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

Ching-Li Chai\textsuperscript{a} & Frans Oort\textsuperscript{b}

version 8, December 18, 2013

Abstract

A classical theorem of Honda and Tate asserts that for every Weil \( q \)-number \( \pi \), 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 fact that for a given CM field \( L \) and a given CM type \( \Phi \) for \( L \), there exists a CM abelian variety with CM type \(( L, \Phi )\) 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. \( q \in p^{N>0} \). Recall that an algebraic integer \( \pi \) is a said to be a \textit{Weil} \( q \)-number if \(|\psi(\pi)| = \sqrt{q}\) for every complex embedding \( \psi : \mathbb{Q}(\pi) \rightarrow \mathbb{C} \).

\textit{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 \( \pi_A = F_{r,A,q} : A \rightarrow A^{(q)} = A \) is a Weil \( q \)-number, in the sense that \( \pi_A \) is a root of a monic irreducible polynomial in \( \mathbb{Z}[T] \) all of whose roots are Weil \( q \)-numbers; see [20, p. 70], [19, p. 138] and [10, Th. 4, p. 206]. T. Honda and J. Tate went further; they proved that the map \( A \mapsto \pi_A \) defines a bijection\textsuperscript{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 \( \pi \) and \( \pi' \) are said to be equivalent (or \textit{conjugate}) if there exists a field isomorphism \( \mathbb{Q}(\pi) \cong \mathbb{Q}(\pi') \) which sends \( \pi \) to \( \pi' \). The purpose of this note is to provide a new/algebraic proof of the surjectivity of the above displayed map, formulated below.

\textbf{Theorem I.} \textit{For any Weil \( q \)-number \( \pi \) there exists a simple abelian variety \( A \) over \( \mathbb{F}_q \) (unique up to \( \mathbb{F}_q \)-isogeny) such that \( \pi \) is conjugate to \( \pi_A \).}\textsuperscript{2}

\textsuperscript{a}Partially supported by NSF grant DMS-1200271

\textsuperscript{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.

\textsuperscript{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 [17], and the surjectivity was proved by Honda [6] and Tate [18].

\textsuperscript{2}In [18] a Weil \( q \)-number is said to \textit{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 $L$ 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 $\pi_A$. 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 [14, 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 [18]. 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 [18], are included for the convenience of the readers.

Step 1. Notations.

A Weil $q$-number $\pi$ has exactly one of the following three properties:

- (Q) It can happen that $\psi(\pi) \in \mathbb{Q}$. In this case $q = p^n = q^m$ and $\pi = \pm \sqrt{q} = \pm p^m$.
- (R) It can happen that $\psi(\pi) \not\in \mathbb{Q}$ and $\psi(\pi) \in \mathbb{R}$. In this case $q = p^n = p^{2m+1}$ and $\pi = \pm \sqrt{q} = \pm p^m \sqrt{p}$. In this case every embedding of $\mathbb{Q}(\pi)$ into $\mathbb{C}$ lands into $\mathbb{R}$.
- ($\not\in \mathbb{R}$) If there is one embedding $\psi : \mathbb{Q}(\pi) \rightarrow \mathbb{C}$ such that $\psi(\pi) \not\in \mathbb{R}$ then for every embedding $\psi : \mathbb{Q}(\pi) \hookrightarrow \mathbb{C}$ we have $\psi(\pi) \not\in \mathbb{R}$ and in this case $\mathbb{Q}(\pi)$ is a CM field.

As we know from [18], 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. $\pi \not\in \mathbb{R}$.

Following [18, Th. 1, p. 96], let $M$ be a finite dimensional central division algebra over $\mathbb{Q}(\pi)$, 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 $\nu$ of $\mathbb{Q}(\pi)$ above $p$, the arithmetically normalized local Brauer invariant of $M$ at $\nu$ is

$$\text{inv}_\nu(M) \equiv \frac{\nu(\pi)}{\nu(q)} \langle \mathbb{Q}(\pi)_\nu : \mathbb{Q}_p \rangle \pmod{\mathbb{Z}}.$$

Let $g := \frac{[\mathbb{Q}(\pi) : \mathbb{Q}] \cdot \sqrt{[M : \mathbb{Q}(\pi)]}}{2}$, a positive integer. According to §3, Lemme 2 on p. 100 of [18] 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 [18, 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 $p$

---

3A 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 $\mathbb{R}$).

4This central division algebra $M$ was denoted by $E$ in [18]. If we can find an abelian variety $A$ over $\mathbb{F}_q$ with $\pi_A \sim \pi$ then we would have $\text{End}^0(A) \cong M$ and $\dim(A) = g = \frac{[\mathbb{Q}(\pi) : \mathbb{Q}] \cdot \sqrt{[M : \mathbb{Q}(\pi)]}}{2}$. 

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

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

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 $\pi$ 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 $\rho$ gives a fixed point free involution on $H_v$; in this case (once $\pi$ 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 $v_1, v_2$ above a place $w$ of $L_0$ dividing $p$ with $v_1 \neq \rho(v_1) = v_2$, the complex conjugation $\rho$ defines a bijective map $\rho \circ \rho : H_{v_1} \rightarrow H_{v_2}$. We choose a subset $\Phi_{v_1} \subset H_{v_1}$ with

$$\#(\Phi_{v_1}) = n_{v_1}$$

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 $\Phi_{v_2}$ of the right size and then define $\Phi_{v_1}$ as $\Phi_{v_1} := H_{v_1} - \Phi_{v_2} \circ \rho$.

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

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

i.e. $\Phi_p$ 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

$$j_p \circ \rho : \text{Hom}(L, \overline{\mathbb{Q}}) \overset{\sim}{\rightarrow} \text{Hom}(L, \mathbb{C}_p).$$

The subset $\Phi := (j_p \circ \rho)^{-1}(\Phi_p) \subset \text{Hom}(L, \overline{\mathbb{Q}})$ is a CM type in the usual sense, i.e. $\Phi \cap (\Phi \circ \rho) = \emptyset$ and $\Phi \cup (\Phi \circ \rho) = \text{Hom}(L, \overline{\mathbb{Q}})$.

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

**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 $G = \text{Gal}(N/\mathbb{Q})$. 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 $\rho$ has Dirichlet density $1/[G : 1] > 0$; see [8, 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 \( \lambda \) 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 \( \text{End}(E) \) is non-commutative. Its endomorphism algebra \( \text{End}^0(E) \) is the quaternion division algebra \( \mathbb{Q}_{r,\infty} \) over \( \mathbb{Q} \) in the notation of [2], which is ramified exactly at \( r \) and \( \infty \). Let \( B_1 := E^g \) and let \( D := \text{End}^0(B_1) = M_2(\mathbb{Q}_{r,\infty}) \).

**Proposition B.** Let \( L' \) be a totally imaginary quadratic extension of a totally real number field \( L_0' \) such \( [L'_1 : L'_0] \) is even for every place \( v \) of \( L' \) above \( r \). Let \( g' = [L'_0 : \mathbb{Q}] \). There exists a positive involution \( \tau \) on the central simple algebra \( \text{End}_\mathbb{Q}(L_0') \otimes_{\mathbb{Q}} \mathbb{Q}_{r,\infty} \cong M_g(\mathbb{Q}_{r,\infty}) \) over \( \mathbb{Q} \) and a ring homomorphism \( \iota : E \hookrightarrow \text{End}_\mathbb{Q}(L_0') \otimes_{\mathbb{Q}} \mathbb{Q}_{r,\infty} \) such that \( \iota(L') \) is stable under the involution \( \tau \) and \( \tau \) induces the complex conjugation on \( L' \).

**Proof.** Let \( \text{End}_\mathbb{Q}(L_0') \cong M_g(\mathbb{Q}) \) be the algebra of all endomorphisms of the \( \mathbb{Q} \)-vector space underlying \( L_0' \). The trace form \( (x, y) \mapsto \text{Tr}_{L'_0/\mathbb{Q}}(x \cdot y) \) for \( x, y \in L_0' \) is a positive definite quadratic form on \( (\mathbb{Q}-\text{vector space underlying}) \), so its associated involution \( \tau_0 \) on \( \text{End}_\mathbb{Q}(L_0') \) is positive. Multiplication defines a natural embedding \( L_0' \hookrightarrow \text{End}_\mathbb{Q}(L_0') \), and every element of \( L_0' \) is fixed by \( \tau_0 \).

Let \( \tau_2 \) be the canonical involution on \( \mathbb{Q}_{r,\infty} \). The involution \( \tau_1 \otimes \tau_2 \) on \( \text{End}_\mathbb{Q}(L_0') \otimes_{\mathbb{Q}} \mathbb{Q}_{r,\infty} \) is clearly positive because \( \tau_2 \) is. It is also clear that the subalgebra \( B := L_0' \otimes_{\mathbb{Q}} \mathbb{Q}_{r,\infty} \) of \( \text{End}_\mathbb{Q}(L_0') \otimes_{\mathbb{Q}} \mathbb{Q}_{r,\infty} \) is stable under \( \tau \). Moreover \( B \) is a positive definite quaternion division algebra over \( L_0' \), so the restriction to \( B \) of the positive involution \( \tau \) 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 \( \tau \).

**Corollary C.** (i) There exists a polarization \( \mu_1 : B_1 \rightarrow B_1^t \) and an embedding \( L \hookrightarrow \text{End}^0(B_1) = D \) such that the image of \( L \) in \( D = \text{End}^0(B_1) \) is stable under the Rosati involution attached to \( \mu_1 \).

(ii) There exists an isogeny \( \alpha : B_1 \rightarrow B_0 \) over \( \overline{\mathbb{F}}_r \) such that the embedding \( L \hookrightarrow \text{End}^0(B_1) = \text{End}^0(B_0) \) factors through an action

\[
t_0 : \mathcal{O}_L \hookrightarrow \text{End}(B_0)
\]

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

\[
\mu_0 := m \cdot (\alpha^t)^{-1} \circ \mu_1 \circ \alpha^{-1} : B_0 \rightarrow B_0^t
\]

is a polarization on \( B_0 \) and the Rosati involution \( \tau_{\mu_0} \) attached to \( \mu_0 \) induces the complex conjugation on the image of \( L \) in \( \text{End}^0(B_0) \).

**Proof.** The statement (i) follows from Proposition B in view of the general structure of the Néron-Severi group \( \text{NS}(B) \) of \( B \) and the ample cone in \( \text{NS}(B) \) explained in [10, §21 pp. 208–210]. The statements (ii) and (iii) follow from (i).\( \square \)

\(^5\)This cubic equation defines an elliptic curve with CM by \( \mathbb{Z}[\mu_3] \), and 2 is inert in \( \mathbb{Q}(\mu_3) \).
From now on we fix $(L, \Phi)$ as in Step 1, with $r$ as in Proposition A, and

$$(B_0, \iota_0 : \mathcal{O}_L \hookrightarrow \text{End}(B_0), \mu_0 : B_0 \to B_0')$$

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 $i_{r,ur} : W(\mathbb{F}_r)[1/p] \hookrightarrow \overline{\mathbb{Q}}_r$. We have bijections

$$\text{Hom}(L, C_p) \xrightarrow{j_r \circ ?} \text{Hom}(L, \overline{\mathbb{Q}}) \xrightarrow{j_r \circ ?} \text{Hom}(L, \overline{\mathbb{Q}}_r) \xrightarrow{i_{r,ur} \circ ?} \text{Hom}(L, W(\mathbb{F}_r)[1/r])$$

The last arrow

$$\text{Hom}(L, \overline{\mathbb{Q}}_r) \xrightarrow{i_{r,ur} \circ ?} \text{Hom}(L, W(\mathbb{F}_r)[1/r])$$

is a bijection because $r$ is unramified in $L$. We regard the $p$-adic CM type $\Phi_p$ as an $r$-adic CM type $\Phi_r \subset \text{Hom}(L, W(\mathbb{F}_r)[1/r])$ 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 $w$ of $L_0$ above $r$, the $w$-adic completion $L_w := L \otimes_{L_0} L_{0,w}$ of $L$ is an unramified quadratic extension field of the $w$-adic completion $L_{0,w} \cong \mathbb{Q}_r$ of $L_0$, and the intersection $\Phi_w := \Phi_r \cap \text{Hom}(L_w, W(\mathbb{F}_r)[1/r])$ is a singleton.

**Step 5. Lifting to a CM abelian variety in characteristic zero.**

**Theorem II.** Let $(B_0, \iota_0 : \mathcal{O}_L \hookrightarrow \text{End}(B), \mu_0 : B_0 \to B_0')$ be an $([L : \mathbb{Q}]/2)$-dimensional polarized supersingular abelian variety with an action by $\mathcal{O}_L$ such that the subring $\mathcal{O}_L \subset \text{End}^d(B_0)$ is stable under the Rosati involution $\tau_{\mu_0}$ as in Corollary C. There exists a lifting $(B, \iota, \mu)$ of the triple $(B, \iota_0, \mu_0)$ to the ring $W(\mathbb{F}_r)$ of $r$-adic Witt vectors with entries in $\mathbb{F}_r$ such that the generic fiber $B_0$ is an abelian variety whose $r$-adic CM type is equal to $\Phi_r$.

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

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

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

$$B_0[r^\infty] \cong \prod_w B_0[w^\infty]$$

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

$$B_0'[r^\infty] \cong \prod_w B_0'[w^\infty]$$

of the $r$-divisible group attached to the dual $B_0'$ of $B_0$. The action of $\mathcal{O}_L$ on $B_0$ induces an action of $\mathcal{O}_L$ on $B_0'$ by $y \mapsto (\iota_0(\rho(y)))^t$ for every $y \in \mathcal{O}_L$, so that the polarization $\mu_0 : B_0 \to B_0'$ is $\mathcal{O}_L$-linear. The quasi-polarization $\mu_0[r^\infty] : B_0[r^\infty] \to B_0'[r^\infty]$ decomposes into a product of quasi-polarizations $\mu_0[w^\infty] : B_0[w^\infty] \to B_0'[w^\infty]$ on the $\mathcal{O}_{L,w}$-linear $r$-divisible groups $B_0[w^\infty]$ of height $2$.

It suffices to show that for each place $w$ of $L_0$ above $r$, the $\mathcal{O}_{L,w}$-linearly polarized $r$-divisible group $(B_0[w^\infty], \iota_0[w^\infty], \mu_0[w^\infty])$ over $\mathbb{F}_r$ can be lifted to $W(\mathbb{F}_r)$ with $r$-adic
CM type $\Phi_w$. For then the Serre-Tate theorem of deformation of abelian schemes tells us that $(B_0, \iota_0, \mu_0)$ can be lifted over $W(\overline{F}_r)$ to a formal abelian scheme $\mathfrak{B}$ with an action by $\mathcal{O}_L$ and an $\mathcal{O}_L$-linear polarization whose $r$-adic CM type is $\Phi_r$; see [7], [9, Ch. V, Th. 2.3] on page 166. Grothendieck’s algebraization theorem implies that $\mathfrak{B}$ comes from a unique abelian scheme $B$ over $W(\overline{F}_r)$, see [3, III 1.5.4].

For any $r$-adic place $w$ among the $g$ places of $L_0$ above $r$, the existence of a CM lifting to $W(\overline{F}_r)$ of the $\mathcal{O}_{L,w}$-linear polarized $r$-divisible group $(B_0[w^\infty], \iota_0[w^\infty], \mu_0[w^\infty])$ 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 [12, 14.7]. Below is a proof using Lubin-Tate formal groups.

By [11, Th. 1], there exists a one-dimensional formal $p$-divisible group $X$ of height 2, over $W(\overline{F}_r)$ plus an action $\beta : \mathcal{O}_{L,w} \to \text{End}(X)$ of $\mathcal{O}_{L,w}$ on $X$ whose $r$-adic CM type is $\Phi_w$. Let

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

be the closed fiber of $(X, \beta)$. It is well-known that the $\mathcal{O}_{L,w}$-linear $p$-divisible group $(X_0, \beta_0)$ over $\overline{F}_r$ is isomorphic to $(B_0[w^\infty], \iota_0[w^\infty])$; we choose and fix such an isomorphism and identify $(B_0[w^\infty], \iota_0[w^\infty])$ with $(X_0, \beta_0)$. The Serre dual $X^t$ of $X$, with the $\mathcal{O}_{L,w}$-action defined by $\gamma : b \mapsto (\beta(\rho(b))^\dagger \quad \forall b \in \mathcal{O}_{L,w}$, also has CM type $\Phi_w$. Let $(X_0^t, \gamma_0)$ be the closed fiber of $(X^t, \gamma)$. The natural map

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

defined by reduction modulo $r$ is a bijection: [11, Thm. 1] implies that $(X^t, \gamma)$ is isomorphic to $(X, \beta)$, and after identifying them via a chosen isomorphism both the source and the target of $\xi$ are isomorphic to $\mathcal{O}_{L,w}$ so that $\xi$ is an $\mathcal{O}_{L,w}$-linear isomorphism.

Under the identification of $(X_0, \beta_0)$ with $(B_0[w^\infty], \iota_0[w^\infty])$ specified above, the quasi-polarization $\mu_0[w^\infty]$ on $B_0[w^\infty]$ is identified with a quasi-polarization $\nu_0$ on $X_0$. The quasi-polarization $\nu_0 : X_0 \to X_0^t$ extends over $W(\kappa_{L,w})$ to a quasi-polarization $\nu : X \to X^t$ because $\xi$ is a bijection. We have shown that the triple $(B_0[w^\infty], \iota_0[w^\infty], \mu_0[w^\infty])$ can be lifted over $W(\overline{F}_r)$.

**Remark.** One can also prove the existence of a lifting of $(B_0[w^\infty], \iota_0[w^\infty], \mu_0[w^\infty])$ to $W(\overline{F}_r)$ using the Grothendieck-Messing deformation theory for abelian schemes. The point is that the deformation functor for $(B_0[w^\infty], \iota_0[w^\infty])$ is represented by $\text{Spf}(W(\overline{F}_r))$ because $\mathcal{O}_{L,w}$ is unramified over $\mathbb{Z}_p$.

We fix the generic fiber $(B_0, \iota, \nu)$ of a lifting as in Theorem II over the fraction field $W(\overline{F}_r)[1/r]$ of $W(\overline{F}_r)$ with an $\mathcal{O}_L$-linear action $\iota : \mathcal{O}_L \hookrightarrow \text{End}(B_0)$, whose $r$-adic CM type is $\Phi_r$.

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

We have arrived at a situation where we have an abelian variety $B_0$ over a field of characteristic zero with an action $\mathcal{O}_L \hookrightarrow \text{End}(B_0)$ by $\mathcal{O}_L$, whose $r$-adic CM type with respect to an embedding of the base field in $\overline{F}_r$ is equal to the $r$-adic CM type $\Phi_r$ 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. [16, Prop. 26, p. 109] or [1, Prop. 1.5.4.1]. By [15, 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 $\delta$ of characteristic $p$ with $F_q \subset \delta$.

We have arrived at the following situation.
We have a CM abelian variety \((C, L \hookrightarrow \End^0(C))\) of dimension \(g = [L : \mathbb{Q}]/2\) over a number field \(K\), of \(p\)-adic CM type \(\Phi_p\) 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 \(\pi\) is effective.

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

- \(\pi^i\) and \(\pi_{C_0}\) 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 \(\Phi\) in Step 2 and by [18], Lemme 5 on page 103, we know that \(\pi^i\) and \(\pi_{C_0}\) have the same valuation at every place above \(p\). As remarked in [18, p. 103/104], the essence of this step is the “factorization of a Frebenius endomorphism into a product of prime ideals” in [16].

This shows that \(\pi^i/\pi_{C_0}\) 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 \(\pi^i/\pi_{C_0}\) is a root of unity in \(\mathcal{O}_L\). See for instance [5, §34 Hilfsatz a)]; the main point is that the set

\[
\{ y \in \mathcal{O}_L \mid |\psi(y)| \leq 1 \forall \text{ complex embedding } \psi : L \hookrightarrow \mathbb{C} \}
\]

is finite because the image of \(\mathcal{O}_L\) in \(\prod L_{\nu}\) is a lattice, where the index \(\nu\) runs through all archimedian places of \(L\), hence \(\pi^i/\pi_{C_0} = y \in \mathcal{O}_L\) is a root of unity. 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 \(\pi^{ij}\) is effective, because it is (conjugate to) the \(q^{ij}\)-Frobenius of the base change of \(C_0\) to \(\mathbb{F}_{q^i}\). By [18, Lemma 1, p. 100] this implies that \(\pi\) is effective, and this ends the proof of the theorem in the introduction. \(\square\)

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 \(\pi\) 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 \(\pi\) 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 \(L/\mathbb{Q}\) 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 \(\pi\) is the \(q\)-Frobenius of a supersingular elliptic curve over \(\mathbb{F}_q\), see Step 1, and \(\pi\) 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 \(\pi\); by [18, Lemme 1] on page 100 we conclude \(\pi\) is effective.

The 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).
References


Ching-Li Chai
Inst. of Math., Academia Sinica
6F Astr-Math Building
No. 1, Sec. 4, Roosevelt Rd.
Taipei 10617, Taiwan (R.O.C.)
chai@math.sinica.edu.tw
and
Department of Mathematics
University of Pennsylvania
Philadelphia, PA 19104-6395
USA
chai@math.upenn.edu
www.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/