CM Liftings

Frans Oort

Notes for a talk at the conference
Lifting Problems and Galois Theory
BIRS Workshop August 2015

In this talk we discuss the question whether any abelian variety A_0 defined over a finite field $\kappa = \mathbb{F}_q$ admits a CM lifting to characteristic zero.

We will see results by Deuring (1941), Weil (1948), Tate (1966), Honda(1968), a results on isogenies (1992), and various questions and full answers as given in the book (2014):
Brian Conrad, Ching-Li Chai and Frans Oort:
Complex multiplication and lifting problems.
In short, we see the "flow of mathematics", the history of this topic from Hasse (1933) to final answers to these questions (2014).

1 Lifting an endomorphism of an elliptic curve, Deuring 1941

(1.1) Theorem (Deuring, 1941). *Let E_0 be an elliptic curve over a finite field $\kappa = \mathbb{F}_q$. Let $\beta \in \mathrm{End}(E_0)$ be an endomorphism. The pair (E_0, β) can be lifted to characteristic zero.*

(1.2) Remark. An elliptic curve E in positive characteristic p is called *supersingular* if $E \otimes k$ has no points of order exactly p (where k is an algebraically closed field); we say E is *ordinary* if $E \otimes k$ does have a point of order exactly p.

For an elliptic curve E over a finite field $\kappa = \mathbb{F}_q$ Deuring proved the following three possibilities occur for the endomorphism algebra $D := \mathrm{End}^0(E) = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$:

- **(ord)** The algebra D is an imaginary quadratic field in which p is split; in this case E is ordinary. In this case $\mathrm{End}^0(E) = \mathrm{End}^0(E \otimes k)$, where k is the algebraic closure of κ.
- **(ss D non-maximal)** The algebra D is an imaginary quadratic field in which p is split; in this case E is supersingular. In this case $\mathrm{End}^0(E) \subsetneqq \mathrm{End}^0(E \otimes k)$.
- **(ss D maximal)** The algebra $D := \mathrm{End}^0(E) \cong \mathbb{Q}_{\infty,p}$ is the quaternion algebra non-split precisely above the places ∞ and p of $\mathbb{Q}$. In this case E is supersingular.

Note in particular, that for an elliptic curve over a finite field $\mathrm{End}(E) \supsetneqq \mathbb{Z}$; this was unknown to Hasse in 1933, but observed for the first time by Deuring in 1941.

Note that in case **(ss D maximal)** the pair $(E_0, \mathrm{End}(_0))$ *cannot be lifted to characteristic zero.* We will encounter this phenomenon many times: the additional structure in characteristic p is "too large" to be realized in characteristic zero.

2 The pRH for abelian varieties, Weil 1948

For an abelian variety A over a finite field $\kappa = \mathbb{F}_q$, with $q = p^n$ we write $\pi = \pi_A = \mathrm{Frob}_{A/\kappa}$ for the Frobenius "$\pi = F^n$"; this map is given on geometric points by "raising all coordinates to the power q".

(2.1) Theorem (Weil, 1948). *For a simple abelian variety A over a finite field $\kappa = \mathbb{F}_q$ and any embedding $\psi : \mathbb{Q}(\pi) \to \mathbb{C}$ we have*

$$\mid \psi(\pi) \mid = \sqrt{q} \qquad \text{(pRH)}$$

This is "the Riemann hypothesis in characteristic p". I use notation (pRH) in order to distinguish this from the classical Riemann Hypothesis (RH).

(2.2) For $q = p^n$ we say an algebraic number π is a Weil q-number if it is an algebraic integer with

$$\mid \psi(\pi) \mid = \sqrt{q}, \quad \forall\ \psi : \mathbb{Q}(\pi) \to \mathbb{C}.$$

Note that $\mathrm{End}(A)$ is of finite $\mathbb{Z}$-rank, hence any π_A as above is an algebraic integer, and by (pRH) we see it is a Weil q-number.

(2.3) Note that Weil numbers are easy to construct: either π is real with $\mid \pi \mid = \sqrt{q}$ or π is non-real, and it is a zero of a polynomial $T^2 - \beta T + q$, where β is a totally real number and $\psi(\beta)^2 - 4q < 0$ for any embedding ψ into $\mathbb{R}$.

3 CM abelian varieties

(3.1) An abelian variety B over a field K s called *simple* if 0 and B are the only abelian subvarieties. The theorem of Poincaré-Weil (valid over any base field) says that any abelian variety A over K is isogenous over K with a product of simple abelian varieties.

A simple abelian variety B over a field K is said to admit *sufficiently many complex multiplications* if there exists a field L with $L \subset \mathrm{End}^0(B)$ and $[L : \mathbb{Q}] = 2{\cdot}\mathrm{dim}(B)$. We abbreviate this by saying that B is a CM abelian variety. An abelian variety A is called a CM abelian variety if it is isogenous with a product of simple CM abelian varieties. Equivalently: A is called a CM abelian variety if $\mathrm{End}^0(A)$ contains a commutative semi-simple subalgebra of rank $2{\cdot}\mathrm{dim}(A)$ over $\mathbb{Q}$.

(3.2) CM type. Let B be a simple CM abelian variety over a field $K \supset \mathbb{Q}$ *of characteristic zero*; in this case $L = \mathrm{End}^0(B)$ is a field (note in positive characteristic this is not true in general), it is a CM field. The action on B induces a representation on the tangent space

$$L \to \mathrm{GL}(\mathfrak{t}_{B,0}).$$

As L is commutative, this action, over $\mathbb{C}$ can be described by its characters, and this set, or equivalently this representation is called the CM type of the CM abelian variety B.

Important property. Let L be a CM field of degree $2g$ with $L \cong \mathrm{End}^0(A)$ in characteristic zero, with $\mathrm{dim}(A) = 2g$. Let the action of L on $\mathfrak{t} := \mathfrak{t}_{A,0}$ be given by $\Phi = \{\varphi_1, \cdots, \varphi_g\}$ (this is called the CM type of the action), where $\varphi_j : L \to \mathbb{C}$. It follows that

$$\varphi \in \Phi \quad \Longrightarrow \quad \overline{\varphi} \notin \Phi, \quad \Phi \sqcup \overline{\Phi} = \mathrm{Hom}(L, \mathbb{C}),$$

because

$$\mathrm{H}_1(A(\mathbb{C}),\mathbb{R}) \quad\cong\quad \mathfrak{t}\oplus\bar{\mathfrak{t}}$$

is an L-module of rank one. This characterizes CM types; every Φ having this property shows up as a CM type of a CM abelian variety over $\mathbb{C}$.

Easy example. Suppose $L=\mathbb{Q}(\zeta_5)$; let $z\in\mathbb{C}$ with $z^5=1$, and $z\neq 1$. The set $\mathrm{Hom}(L,\mathbb{C})$ is given by the four maps $\zeta_5\mapsto z^j$, with $1\leq j\leq 4$. In this notation the possible CM types are $\{z^1,z^2\}$, $\{z^1,z^3\}$, $\{z^2,z^4\}$. Up to conjugation there is only one CM Type in this case.

An isogeny of CM *abelian varieties $B\sim_K C$ gives "equal" representations*: the isogeny gives an isomorphism $\mathrm{End}^0(B)\cong\mathrm{End}^0(C)$ and it induces an isomorphism $\mathfrak{t}_{B,0}\cong_K\mathfrak{t}_{C,0}$ in an equivariant way.

(3.3) An example. Suppose the base field is $\mathbb{C}$, and a curve C is given by $Y^5=X^3-1$. We see that the genus of C equals $g=4$: the map $(x,y)\mapsto(x)$ gives a cyclic cover $C\to\mathbb{P}^1$ of degree 5, with 4 total ramification points, and the Riemann - Hurwitz formula gives

$$2g-2=5\cdot(-2)+4\cdot(5-1),\quad\text{hence}\quad g=4.$$

Let $J=\mathrm{Jac}(C)$. We see that $y\mapsto\zeta_5\cdot y$ and $x\mapsto\zeta_3\cdot y$ shows

$$\mathbb{Q}(\zeta_{15})\subset\mathrm{End}^0(J);\quad\text{write}\quad\zeta=\zeta_{15},\ \ \zeta^5=\zeta_3,\ \ \zeta^3=\zeta_5.$$

As $[\mathbb{Q}(\zeta_{15}):\mathbb{Q}]=8$ we see that J is a CM abelian variety over $\mathbb{C}$. A basis for the regular differentials on C is given by

$$\{\frac{dx}{y^2},\frac{dx}{y^3},\frac{dx}{y^4},\frac{xdx}{y^4}\}.$$

The representation, the CM type of J, on this basis is given by

$$\{\zeta^5\cdot\zeta^{-6}=\zeta^{-1},\zeta^{-4},\zeta^{-7},\zeta^{-2}\}=\{\zeta^{14},\zeta^{11},\zeta^{8},\zeta^{13}\}=\Phi;$$

we see this is a CM type for $\mathbb{Q}(\zeta_{15})$: the complement of Φ indeed is its complex conjugate $\{\zeta,\zeta^4,\zeta^7,\zeta^2\}$.

(3.4) Do not use the terminology CM type in positive characteristic. Suppose A is an abelian variety in characteristic p. We obtain a representation $\mathrm{End}(A)\to\mathrm{GL}(\mathfrak{t}_{A,0})$. This does not extend to $\mathrm{End}^0(A)$. This representation factors through $\mathrm{End}(A)/(p)$. An isogeny $A\sim_K B$ in general does not give an isomorphism between $\mathfrak{t}_{A,0}$ and $\mathfrak{t}_{B,0}$. The action of $\mathrm{End}(A)/(p)$ on $\mathfrak{t}_{A,0}$ and of $\mathrm{End}(B)/(p)$ on $\mathfrak{t}_{B,0}$ are not "equal" in many situations. Hence we should not use the terminology "CM type in positive characteristic". Actually, as we will see, it is this change of representation that makes the CM lifting problem hard and interesting and accessible .– This remarks will be made explicit in a crucial example below. It is one of the most important details to understand CM liftings.

4 Abelian varieties over a finite field, Tate 1966

Results by Deuring (1941) inspired Tate to prove results on ℓ-adic representations on abelian varieties over a finite field (starting a whole string of theorems and conjectures). (We will not discuss the important case of ℓ-adic representations.) One of these is:

(4.1) Theorem (Tate, 1966) *Any abelian variety over a finite field is a* CM *abelian variety.*

(4.2) For a given Weil q-number $\pi = \pi_A$ with $q = p^n$ Tate shows how to compute the dimension of this simple A and the structure of $\mathrm{End}^0(A)$ knowing π_A: for

$$\mathbb{Q} \subset L := \mathbb{Q}(\pi) \subset D := \mathrm{End}^0(A)$$

the field L is central in the division algebra D,
no real place of L splits in D,
every place prime to p splits in D/L and
for every place v above p in L the Brauer invariant is given by

$$\mathrm{inv}_{B/L} \equiv v(\pi_A)\frac{f_v}{n} \pmod 1,$$

where f_v stands for the residue degree at v. See [11], Th. 1 on page 96.

5 Honda - Tate theory, 1968

As proved by Weil (1948) we know that π_A is a Weil q-number, and we can define the map

$$\{\text{simple abelian variety over } \mathbb{F}_q\}/\sim \quad \xrightarrow{\sim} \quad \{\text{Weil } q-\text{number}\}/\sim$$

Here the left hand $\sim$ means isogeny of abelian variety, the right hand $\sim$ stands for conjugacy, i.e. $\pi \sim \pi'$ if there exists an isomorphism $\mathbb{Q}(\pi) \cong \mathbb{Q}(\pi')$ mapping π to π'. Isogenous abelian varieties give conjugated Weil numbers; hence this map is well defined.

(5.1) **Theorem** (Honda, Tate). *For $q = p^n$ this map is bijective.*
Injectivity was proved by Tate and the most important aspect of subjectivity was proved by Honda (and by Tate showing that indeed this works over a finite field without extending that field).

The proof by Honda uses CM-theory and complex parametrization of abelian varieties, plus reduction to characteristic p. For a different proof, not using complex uniformization, see [2].

(5.2) **Interesting exercise.** Describe all Weil q-numbers appearing for some q and some elliptic curve over $\mathbb{F}_q$. See [12], Th. 4.1 on page 536, and [9], 14.6

(5.3) **An example** (the "*toy model* "). Suppose p is a prime number with $p \equiv 2, 3 \pmod 5$; equivalently: the prime number p is remains prime in $L := \mathbb{Q}(\zeta_p)$. Clearly $\pi = p{\cdot}\zeta_5$ is a Weil p^2-number. Hence by Honda-Tate theory there exists (an isogeny class of) an abelian variety A with $\pi_A \sim \pi$. We see $[L : \mathbb{Q}] = 4$. This field has no real place; hence the Brauer invariant above p in D/L equals zero. Hence there is no ramification in D/L, we conclude $L = D$ and $\dim(A) = 2$. Moreover $\pi^5 = (p{\cdot}\zeta_5)^5 = p^5$ is real; this shows $A \otimes \mathbb{F}_{p^{10}}$ is isogenous with a product of two supersingular elliptic curves.
Try to consider: does A over $\mathbb{F}_q$ with $q = p^2$ as given above admit a CM lift to characteristic zero?

(5.4) **Theorem** (Honda) *For any abelian variety A over $\kappa = \mathbb{F}_q$ there exists a finite extension $\kappa \subset \kappa'$ and an isogeny $A \otimes_\kappa \kappa' = A' \sim_{\kappa'} B_0$ such that B_0 admits a* CM *lift to characteristic zero.*
This is part of (the proof of) the Honda-Tate theory: the surjectivity follows from a construction of a CM abelian variety in characteristic zero reducing mod p to an abelian variety having Weil number equal to some power of the given π.

6 CM lifting questions

Question. Does every abelian variety A_0 defined over a finite field $\kappa = \mathbb{F}_q$ admit a CM lifting to characteristic zero?

We know by Honda that a CM *lifting is possible after extending the base field and applying an isogeny.*

- Is a field extension necessary ?
- Is an isogeny necessary?

(6.1) We now know that we have to make this question more precise:

- Do we want a lift to an arbitrary mixed characteristic integral domain?
- Do we want a lift to a *normal* mixed characteristic integral domain?

(6.2) The residual reflex condition. We will see that the answers to these different questions are different, see [1], 2.1.5 - 2.1.7.
Example. (We use the toy model.) Let $p \equiv 2,\ 3 \pmod 5$ and let B_0 be any abelian variety over $\kappa = \mathbb{F}_q$ with $q = p^2$ and $\pi_{B_0} \sim \pi := p{\cdot}\zeta_5$.
Claim. *The abelian variety B_0/κ does not admit a CM lift to a* normal *mixed characteristic integral domain.*
Proof. We know $\mathrm{End}^0(B) = L = \mathbb{Q}(\zeta_5)$; if a CM lift would exist, it would have CM by (an order in) $L = \mathbb{Q}(\zeta_5)$. Suppose the lift $\mathcal{B} \to \mathrm{Spec}(R)$ is to $K \supset R \to \kappa = \mathbb{F}_q = \mathbb{F}_{p^2}$. The CM abelian variety $B := \mathcal{B} \otimes_R K$ has CM by $L = \mathbb{Q}(\zeta_5)$. By CM theory in characteristic zero we know that the field K does contain the reflex field of L. This is a CM field (with possibly other properties) contained in L. However L only contains two proper subfields:

$$\mathbb{Q} \text{ and } L_0 \text{ and the maximal real subfield of } L$$

(this follows because $L/\mathbb{Q}$ is Galois with Galois group cyclic of order 4). Conclusion: any field over which B allows CM by L contains L. Suppose R is normal. Then any residue class field in characteristic p contains the residue class field of L, which is $\mathbb{F}_{p^4}$. Because

$$\mathbb{F}_{p^4} \not\subset \kappa = \mathbb{F}_{p^2}$$

we derive a contradiction; *this shows B_0 does admit a* CM *lift to a* normal *mixed characteristic integral domain.*

Remark. In Chapter 2 of [1] we see that the residual reflex condition is "the only obstruction" to the existence of CM lifting up to isogeny over a normal local domain in characteristic zero.

However the previous proof does not exclude the possibility of a lift to a mixed characteristic integral domain. Let me give you two examples of an integral domain, where normalization gives a non-trivial extension of the residue class field.
Example. Let $\kappa \subsetneq \kappa'$ be a non-trivial algebraic extension of fields. Consider a ring of formal power series

$$\Gamma = \{\sum_j a_j T^j \mid a_0 \in \kappa, \quad a_j \in \kappa' \quad \forall j > 0\}.$$

We see that Γ is a local domain, with residue class field κ and with field of fractions $K := Q(\Gamma)$. We show that the integral closure $\Gamma^{\sim}$ of $\Gamma \subset K$ equals $\Gamma^{\sim} = \kappa'[[T]$. Indeed, $\beta \in \kappa'$ can be written as $\beta = \beta{\cdot}T/T$. hence $\beta \in K$; we conclude $K = \kappa'((T))$. Any $\beta \in \kappa'$ satisfies its minimal equation $\beta^n = \sum_{n>j\geq 0} \gamma_j \beta^j$. with $\gamma_j \in \kappa \subset \Gamma$. Hence β is integral over Γ. This shows that the integral closure of Γ inside K equals $\Gamma^{\sim} = \kappa'[[T]$, and the residue class field of the local ring $\Gamma^{\sim}$ equals κ'.

A similar example can be constructed in mixed characteristic: take an algebraic extension of perfect fields in characteristic p. Let $\Delta = W_\infty(\kappa')$ be the ring of infinite Witt vectors, and

$$\Gamma := \{\delta \in \Delta \mid \delta \bmod p \in \kappa\}.$$

Again, here we see that the residue class field of this local ring Γ equals κ, and the normalization $\Gamma^{\sim} = \Delta$ has reside class field κ'.

We will see that such rings naturally appear in our solutions of lifting problems especially in the case of the CM lifting problem.

(6.3) Exercise Let $\kappa \subset \kappa'$ be an extension of fields or arbitrary characteristic. Let Γ be the ring of power series $\sum_j a_j T^j$ with $a_0 \in \kappa$ and $a_j \in \kappa' \ \ \forall j > 0$. Under which conditions on $\kappa \subset \kappa'$ is Γ a normal domain?

7 (Almost) ordinary abelian varieties

(7.1) Notation. For an abelian variety A over $K \supset \mathbb{F}_p$ we write $f = f(A)$ for its p-rank, i.e. the integer defined by

$$A[p](k) \cong (\mathbb{Z}/p)^f;$$

here $[p]$ means taking the kernel by multiplication by p, and k is an algebraically closed field containing K.
Well known: $0 \leq f(A) \leq \dim(A)$, and all values do occur.

Definition. An abelian variety A with $f(A) = \dim(A)$ is called an *ordinary abelian variety.* An abelian variety A with $f(A) = \dim(A) - 1$ is called an *almost ordinary abelian variety.*

(7.2) Theorem (Serre and Tate 1964). *Let A be an* ordinary *abelian variety over a perfect field $K \supset \mathbb{F}_p$. The pair $(A, \mathrm{End}(A))$ can be lifted to an abelian variety with these endomorphisms in characteristic zero.*

(7.3) Theorem (Deuring 1941, FO 1973 and 1985). *A* CM almost ordinary *abelian variety in positive characteristic can be lifted to a* CM *abelian variety in characteristic zero.*

(7.4) Notation. We write α_p for the local-local group scheme in characteristic p. for an abelian variety A (or a group scheme, or a p-divisible group) over a perfect field $\kappa \supset \mathbb{F}_p$ we write

$$a(A) = \dim_\kappa \left(\mathrm{Hom}(\alpha_p, A)\right).$$

8 An isogeny is necessary, 1992

We have seen that ordinary and almost ordinary abelian varieties defined over a finite field admit CM liftings. We address the question for other abelian varieties.

(8.1) Theorem (FO, 1992). *Let $g \in \mathbb{Z}_{\geq 3}$, and $0 \leq f \leq g-2$, and $k = \overline{\mathbb{F}_p}$. There exist infinitely many abelian varieties over k of dimension g and p-rank equal to f that do* not *allow a* CM *lift to characteristic zero.*

Sketch of a proof. Suppose $g \geq 3$ and $0 \leq f \leq g-2$ fixed. Construct an abelian variety A over a finite field κ with $\dim(A) = g$ and $f(A) = 2$, and $a(A) = 2$ such that there exists $\alpha_p \subset A$ with $a(A/\alpha_p) = 1$. Let

$$\Gamma := \{B \mid B \cong (A \otimes k)/\alpha, \quad a(B) = 1\}/\cong .$$

Note that

$$B_1 = (A \otimes k)/(\psi_1(\alpha)) \cong B_2 = (A \otimes k)/(\psi_2(\alpha))$$

for $a(B_1) = 1$ implies $\psi_1 = \psi_2$. As the number $a((A \otimes k)/\alpha)$ is lower semi-continuous, and assumes the value one by assumption we see that $\#(\Gamma) = \infty$. Choose coordinates for $\mathrm{Hom}(\alpha_p, A)$; this identifies $\psi : \alpha_p \to A \otimes k$ as a point in $\mathbb{P}^1(k)$ and the elements of Γ coming from $\alpha_p \subset A \otimes K$ give $\Gamma_K \subset \mathbb{P}^1(K)$. Actually, $\#(\mathbb{P}^1(k) \setminus \Gamma) < \infty$.

Crucial property. If $A \otimes k \to (A \otimes k)/\psi(\alpha_p) = B$ has the property with $a(B) = 1$ then we can reconstruct this quotient map from B alone: it follows that $a(B_t) = 1$ and $A \cong (B^t/(\alpha_p))^t$ canonically.

Next one can show that there exists a finite extension $\kappa \subset \kappa'$, and a pro-p-extension $\kappa' \subset \Omega$ such that if $B = (A \otimes k)/(\psi(\alpha))$ admits a CM lift to characteristic zero, then ψ is defined over Ω; this part of the proof uses CM-theory in characteristic zero.

From the fact that

$$\#\left(\mathbb{P}^1(k) \setminus \mathbb{P}^1(\Omega)\right) = \infty$$

and the description of elements of Γ we see that

$$\#\left(\Gamma \setminus \Gamma_\Omega\right) = \infty,$$

which proves the theorem.

In the book *Complex multiplication and lifting problems*, Chapter 3, a proof using p-divisible groups is given, also including the case $g = 2$ and $f = 0$.

9 Survey of CM lifting questions and answers

We survey what has been described above, and we give the main theorem of the book *Complex multiplication and lifting problems*: Chapter 4.

By Honda (1968) we know that a CM lift can be achieved for an abelian variety over a finite field after extending the field and performing an isogeny. Note that in the Honda theory the isogeny is chosen after extending the field.

Isog. We know (1992) that an isogeny is necessary there are many abelian varieties over $k = \overline{\mathbb{F}_p}$ that do not allow a CM lift (but these are abelian varieties with $f \leq g-2$).

ResReflCond. We know there exist abelian varieties over a finite field that do not allow a CM lift to a a *normal* mixed characteristic integral domain, the *residual reflex condition*:

asking for a lift to a *normal* domain, in general extending the field and applying an isogeny is necessary.

(9.1) Theorem (B.Conrad-Chai-FO 2014).*Let A be an abelian variety over a finite field κ. There exists an isogeny $A \sim_\kappa B_0$ such that B_0 admits a* CM *lift to characteristic zero.*

The proof uses many pages of preparations, plus more than 50 pages, and I will not try to indicate a proof here. However it might be instructive to see (part of the methods) in a sketch of the proof in a special case.

(9.2) The toy model allows a CM lifting after a κ-isogeny. We start with $\kappa = \mathbb{F}_{p^2}$ with $p \equiv 2, 3 \pmod 5$, and $\pi = p{\cdot}\zeta_5$. Using Honda-Tate theory we choose an abelian variety A over κ with $\pi_A \sim \pi = p{\cdot}\zeta_5$. Note that $\dim(A) = 2$ is a κ-simple abelian surface, and $\mathbb{Z}[p{\cdot}\zeta_5] \subset \mathrm{End}(A)$ and $\mathrm{End}^0(A) = \mathbb{Q}(\zeta_5)$; moreover A is supersingular, and $A \otimes k \sim E \times E$, where E is a supersingular elliptic curve over $k = \overline{\mathbb{F}_p}$. We write here $\zeta = \zeta_5$.

Using a technique called Serre's tensor construction we can choose an isogeny $A \sim_\kappa B_0$ with

$$\mathrm{End}(B_0) = \mathbb{Z}[\zeta].$$

We are going to show that B_0 satisfies the conclusion of the theorem, i.e. B_0 can be CM *lifted to characteristic zero* (but not lifting the whole of $\mathrm{End}(B_0)$ along), showing the theorem in this special case.

Here are some aspects of the proof in case of this example.

- We have $a(B_0) = 2$; the action of $\mathbb{Z}[\zeta]$ for $\mathfrak{t} := \mathfrak{t}_{B_0,0}$ is on $\mathfrak{t} \otimes k$ given, up to conjugacy, by $\{\zeta, \zeta^4\}$. Side remark: it follows that the pair $(B_0, \mathrm{End}(B_0))$ cannot be lifted to characteristic zero (!!).
- Choose an eigenspace $\psi(\alpha_p) \subset (B_0 \otimes k)$ for the $\mathbb{Z}[\zeta]$-action. Define C_0, over k, by the exact sequence

$$0 \to \alpha_p \xrightarrow{\psi} B_0 \otimes k \longrightarrow C_0 = (B_0 \otimes k)/\psi(\alpha_p) \to 0.$$

- Then $a(C_0) = 1$.
- Then $\mathrm{End}(C_0) \cong \mathbb{Z}[\zeta]$, and the action on $\mathfrak{t}_{C_0,0}$ is given, up to conjugacy, by $\{\zeta, \zeta^3\}$.
- The pair $(C_0, \mathrm{End}(C_0))$ can be lifted to characteristic zero as an ablian scheme $(\mathcal{C}, \mathbb{Z}[\zeta])$ over a ring $K \supset R \to k$ (use CM theory).
- Assume (after a finite base extension) that $\mathcal{C} \otimes K$ has a rational point $s \in \mathcal{C}(K)$ of order exactly p and assume R is a discrete valuation ring. Consider the subgroup $\mathbb{Z}/p \cong <s>= N \subset \mathcal{C} \otimes K$, and its flat extension $\mathcal{N} \subset \mathcal{C}$.
- Claim $\mathcal{B} := \mathcal{C}/\mathcal{N}$ has the property $\mathcal{B} \otimes k \cong B_0 \otimes k$. Here we crucially use $a(C_0) = 1$ and the fact that $B_0 \otimes k \to C_0$ can be canonically reconstructed from $\alpha_p \subset C_0$.
- **Conclusion.** We have constructed a CM lift of $B_0 \otimes k$. However, remark that $\mathbb{Z} + p\mathbb{Z}[\zeta] \subset \mathrm{End}(\mathcal{B})$ but $\mathbb{Z}[\zeta]$ is not contained in $\mathrm{End}(\mathcal{B})$ (!!).

- **Conclusion.** We see that B_0 admits a CM lift to characteristic zero: use the theory of moduli. Note that we see here that the lift can be given over the subring $\Gamma \subset R$ of all elements of R mapping to κ (a typically non-normal ring). (And we know a CM lifting of B_0/κ to a normal domain is not possible.) $\square$

Warning, remark. Hidden in considerations above is the fact that, although algebraization of formal abelian schemes is difficult and often not possible, this is possible for "CM formal abelian schemes" in case the action of the CM algebra is via a CM Type, see [1], Theorem 2.2.3.

Remark. In the toy model we saw that the condition $\mathcal{O}_L \subset \mathrm{End}(B_0)$ was sufficient for the existence of a CM lift in this case. At the time of writing [1] we did not know whether this condition would ensure CM liftability in all cases. (We called this (sCML), the strong CM lifting question.) However, later, Taisong Jing in his UPenn PhD-thesis gave examples of abelian varieties B_0 in positive characteristic with CM by L, such that $\mathcal{O}_L \subset \mathrm{End}(B_0)$, where this B_0 does not admit a CM lifting. See
`https://www.math.upenn.edu/~taisong/`
Strong CM Lifting Problem I, and II.

References

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

[2] C-L. Chai & F. Oort – *An algebraic construction of an abelian variety with a given Weil number.* [To appear in Journ. Algebraic Geometry.]

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

[4] N. Katz – *Serre-Tate local moduli.* In: Algebraic surfaces (Orsay, 1976–78), pp. 138–202, Lecture Notes in Math., 868, Springer, Berlin-New York, 1981.

[5] J. Lubin, J-P.Serre & J. Tate – *Elliptic curves and formal groups.* In: Lecture notes prepared in connection with the seminars held at the Summer Institute on Algebraic Geometry, Whitney Estate, Woods Hole, Massachusetts, July 6 – July 31, 1964. To be found at:
`http://www.jmilne.org/math/Documents/`

[6] F. Oort – *Lifting an endomorphism of an elliptic curve to characteristic zero.* Nederl. Akad. Wetensch. Proc. Ser. A 76=Indag. Math. **35** (1973), 466–470.

[7] F. Oort – *Lifting algebraic curves, abelian varieties and their endomorphisms to characteristic zero.* In *Algebraic geometry, Bowdoin 1985* (S. Bloch, ed.). Proceed. Sympos. Pure Math. **46** Part 2, AMS 1987; pp. 165–195.

[8] F. Oort – *CM-liftings of abelian varieties.* Journ. Alg. Geom. **1**, 1992, 131–146.

[9] F. Oort – *Abelian varieties over finite fields.* In: *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 (D. Kaledin & Y. Tschinkel, ed.). IOS Press 2008, 123–188.

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

[11] J. Tate – *Class d'isogenie des variétés abéliennes sur un corps fini* (d'après T. Honda). Séminaire Bourbaki, 1968/69, no. 352. Lect. Notes Math. 179, Springer-Verlag 1971, 95–110.

[12] W Waterhouse – *Abelian varieties over finite fields.* Ann. Ec. Norm. Sup. **4** Ser. 2 (1969), 521–560

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

[14] A. Weil – *Variétés abéliennes et courbes algébriques.* Actualités Sci. Ind., no. 1064 = Publ. Inst. Math. Univ. Strasbourg 8 (1946). Hermann & Cie. 1948.

Frans Oort
Mathematical Institute
Pincetonplein 5
NL - 3584 CC Utrecht
The Netherlands
email: f.oort@uu.nl