Theta null points of canonical lifts I *

Robert Carls

School of Mathematics and Statistics
University of Sydney
NSW 2006 Australia

tel: +61293515775
fax: +61293514534
email: carls@maths.usyd.edu.au

May 16, 2005

Abstract

In this article we prove the existence of a canonical theta structure for the canonical lift of a given ordinary abelian variety.

1 Introduction

The aim of this article is to provide a theoretical basis for the study of the theta null points of canonical lifts. We prove that there exists a *canonical theta structure* for the canonical lift of an ordinary abelian variety. The canonical theta null point of a canonical lift which is defined in terms of the canonical theta structure forms an arithmetic invariant. In later work [3] we compute equations satisfied by the canonical theta null point of a canonical lift over a 2-adic ring. The resulting equations are related to the formulas that Jean-François Mestre proposed as a generalisation of Gauss' *Arithmetic Geometric Mean* (AGM). For generalised AGM formulas see [9] and [10, §1.3]. Our formulas, like the ones of Mestre, may be used in a point counting algorithm which computes the zeta function of an ordinary abelian variety over a finite field of characteristic 2. For an exposition of Mestre's AGM based point counting algorithm see [15, Ch. 4] and [6]. Another potential application of our formulas is the computation of equations generating class fields of CM fields. We calculate some examples in [3, App. A].

*This work was partially supported by the Australian Research Council grant DP0453134 and by the Spinoza grant of H.W. Lenstra.

Our work is meant to complement Mestre's results and to broaden the understanding of his point counting algorithm. The proof of the existence of the canonical theta structure is an important step in a research program having as goal a generalisation of Mestre's AGM algorithm to arbitrary residue field characteristic.

The main result, Theorem 2.1, was proven during the last two years of the author's postgraduate studies at the universities of Leiden and Groningen. It is an extension of the corresponding result contained in the author's PhD thesis [2, Th. 4.1.1] to the case of residue field characteristic 2.

2 The canonical theta structure

Let R be a complete noetherian local ring with residue field k of characteristic $p > 0$ and let A be an abelian scheme over R of relative dimension g having ordinary reduction. Let $\mathcal{L}$ be an ample line bundle on A. Let $j \geq 1$ and $q = p^j$. It is known that there exists an isogeny of abelian schemes $F : A \to A^{(q)}$ which is uniquely determined up to unique isomorphism by the condition that it lifts the relative q-Frobenius on the special fibre (compare [2, Prop. 2.2.1]). In Section 6.1 we prove the existence of an ample line bundle $\mathcal{L}^{(q)}$ on $A^{(q)}$ satisfying $F^*\mathcal{L}^{(q)} \cong \mathcal{L}^{\otimes q}$ which is uniquely determined up to isomorphism by the condition that $\mathcal{L}^{(q)}$ restricted to the special fibre is the q-Frobenius twist of $\mathcal{L}$. For a precise statement see Theorem 5.1. Assume that we are given an isomorphism

$$(\mathbb{Z}/q\mathbb{Z})^g_R \xrightarrow{\sim} A[q]^{\mathrm{et}} \tag{1}$$

where $A[q]^{\mathrm{et}}$ denotes the maximal étale quotient of $A[q]$.

Theorem 2.1 *Let $\mathcal{L}$ be an ample symmetric line bundle of degree 1 on A. There exists a canonical theta structure of type $(\mathbb{Z}/q\mathbb{Z})^g_R$ for the pair*

$$\left(A^{(q^\delta)}, \left(\mathcal{L}^{(q^\delta)}\right)^{\otimes q}\right) \quad \textit{where} \quad \delta = \begin{cases} 2, & p = 2 \\ 1, & p > 2 \end{cases}$$

depending on the isomorphism (1) .

Theorem 2.1 will be proven in Section 6.3. For the definition of a theta structure we refer to Section 4.3. For the following statement we assume that k is perfect and R admits an automorphism lifting the p-th power Frobenius automorphism of k.

Corollary 2.2 *Let A be a canonical lift and let $\mathcal{L}$ be an ample symmetric line bundle of degree 1 on A. There exists a canonical theta structure of type $(\mathbb{Z}/q\mathbb{Z})^g_R$ for the pair $\left(A, \mathcal{L}^{\otimes q}\right)$ depending on the isomorphism* (1).

Corollary 2.2 will be proven in Section 6.4. The above corollary is expected to hold without the assumption that R admits a lift of the p-th power Frobenius automorphism of k. For a discussion of canonical lifting see [7], [8], [11, Ch. III] and [2, Ch. 2].

3 Notation

Let R be a ring, X an R-scheme and S an R-algebra. By X_S we denote the base extended scheme $X \times_{\mathrm{Spec}(R)} \mathrm{Spec}(S)$. Let $\mathcal{M}$ be a sheaf on X. Then we denote by $\mathcal{M}_S$ the sheaf that one gets by pulling back via the projection $X_S \to X$. Let $I : X \to Y$ be a morphism of R-schemes. Then I_S denotes the morphism that is induced by I via base extension with S. We use the same symbol for a scheme and the fppf-sheaf represented by it. By a *group* we mean a group object in the category of fppf-sheaves. If a representing object has the property of being finite (flat, étale, connected, etc.) then we simply say that it is a finite (flat, étale, connected, etc.) group. Similarly we will say that a morphism of groups is finite (faithfully flat, smooth, etc.) if the groups are representable and the induced morphism of schemes has the corresponding property.

A group (morphism of groups) is called finite locally free if it is finite flat and of finite presentation. The Cartier dual of a finite locally free commutative group G will be denoted by G^D. The multiplication by an integer $n \in \mathbb{Z}$ on G will be denoted by $[n]$. A finite locally free and surjective morphism between groups is called an *isogeny*. By an *elliptic curve* we mean an abelian scheme of relative dimension 1. We use the notion of a *torsor* in the sense of [4, Ch. III, §4, Def. 1.3]. We only consider torsors for the fppf-topology.

4 Theta groups and theta structures

In the following sections we recall some well-known facts about theta groups and theta structures. We refer to [13], [14, Ch. IV, §23], [16, Ch. 8] and [12, Ch. V] for further details. Let R be a ring and G a group over R.

Definition 4.1 *Assume that there exists a central exact sequence of groups*

$$0 \to \mathbb{G}_{m,R} \to G \to H \to 0,$$

where H is a commutative finite locally free group whose rank is the square of an integer. Then the group G is called a theta group *over H.*

By the term *central exact sequence* we mean that $\mathbb{G}_{m,R}$ is mapped into the centre of G. Now let G be a theta group over H. By definition G is a $\mathbb{G}_{m,R}$-torsor over H. It follows by descent that the group G is representable by an affine faithfully flat group scheme of finite presentation over H (see [4, Ch. III, §4, Prop. 1.9]). Let S be an R-algebra. One defines the *commutator pairing* $\mathrm{e} : H \times_R H \to \mathbb{G}_{m,R}$ by lifting x and y in $H(S)$ to $\tilde{x}$ and $\tilde{y}$ in $G(S')$, where $S \to S'$ is a suitable fppf-extension, and by setting

$$\mathrm{e}(x,y) = \tilde{x}\tilde{y}\tilde{x}^{-1}\tilde{y}^{-1}.$$

Because H is abelian we have $\mathrm{e}(x,y) \in \mathbb{G}_{m,R}(S')$. Since $\mathrm{e}(x,y)$ does not depend on the choice of $\tilde{x}$ and $\tilde{y}$ it follows by descent that $\mathrm{e}(x,y) \in \mathbb{G}_{m,R}(S)$.

4.1 The theta group of an ample line bundle

Let A be an abelian scheme over a ring R and $\mathcal{L}$ a line bundle on A. Consider the morphism

$$\varphi_{\mathcal{L}} : A \to \mathrm{Pic}^0_{A/R}, \;\; x \mapsto \langle T_x^*\mathcal{L} \otimes \mathcal{L}^{-1} \rangle$$

where $\langle \cdot \rangle$ denotes the class in $\mathrm{Pic}^0_{A/R}$. We set $\check{A} = \mathrm{Pic}^0_{A/R}$. Note that $\check{A}$ is the dual of A in the category of abelian schemes. It is well-known that the relative Picard functor of A is representable by an algebraic space (compare [1, Ch. 8, Th. 1]). The representability of $\mathrm{Pic}^0_{A/R}$ by a scheme follows from a theorem of M. Raynaud which states that the categories of abelian algebraic spaces and abelian schemes coincide (see [5, Ch. I, Th. 1.9]). We denote the kernel of the morphism $\varphi_{\mathcal{L}}$ by $H(\mathcal{L})$. A line bundle $\mathcal{L}$ on A satisfies $H(\mathcal{L}) = A$ if and only if its class is in $\mathrm{Pic}^0_{A/R}(R)$. Also it is well-known that if $\mathcal{L}$ is relatively ample then $\varphi_{\mathcal{L}}$ is an isogeny. In the latter case we say that $\mathcal{L}$ has degree d if $\varphi_{\mathcal{L}}$ is fibre-wise of degree d. Let S be an R-algebra. We define

$$G(\mathcal{L})(S) = \left\{ \;\; (x, \varphi) \;\; | \;\; x \in H(\mathcal{L})(S), \;\; \varphi : \mathcal{L}_S \xrightarrow{\sim} T_x^*\mathcal{L}_S \;\; \right\}.$$

The functor $G(\mathcal{L})$ has the structure of a group given by the group law

$$\big((y, \psi), (x, \varphi)\big) \mapsto (x + y, T_x^*\psi \circ \varphi).$$

There are natural morphisms

$$G(\mathcal{L}) \to H(\mathcal{L}), \;\; (x, \varphi) \mapsto x \quad \text{and} \quad \mathbb{G}_{m,R} \to G(\mathcal{L}), \;\; \alpha \mapsto (0_A, \tau_\alpha)$$

where 0_A denotes the zero section of A and τ_α denotes the automorphism of $\mathcal{L}$ given by the multiplication with α. The induced sequence of groups

$$0 \to \mathbb{G}_{m,R} \to G(\mathcal{L}) \xrightarrow{\pi} H(\mathcal{L}) \to 0 \tag{2}$$

is central and exact. Now let $\mathcal{L}$ be relatively ample of degree d. Then $H(\mathcal{L})$ is finite locally free of order d^2 and hence $G(\mathcal{L})$ is a theta group. The commutator pairing on $H(\mathcal{L})$ as defined above will be denoted by $\mathrm{e}_{\mathcal{L}}$. One can show that the pairing $\mathrm{e}_{\mathcal{L}}$ is perfect. The perfectness is equivalent to the fact that the centre of $G(\mathcal{L})$ equals $\mathbb{G}_{m,R}$.

4.2 Descent of line bundles along isogenies

Let R be a ring. Let $I : A \to B$ be an isogeny of abelian schemes over R and K its kernel. Assume we are given a relatively ample line bundle $\mathcal{L}$ on A and $K \subseteq H(\mathcal{L})$. Define G' by the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{G}_{m,R} & \longrightarrow & G(\mathcal{L}) & \longrightarrow & H(\mathcal{L}) & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle \mathrm{id}} & & \uparrow & & \uparrow{\scriptstyle i} & & \\ 0 & \longrightarrow & \mathbb{G}_{m,R} & \longrightarrow & G' & \xrightarrow{\pi} & K & \longrightarrow & 0, \end{array} \tag{3}$$

where the second row is the pull back of the first via the inclusion $K \overset{i}{\hookrightarrow} H(\mathcal{L})$, i.e. the right hand square is Cartesian. Let U be an R-algebra and $\mathcal{M}$ a line bundle on B_U. Suppose we are given an isomorphism $\alpha : I_U^*\mathcal{M} \overset{\sim}{\to} \mathcal{L}_U$. We define a morphism $s_\alpha : K_U \to G'_U$ by mapping $x \in K(W)$, where W is a U-algebra, to $\big(x, T_x^*\alpha_W \circ \alpha_W^{-1}\big)$. This is well-defined because $T_x^* I_W^* \mathcal{M}_W = I_W^* \mathcal{M}_W$. It is clear that $\pi_U \circ s_\alpha = \mathrm{id}$ where π is as in diagram (3). We define

$$S_K(U) = \{\ s : K_U \to G'_U \ \mid\ \pi_U \circ s = \mathrm{id}\ \}$$

and denote by $D_{\mathcal{L}}(U)$ the set of isomorphism classes of line bundles $\mathcal{M}$ on B_U such that $I_U^*\mathcal{M} \cong \mathcal{L}_U$. The following classical result about the descent of line bundles was proven by Alexander Grothendieck.

Proposition 4.2 *The functorial map*

$$S_K(U) \to D_{\mathcal{L}}(U),\ \ (\mathcal{M}, \alpha) \mapsto s_\alpha$$

establishes an isomorphism of functors $S_K \overset{\sim}{\to} D_{\mathcal{L}}$.

Compare [14, Ch. IV, §23, Th. 2] or [1, Ch. 6.1, Th. 4].

4.3 Theta structures

In the following we define the standard theta group of a given type. Let K be a commutative finite locally free group of square order over a base ring R. We set $H(K) = K \times_R K^D$ and define a group law on $G(K) = \mathbb{G}_{m,R} \times_R H(K)$ by setting

$$(\alpha_1, x_1, l_1) * (\alpha_2, x_2, l_2) = (\alpha_1 \cdot \alpha_2 \cdot l_2(x_1), x_1 + x_2, l_1 \cdot l_2).$$

We have an exact sequence of groups

$$0 \to \mathbb{G}_{m,R} \to G(K) \to H(K) \to 0$$

where the left hand map is given by $\alpha \mapsto (\alpha, 0, 1)$ and the right hand map is the projection on $H(K)$. The centre of $G(K)$ is given by $\mathbb{G}_{m,R}$. We conclude that $G(K)$ is a theta group. We denote the corresponding commutator pairing by e_K. Using the definition of the multiplication in $G(K)$ one computes

$$\mathrm{e}_K\big((x_1, l_1), (x_2, l_2)\big) = \frac{l_2(x_1)}{l_1(x_2)}. \tag{4}$$

We remark that e_K is a perfect pairing. Now assume we are given an abelian scheme A over R and a relatively ample line bundle $\mathcal{L}$ on A.

Definition 4.3 *A* theta structure *of type K for the pair $(A, \mathcal{L})$ is an isomorphism $\Theta : G(K) \overset{\sim}{\to} G(\mathcal{L})$ making the diagram*

$$\begin{array}{ccc} \mathbb{G}_{m,S} & \longrightarrow & G(\mathcal{L}) \\ \uparrow{\scriptstyle \mathrm{id}} & & \uparrow{\scriptstyle \Theta} \\ \mathbb{G}_{m,S} & \longrightarrow & G(K) \end{array}$$

commutative. Here the horizontal arrows are the natural inclusions.

Next we want to give another characterisation of a theta structure.

Definition 4.4 *A* Lagrangian decomposition *for $H(\mathcal{L})$ of type K is an isomorphism*

$$\delta : H(K) \xrightarrow{\sim} H(\mathcal{L}),$$

which is compatible with the commutator pairings $\mathrm{e}_{\mathcal{L}}$ and e_K.

Let δ be a Lagrangian decomposition for $H(\mathcal{L})$ of type K. We can consider K and K^D as subgroups of $H(\mathcal{L})$ via δ. Assume we are given a pair (u, v) where u and v are sections of the pull back of the extension

$$0 \to \mathbb{G}_{m,R} \to G(\mathcal{L}) \xrightarrow{\pi} H(\mathcal{L}) \to 0 \tag{5}$$

along the inclusions $K \hookrightarrow H(\mathcal{L})$ and $K^D \hookrightarrow H(\mathcal{L})$, respectively. We define a morphism $\Theta_{u,v} : G(K) \to G(\mathcal{L})$ by $\Theta_{u,v}(\alpha, x, l) = \alpha \cdot v(l) \cdot u(x)$.

Proposition 4.5 *The map*

$$(\delta, u, v) \mapsto \Theta_{u,v} \tag{6}$$

gives a bijection between the set of triples as above and the set of theta structures for $(A, \mathcal{L})$ of type K.

Proof. First we have to show that the map (6) is well-defined. We claim that $\Theta_{u,v}$ is a theta structure of type K for $(A, \mathcal{L})$. We have

$$\Theta_{u,v}\big((\alpha_1, x_1, l_1) * (\alpha_2, x_2, l_2)\big) = \alpha_1 \cdot \alpha_2 \cdot l_2(x_1) \cdot v(l_1) \cdot v(l_2) \cdot u(x_1) \cdot u(x_2).$$

By the definition of the pairing $\mathrm{e}_{\mathcal{L}}$ it follows that

$$v(l_2) \cdot u(x_1) = \mathrm{e}_{\mathcal{L}}\big(\delta(l_2), \delta(x_1)\big) \cdot u(x_1) \cdot v(l_2).$$

Since δ is a Lagrangian decomposition we have

$$\mathrm{e}_{\mathcal{L}}\big(\delta(0, l_2), \delta(x_1, 1)\big) = \mathrm{e}_K\big((0, l_2), (x_1, 1)\big) = \frac{1}{l_2(x_1)}.$$

The right hand equality follows by (4). This proves that $\Theta_{u,v}$ is a morphism of groups. Clearly $\Theta_{u,v}$ is $\mathbb{G}_{m,R}$-equivariant.

Next we prove that $\Theta_{u,v}$ is an isomorphism by giving an inverse. Let g be a point of $G(\mathcal{L})$. Then we have $\pi(g) = \delta(x_g, l_g)$ for uniquely determined $x_g \in K$ and $l_g \in K^D$. Here π denotes the projection map of the extension (5). Now g and $\Theta_{u,v}(1, x_g, l_g)$ both lift $\delta(x_g, l_g)$. Hence they differ by a unique scalar α_g, i.e. $g = \Theta_{u,v}(\alpha_g, x_g, l_g)$. An inverse of $\Theta_{u,v}$ is given by the morphism $g \mapsto (\alpha_g, x_g, l_g)$.

In order to complete the proof of Proposition 4.5 it is sufficient to give an inverse of the map (6). Assume we are given a theta structure Θ of type K for the pair $(A, \mathcal{L})$. The isomorphism Θ induces an isomorphism $\delta_\Theta : H(K) \xrightarrow{\sim} H(\mathcal{L})$. By the definition of the commutator pairing it follows that the isomorphism δ_Θ

is a Lagrangian decomposition. There are two natural sections of the natural projection $G(\mathcal{L}) \to H(\mathcal{L})$ over K and K^D given by

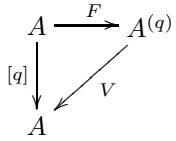
$$u_\Theta : (x,1) \mapsto \Theta\big(1,x,1\big) \quad \text{and} \quad v_\Theta : (0,l) \mapsto \Theta\big(1,0,l\big),$$

respectively. Here we consider K and K^D as subgroups of $H(\mathcal{L})$ via δ_Θ. An inverse of (6) is given by $\Theta \mapsto \big(\delta_\Theta, u_\Theta, v_\Theta\big)$. This finishes the proof of the proposition. □

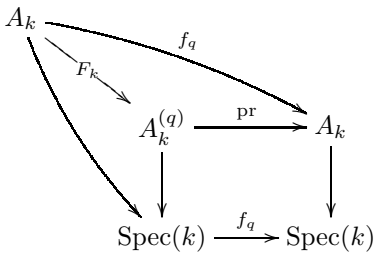
5 Descent along lifts of relative Frobenius and Verschiebung

In the following we recall some facts about the existence of Frobenius lifts and the descent of line bundles along lifts of Frobenius and Verschiebung. Theorem 5.1 and 5.2 are known to the experts but they are not yet available in the literature. We prove them in Section 6.1 and 6.2.

Let R be a complete noetherian local ring with residue class field k of characteristic $p > 0$ and A an abelian scheme having ordinary reduction. Let $j \geq 1$ and $q = p^j$. It is known that there exists an abelian scheme $A^{(q)}$ over R and a commutative diagram of isogenies



such that F_k equals the relative q-Frobenius (compare [2, Prop. 2.2.1]). The latter condition determines F uniquely. The kernel of F is given by $A[q]^{\mathrm{loc}}$ which is defined to be the connected component of $A[q]$. The condition that F_k equals the relative q-Frobenius means that there exists a commutative diagram



where f_q denotes the absolute q-Frobenius, the vertical maps are the structure maps and the square is Cartesian. Let $\mathcal{L}$ be a line bundle on A. We have a natural isomorphism

$$F_k^* \mathrm{pr}^* \mathcal{L}_k = f_q^* \mathcal{L}_k \xrightarrow{\sim} \mathcal{L}_k^{\otimes q} \tag{7}$$

given by $l \otimes 1 \mapsto l^{\otimes q}$.

Theorem 5.1 *Assume that $\mathcal{L}$ is an ample line bundle on R. There exists a line bundle $\mathcal{L}^{(q)}$ on $A^{(q)}$ determined uniquely up to isomorphism by the following two conditions:*

$$\left(\mathcal{L}^{(q)}\right)_k \cong \mathrm{pr}^*\mathcal{L}_k \quad \textit{and} \quad F^*\mathcal{L}^{(q)} \cong \mathcal{L}^{\otimes q}.$$

Moreover, the line bundle $\mathcal{L}^{(q)}$ is ample and has the same degree as $\mathcal{L}$.

A proof of Theorem 5.1 is presented in Section 6.1.

Theorem 5.2 *Assume that $\mathcal{L}$ is an ample symmetric line bundle on A.*

1. *Let $p > 2$. There exists an isomorphism*

$$V^*\mathcal{L} \xrightarrow{\sim} \left(\mathcal{L}^{(q)}\right)^{\otimes q}. \tag{8}$$

2. *Let $p = 2$. Assume we are given an isomorphism*

$$A[2] \xrightarrow{\sim} A[2]^{\mathrm{loc}} \times A[2]^{\mathrm{et}}. \tag{9}$$

There exists a line bundle $\mathcal{L}_0$ on A with $\langle\mathcal{L}_0\rangle \in \mathrm{Pic}^0_{A/R}[2](R)$ such that

$$V^*\left(\mathcal{L} \otimes \mathcal{L}_0\right) \xrightarrow{\sim} \left(\mathcal{L}^{(q)}\right)^{\otimes q}.$$

The class of $\mathcal{L}_0$ depends on the isomorphism (9) .

A proof of Theorem 5.2 will be given in Section 6.2. The isomorphism (8) does not always exist in the case $p = 2$. This is illustrated by the following example.

Example: We assume k to be an algebraically closed field of characteristic 2. Let E be an ordinary elliptic curve over k and Q_2 the unique non-zero point in $E^{(2)}[2](k)$. Note that Q_2 is a generator of the kernel of the Verschiebung $V : E^{(2)} \to E$. We have

$$V^*(0_E) = (0_{E^{(2)}}) + (Q_2) \not\sim 2 \cdot (0_{E^{(2)}})$$

where 0_E and $0_{E^{(2)}}$ denote the zero sections of E and $E^{(2)}$ and $\sim$ stands for linear equivalence of Weil divisors. Let Q be the unique non-zero point in $E[2](k)$ and $R \in E^{(2)}[4](k)$ such that $2R = Q_2$. We have

$$V^*(Q) = (R) + (R + Q_2) \sim 2(0_{E^{(2)}}).$$

6 The proofs

In the following we prove the results of Section 2 and Section 5.

6.1 Proof of Theorem 5.1

In the following we prove Theorem 5.1. We use the notation of Section 5. Let A be an abelian scheme over R having ordinary reduction and let $\mathcal{L}$ be an ample line bundle on A. Let $K = A[q]^{\mathrm{loc}}$ and let G' be defined by the Cartesian diagram

$$\begin{array}{ccc} G(\mathcal{L}^{\otimes q}) & \longrightarrow & H(\mathcal{L}^{\otimes q}) \\ \uparrow & & \uparrow \\ G' & \longrightarrow & K. \end{array}$$

Remark 6.1 *The group G' is commutative.*

Proof. The commutativity of G' is equivalent to the condition that the commutator pairing $\mathrm{e}_{\mathcal{L}^{\otimes q}} : H(\mathcal{L}^{\otimes q}) \times H(\mathcal{L}^{\otimes q}) \to \mathbb{G}_m$ is trivial on K. Let T be an R-algebra and $x \in K(T)$. Then the map $e_{\mathcal{L}^{\otimes q}}(x, \cdot) : K_T \to \mathbb{G}_{m,T}$ is a T-valued point of $K^D \cong \check{A}[q]^{\mathrm{et}}$ where $\check{A}$ denotes the dual abelian scheme. The morphism $K \to \check{A}[q]^{\mathrm{et}}$ given by $x \mapsto e_{\mathcal{L}^{\otimes q}}(x, \cdot)$ is equal to the zero morphism since the image of K is connected and hence equals the image of the unit section in $\check{A}[q]^{\mathrm{et}}$ which forms a connected component. □

The main ingredient in the proof of Theorem 5.1 is the following result.

Lemma 6.2 *The functor S_K (defined in Section 4.2) is a K^D-torsor over R.*

Proof. Let U be an R-algebra. The group $K^D(U) = \underline{\mathrm{Hom}}(K, \mathbb{G}_m)(U)$ acts on $S_K(U)$ by translation. This action is transitive and faithful whenever $S_K(U)$ is non-empty. Consider the extension

$$0 \to \mathbb{G}_{m,R} \to G' \to K \to 0. \tag{10}$$

It remains to show that (10) has a section over an fppf-extension of R. Taking q-torsion we get an exact sequence

$$0 \to \mu_{q,R} \to G'[q] \to K \to 0. \tag{11}$$

The exactness of (11) follows from the Snake Lemma and the exactness of the Kummer sequence. By Remark 6.1 the group $G'[q]$ is commutative. Note that $G'[q]$ is a $\mu_{q.R}$-torsor over K. It follows by [4, Ch. III, §4, Prop. 1.9] that the group $G'[q]$ is finite locally free. Applying Cartier duality to (11) we get an exact sequence

$$0 \to K^D \to G'[q]^D \xrightarrow{\pi} \mathbb{Z}/q\mathbb{Z} \to 0. \tag{12}$$

We remark that (11) is split if and only if (12) is split. We can lift a generator of $\mathbb{Z}/q\mathbb{Z}$ to an element $x \in G'[q]^D(R')$ where $R \to R'$ is a suitable fppf-extension. Clearly x has order q. This gives a splitting of (12) over R'. As a consequence the extensions (10)–(11) are split over R'. □

Corollary 6.3 *The functor S_K is representable by a finite étale scheme.*

Proof. The representability by a finite locally free R-scheme follows from Lemma 6.2 and [4, Ch. III, §4, Prop. 1.9]. Since A has ordinary reduction, we have $K^D = \underline{\mathrm{Hom}}_R(K, \mathbb{G}_m) \cong \check{A}[q]^{\mathrm{et}}$ where $\check{A}$ denotes the dual of A. It follows by descent that S_K is étale. □

Now we can complete the proof of Theorem 5.1. We have already seen that there exists a canonical k-rational point of S_K given by the isomorphism (7). By Corollary 6.3 and the theory of finite étale schemes over Henselian local rings there exists a unique R-rational point of S_K reducing to the above k-rational point. The first part of the claim of Theorem 5.1 now follows from Proposition 4.2. The second part of the claim states that the line bundle $\mathcal{L}^{(q)}$ is ample and of the same degree as $\mathcal{L}$. It suffices to verify the claim on the special fibre. It is obvious from the construction that $\mathcal{L}_k^{(q)}$ is ample and has the same degree as $\mathcal{L}_k$. This finishes the proof of Theorem 5.1.

6.2 Proof of Theorem 5.2

We use the notation of Section 5. We set

$$\mathcal{L}' = \left(V^*\mathcal{L}\right)^{-1} \otimes \left(\mathcal{L}^{(q)}\right)^{\otimes q}.$$

We have $\langle \mathcal{L}' \rangle \in \mathrm{Pic}^0_{A^{(q)}/R}(R)$. In order to prove the proposition we have to show that $\mathcal{L}'$ is trivial. By the symmetry of $\mathcal{L}$ we conclude that

$$F^*(V^*\mathcal{L}) \cong [q]^*\mathcal{L} \cong \mathcal{L}^{\otimes q^2}.$$

Together with Theorem 5.1 this implies that $F^*\mathcal{L}'$ is trivial on A. This means that $\langle \mathcal{L}' \rangle$ is in the kernel of the dual $\check{F} = \mathrm{Pic}^0(F)$ of F. The group $\mathrm{Ker}(\check{F})$ is the Cartier dual of $\mathrm{Ker}(F)$ and hence is annihilated by the isogeny $[q]$. As a consequence $\langle \mathcal{L}' \rangle$ has order dividing q. Since we have assumed $\mathcal{L}$ to be symmetric it follows that $\mathcal{L}^{(q)}$ and $\mathcal{L}'$ are symmetric. We conclude that

$$\langle \mathcal{L}' \rangle \in \mathrm{Pic}^0_{A^{(q)}/R}[2](R).$$

By the above discussion the element $\langle \mathcal{L}' \rangle$ has order dividing the greatest common divisor of q and 2. If $p > 2$ we conclude that $\mathcal{L}'$ is trivial and Theorem 5.2 is proven.

Assume now that $p = 2$. We claim that there exists a line bundle $\mathcal{L}_0$ on A with $\langle \mathcal{L}_0 \rangle \in \mathrm{Pic}^0_{A/R}[2](R)$ such that $V^*\mathcal{L}_0 \cong \mathcal{L}'$. We set $\check{A} = \mathrm{Pic}^0_{A/R}$ and $\check{V} = \mathrm{Pic}^0(V)$. Then $\left(\check{A}\right)^{(q)} = \mathrm{Pic}^0_{A^{(q)}/R}$. The isogeny $\check{V} : \check{A} \to \check{A}^{(q)}$ induces a morphism of connected-étale sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \check{A}[2]^{\mathrm{loc}} & \longrightarrow & \check{A}[2] & \xrightarrow{\pi} & \check{A}[2]^{\mathrm{et}} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \check{V}[2]^{\mathrm{loc}}} & & \downarrow{\scriptstyle \check{V}[2]} & & \downarrow{\scriptstyle \check{V}[2]^{\mathrm{et}}} & & \\ 0 & \longrightarrow & \check{A}^{(q)}[2]^{\mathrm{loc}} & \longrightarrow & \check{A}^{(q)}[2] & \xrightarrow{\pi^{(q)}} & \check{A}^{(q)}[2]^{\mathrm{et}} & \longrightarrow & 0. \end{array} \tag{13}$$

Note that one cannot embed a non-zero finite étale R-group into a connected one. It follows by the Snake Lemma that $\check{V}[2]^{\mathrm{et}}$ is a monomorphism. Comparing ranks we conclude that $\check{V}[2]^{\mathrm{et}}$ is an isomorphism. By the cokernel property of the morphism $\check{V}[2]^{\mathrm{et}} \circ \pi$ there exists a section $s : \check{A}^{(q)}[2]^{\mathrm{et}} \to \check{A}^{(q)}[2]$ of the projection $\pi^{(q)}$. The image of $\check{A}^{(q)}[2]^{\mathrm{et}}$ under $\pi^{(q)}$ coincides with the kernel of $\check{F}$. Recall that the latter contains $\langle \mathcal{L}' \rangle$. As a consequence there exists an $x \in \check{A}^{(q)}[2]^{\mathrm{et}}$ such that $s(x)$ equals $\langle \mathcal{L}' \rangle$. Using the isomorphism (9) we map the point $(\check{V}[2]^{\mathrm{et}})^{-1}(x)$ to an element of $\check{A}[2]$ whose image under $\check{V}[2]$ equals $\langle \mathcal{L}' \rangle$. This proves our claim and completes the proof of the theorem.

6.3 Proof of Theorem 2.1

We use the notation of Section 2. Let A be an abelian scheme of relative dimension g over R having ordinary reduction and $\mathcal{L}$ an ample line bundle of degree 1 on A. Let $K = (\mathbb{Z}/q\mathbb{Z})^g_R$. Assume we are given an isomorphism

$$K \xrightarrow{\sim} A[q]^{\mathrm{et}}. \tag{14}$$

The isogeny $F : A \to A^{(q)}$ induces a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A[q]^{\mathrm{loc}} & \longrightarrow & A[q] & \longrightarrow & A[q]^{\mathrm{et}} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle F[q]^{\mathrm{loc}}} & & \downarrow{\scriptstyle F[q]} & & \downarrow{\scriptstyle F[q]^{\mathrm{et}}} & & \\ 0 & \longrightarrow & A^{(q)}[q]^{\mathrm{loc}} & \longrightarrow & A^{(q)}[q] & \longrightarrow & A^{(q)}[q]^{\mathrm{et}} & \longrightarrow & 0. \end{array} \tag{15}$$

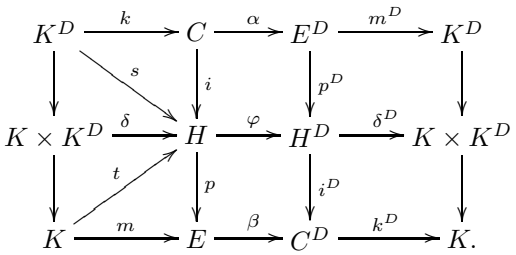
The induced morphism $F[q]^{\mathrm{et}}$ is an isomorphism. Composing the isomorphism (14) with $F[q]^{\mathrm{et}}$ we get an isomorphism $m : K \xrightarrow{\sim} A^{(q)}[q]^{\mathrm{et}}$. The isomorphism $F[q]^{\mathrm{et}}$ induces a unique section $r : A^{(q)}[q]^{\mathrm{et}} \to A^{(q)}[q]$ of the natural projection $A^{(q)}[q] \to A^{(q)}[q]^{\mathrm{et}}$. We define $t = r \circ m$ and set $H = A^{(q)}[q]$, $C = A^{(q)}[q]^{\mathrm{loc}}$ and $E = A^{(q)}[q]^{\mathrm{et}}$. Let $\mathrm{e}(\cdot,\cdot)$ denote the commutator pairing on

$$H = H\left(\left(\mathcal{L}^{(q)}\right)^{\otimes q}\right).$$

Since e is a perfect pairing it induces an isomorphism $\varphi : H \xrightarrow{\sim} H^D$, $x \mapsto \mathrm{e}(x,\cdot)$. Note that C is mapped to the connected component of H^D. As a matter of fact the connected component of H^D is given by E^D. Hence the isomorphism φ induces isomorphisms $\alpha : C \xrightarrow{\sim} E^D$ and $\beta : E \xrightarrow{\sim} C^D$ on the local and étale part of H. We define $k = -(\alpha^{-1} \circ m^{-D}) : K^D \xrightarrow{\sim} C$ and set $s = i \circ k$.

Lemma 6.4 *The morphism $\delta = s \oplus t$ is a Lagrangian decomposition of type K for H.*

Proof. Consider the commutative diagram



By definition we have $m^D \circ \alpha \circ k = -\mathrm{id}$. Since the pairing e is alternating it follows that $\varphi^D = -\varphi$. As a consequence we have $\beta^D = -\alpha$. Hence

$$k^D \circ \beta \circ m = \big(m^D \circ (-\alpha) \circ k\big)^D = \mathrm{id}.$$

The commutator pairing e_K on $K \times K^D$ gives an isomorphism

$$\tau : K \times K^D \to K \times K^D, \;\; z \mapsto \mathrm{e}_K\big(z, \cdot\big).$$

One computes $\tau\big((x,l)\big) = (x, l^{-1})$. We conclude that $\tau = \delta^D \circ \varphi \circ \delta$ which proves that δ is compatible with the natural commutator pairings on H and $K \times K^D$. □

Now the images of K and K^D under δ equal the kernels of the lifts of the Verschiebung $V : A^{(q)} \to A$ and the relative q-Frobenius $F : A^{(q)} \to A^{(q^2)}$, respectively.

First assume that $p > 2$. Combining Theorem 5.1, Theorem 5.2 and Proposition 4.2 we get sections

$$u : K \to G\left(\big(\mathcal{L}^{(q)}\big)^{\otimes q}\right) \quad \text{and} \quad v : K^D \to G\left(\big(\mathcal{L}^{(q)}\big)^{\otimes q}\right)$$

of the natural projection $G\left(\big(\mathcal{L}^{(q)}\big)^{\otimes q}\right) \to H$. Here K and K^D are considered as subgroups of H via the level structure δ constructed above. By Proposition 4.5 the triple (δ, u, v) gives a theta structure of type K for the pair $\left(A, \big(\mathcal{L}^{(q)}\big)^{\otimes q}\right)$.

The above proof applies to the case $p = 2$ with some minor change. Assume that $p = 2$. We claim that there exists a canonical theta structure of type $(\mathbb{Z}/q\mathbb{Z})^g_R$ for the pair

$$\left(A^{(2q)}, \big(\mathcal{L}^{(2q)}\big)^{\otimes q}\right).$$

We can argue as above replacing A by $A^{(2)}$. Theorem 5.2.2 requires the choice of an isomorphism

$$A^{(2)}[2] \xrightarrow{\sim} A^{(2)}[2]^{\mathrm{loc}} \times A^{(2)}[2]^{\mathrm{et}}.$$

We claim that there is a canonical choice. It is induced by the restriction of the isomorphism $F[q]^{\mathrm{et}}$ as above to $A[2]$. This finishes the proof of Theorem 2.1.

6.4 Proof of Corollary 2.2

We use the notation of Section 2. Our proof can easily be adapted to the general case. Assume that k is perfect and A is the canonical lift of A_k. Let σ denote an automorphism of R lifting the (δq)-th power automorphism of k where δ is as in Theorem 2.1. We denote by $A^{(\sigma)}$ the pull back of A by the automorphism σ^{-1}. On $A^{(\sigma)}$ there exists an ample symmetric line bundle $\mathcal{L}^{(\sigma)}$ of degree 1 which is defined to be the pull back of $\mathcal{L}$ along the projection $A^{(\sigma)} \to A$.

We set $A' = \left(A^{(\sigma)}\right)^{(\delta q)}$. Since A' is a canonical lift of A_k it follows by uniqueness that there exists an isomorphism $\tau : A \xrightarrow{\sim} A'$. We set

$$\mathcal{M} = \tau^* \left(\left(\mathcal{L}^{(\sigma)}\right)^{(\delta q)} \right).$$

We claim that $\mathcal{M}^{\otimes q} \cong \mathcal{L}^{\otimes q}$. We set $\mathcal{L}' = \mathcal{L} \otimes \mathcal{M}^{-1}$. Our claim follows from the fact that $\mathcal{M}$ and $\mathcal{L}$ are symmetric and hence

$$\langle \mathcal{L}' \rangle \in \mathrm{Pic}^0_{A/R}[2](R).$$

By Theorem 2.1 the line bundle $\mathcal{M}^{\otimes q}$ has a canonical theta structure of type $(\mathbb{Z}/q\mathbb{Z})^g_R$. The latter gives a canonical theta structure for $\mathcal{L}^{\otimes q}$. This completes the proof of the corollary.

Acknowledgements

I owe thanks to Bas Edixhoven for assisting me with the proof of Theorem 2.1. Without him this article probably would not exist. I'm indebted to Ben Moonen and Michel Raynaud who independently from each other communicated to me the proof of Theorem 5.2.1 that we present in Section 6.2. Their proof supersedes the author's original proof based on an idea which was the outcome of a discussion with Frans Oort.

References

[1] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models.* Number 21 in Ergebnisse der Mathemathik, 3. Folge. Springer-Verlag, 1990.

[2] Robert Carls. *A generalized Arithmetic Geometric Mean.* PhD thesis, University of Groningen, Netherlands, 2004.

[3] Robert Carls. Theta null points of canonical lifts II. unpublished, 2005.

[4] Michel Demazure and Pierre Gabriel. *Groupes Algébriques, Tome I.* North-Holland Publishing Company, Amsterdam, 1970.

[5] Gerd Faltings and Ching-Li Chai. *Degeneration of abelian varieties.* Number 22 in Ergebnisse der Mathematik, 3. Folge. Springer-Verlag, 1990.

[6] Reynald Lercier and David Lubicz. A quasi-quadratic time algorithm for hyperelliptic curve point counting. unpublished, available at http://www.math.u-bordeaux.fr/∼lubicz, 2003.

[7] Jonathan Lubin, Jean-Pierre Serre, and John Tate. Elliptic curves and formal groups. unpublished, available at http://www.ma.utexas.edu/users/voloch/lst.html.

[8] William Messing. *The crystals associated to Barsotti-Tate groups*. Number 264 in Lecture Notes in Mathematics. Springer-Verlag, 1972.

[9] Jean-François Mestre. Moyenne de Borchardt et intégrales elliptiques. *Comptes Rendus de Académie de Sciences Paris, Série I Mathématique*, 313(5):273–276, 1991.

[10] Jean-François Mestre. Algorithmes pour compter des points en petite caractéristique en genre 1 et 2. unpublished, rédigé par D. Lubicz, available at http://www.math.univ-rennes1.fr/crypto/2001-02/mestre.ps, 2002.

[11] Ben Moonen. *Special points and linearity properties of Shimura varieties*. PhD thesis, Universiteit Utrecht, The Netherlands, 1995.

[12] Laurent Moret-Bailly. *Pinceaux de variétés abéliennes*, volume 129 of *Astérisque*. Société Mathématiques de France, 1985.

[13] David Mumford. On the equations defining abelian varieties I. *Inventiones Mathematicae*, 1:287–354, 1966.

[14] David Mumford. *Abelian varieties*. Oxford University Press, London, 1970.

[15] Christophe Ritzenthaler. *Problèmes arithmétiques relatifs à certaines familles de courbes sur les corps finis*. PhD thesis, Université Paris 7, Denis-Diderot, France, 2003.

[16] Gerhard van der Geer and Ben Moonen. Abelian varieties. unpublished, available at http://www.science.uva.nl/∼bmoonen.