Special Subvarieties Arising from Families of Cyclic Covers of the Projective Line

Dedicated to Frans Oort on the occasion of his 75th birthday

Ben Moonen

Received: July 14, 2010
Revised: September 2, 2010

Communicated by Peter Schneider

Abstract. We consider families of cyclic covers of $\mathbb{P}^1$, where we fix the covering group and the local monodromies and we vary the branch points. We prove that there are precisely twenty such families that give rise to a special subvariety in the moduli space of abelian varieties. Our proof uses techniques in mixed characteristics due to Dwork and Ogus.

2010 Mathematics Subject Classification: 11G15, 14H40, 14G35
Keywords and Phrases: Special subvarieties, Jacobians, complex multiplication

Introduction

According to a conjecture of Coleman, if we fix a genus $g \geqslant 4$ and consider smooth projective curves C over $\mathbb{C}$ of genus g, there should be only finitely many such curves, up to isomorphism, such that $\mathrm{Jac}(C)$ is an abelian variety of CM type. This conjecture is known to be false for $g \in \{4, 5, 6, 7\}$, by virtue of the fact that for these genera there exist special subvarieties $S \subset \mathscr{A}_g$ (also known as subvarieties of Hodge type) of positive dimension that are contained in the (closed) Torelli locus and that meet the open Torelli locus.

All known examples of such special subvarieties S arise from families of cyclic covers of $\mathbb{P}^1$. As input for this we fix integers $m \geqslant 2$ and $N \geqslant 4$, together with an N-tuple $a = (a_1, \ldots, a_N)$; then we consider cyclic covers $C_t \to \mathbb{P}^1$

with covering group $\mathbb{Z}/m\mathbb{Z}$, branch points $t_1, \ldots, t_N$ in $\mathbb{P}^1$, and with local monodromy a_i about t_i. Varying the branch points we obtain an $(N-3)$-dimensional closed subvariety $Z = Z(m,N,a) \subset \mathscr{A}_g$ given by the Jacobians of the curves C_t, and for certain choices of (m,N,a) it can be shown that Z is a special subvariety.

The main purpose of this paper is to give a list of monodromy data (m,N,a) such that $Z(m,N,a)$ is special, and to prove that there are no further such examples.

By construction, the Jacobians J_t come equipped with an action of the group ring $\mathbb{Z}[\mu_m]$. This action defines a special subvariety $S(\mu_m) \subset \mathscr{A}_g$ that contains Z and whose dimension can be easily calculated in terms of the given monodromy data (m,N,a). We always have $N-3 \leqslant \dim S(\mu_m)$, and if equality holds $Z = S(\mu_m)$ is special. To search for triples (m,N,a) for which $\dim S(\mu_m) = N-3$ is something that can be done on a computer, and it is therefore surprising that this appears not to have been done until recently. Thus, while examples in genera 4 and 6 have been given by de Jong and Noot in [6]—and in fact, these examples at least go back to Shimura's paper [24]—examples with $g=5$ and $g=7$ were found only much later; see Rohde [22]. At any rate, with the help of a computer program we find twenty examples with $\dim S(\mu_m) = N-3$. The main result of this paper is that this list is complete:

Main theorem. — Consider monodromy data (m,N,a) as above. Then the closed subvariety $Z(m,N,a) \subset \mathscr{A}_{g,\mathbb{C}}$ is special if and only if (m,N,a) is equivalent to one of the twenty triples listed in Table 1.

Note that if $N-3 < \dim S(\mu_m)$, which means that the inclusion $Z \subset S(\mu_m)$ is strict, Z could a priori still be a special subvariety. The main point of our result is that even in these cases we are able to prove that Z is not special.

To get a feeling for the difficulty of the problem, consider, as an example, the family of (smooth projective) curves of genus 8 given by $y^{10} = x(x-1)(x-t)^2$, where $t \in T = \mathbb{P}^1_{\mathbb{C}} \setminus \{0,1,\infty\}$ is a parameter. The corresponding family of Jacobians $J \to T$ decomposes, up to isogeny, as a product $J^{\mathrm{old}} \times J^{\mathrm{new}}$ of two abelian fourfolds. (The old part comes from the quotient family $u^5 = x(x-1)(x-t)^2$; the new part is the family of Pryms.) Both J^{old} and J^{new} give rise to a 1-dimensional special subvariety in $\mathscr{A}_4$, and they both admit an action by $\mathbb{Z}[\zeta_5] = \mathbb{Z}[\zeta_{10}]$, with the same multiplicities on the tangent spaces at the origin. A priori it might be true that J^{old} and J^{new} are isogenous, in which case the family $J \to T$ would define a special subvariety in $\mathscr{A}_8$. Our theorem says, in this particular example, that this does not happen.

From the perspective of special points and the André-Oort conjecture, one could state the problem, in the example at hand, as follows. There are infinitely many values for t such that J^{old}_t is of CM type; likewise for J^{new}_t. Do there exist infinitely many t such that J^{old}_t and J^{new}_t are simultaneously of CM type?

Our theorem, combined with a result of Yafaev [25], implies the answer is *no*, at least if we assume the Generalized Riemann Hypothesis. See Corollary 3.7.

Our proof of the main theorem uses techniques from characteristic p and is based on a method that in some particular cases has already been used by de Jong and Noot in [6], Section 5. For a suitable choice of a prime number p, the Jacobians in our family will, at least generically, have ordinary reduction in characteristic p. Moreover, if we assume $Z(m, N, a) \subset \mathscr{A}_g$ to be special then by a result of Noot [18] we can arrange things in such a way that the canonical liftings of these ordinary reductions are again Jacobians. Already over the Witt vectors of length 2 this is a very restrictive condition that, using the results of Dwork and Ogus in [8], can be turned into something computable.
In individual cases (such as the example sketched above, or the examples treated in [6]), these techniques give a rather effective method to prove that some given family of curves does not give rise to a special subvariety in $\mathscr{A}_{g,\mathbb{C}}$. To do this for arbitrary data (m, N, a) is much harder, and some perseverance is required to deal with the combinatorics that is involved. It would be interesting to have a purely Hodge-theoretic proof of the main theorem; as it is, we do not even have a Hodge-theoretic method that works well in individual examples.

Let us give an overview the contents of the individual sections. In Section 1 we quickly review the notion of a special subvariety and we summarize some facts we need. In Section 2 we introduce the families of curves that we want to consider. In Section 3 we discuss the special subvariety $S(\mu_m)$ that contains $Z(m, N, a)$, we give the list of data (m, N, a) for which $Z(m, N, a) = S(\mu_m)$ and we state the main results. Sections 4 and 5 contain the main technical tools for the proof. In Section 4 we discuss how the VHS associated with our family of curves decomposes and we give some results about the monodromy of the summands. In Section 5 we briefly review the techniques of [8] and we give some refinements that we need in order to deal with hyperelliptic families. In Sections 6 and 7, finally, we prove the main theorem, first in the case $N = 4$, then for $N \geqslant 5$. We refer to the beginning of Section 6 for a brief explanation of how the proof works.

Acknowledgements. I thank Frans Oort for his encouragement and for stimulating discussions. It is a great pleasure to dedicate this paper to him. I thank Dion Gijswijt and Fokko van de Bult for helpful suggestions related to the combinatorics involved in the proof of Lemma 7.2. Further I thank Maarten Hoeve, who wrote two Python programs (available upon request from the author) to test some of the properties we need. The results of one of these programs are used in the proof of Lemma 7.2. Finally, I thank the referee for his or her comments on the paper and for some very helpful suggestions regarding the exposition.

Notation. If x is a real number, $\langle x\rangle = x - \lfloor x\rfloor$ denotes its fractional part. For $a \in \mathbb{Z}/m\mathbb{Z}$ or $a \in \mathbb{Z}$ we denote by $[a]_m$ the unique representative of the class a (resp. the class a mod m) in $\{0, \ldots, m-1\}$.

1. Some preliminaries about special subvarieties

In this section we work over $\mathbb{C}$. We recall the notion of a special subvariety. For further details we refer to [12], where the terminology "subvarieties of Hodge type" was used, and [20].

(1.1) Consider the moduli space $\mathscr{A}_{g,[n]}$ of g-dimensional principally polarized abelian varieties with a level n structure, for some $n \geqslant 3$. We first briefly recall the description of this moduli space as a Shimura variety.
Let $V_{\mathbb{Z}} := \mathbb{Z}^{2g} \subset V := \mathbb{Q}^{2g}$, and let $\Psi\colon V_{\mathbb{Z}} \times V_{\mathbb{Z}} \to \mathbb{Z}$ be the standard symplectic form. Let $G := \mathrm{CSp}(V_{\mathbb{Z}}, \Psi)$ be the group of symplectic similitudes. Let $\mathbb{S} := \mathrm{Res}_{\mathbb{C}/\mathbb{R}}\, \mathbb{G}_m$ be the Deligne torus, and let $\mathfrak{H}$ be the space of homomorphisms $h\colon \mathbb{S} \to G_{\mathbb{R}}$ that define a Hodge structure of type $(-1,0)+(0,-1)$ on $V_{\mathbb{Z}}$ for which $\pm(2\pi i)\cdot\Psi$ is a polarization. The pair $(G_{\mathbb{Q}}, \mathfrak{H})$ is a Shimura datum, and $\mathscr{A}_g$ can be described as the associated Shimura variety. Concretely, if $K_n := \bigl\{g \in G(\hat{\mathbb{Z}}) \bigm| g \equiv 1 \bmod n\bigr\}$ then $\mathscr{A}_{g,[n]}(\mathbb{C}) \cong G(\mathbb{Q})\backslash\mathfrak{H} \times G(\mathbb{A}_{\mathrm{fin}})/K_n$.
In order to define special subvarieties, consider an algebraic subgroup $H \subset G_{\mathbb{Q}}$ such that
$$Y_H := \bigl\{h \in \mathfrak{H} \bigm| h \text{ factors through } H_{\mathbb{R}}\bigr\}$$
is non-empty. The group $H(\mathbb{R})$ acts on Y_H by conjugation. It can be shown (see [11], Section I.3, or [12], 2.4) that Y_H is a finite union of orbits under $H(\mathbb{R})$. We remark that the condition that Y_H is non-empty imposes strong restrictions on H; it implies, for instance, that H is reductive. If $Y^+ \subset Y_H$ is a connected component and $\eta K_n \in G(\mathbb{A}_{\mathrm{fin}})/K_n$, the image of $Y^+ \times \{\eta K_n\}$ in $\mathscr{A}_{g,[n]}$ is an algebraic subvariety.

(1.2) *Definition.* — A closed irreducible algebraic subvariety $S \subset \mathscr{A}_{g,[n]}$ is called a *special subvariety* if there exist $Y^+ \subset Y_H$ and $\eta K_n \in G(\mathbb{A}_{\mathrm{fin}})/K_n$ as above such that $S(\mathbb{C})$ is the image of $Y^+ \times \{\eta K_n\}$ in $\mathscr{A}_{g,[n]}(\mathbb{C})$.

We refer to [12] and [20] for alternative descriptions and basic properties of special subvarieties.

(1.3) As level structures play no role in what we are doing, we prefer to state our results in terms of the moduli stack $\mathscr{A}_g$. Of course this is a stack, not a variety, but we allow ourselves to abuse terminology and speak of special subvarieties in $\mathscr{A}_g$ (over $\mathbb{C}$), where "special substack" would perhaps be more correct. By definition, then, a special subvariety $S \subset \mathscr{A}_g$ is a closed, reduced and irreducible algebraic substack such that for some (equivalently: any) $n \geqslant 3$ the irreducible components of the inverse image of S under the natural map

$\mathscr{A}_{g,[n]} \to \mathscr{A}_g$ are special. (It is in fact enough to require that some irreducible component is special.)

(1.4) Let $f\colon X \to T$ be a family of g-dimensional abelian varieties over an irreducible non-singular complex algebraic variety T. Choose a principal polarization λ of X/T, and let $\phi\colon T \to \mathscr{A}_g$ be the resulting morphism. Whether or not the closure of $\phi(T)$ is a special subvariety of $\mathscr{A}_g$ only depends on the isogeny class of the generic fibre of X/T as an abelian variety over the function field of T. If we replace X/T by an isogenous family or choose a different λ, the morphism ϕ is replaced by some other morphism $\phi'\colon T \to \mathscr{A}_g$, but if $\overline{\phi(T)}$ is special then so is $\overline{\phi'(T)}$. (This is even true without the assumption that λ is a principal polarization, but we shall not need this.) Without ambiguity we may therefore say that X/T is special if $\overline{\phi(T)} \subset \mathscr{A}_g$ is special for some choice of a polarization.
One property we shall use is that if X/T is isogenous to $Y_1 \times Y_2$ and X is special, the factors Y_i are both special. The converse is not true: if Y_1/T and Y_2/T are special, it is not necessarily the case that $(Y_1 \times Y_2)/T$ is special.

(1.5) Let $f\colon X \to T$ be as in 1.4. Consider the $\mathbb{Q}$-VHS over T with fibres the first cohomology groups $H^1(X_t, \mathbb{Q})$. Let $b \in T(\mathbb{C})$ be a Hodge-generic point for this VHS, and let $M \subset \mathrm{GL}\bigl(H^1(X_b,\mathbb{Q})\bigr)$ be the generic Mumford-Tate group of the family. Choose a principal polarization λ of X/T, let $\phi\colon T \to \mathscr{A}_g$ be the resulting morphism, and write $Z := \overline{\phi(T)}$. Finally, let $S \subset \mathscr{A}_g$ be the smallest special subvariety containing Z.
In order to calculate the dimension of S, it suffices to know the adjoint real group $M^{\mathrm{ad}}_{\mathbb{R}}$. More precisely, if $M^{\mathrm{ad}}_{\mathbb{R}} = Q_1 \times \cdots \times Q_r$ is the decomposition of this group as a product of simple factors, $\dim(S) = \sum_{i=1}^r d(Q_i)$, where $d(Q_i)$ is a contribution that only depends on the isomorphism class of the simple group Q_i. The only cases that are relevant for us are that

- $d(Q) = 0$ if Q is anisotropic (compact);
- $d(Q) = pq$ if $Q \cong \mathrm{PSU}(p,q)$;
- $d(Q) = h(h+1)/2$ if $Q \cong \mathrm{PSp}_{2h}$.

2. The setup

In this section, given data (m,N,a) as in the introduction (see 2.1 below), we construct a family of cyclic covers of $\mathbb{P}^1$ over some base scheme T. For later purposes we shall do this over a ring R of finite type over $\mathbb{Z}$.

(2.1) Let m and N be integers with $m \geqslant 2$ and $N \geqslant 2$, and consider an N-tuple of positive integers $a = (a_1,\ldots,a_N)$ such that $\gcd(m,a_1,\ldots,a_N) = 1$. We further require that $a_i \not\equiv 0$ modulo m for all i and $\sum_{i=1}^N a_i \equiv 0$ modulo m. The triple (m,N,a) serves as input for our constructions.
We call two such triples (m,N,a) and (m',N',a') equivalent if $m = m'$ and $N = N'$ and if the classes of a and a' in $(\mathbb{Z}/m\mathbb{Z})^N$ are in the same orbit under

$(\mathbb{Z}/m\mathbb{Z})^* \times \mathfrak{S}_N$. Here we let $(\mathbb{Z}/m\mathbb{Z})^*$ act diagonally by multiplication, and the symmetric group $\mathfrak{S}_N$ acts by permutation of the indices.
In what follows we shall usually assume $N \geqslant 4$ but for some arguments it is useful to allow N to be 2 or 3.

(2.2) Let (m, N, a) be a triple as in 2.1. Let R be the ring $\mathbb{Z}[1/m, u]/\Phi_m$ with Φ_m the mth cyclotomic polynomial. We write $\zeta \in R$ for the class of u; it is a root of unity of order m. We embed R into $\mathbb{C}$ by sending ζ to $\exp(2\pi i/m)$. The element ζ defines an isomorphism of R-group schemes $(\mathbb{Z}/m\mathbb{Z})_R \xrightarrow{\sim} \mu_{m,R}$ by $(b \bmod m) \mapsto \zeta^b$.
Let $U \subset (\mathbb{A}^1_R)^N$ be the complement of the big diagonals. In other words, U is the R-scheme of ordered N-tuples $(t_1, \dots, t_N)$ of distinct points in $\mathbb{A}^1$. Let $B \subset \mathbb{P}^2_U$ be the projective curve over U obtained as the Zariski closure of the affine curve whose fibre over a point $(t_1, \dots, t_N)$ is given by

$$y^m = (x - t_1)^{a_1} \cdots (x - t_N)^{a_N} = \prod_{i=1}^{N} (x - t_i)^{a_i} .$$

We have a μ_m-action on B over U by $\zeta \cdot (x, y) = (x, \zeta \cdot y)$. The rational function x defines a morphism $\pi_B \colon B \to \mathbb{P}^1_U$.
There exist an open subscheme $T \subset U$, a smooth proper curve $f \colon C \to T$ equipped with an action of $\mu_{m,T}$, and a $\mu_{m,T}$-equivariant morphism $\rho \colon C \to B_T$, such that for every point $t \in T$ the morphism on fibres $\rho_t \colon C_t \to B_t$ is a normalization of B_t. Let $\pi := \pi_B \circ \rho \colon C \to \mathbb{P}^1_T$, which is a finite morphism that realizes $\mathbb{P}^1_T$ as the quotient of C by the action of $\mu_{m,T}$. If the context requires it, we include the data (m, N, a) in the notation, writing $C = C(m, N, a)$ for instance. Further we write $J \to T$ for the Jacobian of C over T.
If k is a field and $t = (t_1, \dots, t_N) \in T(k)$, we can also describe $\pi_t \colon C_t \to \mathbb{P}^1_k$ as the μ_m-cover of $\mathbb{P}^1_k$ with branch points $t_1, \dots, t_N$ and local monodromy about t_i given by the element $\zeta^{a_i} \in \mu_m$.
The assumption that $\gcd(m, a_1, \dots, a_N) = 1$ implies that the fibres of $f \colon C \to T$ are geometrically irreducible. Let $r_i := \gcd(m, a_i)$. The Hurwitz formula gives that the fibres have genus

$$g = 1 + \frac{(N-2)m - \sum_{i=1}^N r_i}{2} , \qquad (2.2.1)$$

so we obtain a morphism $\psi \colon T \to \mathscr{M}_g$ over R. Define

$$\phi \colon T \to \mathscr{A}_g \qquad (2.2.2)$$

to be the composition of ψ with the Torelli morphism. Up to isomorphism, the morphism ψ, and hence also ϕ, only depends on the equivalence class of the triple (m, N, a) for the equivalence relation defined in 2.1.

(2.3) *Remark.* — For computational purposes we have restricted our attention to the case where all branch points t_i are in $\mathbb{A}^1 \subset \mathbb{P}^1$, and we have not fixed any of these branch points, thereby creating some redundancy and excluding families where one of the branch points is fixed to be the point at ∞. For our main results, the only thing that really matters is the closure of the image of $\phi_{\mathbb{C}}\colon T_{\mathbb{C}} \to \mathscr{A}_{g,\mathbb{C}}$. For instance, while the family of curves $y^{10} = x(x-1)(x-\lambda)$ is not among the families we consider (the point at ∞ being a branch point), the subvariety of $\mathscr{A}_9$ we obtain from this family is the same as the one obtained by taking $m = 10$, with $N = 4$ and $a = (1,1,1,7)$.

(2.4) *Convention.* — In what follows we shall in several steps replace the base scheme T by a subscheme. In such a case, it will be understood that we replace C by its restriction to the new base scheme, and we again write $f\colon C \to T$ for the curve thus obtained. Similarly, we retain the notation for various other objects associated with our family of curves.

(2.5) *Notation.* — Let M be a module over some commutative R-algebra, or a sheaf on some R-scheme, on which the group scheme μ_m acts. For $n \in \mathbb{Z}/m\mathbb{Z}$ we write

$$M_{(n)} := \left\{ x \in M \mid \zeta(x) = \zeta^n \cdot x \right\},$$

which in the sheaf case has to be interpreted on the level of local sections. We refer to $M_{(n)}$ as the n-eigenspace of M. We have $M = \oplus_{n \in \mathbb{Z}/m\mathbb{Z}} M_{(n)}$.

(2.6) Recall that $r_i = \gcd(m, a_i)$. Consider the μ_m-cover $\pi\colon C_t \to \mathbb{P}^1$ for some $t \in T(k)$, where k is a field. For $i \in \{1, \ldots, N\}$ and $n \in \mathbb{Z}$, let

$$l(i,n) := -1 + \left\lceil \frac{r_i - na_i}{m} \right\rceil = \left\lfloor \frac{-na_i}{m} \right\rfloor,$$

where the second equality easily follows from the fact that $r_i = \gcd(m, a_i)$. Consider the differential forms

$$\omega_{n,\nu} := y^n \cdot (x - t_1)^\nu \cdot \prod_{i=1}^{N} (x - t_i)^{l(i,n)} \cdot dx, \tag{2.6.1}$$

and note that these only depend on the pair $(n \bmod m, \nu)$.

The following result is standard.

(2.7) *Lemma.* — *Let $n \in \mathbb{Z}/m\mathbb{Z}$ with $n \neq 0$. The forms $\omega_{n,\nu}$ for $0 \leqslant \nu \leqslant -2 + \sum_{i=1}^N \left\langle \frac{-na_i}{m} \right\rangle$ are regular 1-forms on C_t and they form a k-basis for $H^0(C_t, \Omega^1)_{(n)}$.*

3. The special subvariety given by the action of the covering group

In this section we work over $\mathbb{C}$ and we fix a triple (m, N, a) as in 2.1 with $N \geqslant 4$. We retain the notation introduced in the previous section, with the convention that all objects are now considered over $\mathbb{C}$ via the chosen embedding $R \hookrightarrow \mathbb{C}$.

(3.1) *Definition.* — We let $Z(m, N, a) \subset \mathscr{A}_{g,\mathbb{C}}$ be the scheme-theoretic (or rather, stack-theoretic) image of the morphism ϕ: $T \to \mathscr{A}_g$ of (2.2.2).

In other words, $Z(m, N, a)$ is the reduced closed substack of $\mathscr{A}_{g,\mathbb{C}}$ with underlying topological space $\overline{\phi(T)}$. We note that $Z(m, N, a)$ only depends on the equivalence class of (m, N, a) and does not depend on the choice of the open subscheme T in 2.1. The dimension of $Z(m, N, a)$ equals $N - 3$.

(3.2) *Notation.* — It will be convenient to write

$$I(m) := \big[(\mathbb{Z}/m\mathbb{Z}) \setminus \{0 \bmod m\}\big]/\{\pm 1\}\,. \tag{3.2.1}$$

Recall that $\langle x\rangle$ denotes the fractional part of x. For $n \in \mathbb{Z}/m\mathbb{Z}$ we define

$$d_n := \begin{cases} -1 + \sum_{i=1}^{N} \left\langle \frac{-na_i}{m} \right\rangle & \text{if } n \not\equiv 0, \\ 0 & \text{if } n \equiv 0, \end{cases} \tag{3.2.2}$$

which by Lemma 2.7 is the dimension of the (n)-eigenspace of $H^0(C_t, \Omega^1)$, for any $t \in T(\mathbb{C})$.

(3.3) The substack $Z(m, N, a) \subset \mathscr{A}_g$ is contained in a special subvariety $S(\mu_m) \subset \mathscr{A}_g$ determined by the action of $\mathbb{Z}[\mu_m]$ on the relative Jacobian $J \to T$. More precisely, $S(\mu_m)$ is the largest closed, reduced and irreducible substack $S \subset \mathscr{A}_g$ containing $Z(m, N, a)$ such that the homomorphism $\mathbb{Z}[\mu_m] \to \mathrm{End}(J/T)$ induced by the action of μ_m on C/T extends to an action of $\mathbb{Z}[\mu_m]$ on the universal abelian scheme over S.
Choose a base point $b \in T(\mathbb{C})$, and let (J_b, λ) be the corresponding Jacobian with its principal polarization. With $(V_{\mathbb{Z}}, \Psi)$ as in 1.1, choose a symplectic similitude σ: $H_1(J_b, \mathbb{Z}) \xrightarrow{\sim} V_{\mathbb{Z}}$, where we equip $H_1(J_b, \mathbb{Z})$ with its Riemann form (i.e., the polarization, in the sense of Hodge theory, that corresponds with λ). Via σ, the action of μ_m on J_b induces a structure of a $\mathbb{Q}[\mu_m]$-module on $V = V_{\mathbb{Z}} \otimes \mathbb{Q}$. Consider the algebraic subgroup $H \subset G_{\mathbb{Q}} = \mathrm{CSp}(V, \Psi)$ of $\mathbb{Q}[\mu_m]$-linear symplectic similitudes, i.e., the subgroup given by

$$H := \mathrm{GL}_{\mathbb{Q}[\mu_m]}(V) \cap \mathrm{CSp}(V, \Psi)\,.$$

With notation as in 1.1, the image of $Y_H \subset \mathfrak{H}$ under the map

$$\mathfrak{H} \twoheadrightarrow G(\mathbb{Z})\backslash\mathfrak{H} \cong G(\mathbb{Q})\backslash\mathfrak{H} \times G(\mathbb{A}_{\mathrm{fin}})/G(\hat{\mathbb{Z}}) \cong \mathscr{A}_g(\mathbb{C})$$

is (the set of $\mathbb{C}$-points of) a finite union of algebraic subvarieties of $\mathscr{A}_g$, and the special subvariety $S(\mu_m)$ is the unique irreducible component of this image that contains $Z(m, N, a)$.
The dimension of $S(\mu_m)$ is given by

$$(3.3.1) \qquad \dim S(\mu_m) = \sum d_{-n} d_n + \begin{cases} \frac{d_k(d_k+1)}{2} & \text{if } m = 2k \text{ is even,} \\ 0 & \text{if } m \text{ is odd,} \end{cases}$$

where the first sum runs over the pairs $\pm n \in I(m)$ with $2n \not\equiv 0$. See [14], Section 5; see also Remark 4.6 below.
In particular, as $Z(m, N, a) \subset S(\mu_m)$ we have

$$(3.3.2) \qquad N - 3 \leqslant \dim S(\mu_m)\,.$$

If equality holds then $Z(m, N, a) = S(\mu_m) \subset \mathscr{A}_g$ is a special subvariety; it then follows that among the Jacobians J_t, for $t \in T(\mathbb{C})$, there are, up to isomorphism, infinitely many Jacobians of CM type. (Here we use that on a special subvariety the CM points lie dense.)

(3.4) *Inventory of examples.* — Table 1 lists twenty triples (m, N, a) with $N \geqslant 4$ for which $N - 3 = \dim S(\mu_m)$, so that $Z(m, N, a) \subset \mathscr{A}_{g,\mathbb{C}}$ is a special subvariety. Our assumption that $N \geqslant 4$ means we are only considering the cases that give rise to a special subvariety of positive dimension.
The first column of the table gives a number that we assign to each example for reference. The examples are sorted first by genus, then by degree of the cover. The second column gives the genus of the curves in the family. In the next three columns we give the data (m, N, a). In most cases there is a unique $a = (a_1, \ldots, a_N)$ in its equivalence class such that $1 \leqslant a_1 \leqslant \cdots \leqslant a_N \leqslant m - 1$ with $\sum a_i = 2m$, and if there is a unique such representative, this is the one we list. If $N = 4$ there are usually two such representatives, the second one being $(m - a_4, m - a_3, m - a_2, m - a_1)$; we list the one which lexicographically comes first. In the last column we give references to places in the literature where the example can be found. Here "S(i)" refers to example (i) in [24], "Mi" refers to example i in the appendix of [17], and dJN(1.3.i) refers to example (1.3.i) in [6]. These examples can also be found in [22]; see 4.8 below.

(3.5) *Remark.* — If we have a triple (m, N, a) as in 2.1 with $N = 3$, the associated subvariety $Z = Z(m, N, a)$ is a special point in $\mathscr{A}_g$.

The following theorem is the main result of this paper. It says that the list of examples in Table 1 is exhaustive.

(3.6) *Theorem.* — *Consider data (m, N, a) as in* 2.1*, with $N \geqslant 4$. Then $Z(m, N, a) \subset \mathscr{A}_{g,\mathbb{C}}$ is a special subvariety if and only if (m, N, a) is equivalent to one of the twenty examples listed in* Table 1.

By what was explained above, it only remains to be shown that $Z(m, N, a)$ is not special if (m, N, a) is not equivalent to one of the triples in the table. In 4.9

	genus	m	N	a	references
(1)	1	2	4	$(1,1,1,1)$	
(2)	2	2	6	$(1,1,1,1,1,1)$	
(3)	2	3	4	$(1,1,2,2)$	
(4)	2	4	4	$(1,2,2,3)$	
(5)	2	6	4	$(2,3,3,4)$	
(6)	3	3	5	$(1,1,1,1,2)$	S(1), M41
(7)	3	4	4	$(1,1,1,1)$	
(8)	3	4	5	$(1,1,2,2,2)$	S(3), M43
(9)	3	6	4	$(1,3,4,4)$	
(10)	4	3	6	$(1,1,1,1,1,1)$	S(2), M23, dJN(1.3.1)
(11)	4	5	4	$(1,3,3,3)$	S(4), dJN(1.3.2)
(12)	4	6	4	$(1,1,1,3)$	
(13)	4	6	4	$(1,1,2,2)$	
(14)	4	6	5	$(2,2,2,3,3)$	
(15)	5	8	4	$(2,4,5,5)$	
(16)	6	5	5	$(2,2,2,2,2)$	S(5), M44
(17)	6	7	4	$(2,4,4,4)$	S(6), dJN(1.3.3)
(18)	6	10	4	$(3,5,6,6)$	
(19)	7	9	4	$(3,5,5,5)$	
(20)	7	12	4	$(4,6,7,7)$	

Table 1: monodromy data that give rise to a special subvariety

we shall first prove this for $m = 2$. In Section 6 we shall prove the theorem for $N = 4$. The case $N > 4$ is treated in Section 7.
Combining the theorem with the main result of [25] we obtain, for $N = 4$, the following finiteness result for the number of CM fibres.

(3.7) *Corollary. — Assume the Generalized Riemann Hypothesis for CM* *fields. If we have a triple (m, N, a) with $N = 4$ and the equivalence class of this triple is not among the twenty examples listed in* Table 1 *then up to isomorphism there are finitely many Jacobians of CM type in the family $J \to T_{\mathbb{C}}$.*

4. Decomposition of the variation of Hodge structure

In this section we again work over $\mathbb{C}$. We fix a triple (m, N, a) as in 2.1 with $N \geqslant 4$. The corresponding family of curves $C \to T$ gives rise to a variation of Hodge structure over T (over $\mathbb{C}$) on which $\mathbb{Q}[\mu_m]$ acts. We describe the resulting decomposition of the VHS, and we give some results about the monodromy of the summands.

(4.1) Let (m, N, a) be as in 2.1. For $n \in \mathbb{Z}/m\mathbb{Z}$, let $N(n)$ be the number of indices $i \in \{1, \ldots, N\}$ such that $na_i \not\equiv 0$ modulo m. In particular, $N(n) = N$ if $n \in (\mathbb{Z}/m\mathbb{Z})^*$. If $n \neq 0$ then $d_n + d_{-n} = N(n) - 2$.
Let $m' \geqslant 2$ be a divisor of m, say with $m = rm'$. Write $N' := N(r \bmod m)$, and consider the N'-tuple a' in $(\mathbb{Z}/m'\mathbb{Z})^{N'}$ obtained from the N-tuple $(a_1 \bmod m', \ldots, a_N \bmod m')$ by omitting the zero entries. Then (m', N', a') is again a triple as in 2.1; we refer to it as the triple obtained from (m, N, a) by reduction modulo m'.

(4.2) As in 2.2, consider the family of curves $f\colon C \to T$ associated with the triple (m, N, a), where, as in the previous section, we work over $\mathbb{C}$. The cohomology groups $H^1(C_t, \mathbb{Q})$ are the fibres of a polarized $\mathbb{Q}$-VHS with underlying local system $\mathbb{V} := R^1 f_*^{\mathrm{an}} \mathbb{Q}_C$. This $\mathbb{Q}$-VHS comes equipped with an action of the group ring $\mathbb{Q}[\mu_m] = \prod_{d|m} K_d$, where $K_d = \mathbb{Q}[t]/\Phi_d$ is the cyclotomic field of dth roots of unity. Accordingly we have a decomposition of $\mathbb{Q}$-VHS,

$$\mathbb{V} = \oplus_{d|m} \mathbb{V}^{[d]}\,, \tag{4.2.1}$$

where $\mathbb{V}^{[d]}$ is a polarized $\mathbb{Q}$-VHS over T equipped with an action of K_d.

(4.3) Let (m, N, a) be as in 2.1, with $N \geqslant 4$. Let $m' \geqslant 2$ be a proper divisor of m, and let (m', N', a') be the triple obtained from (m, N, a) by reduction modulo m', as in 4.1.
Let $\rho\colon \mathbb{A}^N \to \mathbb{A}^{N'}$ be the projection map, omitting the coordinates x_i for all indices i with $a_i \equiv 0$ modulo m'. Performing the construction of 2.2 we may choose $T = T(m, N, a) \subset \mathbb{A}^N$ and $T' = T(m', N', a') \subset \mathbb{A}^{N'}$ such that ρ maps T to T'. (The map $T \to T'$ is then dominant.) If $f'\colon C' \to T'$ is the family of curves associated with the triple (m', N', a'), the pull-back $\rho^* C' = C' \times_{T'} T$ can be identified with the quotient of C/T modulo the action of $\mu_r \subset \mu_m$, where $r = m/m'$.
Let $\mathbb{V}' = \mathbb{V}(m', N', a')$ be the $\mathbb{Q}$-VHS over T' associated with the triple (m', N', a'). The quotient morphism $C \to \rho^* C'$ over T gives a map $\rho^* \mathbb{V}' \to \mathbb{V}$

and this induces an isomorphism $\rho^*\mathbb{V}' \cong \oplus_{d|m'}\mathbb{V}^{[d]}$. We refer to the sub-$\mathbb{Q}$-VHS $\rho^*\mathbb{V}'$ as the *old part* associated with the divisor m'. The direct summand $\mathbb{V}^{[m]} \subset \mathbb{V}$ is called the *new part*; in the decomposition (4.2.1) it is the only direct summand that is not contained in an old part.

(4.4) *Lemma. — Let the notation and assumptions be as in* 4.3. *Let $g = g(m,N,a)$ and $g' = g(m',N',a')$ be the respective genera. If $Z(m,N,a) \subset \mathscr{A}_{g,\mathbb{C}}$ is a special subvariety then $Z(m',N',a') \subset \mathscr{A}_{g',\mathbb{C}}$ is special, too.*

Proof. Suppose $Z(m,N,a)$ is special. Write $J = J(m,N,a) \to T$ and $J' = J(m',N',a') \to T'$ for the respective Jacobians. Then ρ^*J' is an isogeny factor of J. Hence, if $\theta\colon T \to \mathscr{A}_{g',\mathbb{C}}$ is the morphism corresponding to ρ^*J', it follows from 1.4 that the Zariski closure of the image of θ is a special subvariety. But θ is just the composition of the projection $\rho\colon T \to T'$, which is dominant, and the morphism $\phi(m',N',a')\colon T' \to \mathscr{A}_{g',\mathbb{C}}$ associated with the data (m',N',a'). Hence the closure of the image of θ is $Z(m',N',a')$. □

(4.5) With notation as in 2.5, the $\mathbb{C}$-local system $\mathbb{V}_{\mathbb{C}}$ decomposes as $\mathbb{V}_{\mathbb{C}} = \oplus_{n\in\mathbb{Z}/m\mathbb{Z}}\mathbb{V}_{\mathbb{C},(n)}$. The relation with (4.2.1) is that $\mathbb{V}_{\mathbb{C}}^{[d]}$ is the sum of all $\mathbb{V}_{\mathbb{C},(n)}$ with $\mathrm{ord}(n) = d$. We have $V_{\mathbb{C},(0)} = 0$, and for $n \neq 0$ the $\mathbb{C}$-local system $\mathbb{V}_{\mathbb{C},(n)}$ has rank $N(n) - 2$, where $N(n)$ is defined as in 4.1. (See also [7], Section 2.)
With real coefficients, and with $I(m)$ as in (3.2.1), we have a decomposition of $\mathbb{R}$-VHS

$$\mathbb{V}_{\mathbb{R}} = \left(\bigoplus_{\pm n\in I(m),2n\not\equiv 0} \mathbb{V}_{\mathbb{R},(\pm n)}\right) \oplus \mathbb{V}_{\mathbb{R},(\frac{m}{2})}\,,$$

where the last summand only occurs if m is even. The decomposition is such that

$$\mathbb{V}_{\mathbb{R},(\pm n)} \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{V}_{\mathbb{C},(n)} \oplus \mathbb{V}_{\mathbb{C},(-n)}$$

and

$$\mathbb{V}_{\mathbb{R},(\frac{m}{2})} \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{V}_{\mathbb{C},(\frac{m}{2})} \quad \text{(for even } m)\,.$$

On the summand $\mathbb{V}_{\mathbb{R},(\pm n)}$ the polarization of the VHS induces a (-1)-hermitian form $\beta_{\pm n}$ of signature (d_n, d_{-n}); see also [7], Corollary (2.21) and (2.23). In case m is even, the polarization induces a symplectic form $\beta_{\frac{m}{2}}$ on $\mathbb{V}_{\mathbb{R},(\frac{m}{2})}$.
As in 3.3 we choose a base point $b \in T(\mathbb{C})$, and a symplectic similitude $\sigma\colon H^1(J_b,\mathbb{Q}) \xrightarrow{\sim} V$. Via this similitude, we identify V with the fibre of $\mathbb{V}$ at b. Correspondingly, we write $V_{\mathbb{R},(\pm n)}$ for the direct summand of $V_{\mathbb{R}}$ that under σ maps to the fibre at b of $\mathbb{V}_{\mathbb{R},(\pm n)}$.
For what follows, it will be convenient to choose the base point b to be a Hodge-generic point with respect to the variation $\mathbb{V}$, so from now on we assume this. Define $\mathrm{Mon} \subset \mathrm{GL}(V)$ and $\mathrm{Hdg} \subset \mathrm{GL}(V)$ to be the algebraic monodromy groups of the $\mathbb{Q}$-local system $\mathbb{V}$ and the Hodge group of the fibre at b, respectively. (Since we have chosen b to be Hodge-generic, Hdg is the generic Hodge group of the VHS.) By [3], Theorem 1, the identity component Mon^0 is a semisimple normal subgroup of Hdg.

(4.6) *Remark.* — The generic Hodge group Hdg is contained in the algebraic group $H := \mathrm{GL}_{\mathbb{Q}[\mu_m]}(V) \cap \mathrm{CSp}(V, \Psi)$ considered in 3.3. Extending scalars to $\mathbb{R}$ we have

$$H_{\mathbb{R}} \cong \left(\prod_{\pm n \in I(m), 2n \not\equiv 0} \mathrm{U}(V_{\mathbb{R},(\pm n)}, \beta_{\pm n}) \right) \times \mathrm{Sp}(V_{\mathbb{R},(\frac{m}{2})}, \beta_{\frac{m}{2}}) \,, \tag{4.6.1}$$

where the symplectic factor only occurs if m is even. Our formula (3.3.1) follows from this together with what was explained in 1.5.

We have $\mathrm{Mon}^0 \subset \mathrm{Hdg} \subset H$. The next proposition gives us information about the projections of the $\mathbb{R}$-group $\mathrm{Mon}^0_{\mathbb{R}}$ onto the various factors in the decomposition (4.6.1).

(4.7) *Proposition.* — (i) *Suppose we have $\pm n \in I(m)$ with $2n \not\equiv 0$ such that $d_n \geqslant 1$ and $d_{-n} \geqslant 1$. Then the image of* $\mathrm{Mon}^0_{\mathbb{R}}$ *in* $\mathrm{U}(V_{\mathbb{R},(\pm n)}, \beta_{\pm n})$ *is the special unitary group* $\mathrm{SU}(V_{\mathbb{R},(\pm n)}, \beta_{\pm n})$*, which is isomorphic to* $\mathrm{SU}(d_n, d_{-n})$.
(ii) *If m is even, the group* $\mathrm{Mon}^0_{\mathbb{R}}$ *projects surjectively to the symplectic group* $\mathrm{Sp}(V_{\mathbb{R},(\frac{m}{2})}, \beta_{\frac{m}{2}})$*, which is isomorphic to* $\mathrm{Sp}_{2h,\mathbb{R}}$ *with* $h = d_{\frac{m}{2}}$.

Proof. For (i), see Rohde [22], Theorem 5.1.1. For (ii), assume m is even, and let $h := d_{\frac{m}{2}}$. There are then $2h+2$ indices i for which a_i is even, and without loss of generality we may assume these are the indices $i \in \{1, \ldots, 2h+2\}$. With the above notation, $\mathbb{V}_{\mathbb{R},(\frac{m}{2})}$ is the same as $\mathbb{V}^{[2]}_{\mathbb{R}}$, and if we define $\mathrm{Mon}^{[2]} \subset \mathrm{GL}(V^{[2]})$ as the algebraic monodromy group of the $\mathbb{Q}$-local system $\mathbb{V}^{[2]}$ then the image of Mon^0 in $\mathrm{Sp}(V_{\mathbb{R},(\frac{m}{2})}, \beta_{\frac{m}{2}})$ equals $\mathrm{Mon}^{[2],0}_{\mathbb{R}}$. Further, $\mathbb{V}^{[2]}$ is just the local system obtained from the family of hyperelliptic curves $u^2 = (x - t_1) \cdots (x - t_{2h+2})$; cf. 4.3. By [1], Theorem 1 (see also [2]), the connected algebraic monodromy group of this local system is the full symplectic group. $\square$

(4.8) Let (m, N, a) be a triple as in 2.1, with $N \geqslant 4$. Consider the following condition.

$$\begin{array}{l} \text{There exists a } \pm n \in I(m) \text{ with } \{d_n, d_{-n}\} = \{1, N-3\}, \\ \text{and for all other } \pm n' \in I(m), \text{ either } d_{n'} = 0 \text{ or } d_{-n'} = 0. \end{array} \tag{4.8.1}$$

All examples in Table 1, with the exception of Example 2, satisfy this condition. It has been proven by Rohde in [22] that these nineteen examples are the only examples (up to equivalence) of triples (m, N, a) with $N \geqslant 4$ that satisfy (4.8.1).

(4.9) We now prove Theorem 3.6 for $m = 2$. In this case N is even, $g = (N-2)/2$, and up to equivalence $a = (1, \ldots, 1)$ is the only possibility. Further, $Z(2, N, a) \subset \mathscr{A}_{g,\mathbb{C}}$ is the closure of the hyperelliptic locus in $\mathscr{A}_g$. The assertion is that this is not special for $g \geqslant 3$. This is true because for $g \geqslant 3$ the hyperelliptic locus is not dense in $\mathscr{A}_g$, whereas by (ii) of Proposition 4.7 the generic Hodge group Hdg is the full symplectic group.

In what follows we may therefore assume $m > 2$.

5. Canonical liftings of ordinary Jacobians in positive characteristic

(5.1) We need to recall some definitions and results from the paper [8] by Dwork and Ogus. We first discuss their theory in a general setting. After that, from 5.4 on, we return to the specific families of curves that interest us, and we explain how the results of [8] apply to that situation.
Given an irreducible base scheme T and a smooth projective curve $f\colon C \to T$ we write $\omega_{C/T}$ for $\Omega^1_{C/T}$. Consider the Hodge bundle $\mathbb{E} = \mathbb{E}(C/T) := f_*\omega_{C/T}$, which is a vector bundle on T of rank g, the genus of the fibres. We have a Kodaira-Spencer map KS: $\mathrm{Sym}^2(\mathbb{E}) \to \Omega^1_{T/R}$ and we define

$$\mathscr{K} = \mathscr{K}(C/T) := \mathrm{Ker}\big(\mathrm{Sym}^2(\mathbb{E}) \xrightarrow{\mathrm{mult}} f_*(\omega_{C/T}^{\otimes 2})\big)\,,$$

$$\mathscr{Q} = \mathscr{Q}(C/T) := \mathrm{Coker}\big(f_*(\omega_{C/T}^{\otimes 2})^\vee \xrightarrow{\mathrm{mult}^\vee} \mathrm{Sym}^2(\mathbb{E})^\vee\big)\,,$$

where "mult" is the multiplication map. We remark that $\mathscr{Q}$ can be thought of as the pull-back to T of the normal bundle to the Torelli locus inside $\mathscr{A}_g$. Outside the hyperelliptic locus, mult is surjective and $\mathscr{K}$ is the dual of $\mathscr{Q}$.

(5.2) Let k be an algebraically closed field of characteristic $p > 0$. Consider a smooth projective curve C/k of genus g such that its Jacobian J is ordinary. Let λ be the natural principal polarization of J. By Serre-Tate theory (see [9] or [10], Chap. 5) we have a canonical lifting of (J, λ) to a principally polarized abelian variety $(J^{\mathrm{can}}, \lambda^{\mathrm{can}})$ over the ring of Witt-vectors $W(k)$. In general, for $g \geqslant 4$ this canonical lifting is not the Jacobian of a curve over $W(k)$. More precisely, Dwork and Ogus show that in general not even the canonical lifting over $W_2(k)$, the Witt-vectors of length 2, is again a Jacobian.
Following [8] we call the ordinary curve C/k *pre-W_2-canonical* if there exists a smooth projective curve Y over $W_2(k)$ such that $(J^{\mathrm{can}}, \lambda^{\mathrm{can}})$ over $W_2(k)$ is isomorphic, as a principally polarized abelian variety, to the Jacobian of Y.
The main advantage of working modulo p^2 is that in this case there is a natural class $\beta_{C/k}$ in $\mathscr{Q}(C/k)$ that vanishes if and only if C/k is pre-W_2-canonical; see [8], Prop. (2.4). This invariant $\beta_{C/k}$ cannot be defined in a family of curves (in a sense that can be made precise, see [8], § 3), but its Frobenius pullback can, as we shall discuss next.
Let T be a smooth k-scheme, and let $F_T\colon T \to T$ be its absolute Frobenius endomorphism. Consider a smooth projective curve $f\colon C \to T$ such that all fibres C_t are ordinary. This assumption permits us to view the inverse Cartier operator as an $\mathscr{O}_T$-linear homomorphism

$$\gamma\colon F_T^*\mathbb{E} \to \mathbb{E}\,,$$

with $\mathbb{E} = \mathbb{E}(C/T)$ the Hodge bundle. This map γ is the inverse transpose of the Frobenius action on $R^1 f_* \mathscr{O}_C$.

Dwork and Ogus define a global section $\tilde{\beta}_{C/T}$ of $F_T^* \mathscr{Q}(C/T)$ such that for any $t \in T(k)$ the value of $\tilde{\beta}_{C/T}$ at t is $F_k^*(\beta_{C_t/k})$. See [8], Prop. 2.7.

The sheaf $F_T^* \mathscr{Q}(C/T)$ comes equipped with a canonical flat connection

$$\nabla \colon F_T^* \mathscr{Q}(C/T) \to F_T^* \mathscr{Q}(C/T) \otimes \Omega^1_{T/k}\,.$$

In particular, still with T smooth over k, if C_t/k is pre-W_2-canonical for all $t \in T(k)$, the section $\tilde{\beta}_{C/T}$ is zero, so certainly $\nabla \tilde{\beta}_{C/T} = 0$. One of the main points of [8], then, is that $\nabla \tilde{\beta}_{C/T}$ can be calculated explicitly. The result is easiest to state under the additional hypothesis that the fibres C_t are not hyperelliptic. We note that this assumption is not always satisfied in the situation we want to consider. In Prop. 5.8 we shall give a modified version of the next result that also works for hyperelliptic families.

If the C_t are not hyperelliptic, the multiplication map $\mathrm{Sym}^2(\mathbb{E}) \to f_*(\omega^{\otimes 2})$ is surjective, so, with notation as introduced in 5.1, $\tilde{\beta}_{C/T}$ can be viewed as an $\mathscr{O}_T$-linear map $F_T^* \mathscr{K} \to \mathscr{O}_T$.

The following result is [8], Prop. 3.2. (In [8] the result is stated under some versality assumption on the family C/T but one easily verifies that their Prop. 3.2 is true without this assumption.)

(5.3) *Proposition (Dwork-Ogus). — With assumptions and notation as above, and assuming the curves C_t to be non-hyperelliptic, $-\nabla(\tilde{\beta}_{C/T}) \colon F_T^* \mathscr{K} \to \Omega^1_{T/k}$ is equal to the composition*

$$F_T^* \mathscr{K} \xhookrightarrow{\text{incl}} F_T^* \mathrm{Sym}^2(\mathbb{E}) \xrightarrow{\mathrm{Sym}^2(\gamma)} \mathrm{Sym}^2(\mathbb{E}) \xrightarrow{\text{KS}} \Omega^1_{T/k}\,.$$

(5.4) *Assumptions.* — In the rest of this section we fix data (m, N, a) as in 2.1 with $m > 2$ and $N \geqslant 4$, and we consider the family of curves $f \colon C \to T$ as constructed in 2.2. We assume that (m, N, a) is not equivalent to one of the triples listed in Table 1. We further assume that the closed subvariety $Z(m, N, a) \subset \mathscr{A}_{g,\mathbb{C}}$ is a special subvariety; our aim is to derive a contradiction. Without loss of generality we may suppose (m, N, a) is minimal with respect to the above assumptions, by which we mean that there is no triple (m', N', a') that satisfies our assumptions and for which we have $4 \leqslant N' < N$ or $N' = N$ and $2 \leqslant m' < m$. In particular, it follows from Lemma 4.4 that if m' is a proper divisor of m and (m', N', a') is obtained from (m, N, a) by reduction modulo m', as in 4.3, either $N' \leqslant 3$ or (m', N', a') is equivalent to one of the twenty triples listed in Table 1.

(5.5) *Lemma.* — (i) *The subsheaf* $f_*(\omega_{C/T}^{\otimes 2})_{(0)}$ *of* μ_m*-invariant sections of* $f_*(\omega_{C/T}^{\otimes 2})$ *is a locally free* $\mathscr{O}_T$*-module of rank* $N-3$.
(ii) *The Kodaira-Spencer morphism* $\mathrm{KS}\colon \mathrm{Sym}^2(\mathbb{E}) \to \Omega^1_{T/R}$ *factors over the composite map*

$$\mathrm{Sym}^2(\mathbb{E}) \xrightarrow{\mathrm{pr}} \mathrm{Sym}^2(\mathbb{E})_{(0)} \xrightarrow{\mathrm{mult}} f_*(\omega_{C/T}^{\otimes 2})_{(0)}$$

and the induced map $\mathrm{KS}_{(0)}\colon f_*(\omega_{C/T}^{\otimes 2})_{(0)} \to \Omega^1_{T/R}$ *is a fibrewise injective homomorphism of vector bundles.*

Proof. (i) By a result of Chevalley and Weil in [5], for every $t \in T(\mathbb{C})$ the subspace of μ_m-invariants in $H^0(C_t, \Omega^{\otimes 2})$ has dimension $N-3$.
(ii) The fibre of $\mathrm{Sym}^2(\mathbb{E})_{(0)}$ at a point t is dual to the space $H^1(C_t, \Theta)_{(0)}$, which parametrizes the deformations of C_t for which the μ_m-action deforms along. Since we have a μ_m-action on the whole family C/T, the Kodaira-Spencer map factors through the projection $\mathrm{Sym}^2(\mathbb{E}) \to \mathrm{Sym}^2(\mathbb{E})_{(0)}$. For any family of curves it also factors through the multiplication map $\mathrm{Sym}^2(\mathbb{E}) \to f_*(\omega_{C/S}^{\otimes 2})$; hence KS factors through $f_*(\omega_{C/T}^{\otimes 2})_{(0)}$. The last assertion of (ii) just says that at any $t \in T(k)$ our family is complete in the sense of deformation theory: if $D \to \mathrm{Spec}\bigl(k[\epsilon]\bigr)$ is a first-order deformation of C_t with its μ_m-action, $D/k[\epsilon]$ can be obtained by pull-back from our family. This is clear, as the quotient D/μ_m is isomorphic to $\mathbb{P}^1_{k[\epsilon]}$. □

(5.6) *Lemma.* — *There exists a prime number* p *with* $p \equiv 1$ *modulo* m *and, for* $\mathfrak{p}$ *a prime of* $R = \mathbb{Z}[1/m, u]/\Phi_m$ *above* p*, a dense open subset* U *of* $T_0 := T \otimes_R (R/\mathfrak{p})$*, such that for any algebraically closed field* k *of characteristic* p *and any* $t \in U(k)$ *the curve* C_t *is ordinary and the Jacobian* J_t *is pre-*W_2*-canonical.*

Proof. Let p be any prime number with $p \equiv 1 \bmod m$. Note that in this case $R/\mathfrak{p} = \mathbb{F}_p$ for any prime $\mathfrak{p} \subset R$ above p. We write $T \otimes \mathbb{F}_p$ for $T \otimes_R (R/\mathfrak{p})$. By [4], Prop. 7.4, there is a Zariski open $U \subset T \otimes \mathbb{F}_p$ such that C_t is ordinary for all $t \in U(k)$. On the other hand, by a theorem of Noot [18], [19], in the slightly more precise formulation of [13], Thm. 4.2, the assumption that $Z = Z(m, N, a)$ is special implies that for p large enough and $t \in T_0(k)$ any ordinary point, the canonical lifting of J_t gives a $W(k)$-valued point of Z. In particular, J_t is then pre-W_2-canonical. □

(5.7) For most choices of (m, N, a) the general member in our family of curves $C \to T$ is not hyperelliptic. In this case we may, and will, choose p and U in Lemma 5.6 such that the curves C_t with $t \in U(k)$ are non-hyperelliptic.
It may happen, however, that $Z(m, N, a)$ is fully contained in the hyperelliptic locus, in which case we call (m, N, a) a hyperelliptic triple. This occurs, for instance, if $m = 2m'$ is even and a is of the form $(a_1, a_2, m', \ldots, m')$, or if $N = 4$ and $a = (1, 1, m-1, m-1)$. In such a case we will just choose p and U as in Lemma 5.6.

The following variant of Prop. 5.3 is the essential tool in our proof of Theorem 3.6. Let p and U be chosen as above, and let $C_U \to U$ be the restriction of C/T to U. With notation as in 2.5 and 5.1 we have eigenspace decompositions $\mathscr{Q}(C_U/U) = \oplus_{n\in\mathbb{Z}/m\mathbb{Z}}\, \mathscr{Q}_{(n)}$; likewise for other $\mathscr{O}_U[\mu_m]$-modules such as $\mathscr{K}(C_U/U)$ and $\mathbb{E}_U = \mathbb{E}(C_U/U)$. Accordingly we can write $\tilde{\beta}_{C_U/U} = \sum_n \tilde{\beta}_{(n)}$, with $\tilde{\beta}_{(n)}$ a section of $F_U^*\mathscr{Q}_{(n)}$.

(5.8) *Proposition. — With assumptions and notation as in* 5.4 *and* 5.7*, the composite map*

(5.8.1)

$$F_U^*\mathscr{K}_{(0)} \xhookrightarrow{\text{incl}} F_U^*\mathrm{Sym}^2(\mathbb{E}_U)_{(0)} \xrightarrow{\mathrm{Sym}^2(\gamma)} \mathrm{Sym}^2(\mathbb{E}_U)_{(0)} \xrightarrow{\mathrm{mult}_{(0)}} f_*(\omega_{C/U}^{\otimes 2})_{(0)}$$

is zero.

Proof. If (m, N, a) is non-hyperelliptic this is immediate from Prop. 5.3 together with (ii) of Lemma 5.5. So from now on we may assume that $Z(m, N, a)$ is contained in the hyperelliptic locus. Let $\iota \in \mathrm{Aut}(C_U/U)$ be the hyperelliptic involution. We remark that ι may or may not be contained in the subgroup $\mu_m \subset \mathrm{Aut}(C_U/U)$; by inspection of the hyperelliptic examples mentioned in 5.7 we see that both cases occur.

Let $\omega = \Omega^1_{C_U/U}$. In the hyperelliptic case the multiplication map $\mathrm{Sym}^2(\mathbb{E}_U) \to f_*(\omega^{\otimes 2})$ is no longer surjective. However, if we denote the invariants under the action of ι by a subscript "even",

$$\mathrm{mult}_{(\mathrm{even})} \colon \mathrm{Sym}^2(\mathbb{E}_U)_{(\mathrm{even})} \to f_*(\omega^{\otimes 2})_{(\mathrm{even})}$$

is again surjective; see for instance [21], Lemmas 2.12 and 2.13. The assumption that $Z(m, N, a)$ is fully contained in the hyperelliptic locus implies that $f_*(\omega^{\otimes 2})_{(0)} \subset f_*(\omega^{\otimes 2})_{(\mathrm{even})}$. Hence also $\mathrm{mult}_{(0)}$ is surjective, and we may view $\tilde{\beta}_{(0)}$ as an $\mathscr{O}_U$-linear map $F_U^*\mathscr{K}_{(0)} \to \mathscr{O}_U$.

Our assumptions imply that $\tilde{\beta}_{(0)}$, hence also $\nabla\tilde{\beta}_{(0)}$, is zero, so all that remains to be checked is that for the 0-component the analogue of Prop. 5.3 holds. For this we can follow the proof of [8], Prop. 3.2: The proof that loc. cit. diagram (3.2.9) is commutative does not use the assumption that the curves are non-hyperelliptic and therefore goes through in the hyperelliptic case. Moreover, in the notation of that proof, we can choose the lifted family $\boldsymbol{Y}/\boldsymbol{T}$ (where Y/T is our C_U/U) such that it has an action of μ_m. Taking 0-components in diagram (3.2.9) then gives that $-\nabla\tilde{\beta}_{(0)}$ equals the composition of (5.8.1) and $\mathrm{KS}_{(0)}$, and by (ii) of Lemma 5.5 we conclude that the map (5.8.1) is zero. □

(5.9) *Lemma. — Write $q = (p-1)/m$. Let $n \in \mathbb{Z}/m\mathbb{Z}$, and let $A = A_n(t) \in \mathrm{GL}_{d_n}(\mathscr{O}_U)$ be the matrix of the Cartier operator $\gamma^{-1}\colon \mathbb{E}_{U,(n)} \to F_U^*\mathbb{E}_{U,(n)}$ with regard to the frames*

$$\omega_{n,0}, \ldots, \omega_{n,d_n-1}\,, \quad \textit{respectively} \quad \omega_{n,0}\otimes 1, \ldots, \omega_{n,d_n-1}\otimes 1\,.$$

Then the matrix coefficient $A_{\rho,\sigma}$*, for* ρ*,* $\sigma \in \{0,\ldots,d_n-1\}$*, equals*

$$(5.9.1)\qquad (-1)^{\Sigma}\cdot \sum_{j_1+\cdots+j_N=\Sigma} \binom{q\cdot[-na_1]_m}{j_1}\cdots\binom{q\cdot[-na_N]_m}{j_N}\cdot t_1^{j_1}\cdots t_N^{j_N}\,,$$

where $\Sigma = (d_n-\sigma)(p-1)+(\rho-\sigma)$*.*

Proof. This is the dual version of [4], Lemma 5.1, part (i). □

We remark that the result of Bouw in [4] is valid in a more general context. She uses this to prove the existence of cyclic covers whose p-rank reaches a natural upper bound imposed by the local monodromy data; see [4], Thm. 6.1.

6. Proof of the main result: four branch points

In this section we prove Theorem 3.6 in the case $N=4$. Let us first try to explain the idea of the argument, by way of guide for the reader.
Assume we have a triple (m,N,a) that is not one of the twenty examples in Table 1 but such that $Z(m,N,a)$ is special. We want to show that this is impossible. We have the family of curves $C\to T$ over a ring R of finite type over $\mathbb{Z}$; we then consider the reduction modulo p, with p chosen as in 5.7. The nontrivial information we have, exploiting the assumption that $Z(m,N,a)$ is special, is that this gives a family of ordinary Jacobians in characteristic p such that the canonical liftings over $W_2(k)$ are again Jacobians. In Prop. 5.8 we have translated this, based on the theory in [8], into the vanishing of a certain abstractly defined map. Lemma 5.9 enables us to calculate this map explicitly. To apply this, we need a differential form that gives us an element in the source of the map (5.8.1); we write down such a form in 6.2 below. The fact that the image of this element is zero then gives us a polynomial identity (6.2.1). By some combinatorial arguments we then show that this identity cannot hold if (m,N,a) is not equivalent to one of the twenty special triples in Table 1.

(6.1) We retain the assumptions made in 5.4. In addition we assume $N=4$. Let

$$\mathscr{D}(m,a) := \bigl\{\pm n\in I(m)\bigm| d_n=d_{-n}=1\bigr\}\,.$$

(Here $I(m)$ is as defined in (3.2.1) and d_n is given by (3.2.2). Though not indicated in the notation, d_n depends on a.)
If $\pm n\in\mathscr{D}(m,a)$, the equalities $d_n=d_{-n}=1$ imply that $na_i\not\equiv 0$ modulo m for all $i\in\{1,\ldots,4\}$. Hence,

$$(6.1.1)\qquad [-na_i]_m = m-[na_i]_m \quad\text{for all } i,\qquad \text{and}\qquad \sum_{i=1}^{4}[-na_i]_m = 2m\,,$$

where we recall that $[b]_m$ denotes the representative of the class (b mod m) in $\{0,1,\ldots,m-1\}$.

We first observe that $\dim S(\mu_m) > 1$. Indeed, if $\dim S(\mu_m) = 1$ then (4.8.1) holds, and by the results of [22], Chapter 6, (m, N, a) is one of the triples in Table 1, which contradicts our assumptions.
For $n \in \mathbb{Z}/m\mathbb{Z}$ we have $d_n + d_{-n} \leqslant 2$, and if m is even then $d_{\frac{m}{2}} \leqslant 1$. The inequality $\dim S(\mu_m) > 1$ is therefore equivalent to the fact that $\#\mathscr{D}(m,a) \geqslant 2$. Choose two distinct pairs $\pm n$ and $\pm n'$ in $\mathscr{D}(m,a)$. Note that if m is even, we may have $n = -n$ or $n' = -n'$.

(6.2) Choose p and U as in Lemma 5.6, where we may further assume that the curves C_t for $t \in U(k)$ are either all non-hyperelliptic or all hyperelliptic. We keep the notation introduced in the previous section; in particular we recall that $\mathscr{K}(C_U/U) = \oplus_{n\in\mathbb{Z}/m\mathbb{Z}}\mathscr{K}_{(n)}$.
It follows from (6.1.1) and the definition of the forms $\omega_{n,\nu}$ in (2.6.1) that

$$\eta := \omega_{n,0} \otimes \omega_{-n,0} - \omega_{n',0} \otimes \omega_{-n',0}$$

is a section of $\mathscr{K}_{(0)}$. For $\nu \in \{\pm n, \pm n'\}$ the matrix $A_\nu = A_\nu(t)$ of Lemma 5.9 is a polynomial in $\mathbb{F}_p[t_1,\ldots,t_4]$. As the Jacobians of the curves C_t for $t \in U(k)$ are ordinary, the Cartier operator γ^{-1} in Lemma 5.9 is an isomorphism of vector bundles, so $A_\nu(t)$ is invertible as a section of $\mathscr{O}_U$. Because $\omega_{n,0}\cdot\omega_{-n,0} = \omega_{n',0}\cdot\omega_{-n',0}$ is a non-zero section of $f_*(\omega^{\otimes 2})$, it follows from Prop. 5.8 that

$$A_n \cdot A_{-n} = A_{n'} \cdot A_{-n'} \tag{6.2.1}$$

as polynomials.
Define $B_\nu := A_\nu|_{t_1=0}$, the polynomial obtained from A_ν by substituting $t_1 = 0$. Explicitly,
(6.2.2)

$$B_\nu = (-1)^{p-1} \cdot \sum_{j_2+j_3+j_4=p-1} \binom{q\cdot[-\nu a_2]_m}{j_2} \cdots \binom{q\cdot[-\nu a_4]_m}{j_4} \cdot t_2^{j_2} t_3^{j_3} t_4^{j_4}\,.$$

Fix an index $\iota \in \{2,3,4\}$, and write $\{1,2,3,4\} = \{1,\iota\} \amalg \{\kappa,\lambda\}$. Let $v_n(\iota)$ be the largest integer v such that B_n is divisible by t_ι^v. From (6.2.2) and (6.1.1) we find

$$\begin{aligned} v_n(\iota) &= \max\bigl\{0, (p-1) - q\cdot[-na_\kappa]_m - q\cdot[-na_\lambda]_m\bigr\} \\ &= \max\bigl\{0, q\cdot[na_\kappa]_m + q\cdot[na_\lambda]_m - (p-1)\bigr\}\,, \end{aligned}$$

and similarly for $v_{-n}(\iota)$.
Next let $w_{\pm n}(\iota)$ be the largest integer w such that $B_n \cdot B_{-n}$ is divisible by t_ι^w. We find

$$\begin{aligned} w_{\pm n}(\iota) = \max&\bigl\{0, q\cdot[na_\kappa]_m + q\cdot[na_\lambda]_m - (p-1)\bigr\} \\ &+ \max\bigl\{0, q\cdot[-na_\kappa]_m + q\cdot[-na_\lambda]_m - (p-1)\bigr\}\,, \end{aligned}$$

which by (6.1.1) we can rewrite as

$$\begin{aligned} w_{\pm n}(\iota) &= \max\bigl\{0, q\cdot[na_\kappa]_m + q\cdot[na_\lambda]_m - (p-1)\bigr\} \\ &\quad + \max\bigl\{0, q\cdot[na_1]_m + q\cdot[na_\iota]_m - (p-1)\bigr\} \\ &= q\cdot\max\bigl\{[na_1]_m + [na_\iota]_m, [na_\kappa]_m + [na_\lambda]_m\bigr\} - (p-1)\,. \end{aligned} \tag{6.2.3}$$

(6.3) *Lemma.* — *Consider two 4-tuples* (b_1, b_2, b_3, b_4) *and* (b'_1, b'_2, b'_3, b'_4) *in* $\{1, \ldots, m-1\}^4$ *with* $\sum_{i=1}^4 b_i = 2m = \sum_{i=1}^4 b'_i$. *Suppose that for all partitions* $\{1,2,3,4\} = \{1,\iota\} \amalg \{\kappa,\lambda\}$ *we have* $\{b_1 + b_\iota, b_\kappa + b_\lambda\} = \{b'_1 + b'_\iota, b'_\kappa + b'_\lambda\}$ *as sets. Then there is an even permutation* $\sigma \in A_4$ *of order* 2 *such that either* $b'_i = b_{\sigma(i)}$ *for all* i *or* $b'_i = m - b_{\sigma(i)}$ *for all* i.

Proof. Straightforward checking of all $8 = 2^3$ possible combinations (two for each partition). □

(6.4) The relation (6.2.1) implies that for any partition $\{1,2,3,4\} = \{1,\iota\} \amalg \{\kappa,\lambda\}$ we have $w_{\pm n}(\iota) = w_{\pm n'}(\iota)$. Since $\sum_{i=1}^4 [na_i]_m = 2m = \sum_{i=1}^4 [n'a_i]_m$, it follows from (6.2.3) that

$$\big\{[na_1]_m + [na_\iota]_m, [na_\kappa]_m + [na_\lambda]_m\big\} = \big\{[n'a_1]_m + [n'a_\iota]_m, [n'a_\kappa]_m + [n'a_\lambda]_m\big\}$$

as sets. By the lemma it follows, possibly after replacing n by $-n$, which we may do, that there is an even permutation $\sigma \in A_4$ of order 2 such that $[n'a_i]_m = [na_{\sigma(i)}]_m$ for all i. As the pairs $\pm n$ and $\pm n'$ are distinct, $\sigma \neq 1$. Possibly after a permutation of the indices we may therefore assume that

$$\begin{aligned} &[n'a_1]_m = [na_2]_m\,, \qquad [n'a_3]_m = [na_4]_m\,, \\ &[n'a_2]_m = [na_1]_m\,, \qquad [n'a_4]_m = [na_3]_m\,. \end{aligned} \tag{6.4.1}$$

Since $\gcd(m, a_1, \ldots, a_4) = 1$ this implies that $\gcd(m,n) = \gcd(m,n')$.

(6.5) Let $r = \gcd(n,m)$. Let $m' = m/r$, and consider the triple (m', N', a') obtained from (m,N,a) by reduction modulo m'. Then we have a bijection $\mathscr{D}(m,a) \xrightarrow{\sim} \mathscr{D}(m',a')$ by $(\pm n) \mapsto (\pm \frac{n}{r})$. Hence $\#\mathscr{D}(m',a') \geqslant 2$. In particular, $N' = 4$, and (m',N',a') is not equivalent to one of the triples listed in Table 1. By our minimality assumption on (m,N,a), see 5.4, it therefore follows that $r = 1$. Hence we may replace the 4-tuple a by $n'a = (n'a_1, \ldots, n'a_4)$, which means we may set $n' = 1$ in the above. In this case, (6.4.1) tells us that $n^2 = 1$ in $(\mathbb{Z}/m\mathbb{Z})$, and the 4-tuple a has the form $a = (a_1, na_1, a_3, na_3)$ with $n \neq \pm 1$ and

$$(n+1)(a_1 + a_3) = 2m\,. \tag{6.5.1}$$

From these relations we want to deduce that there is a pair $\pm\nu \in \mathscr{D}(m,a)$ with $\gcd(m,\nu) \neq 1$, thereby obtaining a contradiction. Write $m = 2^k \cdot M$ with M odd.

First assume $n \not\equiv -1$ modulo M. For an odd prime number ℓ and an exponent $e \geqslant 1$, the congruence $n^2 \equiv 1 \bmod \ell^e$ only has $n \equiv \pm 1$ as solutions. Hence there is an odd prime divisor ℓ of m such that $n \not\equiv -1 \bmod \ell$. But then (6.5.1) gives $a_1 + a_3 \equiv 0 \bmod \ell$, and since $\gcd(m, a_1, \ldots, a_4) = 1$ we further have $a_1 \not\equiv 0 \bmod \ell$ and $a_3 \not\equiv 0 \bmod \ell$. Taking $\nu := m/\ell$ we find that $\pm\nu \in \mathscr{D}(m,a)$; contradiction.

The only remaining possibility is that $n \equiv -1$ modulo M, and therefore $n \not\equiv -1 \bmod 2^k$. In particular, $k \geqslant 2$. In this case (6.5.1) implies $a_1 + a_3 \equiv 0 \bmod 4$, in which case $\pm m/4 \in \mathscr{D}(m,a)$; contradiction. This completes the proof of Thm. 3.6 in the case $N = 4$.

7. Proof of the main result: five or more branch points

We now turn to the case $N \geqslant 5$. The idea behind the proof is the same as in the previous section, but there are some additional difficulties. In 7.2 and 7.3 we prove two technical results. Once we have these, we can again write down elements in the source of the map (5.8.1). Similar to what we did in Section 6, this gives us polynomial identities (7.4.1), and with some elementary combinatorial arguments we can then conclude the proof.

(7.1) *Assumptions.* — We retain the assumptions made in 5.4. In addition we now assume $N \geqslant 5$. Again we assume (m, N, a) is minimal. Because we have already proven Thm. 3.6 for $N = 4$, it is again true that if m' is a proper divisor of m and (m', N', a') is obtained from (m, N, a) by reduction modulo m', either $N' \leqslant 3$ or (m', N', a') is equivalent to one of the twenty triples listed in Table 1.

(7.2) *Lemma.* — *With assumptions as in* 7.1*, there exists an index $n \in (\mathbb{Z}/m\mathbb{Z})^*$ such that $\{d_n, d_{-n}\} \neq \{0, N-2\}$.*

With the terminology introduced in 4.3, the lemma says that the new part of the local system $\mathbb{V}$ (as in Section 4) is not isotrivial.

Proof. We assume $\{d_n, d_{-n}\} = \{0, N-2\}$ for all $n \in (\mathbb{Z}/m\mathbb{Z})^*$, and we seek to derive a contradiction. It will be convenient to consider the function $\delta_a \colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}_{\geqslant 0}$ given by $\delta_a(n) = \sum_{i=1}^N \left\langle \frac{-na_i}{m} \right\rangle$. Note that for $n \neq 0$ the d_n defined in (3.2.2) equals $-1 + \delta_a(n)$. For $n \in (\mathbb{Z}/m\mathbb{Z})^*$ we have $\delta_a(n) \geqslant 1$ and $\delta_a(n) + \delta_a(-n) = N$. Our assumption is equivalent to the condition that

$$\{\delta_a(n), \delta_a(-n)\} = \{1, N-1\} \quad \text{for all } n \in (\mathbb{Z}/m\mathbb{Z})^* . \tag{7.2.1}$$

Possibly after replacing $a = (a_1, \ldots, a_N)$ by $-a$, we may assume $\delta_a(1) = 1$, which means that

$$[a_1]_m + \cdots + [a_N]_m = m \,. \tag{7.2.2}$$

We divide the proof into a couple of steps.

Step 1. Our first goal is to show that $m > 60$. For a given m, (7.2.2) leaves only finitely many possible triples (m, N, a), up to equivalence. With the help of a small computer program we check that for $m \leqslant 60$ the only two possibilities with $N \geqslant 5$ and $\{\delta_a(n), \delta_a(-n)\} = \{1, N-1\}$ for all $n \in (\mathbb{Z}/m\mathbb{Z})^*$ are given (up to equivalence) by

$$m = 6\,, \quad N = 5\,, \quad a = (1,1,1,1,2)\,; \tag{7.2.3}$$

$$(7.2.4) \qquad m = 6\,, \quad N = 6\,, \quad a = (1,1,1,1,1,1)\,.$$

So it remains to show that for these triples, $Z(m,N,a)$ is not special.
In case (7.2.3), we have $g = 7$ and the family of Jacobians $J \to T$ decomposes, up to isogeny, as a product of three factors: $J \sim Y_1 \times Y_2 \times Y_3$, with

— Y_1 a pull-back of the Legendre family of elliptic curves, which is Example 1 in Table 1; this is the old factor corresponding to the divisor 2 of m,
— Y_2 a pull-back of Example 6; this is the old factor corresponding to the divisor 3 of m,
— Y_3 the new part.

(The new part Y_3 is in fact an isotrivial family of 3-dimensional abelian varieties of CM type, but we will not need this.) Let $b \in T(\mathbb{C})$ be a Hodge-generic point. The fibre $Y_{1,b}$ is an elliptic curve with endomorphism ring $\mathbb{Z}$; its Hodge group is isomorphic with SL_2. The fibre $Y_{2,b}$ is an abelian threefold that is easily seen to be simple. (E.g., use the fact that Example 6 is special, together with [23], Thm. 5.) By [16], Prop. 3.8 the Hodge group of $Y_{1,b} \times Y_{2,b}$ is the product of the two Hodge groups. Hence the smallest special subvariety $S \subset \mathscr{A}_7$ that contains $Z(m,N,a)$ has dimension at least $1+2=3$ (see 1.5), and since $N-3 = 2 < 3$ this means that $Z(m,N,a)$ is not special.
In case (7.2.4), we have $g = 10$ and the family of Jacobians $J \to T$ decomposes, up to isogeny, as a product of three factors: $J \sim Y_1 \times Y_2 \times Y_3$, with

— Y_1 a pull-back of Example 2; this is the old factor corresponding to the divisor 2 of m,
— Y_2 a pull-back of Example 10; this is the old factor corresponding to the divisor 3 of m,
— Y_3 the new part.

(In this case the new part Y_3 is an isotrivial family of 4-dimensional abelian varieties of CM type; again we will not need this.) For a Hodge-generic point $b \in T(\mathbb{C})$ the fibre $Y_{1,b}$ is an abelian surface with endomorphism ring $\mathbb{Z}$; its Hodge group $H_1 = \mathrm{Hdg}(Y_{1,b})$ is isomorphic with Sp_4. The fibre $Y_{2,b}$ is an abelian fourfold. By Thm. 1.1 of [26] we have $\mathrm{End}(Y_{2,b}) = \mathbb{Z}[\zeta_3]$, and the tangent multiplicities for the factor Y_2 (=Example 10) are given by $d_{(1 \bmod 3)} = 3$ and $d_{(2 \bmod 3)} = 1$. By [15], 7.4, it follows that for the generic Hodge group $H_2 = \mathrm{Hdg}(Y_{2,b})$ we have $H_{2,\mathbb{R}} \cong \mathrm{U}(1,3)$. If $H = \mathrm{Hdg}(J_b)$ is the generic Hodge group in our family of Jacobians, H projects surjectively to H_1 and H_2. It follows that among the simple factors of $H_{\mathbb{R}}^{\mathrm{ad}}$ both a factor PSp_4 and a factor $\mathrm{PSU}(1,3)$ occur; this implies that the smallest special subvariety $S \subset \mathscr{A}_7$ that contains $Z(m,N,a)$ has dimension at least $3+3=6$ (again see 1.5), and since $N-3 = 3 < 6$ this means that $Z(m,N,a)$ is not special.

Step 2. The function δ_a has the property that $\delta_a(n_1+n_2) \leqslant \delta_a(n_1) + \delta_a(n_2)$. In particular, if n_1, n_2 and n_1+n_2 are all in $(\mathbb{Z}/m\mathbb{Z})^*$ then by (7.2.1) we have the implication

$$(7.2.5) \qquad \delta_a(n_1) = \delta_a(n_2) = 1 \quad \Rightarrow \quad \delta_a(n_1+n_2) = 1\,.$$

Step 3. Next we show that m is not divisible by 2, 3 or 5. Let $p \in \{2, 3, 5\}$, and suppose m is divisible by p. Let $m' = m/p$ and let (m', N', a') be obtained from (m, N, a) by reduction modulo m'. The new triple cannot be one of the examples listed in Table 1, for this would imply (by inspection of the table) that $m = p \cdot m' \leqslant 5 \cdot 12 = 60$, which we have excluded. Hence our minimality assumption on the triple (m, N, a) implies that $N' \leqslant 3$.

Since $N \geqslant 5$, there are at least two indices i such that $a_i \equiv 0$ modulo m'. For $p = 2$ this contradicts (7.2.2). Hence $2 \in (\mathbb{Z}/m\mathbb{Z})^*$ and by repeated application of (7.2.5), starting from $\delta_a(1) = 1$, we find that $\delta_a(2^k) = 1$ for all k.

For $p = 3$ the only possibility left, in view of (7.2.2), is that there are precisely two indices i with $[a_i]_m = m/3$ and that $[a_i]_m < m/3$ for all remaining indices. This contradicts the fact that $\delta_a(2) = 1$. Hence 3 does not divide m.

Finally take $p = 5$. The fact that $\delta_a(2) = 1$ implies that there is a unique index i with $[a_i]_m > m/2$ and that $[a_i]_m < m/2$ for all remaining indices. Since $N \geqslant 5$ and $N' \leqslant 3$ this leaves (possibly after a permutation of the indices) two possibilities: either

$$[a_1]_m = 3m/5\,, \quad [a_2]_m = m/5\,, \quad [a_i]_m < m/5 \quad \text{for all } i > 2,$$

or

$$m/2 < [a_1]_m < 3m/5\,, \quad [a_2]_m = [a_3]_m = m/5\,, \quad [a_i]_m < m/5 \quad \text{for all } i > 3.$$

In both cases we get a contradiction with the fact that $\delta_a(4) = 1$.

Step 4. We now show that m has at most four distinct prime divisors. To see this, let p be any prime divisor of m, let $m' = m/p$ and let (m', N', a') be obtained from (m, N, a) by reduction modulo m'. If the new triple is one of the examples listed in Table 1, it can only be Example 17, for otherwise inspection of the table gives that m' (and hence m) is divisible by 2, 3, or 5, which we have excluded. Example 17 has $N' = 4$ branch points, so this fact, together with our minimality assumption on the triple (m, N, a), implies that $N' \leqslant 4$.

The previous argument shows that for any prime divisor p of m, there are at most 4 indices i such that a_i is not divisible by m/p. On the other hand, $a_i \not\equiv 0 \bmod m$, so for a given index i there can be at most one prime divisor p of m such that a_i is divisible by m/p. As $N \geqslant 5$ it follows that m has at most four distinct prime divisors.

Step 5; conclusion of the proof. Combining the conclusion of Step 3 with (7.2.5), we find that for all $\rho \in \{1, 2, 3, 4, 5\}$ we have $(\rho \bmod m) \in (\mathbb{Z}/m\mathbb{Z})^*$ and $\delta_a(\rho \bmod m) = 1$.

Let ν be an integer such that $\gcd(m, \nu) = 1$ and $\delta_a(\nu \bmod m) = 1$. Let ρ be the smallest positive integer such that $\gcd(m, \nu + \rho) = 1$. The fact that m has at most four distinct prime divisors, all greater than 5, implies that $\rho \leqslant 5$. But then $\gcd(\rho, m) = 1$ and from (7.2.5) we get that $\delta_a(\nu + \rho \bmod m) = 1$. Repeating this, we find that $\delta_a(n) = 1$ for all $n \in (\mathbb{Z}/m\mathbb{Z})^*$, which contradicts the fact that $\delta_a(n) + \delta_a(-n) = N > 3$. This completes the proof of the lemma. $\square$

(7.3) Our next goal is to show there exist two distinct pairs $\pm n$ and $\pm n'$ in $I(m)$ with

$$d_{-n} = d_{-n'} = 1\,, \quad \text{and} \quad d_n = d_{n'} = N-3\,. \tag{7.3.1}$$

(In particular, $n \not\equiv 0$ and $n' \not\equiv 0$.) For this we work over $\mathbb{C}$ and we consider the generic Mumford-Tate group M of the family C/T. As in 1.5, let $M_{\mathbb{R}}^{\mathrm{ad}} = Q_1 \times \cdots \times Q_r$ be the decomposition of $M_{\mathbb{R}}^{\mathrm{ad}}$ as a product of simple factors. The assumption that $Z(m,N,a)$ is special means that $N-3 = \sum_{i=1}^r d(Q_i)$, with notation as in 1.5. Further, this assumption implies that the connected algebraic monodromy group Mon^0 of the family is a normal subgroup of M; in particular, $\mathrm{Mon}_{\mathbb{R}}^{0,\mathrm{ad}} = \prod_{i\in K} Q_i$ for some subset $K \subset \{1,\ldots,r\}$.
By Lemma 7.2 there exists an index n in $(\mathbb{Z}/m\mathbb{Z})^*$ with $\{d_n, d_{-n}\} \neq \{0, N-2\}$. By Prop. 4.7 it follows that one of the simple factors Q_i, say Q_1, is a $\mathrm{PSU}(d_n, d_{-n})$, which gives $d(Q_1) = d_n d_{-n}$. Because $n \in (\mathbb{Z}/m\mathbb{Z})^*$ we have $d_n + d_{-n} = N-2$; hence $d_n d_{-n} \geqslant N-3$ with equality of and only if $\{d_n, d_{-n}\} = \{1, N-3\}$. Possibly after replacing n by $-n$ we therefore have $d_n = N-3$ and $d_{-n} = 1$. Further, the relation $N-3 = \sum_{i=1}^r d(Q_i)$ implies that all other simple factors $Q_2,\ldots,Q_r$ are anisotropic (i.e., compact).
Our assumptions imply that there is another index pair $\pm n' \in I(m)$ with $d_{n'} \neq 0$ and $d_{-n'} \neq 0$, for if this is not the case then (m,N,a) satisfies (4.8.1), which implies it is one of the examples of Table 1. If $m = 2m'$ is even and $n' = m'$ then by Prop. 4.7 one of the factors Q_i is a PSp_{2h} with $h = d_{n'} > 0$. As $N-3 \geqslant 2$, this factor cannot be the factor $Q_1 = \mathrm{PSU}(1, N-3)$, and since PSp_{2h} is not anisotropic we arrive at a contradiction. So $n' \neq -n'$, and, again by Prop. 4.7, one of the Q_i is a non-compact unitary factor $\mathrm{PSU}(d_{n'}, d_{-n'})$. This factor must be the factor Q_1; hence $\{d_{n'}, d_{-n'}\} = \{1, N-3\}$, which gives what we want.

(7.4) Consider two distinct pairs $\pm n$ and $\pm n'$ in $I(m)$ for which (7.3.1) holds. Let $\Gamma \in \mathrm{GL}_{N-3}(\mathscr{O}_U)$ be the matrix of $\gamma_{(n)}\colon F_U^*\mathbb{E}_{U,(n)} \to \mathbb{E}_{U,(n)}$ with regard to the frames given by the forms $\omega_{n,\sigma}$. It is the inverse of the matrix $A = A_n$ of Lemma 5.9. Similarly, let Γ' be the matrix of $\gamma_{(n')}$, and let $A' = A_{n'}$ be its inverse. Further, let c and c' be the sections of $\mathscr{O}_U^*$ (the inverses of the 1×1 matrices A_{-n} and $A_{-n'}$ of Lemma 5.9) such that $\gamma(\omega_{-n,0}\otimes 1) = c\cdot\omega_{-n,0}$ and $\gamma(\omega_{-n',0}\otimes 1) = c\cdot\omega_{-n',0}$.
For $\sigma \in \{0,1,\ldots,N-4\}$, let $\eta_\sigma \in \Gamma(U, \mathscr{K}_{(0)})$ be given by

$$\eta_\sigma := \omega_{-n,0}\otimes\omega_{n,\sigma} - \omega_{-n',0}\otimes\omega_{n',\sigma}\,.$$

As $\omega_{-n,0}\cdot\omega_{n,\rho} = \omega_{-n',0}\cdot\omega_{n',\rho}$ as sections of $f_*(\omega^{\otimes 2})$, the image of η_σ under $\mathrm{Sym}^2(\gamma)$ equals

$$\sum_{\rho=0}^{N-4} \bigl(c\cdot\Gamma_{\rho,\sigma} - c'\cdot\Gamma'_{\rho,\sigma}\bigr)\cdot(\omega_{-n,0}\cdot\omega_{n,\rho})\,.$$

Because the sections $\omega_{-n,0} \cdot \omega_{n,\rho}$ for $\rho \in \{0, \ldots, N-4\}$ are linearly independent, it follows from Prop. 5.8 that $c \cdot \Gamma_{\rho,\sigma} - c' \cdot \Gamma'_{\rho,\sigma}$ for all σ, $\rho \in \{0, 1, \ldots, N-4\}$, which can be rewritten as

$$c^{-1} \cdot A_{\rho,\sigma} = c^{\prime,-1} \cdot A'_{\rho,\sigma} \,. \tag{7.4.1}$$

Choose two distinct indices κ, λ in $\{1, 2, \ldots, N\}$, and write $\{1, \ldots, N\} = \{\kappa, \lambda\} \amalg I$. For $\nu \in \{0, 1\}$, define $v_n(\nu)$ to be the largest integer v such that $A_{\nu,\nu}|_{t_\kappa=0}$ is divisible by t_λ^v. Similarly, let v_{-n} be the largest integer v such that $c^{-1}|_{t_\kappa=0}$ is divisible by t_λ^v. Using the explicit formulas for c^{-1} and the matrix A from Lemma 5.9, we find

$$\begin{aligned} v_{-n} &= \max\Big\{0, (p-1) - q \cdot \sum_{i \in I} [na_i]_m\Big\}\,, \\ v_n(0) &= \max\Big\{0, (N-3)(p-1) - q \cdot \sum_{i \in I} [-na_i]_m\Big\}\,, \\ v_n(1) &= 0\,. \end{aligned}$$

(Recall that $q = (p-1)/m$.)
Next we define $w_n(\nu) = v_{-n} + v_n(\nu)$ to be the largest integer w such that $\big(c^{-1} \cdot A_{\nu,\nu}\big)|_{t_\kappa=0}$ is divisible by t_λ^w. Similar to (6.1.1), it follows from the fact that $d_{-n} = 1$ and $d_n = N-3$ that $[-na_i]_m = m - [na_i]_m$ for all i and $\sum_{i=1}^N [na_i]_m = 2m$. Using these relations we obtain

$$\begin{aligned} w(0) &= \max\Big\{(p-1) - q \cdot \sum_{i \notin I} [na_i]_m, (p-1) - q \cdot \sum_{i \in I} [na_i]_m\Big\} \\ &= \Big|(p-1) - q \cdot \sum_{i \notin I} [na_i]_m\Big| = q \cdot \big|m - [na_\kappa]_m - [na_\lambda]_m\big|\,, \\ w(1) &= \max\Big\{0, (p-1) - q \cdot \sum_{i \in I} [na_i]_m\Big\} \\ &= \max\Big\{0, (p-1) - q \cdot \sum_{i \notin I} [na_i]_m\Big\} = q \cdot \max\big\{0, [na_\kappa]_m + [na_\lambda]_m - m\big\}\,. \end{aligned}$$

We can do the same calculations for the pair $\pm n'$; let us call $w'(0)$ and $w'(1)$ the resulting values. From (7.4.1) we get the relations $w(0) = w'(0)$ and $w(1) = w'(1)$. It follows that for all choices of κ and λ we have $[na_\kappa]_m + [na_\lambda]_m = [n'a_\kappa]_m + [n'a_\lambda]_m$. This readily implies that $[na_i]_m = [n'a_i]_m$ for all $i \in \{1, \ldots, N\}$. As $\gcd(m, a_1, \ldots, a_N) = 1$ it follows that $n = n'$, which contradicts our assumption that the pairs $\pm n$ and $\pm n'$ are distinct. This completes the proof of Theorem 3.6. $\square$

References

[1] N. A'Campo, *Tresses, monodromie et le groupe symplectique.* Comment. Math. Helv. 54 (1979), 318–327.

[2] J. Achter, R. Pries, *The integral monodromy of hyperelliptic and trielliptic curves.* Math. Ann. 338 (2007), 187–206.

[3] Y. André, *Mumford-Tate groups of mixed Hodge structures and the theorem of the fixed part.* Compositio Math. 82 (1992), 1–24.

[4] I. Bouw, *The p-rank of ramified covers of curves.* Compositio Math. 126 (2001), 295–322.

[5] C. Chevalley, A. Weil, *Über das Verhalten der Integrale 1. Gattung bei Automorphismen des Funktionenkörpers.* Abh. Math. Semin. Univ. Hambg. 10 (1934), 358–361.

[6] J. de Jong, R. Noot, *Jacobians with complex multiplication.* In: Arithmetic algebraic geometry (Texel, 1989), Progr. Math. 89, Birkhäuser, 1991, pp. 177–192.

[7] P. Deligne, G. Mostow, *Monodromy of hypergeometric functions and non-lattice integral monodromy.* Inst. Hautes Études Sci. Publ. Math. 63 (1986), 5–89.

[8] B. Dwork, A. Ogus, *Canonical liftings of Jacobians.* Compositio Math. 58 (1986), 111–131.

[9] N. Katz, *Serre-Tate local moduli.* In: Algebraic surfaces, Lecture Notes in Math. 868, Springer-Verlag, 1981, pp. 138–202.

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

[11] B. Moonen, *Special points and linearity properties of Shimura varieties.* PhD thesis, University of Utrecht, 1995.

[12] B. Moonen, *Linearity properties of Shimura varieties. I.* J. Alg. Geom. 7 (1998), 539–567.

[13] B. Moonen, *Linearity properties of Shimura varieties. II.* Compositio Math. 114 (1998), 3–35.

[14] B. Moonen, F. Oort, *The Torelli locus and special subvarieties.* Preprint, August 2010, 43pp.

[15] B. Moonen, Yu. Zarhin, *Hodge classes and Tate classes on simple abelian fourfolds.* Duke Math. J. 77 (1995), 553–581.

[16] B. Moonen, Yu. Zarhin, *Hodge classes on abelian varieties of low dimension.* Math. Ann. 315 (1999), 711–733.

[17] G. Mostow, *On discontinuous action of monodromy groups on the complex n-ball.* J. Amer. Math. Soc. 1 (1988), 555–586.

[18] R. Noot, *Hodge classes, Tate classes, and local moduli of abelian varieties.* PhD thesis, University of Utrecht, 1992.

[19] R. Noot, *Models of Shimura varieties in mixed characteristic.* J. Alg. Geom. 5 (1996), 187–207.

[20] R. Noot, *Correspondances de Hecke, action de Galois et la conjecture d'André-Oort (d'après Edixhoven et Yafaev).* Sém. Bourbaki, Exp. 942.

Astérisque 307 (2006), 165–197.
[21] F. Oort, J. Steenbrink, *The local Torelli problem for algebraic curves.* In: Journées de Géometrie Algébrique d'Angers, Sijthoff & Noordhoff, 1980, pp. 157–204.
[22] J. Rohde, *Cyclic coverings, Calabi-Yau manifolds and complex multiplication.* Lecture Notes in Math. 1975, Springer, 2009.
[23] G. Shimura, *On analytic families of polarized abelian varieties and automorphic functions.* Ann. of Math. (2) 78 (1963), 149–192.
[24] G. Shimura, *On purely transcendental fields of automorphic functions of several variable.* Osaka J. Math. 1 (1964), 1–14.
[25] A. Yafaev, *A conjecture of Yves André's.* Duke Math. J. 132 (2006), 393–407.
[26] Yu. Zarhin, *The endomorphism rings of Jacobians of cyclic covers of the projective line.* Math. Proc. Cambridge Philos. Soc. 136 (2004), 257–267.

Ben Moonen
University of Amsterdam
KdV Institute for Mathematics
PO Box 94248
1090 GE Amsterdam
The Netherlands