Algebraic Geometry 2 (5) (2015) 654–663
doi:10.14231/AG-2015-028

An algebraic construction of an abelian variety with a given Weil number

Ching-Li Chai and Frans Oort

Dedicated to the memory of Taira Honda

Abstract

A classical theorem of Honda and Tate asserts that for every Weil q-number π, there exists an abelian variety over the finite field $\mathbb{F}_q$, unique up to $\mathbb{F}_q$-isogeny. The standard proof (of the existence part in the Honda–Weil theorem) uses the the fact that for a given CM field L and a given CM type Φ for L, there exists a CM abelian variety with CM type (L, Φ) over a field of characteristic 0. The usual proof of the last statement uses complex uniformization of (the set of $\mathbb{C}$-points of) abelian varieties over $\mathbb{C}$. In this short note we provide an algebraic proof of the existence of a CM abelian variety over an integral domain of characteristic 0 with a given CM type, resulting in an algebraic proof of the existence part of the Honda–Tate theorem which does not use complex uniformization.

1. Introduction

Throughout this note p is a fixed prime number, and the symbol q stands for some positive power of p, that is, $q \in p^{\mathbb{N}>0}$. Recall that an algebraic integer π is a said to be a *Weil q-number* if $|\psi(\pi)| = \sqrt{q}$ for every complex embedding $\psi\colon \mathbb{Q}(\pi) \hookrightarrow \mathbb{C}$.

A celebrated theorem of Weil, which was the starting point of new developments in arithmetic algebraic geometry, states that for any abelian variety A over the finite field $\mathbb{F}_q$ its associated q-Frobenius morphism $\pi_A = \mathrm{Fr}_{A,q}\colon A \to A^{(q)} = A$ is a Weil q-number, in the sense that π_A is a root of a monic irreducible polynomial in $\mathbb{Z}[T]$ all of whose roots are Weil q-numbers; see [Wei48, Chapitre 3, X, N^o 70], [WM71, Theorem 8, p. 58] and [Mum70, IV.21, Theorem 4, p. 206]. Honda and Tate went further; they proved that the map $A \mapsto \pi_A$ defines a *bijection*

$$\{\text{simple abelian variety over } \mathbb{F}_q\}/(\mathrm{mod}\,\mathbb{F}_q\text{-isogeny}) \quad \xrightarrow{\sim} \quad \{\text{Weil } q\text{-numbers}\}/\sim \qquad (1)$$

from the set of isogeny classes of simple abelian varieties over $\mathbb{F}_q$ to the set of Weil q-numbers up to equivalence, where two Weil numbers π and π' are said to be equivalent (or *conjugate*) if there exists a field isomorphism $\mathbb{Q}(\pi) \cong \mathbb{Q}(\pi')$ which sends π to π'. This map is well defined because of the above theorem of Weil, and because isogenous abelian varieties have conjugate Frobenius

Received 22 December 2013, accepted in final form 21 April 2015.
2010 Mathematics Subject Classification 11G10, 11G15.
Keywords: abelian variety, complex multiplication, CM field, Weil number, lifting.

The first author is partially supported by NSF grant DMS-1200271

endomorphisms. The injectivity was proved by Tate in [Tat66], and the surjectivity was proved by Honda [Hon68] and Tate [Tat71].

The purpose of this note is to provide a new, algebraic proof of the surjectivity of (1), formulated below.

Theorem I. *For any Weil q-number π there exists a simple abelian variety A over $\mathbb{F}_q$ (*unique up to $\mathbb{F}_q$-isogeny*) such that π is conjugate to π_A.*

In [Tat71] a Weil q-number is said to *effective* if it is conjugate to the q-Frobenius of an abelian variety over $\mathbb{F}_q$. Theorem I asserts that every Weil number is effective.

Remarks. (1) In the course of the proof of Theorem I we will show, in Theorem II in Step 5, that *every CM type for a CM field L is realized by an abelian variety of dimension $[L:\mathbb{Q}]/2$ with complex multiplication by L in characteristic* 0. Recall that number field L is a *CM field* if there exists a subfield $L_0 \subset L$ with $[L:L_0]=2$ such that L_0 is totally real (every embedding of L_0 into $\mathbb{C}$ lands into $\mathbb{R}$) and L is totally complex (no embedding of L into $\mathbb{C}$ lands into $\mathbb{R}$). A CM type of a CM field L as above with values in a field E of characteristic 0 is a subset Φ of embeddings of L into E such that $\mathrm{card}(\Phi)=[L_0:\mathbb{Q}]$ and $\Phi\circ\rho\cap\Phi=\emptyset$, where ρ is the non-trivial automorphism of L/L_0 (the "complex conjugation" for L/L_0).

(2) Proofs of Theorems I and II have been given by constructing a CM abelian variety over $\mathbb{C}$ (using complex uniformization and GAGA) with properties which ensure that the reduction modulo p of this CM abelian variety gives a Weil number which is a power of π_A. We construct such a CM abelian variety by algebraic methods, without using complex uniformization. The remark in Step 8 gives this proof in the special case when the dimension g of the abelian variety is 1; that proof is a guideline for the proof below for arbitrary g. In a sense this algebraic proof answers a question posed in [Oor08, 22.4].

2. Proof of two theorems

The rest of this article is devoted to the proof of Theorems I and II, separated into a number of steps. We will follow the general strategy in [Tat71]. Only Steps 3–5 are new, where complex uniformization is replaced by algebraic methods in the construction of CM abelian varieties with a given CM type (Theorem II). Steps 1 and 2 are preparatory in nature, recalling some general facts and notation for the rest of the proof. Steps 6–8, already in [Tat71], are included for the convenience of the readers.

Step 1. Notation

A Weil q-number π has exactly one of the following three properties:

- ($\mathbb{Q}$) We have $\psi(\pi)\in\mathbb{Q}$. In this case $q=p^n=p^{2m}$ and $\pi=\pm\sqrt{q}=\pm p^m$.
- ($\mathbb{R}$) We have $\psi(\pi)\notin\mathbb{Q}$ and $\psi(\pi)\in\mathbb{R}$. In this case $q=p^n=p^{2m+1}$ and $\pi=\pm\sqrt{q}=\pm p^m\cdot\sqrt{p}$. Moreover, every embedding of $\mathbb{Q}(\pi)$ into $\mathbb{C}$ lands into $\mathbb{R}$.
- ($\notin\mathbb{R}$) If there is one embedding $\psi'\colon\mathbb{Q}(\pi)\hookrightarrow\mathbb{C}$ such that $\psi'(\pi)\notin\mathbb{R}$, then for every embedding $\psi\colon\mathbb{Q}(\pi)\hookrightarrow\mathbb{C}$ we have $\psi(\pi)\notin\mathbb{R}$ and in this case $\mathbb{Q}(\pi)$ is a CM field.

As we know from [Tat71, § 1, Exemple a)], every real Weil q-number comes from an abelian variety over $\mathbb{F}_q$, so the first two cases have been taken care of. Therefore in order to prove Theorem I, we may and do assume that we are in the third case, that is, $\pi\notin\mathbb{R}$.

Following [Tat71, Théorème 1], let M be a finite-dimensional central division algebra[1] over $\mathbb{Q}(\pi)$, uniquely determined (up to non-unique isomorphism) by the following local conditions:

(i) The central division algebra M is ramified at all real places of $\mathbb{Q}(\pi)$.

(ii) The algebra M is split at all finite places of $\mathbb{W}(\pi)$ which are prime to p.

(iii) For every place ν of $\mathbb{Q}(\pi)$ above p, the arithmetically normalized local Brauer invariant of M at ν is

$$\mathrm{inv}_\nu(M) \equiv \frac{\nu(\pi)}{\nu(q)}[\mathbb{Q}(\pi)_\nu : \mathbb{Q}_p] \pmod{\mathbb{Z}}\,.$$

Let $g := [\mathbb{Q}(\pi) : \mathbb{Q}]\cdot\sqrt{[M : \mathbb{Q}(\pi)]}/2$, a positive integer. According to [Tat71, Lemme 2] there exists a CM field L with $\mathbb{Q}(\pi) \subset L \subset M$ and $[L : \mathbb{Q}] = 2g$. Let L_0 be the maximal totally real subfield of L.

Step 2. Choosing a CM type for L

We follow the way a suitable p-adic CM type is chosen on pages 103–105 of [Tat71]; however, our notation will be slightly different, and we will not use Lemma 4 nor Lemma 5 of [Tat71]. A prime above p in $\mathbb{Q}(\pi)$ will be denoted by u. A prime in L_0 above p will be denoted by w, and a prime in L above p will be denoted by v. We write ρ for the involution of the quadratic extension L/L_0 (which "is" the complex conjugation). Following Tate, we write

$$H_v = \mathrm{Hom}(L_v, \mathbb{C}_p) \quad \text{and} \quad \mathrm{Hom}(L, \mathbb{C}_p) = \coprod_{v|p} H_v\,,$$

where $\mathbb{C}_p$ is the p-adic completion of an algebraic closure of $\mathbb{Q}_p$. Let

$$n_v := \frac{v(\pi)}{v(q))} \cdot \#(H_v) \in \mathbb{N}$$

for each place v of L above p. Using properties of π, we choose a suitable p-adic CM type for L by choosing a subset $\coprod_{v|w}\Phi_v \subset \coprod_{v|w} H_v$ for each place w of L_0 above p, as follows.

– $(v = \rho(v))$ For any v with $v = \rho(v)$ the map ρ gives a fixed-point-free involution on H_v; in this case (once π and L are fixed and v is chosen) we choose a subset $\Phi_v \subset H_v$ with

$$\#(\Phi_v) = \frac{1}{2} \cdot \#(H_v)\,.$$

Note that $v(\pi) = \frac{1}{2}v(q)$ in this case and we have

$$n_v = \frac{1}{2} \cdot \#(H_v) = (v(\pi)/v(q)) \cdot \#(H_v)\,.$$

– $(v \neq \rho(v))$ For any pair v_1, v_2 above a place w of L_0 dividing p with $v_1 \neq \rho(v_1) = v_2$, the complex conjugation ρ defines a bijective map

$$\psi \longmapsto \psi \circ \rho$$

from H_{v_1} to H_{v_2}, through composition with ρ. We choose a subset $\Phi_{v_1} \subset H_{v_1}$ with

$$\#(\Phi_{v_1}) = n_{v_1} \quad \text{and we define} \quad \Phi_{v_2} := H_{v_2} - \Phi_{v_1} \circ \rho\,.$$

Observe that indeed $n_{v_i} + n_{\rho(v_i)} = [L_v : \mathbb{Q}_p] = \#(H_{v_i})$ for $i = 1, 2$. We could as well have first chosen Φ_{v_2} of the right size and then defined Φ_{v_1} as $\Phi_{v_1} := H_{v_1} - \Phi_{v_2} \circ \rho$.

[1] This central division algebra M was denoted by E in [Tat71]. If we can find an abelian variety A over $\mathbb{F}_q$ with $\pi_A \sim \pi$, then we will have $\mathrm{End}^0(A) \cong M$ and $\dim(A) = g = [\mathbb{Q}(\pi) : \mathbb{Q}]\cdot\sqrt{[M : \mathbb{Q}(\pi)]}/2$.

Define a CM type $\Phi_p \subset \mathrm{Hom}(L, \mathbb{C}_p) = \coprod_{v|p} H_v$ by setting $\Phi_p = \coprod_{v|p} \Phi_v$. By construction we have

$$\Phi_p \cap (\Phi_p \circ \rho) = \emptyset \quad \text{and} \quad \Phi_p \cup (\Phi_p \circ \rho) = \mathrm{Hom}(L, \mathbb{C}_p)\,;$$

that is, Φ_p is a p-adic CM type for the CM field L. Let $j_p \colon \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}_p$. The injection j_p induces a bijection

$$\psi \longmapsto j_p \circ \psi$$

from $\mathrm{Hom}(L, \overline{\mathbb{Q}})$ to $\mathrm{Hom}(L, \mathbb{C}_p)$, through composition with j_p. The subset $\Phi := (j_p \circ ?)^{-1}(\Phi_p) \subset \mathrm{Hom}(L, \overline{\mathbb{Q}})$ is a CM type in the usual sense; that is, $\Phi \cap (\Phi \circ \rho) = \emptyset$ and $\Phi \cup (\Phi \circ \rho) = \mathrm{Hom}(L, \overline{\mathbb{Q}})$.

We fix the notation $\Phi_p \subset \mathrm{Hom}(L, \mathbb{C}_p)$ for the p-adic CM type constructed above and the corresponding CM type $\Phi \subset \mathrm{Hom}(L, \overline{\mathbb{Q}})$.

Step 3. Choosing a prime number r

Proposition A. *For a given* CM *field L there exists a rational prime number r unramified in L such that r splits completely in L_0 and every place of L_0 above r is inert in L/L_0.*

Proof. Let N be the smallest Galois extension of $\mathbb{Q}$ containing L, and let $G = \mathrm{Gal}(N/\mathbb{Q})$. Note that the element $\rho \in G$ induced by complex conjugation is a central element of order 2. By Chebotarev's theorem the set of rational primes unramified in N whose Frobenius conjugacy class in G is ρ has Dirichlet density $1/[G : 1] > 0$; see [Lan70, VIII.4, Theorem 10]. Any prime number r in this subset satisfies the required properties. □

Step 4. Constructing a supersingular abelian variety with an action by L

We know that for every prime number (r in our case) there exists a supersingular elliptic curve E in characteristic r. When $r > 2$ we know that there exist values of the parameter λ such that corresponding elliptic curves over $\overline{\mathbb{F}}_r$ in the Legendre family $Y^2 = X(X-1)(X-\lambda)$ are supersingular; see [Har77, Chapter 4, Corollary 4.22]. In characteristic 2 the elliptic curve given by the cubic equation $Y^2 + Y = X^3$ is supersingular. (This cubic equation defines an elliptic curve with CM by $\mathbb{Z}[\mu_3]$, and 2 is inert in $\mathbb{Q}(\mu_3)$.)

Let E be a supersingular elliptic curve over the base field $\kappa := \overline{\mathbb{F}}_r$; we know that $\mathrm{End}(E)$ is non-commutative. Its endomorphism algebra $\mathrm{End}^0(E)$ is the quaternion division algebra $\mathbb{Q}_{r,\infty}$ over $\mathbb{Q}$ in the notation of [Deu41], which is ramified exactly at r and ∞.

Proposition B. *Let L' be a totally imaginary quadratic extension of a totally real number field L'_0 such that $[L'_v : \mathbb{Q}_r]$ is even for every place v of L' above r. Let $g' = [L'_0 : \mathbb{Q}]$. There exist a positive involution τ on the central simple algebra $\mathrm{End}_{\mathbb{Q}}(L'_0) \otimes_{\mathbb{Q}} \mathbb{Q}_{r,\infty} \cong \mathrm{M}_{g'}(\mathbb{Q}_{r,\infty})$ over $\mathbb{Q}$ and a ring homomorphism $\iota \colon E \hookrightarrow \mathrm{End}_{\mathbb{Q}}(L'_0) \otimes_{\mathbb{Q}} \mathbb{Q}_{r,\infty}$ such that $\iota(L')$ is stable under the involution τ and τ induces the complex conjugation on L'.*

Proof. Let $\mathrm{End}_{\mathbb{Q}}(L'_0) \cong \mathrm{M}_{g'}(\mathbb{Q})$ be the algebra of all endomorphisms of the $\mathbb{Q}$-vector space underlying L'_0. The trace form $(x, y) \mapsto \mathrm{Tr}_{L'_0/\mathbb{Q}}(x \cdot y)$ for $x, y \in L'_0$ is a positive definite quadratic form on (the $\mathbb{Q}$-vector space underlying) L'_0, so its associated involution τ_1 on $\mathrm{End}_{\mathbb{Q}}(L'_0)$ is positive. Multiplication defines a natural embedding $L'_0 \hookrightarrow \mathrm{End}_{\mathbb{Q}}(L'_0)$, and every element of L'_0 is fixed by τ_1.

Let τ_2 be the canonical involution on $\mathbb{Q}_{r,\infty}$. The involution $\tau_1 \otimes \tau_2$ on $\mathrm{End}_{\mathbb{Q}}(L'_0) \otimes_{\mathbb{Q}} \mathbb{Q}_{r,\infty}$ is clearly positive because τ_2 is. It is also clear that the subalgebra $B := L'_0 \otimes_{\mathbb{Q}} \mathbb{Q}_{r,\infty}$ of $\mathrm{End}_{\mathbb{Q}}(L'_0) \otimes_{\mathbb{Q}}$

$\mathbb{Q}_{r,\infty}$ is stable under τ. Moreover, B is a positive definite quaternion division algebra over L_0', so the restriction to B of the positive involution τ is the canonical involution on B.

The assumptions on L' imply that there exists an L_0'-linear embedding $L' \hookrightarrow B$. From the elementary fact that every $\mathbb{R}$-linear embedding of $\mathbb{C}$ in the Hamiltonian quaternions $\mathbb{H}$ is stable under the canonical involution on $\mathbb{H}$, we deduce that the subalgebra $L' \otimes_{\mathbb{Q}} \mathbb{R} \subset B \otimes_{\mathbb{Q}} \mathbb{R}$ is stable under the canonical involution of $B \otimes_{\mathbb{Q}} \mathbb{R}$, which implies that L' is stable under τ. □

Corollary C. (i) *Let $B_1 := E^g$. There exist a polarization $\mu_1 \colon B_1 \to B_1^t$ and an embedding $L \hookrightarrow \mathrm{End}^0(B_1) = \mathrm{M}_g(\mathbb{Q}_{r,\infty})$ such that the image of L is stable under the Rosati involution attached to μ_1.*

(ii) *There exists an isogeny $\alpha \colon B_1 \to B_0$ over $\overline{\mathbb{F}}_r$ such that the embedding $L \hookrightarrow \mathrm{End}^0(B_1) = \mathrm{End}^0(B_0)$ factors through an action*

$$\iota_0 \colon \mathcal{O}_L \hookrightarrow \mathrm{End}(B_0)$$

of $\mathcal{O}_L$ on B_0, where $\mathcal{O}_L$ is the ring of all algebraic integers in L.

(iii) *There exists a positive integer m such that the isogeny*

$$\mu_0 := m \cdot (\alpha^t)^{-1} \circ \mu_1 \circ \alpha^{-1} : B_0 \to B_0^t$$

is a polarization on B_0 and the Rosati involution τ_{μ_0} attached to μ_0 induces the complex conjugation on the image of L in $\mathrm{End}^0(B_0)$.

Proof. Statements (ii) and (iii) follow from statement (i). For the proof statement (i), first recall from [Mum70, § 21 Application III] that after one has fixed an ample invertible $\mathcal{O}_{B_1}$-module $\mathscr{L}$ on the abelian variety B_1, say the tensor product of pullbacks of $\mathcal{O}_E(o_E)$ via the g projections $\mathrm{pr}_i \colon B_1 \to E$, where o_E is the zero section of E, the Néron–Severi group $\mathrm{NS}^0(B_1) = \mathrm{NS}(B_1) \otimes \mathbb{Q}$ is identified with the subgroup of $\mathrm{End}^0(B_1)$ fixed under the Rosati involution $*_{\mathscr{L}}$ and the classes of ample line bundles in $\mathrm{NS}(B_1) \otimes \mathbb{Q}$ are exactly the totally positive elements in the formally real Jordan algebra $\mathrm{NS}(B_1)$. The Jordan algebra structure here is defined using the class of the ample line bundle $\mathscr{L}$.

On the other hand, one knows from the Noether–Skolem theorem and basic properties of positive involutions on semisimple algebras that for every positive involution $*'$ on $\mathrm{End}^0(B_1)$ there exists an element $c \in \mathrm{End}^0(B_1)^\times$ such that $*'(c) = c = *_{\mathscr{L}}(c)$ and $*'(x) = c^{-1} \cdot *_{\mathscr{L}} \cdot c$ for all $x \in \mathrm{End}^0(B_1)$; see for instance [Kot92, Lemma 2.11]. Moreover, the element c is either totally positive or totally negative because the center of the simple algebra $\mathrm{End}^0(B_1)$ is $\mathbb{Q}$.

Apply Proposition B to the case $L' = L$. From the facts recalled in the preceding paragraphs we see that the positive involution τ constructed in Proposition B has the form $\tau = \mathrm{Ad}(c)^{-1} \circ *_{\mathscr{L}}$, and c can be taken to be a totally positive element in $\mathrm{NS}(B_1)$. In other words, τ is the Rosati involution attached to the polarization $\phi_{\mathscr{L}} \circ c$, where $\phi_{\mathscr{L}}$ is the polarization on B_1 defined by the ample line bundle $\mathscr{L}$. □

From now on we fix (L, Φ) as in Step 1, with r as in Proposition A and

$$(B_0\,,\ \iota_0 \colon \mathcal{O}_L \hookrightarrow \mathrm{End}(B_0)\,,\ \mu_0 : B_0 \to B_0^t)$$

as in Corollary C. We fix an algebraic closure $\overline{\mathbb{Q}}_r$ of $\mathbb{Q}_r$, an embedding $j_r \colon \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_r$ and an embedding $i_{r,\mathrm{ur}} \colon W(\overline{\mathbb{F}}_r)[1/p] \hookrightarrow \overline{\mathbb{Q}}_r$. We have bijections

$$\mathrm{Hom}(L, \mathbb{C}_p) \xleftarrow[\sim]{j_p \circ ?} \mathrm{Hom}(L, \overline{\mathbb{Q}}) \xrightarrow[\sim]{j_r \circ ?} \mathrm{Hom}(L, \overline{\mathbb{Q}}_r) \xleftarrow[\sim]{i_r \circ ?} \mathrm{Hom}(L, W(\overline{\mathbb{F}}_r)[1/r])\,.$$

The last arrow

$$\mathrm{Hom}(L,\overline{\mathbb{Q}}_r) \xleftarrow[\sim]{i_r\circ ?} \mathrm{Hom}(L, W(\overline{\mathbb{F}}_r)[1/r])$$

is a bijection because r is unramified in L. We regard the p-adic CM type Φ_p as an r-adic CM type $\Phi_r \subset \mathrm{Hom}(L, W(\overline{\mathbb{F}}_r)[1/r])$ via the bijection $(j_r\circ ?)\circ(j_p\circ ?)^{-1}$; that is,

$$\Phi_r := (j_r\circ ?)\circ(j_p\circ ?)^{-1}(\Phi_p) = (j_r\circ ?)(\Phi)\,.$$

For each place $\mathfrak{w}$ of L_0 above r, the $\mathfrak{w}$-adic completion $L_\mathfrak{w} := L\otimes_{L_0} L_{0,\mathfrak{w}}$ of L is an unramified quadratic extension field of the $\mathfrak{w}$-adic completion $L_{0,\mathfrak{w}} \cong \mathbb{Q}_r$ of L_0, and the intersection $\Phi_\mathfrak{w} := \Phi_r \cap \mathrm{Hom}(L_\mathfrak{w}, W(\overline{\mathbb{F}}_r)[1/r])$ is a singleton.

Step 5. Lifting to a CM abelian variety in characteristic 0

Theorem II. *Let $(B_0, \iota_0\colon \mathcal{O}_L \hookrightarrow \mathrm{End}(B), \mu_0\colon B_0 \to B_0^t)$ be an $([L:\mathbb{Q}]/2)$-dimensional polarized supersingular abelian variety with an action by $\mathcal{O}_L$ such that the subring $\mathcal{O}_L \subset \mathrm{End}^0(B_0)$ is stable under the Rosati involution τ_{μ_0} as in Corollary C. There exists a lifting $(\mathcal{B}, \iota, \mu)$ of the triple (B, ι_0, μ_0) to the ring $W(\overline{\mathbb{F}}_r)$ of r-adic Witt vectors with entries in $\overline{\mathbb{F}}_r$, where $\mathcal{B}$ is an abelian scheme over $W(\overline{\mathbb{F}}_r)$ whose closed fiber is B, the homomorphism $\iota\colon \mathcal{O}_L \to \mathrm{End}(\mathcal{B})$ is an action of $\mathcal{O}_L$ on $\mathcal{B}$ which extends ι_0 and $\mu\colon \mathcal{B} \to \mathcal{B}^t$ is a polarization of $\mathcal{B}$ which extends μ_0, such that the generic fiber $\mathcal{B}_\eta$ is an abelian variety whose r-adic CM type is equal to Φ_r.*

Proof. The prime number r was chosen such that for every place $\mathfrak{w}$ of the totally real subfield $L_0 \subset L$, the ring of local integers $\mathcal{O}_{L_0,w}$ of the $\mathfrak{w}$-adic completion of L_0 is $\mathbb{Z}_p$ and $\mathcal{O}_{L,\mathfrak{w}} := \mathcal{O}_L\otimes_{\mathcal{O}_{L_0}}\mathcal{O}_{L_0,\mathfrak{w}} \cong W(\mathbb{F}_{r^2})$. We have a product decomposition

$$\mathcal{O}_L\otimes_{\mathbb{Z}}\mathbb{Z}_p \cong \prod_{\mathfrak{w}} \mathcal{O}_L\otimes_{\mathcal{O}_{L_0}}\mathcal{O}_{L_0,\mathfrak{w}} \cong \prod_{\mathfrak{w}} \mathcal{O}_{L,\mathfrak{w}}\,,$$

where $\mathfrak{w}$ runs over the g places of L_0 above r. The g idempotents associated with this decomposition of $\mathcal{O}_L\otimes_{\mathbb{Z}}\mathbb{Z}_p$ define a decomposition

$$B_0[r^\infty] \cong \prod_{\mathfrak{w}} B_0[\mathfrak{w}^\infty]$$

of the r-divisible group $B_0[r^\infty]$ into a product of g factors, where each factor $B_0[\mathfrak{w}^r]$ is a height 2 r-divisible group with an action by $\mathcal{O}_\mathfrak{w}$. Similarly, we have a decomposition

$$B_0^t[r^\infty] \cong \prod_{\mathfrak{w}} B_0^t[\mathfrak{w}^\infty]$$

of the r-divisible group attached to the dual B_0^t of B_0. The action of $\mathcal{O}_L$ on B_0 induces an action of $\mathcal{O}_L$ on B_0^t by $y \mapsto (\iota_0(\rho(y)))^t$ for every $y \in \mathcal{O}_L$, so that the polarization $\mu_0\colon B_0 \to B_0^t$ is $\mathcal{O}_L$-linear. The polarization μ_0 on the abelian variety B_0 induces a polarization[2] $\mu_0[r^\infty]\colon B_0[r^\infty] \to B_0^t[r^\infty]$ on the r-divisible group; this polarization $\mu_0[r^\infty]$ decomposes into a product of polarizations $\mu_0[w^\infty]\colon B_0[\mathfrak{w}^\infty] \to B_0^t[r^\infty]$ on the $\mathcal{O}_{L,\mathfrak{w}}$-linear r-divisible groups $B_0[\mathfrak{w}^\infty]$ of height 2.

[2]In this article a *polarization* $Y = (Y_n)_{n\geqslant 1} \to S$ of a p-divisible group Y over a base scheme S is, by definition, an isogeny $\nu\colon Y \to Y^t$ over S from Y to its Serre dual Y^t which is symmetric in the sense that $\nu^t = \nu$. Recall that the Serre dual Y^t of Y is the p-divisible group $(Y_n^t)_{n\geqslant 1}$ whose p^n-torsion subgroup is the Cartier dual Y_n^t of $Y_n = Y[p^n]$; see [Mes72, Chapter I, Subsection 2.4.4]. The double dual $(Y^t)^t$ of Y is canonically isomorphic to Y, so the dual ν^t of an S-homomorphism $\nu\colon Y \to Y^t$ is again an S-homomorphism from Y to Y^t.

In the literature the terminology "quasi-polarization" is often used, to distinguish it from the notion of polarizations of abelian schemes. Here we have dropped the prefix "quasi" to avoid possible association with the notion of "quasi-isogeny".

It suffices to show that for each place $\mathfrak{w}$ of L_0 above r, the $\mathcal{O}_{L,\mathfrak{w}}$-linearly polarized r-divisible group $(B_0[\mathfrak{w}^\infty], \iota_0[\mathfrak{w}^\infty], \mu_0[\mathfrak{w}^\infty])$ over $\overline{\mathbb{F}}_r$ can be lifted to $W(\overline{\mathbb{F}}_r)$ with r-adic CM type $\Phi_\mathfrak{w}$. For then the Serre–Tate theorem of deformation of abelian schemes tells us that (B_0, ι_0, μ_0) can be lifted over $W(\overline{\mathbb{F}}_r)$ to a formal abelian scheme $\mathfrak{B}$ with an action $\hat{\iota}\colon \mathcal{O}_L \to \mathrm{End}(\mathfrak{B})$ whose r-adic CM type is Φ_r, together with an $\mathcal{O}_L$-linear symmetric isogeny $\hat{\mu}\colon \mathfrak{B} \to \mathfrak{B}^t$ from the formal abelian scheme $\mathfrak{B}$ to its dual whose closed fiber is the polarization μ_0 on B_0; see either [Kat81] or [Mes72, Theorem 2.3] for the Serre–Tate theorem. The pullback by

$$(\mathrm{id}_\mathfrak{B}, \hat{\mu})\colon \mathfrak{B} \to \mathfrak{B} \times_{\mathrm{Spec}(W(\overline{\mathbb{F}}_r))} \mathfrak{B}^t$$

of the Poincaré line bundle on $\mathfrak{B} \times_{\mathrm{Spec}(W(\overline{\mathbb{F}}_r)} \mathfrak{B}^t$ is an invertible $\mathcal{O}_\mathfrak{B}$-module on the formal scheme $\mathfrak{B}$ whose restriction to the closed fiber B_0 is *ample*. The existence of an ample invertible $\mathcal{O}_\mathfrak{B}$-module on $\mathfrak{B}$ implies, by Grothendieck's algebraization theorem [EGA3, § 5.4], that the formal abelian scheme $\mathfrak{B}$ comes from a unique abelian scheme $\mathcal{B}$ over $W(\overline{\mathbb{F}}_r)$ and that the CM structure $(\mathfrak{B}, \hat{\iota})$ on the formal abelian scheme $\mathfrak{B}$ descends uniquely to a CM structure $(\mathcal{B}, \iota)$ on the abelian scheme $\mathcal{B}$ over $W(\overline{\mathbb{F}}_r)$ with r-adic CM type Φ_r.

For any r-adic place $\mathfrak{w}$ among the g places of L_0 above r, the existence of a CM lifting to $W(\overline{\mathbb{F}}_r)$ of the $\mathcal{O}_{L,\mathfrak{w}}$-linear polarized r-divisible group $(B_0[\mathfrak{w}^\infty], \iota_0[\mathfrak{w}^\infty], \mu_0[\mathfrak{w}^\infty])$ of height 2 goes back to Deuring, who proved that a supersingular elliptic curve with a given endomorphism can be lifted to characteristic 0; see [Deu41, Hilfssatz, p. 259] and its proof; the case we need here is [Oor87, Lemma 14.7]. Below is a proof using Lubin–Tate formal groups.

By [LT65, Theorem 1], there exists a 1-dimensional formal p-divisible group X of height 2 over $W(\overline{\mathbb{F}}_r)$ plus an action $\beta\colon \mathcal{O}_{L,\mathfrak{w}} \to \mathrm{End}(X)$ of $\mathcal{O}_{L,\mathfrak{w}}$ on X whose r-adic CM type is $\Phi_\mathfrak{w}$. Let

$$(X_0, \beta_0\colon \mathcal{O}_{L,\mathfrak{w}} \to \mathrm{End}(X_0)) := (X, \beta) \times_{\mathrm{Spec}(W(\overline{\mathbb{F}}_r))} \mathrm{Spec}(\overline{\mathbb{F}}_r)$$

be the closed fiber of (X, β). It is well known that the $\mathcal{O}_{L,\mathfrak{w}}$-linear p-divisible group (X_0, β_0) over $\overline{\mathbb{F}}_r$ is isomorphic to $(B_0[\mathfrak{w}^\infty], \iota_0[\mathfrak{w}^\infty])$. (Let us sketch a proof based on the structure of the quaternion division algebra $\mathrm{End}^0(X_0)$ over $\mathbb{Q}_p$. Both X_0 and $B_0[\mathfrak{w}^\infty]$ are p-divisible groups of height 2 and slope 1/2, hence they are isomorphic. After we identify X_0 with $B_0[\mathfrak{w}^\infty]$, the CM structure $\iota_0[\mathfrak{w}^\infty]$ on $B_0[\mathfrak{w}^\infty]$ is identified with a homomorphism $\beta_0'\colon \mathcal{O}_{L,\mathfrak{w}} \to \mathrm{End}(X_0)$, and we know that $\mathrm{End}(X_0)$ is the ring of integral elements in $\mathrm{End}^0(X_0)$. According to the Noether–Skolem theorem, there exists an element $u \in \mathrm{End}^0(X_0)^\times$ such that $\beta_0'(a) = u \cdot \beta_0(a) \cdot u^{-1}$ for every $a \in \mathcal{O}_{L,\mathfrak{w}}$. Because the two CM structures β_0' and β_0 have the same CM type, the normalized valuation of u in $\mathrm{End}^0(X_0)$ is even. In other words, u is of the form $u = p^m \cdot u_1$ with $m \in \mathbb{Z}$ and $u_1 \in \mathrm{End}(X_0)^\times$, so the automorphism u_1 of X_0 defines an isomorphism between the two $\mathcal{O}_{L,\mathfrak{w}}$-linear p-divisible groups (X_0, ι_0) and (X_0, ι_0').)

We choose and fix an isomorphism between $(B_0[\mathfrak{w}^\infty], \iota_0[\mathfrak{w}^\infty])$ and (X_0, β_0), and use this chosen isomorphism to identify these two p-divisible groups over $\overline{\mathbb{F}}_r$ with their CM structures. The Serre dual X^t of X, with the $\mathcal{O}_{L,\mathfrak{w}}$-action defined by $\gamma\colon b \mapsto (\beta(\rho(b)))^t$ for all $b \in \mathcal{O}_{L,\mathfrak{w}}$, also has CM type $\Phi_\mathfrak{w}$. Let (X_0^t, γ_0) be the closed fiber of (X^t, γ). The natural map

$$\xi\colon \mathrm{Hom}\big((X, \beta), (X^t, \gamma)\big) \longrightarrow \mathrm{Hom}\big((X_0, \beta_0), (X_0^t, \gamma_0)\big)$$

defined by reduction modulo r is a bijection: [LT65, Theorem 1] implies that (X^t, γ) is isomorphic to (X, β), and after we identify them via a chosen isomorphism both the source and the target of ξ are isomorphic to $\mathcal{O}_{L,\mathfrak{w}}$, so that ξ is an $\mathcal{O}_{L,\mathfrak{w}}$-linear isomorphism.

Under the identification of (X_0, β_0) with $(B_0[\mathfrak{w}^\infty], \iota_0[\mathfrak{w}^\infty])$ specified above, the polarization $\mu_0[\mathfrak{w}^\infty]$ on $B_0[\mathfrak{w}^\infty]$ is identified with a polarization ν_0 on X_0. The polarization $\nu_0\colon X_0 \to X_0^t$

extends over $W(\kappa_{L,\mathfrak{w}})$ to a polarization $\nu : X \to X^t$ because ξ is a bijection. We have shown that the triple $(B_0[\mathfrak{w}^\infty], \iota_0[\mathfrak{w}^\infty], \mu_0[\mathfrak{w}^\infty])$ can be lifted over $W(\overline{\mathbb{F}}_r)$. □

Remark. One can also prove the existence of a lifting of $(B_0[\mathfrak{w}^\infty], \iota_0[\mathfrak{w}^\infty], \mu_0[\mathfrak{w}^\infty])$ to $W(\overline{\mathbb{F}}_r)$ using the Grothendieck–Messing deformation theory for abelian schemes, as documented in [Mes72, Chapter V, Theorems 1.6 and 2.3]. The point is that the deformation functor for $(B_0[\mathfrak{w}^\infty], \iota_0[\mathfrak{w}^\infty])$ is represented by $\mathrm{Spf}(W(\overline{\mathbb{F}}_r))$ because $\mathcal{O}_{L,\mathfrak{w}}$ is unramified over $\mathbb{Z}_p$.

We fix the generic fiber $(\mathcal{B}_\eta, \mu, \iota)$ of a lifting as in Theorem II over the fraction field $W(\overline{\mathbb{F}}_r)[1/r]$ of $W(\overline{\mathbb{F}}_r)$ with an $\mathcal{O}_L$-linear action $\iota\colon \mathcal{O}_L \hookrightarrow \mathrm{End}(\mathcal{B}_\eta)$, whose r-adic CM type is Φ_r.

Step 6. Changing to a number field and reducing modulo p

We have arrived at a situation where we have an abelian variety $\mathcal{B}_\eta$ over a field of characteristic 0 with an action $\mathcal{O}_L \hookrightarrow \mathrm{End}(\mathcal{B}_\eta)$ by $\mathcal{O}_L$, whose r-adic CM type with respect to an embedding of the base field in $\overline{\mathbb{Q}}_r$ is equal to the r-adic CM type Φ_r constructed at the end of Step 4.

We know that any CM abelian variety in characteristic 0 can be defined over a number field K; see for example [ShT61, Proposition 26] or [CCO14, Proposition 1.5.4.1]. By [SeT68, Theorem 6] we may assume, after passing to a suitable finite extension of K, that this CM abelian variety has good reduction at *every* place of K above p. Again, we may pass to a finite extension of K, if necessary, to ensure that K has a place with residue field δ of characteristic p with $\mathbb{F}_q \subset \delta$. We have arrived at the following situation:

> *We have a* CM *abelian variety* $(C, L \hookrightarrow \mathrm{End}^0(C))$ *of dimension* $g = [L : \mathbb{Q}]/2$ *over a number field* K*, of* p*-adic* CM *type* Φ_p *with respect to an embedding* $K \hookrightarrow \mathbb{C}_p$ *such that* C *has good reduction* C_0 *at a* p*-adic place of* K *induced by the embedding* $K \hookrightarrow \mathbb{C}_p$ *and the residue class field of that place contains* $\mathbb{F}_q$*.*

Step 7. Some power of π is effective

Let $i \in \mathbb{Z}_{>0}$ be such that $\delta = \mathbb{F}_{q^i}$. We have C_0 over δ and $\pi^i,\ \pi_{C_0} \in L$.

- We know that π^i and π_{C_0} are units at all places of L not dividing p.
- We know that these two algebraic numbers have the same absolute value under every embedding into $\mathbb{C}$.
- By the construction of Φ in Step 2 and by [Tat71, Lemme 5], we know that π^i and π_{C_0} have the same valuation at every place above p. As remarked in [Tat71, pp. 103–104], the essence of this step is the "factorization of a Frobenius endomorphism into a product of prime ideals" in [ShT61, Section 13].

This shows that π^i/π_{C_0} is a unit locally everywhere and has absolute value equal to 1 at all infinite places. This implies, by standard finiteness properties for algebraic number fields, that π^i/π_{C_0} is a root of unity in $\mathcal{O}_L$. See for instance [Hec23, § 34, Hilfsatz a)] or [Wei67, Chapter IV, § 4, Theorem 8]. We conclude that there exists a positive integer j such that $\pi^{ij} = (\pi_{C_0})^j$.

Step 8. End of the proof

The previous step shows that π^{ij} is effective, because it is (conjugate to) the q^{ij}-Frobenius of the base change of C_0 to $\mathbb{F}_{q^{ij}}$. By [Tat71, Lemme 1] this implies that π is effective, and this ends the proof of Theorem I.

Remark. When $g = 1$, the proof of Theorem I is easier. This simple proof, sketched below, was the starting point of this note.

Suppose that π is a Weil q-number and $L = \mathbb{Q}(\pi)$ is an imaginary quadratic field such that the positive integer g, defined by p-adic properties of π, is equal to 1. This means that either (first case) there is an $i \in \mathbb{Z}_{>0}$ with $\pi^i \in \mathbb{Q}$, or (second case) for every i we have $L = \mathbb{Q}(\pi^i)$, with p split in L/Q and at one place v above p in L we have $v(\pi)/v(q) = 1$, while at the other place v' above p we have $v'(\pi)/v'(q) = 0$. If $\pi^i \in \mathbb{Q}$, we know that π is the q-Frobenius of a supersingular elliptic curve over $\mathbb{F}_q$, see Step 1, and π is effective. If the second case occurs, we choose a prime number r which is inert in $L/\mathbb{Q}$, then choose a supersingular elliptic curve in characteristic r, lift it to characteristic 0 together with an action of (an order in) L. The reduction modulo p (over some extension of $\mathbb{F}_p$) gives an elliptic curves whose Frobenius is a power of π; by [Tat71, Lemme 1] we conclude π is effective.

The idea of the proof of the general case is the same as that of the proof described in the previous paragraph when $g = 1$, except that (as we do in Steps 2, 4 and 5) we have to specify the CM type in order to keep control of the p-adic properties of the abelian variety eventually constructed. Note that the CM lifting problem treated in the proof of Theorem II is exactly the same as in the $g = 1$ case (in view of the Serre–Tate theorem).

Acknowledgements

We would like to thank the referee for several suggestions.

References

CCO14 C.-L. Chai, B. Conrad and F. Oort, *Complex multiplication and lifting problems*, Mathematical Surveys and Monographs, vol. 195 (Amer. Math. Soc., Providence, RI, 2014); http://dx.doi.org/10.1090/surv/195.

Deu41 M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272; http://dx.doi.org/10.1007/BF02940746.

EGA3 A. Grothendieck and J. Dieudonné, *Éléments de géométrie algébrique: III. Étude cohomologique des faisceaux cohérents, Première partie*, Publ. Math. Inst. Hautes Études Sci. **11** (1961), 5–167; http://www.numdam.org/item?id=PMIHES_1961__11__5_0.

Har77 R. Hartshorne, *Algebraic geometry*, Grad. Texts in Math., vol. 52 (Springer-Verlag, New York – Heidelberg, 1977); http://dx.doi.org/10.1007/978-1-4757-3849-0.

Hec23 E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen* (Akademische Verlagsgesellschaft, Leipzig, 1923).

Hon68 T. Honda, *Isogeny classes of abelian varieties over finite fields*, J. Math. Soc. Japan **20** (1968), no. 1–2, 83–95; http://doi.org/10.2969/jmsj/02010083.

Kat81 N. Katz, *Appendix to Exposé V: Cristaux ordinaires et coordonnées canoniques*, Algebraic surfaces (Orsay, 1976–78), Lecture Notes in Math., vol. 868 (Springer, Berlin – New York, 1981), 127–137; http://doi.org/10.1007/BFb0090648.

Kot92 R. E. Kottwitz, *Points on some Shimura varieties over finite fields*, J. Amer. Math. Soc. **5** (1992), no. 2, 373–444; http://dx.doi.org/10.2307/2152772.

Lan70 S. Lang, *Algebraic number theory* (Addison-Wesley Publishing Co., Inc., Reading, Mass. – London – Don Mills, Ont., 1970).

LT65 J. Lubin and J. Tate, *Formal complex multiplication in local fields*, Ann. of Math. (2) **81** (1965), no. 2, 380–387; http://dx.doi.org/10.2307/1970622.

Mes72 W. Messing, *The crystals associated to Barsotti–Tate groups: with applications to abelian schemes*, Lecture Notes in Math., vol. 264 (Springer-Verlag, Berlin – New York, 1972); http://dx.doi.org/10.1007/BFb0058301.

Mum70 D. Mumford, *Abelian varieties*, Tata Inst. Fund. Res. Stud. Math., vol. 5 (Oxford University Press, London, 1970).

Oor87 F. Oort, *Lifting algebraic curves, abelian varieties, and their endomorphisms to characteristic zero*, Algebraic Geometry, Bowdoin, 1985 (Brunswick, Maine, 1985), Proc. Sympos. Pure Math., vol. 46 (Amer. Math. Soc., Providence, RI, 1987), Part 2, 165–195; http://dx.doi.org/10.1090/pspum/046.2/927980.

Oor08 ———, *Abelian varieties over finite fields*, Higher-Dimensional Geometry over Finite Fields (Göttingen, 2007), (eds D. Kaledin and Y. Tschinkel), NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., vol. 16 (IOS, Amsterdam, 2008), 123–188.

SeT68 J-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), no. 3, 492–517; http://dx.doi.org/10.2307/1970722.

ShT61 G. Shimura and Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Publ. Math. Soc. Japan, vol. 6 (The Mathematical Society of Japan, Tokyo, 1961).

Tat66 J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144; http://dx.doi.org/10.1007/BF01404549.

Tat71 ———, *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)*, Séminaire Bourbaki, 1968/69, Exp. no. 352, Lecture Notes in Math., vol. 175 (Springer, Berlin, 1971), 95–110, http://dx.doi.org/10.1007/BFb0058807.

Wei48 A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Ind., no. 1041 (Hermann et Cie., Paris, 1948).

Wei67 ———, *Basis number theory*, Grundlehren math. Wiss., vol. 144 (Springer-Verlag, Berlin, 1967); http://dx.doi.org/10.1007/978-3-662-00046-5.

WM71 W. C. Waterhouse and J. S. Milne, *Abelian varieties over finite fields*, 1969 Number Theory Institute (Proc. Sympos. Pure Math., vol. XX, State Univ. New York, Stony Brook, NY, 1969) (Amer. Math. Soc., Providence, R.I., 1971), 53–64.

Ching-Li Chai chai@math.upenn.edu
Department of Mathematics, University of Pennsylvania, 209 S. 33rd St., Philadephia, PA 19003-6395, USA

Frans Oort f.oort@uu.nl
Mathematical Institute, Utrecht University, Pincetonplein 5, 3584 CC Utrecht NL, The Netherlands