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

Ching-Li Chai[a] & Frans Oort[b]

version 10, April 20, 2015

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.

Dedicated to the memory of Taira Honda.

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

A celebrated theorem of A. 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 $\pi_A = \mathrm{Fr}_{A,q} : A \to A^{(q)} = A$ 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 [21, p. 70], [20, p. 138] and [11, Th. 4, p. 206]. T. Honda and J. Tate went further; they proved that the map $A \mapsto \pi_A$ defines a *bijection*[1]

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

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'. The purpose of this note is to provide a new/algebraic proof of the surjectivity of the above displayed map, 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.*[2]

[a]Partially supported by NSF grant DMS-1200271

[b]The Institute of Mathematics of *Academia Sinica* is gratefully acknowledged for excellent working conditions and for hospitality during a visit of the second-named author in November / December 2012.

[1]This map is well-defined because of the above theorem of Weil, and because isogenous abelian varieties have conjugate Frobenius endomorphisms. The injectivity was proved by Tate in [18], and the surjectivity was proved by Honda [6] and Tate [19].

[2]In [19] 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. (a) 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* [3] L *is realized by an abelian variety of dimension* $[L:\mathbb{Q}]/2$ *with complex multiplication by* L *in characteristic zero.*

(b) Proofs of these theorems were 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 $g=1$; that proof is a guideline for the proof below for arbitrary g. In a sense this algebraic proof answers a question posed in [15, 22.4].

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 [19]. 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 set of notations for the rest of the proof. Steps 6-8, already in [19], are included for the convenience of the readers.

Step 1. Notations.
A Weil q-number π has exactly one of the following three properties:

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

As we know from [19], page 97 Example (a) that 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, i.e. $\pi\notin\mathbb{R}$.

Following [19, Th. 1, p. 96], let M be a finite dimensional central division algebra over $\mathbb{Q}(\pi)$,[4] uniquely determined (up to non-unique isomorphism) by the following local conditions:

(i) M is ramified at all real places of $\mathbb{Q}(\pi)$,

(ii) M split at all finite places of $\mathbb{W}(\pi)$ which are prime to p, and

(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 § 3, Lemme 2 on p. 100 of [19] 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 [19, pp. 103–105]; however our notation will be slightly different. 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

[3] A number field L is a *CM field* 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 $\mathbb{R}$) L is totally complex (no embedding of L into $\mathbb{C}$ lands into $\mathbb{R}$).

[4] This central division algebra M was denoted by E in [19]. If we can find an abelian variety A over $\mathbb{F}_q$ with $\pi_A\sim\pi$ then we would have $\mathrm{End}^0(A)\cong M$ and $\dim(A)=g=[\mathbb{Q}(\pi):\mathbb{Q}]\cdot\sqrt{[M:\mathbb{Q}(\pi)]}/2$.

for the involution of the quadratic extension L/L_0 (which "is" the complex conjugation). Following Tate we write

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

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
$$\#(\Phi_v) = (1/2) \cdot \#(H_v).$$
Note that $v(\pi) = (1/2)v(q)$ in this case and we have
$$n_v = (1/2) \cdot \#(H_v) = (v(\pi)/v(q)) \cdot \#(H_v).$$

- $[v \neq \rho(v)]$ For any pair v_1, v_1 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 $? \circ \rho : H_{v_1} \to H_{v_2}$. We choose a subset $\Phi_{v_1} \subset H_{v_1}$ with
$$\#(\Phi_{v_1}) = n_{v_1} \text{ and we define } \Phi_{v_2} := H_{v_2} - \Phi_{v_1} \circ \rho.$$
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 chosen first Φ_{v_2} of the right size and then define Φ_{v_1} as $\Phi_{v_1} := H_{v_1} - \Phi_{v_2} \circ \rho$.

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

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

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

$$j_p \circ ?\colon \mathrm{Hom}(L, \overline{\mathbb{Q}}) \xrightarrow{\sim} \mathrm{Hom}(L, \mathbb{C}_p).$$

The subset $\Phi := (j_p \circ ?)^{-1}(\Phi_p) \subset \mathrm{Hom}(L, \overline{\mathbb{Q}})$ is a CM type in the usual sense, i.e. $\Phi \cap (\Phi \circ \rho) = \emptyset$ 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 [9, VIII.4, Th. 10]. Any prime number r in this subset satisfies the required properties. $\square$

Step 4. Construct 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 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 see [4, 4.4.2]. In characteristic 2 the elliptic curve given by the cubic equation $Y^2 + Y = X^3$ is supersingular.[5]

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 [2], which is ramified exactly at r and ∞. Let $B_1 := E^g$ and let $D := \mathrm{End}^0(B_1) = \mathrm{M}_g(\mathbb{Q}_{r,\infty})$.

Proposition B. *Let L' be a totally imaginary quadratic extension of a totally real number field L'_0 such $[L'_v : \mathbb{Q}_r]$ is even for every place v of L' above r. Let $g' = [L'_0 : \mathbb{Q}]$. There exists 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) *There exists a polarization $\mu_1 : B_1 \to B_1^t$ and an embedding $L \hookrightarrow \mathrm{End}^0(B_1) = D$ such that the image of L in $D = \mathrm{End}^0(B_1)$ is stable under the Rosati involution attached to μ_1.*

(ii) *There exists an isogeny $\alpha : B_1 \to B_0$ 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*

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

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. The statements (ii) and (iii) follow from (i). For the proof statement (i), recall first from [11, §21 pp. 208–210] that after one fixed an ample invertible $\mathcal{O}_{B_1}$-module $\mathscr{L}$ on the abelian variety $B_1 := E^g$, say the tensor product of pullbacks of $\mathcal{O}_E(o_E)$ via the g projections $\mathrm{pr}_i : B_1 \to E$, 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

[5] This cubic equation defines an elliptic curve with CM by $\mathbb{Z}[\mu_3]$, and 2 is inert in $\mathbb{Q}(\mu_3)$.

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 [8, Lemma 2.11]. Moreover the element c in the previous sentence 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 when $L' = L$. 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

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

as in Corollary C. We fix an algebraic closure $\overline{\mathbb{Q}}_r$ of $\mathbb{Q}_r$, an embedding $j_r : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_r$, and an embedding $i_{r,\mathrm{ur}} : W(\overline{\mathbb{F}}_r)[1/p] \hookrightarrow \overline{\mathbb{Q}}_r$. 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 $(j_r \circ ?) \circ (j_p \circ ?)^{-1}$, i.e.

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

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 zero.**

Theorem II. *Let $(B_0, \iota_0 : \mathcal{O}_L \hookrightarrow \mathrm{End}(B), \mu_0 : B_0 \to B_0^t)$ 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, and $\iota : \mathcal{O}_L \to \mathrm{End}(\mathcal{B})$ is an action of $\mathcal{O}_L$ on $\mathcal{B}$ which extends ι_0 and $\mu : \mathcal{B} \to \mathcal{B}^t$ 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 so 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 to the above 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 $\mu_0 : B_0 \to B_0^t$ is $\mathcal{O}_L$-linear. The polarization μ_0 on the abelian variety B_0 induces a polarization[6] $\mu_0[r^\infty] : B_0[r^\infty] \to B_0^t[r^\infty]$ on the r-divisible group $\mu_0[r^\infty]$, which decomposes into a product of polarizations $\mu_0[w^\infty] : B_0[\mathfrak{w}^\infty] \to B_0^t[r^\infty]$ on the $\mathcal{O}_{L,\mathfrak{w}}$-linear r-divisible groups $B_0[\mathfrak{w}^\infty]$ of height 2.

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 $\hat{\iota} : \mathcal{O}_L \to \mathrm{End}(\mathfrak{B})$ whose r-adic CM type is Φ_r, together with an $\mathcal{O}_L$-linear symmetric isogeny $\hat{\mu} : \mathfrak{B} \to \mathfrak{B}^t$ from the formal abelian scheme $\mathfrak{B}$ to its dual whose closed fiber is the polarization μ_0 on B_0; see either [7] or Thm. 2.3 on p. 166 of [10] for the Serre-Tate theorem. The pull-back by

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

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 [3, III §5.4, pp. 156–158], that the formal abelian scheme $\mathfrak{B}$ comes from a unique abelian scheme $\mathcal{B}$ over $W(\overline{\mathbb{F}}_r)$, and 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 zero, see [2, p. 259] and the proof on pp. 259-263; the case we need here is [13, 14.7]. Below is a proof using Lubin-Tate formal groups.

By [12, Th. 1], there exists a one-dimensional formal p-divisible group X of height 2, over $W(\overline{\mathbb{F}}_r)$ plus an action $\beta : \mathcal{O}_{L,\mathfrak{w}} \to \mathrm{End}(X)$ of $\mathcal{O}_{L,\mathfrak{w}}$ on X whose r-adic CM type is $\Phi_{\mathfrak{w}}$. Let

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

[6] In this article a *polarization* of a p-divisible group $Y = (Y_n)_{n \geq 1} \to S$ over a base scheme S is, by definition, an isogeny $\nu : Y \to Y^t$ 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 $(Y_n^t)_{n \geq 1}$ whose p^n-torsion subgroup is the Cartier dual Y_n^t of $Y_n = Y[p^n]$'s; see [10, Ch. I (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 $\nu : Y \to Y^t$ 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".

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 $(B_0[\mathfrak{w}^\infty],\iota_0[\mathfrak{w}^\infty])$.[7]

We choose and fix an isomorphism between $(B_0[\mathfrak{w}^\infty],\iota_0[\mathfrak{w}^\infty])$ with (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 $\gamma: b\mapsto (\beta(\rho(b)))^t$ $\forall\, b\in\mathcal{O}_{L,\mathfrak{w}}$, also has CM type $\Phi_{\mathfrak{w}}$. Let (X_0^t,γ_0) be the closed fiber of (X^t,γ). The natural map

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

defined by reduction modulo r is a bijection: [12, Thm. 1] implies that (X^t,γ) is isomorphic to (X,β), and after identifying 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 $\nu_0: X_0\to X_0^t$ 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 $W(\overline{\mathbb{F}}_r)$. $\square$

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 Ch. V, Theorems (1.6) and (2.3) of [10]. 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 $\iota:\mathcal{O}_L\hookrightarrow\mathrm{End}(\mathcal{B}_\eta)$, whose r-adic CM type is Φ_r.

Step 6. Change to a number field and reduce modulo p .

We have arrived at a situation where we have an abelian variety $\mathcal{B}_\eta$ over a field of characteristic zero 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 e.g. [17, Prop. 26, p. 109] or [1, Prop. 1.5.4.1]. By [16, Th. 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 arrive 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.

[7] We 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 two 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 $\beta_0':\mathcal{O}_{L,\mathfrak{w}}\to\mathrm{End}(X_0)$, 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').

Let $i \in \mathbb{Z}_{>0}$ such that $\delta = \mathbb{F}_{q^i}$. We have C_0 over δ and π^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 [19], Lemme 5 on page 103, we know that π^i and π_{C_0} have the same valuation at every place above p. As remarked in [19, p. 103/104], the essence of this step is the "factorization of a Frobenius endomorphism into a product of prime ideals" in [17].

This shows that π^i/π_{C_0} is a unit locally everywhere and has absolute value equal to one 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 [5, §34 Hilfsatz a)] or [22, Ch. IV §4 Thm. 8]. We conclude that there exists a positive integer $j \in \mathbb{Z}_{>0}$ 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 [19, Lemma 1, p. 100] this implies that π is effective, and this ends the proof of the theorem in the introduction. □

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 (the first case) either that there is an $i \in \mathbb{Z}_{>0}$ with $\pi^i \in \mathbb{Q}$, or (the second case) that 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 zero 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 [19, Lemme 1] on page 100 we conclude π is effective.

Th scheme of the proof of the general case is the same as 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).

Acknowledgement. We would like to thank the referee for several suggestions.

References

[1] C.-L. Chai, B. Conrad & F. Oort – *Complex multiplication and lifting problems.* Math. Surveys and Monographs **195**, Amer. Math. Soc., 2014.

[2] M. Deuring – *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper.* Abh. Math. Sem. Hamburg, **14** (1941), 197–272.

[3] A. Grothendieck & J. Dieudonné – *Élements de géométrie algébriue,* III[1]. *Étude cohomologique des faisceaux cohérents.* Publ. Math. IHES **11**, 1961.

[4] R. Hartshorne – *Algebraic geometry.* Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.

[5] E. Hecke – *Vorlesungen über die Theorie der algebraischen Zahlen.* Akademische Verlagsgesellschaft, Leipzig, 1923.

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

[7] N. Katz – Appendix to Exposé V: *Cristaux ordinaires et coordonnées canoniques.* Algebraic surfaces (Orsay, 1976–78), Lecture Notes in Mathematics, vol. 868, Springer-Verlag, Berlin, 1981, Appendix to an article of P. Deligne, pp. 127–137.

[8] R. Kottwitz – *Points of some Shimura varieties over finite fields.* J. Amer. Math. Soc. **5** (1992), 373–444.

[9] S. Lang – *Algebraic number theory.* Addison-Wesley Publishing Co., Inc., Reading, Mass.-London-Don Mills, Ont. 1970.

[10] W. Messing – *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes.* Lecture Notes in Mathematics, vol. 264, Springer-Verlag, Berlin, 1972.

[11] D. Mumford – *Abelian varieties.* Tata Institute of Fundamental Research Studies in Math. 5, Oxford University Press, London, 1970.

[12] J. Lubin & J. Tate – *Formal complex multiplication* Ann. of Math. **81** (1965), 380–387.

[13] F. Oort – *Lifting algebraic curves, abelian varieties, and their endomorphisms to characteristic zero.* Algebraic geometry, Bowdoin, 1985 (Brunswick, Maine, 1985), Proc. Sympos. Pure Math., 46, Part 2, pp. 165–195, Amer. Math. Soc., Providence, RI, 1987.

[14] F. Oort – *Moduli of abelian varieties in mixed and in positive characteristic.* The Handbook of Moduli (G. Farkas, I, Morrison, editors), Vol. III, pp. 75–134. Adv. Lect. Math. (ALM) **26**, Int. Press, Somerville, MA, 2013.

[15] F. Oort – *Abelian varieties over finite fields.* Summer School on "Varieties over finite fields", Göttingen, 25-VI — 6-VII-2007. Higher-dimensional geometry over finite fields. Proceedings of the NATO Advanced Study Institute 2007 (Editors: Dmitry Kaledin, Yuri Tschinkel). IOS Press, 2008, 123–188.

[16] J-P. Serre & J. Tate – *Good reduction of abelian varieties.* Ann. of Math. **88** (1968). 492–517.

[17] G. Shimura & Y. Taniyama – *Complex multiplication of abelian varieties and its applications to number theory.* Publications of the Mathematical Society of Japan, Vol. 6. The Mathematical Society of Japan, Tokyo 1961.

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

[19] J. Tate – *Classes d'isogénie des variétés abéliennes sur un corps fini* (d'après T. Honda). Séminaire Bourbaki, 1968/69, no. 352. Lecture Notes Mathematics 179, Springer-Verlag, 1971, 95–110.

[20] W. Waterhouse & J. Milne – *Abelian varieties over finite fields.* 1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969), 53–64.

[21] A. Weil – *Sur les courbes algébriques et les variétés qui s'en déduisent.* Act. Sci. Ind., no. 1041, Publ. Inst. Math. Univ. Strasbourg 7 (1945). Hermann et Cie., Paris, 1948.

[22] A. Weil – *Basis number theory.* Springer-Verlag, 1971.

Ching-Li Chai
Department of Mathematics
University of Pennsylvania
Philadelphia, PA 19104-6395
USA
chai@math.upenn.edu
chai@math.upenn.edu/~chai/

Frans Oort
Mathematical Institute
Pincetonplein 5
3584 CC Utrecht NL
The Netherlands
f.oort@uu.nl
www.staff.science.uu.nl/~oort0109/