LMS J. Comput. Math. 14 (2011) 179–199 © 2011 Author
doi:10.1112/S1461157010000410

Families of explicitly isogenous Jacobians of variable-separated curves

Benjamin Smith

Abstract

We construct six infinite series of families of pairs of curves (X, Y) of arbitrarily high genus, defined over number fields, together with an explicit isogeny from the Jacobian of X to the Jacobian of Y splitting multiplication by 2, 3 or 4. For each family, we compute the isomorphism type of the isogeny kernel and the dimension of the image of the family in the appropriate moduli space. The families are derived from Cassou-Noguès and Couveignes' explicit classification of pairs (f, g) of polynomials such that $f(x_1) - g(x_2)$ is reducible.

Supplementary materials are available with this article.

1. *Introduction*

Our goal in this article is to give algebraic constructions of explicit isogenies of Jacobians of high-genus curves; we are motivated by the scarcity of examples. Isogenies of Jacobians are special in genus greater than three, in the sense that quotients of Jacobians are generally not Jacobians. More precisely, if $\phi : J_X \to J_Y$ is an isogeny of Jacobians (that is, a geometrically surjective, finite homomorphism respecting the canonical principal polarisations), then its kernel is a maximal m-Weil isotropic subgroup of the m-torsion $J_X[m]$ for some integer m. On the other hand, if S is a subgroup of $J_X[m]$ satisfying this same property, then the quotient $J_X \to J_X/S$ is an isogeny of principally polarised abelian varieties, but in general J_X/S is only isomorphic to a Jacobian if the genus of X is at most three (see [**35**] and [**15**, Theorem 6]).

Nevertheless, families of non-isomorphic pairs of isogenous Jacobians of high-genus curves exist: recently Mestre [**33**] and the author [**41**] have constructed families of hyperelliptic examples. Here, we extend the results of [**41**] to derive new families of isogenies of non-hyperelliptic Jacobians in arbitrarily high genus. Theorem 1.1 summarises our results.

Definition 1. If ϕ is an isogeny with kernel isomorphic to a group G, then we say that ϕ is a G-isogeny. (The conventional notation replaces G with a tuple of its abelian invariants; but our notation is more useful in higher dimensions, where such tuples are typically very long.)

Definition 2. For all positive integers d and n, we define the integer $g_n(d)$ by

$$g_n(d) := \tfrac{1}{2}((n-1)(d-1) - (\gcd(n, d) - 1)).$$

Theorem 1.1. *For each integer $d > 1$ and for each row of Table 1, there exists a ν-dimensional family of explicit G-isogenies of Jacobians of curves of genus $g_n(d)$, defined over a CM field of degree e; and, if d is in S, then the generic fibre is an isogeny of absolutely simple Jacobians (here $\mathcal{P}$ denotes the set of primes).*

Proof. This follows from Propositions 8.1–14.1. □

Received 8 September 2010; revised 4 March 2011.

2000 Mathematics Subject Classification 14K02 (primary), 11G30, 11Y99 (secondary).

The proof of Theorem 1.1 is organised as follows: in Section 3, we associate a family of pairs of curves $(\mathcal{X}, \mathcal{Y})$ to each integer $d > 1$ and each pair of polynomials (Q_X, Q_Y) such that $Q_X(x_1) - Q_Y(x_2)$ has a non-trivial factorisation. We also give a correspondence $\mathcal{C}$ on $\mathcal{X} \times \mathcal{Y}$ inducing an explicit homomorphism $\phi_{\mathcal{C}} : \mathcal{J}_{\mathcal{X}} \to \mathcal{J}_{\mathcal{Y}}$. In Sections 4 and 5, we develop methods to determine the number of moduli and the kernel structure of $\phi_{\mathcal{C}}$. We recall the classification of Cassou-Noguès and Couveignes [**10**] in Section 6 and then apply our constructions to their polynomials in Sections 8–13. Finally, in Section 14, we list some values of d where $\mathcal{J}_{\mathcal{X}}$ and $\mathcal{J}_{\mathcal{Y}}$ are known to be absolutely simple.

Connections to prior work

The chief contribution of this work is the construction of non-hyperelliptic families: to our knowledge, all of the families of isogenies of Jacobians in genus $g > 3$ in the literature are of hyperelliptic Jacobians. The non-hyperelliptic families (those with $d > 2$) are all new. Technically, the main improvement over [**41**] is a more sophisticated approach to computing the action on differentials: this allows us to treat all $d > 1$ simultaneously, and to determine the isogeny kernel structures when $d > 2$ (the approach in [**41**] uses an explicit description of the 2-torsion specific to hyperelliptic curves). The hyperelliptic families (those with $d = 2$) all appear in earlier works: the families $\phi_{2,7}$, $\phi_{2,11}$, $\phi_{2,13}$, $\phi_{2,15}$, $\phi_{2,21}$ and $\phi_{2,31}$ are isomorphic to the 'linear construction' families in [**41**]. The subfamily of $\phi_{2,7}$ with $s_2 = 0$ and the fibre of $\phi_{2,11}$ at $s_2 = 0$ appear in Kux's thesis [**31**, Examples, pp. 59–60]. The endomorphisms of Proposition 7.1 with $d = 2$ are isomorphic to those described by Tautz, Top and Verberkmoes [**42**].

Notation

Throughout, K denotes a field of characteristic 0 and ζ_n denotes a primitive nth root of unity in $\overline{\mathbb{Q}}$ (and $\overline{K}$). Automorphisms of $K/\mathbb{Q}$ act on polynomials over K by acting on their coefficients: if $f(x) = \sum_i f_i x^i$, then $f^\sigma(x) = \sum_i f_i^\sigma x^i$.

Data files

Six files accompany this article (`degree-n.m`, for `n` in $\{7, 11, 13, 15, 21, 31\}$), containing the coefficients of the polynomials and matrices that appear in Sections 8–13. (These objects are too big to be useful in printed form: for example, the matrix $M_{30}(A_{31})$ in the proof of Proposition 13.1 is a 30×30 matrix over a sextic number field, with 436 non-zero entries.) Each file is a program in the Magma language [**4**, **5**], but they should be easily adaptable for use in other computational algebra systems; in any case, the reader need not be familiar with Magma to make use of the data. The files are available from the publisher's website.

Part I. General constructions

2. *Correspondences*

We begin with a brief review of the theory of correspondences. (See [**3**, § 11.5] and [**23**, § 16] for further detail.)

Table 1. *Values of n, ν, e, G, S for Theorem 1.1.*

n	ν	e	G	S
7	d	2	$(\mathbb{Z}/2\mathbb{Z})^{g_7(d)}$	$\mathbb{Z}_{\geqslant 2}$
11	$d-1$	2	$(\mathbb{Z}/3\mathbb{Z})^{g_{11}(d)}$	$\mathcal{P}\backslash\{11\}$
13	d	4	$(\mathbb{Z}/3\mathbb{Z})^{g_{13}(d)}$	$\mathbb{Z}_{\geqslant 2}$
15	d	2	$(\mathbb{Z}/4\mathbb{Z})^{g_{15}(d)-g_5(d)-g_3(d)} \times (\mathbb{Z}/2\mathbb{Z})^{2g_5(d)+2g_3(d)}$	$\mathcal{P}\backslash\{3, 5, 7\}$
21	$d-1$	2	$(\mathbb{Z}/4\mathbb{Z})^{g_{21}(d)-g_3(d)} \times (\mathbb{Z}/2\mathbb{Z})^{2g_3(d)}$	$\mathcal{P}\backslash\{3, 5, 7\}$
31	$d-1$	6	$((\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})^2 \times (\mathbb{Z}/2\mathbb{Z})^2)^{g_{31}(d)/3}$	$\mathcal{P}\backslash\{3, 5, 31\}$

https://doi.org/10.1112/S1461157010000410 Published online by Cambridge University Press

Let X and Y be (projective, irreducible, non-singular) curves over a field K, and let C be a curve on the surface $X \times Y$. The natural projections from $X \times Y$ restrict to morphisms $\pi_X^C : C \to X$ and $\pi_Y^C : C \to Y$, which in turn induce pullback and pushforward homomorphisms on divisor classes: in particular, we have homomorphisms

$$(\pi_X^C)^* : \mathrm{Pic}(X) \to \mathrm{Pic}(C) \quad \text{and} \quad (\pi_Y^C)_* : \mathrm{Pic}(C) \to \mathrm{Pic}(Y).$$

Both $(\pi_X^C)^*$ and $(\pi_Y^C)_*$ map degree-0 classes to degree-0 classes, and so induce homomorphisms of Jacobians (and, *a fortiori*, of principally polarised abelian varieties). Composing, we get a homomorphism of Jacobians

$$\phi_C := (\pi_Y^C)_* \circ (\pi_X^C)^* : J_X \longrightarrow J_Y;$$

we say that C *induces* ϕ_C. We emphasise that ϕ_C is completely explicit, given equations for C: we can evaluate $\phi_C(P)$ for any P in J_X by choosing a representative divisor from the corresponding class in $\mathrm{Pic}^0(X)$, pulling it back to C via $(\pi_X^C)^*$, and pushing the result forward onto Y via $(\pi_Y^C)_*$. Extending $\mathbb{Z}$-linearly so that $\phi_{C_1+C_2} = \phi_{C_1} + \phi_{C_2}$, we may take C to be an arbitrary divisor on $X \times Y$. We call divisors on $X \times Y$ *correspondences*.

The map $C \mapsto \phi_C$ defines a homomorphism $\mathrm{Div}(X \times Y) \to \mathrm{Hom}(J_X, J_Y)$; its kernel is generated by the principal divisors and the fibres of π_X and π_Y. The map is surjective: every homomorphism $\phi : J_X \to J_Y$ is induced by some correspondence Γ_ϕ on $X \times Y$ (we may take $\Gamma_\phi = (\phi \circ \alpha_X \times \alpha_Y)^* \mu^*(\Theta_Y)$, where $\alpha_X : X \hookrightarrow J_X$ and $\alpha_Y : Y \hookrightarrow J_Y$ are the canonical inclusions, Θ_Y is the theta divisor on J_Y and $\mu : J_Y \times J_Y \to J_Y$ is the subtraction map). We therefore have an isomorphism

$$\mathrm{Pic}(X \times Y) \cong \mathrm{Pic}(X) \oplus \mathrm{Pic}(Y) \oplus \mathrm{Hom}(J_X, J_Y).$$

Exchanging the roles of X and Y in the above, we obtain the image of ϕ_C under the Rosati involution:

$$\phi_C^\dagger = (\pi_X^C)_* \circ (\pi_Y^C)^* : J_Y \longrightarrow J_X.$$

(Recall that $\phi_C^\dagger := \lambda_X^{-1} \circ \hat{\phi}_C \circ \lambda_Y$, where $\hat{\phi}_C : \widehat{J}_Y \to \widehat{J}_X$ is the dual homomorphism and $\lambda_X : J_X \xrightarrow{\sim} \widehat{J}_X$ and $\lambda_Y : J_Y \xrightarrow{\sim} \widehat{J}_Y$ are the canonical principal polarisations.)

Composition of homomorphisms corresponds to fibred products of correspondences: if X, Y and Z are curves, and C and D are correspondences on $X \times Y$ and $Y \times Z$, respectively, then $C \times_Y D$ is a correspondence on $X \times Z$, and

$$\phi_D \circ \phi_C = \phi_{(C \times_Y D)}.$$

Let $\Omega(X)$ and $\Omega(Y)$ denote the $g_n(d)$-dimensional K-vector spaces of regular differentials on X and Y, respectively. The homomorphism $\phi_C : J_X \to J_Y$ induces a homomorphism of differentials

$$D(\phi_C) : \Omega(X) \longrightarrow \Omega(Y)$$

(see [39] for details). The image of a regular differential ω on X under $D(\phi_C)$ is

$$D(\phi_C)(\omega) = \mathrm{Tr}_{\Omega(Y)}^{\Omega(C)}(\omega),$$

where the inclusion $\Omega(X) \hookrightarrow \Omega(C)$ and the trace $\Omega(C) \to \Omega(Y)$ are induced by the natural inclusions of $K(X)$ and $K(Y)$ in $K(C)$. The map $\phi_C \mapsto D(\phi_C)$ extends to a faithful representation

$$D(\cdot) : \mathrm{Hom}(J_X, J_Y) \to \mathrm{Hom}(\Omega(X), \Omega(Y))$$

(the faithfulness depends on the fact that K has characteristic 0). We view differentials as row vectors, and homomorphisms as matrices acting by multiplication on the right. Composition of homomorphisms corresponds to matrix multiplication:

$$D(\phi_2 \circ \phi_1) = D(\phi_1) D(\phi_2)$$

https://doi.org/10.1112/S1461157010000410 Published online by Cambridge University Press

for all $\phi_1 : J_X \to J_Y$ and $\phi_2 : J_Y \to J_Z$. In particular, if $Y = X$, then $D(\cdot)$ is a representation of rings; in general, $D(\cdot)$ is a representation of left $\mathrm{End}(J_X)$- and right $\mathrm{End}(J_Y)$-modules.

EXAMPLE 1. Suppose that X is a curve with affine plane model $X : F(x, y) = 0$, and let x_1, y_1 and x_2, y_2 denote the coordinate functions on the first and second factors of $X \times X$, respectively. Our first example of a non-trivial correspondence is the diagonal

$$\Delta_X := V(y_1 - y_2, x_1 - x_2) \subset X \times X,$$

which induces the identity map: $\phi_{\Delta_X} = [1]_{J_X}$. More generally, if ψ is an automorphism of X, then $(\mathrm{Id} \times \psi)(X)$ is a correspondence on $X \times X$ inducing ψ.

EXAMPLE 2. Let X and Y be curves with affine plane models $X : F_X(x_1, y_1) = 0$ and $Y : F_Y(x_2, y_2) = 0$. For any polynomial $A(x_1, y_1, x_2, y_2)$, the correspondence $C = V(A)$ is rationally equivalent to a sum of fibres of π_X and π_Y, and so induces the trivial homomorphism: on the level of degree-0 divisor classes,

$$\phi_C\left(\left[\sum_{P \in X(\overline{K})} n_P(P)\right]\right) = \left[\mathrm{div}\left(\prod_{P \in X(\overline{K})} A(x_1(P), y_1(P), x_2, y_2)^{n_P}\right)\right] = 0.$$

In particular, correspondences inducing non-zero homomorphisms must be cut out by more than one defining equation (cf. Example 1 in Section 2).

3. *Variable-separated curves and correspondences*

Now let X and Y be variable-separated plane curves over K: that is, we suppose that X and Y have affine plane models

$$X : P_X(y_1) = Q_X(x_1) \quad \text{and} \quad Y : P_Y(y_2) = Q_Y(x_2),$$

where P_X, Q_X, P_Y and Q_Y are polynomials over K. (This includes elliptic, hyperelliptic and superelliptic X and Y.) We restrict our attention to the case where P_X, P_Y, Q_X and Q_Y are indecomposable: that is, they cannot be written as compositions of polynomials of degree at least two (cf. Remark 4 in Section 6).

Our aim is to give examples of correspondences inducing non-trivial homomorphisms. If $C = V(A)$ for some polynomial A, then $\phi_C = 0$ (cf. Example 2); so we need to find divisors on $X \times Y$ defined by at least two equations. We investigate the simplest non-trivial case, where each involves only two variables:

$$C = V(A(x_1, x_2), B(y_1, y_2)) \subset X \times Y.$$

We immediately reduce to the case where $P_X = P_Y$ and $B(y_1, y_2) = y_1 - y_2$: let Z be the curve defined by $Z : P_X(v) = Q_Y(u)$, and define correspondences $C_1 = V(A(x_1, u), y_1 - v)$ and $C_2 = V(u - x_2, B(v, y_2))$ on $X \times Z$ and $Z \times Y$, respectively. Then $C = C_1 \times_Z C_2$, so

$$\phi_C = \phi_{C_2} \circ \phi_{C_1}.$$

Replacing Y with Z and C with C_1 (or X with Z and C with C_2), we reduce to the study of curves and correspondences defined by

$$X : P(y_1) = Q_X(x_1), \quad Y : P(y_2) = Q_Y(x_2), \quad C = V(y_1 - y_2, A(x_1, x_2)).$$

For C to be one dimensional, we must have $A(x_1, x_2) \mid (Q_X(x_1) - Q_Y(x_2))$; we will see in Section 6 that the existence of such a non-trivial factor is special. It is noted in [**10**, § 2.1] that if Q_X and Q_Y are indecomposable, then the existence of a non-trivial A implies that Q_X and Q_Y have the same degree:

$$n := \deg Q_X = \deg Q_Y;$$

and further that there exists some integer r such that

$$r = \deg_{x_1}(A(x_1, x_2)) = \deg_{x_2}(A(x_1, x_2)) = \deg_{\mathrm{tot}}(A(x_1, x_2)),$$

https://doi.org/10.1112/S1461157010000410 Published online by Cambridge University Press

so we may write

$$A(x_1, x_2) = \sum_{i=0}^{r} c_i(x_2) x_1^{r-i} \quad \text{with } \deg c_i \leqslant i \text{ for all } 0 \leqslant i \leqslant r. \tag{3.1}$$

We have no restrictions on P, so we let it be (almost) generic[†]: for each integer $d > 1$, we let $s_2, \ldots, s_d$ be free parameters, and define P_d to be the polynomial

$$P_d(y) := y^d + s_2 y^{d-2} + \ldots + s_{d-1} y + s_d.$$

Note that P_d is indecomposable. Henceforward, therefore, we consider families of curves $\mathcal{X}$ and $\mathcal{Y}$ and correspondences $\mathcal{C}$ in the form

$$\boxed{\begin{array}{c} \mathcal{X} : P_d(y_1) = Q_X(x_1), \quad \mathcal{Y} : P_d(y_2) = Q_Y(x_2), \\ \\ \mathcal{C} = V(y_1 - y_2, A(x_1, x_2)) \subset \mathcal{X} \times \mathcal{Y}, \\ \\ \text{with} Q_X \text{ and } Q_Y \text{ indecomposable of degree } n, \text{ and } A \text{ as in equation (3.1).} \end{array}} \tag{3.2}$$

The families are parametrised by $s_2, \ldots, s_d$, together with any parameters in the coefficients of Q_X and Q_Y. The special case $d = 2$, which produces hyperelliptic families, is the 'linear construction' of [41] (with $s = -s_2$).

The Newton polygon of $\mathcal{X}$ (and $\mathcal{Y}$) is

$$\mathcal{N}(d, n) = \{(\lambda_1, \lambda_2) \in \mathbb{R}^2_{\geqslant 0} : d\lambda_1 + n\lambda_2 \leqslant dn\}.$$

The families $\mathcal{X}$ and $\mathcal{Y}$ have (generically) non-singular projective models in the weighted projective plane $\mathbb{P}(d, n, 1)$, which is the projective toric surface associated to $\mathcal{N}(d, n)$ (we see in [37] that $\mathbb{P}(d, n, 1) = \mathbb{P}(d/m, n/m, 1)$, where $m = \gcd(d, n)$).

We let $\mathcal{P}(d, n)$ denote the set of integer interior points of the Newton polygon:

$$\mathcal{P}(d, n) = \{(\lambda_1, \lambda_2) \in \mathbb{Z}^2_{>0} : d\lambda_1 + n\lambda_2 < dn\}.$$

The geometric genus of $\mathcal{X}$ (and of $\mathcal{Y}$) is equal to $\#\mathcal{P}(d, n)$, and it is easily verified that if $g_n(d)$ is the function of Definition 2, then

$$g_{\mathcal{X}} = g_{\mathcal{Y}} = \#\mathcal{P}(d, n) = g_n(d).$$

Remark 1. Most known non-trivial examples of explicit isogenies of Jacobians, including the isogenies of Richelot [6], Mestre [33] and Vélu [43] and the endomorphisms of Brumer [7] and Hashimoto [27], are *not* induced by correspondences in the form of equation (3.2). However, the explicit real multiplications of Mestre [34] and Tautz, Top and Verberkmoes [42] are in the form of equation (3.2).

Remark 2. Our construction generalises readily to the case where P_d, Q_X and Q_Y are rational functions instead of polynomials. While this yields many more families, it also complicates the algorithmic aspects of our constructions below.

4. *Isomorphisms and moduli*

We want to compute the number of moduli of $\mathcal{X}$: that is, the dimension of the image of $\mathcal{X}$ in the moduli space $\mathcal{M}_{g_n(d)}$ of curves of genus $g_n(d)$ over $\overline{K}$. By Torelli's theorem, this is also the dimension of the image of the family $\phi_{\mathcal{C}}$ in the appropriate moduli space of homomorphisms of principally polarised abelian varieties.

[†]We could define P_d to be the generic monic polynomial of degree d, but we can always change variables to remove its trace term in characteristic zero, and this will be convenient in the following.

https://doi.org/10.1112/S1461157010000410 Published online by Cambridge University Press

We will adapt the methods of Koelman's thesis [30] to compute the number of moduli. Up to automorphism, we can determine the form of the polynomials defining any isomorphism between curves in $\mathcal{X}$ by considering column structures and column vectors on the projective toric surface associated to $\mathcal{N}(d,n)$, where $\mathcal{X}$ has a convenient non-singular embedding (see [8, 11, 30] for details).

More specifically, for $d>2$, we embed $\mathcal{X}$ in $\mathbb{P}(d,n,1)$. The $\overline{K}$-isomorphisms between distinct curves in $\mathcal{X}$ must then take the form

$$(x,y)\longmapsto(ax+b,ey) \tag{4.1}$$

for some a, b and e in $\overline{K}$ with a and e non-zero. When $d=2$, it is more convenient to embed $\mathcal{X}$ in $\mathbb{P}(1,g_n(d)+1,1)$; the $\overline{K}$-isomorphisms must then take the form

$$(x,y)\longmapsto((ax+b)/(cx+d),ey/(cx+d)^{(g_n(d)+1)}) \tag{4.2}$$

for a, b, c, d and e in $\overline{K}$ with e and $ad-bc$ non-zero.

LEMMA 4.1. *Let $d>1$ be an integer, K a subfield of $\mathbb{C}$ and $f(x)=\sum_{i=0}^{n}f_ix^{n-i}$ a polynomial over K or $K(t)$, where t is a free parameter, such that $g_n(d)>1$ and*

$$(1)\ f_0=1,\quad (2)\ f_1=0,\quad (3)\ f_2\neq 0\quad \textit{and}\quad (4)\ f_3=\kappa f_2\ \textit{ for some } \kappa\in K.$$

Let $\mathcal{X}$ be the family defined by $\mathcal{X}:P_d(y)=f(x)$. Then:

(i) *if f_i is in $K(t)\backslash K$ for some $2\leqslant i<n$, then $\mathcal{X}$ has d moduli;*

(ii) *otherwise, $\mathcal{X}$ has $d-1$ moduli.*

Proof. Let $\mathcal{U}$ be the open subfamily of $\mathcal{X}$, where $s_2,\dots,s_d$ are all non-zero. It suffices to show that the intersection of $\mathcal{U}$ with the isomorphism class of any curve in $\mathcal{U}$ is finite. First, observe that $\mathcal{U}$ has no non-trivial constant subfamilies: the parameters $s_1,\dots,s_d$ (and t in case (i)) appear in distinct coefficients of the defining equation of $\mathcal{U}$. Hence, it is enough to show that there are only finitely many possible defining equations for isomorphisms from a fixed curve in $\mathcal{U}$ to other curves in $\mathcal{U}$. Every such isomorphism has the form of equation (4.1) (or equation (4.2) for $d=2$). But the defining equation of the codomain curve must satisfy (1)–(4), which determine e and $ax+b$ (or $(ax+b)/(cx+d)$) up to a finite number of choices. □

5. *The representation on differentials*

Let $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{C}$ be as in equation (3.2). We want to make the representation $D(\phi_{\mathcal{C}})$ of Section 2 completely explicit, with a view to determining the structure of $\ker\phi_C$. It suffices to consider the generic fibres X, Y and C of $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{C}$, respectively. In this section, K denotes the field of definition of X, Y and C.

First, we partition $\mathcal{P}(d,n)$ into disjoint 'vertical' slices:

$$\mathcal{P}(d,n)=\bigsqcup_{i=1}^{b_{d,n}}\{(i,j):1\leqslant j\leqslant p_{d,n}(i)\}, \tag{5.1}$$

where

$$b_{d,n}:=\max\{i:(i,j)\in\mathcal{P}(d,n)\}=\lceil(1-1/n)d\rceil-1$$

and

$$p_{d,n}(i):=\lceil(1-i/d)n\rceil-1\quad\text{for } 1\leqslant i\leqslant b_{d,n}.$$

We fix a basis for the spaces of regular differentials on X and Y:

$$\Omega(X)=\langle\omega_{i,j}:(i,j)\in\mathcal{P}(d,n)\rangle\quad\text{and}\quad\Omega(Y)=\langle\omega'_{i,j}:(i,j)\in\mathcal{P}(d,n)\rangle,$$

https://doi.org/10.1112/S1461157010000410 Published online by Cambridge University Press

where

$$\omega_{i,j} := \frac{y_1^{i-1}}{P_d'(y_1)} d(x_1^j) \quad \text{and} \quad \omega'_{i,j} := \frac{y_2^{i-1}}{P_d'(y_2)} d(x_2^j).$$

This fixes isomorphisms of $\Omega(X)$ and $\Omega(Y)$ with $K^{g_n(d)}$; we view regular differentials on X and Y as row $g_n(d)$-vectors over K. If we define subspaces

$$\Omega(X)_i := \langle \omega_{i,j} : 1 \leqslant j \leqslant p_{d,n}(i) \rangle \quad \text{and} \quad \Omega(Y)_i := \langle \omega'_{i,j} : 1 \leqslant j \leqslant p_{d,n}(i) \rangle$$

for $1 \leqslant i \leqslant b_{d,n}$, then the partition of equation (5.1) induces direct sum decompositions

$$\Omega(X) = \bigoplus_{i=1}^{b_{d,n}} \Omega(X)_i \quad \text{and} \quad \Omega(Y) = \bigoplus_{i=1}^{b_{d,n}} \Omega(Y)_i. \tag{5.2}$$

Since $y_1 = y_2$ in $K(C)$, the image of $\omega_{i,j}$ under $D(\phi_C)$ is

$$D(\phi_C)(\omega_{i,j}) = \mathrm{Tr}_{\Omega(Y)}^{\Omega(C)} \left(\frac{y_1^{i-1} d(x_1^j)}{P_d'(y_1)} \right) = \frac{y_2^{i-1} d(\mathrm{Tr}_{K(Y)}^{K(C)}(x_1^j))}{P_d'(y_2)} = \frac{y_2^{i-1}}{P_d'(y_2)} dt_j,$$

where

$$t_j := \mathrm{Tr}_{K(x_2)}^{K(x_2)[x_1]/(A(x_1,x_2))}(x_1^j).$$

By definition, t_j is the jth power-sum symmetric polynomial in the roots of A viewed as a polynomial in x_1 over $\overline{K(x_2)}$; but, for $k > 0$, the kth elementary symmetric polynomial in these same roots is equal to $(-1)^k c_k / c_0$, where c_k and c_0 are as in equation (3.1). We can therefore compute the t_j using the Newton–Girard recurrences

$$t_1 = -\frac{c_1}{c_0}, t_2 = -\frac{2c_2 + t_1 c_1}{c_0}, \ldots, t_j = -\frac{j c_j + \sum_{k=1}^{j-1} c_j t_{j-k}}{c_0}.$$

Equation (3.1) implies $\deg t_j \leqslant \deg c_j \leqslant j$, so expanding the t_j in terms of x_2 we write

$$t_j = \sum_{k=0}^{j} \mu_{j,k} x_2^k.$$

In terms of differentials, we have

$$dt_j = d\left(\sum_{k=0}^{j} \mu_{j,k} x_2^k \right) = \sum_{k=1}^{j} \mu_{j,k} d(x_2^k),$$

so

$$D(\phi_C)(\omega_{i,j}) = \sum_{k=1}^{j} \mu_{j,k} \omega'_{i,k}.$$

In particular, $D(\phi_C)$ respects the decomposition of equation (5.2): that is,

$$D(\phi_C)(\Omega(X)_i) \subset \Omega(Y)_i \tag{5.3}$$

for all $1 \leqslant i \leqslant b_{d,n}$. For each $0 < k < n$, we define a matrix

$$M_k(A) := \begin{pmatrix} \mu_{1,1} & 0 & 0 & \ldots & 0 \\ \mu_{2,1} & \mu_{2,2} & 0 & \ldots & 0 \\ \mu_{3,1} & \mu_{3,2} & \mu_{3,3} & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ \mu_{k,1} & \mu_{k,2} & \mu_{k,3} & \ldots & \mu_{k,k} \end{pmatrix}$$

https://doi.org/10.1112/S1461157010000410 Published online by Cambridge University Press

representing $D(\phi_C)|_{\Omega(X)_k} : \Omega(X)_k \to \Omega(Y)_k$. Combining equations (5.2) and (5.3), we have

$$D(\phi_C) = \bigoplus_{i=1}^{b_{d,n}} M_{p_{d,n}(i)}(A). \tag{5.4}$$

The ith summand in equation (5.4) is (by definition) the upper-left $p_{d,n}(i) \times p_{d,n}(i)$ submatrix of $M_{n-1}(A)$, because $p_{d,n}(i) \leqslant n-1$ for all i. Hence, we need only compute $M_{n-1}(A)$ to determine $D(\phi_C)$ for arbitrary d.

Algorithm 1. Computes the maximal block $M_{n-1}(A)$ of the matrix $D(\phi_C)$.

Input An integer $n > 1$ and a polynomial $A(x_1, x_2)$ over K in the form of equation (3.1): that is, $A(x_1, x_2) = \sum_{i=0}^{r} c_i(x_2) x_1^{r-i}$ with $\deg c_i \leqslant i$ for all i.

Output The matrix $M_{n-1}(A)$.

(1) Let $c_i := 0$ for $r < i < n$.

(2) For i in $(1, \ldots, n-1)$ do

(2a) Set $t_i := -(ic_i + \sum_{j=1}^{i-1} c_j t_{i-j})/c_0$.

(2b) For j in $(1, \ldots, n-1)$, let $\mu_{i,j} \in K$ be the coefficient of x_2^j in t_i.

(3) Return the matrix $(\mu_{i,j})$.

The representation of the Rosati dual $\phi_C^\dagger$ is

$$D(\phi_C^\dagger) = \bigoplus_{i=1}^{b_{d,n}} M_{p_{d,n}(i)}(A(x_2, x_1)).$$

We make the following definition for notational convenience.

Definition 3. We define an involution τ on $K[x_1, x_2]$ by

$$\tau(A(x_1, x_2)) := A(x_2, x_1).$$

Lemma 5.1. *With the notation above, if $M_{n-1}(A)M_{n-1}(\tau(A)) = mI_{n-1}$ for some integer m, then $\phi_C^\dagger \phi_C = [m]_{J_X}$ (that is, ϕ_C splits multiplication-by-m on J_X). Further, if m is squarefree, then ϕ_C is a $(\mathbb{Z}/m\mathbb{Z})^{g_n(d)}$-isogeny.*

Proof. We have $D(\phi_C^\dagger \phi_C) = D(\phi_C)D(\phi_C^\dagger)$, so equation (5.4) implies

$$D(\phi_C^\dagger \phi_C) = \bigoplus_{i=1}^{b_{d,n}} (M_{p_{d,n}(i)}(A) M_{p_{d,n}(i)}(\tau(A))).$$

As we noted above, $M_k(A)$ is the upper-left $k \times k$ submatrix of $M_{n-1}(A)$ for all k. Both $M_{n-1}(A)$ and $M_{n-1}(\tau(A))$ are lower-triangular, so $M_k(A)M_k(\tau(A))$ is the upper-left $k \times k$ submatrix of $M_{n-1}(A)M_{n-1}(\tau(A))$, which is mI_{n-1} by hypothesis. Hence, $M_i(A)M_i(\tau(A)) = mI_i$ for all $1 \leqslant i \leqslant b_{d,n}$, and therefore

$$D(\phi_C^\dagger \phi_C) = \bigoplus_{i=1}^{b_{d,n}} mI_i = mI_{g_n(d)}.$$

The faithfulness of $D(\cdot)$ implies $\phi_C^\dagger \phi_C = [m]_{J_X}$, proving the first assertion. The kernel of ϕ_C must be a maximal subgroup of $J_X[m]$ with respect to the property of being isotropic for the m-Weil pairing; when m is squarefree, the second assertion follows from this together with the non-degeneracy of the Weil pairing. □

https://doi.org/10.1112/S1461157010000410 Published online by Cambridge University Press

Lemma 5.1 determines the kernel structure of isogenies splitting multiplication by a squarefree integer. In Sections 11–13, we will derive isogenies splitting multiplication by four and eight; we will need another method to determine their kernel structures. It is helpful to specialise to an isogeny defined over a number field, and then to view the specialised isogeny as an isogeny of complex abelian varieties.

Suppose that K is a number field. Fix an embedding of K into $\mathbb{C}$, and let σ denote complex conjugation; enlarging K if necessary, we assume $K^\sigma = K$. We can view J_X and J_Y as complex tori (cf. [**1**, § 1.3]): identifying $\Omega(X)$ and $\Omega(Y)$ with $\mathbb{C}^{g_n(d)}$, with coordinates corresponding to the elements of $\mathcal{P}(d,n)$, we have period lattices

$$\Lambda_X \left\langle \left(\int_{\gamma_k} \omega_{i,j} : (i,j) \in \mathcal{P}(d,n) \right) : 1 \leqslant k \leqslant 2g_n(d) \right\rangle \subset \mathbb{C}^{g_n(d)}$$

and

$$\Lambda_Y \left\langle \left(\int_{\gamma'_k} \omega'_{i,j} : (i,j) \in \mathcal{P}(d,n) \right) : 1 \leqslant k \leqslant 2g_n(d) \right\rangle \subset \mathbb{C}^{g_n(d)},$$

where $\gamma_1, \ldots, \gamma_{2g_n(d)}$ and $\gamma'_1, \ldots, \gamma'_{2g_n(d)}$ are bases for $H_1(X,\mathbb{Z})$ and $H_1(Y,\mathbb{Z})$, respectively. We then have

$$J_X = \mathbb{C}^{g_n(d)}/\Lambda_X \quad \text{and} \quad J_Y = \mathbb{C}^{g_n(d)}/\Lambda_Y;$$

returning to the isogeny $\phi_C : J_X \to J_Y$, the analytic representation $S(\phi_C) : \mathbb{C}^{g_n(d)} \to \mathbb{C}^{g_n(d)}$ and rational representation $R(\phi_C) : \Lambda_X \to \Lambda_Y$ are given by the matrices

$$S(\phi_C) = D(\phi_C) \quad \text{and} \quad R(\phi_C) = \begin{pmatrix} D(\phi_C) & 0 \\ 0 & D(\phi_C)^\sigma \end{pmatrix}. \tag{5.5}$$

We will compute the structure of $\ker(\phi_C)$ using the relation

$$\ker(\phi_C) \cong \operatorname{coker}(R(\phi_C)) \cong \Lambda_Y / R(\phi_C)(\Lambda_X). \tag{5.6}$$

The first step is a restriction of scalars from K to $\mathbb{Q}$: suppose that $R(\phi_C)$ is defined over the ring $\mathcal{O}_K$ of integers of K (it is sufficient that A be a polynomial over $\mathcal{O}_K$). Fixing a $\mathbb{Z}$-basis $\gamma_1, \ldots, \gamma_e$ of $\mathcal{O}_K$, we have a faithful representation $\rho : \mathcal{O}_K \to \mathrm{Mat}_{e\times e}(\mathbb{Z})$ (made explicit in Algorithm 2), which extends to a homomorphism

$$\rho_* : \mathrm{Mat}_{2g_n(d)\times 2g_n(d)}(\mathcal{O}_K) \longrightarrow \mathrm{Mat}_{2eg_n(d)\times 2eg_n(d)}(\mathbb{Z})$$

mapping a matrix $(a_{i,j})$ to the block matrix $(\rho(a_{i,j}))$. We then have

$$(\Lambda_Y / R(\phi_C)(\Lambda_X))^e \cong \mathbb{Z}^{2eg_n(d)} / \rho_*(R(\phi_C))(\mathbb{Z}^{2eg_n(d)}), \tag{5.7}$$

so we can compute the isomorphism type of $(\ker \phi_C)^e$ by computing the elementary divisors of $\rho_*(R(\phi_C))$. Combining equations (5.4) and (5.5), and applying ρ_*, we have

$$\rho_*(R(\phi_C)) = \bigoplus_{i=1}^{b_{d,n}} \rho_*(M_{p_{d,n}(i)}(A) \oplus M_{p_{d,n}(i)}(A)^\sigma). \tag{5.8}$$

For each $1 \leqslant k \leqslant n-1$, we define

$$G(A,k) := \mathbb{Z}^{2ek} / (\rho_*(M_k(A) \oplus M_k(A)^\sigma)(\mathbb{Z}^{2ek}));$$

then combining equations (5.6), (5.7) and (5.8), we have

$$(\ker(\phi_C))^e \cong \bigoplus_{i=1}^{b_{d,n}} G(A, p_{d,n}(i)). \tag{5.9}$$

We can use this relation to deduce the structure of $\ker(\phi_C)$.

https://doi.org/10.1112/S1461157010000410 Published online by Cambridge University Press

ALGORITHM 2. Computes the sequence $(G(A,k))_{k=1}^{n-1}$.
Input A polynomial $A \in \mathcal{O}_K[x_1, x_2]$ and an integer n.
Output The sequence of groups $G(A,k)$ for $1 \leqslant k \leqslant n-1$.
(1) Compute $M_{n-1}(A)$ using Algorithm 1.
(2) Set $e := [K:\mathbb{Q}]$, and compute a $\mathbb{Z}$-basis $\gamma_1, \ldots, \gamma_e$ of $\mathcal{O}_K$.
(3) For each $1 \leqslant i \leqslant e$, let $\Gamma^{(i)}$ be the $e \times e$ integer matrix such that

$$\gamma_i \gamma_j = \sum_{k=1}^{e} \Gamma^{(i)}_{jk} \gamma_k \quad \text{for all } 1 \leqslant j \leqslant e,$$

and let $\rho : \mathcal{O}_K \to \mathrm{Mat}_{e\times e}(\mathbb{Z})$ be the map $\sum_{i=1}^{e} a_i\gamma_i \mapsto \sum_{i=1}^{e} a_i\Gamma^{(i)}$.
(4) For each $1 \leqslant k \leqslant n-1$,
(4a) Let M be the $2ek \times 2ek$ block matrix

$$M := (\rho(M_{n-1}(A)_{i,j}))_{i,j=1}^{k} \oplus (\rho(M_{n-1}(A)^{\sigma}_{i,j}))_{i,j=1}^{k}.$$

(4b) Compute the Hermite normal form of M; let $(d_1, \ldots, d_{2ek})$ be its elementary divisors.
(4c) Set $G(A,k) := \prod_{i=1}^{2ek} (\mathbb{Z}/d_i\mathbb{Z})$.
(5) Return $(G(A,1), \ldots, G(A,n-1))$.

REMARK 3. In our examples, the generic fibres X, Y and C are defined over $K(s_2, \ldots, s_d)$ or $K(s_2, \ldots, s_d, t)$, where K is a number field. But, if Q_X and Q_Y are defined over K, then so is A, so we can apply Algorithm 2 and use equation (5.9) to deduce the structure of $\ker \phi_C$ without choosing any particular specialisation.

6. *Pairs of polynomials*

To produce non-trivial examples in the form of equation (3.2), we need a source of pairs of polynomials (Q_X, Q_Y) such that $Q_X(x_1) - Q_Y(x_2)$ is reducible. For indecomposable Q_X and Q_Y over $\mathbb{C}$, these pairs have been explicitly classified by Cassou-Noguès and Couveignes [**10**]. The pairs are deeply interesting in their own right: for further background, we refer to the work of Cassels [**9**], Davenport, Lewis and Schinzel [**13, 14**], Feit [**16–18**] and Fried [**20–22**]. An excellent account of the context and importance of these results can be found on Fried's web site [**19**]. The plane curves cut out by the factors themselves are also interesting; Avanzi's thesis [**2**] provides a good introduction to this topic.

DEFINITION 4. We say that polynomials f_1 and f_2 over K are *linear translates* if $f_1(x) = f_2(ax+b)$ for some a, b in $\overline{K}$ with a non-zero. We say that pairs of polynomials (f_1, g_1) and (f_2, g_2) are *equivalent* if there exists some a, b in $\overline{K}$ with a non-zero such that f_1 and $af_2 + b$ are linear translates and g_1 and $ag_2 + b$ are linear translates.

The 'equivalence' of Definition 4 is indeed an equivalence relation on pairs of polynomials. From the point of view of constructing homomorphisms, equivalent pairs of polynomials give rise to isomorphic homomorphisms of Jacobians.

PROPOSITION 6.1. *Let $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{C}$ be as in equation (3.2). Suppose that (Q_Z, Q_W) is equivalent to (Q_X, Q_Y): that is, that $Q_Z(x) = aQ_X(a_1x + b_1) + b$ and $Q_W(x) = aQ_Y(a_2x + b_2) + b$ for some a, b, a_1, b_1, a_2 and b_2 in $\overline{K}$ with a, a_1 and a_2 non-zero.*

(i) *If $A(x_1, x_2)$ is a $\overline{K}$-irreducible factor of $Q_X(x_1) - Q_Y(x_2)$, then $A'(x_1, x_2) = A(a_1x_1 + b_1, a_2x_2 + b_2)$ is a $\overline{K}$-irreducible factor of $Q_Z(x_1) - Q_W(x_2)$.*

(ii) *$(\mathcal{X}, \mathcal{Y})$ is $\overline{K}$-isomorphic to $(\mathcal{W} : P_d(y_1) = Q_W(x_1), \mathcal{Z} : P_d(y_2) = Q_Z(x_2))$, and $\phi_{\mathcal{C}}$ is $\overline{K}$-isomorphic to $\phi_{\mathcal{D}}$, where $\mathcal{D} = V(y_1 - y_2, A'(x_1, x_2)) \subset \mathcal{W} \times \mathcal{Z}$.*

https://doi.org/10.1112/S1461157010000410 Published online by Cambridge University Press

Proof. Part (i) is a straightforward symbolic exercise. For part (ii), let $\alpha := a^{-1/d}$. The family $(\mathcal{Z}, \mathcal{W})$ is $\overline{K}$-isomorphic to $(\mathcal{X}, \mathcal{Y})$ via

$$\begin{aligned}(s_2, \ldots, s_d) &\longmapsto (\alpha^2 s_2, \ldots, \alpha^{d-1} s_{d-1}, \alpha^d s_d - b/a),\\ (x_i, y_i) &\longmapsto (a_i x_i + b_i, \alpha y_i).\end{aligned}$$

This induces a $\overline{K}$-isomorphism between $\mathcal{C}$ and $\mathcal{D}$, so $\phi_{\mathcal{C}} \cong \phi_{\mathcal{D}}$. □

The classification of pairs of indecomposable polynomials (Q_X, Q_Y) over $\mathbb{C}$ such that $Q_X(x_1) - Q_Y(x_2)$ has a non-trivial factor splits naturally into two parts, according to whether Q_X and Q_Y are linear translates or not. Observe that if Q_X and Q_Y are linear translates, then by Proposition 6.1(1) we reduce to the case $Q_Y = Q_X$. We always have a factor $x_1 - x_2$ of $Q_X(x_1) - Q_X(x_2)$; this corresponds to the fact that the endomorphism ring of J_X always contains $\mathbb{Z}$ (cf. Example 1 in Section 2).

THEOREM 6.2 (Fried [**20**]). *Let Q_X be an indecomposable polynomial over $\mathbb{C}$ of degree at least three. Then $(Q_X(x_1) - Q_X(x_2))/(x_1 - x_2)$ is $\overline{K}$-reducible if and only if (Q_X, Q_X) is equivalent to either:*

(i) *the pair (x^n, x^n) for some odd prime n; or*
(ii) *the pair $(D_n(x, 1), D_n(x, 1))$ for some odd prime n, where $D_n(x, 1)$ is the nth Dickson polynomial of the first kind with parameter 1 (see Remark 6 below).*

THEOREM 6.3 (Cassou-Noguès and Couveignes [**10**]). *Let (Q_X, Q_Y) be indecomposable polynomials of degree at least three over $\mathbb{C}$, and let σ denote complex conjugation. Assume the classification of finite simple groups (see Remark 5 below). If Q_X and Q_Y are not linear translates, then $Q_X(x_1) - Q_Y(x_2)$ is reducible if and only if (Q_X, Q_Y) is equivalent (possibly after exchanging Q_X and Q_Y) to:*

(i) *a pair in the one-parameter family (f_7, f_7^σ) defined in Section 8; or*
(ii) *the pair (f_{11}, f_{11}^σ) defined in Section 9; or*
(iii) *a pair in the one-parameter family (f_{13}, f_{13}^σ) defined in Section 10; or*
(iv) *a pair in the one-parameter family $(f_{15}, -f_{15}^\sigma)$ defined in Section 11; or*
(v) *the pair (f_{21}, f_{21}^σ) defined in Section 12; or*
(vi) *the pair (f_{31}, f_{31}^σ) defined in Section 13.*

It follows from Proposition 6.1 that we can give a complete treatment of homomorphisms induced by correspondences in the form of equation (3.2) by applying our constructions to the polynomials of Theorems 6.2 and 6.3. We treat x^n and $D_n(x, 1)$ in Section 7, and the polynomials f_7, f_{11}, f_{13}, f_{15}, f_{21} and f_{31} from Theorem 6.3 in Sections 8–13.

REMARK 4. The restriction to indecomposable polynomials is not too heavy, since we are primarily interested in isogenies of absolutely simple Jacobians. If $Q_X(x) = Q_1(Q_2(x))$ with $\deg Q_2 > 1$, then we have a $(\deg Q_2)$-uple cover $(x, y) \mapsto (Q_2(x), y)$ from $\mathcal{X}$ to $\mathcal{X}' : P_d(y) = Q_1(x)$. If $d > 2$ and $\deg Q_1 > 1$, or if $d = 2$ and $\deg Q_1 > 2$, then $\mathcal{X}'$ has positive genus and $\mathcal{J}_{\mathcal{X}'}$ is a non-trivial isogeny factor of $\mathcal{J}_{\mathcal{X}}$, so $\mathcal{J}_{\mathcal{X}}$ is reducible. If $d = \deg Q_1 = 2$, then $\mathcal{J}_{\mathcal{X}}$ is not necessarily reducible: the 'quadratic construction' in [**41**] is a partial treatment of this case.

REMARK 5. Theorem 6.3 assumes the classification of finite simple groups [**25**]. The classification is only required to prove the completeness of the list of pairs of polynomials (and not for the existence of the factorisations). In particular, Theorem 1.1 does not depend on the classification of finite simple groups; but one corollary of the classification is that every isogeny induced by a correspondence in the form of equation (3.2) is isomorphic to a composition of endomorphisms from the families in Section 7 and isogenies from the families in Theorem 1.1.

https://doi.org/10.1112/S1461157010000410 Published online by Cambridge University Press

Remark 6. Recall that $D_n(x,a)$ is the nth Dickson polynomial of the first kind with parameter a (see [32]): that is, the unique polynomial of degree n such that

$$D_n(x+a/x,a)=x^n+(a/x)^n.$$

In characteristic zero, $D_n(x,1)=2T_n(x/2)$, where T_n is the nth classical Chebyshev polynomial of the first kind. We have $D_n(x,a)=a^{n/2}D_n(a^{-1/2}x,1)$ when $a\neq 0$, so $(D_n(x,a),D_n(x,a))$ is equivalent to $(D_n(x,1),D_n(x,1))$. On the other hand, $D_n(x,0)=x^n$, so Theorem 6.2(i) is essentially a specialisation of Theorem 6.2(ii).

Part II. Families of explicit isogenies

7. *Families with explicit complex and real multiplication*

We now put our techniques into practice. First, consider Theorem 6.2(i): let $Q_X(x)=Q_Y(x)=x^n$ for some odd prime n. For each $d>1$, we derive a family

$$\mathcal{Z}_{d,n}: P_d(y)=x^n$$

of curves of genus $g_n(d)$ with an automorphism $\zeta:(x,y)\mapsto(\zeta_n x,y)$ of order n. We say that $\mathcal{Z}_{d,n}$ is *superelliptic* if $n\nmid d$. The family has $d-2$ moduli: restricting the isomorphisms of Section 4 to $\mathcal{Z}_{d,n}$, we see that every isomorphism class in $\mathcal{Z}_{d,n}$ contains a unique representative with $s_2=1$. We identify ζ with its induced endomorphism of $\mathcal{J}_{\mathcal{Z}_{d,n}}$; its minimal polynomial is the nth cyclotomic polynomial (see [38, § 3] and [36, § 4]). Recalling that

$$x_1^n-x_2^n=\prod_{i=0}^{n-1}(\zeta_n^i x_1-x_2),$$

we consider the correspondences

$$\mathcal{C}_i:=V(y_1-y_2,\zeta_n^i x_1-x_2)\subset \mathcal{Z}_{d,n}\times_{\mathbb{Q}(\zeta_n)(s_2,\dots,s_d)}\mathcal{Z}_{d,n}.$$

We have $\mathcal{C}_i=(\mathrm{Id}\times\zeta^i)(\mathcal{Z}_{d,n})$, so $\phi_{\mathcal{C}_i}=\zeta^i$ (cf. Example 1 in Section 2); the $\mathcal{C}_i$ therefore generate a subring of $\mathrm{End}(\mathcal{J}_{\mathcal{Z}_{d,n}})$ isomorphic to $\mathbb{Z}[\zeta_n]$.

Now consider Theorem 6.2(ii): $Q_X(x)=Q_Y(x)=D_n(x,1)$ for some odd prime n. For each $d>1$, we derive a family

$$\mathcal{W}_{d,n}: P_d(y_i)=D_n(x_i,1)$$

of curves of genus $g_n(d)$ with $d-1$ moduli. In [32, Theorem 3.12], we see that

$$D_n(x_1,1)-D_n(x_2,1)=(x_1-x_2)\prod_{i=1}^{(n-1)/2}A_{n,i}(x_1,x_2),$$

where

$$A_{n,i}(x_1,x_2):=x_1^2+x_2^2-(\zeta_n^i+\zeta_n^{-i})x_1x_2+(\zeta_n^i-\zeta_n^{-i})^2.$$

Proposition 7.1. *The endomorphisms of $\mathcal{J}_{\mathcal{W}_{d,n}}$ induced by the correspondences*

$$C_i:=V(y_1-y_2,A_{n,i}(x_1,x_2))\subset \mathcal{W}_{d,n}\times_{\mathbb{Q}(\zeta_n)(s_2,\dots,s_d)}\mathcal{W}_{d,n}$$

generate a subring of $\mathrm{End}(\mathcal{J}_{\mathcal{W}_{d,n}})$ *isomorphic to* $\mathbb{Z}[\zeta_n+\zeta_n^{-1}]$.

Proof. The family $\mathcal{U}_{d,n}: P_d(v)=u^n+1/u^n$ has an involution $\iota:(u,v)\mapsto(1/u,v)$ and an automorphism $\zeta:(u,v)\mapsto(\zeta_n u,v)$. The double cover $\pi:\mathcal{U}_{d,n}\to\mathcal{W}_{d,n}$ defined by $(u,v)\mapsto(u+u^{-1},v)$ is the quotient of $\mathcal{U}_{d,n}$ by $\langle\iota\rangle$, and $\pi_*\pi^*=[2]_{\mathcal{J}_{\mathcal{W}_{d,n}}}$. Let (x,y) be a generic point on $\mathcal{W}_{d,n}$. On the level of divisors, we have

$$\phi_{C_i}((x,y))=(\alpha_1,y)+(\alpha_2,y),$$

https://doi.org/10.1112/S1461157010000410 Published online by Cambridge University Press

where $\alpha_1+\alpha_2=(\zeta_n^i+\zeta_n^{-i})x$ and $\alpha_1\alpha_2=x^2+(\zeta_n^i-\zeta_n^{-i})^2$. On the other hand,

$$\pi_*(\zeta^i+\zeta^{-i})\pi^*((x,y))=2(\zeta_n^i\beta+\zeta_n^{-i}\beta^{-1},y)+2(\zeta_n^{-i}\beta+\zeta_n^i\beta^{-1},y),$$

where $\beta+\beta^{-1}=x$. A straightforward calculation shows that

$$\{\zeta_n^i\beta+\zeta_n^{-i}\beta^{-1},\zeta_n^{-i}\beta+\zeta_n^i\beta^{-1}\}=\{\alpha_1,\alpha_2\},$$

so

$$\pi_*(\zeta^i+\zeta^{-i})\pi^*((x,y))=2\phi_{C_i}((x,y)),$$

and hence

$$\pi_*(\zeta^i+\zeta^{-i})\pi^*=[2]\phi_{C_i}.$$

Let m_i be the minimal polynomial of $\zeta_n^i+\zeta_n^{-i}$; it is irreducible, and $m_i(\zeta^i+\zeta^{-i})=0$. Working in $\mathbb{Q}(\phi_{C_i})$, we have

$$2m_i(\phi_{C_i})=2m_i(\tfrac{1}{2}\pi_*(\zeta^i+\zeta^{-i})\pi^*)=\pi_*m_i(\zeta^i+\zeta^{-i})\pi^*=0;$$

hence, $m_i(\phi_{C_i})=0$, and the result follows. □

REMARK 7. The family $\mathcal{W}_{2,n}$ is isomorphic to the family $\mathcal{C}_t$ of hyperelliptic curves of genus $(n-1)/2$ described by Tautz *et al.* [42]. Their families extend earlier families of Mestre [34], replacing subgroups of the n-torsion of elliptic curves with the group of nth roots of unity in $\overline{\mathbb{Q}}$. Our construction of $\mathcal{W}_{d,n}$ readily generalises in the other direction to give more families of Jacobians in genus $g_n(d)$ with real multiplication by $\mathbb{Z}[\zeta_n+\zeta_n^{-1}]$ (though, for these families, the Dickson polynomials are replaced by certain rational functions).

8. *Genus $g_7(d)$ families from Theorem 6.3*(i)

Consider Theorem 6.3(i). Let α_7 be an element of $\overline{\mathbb{Q}}$ satisfying

$$\alpha_7^2+\alpha_7+2=0,$$

so $\mathbb{Q}(\alpha_7)=\mathbb{Q}(\sqrt{-7})$. The involution $\sigma:\alpha_7\mapsto 2/\alpha_7$ generates $\mathrm{Gal}(\mathbb{Q}(\alpha_7)/\mathbb{Q})$. Let t be a free parameter, and let f_7 be the polynomial over $\mathbb{Q}(\alpha_7)[t]$ defined by

$$\begin{aligned}f_7(x):=x^7&-7\alpha_7tx^5-7\alpha_7tx^4-7(2\alpha_7+5)t^2x^3-7(4\alpha_7+6)t^2x^2\\&+7((3\alpha_7-2)t^3-(\alpha_7+3)t^2)x+7\alpha_7t^3\end{aligned}$$

(so $f_7=7g$, where g is the polynomial of [10, § 5.1] with $a_2=\alpha_7$ and $T=t$). We have a factorisation

$$f_7(x_1)-f_7^\sigma(x_2)=A_7(x_1,x_2)B_7(x_1,x_2),$$

where

$$A_7=x_1^3-x_2^3-\alpha_7^\sigma x_1^2x_2+\alpha_7x_1x_2^2+(3-2\alpha_7^\sigma)tx_1-(3-2\alpha_7)tx_2+(\alpha_7-\alpha_7^\sigma)t.$$

Both A_7 and B_7 are absolutely irreducible, and $\tau(A_7)=-A_7^\sigma$ and $\tau(B_7)=B_7^\sigma$.

PROPOSITION 8.1. *Let $d>1$ be an integer, and consider the families defined by*

$$\begin{gathered}\mathcal{X}_{d,7}:P_d(y_1)=f_7(x_1),\quad \mathcal{Y}_{d,7}:P_d(y_2)=f_7^\sigma(x_2),\\ \mathcal{C}_{d,7}=V(y_1-y_2,A_7(x_1,x_2))\subset\mathcal{X}_{d,7}\times_{\mathbb{Q}(\alpha_7)(s_2,\dots,s_d,t)}\mathcal{Y}_{d,7}.\end{gathered}$$

The homomorphism $\phi_{d,7}=\phi_{\mathcal{C}_{d,7}}:\mathcal{J}_{\mathcal{X}_{d,7}}\to\mathcal{J}_{\mathcal{Y}_{d,7}}$ is a d-dimensional family of $(\mathbb{Z}/2\mathbb{Z})^{g_7(d)}$-isogenies.

https://doi.org/10.1112/S1461157010000410 Published online by Cambridge University Press

Proof. Both $\mathcal{X}_{d,7}$ and $\mathcal{Y}_{d,7}$ have genus $g_7(d)$, with d moduli by Lemma 4.1. Applying Algorithm 1 to A_7, we find that

$$M_6(A_7) = \begin{pmatrix} \alpha_7 & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha_7 & 0 & 0 & 0 & 0 \\ -3(2\alpha_7+1)t & 0 & \alpha_7^\sigma & 0 & 0 & 0 \\ -4(\alpha_7+4)t & -4(\alpha_7+4)t & 0 & \alpha_7 & 0 & 0 \\ 35(\alpha_7+2)t^2 & -5(2\alpha_7+1)t & -5(\alpha_7-3)t & 0 & \alpha_7^\sigma & 0 \\ -42(\alpha_7-3)t^2 & -21(2\alpha_7-3)t^2 & -6(\alpha_7-3)t & -6(2\alpha_7+1)t & 0 & \alpha_7^\sigma \end{pmatrix}.$$

We have

$$M_6(A_7)M_6(\tau(A_7)) = M_6(A_7)M_6(-A_7^\sigma) = M_6(A_7)M_6(A_7)^\sigma = 2I_6$$

(since $\tau(A_7) = -A_7^\sigma$), so $\phi_{d,7}$ is a family of $(\mathbb{Z}/2\mathbb{Z})^{g_7(d)}$-isogenies by Lemma 5.1. □

Remark 8. We may view $\phi_{d,7}$ as a deformation of an endomorphism of the superelliptic Jacobian $\mathcal{J}_{\mathcal{Z}_{d,7}}$ of Section 7. Embed $\mathbb{Z}[\alpha_7]$ in $\mathbb{Z}[\zeta_7]$, identifying α_7 with $\zeta_7+\zeta_7^2+\zeta_7^4$. At $t=0$, both $\mathcal{X}_{d,7}$ and $\mathcal{Y}_{d,7}$ specialise to $\mathcal{Z}_{d,7}$, which has an automorphism $\zeta:(x,y)\mapsto(\zeta_7 x, y)$ of order 7, while $\mathcal{C}_{d,7}$ specialises to

$$\begin{aligned} C_0 &= V(y_1-y_2, x_1^3 - x_1^2x_2 + \alpha_7^\sigma x_1x_2^2 - x_2^3) \\ &= \sum_{i\in\{1,2,4\}} V(y_1-y_2, \zeta_7^i x_1 - x_2) \subset \mathcal{Z}_{d,7} \times_{\mathbb{Q}(\alpha_7)(s_2,\ldots,s_d)} \mathcal{Z}_{d,7}. \end{aligned}$$

Each $V(y_1-y_2,\zeta_7^i x_1 - x_2)$ induces ζ^i on $\mathcal{J}_{\mathcal{Z}_{d,7}}$, so $\phi_{C_0} = \zeta+\zeta^2+\zeta^4 = [\alpha_7]_{\mathcal{J}_{\mathcal{Z}_{d,7}}}$. Therefore, $\phi_{d,7}$ is a one-parameter deformation of $[\alpha_7]_{\mathcal{J}_{\mathcal{Z}_{d,7}}}$, which splits $[2]_{\mathcal{J}_{\mathcal{Z}_{d,7}}}$. (This gives an alternative proof of Proposition 8.1.)

Remark 9. Given any hyperelliptic curve X of genus three and a maximal 2-Weil isotropic subgroup S of $J_X[2]$, there exist a (possibly reducible, and generally non-hyperelliptic) curve Y of genus three and an isogeny $\phi: J_X \to J_Y$ with kernel S, which may be defined over a quadratic extension of $K(S)$. An algorithm to compute equations for Y and ϕ when S is generated by differences of Weierstrass points appears in [**40**]. Mestre [**33**] gives a four-parameter family of $(\mathbb{Z}/2\mathbb{Z})^3$-isogenies of hyperelliptic Jacobians; their kernels are also generated by differences of Weierstrass points. Since $\mathcal{J}_{\mathcal{X}_{2,7}}[2]$ is generated by differences of Weierstrass points, which correspond to roots of f_7 together with the point at infinity, we can factor f_7 (or a reduction at some well-chosen prime) over its splitting field, and then explicitly compute the restriction of $\phi_{2,7}$ to $\mathcal{J}_{\mathcal{X}_{2,7}}[2]$ to show that its kernel is *not* generated by differences of Weierstrass points. Therefore, $\phi_{2,7}$ is not one of the isogenies of [**40**] or [**33**].

9. *Genus $g_{11}(d)$ families from Theorem 6.3*(ii)

Consider Theorem 6.3(ii). Let α_{11} be an element of $\overline{\mathbb{Q}}$ satisfying

$$\alpha_{11}^2 + \alpha_{11} + 3 = 0,$$

so $\mathbb{Q}(\alpha_{11}) = \mathbb{Q}(\sqrt{-11})$. The involution $\sigma:\alpha_{11}\mapsto 3/\alpha_{11}$ generates $\mathrm{Gal}(\mathbb{Q}(\alpha_{11})/\mathbb{Q})$. Let f_{11} be the polynomial over $\mathbb{Q}(\alpha_{11})$ defined by

$$\begin{aligned} f_{11}(x) := {} & x^{11} + 11\alpha_{11}x^9 + 22x^8 - 33(\alpha_{11}+4)x^7 + 176\alpha_{11}x^6 - 33(7\alpha_{11}-5)x^5 \\ & - 330(\alpha_{11}+4)x^4 + 693(\alpha_{11}+1)x^3 - 220(5\alpha_{11}-1)x^2 - 33(8\alpha_{11}+47)x + 198\alpha_{11} \end{aligned}$$

https://doi.org/10.1112/S1461157010000410 Published online by Cambridge University Press

(so $f_{11} = 11g$, where g is the polynomial of [**10**, § 5.2] with $a_2 = \alpha_{11}^\sigma$). We have a factorisation $f_{11}(x_1) - f_{11}^\sigma(x_2) = A_{11}(x_1, x_2)B_{11}(x_1, x_2)$, where

$$\begin{aligned} A_{11}(x_1, x_2) = {} & x_1^5 - \alpha_{11}x_1^4x_2 - x_1^3x_2^2 + (4\alpha_{11} + 2)x_1^3 + x_1^2x_2^3 + (\alpha_{11} + 6)x_1^2x_2 - (2\alpha_{11} - 10)x_1^2 \\ & - (\alpha_{11} + 1)x_1x_2^4 + (\alpha_{11} - 5)x_1x_2^2 - (12\alpha_{11} + 6)x_1x_2 + (8\alpha_{11} - 7)x_1 - x_2^5 \\ & + (4\alpha_{11} + 2)x_2^3 - (2\alpha_{11} + 12)x_2^2 + (8\alpha_{11} + 15)x_2 + 12\alpha_{11} + 6. \end{aligned}$$

Both A_{11} and B_{11} are absolutely irreducible, and $\tau(A_{11}) = -A_{11}^\sigma$ and $\tau(B_{11}) = B_{11}^\sigma$.

PROPOSITION 9.1. *Let $d > 1$ be an integer, and consider the families defined by*

$$\begin{gathered} \mathcal{X}_{d,11} : P_d(y_1) = f_{11}(x_1), \quad \mathcal{Y}_{d,11} : P_d(y_2) = f_{11}^\sigma(x_2), \\ \mathcal{C}_{d,11} = V(y_1 - y_2, A_{11}(x_1, x_2)) \subset \mathcal{X}_{d,11} \times_{\mathbb{Q}(\alpha_{11})(s_2,\ldots,s_d)} \mathcal{Y}_{d,11}. \end{gathered}$$

The induced homomorphism $\phi_{d,11} = \phi_{\mathcal{C}_{d,11}} : \mathcal{J}_{\mathcal{X}_{d,11}} \to \mathcal{J}_{\mathcal{Y}_{d,11}}$ is a $(d-1)$-dimensional family of $(\mathbb{Z}/3\mathbb{Z})^{g_{11}(d)}$-isogenies.

Proof. Both $\mathcal{X}_{d,11}$ and $\mathcal{Y}_{d,11}$ have genus $g_{11}(d)$, and $d-1$ moduli by Lemma 4.1. As in Proposition 8.1, we calculate $M_{10}(A_{11})$ (given in `degree-11.m`) using Algorithm 1; its diagonal entries are all either α_{11} or α_{11}^σ. Using $\tau(A_{11}) = -A_{11}^\sigma$, we find that

$$M_{10}(A_{11})M_{10}(\tau(A_{11})) = M_{10}(A_{11})M_{10}(A_{11})^\sigma = 3I_{10},$$

so $\phi_{d,11}$ is a family of $(\mathbb{Z}/3\mathbb{Z})^{g_{11}(d)}$-isogenies by Lemma 5.1. □

10. *Genus $g_{13}(d)$ families from Theorem 6.3*(iii)

Consider Theorem 6.3(iii). Let β_{13} and α_{13} be elements of $\overline{\mathbb{Q}}$ satisfying

$$\beta_{13}^2 - 5\beta_{13} + 3 = 0 \quad \text{and} \quad \alpha_{13}^2 + (\beta_{13} - 2)\alpha_{13} + \beta_{13} = 0.$$

The field $\mathbb{Q}(\alpha_{13}) = \mathbb{Q}(\sqrt{-3\sqrt{13} + 1})$ is an imaginary quadratic extension of the real quadratic field $\mathbb{Q}(\beta_{13}) = \mathbb{Q}(\sqrt{13})$. The involution $\sigma : \alpha_{13} \mapsto \beta_{13}/\alpha_{13}$ generates $\mathrm{Gal}(\mathbb{Q}(\alpha_{13})/\mathbb{Q}(\beta_{13}))$. Let t be a free parameter, and let

$$f_{13}(x) = x^{13} + 39((3\beta_{13} - 13)\alpha_{13} - 2\beta_{13} + 8)tx^{11} + \ldots$$

be the polynomial of degree 13 over $\mathbb{Q}(\alpha_{13})[t]$ defined in the file `degree-13.m` (so $f_{13} = 13g$, where g is the polynomial of [**10**, § 5.3] with $a_1 = \alpha_{13}$ and $T = t$). We have a factorisation $f_{13}(x_1) - f_{13}^\sigma(x_2) = A_{13}(x_1, x_2)B_{13}(x_1, x_2)$, where

$$\begin{aligned} A_{13}(x_1, x_2) = {} & x_1^4 + x_2^4 + (\beta_{13} - 3)x_1^2x_2^2 - 9(3\beta_{13} - 14)tx_1x_2 + 12(47\beta_{13} - 202)t^2 \\ & - ((\beta_{13} - 4)\alpha_{13} + 2)x_1^3x_2 + ((\beta_{13} - 4)\alpha_{13} - \beta_{13} + 3)x_1x_2^3 \\ & + 3((17\beta_{13} - 73)\alpha_{13} - 12\beta_{13} + 50)tx_1^2 - 3((17\beta_{13} - 73)\alpha_{13} - 10\beta_{13} + 45)tx_2^2 \\ & + 3((5\beta_{13} - 22)\alpha_{13} - 9\beta_{13} + 38)tx_1 - 3((5\beta_{13} - 22)\alpha_{13} + 2\beta_{13} - 9)tx_2. \end{aligned}$$

Both A_{13} and B_{13} are absolutely irreducible, and $\tau(A_{13}) = A_{13}^\sigma$ and $\tau(B_{13}) = -B_{13}^\sigma$.

PROPOSITION 10.1. *Let $d > 1$ be an integer, and consider the families defined by*

$$\begin{gathered} \mathcal{X}_{d,13} : P_d(y_1) = f_{13}(x_1), \quad \mathcal{Y}_{d,13} : P_d(y_2) = f_{13}^\sigma(x_2), \\ \mathcal{C}_{d,13} = V(y_1 - y_2, A_{13}(x_1, x_2)) \subset \mathcal{X}_{d,13} \times_{\mathbb{Q}(\alpha_{13})(s_2,\ldots,s_d,t)} \mathcal{Y}_{d,13}. \end{gathered}$$

The induced homomorphism $\phi_{d,13} := \phi_{\mathcal{C}_{d,13}} : \mathcal{J}_{\mathcal{X}_{d,13}} \to \mathcal{J}_{\mathcal{Y}_{d,13}}$ is a d-dimensional family of $(\mathbb{Z}/3\mathbb{Z})^{g_{13}(d)}$-isogenies.

https://doi.org/10.1112/S1461157010000410 Published online by Cambridge University Press

Proof. Both $\mathcal{X}_{d,13}$ and $\mathcal{Y}_{d,13}$ have genus $g_{13}(d)$, with d moduli by Lemma 4.1. We compute $M_{12}(A_{13})$ (given in `degree-13.m`) using Algorithm 1; its diagonal is

$$(\lambda_1, \lambda_2, \lambda_1, \lambda_1^\sigma, \lambda_2, \lambda_2, \lambda_2^\sigma, \lambda_2^\sigma, \lambda_1, \lambda_1^\sigma, \lambda_2^\sigma, \lambda_1^\sigma),$$

where $\lambda_1 = (\beta_{13} - 4)\alpha_{13} + 2$ and $\lambda_2 = \alpha_{13} + 1$ both have norm 3 in $\mathbb{Q}(\beta_{13})$. We find that

$$M_{12}(A_{13})M_{12}(\tau(A_{13})) = M_{12}(A_{13})M_{12}(A_{13})^\sigma = 3I_{12}$$

(since $\tau(A_{13}) = A_{13}^\sigma$), so the result follows from Lemma 5.1. □

Remark 10. As in Section 8, we may view $\phi_{d,13}$ as a deformation of an endomorphism of a superelliptic Jacobian. We embed $\mathbb{Z}[\alpha_{13}]$ in $\mathbb{Z}[\zeta_{13}]$, identifying α_{13} with $1 + \zeta_{13}^3 + \zeta_{13}^9$; then $\lambda_1 = 1 + \zeta_{13}^7 + \zeta_{13}^8 + \zeta_{13}^{11}$. At $t = 0$, both $\mathcal{X}_{d,13}$ and $\mathcal{Y}_{d,13}$ specialise to the family $\mathcal{Z}_{d,13}$ of Section 7, while $\mathcal{C}_{d,13}$ specialises to

$$C_0 = \sum_{i \in \{0,7,8,11\}} V(y_1 - y_2, \zeta_{13}^i x_1 - x_2) \subset \mathcal{Z}_{d,13} \times_{\mathbb{Q}(\alpha_{13})(s_2,\ldots,s_d)} \mathcal{Z}_{d,13}.$$

Each $V(y_1 - y_2, \zeta_{13}^i x_1 - x_2)$ induces the automorphism $\zeta^i : (x, y) \mapsto (\zeta_{13}^i x, y)$ of $\mathcal{J}_{\mathcal{Z}_{d,13}}$, so

$$\phi_{C_0} = [1] + \zeta^7 + \zeta^8 + \zeta^{11} = [\lambda_1]_{\mathcal{J}_{\mathcal{Z}_{d,13}}};$$

hence, $\phi_{d,13}$ is a one-parameter deformation of $[\lambda_1]_{\mathcal{J}_{\mathcal{Z}_{d,13}}}$, which splits $[3]_{\mathcal{J}_{\mathcal{Z}_{d,13}}}$.

11. *Genus $g_{15}(d)$ families from Theorem 6.3*(iv)

Consider Theorem 6.3(iv). Let α_{15} be an element of $\overline{\mathbb{Q}}$ satisfying

$$\alpha_{15}^2 - \alpha_{15} + 4 = 0,$$

so $\mathbb{Q}(\alpha_{15}) = \mathbb{Q}(\sqrt{-15})$; the involution $\sigma : \alpha_{15} \mapsto 4/\alpha_{15}$ generates $\mathrm{Gal}(\mathbb{Q}(\alpha_{15})/\mathbb{Q})$. Let

$$f_{15}(x) = x^{15} + 15(\alpha_{15} - 1)tx^{13} + 15(\alpha_{15} + 7)tx^{12} + \ldots$$

be the polynomial of degree 15 over $\mathbb{Q}(\alpha_{15})[t]$ defined in the file `degree-15.m` (so $f_{15} = 15g$, where g is the polynomial of [**10**, § 5.4] with $a_1 = \alpha_{15}$ and $T = t$). We have a factorisation $f_{15}(x_1) - (-f_{15}^\sigma(x_2)) = A_{15}(x_1, x_2)B_{15}(x_1, x_2)$, where A_{15} and B_{15} are absolutely irreducible polynomials of total degree seven and eight respectively (also defined in `degree-15.m`), with $\tau(A_{15}) = A_{15}^\sigma$ and $\tau(B_{15}) = B_{15}^\sigma$.

Proposition 11.1. *Let $d > 1$ be an integer, and consider the families defined by*

$$\mathcal{X}_{d,15} : P_d(y_1) = f_{15}(x_1), \quad \mathcal{Y}_{d,15} : P_d(y_2) = f_{15}^\sigma(x_2),$$
$$\mathcal{C}_{d,15} = V(y_1 - y_2, A_{15}(x_1, x_2)) \subset \mathcal{X}_{d,15} \times_{\mathbb{Q}(\alpha_{15})(s_2,\ldots,s_d,t)} \mathcal{Y}_{d,15}.$$

The induced homomorphism $\phi_{d,15} := \phi_{\mathcal{C}_{d,15}} : \mathcal{J}_{\mathcal{X}_{d,15}} \to \mathcal{J}_{\mathcal{Y}_{d,15}}$ is a d-dimensional family of $(\mathbb{Z}/4\mathbb{Z})^{g_{15}(d) - g_5(d) - g_3(d)} \times (\mathbb{Z}/2\mathbb{Z})^{2(g_5(d) + g_3(d))}$-isogenies.

Proof. Both $\mathcal{X}_{d,15}$ and $\mathcal{Y}_{d,15}$ have genus $g_{15}(d)$, with d moduli by Lemma 4.1. We compute $M_{14}(A_{15})$ (given in `degree-15.m`) using Algorithm 1. We find that

$$M_{14}(A_{15})M_{14}(\tau(A_{15})) = M_{14}(A_{15})M_{14}(A_{15})^\sigma = 4I_{14}$$

(using $\tau(A_{15}) = A_{15}^\sigma$), so $\phi_{d,15}$ splits multiplication-by-four by Lemma 5.1. After specializing t, Algorithm 2 gives $G(A_{15}, k) \cong (\mathbb{Z}/4\mathbb{Z})^{2(k - m(k))} \times (\mathbb{Z}/2\mathbb{Z})^{4m(k)}$, where $m(k) = \#\{i : 1 \leqslant i \leqslant k, \gcd(i, 15) \neq 1\}$, for each $1 \leqslant k \leqslant 14$. Each of the $g_{15}(d)$ points (i, j) in $\mathcal{P}(d, 15)$ therefore contributes a factor of either $(\mathbb{Z}/4\mathbb{Z})^2$ or $(\mathbb{Z}/2\mathbb{Z})^4$ to $(\ker(\phi_{d,15}))^2$, according to

https://doi.org/10.1112/S1461157010000410 Published online by Cambridge University Press

whether $\gcd(j,15)=1$ or not. The number of points (i,j) in $\mathcal{P}(d,15)$ with $\gcd(j,15)\neq 1$ is equal to $g_3(d)+g_5(d)$, so

$$(\ker\phi_{d,15})^2 \cong (\mathbb{Z}/4\mathbb{Z})^{2(g_{15}(d)-g_5(d)-g_3(d))}\times(\mathbb{Z}/2\mathbb{Z})^{4(g_5(d)+g_3(d))};$$

the result follows. (See Remark 11 below for more detail o the kernel structure.) □

Remark 11. As in Sections 8 and 10, we may view $\phi_{d,15}$ as a deformation of an endomorphism of a superelliptic Jacobian. Let $S=\{0,1,2,4,5,8,10\}$; we embed $\mathbb{Z}[\alpha_{15}]$ in $\mathbb{Z}[\zeta_{15}]$, identifying α_{15} with $\sum_{i\in S}\zeta_{15}^i$. At $t=0$, the family $\mathcal{X}_{d,15}$ specialises to $\mathcal{Z}_{d,15}: P_d(y_1)=x_1^{15}$, which has an automorphism $\zeta:(x_1,y_1)\mapsto(\zeta_{15}x,y)$, while $\mathcal{Y}_{d,15}$ specialises to $\mathcal{Z}'_{d,15}: P_d(y_2)=-x_2^{15}$, which is isomorphic to $\mathcal{Z}_{d,15}$ via $\iota:(x_2,y_2)\mapsto(-x_2,y_2)$. Meanwhile, A specialises to $A_0=\prod_{i\in S}(\zeta_{15}^i x_1+x_2)$, so $\mathcal{C}_{d,15}$ specialises to

$$C_0=\sum_{i\in S}V(y_1-y_2,\zeta_{15}^i x_1+x_2)\subset \mathcal{Z}_{d,15}\times_{\mathbb{Q}(\alpha_{15})(s_2,\ldots,s_d)}\mathcal{Z}'_{d,15},$$

and $\phi_{C_0}=\iota\sum_{i\in S}\zeta^i=\iota[\alpha_{15}]_{\mathcal{J}_{\mathcal{Z}_{d,15}}}$. Hence, $\phi_{d,15}$ is a one-parameter deformation of an isogeny isomorphic to the endomorphism $[\alpha_{15}]_{\mathcal{J}_{\mathcal{Z}_{d,15}}}$.

We gain further insight into the structure of $\ker\phi_{C_0}$, and hence $\ker\phi_C$, by decomposing $\mathcal{J}_{\mathcal{Z}_{d,15}}$. We may view $\mathcal{J}_{\mathcal{Z}_{d,5}}$ and $\mathcal{J}_{\mathcal{Z}_{d,3}}$ as abelian subvarieties of $\mathcal{J}_{\mathcal{Z}_{d,15}}$ via the covers $\mathcal{Z}_{d,15}\to\mathcal{Z}_{d,5}$ and $\mathcal{Z}_{d,15}\to\mathcal{Z}_{d,3}$, defined by $(x_i,y_i)\mapsto(x_i^3,y_i)$ and $(x_i,y_i)\mapsto(x_i^5,y_i)$, respectively. The endomorphism $\psi=\iota\circ\phi_{C_0}$ of $\mathcal{J}_{\mathcal{Z}_{d,15}}$ is induced by $V(y_1-y_2,A_0(x_1,-x_2))$. The matrix $M_{14}(A_0(x_1,-x_2))$ is diagonal:

$$M_{14}(A_0(x_1,-x_2))=\operatorname{diag}(\alpha_{15}^\sigma,\alpha_{15}^\sigma,2,\alpha_{15}^\sigma,-2,2,\alpha_{15},\alpha_{15}^\sigma,2,-2,\alpha_{15},2,\alpha_{15},\alpha_{15}).$$

Considering equation (5.4), we see that $D(\psi)(\omega_{i,j})=2\omega_{i,j}$ whenever $j=3$, 6, 9 and 12 (that is, when $\omega_{i,j}$ is the pullback of a differential on $\mathcal{Z}_{d,5}$), so ψ acts as $[2]_{\mathcal{J}_{\mathcal{Z}_{d,15}}}$ on $\mathcal{J}_{\mathcal{Z}_{d,5}}\subset\mathcal{J}_{\mathcal{Z}_{d,15}}$. Similarly, $D(\phi_{C_0})(\omega_{i,j})=-2\omega_{i,j}$ for $j=5$ and 10 (when $\omega_{i,j}$ is the pullback of a differential on $\mathcal{Z}_{d,3}$), so ψ acts as $[-2]_{\mathcal{J}_{\mathcal{Z}_{d,15}}}$ on $\mathcal{J}_{\mathcal{Z}_{d,3}}\subset\mathcal{J}_{\mathcal{Z}_{d,15}}$. Looking at the other entries on the diagonal, we see that ψ acts as multiplication-by-α_{15} on the $(g_{15}(d)-g_5(d)-g_3(d))$-dimensional complementary subvariety $\mathcal{A}$ of $\mathcal{J}_{\mathcal{Z}_{d,3}}\times\mathcal{J}_{\mathcal{Z}_{d,5}}$ in $\mathcal{J}_{\mathcal{Z}_{d,15}}$. This gives us a clearer description of the isomorphism in the proof of Proposition 11.1: the factors $(\mathbb{Z}/4\mathbb{Z})^{g_{15}(d)-g_3(d)-g_5(d)}$, $(\mathbb{Z}/2\mathbb{Z})^{2g_3(d)}$ and $(\mathbb{Z}/2\mathbb{Z})^{2g_5(d)}$ correspond to $\ker(\psi|_{\mathcal{A}})$, $\ker(\phi|_{\mathcal{J}_{\mathcal{Z}_{d,3}}})$ and $\ker(\phi|_{\mathcal{J}_{\mathcal{Z}_{d,5}}})$, respectively.

12. *Genus $g_{21}(d)$ families from Theorem 6.3*(v)

Consider Theorem 6.3(v). Let α_{21} be an element of $\overline{\mathbb{Q}}$ satisfying

$$\alpha_{21}^2-\alpha_{21}+2=0,$$

so $\mathbb{Q}(\alpha_{21})=\mathbb{Q}(\sqrt{-7})$; the involution $\sigma:\alpha_{21}\mapsto 2/\alpha_{21}$ generates $\mathrm{Gal}(\mathbb{Q}(\alpha_{21})/\mathbb{Q})$. Let

$$f_{21}(x)=x^{21}+(42\alpha_{21}+42)x^{19}+(84\alpha_{21}+84)x^{18}+(2331\alpha_{21}-861)x^{17}+\ldots$$

be the polynomial of degree 21 over $\mathbb{Q}(\alpha_{21})$ defined in the file `degree-21.m` (such that $f_{21}(x)=2^{21}g(x/2)$, where g is the polynomial of [**10**, § 5.5] with $a_1=\alpha_{21}$). We have a factorisation $f_{21}(x_1)-f_{21}^\sigma(x_2)=A_{21}(x_1,x_2)B_{21}(x_1,x_2)$, where

$$\begin{aligned}A_{21}(x_1,x_2)=\;&x_1^5+(\alpha_{21}+1)x_1^4x_2+2\alpha_{21}x_1^3x_2^2+(10\alpha_{21}+18)x_1^3+(2\alpha_{21}-2)x_1^2x_2^3\\&+(32\alpha_{21}-8)x_1^2x_2+(20\alpha_{21}+4)x_1^2+(\alpha_{21}-2)x_1x_2^4+(32\alpha_{21}-24)x_1x_2^2\\&+(32\alpha_{21}-16)x_1x_2+(107\alpha_{21}+55)x_1-x_2^5+(10\alpha_{21}-28)x_2^3\\&+(20\alpha_{21}-24)x_2^2+(107\alpha_{21}-162)x_2+136\alpha_{21}-68.\end{aligned}$$

Both A_{21} and B_{21} are absolutely irreducible, and $\tau(A_{21})=-A_{21}^\sigma$ and $\tau(B_{21})=B_{21}^\sigma$.

https://doi.org/10.1112/S1461157010000410 Published online by Cambridge University Press

PROPOSITION 12.1. *Let $d>1$ be an integer, and consider the families defined by*

$$\mathcal{X}_{d,21} : P_d(y_1) = f_{21}(x_1), \quad \mathcal{Y}_{d,21} : P_d(y_2) = f_{21}^{\sigma}(x_2),$$
$$\mathcal{C}_{d,21} = V(y_1 - y_2, A_{21}(x_1, x_2)) \subset \mathcal{X}_{d,21} \times_{\mathbb{Q}(\alpha_{21})(s_2,\ldots,s_d)} \mathcal{Y}_{d,21}.$$

The induced homomorphism $\phi_{d,21} := \phi_{\mathcal{C}_{d,21}} : \mathcal{J}_{\mathcal{X}_{d,21}} \to \mathcal{J}_{\mathcal{Y}_{d,21}}$ is a $(d-1)$-dimensional family of $(\mathbb{Z}/4\mathbb{Z})^{g_{21}(d)-g_3(d)} \times (\mathbb{Z}/2\mathbb{Z})^{2g_3(d)}$-isogenies.

Proof. Both $\mathcal{X}_{d,21}$ and $\mathcal{Y}_{d,21}$ have genus $g_{21}(d)$, with $d-1$ moduli by Lemma 4.1. We compute $M_{20}(A_{21})$ (given in `degree-21.m`) using Algorithm 1. We find that

$$M_{20}(A_{21})M_{20}(\tau(A_{21})) = M_{20}(A_{21})M_{20}(A_{21})^{\sigma} = 4I_{20}$$

(since $\tau(A_{21}) = -A_{21}^{\sigma}$), so ϕ_{21} splits multiplication-by-four by Lemma 5.1. Applying Algorithm 2, we see that $G(A_{21}, k) \cong (\mathbb{Z}/4\mathbb{Z})^{k-\lfloor k/7 \rfloor} \times (\mathbb{Z}/2\mathbb{Z})^{2\lfloor k/7 \rfloor}$ for $1 \leqslant k \leqslant 20$. Hence, each point (i, j) in $\mathcal{P}(d, 21)$ contributes a factor of either $(\mathbb{Z}/4\mathbb{Z})^2$ or $(\mathbb{Z}/2\mathbb{Z})^4$ to $(\ker(\phi_{d,21}))^2$, according to whether 7 divides j or not. Therefore,

$$(\ker \phi_{d,21})^2 \cong (\mathbb{Z}/4\mathbb{Z})^{2(g_{21}(d)-g_3(d))} \times (\mathbb{Z}/2\mathbb{Z})^{4g_3(d)},$$

and the result follows. □

13. *Genus $g_{31}(d)$ families from Theorem 6.3*(vi)

Consider Theorem 6.3(vi). Let α_{31} and β_{31} be elements of $\overline{\mathbb{Q}}$ satisfying

$$\beta_{31}^3 - 13\beta_{31}^2 + 46\beta_{31} - 32 = 0 \quad \text{and} \quad \alpha_{31}^2 - 1/2(\beta_{31}^2 - 7\beta_{31} + 4)\alpha_{31} + \beta_{31} = 0.$$

Note that $\mathbb{Q}(\alpha_{31})$ is a sextic CM field, and $\mathbb{Q}(\beta_{31})$ is its totally real cubic subfield. The involution $\sigma : \alpha_{31} \mapsto \beta_{31}/\alpha_{31}$ generates $\mathrm{Gal}(\mathbb{Q}(\alpha_{31}/\mathbb{Q}(\beta_{31}))$. Let

$$\begin{aligned} f_{31}(x) = x^{31} &- 31(\tfrac{1}{4}(\beta_{31}^2 - 5\beta_{31} - 10)\alpha_{31} - (\beta_{31}^2 - 7\beta_{31} + 12))x^{29} \\ &- 31(\tfrac{1}{2}(\beta_{31}^2 - 5\beta_{31} - 10)\alpha_{31} - (2\beta_{31}^2 - 14\beta_{31} + 24))x^{28} + \ldots \end{aligned}$$

be the polynomial of degree 31 over $\mathbb{Q}(\alpha_{31})$ defined in the file `degree-31.m` (such that $f_{31}(x) = 2^{31}g(x/2)$, where g is the polynomial of [**10**, § 5.6] with $a_1 = \alpha_{31}$). We have a factorisation $f_{31}(x_1) - f_{31}^{\sigma}(x_2) = A_{31}(x_1, x_2)B_{31}(x_1, x_2)$, where A_{31} and B_{31} are absolutely irreducible polynomials of total degree 15 and 16, respectively, with $\tau(A_{31}) = -A_{31}^{\sigma}$ and $\tau(B_{31}) = B_{31}^{\sigma}$.

PROPOSITION 13.1. *Let $d>1$ be an integer, and consider the families defined by*

$$\mathcal{X}_{d,31} : P_d(y_1) = f_{31}(x_1), \quad \mathcal{Y}_{d,31} : P_d(y_2) = f_{31}^{\sigma}(x_2),$$
$$\mathcal{C}_{d,31} = V(y_1 - y_2, A_{31}(x_1, x_2)) \subset \mathcal{X}_{d,31} \times_{\mathbb{Q}(\alpha_{31})(s_2,\ldots,s_d)} \mathcal{Y}_{d,31}.$$

The induced homomorphism $\phi_{d,31} := \phi_{\mathcal{C}_{d,31}} : \mathcal{J}_{\mathcal{X}_{d,31}} \to \mathcal{J}_{\mathcal{Y}_{d,31}}$ is a $(d-1)$-dimensional family of $(\mathbb{Z}/8\mathbb{Z})^{g_{31}(d)/3} \times (\mathbb{Z}/4\mathbb{Z})^{2g_{31}(d)/3} \times (\mathbb{Z}/2\mathbb{Z})^{2g_{31}(d)/3}$-isogenies.

Proof. Both $\mathcal{X}_{d,31}$ and $\mathcal{Y}_{d,31}$ have genus $g_{31}(d)$, with $d-1$ moduli by Lemma 4.1. We compute $M_{30}(A_{31})$ (given in `degree-31.m`) using Algorithm 1. We see that

$$M_{30}(A_{31})M_{30}(\tau(A_{31})) = M_{30}(A_{31})M_{30}(A_{31})^{\sigma} = 8I_{30}$$

(using $\tau(A_{31}) = -A_{31}^{\sigma}$), so $\phi_{d,31}$ splits multiplication-by-eight by Lemma 5.1. Algorithm 2 gives $G(A_{31}, k) \cong ((\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})^2 \times (\mathbb{Z}/2\mathbb{Z})^2)^{2k}$ for $1 \leqslant k \leqslant 30$, so

$$(\ker(\phi_{d,31}))^6 \cong ((\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})^2 \times (\mathbb{Z}/2\mathbb{Z})^2)^{2g_{31}(d)};$$

the result follows. □

https://doi.org/10.1112/S1461157010000410 Published online by Cambridge University Press

14. *Absolute simplicity*

We want to verify that our isogenies $\phi : \mathcal{J}_{\mathcal{X}} \to \mathcal{J}_{\mathcal{Y}}$ do not arise from products of isogenies of lower-dimensional abelian varieties. To this end, where possible, we show that the generic fibres of $\mathcal{J}_{\mathcal{X}}$ and $\mathcal{J}_{\mathcal{Y}}$ are absolutely simple.

PROPOSITION 14.1. *The generic fibres of $\mathcal{J}_{\mathcal{X}_{d,n}}$ and $\mathcal{J}_{\mathcal{Y}_{d,n}}$ are absolutely simple for:*

(i) $n = 7$ *and all* $d \geqslant 2$;
(ii) $n = 11$ *and all prime* $d \neq 11$;
(iii) $n = 13$ *and all* $d \geqslant 2$;
(iv) $n = 15$ *and all prime* $d \notin \{3, 5, 7\}$;
(v) $n = 21$ *and all prime* $d \notin \{3, 5, 7\}$;
(vi) $n = 31$ *and all prime* $d \notin \{3, 5, 31\}$.

Proof. We need only prove absolute simplicity for each $\mathcal{J}_{\mathcal{X}_{d,n}}$ (the existence of the isogeny $\phi_{d,n}$ then implies that $\mathcal{J}_{\mathcal{Y}_{d,n}}$ is absolutely simple). If $\mathcal{J}_{\mathcal{X}_{d,n}}$ is reducible, then so are all of its specialisations; so it suffices to exhibit an absolutely simple specialisation of $\mathcal{J}_{\mathcal{X}_{d,n}}$. We can do this for many (d, n) by applying results of Zarhin to hyperelliptic or superelliptic specialisations. For $n = 7$ and 13, we specialise at $t = 0$; then we apply [**45**, Theorem 1.1] for $d \geqslant 5$ and [**46**, Theorem 1.2] for $d = 3$ and 4. (We cannot use this approach for $n = 15$, because the specialisation at $t = 0$ is always reducible: cf. Remark 11 in Section 11.) For $n = 11$, 15, 21 and 31 and all prime d not dividing $n(n-1)$, we specialise at $(s_2, \ldots, s_d) = (0, \ldots, 0)$ and apply [**47**, Corollary 1.8]. For $(d, n) = (2, 7)$, $(2, 21)$ and $(2, 31)$, we specialise at $s_2 = 0$ and apply [**44**, Theorem 2.3]. For some of the remaining cases, we can use the fact that $\mathcal{X}_{d,n}$ is defined over a number field; by [**12**, Lemma 6], it suffices to exhibit an absolutely simple reduction of a specialisation of $\mathcal{J}_{\mathcal{X}_{d,n}}$ modulo a prime of good reduction. We prove absolute simplicity of reductions by computing Weil polynomials (using Gaudry and Gürel's algorithm [**24**] for superelliptic curves, and the Magma system's implementation [**26**] of Kedlaya's algorithm [**29**] for hyperelliptic curves) and applying [**28**, Proposition 3]. For $(d, n) = (2, 11)$, we specialise at $s_2 = 0$ and reduce at a prime over 7; for $(d, n) = (2, 13)$, we specialise at $(s_2, t) = (1, 0)$ and reduce at a prime over 53; for $(d, n) = (2, 15)$, we specialise at $(s_2, t) = (0, 1)$ and reduce at a prime over 17; and for $(d, n) = (5, 11)$, we specialise at $(s_2, \ldots, s_5) = (0, \ldots, 0)$ and reduce at a prime over 31. □

The list of values of n and d in Proposition 14.1 is not intended to be exhaustive; it simply reflects the practical and theoretical limits of the results used in the proof. We would like to prove simplicity for at least all prime d; but the Gaudry–Gürel algorithm requires n and d to be coprime, so we cannot apply it to cases such as $(d, n) = (11, 11)$. Further, we can only use the Howe–Zhu criterion [**28**, Proposition 3] to prove the absolute simplicity of a simple reduction J_X if the residue field $\mathbb{F}_q$ contains a primitive dth root of unity, so that the superelliptic automorphism ζ is rational. Briefly, the criterion states that if J_X is simple and $\mathbb{Q}(\pi) = \mathbb{Q}(\pi^e)$ for all $e > 1$ (where π denotes the qth power Frobenius endomorphism of J_X), then J_X is absolutely simple. But, if ζ is defined over $\mathbb{F}_{q^e}$ for some $e > 1$, then π^e commutes with ζ but π does not, so $\mathbb{Q}(\pi^e)$ is not equal to $\mathbb{Q}(\pi)$, and the criterion cannot prove absolute simplicity for J_X. Indeed, if J_X is ordinary then the converse of the criterion applies, implying that J_X is *not* absolutely simple. This restriction rules out many small primes of reduction, rendering the computation of the zeta function much more expensive. Computing Weil polynomials with which the Howe–Zhu criterion might succeed for $(d, n) = (7, 15)$, $(5, 21)$, $(3, 31)$ and $(5, 31)$ will therefore require highly optimised implementations and significant computing resources.

https://doi.org/10.1112/S1461157010000410 Published online by Cambridge University Press

Acknowledgements. We thank John Voight, for his suggestions at the *Explicit Methods in Number Theory* workshop at the FWO in Oberwolfach, 2009; the workshop organisers and the FWO itself, for the fruitful environment in which this work was begun; Wouter Castryck, for his patient help and for pointing out Koelman's thesis; and Frederik Vercauteren, for sharing his implementation of the Gaudry–Gürel point-counting algorithm.

References

1. E. Arbarello, M. Cornalba, P. A. Griffiths and J. Harris, *Geometry of algebraic curves,* vol. 1, Grundlehren der Mathematischen Wissenschaften 267 (Springer, Berlin, 1984).
2. R. M. Avanzi, 'A study on polynomials in separated variables with low genus factors', PhD Thesis, Universität Essen, 2001.
3. Ch. Birkenhake and H. Lange, *Complex abelian varieties*, 2nd edn, Grundlehren der Mathematischen Wissenschaften 302 (Springer, Berlin, 2004).
4. W. Bosma and J. J. Cannon, *Handbook of magma functions* (School of Mathematics and Statistics, University of Sydney, 1995).
5. W. Bosma, J. J. Cannon and C. Playoust, 'The Magma algebra system. I. The user language', *J. Symbolic Comput.* 24 (1997) no. 3–4, 235–265.
6. J.-B. Bost and J.-F. Mestre, 'Moyenne arithmético–géometrique et périodes des courbes de genre 1 et 2', *Gaz. Math.* 38 (1988) 36–64.
7. A. Brumer, 'The rank of $J_0(N)$', *Astérisque* 228 (1995) 41–68.
8. W. Bruns and J. Gubeladze, 'Polytopal linear groups', *J. Algebra* 218 (1999) 715–737.
9. J. W. S. Cassels, 'Factorization of polynomials in several variables', *Proceedings of the 15th scandinavian congress,* Oslo 1968, Lecture Notes in Mathematics 118 (Springer, New York, 1970) 1–17.
10. P. Cassou-Noguès and J.-M. Couveignes, 'Factorisations explicities de $g(y) - h(z)$', *Acta Arith.* 87 (1999) no. 4, 291–317.
11. W. Castryck and J. Voight, 'On nondegeneracy of curves', *Algebra Number Theory* 3 (2009) no. 3, 255–281.
12. C.-L. Chai and F. Oort, 'A note on the existence of absolutely simple Jacobians', *J. Pure Appl. Algebra* 155 (2001) no. 2–3, 115–120.
13. H. Davenport, D. J. Lewis and A. Schinzel, 'Equations of the form $f(x) = g(y)$', *Q. J. Math. Oxford* 12 (1961) 304–312.
14. H. Davenport and A. Schinzel, 'Two problems concerning polynomials', *J. reine angew. Math.* 214 (1964) 386–391.
15. R. Donagi and R. Livné, 'The arithmetic–geometric mean and isogenies for curves of higher genus', *Ann. Sc. Norm. Super. Pisa Cl. Sci.* (4) 28 (1999) no. 2, 323–339.
16. W. Feit, 'Automorphisms of symmetric balanced incomplete block designs', *Math. Z.* 118 (1970) 40–49.
17. W. Feit, 'On symmetric balanced incomplete block designs with doubly transitive automorphism groups', *J. Combin. Theory Ser. A* 14 (1973) 221–247.
18. W. Feit, *Some consequences of the classification of finite simple groups*, Proceedings of Symposia in Pure Mathematics 37 (American Mathematical Society, Providence, RI, 1980) 175–181.
19. M. Fried, Home page, http://www.math.uci.edu/∼mfried/.
20. M. Fried, 'On a conjecture of Schur', *Michigan Math. J.* 17 (1970) 41–55.
21. M. Fried, 'The field of definition of function fields and a problem in the reducibility of polynomials in two variables', *Illinois J. Math.* 17 (1973) 128–146.
22. M. Fried, *Exposition on an arithmetic–group theoretic connection via Riemann's existence theorem*, Proceedings of Symposia in Pure Mathematics 37 (American Mathematical Society, Providence, RI, 1980) 571–602.
23. W. Fulton, *Intersection theory*, 2nd edn (Springer, Berlin, 1998).
24. P. Gaudry and N. Gürel, 'An extension of Kedlaya's point-counting algorithm to superelliptic curves', *Advances in cryptology: ASIACRYPT 2001*, Lecture Notes in Computer Science 2248 (ed. C. Boyd; Springer, Berlin, 2001) 480–494.
25. D. Gorenstein, R. Lyons and R. Solomon, *The classification of the finite simple groups*, Mathematical Surveys and Monographs 40.1 (American Mathematical Society, Providence, RI, 1994).
26. M. C. Harrison, 'Some notes on Kedlaya's algorithm for hyperelliptic curves', Preprint, 2010, arXiv math.NT/1006.4206 v1.
27. K.-I. Hashimoto, 'On Brumer's family of RM-curves of genus two', *Tohoku Math. J.* (2) 52 (2000) no. 4, 475–488.
28. E. W. Howe and H. J. Zhu, 'On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field', *J. Number Theory* 92 (2002) 139–163.
29. K. S. Kedlaya, 'Counting points on hyperelliptic curves using Monsky–Washnitzer cohomology', *J. Ramanujan Math. Soc.* 16 (2001) no. 4, 323–338.
30. R. J. Koelman, 'The number of moduli of families of curves on toric surfaces', PhD Thesis, Catholic University, Nijmegen, 1991.

31. G. Kux, 'Construction of algebraic correspondences between hyperelliptic function fields using Deuring's theory', PhD Thesis, Universität Kaiserslautern, 2004.
32. R. Lidl, G. L. Mullen and G. Turnwald, *Dickson polynomials*, Pitman Monographs and Surveys in Pure and Applied Mathematics 65 (Longman Scientific and Technical, Harlow; copublished in the United States, Wiley, New York, 1993).
33. J.-F. Mestre, 'Couples de jacobiennes isogénes de courbes hyperelliptiques de genre arbitraire', Preprint, 2009, arXiv:math.AG/0902.3470 v1.
34. J.-F. Mestre, 'Familles de courbes hyperelliptiques à multiplications réelles', *Arithmetic algebraic geometry* (Texel, 1989), Progress in Mathematics 89 (Birkhäuser, Boston, MA, 1991).
35. F. Oort and K. Ueno, 'Principally polarized abelian varieties of dimension two or three are Jacobian varieties', *J. Fac. Sci. Univ. Tokyo Sect. IA: Math.* 20 (1973) 377–381.
36. B. Poonen and E. F. Schaefer, 'Explicit descent for Jacobians of cyclic covers of the projective line', *J. reine angew. Math.* 488 (1997) 141–188.
37. M. Reid, 'Graded rings and varieties in weighted projective space', Manuscript, www.maths.warwick.ac.uk/∼miles/.
38. E. F. Schaefer, 'Computing a Selmer group of a Jacobian using functions on the curve', *Math. Ann.* 310 (1998) 447–471.
39. G. Shimura, *Abelian varieties with complex multiplication and modular functions*, Princeton Mathematical Series 46 (Princeton University Press, Princeton, NJ, 1998).
40. B. Smith, 'Isogenies and the discrete logarithm problem in Jacobians of genus 3 hyperelliptic curves', *EUROCRYPT 2008*, Lecture Notes in Computer Science 4965 (ed. N. Smart; Springer, Berlin, 2008) 163–180.
41. B. Smith, 'Families of explicit isogenies of hyperelliptic Jacobians', *Arithmetic, geometry, cryptography and coding theory 2009*, Contemporary Mathematics 521 (eds D. Kohel and R. Rolland; American Mathematical Society, Providence, RI, 2010) 121–144.
42. W. Tautz, J. Top and A. Verberkmoes, 'Explicit hyperelliptic curves with real multiplication and permutation polynomials', *Canad. J. Math.* 43 (1991) no. 5, 1055–1064.
43. J. Vélu, 'Isogénies entre courbes elliptiques', *C. R. Acad. Sci. Paris* 273 (1971) 238–241.
44. Yu. G. Zarhin, 'Hyperelliptic Jacobians without complex multiplication, doubly transitive permutation groups and projective representations', *Algebraic number theory and algebraic geometry*, Contemporary Mathematics 300 (eds S. Vostokov and Y. Zarhin; American Mathematical Society, Providence, RI, 2002) 195–210.
45. Yu. G. Zarhin, 'The endomorphism rings of Jacobians of cyclic covers of the projective line', *Math. Proc. Cambridge Philos. Soc.* 136 (2004) no. 2, 257–267.
46. Yu. G. Zarhin, 'Superelliptic Jacobians', *Diophantine geometry*, CRM Series 4 (Edizioni Della Normale, Pisa, 2007) 363–390.
47. Yu. G. Zarhin, 'Endomorphisms of superelliptic Jacobians', *Math. Z.* 261 (2009) 691–707, 709.

Benjamin Smith
INRIA Saclay–Île-de-France
Laboratoire d'Informatique (LIX)
École Polytechnique,
91128 Palaiseau Cedex
France

smith@lix.polytechnique.fr

https://doi.org/10.1112/S1461157010000410 Published online by Cambridge University Press