \leq d-2; \\ &c_{d-1}^* \neq 0; \\ &|c_{d-1}^*| \leq 6; \\ &p \nmid c_d^*; \\ &|c_d^*| \leq \begin{cases} 6 & \text{if } p \neq 2, 3; \\ 3 & \text{otherwise.} \end{cases} \end{aligned}$$

Since (C1') implies $c_1^* = c_2* = \cdots = c_m^* = 0$ by (1), we get by the above

$$\begin{aligned} b \;\; &\leq \;\; \sum_{i=m+1}^{d-2} \frac{3}{\sqrt{p}^i} + \frac{6}{\sqrt{p}^{d-1}} + \frac{12-6a}{2\sqrt{p}^d} \\ &= \;\; 3\frac{\sqrt{p}^{d-m} + \sqrt{p}^2 - a\sqrt{p} - (2-a)}{\sqrt{p}^d(\sqrt{p}-1)}, \end{aligned}$$

which is ≤ 1 if $F(\sqrt{p}, d, m) \geq 0$. On the other hand, by [3, Lemma 2.5.1], we have $b \leq 1$ implies (C2). □

To prove the main theorem for $d \geq 3$, by Lemmas 3 and 4, it suffices to construct a polynomial H with (C1') and (C2'), or (C1') and (C2). The complete proof consists of the following three parts.

4.1. **Part I.** We shall firstly construct H with (C1') and (C2') satisfied for $p \geq 11, d \geq 3$; or $p = 7, , d \geq 4$; or $p = 5, d \geq 4$; or $p = 3, d \geq 5$; or $p = 2, d \geq 10$.

Here we check $F(\sqrt{p}, d, m) \geq 0$ as in (C2') by using the following lemma.

Lemma 5. *Let $F(X, d, m)$ be defined above Lemma 4. Let $G(X, m) := X^{m+1} - X^m - 3$ where $X \geq \sqrt{2}$ and $m \geq 1$. Suppose for a fixed m we have $G(\sqrt{p_0}, m) \geq 0$, $F(\sqrt{p_0}, d_0, m) \geq 0$, and $\frac{\partial F}{\partial X}(X, d_0, m) \geq 0$ for $X \geq \sqrt{p_0}$, then $F(\sqrt{p}, d, m) \geq 0$ for all $p \geq p_0$ and $d \geq d_0$.*

Proof. This is an exercise in Calculus. Firstly, $\frac{\partial G}{\partial X} = X^{m-1}((m+1)X - m) > 0$ for all X, so $G(\sqrt{p_0}, m) \geq 0$ implies that $G(\sqrt{p}, m) \geq 0$ for all $p \geq p_0$. But

$\frac{\partial F}{\partial d}(X,d,m) = X^{d-m}G(X,m)\ln X$, so $\frac{\partial F}{\partial d}(\sqrt{p},d,m) \geq 0$ for $p \geq p_0$. By our assumptions, we have $F(\sqrt{p},d,m) \geq F(\sqrt{p_0},d,m) \geq F(\sqrt{p_0},d_0,m) \geq 0$. □

Given an arbitrary polynomial $f = \sum_{i=0}^{s} a_i X^{s-i}$ over a field, we call a_i the *i-th coefficient* of f. Conditions (C1') and (C2') require the prescription of the first m coefficients of H mod 6 (see the following lemma).

Lemma 6. *Suppose $p_1 = 2, p_2 = 3$. That $m \leq 6$ in Lemma 4 is equivalent to the first m congruences below being satisfied:*

$$\begin{aligned}
c_1 &\equiv 0 \bmod 6\\
c_2 &\equiv -pd \bmod 6\\
c_3 &\equiv 0 \bmod 6\\
c_4 &\equiv -p^2\left(\tfrac{-d(d-3)}{2}\right) \bmod 6\\
c_5 &\equiv 0 \bmod 6\\
c_6 &\equiv -p^3\left(\tfrac{d(d-4)(d-5)}{6}\right) \bmod 6.
\end{aligned}$$

By the Chinese remainder theorem, this is equivalent to the prescription of the first m coefficients of H_1 and H_2. Given a prime l and a positive integer n, if $l \neq 2$ or $n \neq 2$, then there is always an irreducible polynomial over $\mathbf{F}_l$ of degree n with the first coefficient equal to 0. (This can be seen by examining the size of the kernel of the trace map.) We shall use this for the first case below.

$\boxed{\text{Case } p \geq 11, d \geq 3 \text{ or } p = 7, d \geq 4.}$ That $m = 1$ implies (C2'). We may construct irreducibles $H_1 \in \mathbf{F}_2[X]$ of degree $d \geq 3$ and $H_3 \in \mathbf{F}_3[X]$ of degree $d-1 \geq 2$ with their first coefficient equal to 0. Let $H_2 = XH_3$. Thus we get an H with $c_1 \equiv 0 \bmod 6$. So $m = 1$ by Lemma 6.

Since $G(\sqrt{7},1) > 0$, $F(\sqrt{11},3,1) > 0$ (and $F(\sqrt{7},4,1) > 0$), and $\frac{\partial F}{\partial X}(X,3,1) > 0$ for $X \geq \sqrt{7}$, we have (C2') by Lemma 5.

The following lemma (see [5, Corollary 3.2] and its asymptotic version [4, Theorem 8.1]) implies the existence of irreducible polynomials over a finite field with its first m coefficients prescribed.

Lemma 7. *Let l be a prime and m a positive integer. For any $n > 2(m + \log_p(m+1))$ there exists a monic irreducible polynomial over $\mathbf{F}_l$ of degree n with the first m coefficients prescribed.*

$\boxed{\text{Case } p = 5, d \geq 4.}$ That $m = 2$ implies (C2').
(i) $d \geq 8$. By Lemma 7, there exist irreducible polynomials $H_1 \in \mathbf{F}_2[X]$ of degree $d \geq 8$ and $H_3 \in \mathbf{F}_3[X]$ of degree $d-1 \geq 7$ with the first 2 coefficients prescribed. Let $H_2 = XH_3$ we have $m = 2$.
(ii) $d = 4,5,6,7$. Construct H such that

d	H mod 6
4	$X^4 - 2X^2 - X - 1$
5	$X^5 - X^3 - 2X + 3$
6	$X^6 + 2X^2 - X + 3$
7	$X^7 + X^5 + 2X^3 + X^2 - X + 3$

It is easy to verify that $c_1 \equiv 0, c_2 \equiv d \bmod 6$, hence $m = 2$ by Lemma 6.

Note that $G(\sqrt{5},2) > 0$, $F(\sqrt{5},3,2) > 0$ and $\frac{\partial F}{\partial X}(X,3,2) > 0$ for all $X \geq \sqrt{5}$. Thus (C2') follows by Lemma 5.

$\boxed{\text{Case } p = 3, d \geq 5.}$ That $m = 3$ implies (C2').
(i) $d \geq 11$. Lemma 7 implies that we may prescribe the first 3 coefficients;
(ii) $5 \leq d \leq 10$. We choose H to be such that

d	H mod 6
5	$X^5 + 3X^3 - X + 1$
6	$X^6 + 3X^3 + X + 2$
7	$X^7 + 3X^5 + 3X^3 + X^2 + 2$
8	$X^8 + X^2 + 3X + 2$
9	$X^9 + 3X^7 + 3X^5 + 3X^4 - X^3 + X^2 + 3X - 2$
10	$X^{10} - X^2 + 3X - 2.$

It is easy to verify that $c_1 \equiv 0, c_2 \equiv 3d, c_3 \equiv 0 \bmod 6$, hence $m = 3$ by Lemma 6.

Now we note that $G(\sqrt{3}, 3) > 0$, $F(\sqrt{3}, 5, 3) > 0$ and $\frac{\partial F}{\partial X}(X, 5, 3) > 0$ for all $X \geq \sqrt{3}$.

$\boxed{\text{Case } p = 2, d \geq 10.}$ That $m = 6$ implies (C2').
(i) $d \geq 18$. By Lemma 7, there exist irreducible polynomials $H_1 \in \mathbf{F}_2[X]$ of degree $d \geq 18$ and $H_3 \in \mathbf{F}_3[X]$ of degree $d-1 \geq 17$ with the first 6 coefficients prescribed. Let $H_2 = (X+1)H_3$, we have $m = 6$.
(ii)$10 \leq d \leq 17$. We choose H as the follows

d	H mod 6
10	$X^{10} - 2X^8 + 2X^6 + 2X^4 - X^3 - 2X^2 - 2X + 3$
11	$X^{11} + 2X^9 + 2X^7 - 2X^5 - 2X^4 + 3X^2 + 2X + 1$
12	$X^{12} - 2X^6 + X^3 + 2X + 3$
13	$X^{13} - 2X^{11} + 2X^9 + 2X^7 - 2X^6 - 2X^5 + X^4 + X^3 - 2X^2 - X + 3$
14	$X^{14} + 2X^{12} + 2X^{10} + 2X^8 + X^5 - 2X^4 - 2X^2 - 2X + 3$
15	$X^{15} + 2X^9 + 2X^8 - 2X^5 - 2X^4 - 2X^3 - 2X^2 + X + 3$
16	$X^{16} - 2X^{14} + 2X^{12} + 2X^9 + 2X^8 - 2X^7 - 2X^6 + 3X^5 - 2X^4 + 3X^3$ $-2X^2 + X + 3$
17	$X^{17} + 2X^{15} + 2X^{13} + 2X^{10} + 2X^9 + 2X^8 - 2X^7 - 2X^6 + X^3 - 2X^2$ $-2X + 3.$

It is not hard to check that $m = 6$ by Lemma 6.

Now we note $G(\sqrt{2}, 6) > 0$, $F(\sqrt{2}, 10, 6) > 0$ and $\frac{\partial F}{\partial X}(X, 10, 6) > 0$ for all $X \geq \sqrt{2}$.

4.2. **Part II.** We shall secondly construct H with (C1') and (C2') satisfied for $p = 2, d = 6, 7, 8, 9$ and $p = 3, d = 4$. Here we set $m = 0$ and check $b \leq 1$.

$\boxed{\text{Case } p = 2, d = 6, 7, 8, 9.}$ When $d = 6$, let $H^* = X^{12} + 2X^8 + X^7 + 3X^6 + 2X^5 + 8X^4 + 64$, where $H \equiv X^6 + 2X^2 + X + 3 \bmod 6$. When $d = 7$, let $H^* = X^{14} + 5X^{10} + X^7 + 40X^4 + 128$, where $H \equiv X^7 - 2X^5 + X^3 - 2X + 1 \bmod 6$. When $d = 8$, let $H^* = X^{16} + 3X^{10} + 3X^9 + 3X^8 + 6X^7 + 12X^6 + 256$, where $H \equiv X^8 + 2X^6 + 2X^4 + X^2 + 3X - 1 \bmod 6$. When $d = 9$, let $H^* = X^{18} + 4X^{12} + 5X^{10} + 3X^9 + 10X^8 + 32X^6 + 512$, where $H \equiv X^9 - 2X^3 - X + 3 \bmod 6$.

$\boxed{\text{Case } p = 3, d = 4.}$ Let $H^* = X^8 + X^6 + X^5 + X^4 + 3X^3 + 9X^2 + 81$, where $H \equiv X^4 + X^2 + X + 1 \bmod 6$.

4.3. **Part III.** We shall thirdly construct H with (C1') and (C2) satisfied for $p = 2, d = 3, 4, 5$; $p = 3, d = 3$; $p = 5, d = 3$; $p = 7, d = 3$. Here we checked H^* below are all Weil p-polynomials by PARI/GP.

$\boxed{\text{Case } p = 2, d = 4, 5.}$
(i)$d = 4$. Let $H = X^4 + X^3 - 7X^2 - 5X + 5$. Note that $H \bmod 2$ is irreducible and $H \bmod 3$ is a product of a linear factor and an irreducible factor, that is, $H \equiv (X+1)(X^3 - X - 1) \bmod 3$. Note that $H^*(X) = X^8 + X^7 + X^6 + X^5 + X^4 + 2X^3 + 4X^2 + 8X + 16$ is indeed a Weil 2-polynomial.
(ii)$d = 5$. Let $H(X) = X^5 + X^4 - 9X^3 - 7X^2 + 15X + 5$. Note that $H \bmod 29$ is irreducible, and $H \bmod 23$ is a product of a linear factor and an irreducible factor, that is, $H(X) \equiv (X+18)(X^4 + 6X^3 + 21X^2 + 6X + 22) \bmod 23$. Note that $H^* = X^{10} + X^9 + X^8 + X^7 + X^6 + X^5 + 2X^4 + 4X^3 + 8X^2 + 16X + 32$ is indeed a Weil 2-polynomial.
$\boxed{\text{Case } p = 2, d = 3.}$ Let $H = X^3 + X^2 - 5X - 3$.
First of all H^* is indeed a Weil 2-polynomial. Note that $H \bmod 5$ is irreducible and $H \equiv (X+5)(X^2 + 9X + 2) \bmod 13$.
$\boxed{\text{Case } p = 3, d = 3.}$ Let $H = X^3 + X^2 - 8X - 5$.
First of all H^* is indeed a Weil 3-polynomial. Note that $H \bmod 2$ is irreducible and $H \equiv (X+1)(X^2 + 1) \bmod 3$.
$\boxed{\text{Case } p = 5, d = 3.}$ Let $H = X^3 + X^2 - 14X - 9$.
First of all H^* is indeed a Weil 5-polynomial. Note that $H \bmod 2$ is irreducible and $H(X) \equiv (X+6)(X^3 + 2X + 2) \bmod 7$.
$\boxed{\text{Case } p = 7, d = 3.}$ Let $H = X^3 + X^2 - 20X - 13$.
First of all H^* is indeed a Weil 7-polynomial. Note that $H \bmod 2$ is irreducible and $H \equiv (X+1)(X^2 + 1) \bmod 7$.

References

1. C-L Chai and F. Oort, *A note on the existence of absolutely simple Jacobians*, Algebraic Geometry Preprint Server **math.AG/9905063** (11 May 1999).
2. P. Deligne, *Variétés abéliennes ordinaires sur un corps fini*, Invent. Math. **8** (1969), 238–243.
3. S. DiPippo and E. Howe, *Real polynomials with all roots on the unit circle and abelian varieties over finite fields*, J. Number Theory **73** (1998), 426–450.
4. D. R. Hayes, *The distributions of irreducibles in* GF$[q, x]$, Trans. AMS **117** (1965), 101–127.
5. C-N Hsu, *The distribution of irreducible polynomials in* $\mathbf{F}_q[t]$, J. Number theory **61** (1996), 85–96.
6. H.W. Lenstra, Jr. and F. Oort, *Simple abelian varieties having a prescribed formal isogeny type*, J. Pure Appl. Algebra **4** (1974), 47–53.
7. N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, second ed., Graduate Texts in Mathematics, vol. 58, Springer-Verlag, 1984.
8. S. Lang, *Algebra*, third ed., Addison-Wesley, 1993.
9. H-G Rück, *Abelian surfaces and jacobian varieties over finite fields*, Comp. Math. **76** (1990), 351–366.
10. J. Tate, *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)*, Séminaire Bourbaki **21** (1968/69), no. 352, 95–110.

MSRI, 1000 Centennial Drive, Berkeley, CA 94720-5070
E-mail address: zhu@msri.org