Canad. J. Math. Vol. **63** (5), 2011 pp. 992–1024
doi:10.4153/CJM-2011-039-3

The Arithmetic of Genus Two Curves with (4,4)-Split Jacobians

Nils Bruin and Kevin Doerksen

Abstract. In this paper we study genus 2 curves whose Jacobians admit a polarized $(4,4)$-isogeny to a product of elliptic curves. We consider base fields of characteristic different from 2 and 3, which we do not assume to be algebraically closed. We obtain a full classification of all principally polarized abelian surfaces that can arise from gluing two elliptic curves along their 4-torsion, and we derive the relation their absolute invariants satisfy.

As an intermediate step, we give a general description of Richelot isogenies between Jacobians of genus 2 curves, where previously only Richelot isogenies with kernels that are pointwise defined over the base field were considered.

Our main tool is a Galois theoretic characterization of genus 2 curves admitting multiple Richelot isogenies.

1 Introduction

Let k be a field and let C be a curve of genus 2 over k. Let $J = \mathrm{Jac}(C)$ be its Jacobian. The abelian variety is called *decomposable over* k if J is isogenous over k to a product of elliptic curves $E_1 \times E_2$.

A genus 2 curve has a decomposable Jacobian if and only if there is a cover $\phi_1 \colon C \to E_1$ to an elliptic curve E_1. If we take ϕ_1 to be *optimal* (minimal degree would do), this gives rise to a complementary cover $\phi_2 \colon C \to E_2$ and an isogeny of a special type

$$\Phi \colon E_1 \times E_2 \to \mathrm{Jac}(C),$$

which we call an *optimal* (n,n)*-splitting* (Definition 2.7). The construction is also referred to as *gluing* E_1 *and* E_2 *along their* n*-torsion*, and specifying Φ is equivalent to specifying a Weil-pairing inverting isomorphism $\alpha \colon E_1[n] \to E_2[n]$.

There is a considerable literature on (n,n)-splittings, often in the language of elliptic subcovers and mainly dealing with algebraically closed base fields. The first general examples for $n = 2$ were given by Legendre and Jacobi (1832). Later Bolza (1887) considered $n = 3$ and $n = 4$ (see [16, pp. 477, 480]). In recent years, these results have been reconsidered and extended, mainly over an algebraically closed field. For $n = 2$ see [6, Ch. 14], for $n = 3$ see [8, 17, 21, 22], and for $n = 5$ see [8, 18].

In this paper we are concerned with $n = 4$. We compare our results to Bolza's [1] in Appendix A. Our methods require that the covers and isogenies we consider be separable, so we need our base field k not to be of characteristic 2. To simplify our

Received by the editors February 25, 2009; revised August 24, 2010.
Published electronically June 20, 2011.
Research supported by NSERC.
AMS subject classification: **11G30**, 14H40.
Keywords: genus 2 curves, isogenies, split Jacobians, elliptic curves.

https://doi.org/10.4153/CJM-2011-039-3 Published online by Cambridge University Press

computations we sometimes also assume that $\operatorname{char}(k) \neq 3$ and that $\#k > 5$, but this is not essential for the methods we employ.

One significant advantage of considering optimal (n,n)-splittings rather than optimal degree-n covers $\phi\colon C \to E$ is that the codomain of an (n,n)-splitting need not be a Jacobian, which means that boundary cases can be treated more uniformly. Our main result classifies all $(4,4)$-splittings.

Theorem 1.1 *Let J be a principally polarized abelian surface over a field k with $\operatorname{char}(k) \nmid 6$ and $\#k > 5$. Then J admits an optimal $(4,4)$-splitting*

$$\Phi_4\colon E_1 \times E_2 \to J$$

if and only if one of the following holds:

(i) *$J = \operatorname{Jac}(C_4)$, where C_4 is a genus 2 curve admitting a model of the form given in Appendix* C

(ii) *$J = \operatorname{Jac}(C_4')$ and $E_2 = E_1^{(D)}$, where $D = \operatorname{disc}(E_1)$, with*

$$C_4'\colon Y^2 = -64bc\frac{1}{D^3}X^6 + \frac{64}{3}b\frac{1}{D^2}X^5 + 16bc\frac{1}{D^2}X^4 + \frac{224}{27}b\frac{1}{D}X^3 + 4bc\frac{1}{D}X^2 + \frac{4}{3}bX - bc,$$

(iii) *$J = E_1 \times E_2$ and there is a 3-isogeny $E_1 \to E_2$,*

(iv) *$J = E_1/\langle T_2\rangle \times E_1/\langle T_3\rangle$, where $E_1 = E_2$ is an elliptic curve with $E_1[2](k) = \{0, T_1, T_2, T_3\}$*

(v) *$J = \Re_{k(\sqrt{D})/k}(E_1/\langle T_2\rangle)$, where $D = \operatorname{disc}(E_1)$ is a non-square, $E_1[2](k) = \{0, T_1\}$ and $E_1[2](k(\sqrt{D})) = \{0, T_1, T_2, T_3\}$ and $E_2 = E_1^{(D)}$.*

The model C_4' can be obtained as an appropriate specialization of a model for C_4.

Combined with the degree 4 covers explained in Appendix A, this also shows that if $\operatorname{Jac}(C_4)$ is $(4,4)$-split, then C_4 admits an optimal elliptic subcover of degree 4. See [14, Cor. 5.19] for the result for general n.

We use the model (C.1) to describe a birational model of the 2-dimensional locus of optimally $(4,4)$-split Jacobians in the moduli-space of curves of genus 2. The *Igusa invariants* I_2, I_4, I_6, and I_{10} (see [11]) of a genus 2 curve C classify the isomorphism class of C over an algebraically closed field. They are homogeneous polynomials of degrees 2, 4, 6, and 10 respectively in the coefficients of the defining polynomial for a model of the genus two curve. This moduli-space is birational to affine 3-space, as given by the *absolute invariants* of a genus two curve [12]:

$$i_1 = 144\frac{I_4}{I_2^2}, \quad i_2 = -1728\frac{(I_2I_4 - 3I_6)}{I_2^3}, \quad i_3 = 486\frac{I_{10}}{I_2^5}. \tag{1.1}$$

Theorem 1.2 *The absolute invariants i_1, i_2, and i_3 of a genus 2 curve with optimally $(4,4)$-split Jacobian satisfy an equation $\mathfrak{L}$, of weighted degree 90, where i_1, i_2, and i_3 are given weights 2, 3, and 5 respectively.*

The equation $\mathfrak{L}$ is too large to reproduce on paper; it consists of 4574 monomials with coefficients having up to 138 digits. We have therefore made a copy available electronically (see [5]). The surface described by $\mathfrak{L}$ is the *Humbert surface* of discriminant 16 (see [13, Corollary 1.7]).

https://doi.org/10.4153/CJM-2011-039-3 Published online by Cambridge University Press

Remark 1.3 In Appendix A we use Theorem 1.1 to verify a classic result by Bolza [1]. We find that one of his equations has a sign error and that our family is birational to his corrected family.

Our main tool is the observation that an optimal $(4,4)$-splitting Φ_4 factors as

$$\begin{tikzcd} E_1 \times E_2 \arrow[r, "\Phi_2"] \arrow[rr, bend right, "\Phi_4"'] & A \arrow[r, "\Psi"] & J, \end{tikzcd}$$

where Φ_2 is a $(2,2)$-splitting and Ψ is a polarized $(2,2)$-isogeny. A description of $(2,2)$-split principally polarized abelian varieties is already available, and we classify when they admit a further polarized $(2,2)$-isogeny of the desired type.

In general, we have that both A and J are Jacobians. Polarized $(2,2)$-isogenies between Jacobians of genus 2 curves are known as *Richelot isogenies.*

Remark 1.4 We give a full arithmetic description of Richelot isogenies in Proposition 4.3. Previous literature only considered the case where the kernel is pointwise defined over the base field (see [6, 10, 24]).

The paper is laid out in the following way. In Section 2 we give relevant definitions and background material on (n,n)-splittings of a principally polarized abelian surfaces. In Section 3 we review the basic description of $(2,2)$-splittings. Section 4 collects useful results on Richelot isogenies.

In Section 5 we relate $(4,4)$-splittings to a principally polarized abelian surface A admitting multiple polarized $(2,2)$-isogenies. For a polarized $(2,2)$-isogeny $\Phi\colon A \to B$ we write $\Phi^*\colon B \to A$ for the $(2,2)$-isogeny such that $\Phi^* \circ \Phi$ is multiplication by 2. Section 6 considers the case $A = \operatorname{Jac}(C_2)$ and relates the isogenies to Galois-theoretic properties of the Weierstrass points of C_2.

Theorem 1.5 *Let k be a field of characteristic distinct from 2. The Jacobian of a genus 2 curve $C : Y^2 = f(X)$ has two $(2,2)$-isogenies over k if and only if the Galois group of $f(X)$ is contained in $C_2 \times V_4 \subset S_6$ or $\widetilde{S}_3 = \langle (1,3,5)(2,4,6), (12)(36)(45) \rangle \subset S_6$. In the first case,* $\operatorname{Jac}(C)$ *has two isogenies Φ, Ψ such that $\Phi \circ \Psi^*$ is a $(4,2,2)$-isogeny. In the second case, it is a $(4,4)$-isogeny.*

In Section 7 we apply the results from Section 6 to derive a model for C_2. As a corollary, we obtain a model for the universal elliptic curve over $X_E^-(4)$, the modular curve of elliptic curves with 4-torsion anti-isometric to $E[4]$ (see Proposition 7.2). Silverberg [23] already derived such formulas, but the ones we list may be of interest, since they are shorter.

In Section 8 we combine results from Sections 4 and 7 to derive the model for C_4 when both A and J are Jacobians. A finer analysis yields that C_4' can be obtained from C_4 as an appropriate limit and that the cases where both C_4 and C_4' fail to provide a model of a genus 2 curve correspond to surfaces J that are not Jacobians.

2 Split Jacobians

This section introduces some terminology and reviews some basic facts. We believe all results here are well known but were unable to locate a single source that stated them in the desired form, so we gather them here for the convenience of the reader.

Definition 2.1 Let A be an abelian surface over a field k. We say that A is *decomposable* if there exist elliptic curves E_1, E_2 over k such that A is isogenous to $E_1 \times E_2$ over k.

Lemma 2.2 *Let C be a curve of genus 2 over a field k. If* $\mathrm{Jac}(C)$ *is decomposable, then C admits a finite cover $\phi_1 \colon C \longrightarrow E_1$ over k, where E_1 is an elliptic curve.*

Proof We write $J = \mathrm{Jac}(C)$. A k-rational divisor class of degree 1 gives rise to an Abel-Jacobi map $C \hookrightarrow J$ over k, which allows us to consider C as a subvariety of J. In general, we can use the k-rational canonical class κ to define a morphism $C \longrightarrow J$, which, over an algebraic closure $\overline{k}$ corresponds to $\gamma \colon C(\overline{k}) \longrightarrow \mathrm{Pic}^0(C/\overline{k})$, defined by $P \mapsto [2P] - \kappa$. Note that for $P, Q \in C(\overline{k})$ we only have $\gamma(P) = \gamma(Q)$ if $[2P] = [2Q]$, which implies that P, Q are Weierstrass points on C. Hence, the image of γ is birational to C. Moreover, since for a Weierstrass point P we do have $[2P] = \kappa$, we see that the identity $0_J \in J$ lies in the image of γ.

If J is decomposable, then there is an isogeny $\Phi \colon J \longrightarrow E_1 \times E_2$ over k, where E_1, E_2 are elliptic curves over k. Let $\pi_1 \colon E_1 \times E_2 \longrightarrow E_1$ be the projection on the first factor and write $\Phi_1 = \Phi \circ \pi_1$. We claim that $j \circ \Phi_1$ is not constant. If it were, then $\gamma(C)$ would have to lie in the connected component of $\ker(\Phi_1)$ that contains 0_J. But that is a 1-dimensional subgroup scheme of J, so cannot contain a singular model of a curve of genus 2. It follows that $\phi = \gamma \circ \Phi_1 \colon C \longrightarrow E_1$ is a non-constant morphism between (complete, non-singular) irreducible curves and hence a finite cover. ■

The cover in Lemma 2.2 is far from unique, and the one that the proof constructs is unlikely to be of minimal degree. This leads us to consider *optimal* covers, also referred to as *maximal* [9] and *minimal* [13] covers.

Definition 2.3 We call a finite cover $\phi_1 \colon C \to E_1$ *optimal* if for any factorization

$$C \xrightarrow{\phi_1} E_1 = C \xrightarrow{\phi_1'} D \xrightarrow{\psi} E_1$$

we must have $\deg(\phi_1') = \deg(\phi_1)$ or $\deg(\phi_1') = 1$.

It is immediate that any finite cover $\psi \colon C \to E$, where C is of genus 2 and E is an elliptic curve, factors through some optimal cover $\phi_1 \colon C \to E_1$.

We follow Kuhn [17] and Frey–Kani [9]. We write $n = \deg(\phi_1)$. We will need our maps to be separable, so we assume that $\mathrm{char}(k) \nmid n$. We have the induced maps

$$\phi_1^* \colon E_1 \to J \quad \text{and} \quad \phi_{1,*} \colon J \to E_1.$$

The optimality of ϕ_1 implies that ϕ_1^* is injective and that $E_2^* := \ker(\phi_{1,*})$ must be connected and hence an elliptic curve. We write $E_1^* = \phi_1^*(E_1)$.

https://doi.org/10.4153/CJM-2011-039-3 Published online by Cambridge University Press

Since $\phi_{1,*} \circ \phi_1^* = n \cdot \mathrm{id}_{E_1}$, we see that $E_1^* \cap E_2^* = E_1^*[n]$.

We write $\phi_{2,*}\colon J \longrightarrow J/E_1^* =: E_2$ for the projection. We follow Kuhn's argument in [17]. He assumes k is a number field, but his method generalizes. Kuhn proves that if C has a degree 1 divisor class over k that is invariant under the hyperelliptic involution, then there is a cover $\phi_2\colon C \longrightarrow E_2$ of degree n for which $\phi_{2,*}$ is the corresponding push forward. Furthermore, he shows that if n is odd, then such a class exists. For even n, he argues that the map, initially defined over an extension of k where C has a Weierstrass point, actually descends to k. Note that the kernel of $\phi_{2,*}$ is connected, and hence ϕ_2 is optimal. We call $\phi_2\colon C \longrightarrow E_2$ a *complementary cover* to the optimal cover $\phi_1\colon C \longrightarrow E_1$.

The maps ϕ_1, ϕ_2 give rise to an isogeny

$$\phi_1^* + \phi_2^*\colon E_1 \times E_2 \longrightarrow J,$$

where $\Delta = \ker(\phi_1^* + \phi_2^*)$ is the graph of an isomorphism $\alpha\colon E_1[n] \longrightarrow E_2[n]$.

To characterize the nature of this isogeny, we recall some standard terminology on principally polarized abelian varieties. We follow [19]. We recall that a polarized abelian variety is an abelian variety A equipped with an isogeny $\lambda\colon A \longrightarrow A^\vee$, where $A^\vee$ is the dual abelian variety of A, such that λ comes from an ample invertible sheaf on $A_{\overline{k}}$. If λ is an isomorphism, we say that (A, λ) is a *principally polarized abelian variety*. A principal polarization induces, for each n prime to the characteristic, an alternating non-degenerate, bilinear pairing $e_{A[n]}\colon A[n] \times A[n] \longrightarrow \mu_n$, called a *Weil pairing*.

The main result we need is [19, Proposition 16.8], which describes isogenies that respect polarizations. Paraphrased, it yields the following lemma in our particular situation.

Lemma 2.4 *Let* (A, λ_A) *be a principally polarized abelian variety and let* $\Phi\colon A \longrightarrow B$ *be an isogeny with* $\ker(\Phi) \subset A[n]$. *A necessary and sufficient condition for the existence of a polarization* $\lambda_B\colon B \longrightarrow B^\vee$ *such that the diagram*

$$\begin{tikzcd}
A \arrow[r, "n\lambda_A"] \arrow[d, "\Phi"'] & A^\vee \\
B \arrow[r, "\lambda_B"] & B^\vee \arrow[u, "\Phi^\vee"']
\end{tikzcd}$$

commutes, is that $\ker(\Phi)$ *is* isotropic *with respect to* $e_{A[n]}$, *which means that* $e_{A[n]}$ *restricted to* $\ker(\Phi) \times \ker(\Phi)$ *is trivial.*

If A is g-dimensional, then $\deg(n\lambda_A) = n^{2g}$. Since $\deg(\Phi) = \deg(\Phi^\vee)$, a simple degree calculation shows that λ_B is principal if and only if $\deg(\Phi) = n^g$. The nondegeneracy of $e_{A[n]}$ implies that in that case $\ker(\Phi)$ is a *maximal* isotropic subgroup.

Definition 2.5 Let (A, λ_A) and (B, λ_B) be principally polarized abelian varieties of dimension g. We say that an isogeny $\Phi\colon A \longrightarrow B$ is a *polarized* $(n_1, \dots, n_r)$*-isogeny* if $\ker(\Phi)(\overline{k}) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$ and $\Phi^\vee \circ \lambda_B \circ \Phi = n\lambda_A$, where $n^g = \prod_{i=1}^r n_i$.

https://doi.org/10.4153/CJM-2011-039-3 Published online by Cambridge University Press

Using [19, Lemma 16.2] it is straightforward to check that if $\Phi\colon A \to B$ is a polarized (n, n) isogeny between principally polarized abelian surfaces (A, λ_A) and (B, λ_B), then so is $\Phi^\vee\colon B^\vee \to A^\vee$ between $(B^\vee, \lambda_B^{-1})$ and $(A^\vee, \lambda_A^{-1})$. Furthermore if λ' is another polarization on B such that $\Phi^\vee \circ \lambda' \circ \Phi = n\lambda_A$, then $\lambda' = \lambda_B$. This can be seen by observing that the Néron–Severi group of an abelian variety is torsion-free or, more directly, if $n\lambda' = n\lambda_B$, then $\lambda' - \lambda_B$ maps the connected variety A into a finite variety, so it must be constant 0.

Lemma 2.6 *Let C be a genus 2 curve, let $\phi_1\colon C \to E_1$ be an optimal cover of degree n and let $\phi_2\colon C \to E_2$ be a complementary cover. Then $\phi_1^* + \phi_2^*\colon E_1 \times E_2 \to J$ is a polarized (n, n)-isogeny, with dual isogeny $\phi_{1,*} \times \phi_{2,*}\colon J \to E_1 \times E_2$.*

Proof The duality statement is immediate. To prove that the isogeny is polarized, we just have to verify that

$$(\phi_{1,*} \times \phi_{2,*}) \circ (\phi_1^* + \phi_2^*) = (n\,\mathrm{id}_{E_1} \times n\,\mathrm{id}_{E_2})$$

which follows because $\phi_{i,*} \circ \phi_j^* = 0$ and $\phi_{i,*} \circ \phi_i^* = n\,\mathrm{id}_{E_i}$ for $(i, j) = (1, 2), (2, 1)$. Finally, it is an (n, n)-isogeny because the kernel, being the graph of an isomorphism $E_1[n] \to E_2[n]$, indeed has the structure $E_1[n](\bar{k}) \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. ■

We have

$$\Delta = \ker(\phi_1^* + \phi_2^*) = \{(P, \alpha(P)) : P \in E_1[n]\}.$$

For Δ to be maximally isotropic we need for all $P, Q \in E_1[n]$ that

$$1 = e_{(E_1\times E_2)[n]}\big((P, \alpha(P)), (Q, \alpha(Q))\big) = e_{E_1[n]}(P, Q)e_{E_2[n]}\big(\alpha(P), \alpha(Q)\big),$$

which is precisely the case if α is an anti-isometry.

Definition 2.7 Let E_1, E_2 be elliptic curves and let A be a principally polarized abelian surface. Suppose that $\Phi\colon E_1 \times E_2 \to A$ is a polarized isogeny. We say that Φ is an *optimal polarized* (n, n)*-splitting* if $\Delta = \ker(\Phi)$ is the graph of an anti-isometry $\alpha\colon E_1[n] \to E_2[n]$.

A principally polarized abelian surface A equipped with an optimal polarized (n, n)-splitting is an *optimally* (n, n)*-split* principally polarized abelian surface.

Proposition 2.8 *Let C be a genus 2 curve over a field k of characteristic* 0*. If* $\mathrm{Jac}(C)$ *is decomposable, then for some n it admits an optimal (n, n)-splitting.*

Proof Lemma 2.2 guarantees that there is a finite cover $C \to E_1'$, so there is an optimal cover $\phi_1\colon C \to E_1$ as well. Let $n = \deg(\phi_1)$. Lemma 2.6 shows that this gives rise to a polarized (n, n)-isogeny $E_1 \times E_2 \to \mathrm{Jac}(C)$, and we have established that its kernel is the graph of an anti-isometry. ■

https://doi.org/10.4153/CJM-2011-039-3 Published online by Cambridge University Press

An (n, n)-splitting does not have to map to a Jacobian.

Proposition 2.9 *An $(n-1)$-isogeny $\phi\colon E_1 \to E_2$ gives rise to an optimal polarized (n, n)-splitting*

$$\begin{array}{rccccccc}\Phi\colon & E_1 & \times & E_2 & \to & E_1 & \times & E_2\\ & (\ P & , & Q\ ) & \mapsto & (\ \phi^*(Q)+P & , & \phi(P)-Q\ ),\end{array}$$

where $\phi^*\colon E_2 \to E_1$ is the isogeny such that $\phi^* \circ \phi$ is multiplication-by-$(n-1)$.

Proof Note that the restriction $\phi|_{E_1[n]}\colon E_1[n] \to E_2[n]$ yields an anti-isometry. It is straightforward to check that $\Phi \circ \Phi$ is multiplication-by-n and that $\ker(\Phi)$ consists of points $(P, \phi(P))$, with $P \in E[n]$, so the kernel of Φ is indeed that graph of an anti-isometry. ■

3 $(2, 2)$-Split Jacobians

This is a brief description of $(2, 2)$-splittings. We believe the results presented here are well known, but since the construction is central to the rest of the paper and the proofs are simple, we have included them for the convenience of the reader. See also [10] and [6, Ch. 14].

Lemma 3.1 *Let k be a field with $\operatorname{char}(k) \neq 2$ and let $E_1\colon V^2 = f(U)$ be an elliptic curve over k, where $f(U) \in k[U]$ is a monic square-free cubic. Specifying (E_2, α), where E_2 is an elliptic curve over k and $\alpha\colon E_1[2] \to E_2[2]$ is an anti-isometry is equivalent to specifying $a \in k \cup \{\infty\}$ with $f(a) \neq 0$ and $d \in k^\times$ representing an element in $k^\times/k^{\times 2}$ such that*

$$E_2 : \begin{cases} W^2 = -df(U) & \text{if } a = \infty,\\ W^2 = d(U-a)f(U) & \text{otherwise,}\end{cases}$$

where $0_{E_2} \in E_2(k)$ is the unique point with $U(0_{E_2}) = a$ and the anti-isometry is given by $\alpha(0_{E_1}) = 0_{E_2}$ and $\alpha((u, 0)) = (u, 0)$ for any $(u, 0) \in E_1[2](\bar{k}) \setminus \{0_{E_1}\}$.

Proof First note that any group scheme isomorphism $\alpha\colon E_1[2] \to E_2[2]$ is automatically both an isometry and an anti-isometry and that any scheme isomorphism $\alpha'\colon E_1[2] \setminus \{0_{E_1}\} \to E_1[2] \setminus \{0_{E_1}\}$ can be extended uniquely to an isometry.

We first prove that if $\alpha\colon E_1[2] \to E_2[2]$ is a group scheme homomorphism, then E_2 and α can be represented as stated. Note that $U\colon E_1 \to \mathbb{P}^1$ represents the quotient $E_1 \to E_1/\langle -1\rangle$ and that it is ramified over exactly $U(E_1[2]) = \{f(U) = 0\} \cup \{\infty\}$. Similarly, we have $U'\colon E_2 \to E_2/\langle -1\rangle$ and α induces a scheme isomorphism $\gamma\colon \{f(U) = 0\} \to U'(E_2[2] \setminus \{0_{E_2}\}$. Since this is an isomorphism of étale degree 3 subschemes of $\mathbb{P}^1$, it extends uniquely to an isomorphism $\mathbb{P}^1 \to \mathbb{P}^1$. Hence $\gamma^{-1} \circ U'\colon E_2 \to \mathbb{P}^1$ is a degree 2 cover ramified over $\{f(U) = 0\}$ and some fourth point $\gamma^{-1}(U'(0_{E_2})) = a$ (hence $f(a) \neq 0$). It follows that E_2 admits a model as stated and that α is a map as advertised.

Conversely, it is clear that as long as $f(a) \neq 0$, the model for E_2 describes an elliptic curve and α describes a scheme isomorphism $E_1[2] \to E_2[2]$ sending 0_{E_1} to 0_{E_2}, so it does define an anti-isometry. ■

https://doi.org/10.4153/CJM-2011-039-3 Published online by Cambridge University Press

Theorem 3.2 *Let k be a field with $\operatorname{char}(k) \neq 2$. Let E_1, E_2 be elliptic curves given by models*

$$E_1\colon V^2 = f(U) \quad E_2\colon W^2 = d(U-a)f(U)$$

and let $\alpha\colon E_1[2] \to E_2[2]$ be the isometry induced by the identification

$$U(E_1[2] \setminus \{0_{E_1}\}) = U(E_2[2] \setminus \{0_{E_2}\}).$$

If $a \neq \infty$, then the fiber product $C_2 = E_1 \times_{\mathbb{P}^1_U} E_2$ is a curve of genus 2 admitting a model

$$C_2\colon Y^2 = f\left(\tfrac{1}{d}X^2 + a\right),$$

where the double covers $\phi_1\colon C_2 \to E_1$ and $\phi_2\colon C_2 \to E_2$ are induced by the relations

$$U = \tfrac{1}{d}X^2 + a, \quad V = Y, \quad W = XY.$$

Furthermore, the isogeny

$$\phi_1^* + \phi_2^*\colon E_1 \times E_2 \to \operatorname{Jac}(C_2)$$

is the $(2,2)$-splitting corresponding to α.

Proof That C_2 is a model of the fiber product of E_1 and E_2 over the U-line can be verified immediately. If we establish that ϕ_1 is an optimal cover and that ϕ_2 is a complementary cover, then Lemma 2.6 establishes that $\phi_1^* + \phi_2^*$ is a $(2,2)$-splitting. Optimality follows because ϕ_1 and ϕ_2 are of prime degree. It follows that $\phi_1^*\colon E_1 \to \operatorname{Jac}(C_2)$ is injective.

To show that ϕ_2 is complementary we need that $\phi_{2,*} \circ \phi_1^* = 0$. But these are maps that come from a fiber product, so we can compute the composition by taking a divisor on E_1, pushing it down to $\mathbb{P}^1_U$ and pulling it back to E_2. Since we map through a $\mathbb{P}^1$, any degree 0 divisor must map into the principal class on E_2, which establishes that $\phi_{2,*} \circ \phi_1^* = 0$.

It is straightforward to check that $\phi_1^* + (\phi_2^* \circ \alpha)\colon E_1[2] \to \operatorname{Jac}(C_2)$ is zero and hence that the kernel of $\phi_1^* + \phi_2^*$ is indeed the graph of α. ■

Definition 3.3 Let E be an elliptic curve over a separable quadratic extension L/k. We write $\Re_{L/k}(E)$ for the *Weil restriction of scalars* of E with respect to L/k, in the sense of [2, §7.6].

For out purposes, it is sufficient to know that $A = \Re_{L/k}(E)$ is an abelian surface over k that over L is isomorphic to $E \times E^\sigma$, where σ is a non-trivial automorphism of L over k. The product polarization on the latter descends to a k-rational principal polarization on A.

Proposition 3.4 *Let k be a field with $\operatorname{char}(k) \neq 2$. Let E be an elliptic curve over k, let $d \in k^\times$ represent a class in $k^\times/k^{\times 2}$, and let $\alpha\colon E[2] \to E^{(d)}[2]$ be the obvious isometry. Let $\Delta \subset E[2] \times E^{(d)}[2]$ be the graph of α. Then*

$$(E \times E^{(d)})/\Delta = \begin{cases} E \times E & \text{if } d \text{ is a square,} \\ \Re_{k(\sqrt{d})/k)}(E) & \text{otherwise.} \end{cases}$$

https://doi.org/10.4153/CJM-2011-039-3 Published online by Cambridge University Press

Proof If d is square, Proposition 2.9 applies with $n = 2$ and we find the $(2,2)$-isogeny given by $\Phi\colon (P,Q) \mapsto (P+Q, P-Q)$.

If d is not a square, the first case at least gives us a description of Φ over $k(\sqrt{d})$. We just have to check that Φ descends to a morphism over k with the twisted Galois actions on domain and codomain. Both $(E\times E^{(d)})(\overline{k})$ and $\Re_{k(\sqrt{d})/k}(E)(\overline{k})$ are isomorphic to $E(\overline{k}) \times E(\overline{k})$ as groups, but have twisted Galois actions. Let $\chi_d\colon \operatorname{Gal}(\overline{k}/k) \to \{\pm 1\}$ be the quadratic character belonging to $k(\sqrt{d})/k$. The Galois action on $E(\overline{k}) \times E(\overline{k})$ corresponding to $E \times E^{(d)}$ is

$$(P,Q)^\sigma = (P^\sigma, \chi_d(\sigma)Q^\sigma),$$

and the action corresponding to $\Re_{k(\sqrt{d})/k}(E)$ is

$$(P,Q)^\sigma = \begin{cases} (P^\sigma, Q^\sigma) & \text{if } \chi_d(\sigma) = 1,\\ (Q^\sigma, P^\sigma) & \text{if } \chi_d(\sigma) = -1.\end{cases}$$

We want to test that the isogeny $\Phi\colon E(\overline{k}) \times E(\overline{k}) \to E(\overline{k}) \times E(\overline{k})$ defined by $(P,Q) \mapsto (P+Q, P-Q)$ descends to k when we twist domain and codomain to $E \times E^{(d)}$ and $\Re_{k(\sqrt{d})/k}(E)$ respectively. So we must establish that $(\Phi(P,Q))^\sigma = \Phi((P,Q)^\sigma)$ for all $\sigma \in \operatorname{Gal}(\overline{k}/k)$, with the appropriately interpreted twisted action. It is immediate that this is the case if $(\sqrt{d})^\sigma = \sqrt{d}$. In the other case we verify that

$$\begin{aligned}\big(\Phi(P,Q)\big)^\sigma &= (P+Q, P-Q)^\sigma = (P^\sigma - Q^\sigma, P^\sigma + Q^\sigma)\\ &= \big(P^\sigma + \chi_d(\sigma)Q^\sigma, P^\sigma - \chi_d(\sigma)Q^\sigma\big)\\ &= \Phi\big(P^\sigma, \chi_d(\sigma)Q^\sigma\big) = \Phi\big((P,Q)^\sigma\big).\end{aligned}$$

This confirms that the isogeny is indeed defined over k. It also shows that the product polarization on $E\times E$ over $k(\sqrt{d})$ descends to a principal polarization on $\Re_{k(\sqrt{d})/k}(E)$ over k such that Φ is a polarized $(2,2)$-isogeny. ■

4 Polarized $(2,2)$-Isogenies on Jacobians of Genus 2 Curves

The purpose of this section is to describe polarized $(2,2)$-isogenies between Jacobians of genus 2 curves. Such isogenies are called *Richelot isogenies*. After giving an explicit description of the 2-torsion, we review the classical description of Richelot isogenies over algebraically closed base fields, or more generally, base fields with sufficient roots. Most of the material presented here is already known; see [4], [24, Ch. 8], [6, Ch. 9], or [7, § 4]. The new contribution is Proposition 4.3, where we determine the appropriate twist of the codomain for non-algebraically closed base fields.

Let k be a field of odd characteristic, let $\overline{k}$ be an algebraic closure of k, and let C be a curve of genus 2 over k. Then C admits a model of the form

$$C\colon Y^2 = f(X) = f_6X^6 + f_5X^5 + \cdots + f_1X + f_0, \tag{4.1}$$

https://doi.org/10.4153/CJM-2011-039-3 Published online by Cambridge University Press

where $f(X) \in k[X]$ is a square-free polynomial of degree 5 or 6. If k has at least 6 elements, then we can assume that $f_6 \neq 0$. This excludes some curves over $k = \mathbb{F}_3, \mathbb{F}_5$ from our considerations. In fact, such curves have at least 4 rational Weierstrass points, which forces the Galois structure of the kernel of Richelot isogenies defined over k to be of the type that is already covered by the existing literature. Note that $(f_6Y)^2 = f_6^2 f(X)$ is also a model of C over k, so it is not a restriction to insist that the leading coefficient be a cube. We assume that $f_6 = q_2^3$ for some $q_2 \in k$.

First we describe $\operatorname{Jac}(C)[2]$ and its maximal isotropic subgroups. Let $w_1, \dots, w_6$ be the roots of $f(X)$ in $\overline{k}$. The Weierstrass points of C are exactly $T_i = (w_i, 0)$. The non-zero two-torsion points in $\operatorname{Pic}^0(C/\overline{k})$ are exactly the divisor classes $T_{\{i,j\}} = [T_i - T_j] = [T_j - T_i]$, and the Weil-pairing is given by

$$(T_{\{i,j\}}, T_{\{k,l\}})_2 = (-1)^{\#\{i,j,k,l\}}.$$

Let $J = \operatorname{Jac}(C)$. The maximal isotropic subgroups of $J[2]$ are exactly of the form

$$\{0, T_{\{i_1,i_2\}}, T_{\{i_3,i_4\}}, T_{\{i_5,i_6\}}\},$$

where the indices are given by a partition $\{\{i_1, i_2\}, \{i_3, i_4\}, \{i_5, i_6\}\}$ of $\{1, \dots, 6\}$ into three disjoint pairs. For ease of notation, we assume that $(i_1, \dots, i_6) = (1, \dots, 6)$. This data corresponds to specifying a factorization

$$F_j(X) = q_2X^2 + q_{1,j}X + q_{0,j} = q_2(X - w_{2j-1})(X - w_{2j}) \tag{4.2}$$

such that

$$f(X) = F_1(X)F_2(X)F_3(X).$$

We say that $\{F_1(X), F_2(X), F_3(X)\} \subset \overline{k}[X]$ is a *quadratic splitting* of f. We say that $\{F_1(X), F_2(X), F_3(X)\}$ is a quadratic splitting *over* k if it is stable under $\operatorname{Gal}(\overline{k}/k)$. The $F_i(X)$ do not have to be individually defined over k.

Lemma 4.1 *Let C be a curve of genus 2 over a field k of odd characteristic with $\#k > 5$. Suppose $\Delta \subset \operatorname{Jac}(C)[2]$ is a maximal isotropic subgroup scheme over k. Let L be the coordinate ring of $\Delta \setminus \{0\}$. Then there is a quadratic polynomial $Q(X) \in L[X]$ such that C admits a model of the form*

$$C : Y^2 = f(X) = \operatorname{Norm}_{L[X]/k[X]}(Q(X)). \tag{4.3}$$

Conversely, for any cubic étale algebra L/k, any such representation gives rise to a maximal isotropic subgroup scheme $\Delta \subset \operatorname{Jac}(C)[2]$ with $\Delta \setminus \{0\} = \operatorname{Spec}(L)$.

Proof We choose a model of the form (4.1) with $f_6 = q_2^3$. We label the roots $w_1, \dots, w_6$ of $f(X)$ in $\overline{k}$ such that

$$\Delta(\overline{k}) = \{0, T_{\{1,2\}}, T_{\{3,4\}}, T_{\{5,6\}}\}$$

Let $F_j(X)$ be defined as in (4.2). The group $\operatorname{Gal}(\overline{k}/k)$ acts by permutation on $\{T_{\{1,2\}}, T_{\{3,4\}}, T_{\{5,6\}}\}$, and the identification $F_j(X) \mapsto T_{\{2j-1,2j\}}$ is Galois-covariant, so $\{F_1(X), F_2(X), F_3(X)\}$ is a quadratic splitting of $f(X)$ over k. It follows

https://doi.org/10.4153/CJM-2011-039-3 Published online by Cambridge University Press

that there is a polynomial $Q(X) \in L(X)$ that maps to each of the F_j under the three k-algebra homomorphisms $L \to \overline{k}$. This yields that C is indeed of the form (4.3).

For the converse, note that the three images $F_j(X)$ of $Q(X)$ under the three maps $L[X] \to \overline{k}[X]$ give rise to a quadratic splitting $\{F_1(X), F_2(X), F_3(X)\}$ of $f(X)$ over k and hence to a maximal isotropic subscheme $\Delta \subset \operatorname{Jac}(C)[2]$ over k with $\Delta \setminus \{0\} = \operatorname{Spec}(L)$. ■

Next we describe the codomain of a Richelot-isogeny. Suppose $\Delta \subset \operatorname{Jac}(C)[2]$ is a maximal isotropic subgroup scheme over k and let $\{F_1(X), F_2(X), F_3(X)\}$ be the corresponding quadratic splitting. We will describe the principally polarized abelian surface $B = \operatorname{Jac}(C)/\Delta$ when it is a Jacobian itself. We define the *determinant* of the quadratic splitting to be

$$\delta = \det\begin{pmatrix} q_{0,1} & q_{1,1} & q_2 \\ q_{0,2} & q_{1,2} & q_2 \\ q_{0,3} & q_{1,3} & q_2 \end{pmatrix} \tag{4.4}$$

(see [24, p. 117] or [6, p. 89]). If $\delta = 0$, then we say the quadratic splitting $\{F_1(X), F_2(X), F_3(X)\}$ is *singular*. In this case B is a product of elliptic curves over $\overline{k}$. Otherwise, B is the Jacobian of a genus 2 curve over $\overline{k}$, and we say $\{F_1(X), F_2(X), F_3(X)\}$ is *nonsingular*.

For a nonsingular quadratic splitting, the following classical construction gives a curve $\widetilde{C}_1$ such that $B = \operatorname{Jac}(\widetilde{C}_1)$ over $\overline{k}$. Suppose $\{F_1(X), F_2(X), F_3(X)\}$ is nonsingular. Then for $(i, j, k) = (1, 2, 3), (2, 3, 1), (3, 1, 2)$ we define

$$G_i(X) = \delta^{-1} \det\begin{pmatrix} \frac{d}{dX}F_j(X) & \frac{d}{dX}F_k(X) \\ F_j(X) & F_k(X) \end{pmatrix}$$

It is straightforward to check that $\{G_1(X), G_2(X), G_3(X)\} \subset \overline{k}[X]$ is again stable under $\operatorname{Gal}(\overline{k}/k)$. For $d \in k^*$, we consider the curve

$$\widetilde{C}_d\colon d\widetilde{Y}^2 = g(\widetilde{X}) = G_1(\widetilde{X})G_2(\widetilde{X})G_3(\widetilde{X}). \tag{4.5}$$

Lemma 4.2 *If $\delta \neq 0$, then the polynomial g is squarefree of degree 5 or 6.*

Proof This follows by direct computation; see [24, p. 122]. ■

We are now ready to review the Richelot isogeny. From [24, Theorem 8.4.11] or [4, Section 3.1] we know that over $\overline{k}$ we have $B = \operatorname{Jac}(\widetilde{C}_1)$ and that the isogeny is described by a *Richelot correspondence* defined by a curve $\Gamma_d \subset C \times \widetilde{C}_d$ over $\overline{k}$ given by

$$\Gamma_d\colon \begin{cases} F_1(X)G_1(\widetilde{X}) + F_2(X)G_2(\widetilde{X}) = 0 \\ F_1(X)G_1(\widetilde{X})(X - \widetilde{X}) = \sqrt{d}\,\widetilde{Y}Y \\ F_2(X)G_2(\widetilde{X})(X - \widetilde{X}) = -\sqrt{d}\,\widetilde{Y}Y. \end{cases}$$

The curve Γ_d covers both C and $\widetilde{C}_d$. The Richelot isogeny can be computed by taking divisor classes on C, pulling back to Γ_d, and then pushing down to $\widetilde{C}_d$.

https://doi.org/10.4153/CJM-2011-039-3 Published online by Cambridge University Press

There are two cases where it is easy to see for which twist d we have $\mathrm{Jac}(\widetilde{C}_d) = B$.

First, if $F_1, F_2, F_3 \in k[X]$ and $d = 1$, then Γ_d is defined over k and hence $B = \mathrm{Jac}(\widetilde{C}_1)$ over k.

Second, if F_1 and F_2 are quadratic conjugate, say over an extension $k(\sqrt{d})$, then F_3 is necessarily defined over k. Then the set of defining equations for Γ_d is $\mathrm{Gal}(\overline{k}/k)$-stable, and hence Γ_d is defined over k. Since over $\overline{k}$, the curves $\widetilde{C}_d$ and Γ_d are isomorphic to $\widetilde{C}_1$ and Γ_1, it follows from the above discussion that Γ_d describes a correspondence giving rise to an isogeny $\mathrm{Jac}(C) \to \mathrm{Jac}(\widetilde{C}_d)$ of the desired type. Note that $d = \mathrm{disc}(L)$.

Proposition 4.3 *Let C be a genus 2 curve as in* (4.3). *Let $\Delta \subset \mathrm{Jac}(C)[2]$ be the maximal isotropic subgroup scheme over k with $\delta \neq 0$ and $\Delta \setminus \{0\} = \mathrm{Spec}(L)$. Let $d = \mathrm{disc}(L)$. Then $\mathrm{Jac}(C)/\Delta = \mathrm{Jac}(\widetilde{C}_d)$.*

Proof The cases where $\mathrm{Gal}(\overline{k}/k)$ acts non-transitively on $\Delta(\overline{k}) \setminus \{0\}$ have been dealt with above. For the general case we consider a generic model. We will prove it there and all special cases follow by specialization.

We consider the field $K = k(h_0, h_1, h_2, q_{i,j})$ with $i, j \in \{0, 1, 2\}$, let

$$L = K[T]/(T^3 + h_2T^2 + h_1T + h_0),$$

and let $Q(X) \in L[X]$ be defined by

$$Q = \sum_{i,j=0}^{2} q_{i,j} T^j X^i.$$

We now consider the curve $C\colon Y^2 = f(X) = \mathrm{Norm}_{L[X]/k[X]}(Q(X))$ over K.

We have that L/K is a cubic extension with Galois closure $L(\sqrt{d})$ over K. Using the discussion above, we know that $B = \mathrm{Jac}(\widetilde{C}_d)$ over L. However, we know that B itself is defined over K as a principally polarized variety, so B must be some twist of $\mathrm{Jac}(\widetilde{C}_d)$ that trivializes over the cubic extension L. However, we have $\mathrm{Aut}_{\overline{K}}(\mathrm{Jac}(\widetilde{C}_d)) = \mathrm{Aut}_{\overline{K}}(\widetilde{C}_d) = \{\pm 1\}$, so both only have quadratic twists. It follows that the twist must be trivial.

Specialization now yields that for any curve C of the stated form, a polarization preserving isomorphism $\mathrm{Jac}(C)/\Delta \simeq \mathrm{Jac}(\widetilde{C}_d)$ over k exists. ■

5 $(4,4)$-Split Principally Polarized Abelian Surfaces

Let J be a principally polarized abelian surface with an optimal $(4,4)$-splitting $\Phi_4\colon E_1 \times E_2 \to J$ such that the kernel $\Delta_4 \subset E_1[4] \times E_2[4]$ is the graph of an anti-isometry $\alpha_4\colon E_1[4] \to E_2[4]$. Since $E_i[2] \subset E_i[4]$, we also have $\alpha_2 = \alpha_4|_{E_1[2]}\colon E_1[2] \to E_2[2]$. The subgroup $\Delta_2 = \Delta_4 \cap (E_1 \times E_2)[2]$ is the graph of α_2, so we see that Φ_4 factors through an optimal $(2,2)$-splitting $E_1 \times E_2 \to A = (E_1 \times E_2)/\Delta_2$. We use the principal polarizations to identify $E_1 \times E_2, A, J$ with their duals. We obtain the diagram

(5.1)
$$\begin{tikzcd}
E_1 \times E_2 \arrow[r, "2\lambda_{E_1\times E_2}"] \arrow[d, "\Phi_2"] \arrow[dd, bend right, "\Phi_4"'] & (E_1 \times E_2)^\vee \arrow[r, "2"] & (E_1 \times E_2)^\vee \\
A \arrow[r, "\lambda_A"] \arrow[d, "\Psi"] & A^\vee \arrow[u, "\Phi_2^\vee"] \arrow[r, dashed, "2"] & A^\vee \arrow[u, "\Phi_2^\vee"] \\
J \arrow[rr, "\lambda_J"] & & J^\vee \arrow[u, "\Psi^\vee"] \arrow[uu, bend right, "\Phi_4^\vee"']
\end{tikzcd}$$

in which we want to establish that with the addition of the dashed arrow, the diagram is commutative. To lighten our notation, we avoid explicitly referring to the polarizations as much as possible. To this end we introduce the shorthand notation

$$\begin{aligned}
\Psi^* &= \lambda_A^{-1} \circ \Psi^\vee \circ \lambda_J, \\
\Phi_2^* &= \lambda_{E_1\times E_2}^{-1} \circ \Phi_2^\vee \circ \lambda_A, \\
\Phi_4^* &= \lambda_{E_1\times E_2}^{-1} \circ \Phi_4^\vee \circ \lambda_J.
\end{aligned}$$

Lemma 5.1 *The isogeny $\Psi\colon A \to J$ is a polarized $(2,2)$-isogeny. Furthermore,* $\ker(\Psi) \cap \ker(\Phi_2^*) = \{0\}$.

Proof It follows from [19, Lemma 16.2c] that for $p, q \in (E_1 \times E_2)[4]$, we have that $e_{(E_1\times E_2)[4]}(p,q) = e_{A[2]}(\Phi_2(p), \Phi_2(q))$. Hence we see that $\ker(\Psi) = \Phi_2(\Delta_4) \subset A[2]$ is maximal isotropic, so by Lemma 2.4 there is a principal polarization $\lambda'\colon J \to J^\vee$ such that $2\lambda_A = \Psi^\vee \circ \lambda' \circ \Psi$. It follows that

$$\Phi_2^\vee \circ \Psi^\vee \circ \lambda' \circ \Psi \circ \Phi_2 = 4\lambda_{E_1\times E_2} = \Phi_4^\vee \circ \lambda_J \circ \Phi_4,$$

so the image of $(\lambda' - \lambda_J) \circ \Phi_4$ is contained in $\ker(\Phi_4^\vee)$, which is finite. On the other hand, Φ_4 is surjective and J is connected, so $\lambda' - \lambda_J$ is constant and hence $\lambda' = \lambda_J$. This establishes that Ψ is indeed a polarized $(2,2)$-isogeny.

In order to see that $\ker(\Psi) \cap \ker(\Phi_2^*) = \{0\}$, note that Φ_2 is injective on $E_1[2] \times \{0\}$ and maps it onto $\ker(\Phi_2^*)$, because $\Phi_2^* \circ \Phi_2 = 2$. Since $\Psi \circ \Phi_2$ is injective on $E_1[4] \times \{0\}$, it follows that Ψ is also injective on $\Phi_2(E_1[2] \times \{0\}) = \ker(\Phi_2^*)$. This shows that $\ker(\Psi) \cap \ker(\Phi_2^*) = \{0\}$. ■

In fact, whether $\Psi \circ \Phi$ is a $(4,4)$-isogeny is completely determined by $\ker(\Psi) \cap \ker(\Phi^*)$.

Lemma 5.2 *Let A, B, and J be polarized abelian surfaces and suppose that $\Phi^*\colon A \to B$ and $\Psi\colon A \to J$ are polarized $(2,2)$-isogenies. Then $\Psi \circ \Phi\colon B \to J$ is a polarized $(4,4)$-isogeny if and only if* $\ker(\Psi) \circ \ker(\Phi^*) = \{0\}$. *It is a $(4,2,2)$-isogeny if and only if* $\ker(\Psi) \cap \ker(\Phi^*) \simeq \mathbb{Z}/2\mathbb{Z}$, *and it is a $(2,2,2,2)$-isogeny if and only if* $\ker(\Psi) = \ker(\Phi^*)$.

https://doi.org/10.4153/CJM-2011-039-3 Published online by Cambridge University Press

Proof It is immediate that $\Psi \circ \Phi$ is a polarized isogeny. The nature of the isogeny can be read off from the kernel, so we investigate what these isogenies do on the 4-torsion. The isogenies we consider fit in the following commutative diagram.

$$\begin{tikzcd}
B[4] \arrow[rr, "2"] \arrow[dr, "\Phi"'] & & B[4] \arrow[rr, "2"] \arrow[dr, "\Phi"] & & B[4] \\
& A[4] \arrow[ur, "\Phi^*"] \arrow[rr, "2"] \arrow[dr, "\Psi"'] & & A[4] \arrow[ur, "\Phi^*"'] & \\
& & J[4] \arrow[ur, "\Psi^*"'] & &
\end{tikzcd}$$

Each of $B[4](\bar{k}), A[4](\bar{k})$, and $J[4](\bar{k})$ is isomorphic to $(\mathbb{Z}/4\mathbb{Z})^4$ as a $\mathbb{Z}$-module. We normalize the choice of basis such that the Weil pairing on each is given by

$$e(\underline{v}, \underline{w}) = \underline{v}^T \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix} \underline{w}.$$

The following are matrices that correspond to polarized $(2,2)$-isogenies:

$$M = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad M^* = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix},$$

$$N = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad N^* = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix},$$

where $MM^* = NN^* = 2\mathrm{id}$. It is straightforward to check that $\ker(NM) \simeq (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})^2$ and that $\ker(MM) = (\mathbb{Z}/4\mathbb{Z})^2$. Correspondingly, we find $\ker(N) \cap \ker(M^*) \simeq (\mathbb{Z}/2\mathbb{Z})$ and that $\ker(M) \cap \ker(M^*) = 0$, so only the $(4,4)$-isogeny gives rise to trivially intersecting kernels.

It remains to check that these isogenies represent all possibilities. To that end, we observe that a $(2,2)$ isogeny is determined up to isomorphism by its kernel, and that there are 15 maximal isotropic subgroups in $(\mathbb{Z}/2\mathbb{Z})^4$. It is straightforward to check that if we choose two such subgroups K_1, K_2, then there is a transformation $T \in \mathrm{Sp}_4(\mathbb{Z}/2\mathbb{Z})$ such that (TK_1, TK_2) is one of

$$\big(\ker(M^*)[2], \ker(M^*)[2]\big), \big(\ker(M^*)[2], \ker(M)[2]\big), \big(\ker(M^*)[2], \ker(N)[2]\big).$$

This shows that by choice of basis, one can ensure that the isogenies considered are indeed represented by the matrices given. ■

Lemma 3.1 and Theorem 3.2 imply that if $j(E_1) \neq j(E_2)$, then $A = \mathrm{Jac}(C_2)$ for some genus 2 curve C_2. Similarly, we expect J to be a Jacobian outside some special conditions. Remark 5.3 and Proposition 5.4 describe such special conditions. In fact, Theorem 1.1 establishes that these describe all cases where J is not a Jacobian.

Remark 5.3 A 3-isogeny $\phi\colon E_1 \to E_2$ induces an anti-isometry $\alpha_4\colon E_1[4] \to E_2[4]$. By Proposition 2.9, we have $J = E_1 \times E_2$ in this case.

If $j(E_1) \neq 0$, then $j(E_2) \neq j(E_1)$, so $A = \mathrm{Jac}(C_2)$. The 3-isogeny $-\phi$ gives rise to the same A, J but a different $(4,4)$-splitting, so we find that C_2 is a genus 2 curve that is a double cover of E_1 and of E_2 in 3 different ways; see also [10]. If $j(E_1) = j(E_2) = 0$, we find that A is not a Jacobian.

Proposition 5.4 *Let E be an elliptic curve with discriminant D. Suppose that E has a rational point $T_1 \in E[2](k)$ of order two.*

If D is a square, then $E[2](k) = \{0, T_1, T_2, T_3\}$ and E has three 2-isogenies $\phi_i\colon E \to E/\langle T_i\rangle$. The morphism

$$(5.2)\qquad \begin{array}{ccccccccc} \Phi\colon & E & \times & E & \to & E/\langle T_2\rangle & \times & E/\langle T_3\rangle & \\ & (\,P & , & Q\,) & \mapsto & (\,\phi_2(P+Q) & , & \phi_3(P-Q) &) \end{array}$$

is an optimal $(4,4)$-splitting.

If D is not a square, then $E[2](k(\sqrt{D})) = \{0, T_1, T_2, T_3\}$ and (5.2) descends to a $(4,4)$-splitting over k denoted by

$$\Phi'\colon E \times E^{(D)} \to \Re_{k(\sqrt{D})/k}\bigl(E/\langle T_2\rangle\bigr).$$

Proof If E has square discriminant, then we know that the extension generated by $E[2](\bar{k})$ is either k or a cyclic cubic extension. The assumption that $T_1 \in E[2](k)$ implies it is the former.

In this case, it is clear that Φ is an isogeny of degree 16, defined over k. To check that Φ is an optimal $(4,4)$-splitting, we determine $\ker(\Phi)(\bar{k})$. Suppose that $(P, Q) \in \ker(\Phi(\bar{k}))$. Then $Q = P$ if $2P = 0$ or $2P = T_2$, and $Q = -P$ if $2P = T_3$ or $2P = T_2 + T_3$.

We fix generators $E[4](\bar{k}) = \langle P_2, P_3\rangle$ with $2P_2 = T_2$ and $2P_3 = T_3$. Then $Q = \alpha(P)$ where $\alpha\colon E[4](\bar{k}) \to E[4](\bar{k})$ is defined by $P_2 \mapsto P_2$ and $P_3 \mapsto -P_3$. This is indeed an anti-isometry.

If D is a non-square, then we can still define Φ over $k(\sqrt{D})$. The domain and codomain of Φ' are isomorphic over $k(\sqrt{D})$ to those of Φ. Checking that Φ descends to Φ' over k is a straightforward exercise in checking Galois actions. ■

6 2-Level Structure on Curves of Genus 2

The main result in this section is the proof of Theorem 1.5. We also discuss how the result can be interpreted in terms of moduli spaces of genus 2 curves.

Proof of Theorem 1.5 Let $C : Y^2 = f(X)$ be a curve of genus 2 over a field k of odd characteristic and let $J = \mathrm{Jac}(C)$. Recall from Section 4 that $J[2](\bar{k})$ can be represented by differences of Weierstrass points of C. It follows that the action of $\mathrm{Gal}(\bar{k}/k)$

https://doi.org/10.4153/CJM-2011-039-3 Published online by Cambridge University Press

on $J[2](\bar{k})$, which is through $\mathrm{Sp}_4(\mathbb{Z}/2\mathbb{Z})$, factors through the action on the 6 Weierstrass points, which is through S_6. This yields a homomorphism $S_6 \to \mathrm{Sp}_4(\mathbb{Z}/2\mathbb{Z})$ and it is straightforward to check that it is an isomorphism.

We have also seen that maximal isotropic subgroups of $J[2]$ correspond to quadratic splittings of $f(X)$. It is straightforward to check that S_6 acts transitively on the quadratic splittings of $f(X)$. If $J[2]$ has a polarized $(2,2)$-isogeny over k, then $f(X)$ must have a Galois-stable quadratic splitting. We have

$$\mathrm{Stab}_{S_6}\big(\{\{1,2\},\{3,4\},\{5,6\}\}\big) \simeq (C_2)^3 \rtimes S_3.$$

Furthermore, the remaining 14 quadratic splittings have two orbits under $(C_2)^3 \rtimes S_3$, one of length 6 and one of length 8. If $J[2]$ is to have two k-rational polarized $(2,2)$-isogenies then $\mathrm{Gal}(\bar{k}/k)$ should act through the stabilizer subgroup of a representative of one of those orbits. If we pick a stabilizer subgroup of the first orbit, we obtain

$$C_2 \times C_4 = \big\langle (12), (34)(56), (35), 46) \big\rangle$$

stabilizing 3 quadratic splittings

$$\big\{\{1,2\},\{3,4\},\{5,6\}\big\},\ \big\{\{1,2\},\{3,5\},\{4,6\}\big\},\ \big\{\{1,2\},\{3,6\},\{4,5\}\big\} \tag{6.1}$$

and for the second orbit we obtain

$$\widetilde{S_3} = \langle (135)(246), (12)(36)(45) \rangle$$

stabilizing

$$\big\{\{1,2\},\{3,4\},\{5,6\}\big\},\ \big\{\{1,4\},\{2,5\},\{3,6\}\big\},\ \big\{\{1,6\},\{2,3\},\{4,5\}\big\}. \tag{6.2}$$

Combining this with Lemma 5.2 yields that (6.1) corresponds to isogenies that combine to $(4,2,2)$-isogenies and that (6.2) corresponds to isogenies that combine to $(4,4)$-isogenies, completing the proof of Theorem 1.5. ■

Lemma 6.1 *Let k be a field with $\mathrm{char}(k) \neq 2$. Let $\Phi_4\colon E_1 \times E_2 \to J$ be an optimal $(4,4)$-splitting over k that factors through the $(2,2)$-splitting $\Phi_2\colon E_1 \times E_2 \to A$. Suppose that $A = \mathrm{Jac}(C_2)$, where C_2 is a curve of genus 2. Then C_2 admits a model of the form*

$$C_2\colon Y^2 = g(X) = f(X^2) = c_3X^6 + c_2X^4 + c_1X^2 + c_0$$

such that $g(X)$ and $f(X)$ have the same splitting field and $\mathrm{Gal}(g)$ is isomorphic to $\widetilde{S_3}$ as a permutation group.

Proof By Theorem 3.2, the curve C_2 admits a model of the given form, where $V^2 = f(U)$ is a model of E_1. It remains to prove that $g(X)$ and $f(X)$ have the same splitting field.

Let L denote the splitting field of g and let K denote the splitting field of f. Then K is an extension of k, and either L is a degree two extension of K or $L = K$. By Theorem 1.5 we know that $\mathrm{Gal}(L/k) \leq \widetilde{S_3}$.

https://doi.org/10.4153/CJM-2011-039-3 Published online by Cambridge University Press

The three kernels of the $(2,2)$-isogenies that are fixed by $\widetilde{S}_3$ are given by the partitionings in (6.2). A simple verification shows that $\widetilde{S}_3$ acts faithfully on each of these kernels. In particular, if $\{0, T_1, T_2, T_3\}$ is the kernel of the polarized $(2,2)$-isogeny $\mathrm{Jac}(C_2) \to E_1 \times E_2$, then $\widetilde{S}_3$ has the canonical S_3-action on $\{T_1, T_2, T_3\}$. Thus, $\widetilde{S}_3$ has the usual S_3 action on the roots of f. It follows that f and g have the same splitting field. ■

While the proof of and the condition given in Theorem 1.5 are Galois-theoretic, specifying multiple $(2,2)$-isogenies on $\mathrm{Jac}(C)$ amounts to specifying partial level structure, so one expects that the structure of the result is reflected in covers of moduli spaces as well. We will sketch how one can obtain such a formulation.

Let k be a field of characteristic different from 2. Any curve of genus 2 can be obtained by specializing $(f_0, \dots, f_6)$ in the curve

$$C_{\underline{f}} \colon Y^2 = f(X) = f_6X^6 + f_5X^5 + \cdots + f_0$$

over $k(\underline{f}) = k(f_6, f_5, \dots, f_0)$. Similarly, any curve of genus 2 with all of its Weierstrass points labelled can be obtained by specializing $(w_1, \dots, w_6, f_6)$ in the curve

$$C_{\underline{w}} \colon Y^2 = f_6(X - w_1) \cdots (X - w_6)$$

over $k(\underline{w}) = k(f_6, w_1, \dots, w_6)$. Of course, one can just forget a labelling to obtain a curve $C_{\underline{f}}$ from $C_{\underline{w}}$. This allows us to express $k(\underline{w})$ as a finite extension of $k(\underline{f})$ via

$$\begin{aligned} f_5 &= -f_6(w_1 + \cdots + w_6) \\ f_4 &= f_6(w_1w_2 + w_1w_3 + \cdots + w_5w_6) \\ &\ \ \vdots \\ f_0 &= f_6w_1 \cdots w_6 \end{aligned}$$

In fact, $k(\underline{w})$ is a splitting-field of $f(X)$ over $k(\underline{f})$ and $\mathrm{Gal}(k(\underline{w})/k(\underline{f})) = S_6$. As we observed in the proof of Theorem 1.5, $k(\underline{w})$ is also the splitting field of $\mathrm{Jac}(C_{\underline{f}})[2]$ over $k(\underline{f})$. The fractional linear transformations on the X-line below C induce a $\mathrm{PGL}_2(\overline{k})$-action on $k(\underline{f})$ and $k(\underline{w})$. If we divide out by this action, we obtain a relation with the function fields of the coarse moduli spaces $\mathcal{M}_2$ of curves of genus 2 and $\mathcal{M}_2(2)$ of curves of genus 2 with full level 2-structure on their Jacobians, which is an $\mathrm{Sp}_4(\mathbb{F}_2)$-cover of $\mathcal{M}_2$

$$\begin{tikzcd}
k(\underline{w}) \arrow[dr, "\cdot/\mathrm{PGL}_2(k)"] \arrow[dd, "\cdot/S_6"'] & \\
& k(\mathcal{M}_2(2)) \arrow[dd, "\cdot/\mathrm{Sp}_4(\mathbb{F}_2)"] \\
k(\underline{f}) \arrow[dr, "\cdot/\mathrm{PGL}_2(k)"'] & \\
& k(\mathcal{M}_2)
\end{tikzcd}$$

https://doi.org/10.4153/CJM-2011-039-3 Published online by Cambridge University Press

$$\begin{tikzcd}[column sep=small]
 & k(\underline{w}) \arrow[dl, dash] \arrow[dr, dash] & & & & \langle(1)\rangle \arrow[dl, dash] \arrow[dr, dash] & \\
K_2 \arrow[dr, dash] & & K_3 \arrow[dl, dash] & & \widetilde{S}_3 \arrow[dr, dash] & & C_2 \times V_4 \arrow[dl, dash] \\
 & K_1 \arrow[d, dash] & & & & (C_2)^3 \rtimes S_3 \arrow[d, dash] & \\
 & k(\underline{f}) & & & & S_6 &
\end{tikzcd}$$

$$\begin{aligned}
(C_2)^3 \rtimes S_3 &= \langle (12), (34), (56), (13)(24), (15)(26) \rangle \\
\widetilde{S}_3 &= \langle (135)(246), (12)(36)(45) \rangle \\
C_2 \times V_4 &= \langle (12), (34)(56), (35)(46) \rangle
\end{aligned}$$

Figure 6.1: Galois groups associated with intermediate 2-level structure

The subgroups identified in Theorem 1.5 give rise to intermediate fields K_1, K_2, and K_3 as depicted in Figure 6.1 and, by dividing out by $\mathrm{PGL}_2(\mathbb{F}_2)$, to moduli spaces between $\mathcal{M}_2$ and $\mathcal{M}_2(2)$. One of the interesting phenomena here, which does not occur for elliptic curves, is that there are two non-conjugate ways of specifying two maximal isotropic subgroups of $\mathrm{Jac}(C)[2]$ and hence that there are multiple partial level 2 structures that can be imposed on $\mathrm{Jac}(C)[2]$.

7 Bielliptic Genus 2 Curves with S_3 as a Galois group

In Section 5 we saw that a $(4,4)$-splitting $E_1 \times E_2 \longrightarrow J$ gives rise to a $(2,2)$-splitting $E_1 \times E_2 \longrightarrow A$, where A is a principally polarized abelian surface admitting two rational polarized $(2,2)$-isogenies with trivially intersecting kernels.

In this section, we give something close to a universal model for the genus 2 curve C_2 from Lemma 6.1. Since the corresponding moduli space of genus 2 curves is not a fine moduli space (the space $\mathcal{M}_2(2)$ is not even fine), a universal curve does not exist. However, by allowing extra parameters, we can still give a family that covers all possible C_2 by specialization, similar to how any elliptic curve can be obtained by specializing a general Weierstrass model $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$.

Let k be a field of characteristic distinct from 2 or 3. Let C_2 be a genus 2 curve over k with a $(2,2)$-split Jacobian and let E_1 be a degree 2 subcover of C_2. Then E_1 has a model $V^2 = f(U) = U^3 + bU + c$ and $\mathrm{Gal}(f)$, the Galois group of f, is a subgroup of S_3. In order to produce the family, we concentrate on the most general case $\mathrm{Gal}(f) = S_3$. We will argue later that other cases are also parametrized.

https://doi.org/10.4153/CJM-2011-039-3 Published online by Cambridge University Press

By Theorem 3.2, the curve C_2 admits a model $Y^2 = g(X)$, where

$$g(X) = f\Big(\frac{X^2}{d} + a\Big) \text{ with } a, d \in k.$$

Working in the extension $k[U]/(f(U)) = k[r]$, the polynomials f and g factor as

$$f(U) = (U - r)\big(U^2 + rU + (r^2 + b)\big)$$
$$g(X) = \frac{1}{d^3}(X^2 + ad - rd)h(x),$$

where

$$h(X) = X^4 + (dr + 2ad)X^2 + d^2(r^2 + ar + a^2 + b).$$

By Lemma 6.1, we know that g and f have the same splitting field. This means that h must be reducible over $k(r)$. Otherwise h would be irreducible, and we would require a degree 4 extension over $k(r)$ to split h. The following lemma gives a testable condition.

Lemma 7.1 (Kappe and Warren [15]) *Let $h(x) = x^4 + bx^2 + d$ be a polynomial over a field k of characteristic $\neq 2$ and let $\pm\alpha$, $\pm\beta$ be its roots. Then the following conditions are equivalent:*

(1) *$h(x)$ is irreducible over k;*

(2) *The following are not squares in k:*

(i) $b^2 - 4d$,

(ii) $-b + 2\sqrt{d}$, *and*

(iii) $-b - 2\sqrt{d}$.

We can use Lemma 7.1 to determine the conditions on a and d such that h factors as a product of two quadratics over $k(r)$. In our case, the polynomial h will be reducible over $k(r)$ if one of the following is true:

(i) $(dr + 2ad)^2 - 4d^2\left(r^2 + ar + a^2 + b\right)$ is a square in $k(r)$, or

(ii) $-(dr + 2ad) + 2d\sqrt{r^2 + ar + a^2 + b}$ is a square in $k(r)$, or

(iii) $-(dr + 2ad) - 2d\sqrt{r^2 + ar + a^2 + b}$ is a square in $k(r)$.

In case (i), after simplification, we require $-3r^2 - 4b$ to be a square. Observe that this is the discriminant of $x^2 + rx + (r^2 + b)$ and hence occurs exactly when our original polynomial $f(x)$ splits over $k(r)$. This contradicts $\mathrm{Gal}(f) = S_3$, so we ignore this possibility for now.

In the remaining two cases, we require $r^2 + ar + a^2 + b$ to be a square in $k(r)$. Let $t \in k(r)$ such that $r^2 + ar + a^2 + b = t^2$. Since $k(r)$ is a cubic extension of k, we can set $t = t_2r^2 + t_1r + t_0$. It follows that

$$\begin{aligned} r^2 + ar + a^2 + b &= (t_2r^2 + t_1r + t_0)^2 \\ &= t_2^2r^4 + 2t_1t_2r^3 + (t_1^2 + 2t_0t_2)r^2 + 2t_0t_1r + t_0^2 \\ &= (t_1^2 + 2t_0t_2 - bt_2^2)r^2 + (2t_0t_1 - 2bt_1t_2 - ct_2^2)r + (t_0^2 - 2ct_1t_2). \end{aligned}$$

https://doi.org/10.4153/CJM-2011-039-3 Published online by Cambridge University Press

Equating coefficients, we obtain the system of three equations:

$$t_1^2 + 2t_0t_2 - bt_2^2 - 1 = 0$$
$$-a + 2t_0t_1 - 2bt_1t_2 - ct_2^2 = 0$$
$$a^2 + b - t_0^2 + 2ct_1t_2 = 0$$

We obtain an affine variety in $\mathbb{A}^4$ with parameters b and c. This variety has two components, interchanged by $(a, t_0, t_1, t_2) \mapsto (a, -t_0, -t_1, -t_2)$, which can be found either using a primary decomposition of a polynomial ideal (*e.g.*, `PrimaryComponents` in Magma [3]), or by eliminating variables (say a and t_0) via resultants and multivariate GCD, and a multivariate polynomial factorization. Each component is a genus 0 curve in $\mathbb{A}^4$. Using for instance Magma, we can parametrize this curve. Writing s for the parameter, we obtain

$$(7.1) \qquad a = \frac{s^4 - 2bs^2 - 8cs + b^2}{4(s^3 + bs + c)} \qquad t_0 = \frac{-s^4 - 6bs^2 - 4cs - b^2}{4(s^3 + bs + c)}$$
$$t_1 = \frac{-s^3 + bs + 2c}{2(s^3 + bs + c)} \qquad t_2 = \frac{-3s^2 - b}{2(s^3 + bs + c)}.$$

For any $s \in k$, this parametrization gives a value for a such that $r^2 + ar + a^2 + b$ is a square in $k(r)$. Using the parametrization, we can express the square root of $r^2 + ar + a^2 + b$ as

$$\frac{-3s^2 - b}{2(s^3 + bs + c)} r^2 + \frac{-s^3 + bs + 2c}{2(s^3 + bs + c)} r + \frac{-s^4 - 6bs^2 - 4cs - b^2}{4(s^3 + bs + c)}.$$

This allows us to evaluate the expressions in (ii) and (iii). In case (ii) we find that $-(dr + 2ad) + 2d\sqrt{r^2 + ar + a^2 + b}$ becomes

$$\left(-\frac{1}{4(s^3 + bs + c)}\right) \cdot d \cdot F_1,$$

where $F_1 = \left(6s^3 + 2bs\right) r^2 - \left(6s^3 + 2bs\right) r - \left(3s^4 + 2bs^2 - 12cs + 3b^2\right)$. This is a square in $k(r)$ if and only if

$$(7.2) \qquad d = -(s^3 + bs + c) \cdot \square,$$

where $\square$ represents a square in k. Using (7.1) and (7.2), we find that $g(X) = f(X^2/d + a)$ has the same splitting field as f. The Galois group of g is indeed isomorphic to S_3, but its representation in S_6 is $S_3'' = \langle (123)(456), (23)(56) \rangle$, which is not conjugate to $\widetilde{S_3}$ from Section 6. Therefore, $C\colon Y^2 = g(X)$ is not of the form predicted by Lemma 6.1.

In case (iii), we find that $-(dr + 2ad) - 2d\sqrt{r^2 + ar + a^2 + b}$ becomes

$$\left(-\frac{1}{4(s^3 + bs + c)}\right) \cdot d \cdot F_2,$$

where $F_2 = \left(6s^2 + 2b\right) r^2 - (2s^3 + 6bs + 8c)r - (s^4 + 10bs^2 - 20cs + b^2)$. This is a square in $k(r)$ if and only if

$$d = \left(4b^3 + 27c^2\right) \left(s^3 + bs + c\right) \cdot \square = -D \cdot f(s) \cdot \square, \tag{7.3}$$

where $\square$ represents a square in k and D is the discriminant of f.

Using this parametrization, our hyperelliptic curve C_2 is given by $Y^2 = g(X)$ where:

(7.4)

$$g = \frac{1}{(s^3 + bs + c)^3} \left(\frac{1}{\left(4b^3 + 27c^2\right)^3} X^6 + \frac{3\left(s^4 - 2bs^2 - 8cs + b^2\right)}{4\left(4b^3 + 27c^2\right)^2} X^4 \right.$$
$$\left. + \frac{P(b, c, s)}{16\left(4b^3 + 27c^2\right)} X^2 + \frac{\left(s^6 + 5bs^4 + 20cs^3 - 5b^2s^2 - 4bcs - b^3 - 8c^2\right)^2}{64} \right),$$

and where P is given by

$$P = 3s^8 + 4bs^6 - 48cs^5 + 50b^2s^4 + 128bcs^3 + 4b^3s^2 + 192c^2s^2 - 16b^2cs + 3b^4 + 16bc^2.$$

As desired, we find that g has the same splitting field as f and that $\mathrm{Gal}(g) \simeq \widetilde{S_3}$ as found in Section 6. The factorization for g over its splitting field is given in Appendix B.

Let $\phi_1 \colon C_2 \longrightarrow E_1$ be the cover arising from $(X, Y) \mapsto (U, V) = (X^2/d + a, Y)$. Let $\Psi\colon \operatorname{Jac}(C_2) \longrightarrow B$ be one of the other polarized $(2, 2)$-isogenies we have by construction on $\operatorname{Jac}(C_2)$. Let

$$E_s \colon W^2 = -\operatorname{disc}(f) \cdot f(s) \cdot (U - a) \cdot f(U)$$

be the complementary curve and $\phi_2 \colon C_2 \longrightarrow E_s$ the corresponding cover. It is straightforward to check that $\Psi \circ \phi^* \colon E_1 \longrightarrow B$ is injective and hence that $\Phi_4 = \Psi \circ (\phi_1^* + \phi_2^*) \colon E_1 \times E_s \longrightarrow B$ is an optimal $(4, 4)$-splitting of B. This means that the data we have specified (s and Ψ) should also determine an anti-isometry $\alpha_s \colon E_1[4] \longrightarrow E_s[4]$. The ambiguity of choice in Ψ corresponds to the fact that if $\alpha_s \colon E_1[4] \longrightarrow E_s[4]$ is an anti-isometry, then so is $-\alpha_s$.

Let $X^-_{E_1}(4)$ be the completion of the moduli space of elliptic curves with prescribed 4-torsion structure anti-isometric to $E_1[4]$ modulo multiplication by $(\mathbb{Z}/4\mathbb{Z})^\times$. This is a cover of the j-line $X(1)$, Galois over $\overline{k}$, with

$$\operatorname{Aut}_{\overline{k}}(X^-_{E_1}(4)/X(1)) = \mathrm{PSL}_2(\mathbb{Z}/4\mathbb{Z}),$$

so $X^-_{E_1}(4) \longrightarrow X(1)$ is a degree 24 cover.

On the open part of the s-line where the equation for E_s defines an elliptic curve, the map $s \mapsto E_s$ provides a map from the s-line to $X^-_{E_1}(4)$. This map cannot be constant, since $a(s)$ is not constant in s, so we can interpret the s-line as a cover of $X^-_{E_1}(4)$. It turns out to be an isomorphism, and E_s provides a model of the universal elliptic curve over $X^-_{E_1}(4)$. This provides an alternative construction to the one given by Silverberg [23]. Our formulas are shorter.

https://doi.org/10.4153/CJM-2011-039-3 Published online by Cambridge University Press

Proposition 7.2 *Let $b, c \in k$ such that $4b^3 + 27c^2 \neq 0$ and let*

$$E\colon V^2 = f(U) = U^3 + bU + c$$

be an elliptic curve. Let s be a parameter on $\mathbb{P}^1$ and consider

$$E_s\colon W^2 = -\operatorname{disc}(f)\,\big(4(s^3+bs+c)U - (s^4 - 2bs^2 - 8cs + b^2)\big)\, f(U),$$

with $(U, W) = (\frac{s^4-2bs^2-8cs+b^2}{4(s^3+bs+c)}, 0)$ taken to be the identity element. Then E_s is isomorphic to

$$\begin{aligned}
\widetilde{E}_s\colon y^2 &= x^3 + a_4x + a_6 \textit{ with}\\
a_4 &= (4b^3+27c^2)^2(s^8b + 12s^7c - 28/3s^6b^2 - 28s^5bc - 14/3s^4b^3 - 84s^4c^2\\
&\quad + 28/3s^3b^2c - 28/3s^2b^4 - 56s^2bc^2 - 44/3sb^3c - 96sc^3 + b^5 + 20/3b^2c^2)\\
a_6 &= -(4b^3+27c^2)^3(s^{12}c - 8/3s^{11}b^2 - 22s^{10}bc + 88/27s^9b^3 - 88s^9c^2 + 55s^8b^2c\\
&\quad - 176/9s^7b^4 - 308/9s^6b^3c - 176/9s^5b^5 - 176s^5b^2c^2 - 649/9s^4b^4c\\
&\quad - 528s^4bc^3 + 88/27s^3b^6 - 704/9s^3b^3c^2 - 704s^3c^4 + 154/9s^2b^5c\\
&\quad + 352/3s^2b^2c^3 - 8/3sb^7 - 248/9sb^4c^2 - 64sbc^4 - 5/3b^6c\\
&\quad - 560/27b^3c^3 - 64c^5)
\end{aligned}$$

with

$$j(\widetilde{E}_s) = \frac{256}{4b^3+27c^2}\,\frac{\begin{pmatrix} 3bs^8 + 36cs^7 - 28b^2s^6 - 84bcs^5 - 14(b^3+18c^2)s^4 + 28b^2cs^3\\ -28b(b^3+6c^2)s^2 - 4c(11b^3+72c^2)s + 3b^5 + 20b^2c^2\end{pmatrix}^3}{(s^6 + 5bs^4 + 20cs^3 - 5b^2s^2 - 4bcs - b^3 - 8c^2)^4}.$$

The map $s \mapsto E_s$ induces an isomorphism $\mathbb{P}^1 \to X_E^-(4)$, and $\widetilde{E}_s$ provides a model of the universal curve over $X_E^-(4)$. For $s = \infty$ we find that $\widetilde{E}_\infty$ is isomorphic to the quadratic twist $E^{(D)}$ of E by $D = \operatorname{disc}(E)$.

Proof The computation of the model $\widetilde{E}_s$ and its j-invariant are straightforward. It establishes that $s \mapsto j(E_s)$ induces a degree 24 cover $\mathbb{P}^1 \to X(1)$. We have already established that $s \mapsto E_s$ induces a cover $\mathbb{P}^1 \to X_{E_1}^-(4)$. The map induced by $s \mapsto j(E_s)$ factors through $j\colon X_{E_1}^-(4) \to X(1)$, which also has degree 24, so the first map must be of degree 1 and hence an isomorphism.

The only point where the curve defined by $\widetilde{E}_s$ might not be immediately clear is for $s = \infty$. However, we can consider the isomorphic model $y^2 = x^3 + a_4/s^8x + a_6/s^{12}$. Then we find that

$$\frac{a_4}{s^8}\bigg|_{s=\infty} = (4b^3+27c^2)^2b \quad \text{and} \quad \frac{a_6}{s^{12}}\bigg|_{s=\infty} = -(4b^3+27c^2)^3c,$$

which confirms that $E_\infty = E^{(D)}$ with $D = -16(4b^3+27c^2) = \operatorname{disc}(E)$. ■

https://doi.org/10.4153/CJM-2011-039-3 Published online by Cambridge University Press

Note that the description of E_s is even shorter than that of $\widetilde{E}_s$, but E_s has the drawback of not being a Weierstrass-form and not specializing to an elliptic curve for $s^3 + bs + c = 0$. It does show very nicely where the denominator of $j(\widetilde{E}_s)$ comes from. This denominator vanishes exactly when $f(\frac{s^4-2bs^2-8cs+b^2}{4(s^3+bs+c)}) = 0$.

Corollary 7.3 *Let $E_1 \colon V^2 = U^3 + bU + c$ be an elliptic curve. The affine variety $\mathbb{P}^1_s \setminus \{s^6 + 5bs^4 + 20cs^3 - 5b^2s^2 - 4bcs - b^3 - 8c^2\}$ parametrizes principally polarized abelian surfaces J_s together with a pair of optimal $(4,4)$-splittings $\pm\Phi_4 \colon E_1 \times E_s \to J_s$.*

Corollary 7.4 *Let E be an elliptic curve over a field k with $\operatorname{char}(k) \neq 2$. Let D be the discriminant of E. Then there is an anti-isometry $\alpha_4 \colon E[4] \to E^{(D)}[4]$.*

Proof Apart from the proof by specialization that is part of Proposition 7.2, there is also a Galois-representation theoretic way of proving Corollary 7.4. This is interesting because it identifies how $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ permits such an anti-isometry. Let E be an elliptic curve over a field k with discriminant D and let $\rho\colon \operatorname{Gal}(\overline{k}/k) \to \operatorname{Aut}(E[4])$ be the mod 4 Galois representation. We have $\operatorname{Aut}(E[4]) \simeq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$. Let H be the subgroup of elements that act via even permutation on the 2-torsion elements. Note that D is also the discriminant of the 2-torsion algebra, so $\rho^{-1}(H) = \operatorname{Gal}(\overline{k}/k(\sqrt{D}))$.

Consider

$$M = \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$$

and let $\alpha_M \colon E[4] \to E[4]$ be the corresponding automorphism. One can check that $\{M, -M\}$ is the unique conjugacy class of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ of size 2 and that the centralizer of M is H. It follows that α_M is defined over $k(\sqrt{D})$. Furthermore, since

$$M \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} M^T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

we see that $\alpha_M \colon E[4] \to E[4]$ is an *anti*-isometry.

Now consider the quadratic twist $E^{(D)}$ of E. There is an isomorphism $E \to E^{(D)}$ defined over $k(\sqrt{D})$, which when restricted, yields an isometry $\alpha^{(D)} \colon E[4] \to E^{(D)}[4]$. The composition $\alpha^{(D)} \circ \alpha_M \colon E[4] \to E^{(D)}[4]$ is an anti-isometry. Furthermore, if $\sigma \in \operatorname{Gal}(\overline{k}/k)$ and $\sigma(\sqrt{D}) = -\sqrt{D}$, then $\sigma(\alpha_M) = -\alpha_M$ and $\sigma(\alpha^{(D)}) = -\alpha^{(D)}$. Hence, $\sigma(\alpha^{(D)} \circ \alpha_M) = \alpha^{(D)} \circ \alpha_M$, so we see that $E[4]$ and $E^{(D)}[4]$ are anti-isometric over k. ■

In Sections 3 and 5, we already observed that the abelian variety A in (5.1) is generally a Jacobian, a sufficient condition being that $j(E_1) \neq j(E_2)$. We now establish that the model $C_2 \colon Y^2 = g(X)$ with $g(X)$ as in (5.1) specializes to a genus 2 curve such that $A = \operatorname{Jac}(C_2)$ whenever A is a Jacobian.

Lemma 7.5 *Let $\Phi_4 \colon E_1 \times E_2 \to J$ be an optimal $(4,4)$-splitting and let $\Phi_2 \colon E_1 \times E_2 \to A$ be the induced $(2,2)$-splitting as in (5.1). Suppose we have a model $E_1 \colon V^2 = U^3 + bU + c$. If $A = \operatorname{Jac}(C_2)$, where C_2 is some genus 2 curve, then for some $s \in k$ we obtain a model $C_2 \colon Y^2 = g(X)$ with $g(x)$ as in (7.4). Conversely, any C_2 of this form admits a $(2,2)$-splitting Φ_2 and a further polarized $(2,2)$-isogeny $\Psi \colon \operatorname{Jac}(C_2) \to J$ such that $\Psi \circ \Phi_2 \colon E_1 \times E_2 \to J$ is an optimal $(4,4)$-splitting.*

https://doi.org/10.4153/CJM-2011-039-3 Published online by Cambridge University Press

Proof An optimal $(4,4)$-splitting is specified by an anti-isometry $\alpha_4\colon E_1[4] \to E_2[4]$. It follows from Proposition 7.2 that $E_2 \simeq E_s$ for some value of $s \in k \cup \{\infty\}$. If $s = \infty$ or $s^3 + bs + c = 0$, we have $j(E_1) = j(E_2)$, and the induced isometry $E_1[2] \to E_2[2]$ is the obvious one. In this case, $A \simeq E_1 \times E_1$ or $A \simeq \Re_{k(\sqrt{d})/k}(E_1)$; see Section 3. For all the other cases, the discriminant of the polynomial $g(X)$ defined in (7.4) is square-free as long as $j(E_s) \neq \infty$.

For the converse, $\mathrm{Jac}(C_2)$ admits an obvious $(2,2)$-splitting $\Phi_2\colon E_1 \times E_2 \to \mathrm{Jac}(C_2)$. Furthermore, there are two further $(2,2)$-isogenies Ψ defined on $\mathrm{Jac}(C_2)$ by construction. Let $\phi_1\colon C_2 \to E_1$ be the corresponding double cover. It is straightforward to check that $\phi_1^*(E_1[2]) \cap \ker(\Psi) = 0$ and hence that $\Psi \circ \Phi_2$ is an optimal $(4,4)$-splitting. ■

8 A Model for Genus 2 Curves with $(4,4)$-split Jacobian

The next step is to describe a model for a genus 2 curve C_4 with a $(4,4)$-split Jacobian. From Section 5 we know that $\mathrm{Jac}(C_4)$ is the image under a $(2,2)$-isogeny of a $(2,2)$-split principally polarized abelian surface A, admitting three $(2,2)$-isogenies with pairwise trivially intersecting kernels. Whenever $A = \mathrm{Jac}(C_2)$, Lemma 7.5 gives us a model for C_2. Section 4 provides an explicit description of $(2,2)$-isogenies between Jacobians of genus 2 curves.

In this section, we will identify the $(2,2)$-isogenies of $\mathrm{Jac}(C_2)$ defined over k and derive a description of the codomain if it is a Jacobian. This provides us with a description of C_4 with $(4,4)$-split Jacobian in case $A = \mathrm{Jac}(C_2)$.

We consider all 15 different quadratic splittings as in Section 4 over $\bar{k}$ and see which are defined over the base field. As expected, a computer calculation yields that one of the quadratic splittings is singular. It is

$$\{q_2(X-w_1)(X-w_2), q_2(X-w_3)(X-w_4), q_2(X-w_5)(X-w_6)\},$$

where w_i are the roots of g over $k[r,R]$ as listed in Appendix B and $q_2^3 = f_6$ is the leading coefficient of g. This singular splitting is due to the $(2,2)$-isogeny $\Phi_2^*\colon \mathrm{Jac}(C_2) \to E_1 \times E_2$. We also find that applying the Richelot correspondence (4.5) to the 14 generically non-singular quadratic splittings produces only two k-rational sextics, with the remaining twelve defined over $\bar{k}$, but not over k. The two quadratic splittings which yield the k-rational sextics are

(8.1) $\{q_2(X-w_1)(X-w_6), q_2(X-w_2)(X-w_3), q_2(X-w_4)(X-w_5)\}$ and

(8.2) $\{q_2(X-w_1)(X-w_4), q_2(X-w_2)(X-w_5), q_2(X-w_3)(X-w_6)\}$.

Notice that the singular quadratic splitting, together with the two quadratic splittings (8.1) and (8.2) come from the three partitionings that are fixed by $\widetilde{S_3}$, given by (6.2).

Let G_1 and G_2 denote the sextics obtained by applying Richelot's construction (4.5) of f to the quadratic splittings (8.1) and (8.2), respectively. We find that $G_2(X) = G_1(-X)$, and therefore that both models are isomorphic. This reflects that

https://doi.org/10.4153/CJM-2011-039-3 Published online by Cambridge University Press

$E_1 \times E_2$ has an extra automorphism $[1] \times [-1]$, so if Φ_4 is an optimal $(4,4)$-splitting, then $\Phi_4 \circ ([1] \times [-1])$ is another one, with the the same codomain.

Proposition 4.3 allows us to select the right twist

$$C_4 \colon Y^2 = DG_1(X) = F(X) \text{ where } D = \operatorname{disc}(f) = -4b^3 - 27c^2$$

(see Appendix C for $F(X)$ with the extraneous factor f_6^2 removed). Looking at the denominators and the discriminant of the sextic given in Appendix C, we find

$$\operatorname{disc}(F) = \frac{2^6\left(s^3 + bs + c\right)^{22}\left(s^6 + 5bs^4 + 20cs^3 - 5b^2s^2 - 4bcs - b^3 - 8c^2\right)}{\left(4b^3 + 27c^2\right)^{14}\left(3bs^4 + 18cs^3 - 6b^2s^2 - 6bcs - b^3 - 9c^2\right)^{18}}$$

and hence the following proposition.

Proposition 8.1 *The model $C_4 : Y^2 = F(X)$ with $F(X)$ as defined in Appendix* C *describes a genus* 2 *curve unless one of the following holds:*

(i) $4b^3 + 27c^2 = 0$,
(ii) $s^6 + 5bs^4 + 20cs^3 - 5b^2s^2 - 4bcs - b^3 - 8c^2 = 0$,
(iii) $3bs^4 + 18cs^3 - 6b^2s^2 - 6bcs - b^3 - 9c^2 = 0$,
(iv) $s^3 + bs + c = 0$,
(v) $s = \infty$.

Cases (i) *and* (ii) *correspond to situations where either E_1 or E_s is not an elliptic curve. Cases* (iii) *and* (iv) *correspond to $(4,4)$-split principally abelian surfaces that are not Jacobians, as described by Propositions* 2.9 *and* 5.4 *respectively.*

If $j(E_1) \neq 0$, then case (v) *corresponds to a $(4,4)$-splitting $\Phi \colon E_1 \times E_1^{(D)} \to \operatorname{Jac}(C_4')$, where*

$$C_4' \colon Y^2 = -64bc\frac{1}{D^3}X^6 + \frac{64}{3}b\frac{1}{D^2}X^5 + 16bc\frac{1}{D^2}X^4 + \frac{224}{27}b\frac{1}{D}X^3 + 4bc\frac{1}{D}X^2 + \frac{4}{3}bX - bc$$

is a curve of genus 2*. If $j(E_1) = 0$, then case* (v) *is part of case* (iii).

Proof (i) In this case E_1 is not an elliptic curve.
(ii) In Proposition 7.2 we have already seen that this relation implies $j(E_s) = \infty$.
(iii) Let δ denote the determinant of the quadratic splitting (8.1). Then

$$N_{k[r,R]/k}(\delta) = \left(4b^3 + 27c^2\right)^2\left(3bs^4 + 18cs^3 - 6b^2s^2 - 6bcs - b^3 - 9c^2\right)^2,$$

and we know that if (4.4) vanishes, then the codomain of the $(2,2)$-isogeny is a product of elliptic curves over $\overline{k}$. Proposition 8.2 explains this degeneracy.
(iv) If $s^3 + bs + c = 0$, then $(s,0) \in E_1[2]$ is a point of order two. Furthermore, from (7.1) we have $a(s) = \infty$, so the $(2,2)$-splitting Φ_2 through which our $(4,4)$-splitting factors is known to be $E_1 \times E_1 \to E_1 \times E_1$ or $E_1 \times E_1^{(D)} \to \Re_{k(\sqrt{R})/k}(E_1)$, depending on whether $D = \operatorname{disc}(E_1)$ is a square or not. Since $\#\operatorname{SL}_2(\mathbb{Z}/4\mathbb{Z}) = 8 \cdot \#\operatorname{SL}_2(\mathbb{Z}/2\mathbb{Z})$, there are 8 ways over $\overline{k}$ to extend a $(2,2)$-isogeny to a $(4,4)$-isogeny. This also follows from the computation in the proof of Lemma 5.2, where one finds

8 possible kernels for Ψ trivially intersecting $\ker(\Phi^*)$. Since every value of s gives rise to two $(4,4)$-isogenies, we see that with $s=\infty$ and $s^3+bs+c=0$, all possible $(4,4)$-splittings factoring through Φ_2 must occur for these values of s. Proposition 5.4 describes six $(4,4)$ splittings of this type, so together with the two coming from $s=\infty$, these must be all.

(v) The model for C_4 as presented does not specialize well for $s=\infty$, but the isomorphic model

$$C'_{4,s}\colon (s^3Y)^2 = F(xs^2)/s^6$$

does if $b\neq 0$, and for $s=\infty$ we obtain C'_4. Note that for generic s we have a $(4,4)$-splitting

$$\Phi_4\colon E_1\times E_s \longrightarrow \mathrm{Jac}(C'_{4,s}),$$

where the kernel is the graph of an anti-isogeny $E_1[4]\to E_s[4]$ that is independent of s. Since domain and codomain specialize well at $s=\infty$, so must the $(4,4)$-isogeny. If $b=0$, we have $j(E_1)=0$ and we have a 3-isogeny $E_1\longrightarrow E_1^{(D)}$, so case (iii) applies. ■

Proposition 8.2 *Let E and E_s be the elliptic curves described in Proposition* 7.2. *The relation $3bs^4+18cs^3-6b^2s^2-6bcs-b^3-9c^2=0$ corresponds to the existence of a* 3*-isogeny $\phi\colon E\longrightarrow E_s$.*

Proof Note that $J_1=j(E)$ and $J_2=j(E_s)$ are rational functions in s,b,c. We can express the given information in weighted homogeneous polynomial relations in s,b,c with weights $(1,2,3)$ and obtain

$$\begin{aligned}1728b^3-(b^3+27c^2/4)J_1&=0\\ N(b,c,s)-D(b,c,s)J_2&=0\\ 3bs^4+18cs^3-6b^2s^2-6bcs-b^3-9c^2&=0.\end{aligned}$$

When we eliminate b,c,s from these equations, we are left with the classical modular polynomial of level 3 in J_1,J_2. This means that there is a 3-isogeny $\phi\colon E\longrightarrow E_s$ over $\overline{k}$. Indeed, in the light of Proposition 2.9 we expect to find $(4,4)$-split surfaces of this type that are not Jacobians. A priori, the fact that the j-invariants satisfy a modular polynomial only tells us that E and E_s are 3-isogenous over $\overline{k}$. However, we know that only one twist of E_s has $E_s[4]$ anti-isometric to $E[4]$ and similarly, only one twist of E_s can be 3-isogenous to E. From Proposition 2.9 we know they must coincide.

Furthermore, in general there are only 2 anti-isometries between $E[4]$ and $E_s[4]$ for 3-isogenous curves (otherwise $E[4]$ would have extra automorphisms, requiring the Galois representation to be small). This implies that the anti-isometries induced by our parametrization of $X_E^-(4)$ must coincide with the ones from Proposition 2.9 generally and therefore also for any valid specialization of b,c,s. ■

https://doi.org/10.4153/CJM-2011-039-3 Published online by Cambridge University Press

9 Proofs of Theorems 1.1 and 1.2

Proof of Theorem 1.1 In Section 5 we established that a $(4,4)$-splitting factors Φ_4 as

$$\begin{tikzcd} E_1 \times E_2 \arrow[r, "\Phi_2"] \arrow[rr, bend right, "\Phi_4"'] & A \arrow[r, "\Psi"] & J. \end{tikzcd}$$

Let $E_1\colon V^2 = U^3 + bU + C$ be a model for E_1. If A is a Jacobian, then Lemma 7.5 provides a model for C_2 such that $A = \operatorname{Jac}(C_2)$ and if J is a Jacobian $\operatorname{Jac}(C_4)$ as well, then Section 8 shows that (C.1) provides a model for C_4.

More generally, Corollary 7.3 describes that b, c, s together parametrize all J with optimal $(4,4)$-splitting. Proposition 8.1 analyzes all the degeneracies of C_4 and identifies which correspond to the $(4,4)$-splittings described by Propositions 5.4 and 8.2. Together, these give the cases listed in Theorem 1.1. ■

Proof of Theorem 1.2 Recall that the moduli space of genus 2 curves is birational to $\mathbb{A}^3$ and that (i_1, i_2, i_3) as given in (1.1) give coordinates on that space.

Let $\mathcal{X}$ denote the surface inside $\mathbb{A}^3$ describing genus 2 curves with $(4,4)$-split Jacobians. This surface is the Humbert surface of discriminant 16, and it is irreducible (see [13, Corollaries 1.6–1.8] and [20]).

Theorem 1.1 and Proposition 8.1 show that by specializing b, c, s we can generate points on a Zariski-open part of $\mathcal{X}$. In fact, if we set $b = 1$, the points we can generate still lie dense in $\mathcal{X}$. By computing the Igusa invariants of C_4 we obtain rational functions $i_1(c,s), i_2(c,s), i_3(c,s) \in \mathbb{Q}(c,s)$ such that the image of the rational map

$$\begin{array}{ccc} \mathbb{A}^2 & \dashrightarrow & \mathbb{A}^3 \\ (c,s) & \mapsto & \big(i_1(c,s), i_2(c,s), i_3(c,s)\big) \end{array}$$

lies dense in $\mathcal{X}$. The defining equations are too large to compute the image using Gröbner bases or resultants. Instead, we will compute the image by interpolation. Our strategy consists of three steps:

(1) Determine a candidate equation $\mathcal{L}(i_1, i_2, i_3) = 0$ to describe $\mathcal{X}$;
(2) prove that $\mathcal{X}$ is contained in $\mathcal{L}(i_1, i_2, i_3) = 0$;
(3) observe that if the Zariski-closure of $\mathcal{X}$ is a proper subset of $\mathcal{L}(i_1, i_2, i_3) = 0$, then $\mathcal{X}$ must lie on a surface of lower degree and derive a contradiction from that.

For (1), we guessed degree bounds with which to interpolate $\mathcal{L}$ and computed a tentative version $\mathcal{L}_{p_i}(i_1, i_2, i_3) \pmod{p_i}$ via interpolation for 93 consecutive 6-digit primes p_i. For future reference, note that we found a unique solution to the system for each prime p_i.

We then used rational reconstruction to compute a tentative equation $\mathcal{L}(i_1, i_2, i_3) = 0$ over $\mathbb{Q}$. The equation of the surface is too large to reproduce here: $\mathcal{L}$ contains 4574 monomials with coefficients of up to 138 digits. Note that the information we computed should allow us to construct $\mathcal{L} \pmod{N}$, where $N = \prod_{i=1}^{93} p_i \approx 10^{600}$, so the coefficients we found in $\mathcal{L}$ are relatively tiny. This is a strong indicator that we have computed something that indeed has intrinsic meaning

https://doi.org/10.4153/CJM-2011-039-3 Published online by Cambridge University Press

over $\mathbb{Q}$ (at this point, basically what could go wrong is that our degree bound is too low and that we very unluckily have picked interpolation points that happen to map to points satisfying some lower degree equation as well).

For (2), we show that $\mathcal{L}(i_1(c,s), i_2(c,s), i_3(c,s))$ is identically zero in $\mathbb{Q}(c,s)$. The expression $\mathcal{L}\,(i_1(c,s), i_2(c,s), i_3(c,s)) = 0$ gives rise, after clearing denominators, to a polynomial $p(c,s)$ of degrees at most 1800 and 4050 in c and s respectively. We need to establish that $p(c,s) = 0$ as a bivariate polynomial. Expanding $p(c,s)$ explicitly is computationally infeasible, so instead we evaluate $p(c,s)$ over a large number of distinct values for c and s. For a fixed value $s = s_0$, if we show that $p(c, s_0) = 0$ at 1801 distinct values for c, then $p(c, s_0)$ is the zero polynomial on the line $s = s_0$. If we repeat this process on 4501 distinct lines $s = s_i$, then $p(c,s)$ is in fact the zero polynomial. This calculation was performed in parallel on multiple computers over the course of several weeks.

For (3), note that we have now established that the Zariski-closure of $\mathcal{X}$ is indeed contained in $\mathcal{L}(i_1, i_2, i_3) = 0$. Since $\mathcal{X}$ is irreducible (see [13, Corollary 1.8]), proper containment implies that $\mathcal{X}$ must be described by an equation of strictly lower degree. But then we would have found this lower degree equation in step (1) as well. However, we found there that $\mathcal{L}_{p_i}$ was the unique equation below the guessed degree bounds that interpolated the computed images. So $\mathcal{X}$ does not lie in a lower degree surface. ■

A On a Classical Result by Bolza

An 1887 paper by O. Bolza [1] discusses hyperelliptic integrals that can reduce into elliptic integrals by a fourth degree transformation. In the terminology of Section 2, he computes a model of a genus 2 curve with a $(4,4)$-split Jacobian. In this section we relate his results to ours. The formulas given here are available electronically from [5]. Bolza works over $\mathbb{C}$. He gives a 3-parameter family of curves $y^2 = R(x)$, with parameters λ, μ, ν, with a sign error in equation (A.1). Corrected, Bolza's family is given by:

$$\begin{aligned} C_{(\lambda,\mu,\nu)} \colon y^2 = R(x) = \nu' x^6 - 6\lambda\nu' x^5 + 3\left(4\mu\nu' + \lambda\mu'\right)x^4 + 2\left(\lambda\lambda' + 5\nu\nu'\right)x^3 \\ + 3\left(4\mu'\nu + \lambda'\mu\right)x^2 - 6\lambda'\nu x + \nu, \end{aligned}$$

where

$$\text{(A.1)} \qquad \begin{aligned} \lambda' &= -\frac{1}{3}\cdot\frac{2\lambda^2\nu - \lambda\mu^2 - \mu\nu}{-\nu^2 + 3\lambda\mu\nu - 2\mu^3}, \qquad \mu' = \frac{1}{9}\cdot\frac{\lambda^2\mu + \lambda\nu - 2\mu^2}{-\nu^2 + 3\lambda\mu\nu - 2\mu^3}, \\ \nu' &= -\frac{1}{27}\cdot\frac{2\lambda^3 - 3\lambda\mu + \nu}{-\nu^2 + 3\lambda\mu\nu - 2\mu^3}. \end{aligned}$$

He also gives the variable substitutions that turn the hyperelliptic integrals into elliptic integrals. In modern language, he gives the degree 4 maps from the curve $C_{(\lambda,\mu,\nu)}$ to two elliptic curves. Since Bolza is only interested in curves over $\mathbb{C}$, he does not care to determine the appropriate twist, but this is easily adjusted. With

$$z_1 = \frac{\lambda x^4 + 4\lambda\nu x + 3\mu\nu}{\lambda x^2 + 2\lambda x + \frac{3\mu\lambda - 2\nu}{2}}, \qquad z_2 = \frac{\lambda' + 4\lambda'\nu' x^3 + 3\mu'\nu' x^4}{x^2(\lambda' + 2\lambda' x + \frac{3\mu'\lambda' - 2\nu'}{2} x^2)}$$

we find that $C_{(\lambda,\mu,\nu)}$ covers the two curves

$$\begin{aligned} E_{1,(\lambda,\mu,\nu)}\colon w_1^2 = \lambda R_1(z_1) = \lambda(\lambda z_1 - 2\nu)\big(&\nu' z_1^3 - 3(9\lambda^2\nu' - 6\mu\nu' - \lambda\mu')z_1^2 \\ &+ 12(9\lambda\nu\nu' + 3\mu'\nu + \lambda'\mu)z_1 + 12\nu(3\mu\mu' - \lambda\lambda')\big) \end{aligned}$$

and

$$\begin{aligned} E_{2,(\lambda,\mu,\nu)}\colon w_2^2 = \lambda' R_2(z_2) = \lambda'(\lambda' z_2 - 2\nu')(&\nu z_2^3 - 3(9\lambda'^2\nu - 6\mu'\nu - \lambda'\mu)z_2^2 \\ &+ 12\big(9\lambda'\nu'\nu + 3\mu\nu' + \lambda\mu')z_2 + 12\nu'(3\mu'\mu - \lambda'\lambda)\big)\,. \end{aligned}$$

Checking this is straightforward by verifying that $\lambda R_1(z_1)R(x)$ and $\lambda' R_2(z_2)R(x)$ are squares in $\mathbb{Q}(\lambda, \mu, \nu)(x)$.

In order to find the relation between Bolza's family and the model (C.1), we put $E_{1,(\lambda,\mu,\nu)}$ in short Weierstrass form $V^2 = U^3 + bU + c$, where

$$\begin{aligned} b = 3(&\nu^2 - 3\nu\mu\lambda + 2\mu^3)^2\big(2\nu^4\mu - 5\nu^4\lambda^2 + 2\nu^3\mu\lambda^3 + 16\nu^3\lambda^5 - \nu^2\mu^4 \\ &+ 10\nu^2\mu^3\lambda^2 - 45\nu^2\mu^2\lambda^4 - 6\nu\mu^5\lambda + 36\nu\mu^4\lambda^3 - 9\mu^6\lambda^2\big) \\ c = (&\nu^2 - 3\nu\mu\lambda + 2\mu^3)^3\big(\nu^7 - 3\nu^6\mu\lambda - 10\nu^6\lambda^3 - 10\nu^5\mu^3 + 84\nu^5\mu^2\lambda^2 - 138\nu^5\mu\lambda^4 \\ &+ 160\nu^5\lambda^6 - 30\nu^4\mu^4\lambda + 68\nu^4\mu^3\lambda^3 - 78\nu^4\mu^2\lambda^5 - 288\nu^4\mu\lambda^7 - 2\nu^3\mu^6 \\ &+ 30\nu^3\mu^5\lambda^2 - 189\nu^3\mu^4\lambda^4 + 738\nu^3\mu^3\lambda^6 - 18\nu^2\mu^7\lambda + 198\nu^2\mu^6\lambda^3 - 729\nu^2\mu^5\lambda^5 \\ &- 54\nu\mu^8\lambda^2 + 324\nu\mu^7\lambda^4 - 54\mu^9\lambda^3\big)\,. \end{aligned}$$

We compute the linear transformation

$$U = \frac{t_1 z_2 + t_2}{t_3 z_2 + t_4} \quad \text{such that} \quad \lambda' R_2(z_2) = d(U - a)(U^3 + bU + c),$$

where d is specified up to squares, and find

$$\begin{aligned} a &= \frac{(\nu^2 - 3\nu\mu\lambda + 2\mu^3)(2\nu^3\lambda - 3\nu^2\mu^2 - 4\nu^2\lambda^4 + 2\nu\mu^3\lambda + 6\nu\mu^2\lambda^3 - 3\mu^4\lambda^2)}{\mu\lambda - \nu} \\ d &= 3(\nu - \mu\lambda)(\nu^2 - 3\nu\mu\lambda + 2\mu^3)(\nu^2 - 6\nu\mu\lambda + 4\nu\lambda^3 + 4\mu^3 - 3\mu^2\lambda^2). \end{aligned}$$

From

$$a = \frac{s^4 - 2bs^2 - 8cs + b^4}{4(s^3 + bs + c)}$$

https://doi.org/10.4153/CJM-2011-039-3 Published online by Cambridge University Press

one finds one rational choice:

$$s=\frac{(\nu^2-3\nu\mu\lambda+2\mu^3)(\nu^3\lambda+3\nu^2\mu^2-18\nu^2\mu\lambda^2+16\nu^2\lambda^4+10\nu\mu^3\lambda-15\nu\mu^2\lambda^3+3\mu^4\lambda^2)}{\nu-\mu\lambda}.$$

This shows that outside $(\nu-\mu\lambda)(\nu^2-3\nu\mu\lambda+2\mu^3)=0$, Bolza's family maps to the family (C.1). The relation turns out to be birational: both $(\lambda:\mu:\nu)$ and $(s:b:c)$ are naturally coordinates on weighted projective space $\mathbb{P}(1,2,3)$. The formulae above express $(b/s^2, c/s^3)$ as functions in $(\mu/\lambda^2, \nu/\lambda^3)$. Via the appropriate resultant computations and polynomial factorizations, we find

$$\begin{aligned}\psi(b,c,s)&=2b^6+36b^5s^2+45b^4cs+72b^4s^4+45b^3c^2+36b^3cs^3-36b^3s^6\\&\quad+297b^2c^2s^2-378b^2cs^5+54b^2s^8+324bc^3s-81bc^2s^4\\&\quad+324bcs^7+216c^4-324c^3s^3+891c^2s^6-27cs^9\\\frac{\mu}{\lambda^2}&=\frac{(2b^4-15b^2cs+30b^2s^4+9bc^2+90bcs^3+135c^2s^2-27cs^5)\psi(b,c,s)}{3(bs+c+s^3)^2(b^2-6bs^2-12cs-3s^4)^2(4b^3+27c^2)}\\\frac{\nu}{\lambda^3}&=\frac{-\psi(b,c,s)^2}{(bs+c+s^3)^2(b^2-6bs^2-12cs-3s^4)^3(4b^3+27c^2)}.\end{aligned}$$

This shows that outside some codimension one locus, the two families parametrize the same curves up to twist. Note, however, that the formulas for a,b,c,d are of weighted total degrees $13,26,39,15$ in (λ,μ,ν). That means that with appropriate scaling, we can adjust the square class of d, so the two families really do parametrize essentially the same curves.

B The Six Roots of the Defining Polynomial for C_2

Let C_2 be a genus 2 curve over k that is $(2,2)$-isogenous to a genus 2 curve whose Jacobian is optimally $(4,4)$-split (see Lemma 6.1). Then C_2 is a degree 2 cover of an elliptic curve E_1 that admits a model $V^2=f(U)=U^3+bU+c$. A model for C_2 is given in (7.4):

$$f(U)=(U-r)\big(U^2+rU+(r^2+b)\big).$$

Over $k[r,R]:=k[r][U]/[U^2-(-3r^2-4b)]$, we have the factorization

$$f(U)=(U-r)\Big(U-\frac{R}{2}+\frac{r}{2}\Big)\Big(U+\frac{R}{2}+\frac{r}{2}\Big).$$

Using our parametrization for a and d given in equations (7.1) and (7.3) respectively, we can write down the factorization for g over $k[r,R]$:

$$g(X)=f_6\prod_{i=1}^{6}(X-w_i)$$

where

$$f_6=\Big(\frac{1}{-\operatorname{disc}(f)\cdot f(s)}\Big)^3=\frac{1}{\big(4b^3+27c^2\big)^3\big(s^3+bs+c\big)^3}$$

and

$$
\begin{aligned}
w_1 &= \frac{1}{2}\Big(\big(-3s^2 - b\big)\, r^2 + (-4bs - 6c)\, r - bs^2 - 6cs + b^2\Big)\, R\\
w_2 &= \frac{1}{2}\Big(\big(3s^2 + b\big)\, r^2 + (4bs + 6c)\, r + bs^2 + 6cs - b^2\Big)\, R\\
w_3 &= \frac{1}{2}\Big(\big(-3s^2 - b\big)\, r^2 + (2bs + 3c)\, r - bs^2 + 3cs - b^2\Big)\, R\\
&\quad + \frac{1}{2}\Big((-3bs - 9c)\, r^2 + \big(9cs - 2b^2\big)\, r - 4b^2s - 6bc\Big)\\
w_4 &= \frac{1}{2}\Big(\big(3s^2 + b\big)\, r^2 + (-2bs - 3c)\, r + bs^2 - 3cs + b^2\Big)\, R\\
&\quad + \frac{1}{2}\Big((3bs + 9c)\, r^2 + \big(-9cs + 2b^2\big)\, r + 4b^2s + 6bc\Big)\\
w_5 &= \frac{1}{2}\Big(\big(-3s^2 - b\big)\, r^2 + (2bs + 3c)\, r - bs^2 + 3cs - b^2\Big)\, R\\
&\quad + \frac{1}{2}\Big((3bs + 9c)\, r^2 + \big(-9cs + 2b^2\big)\, r + 4b^2s + 6bc\Big)\\
w_6 &= \frac{1}{2}\Big(\big(3s^2 + b\big)\, r^2 + (-2bs - 3c)\, r + bs^2 - 3cs + b^2\Big)\, R\\
&\quad + \frac{1}{2}\Big((-3bs - 9c)\, r^2 + \big(9cs - 2b^2\big)\, r - 4b^2s - 6bc\Big)\,.
\end{aligned}
$$

C A Representation for a $(4,4)$-split Genus 2 Curve

Let E_1 be an elliptic curve over k given by $V^2 = U^3 + bU + c$ for scalars b and c and let C_4 be a genus 2 curve that is a degree 4 cover of E_1. Then there exists a scalar s such that a representation for C_4 is given by $Y^2 = F(X)$, where

$$
\begin{aligned}
F(X) &= \frac{\big(s^3 + bs + c\big)\big(27cs^3 - 18b^2s^2 - 27bcs - 2b^3 - 27c^2\big)}{\big(4b^3 + 27c^2\big)^3\big(3bs^4 + 18cs^3 - 6b^2s^2 - 6bcs - b^3 - 9c^2\big)^3} X^6\\
&\quad + \frac{3\big(s^3 + bs + c\big)^2\big(3s^2 + b\big)}{\big(4b^3 + 27c^2\big)^2\big(3bs^4 + 18cs^3 - 6b^2s^2 - 6bcs - b^3 - 9c^2\big)^3} X^5\\
&\quad + \frac{3\big(s^3 + bs + c\big)E(b,c,s)}{4\big(4b^3 + 27c^2\big)^2\big(3bs^4 + 18cs^3 - 6b^2s^2 - 6bcs - b^3 - 9c^2\big)^3} X^4\\
&\quad + \frac{-\big(s^3 + bs + c\big)^2 G(b,c,s)}{2\big(4b^3 + 27c^2\big)\big(3bs^4 + 18cs^3 - 6b^2s^2 - 6bcs - b^3 - 9c^2\big)^3} X^3\\
&\quad + \frac{-\big(s^3 + bs + c\big)H(b,c,s)}{16\big(4b^3 + 27c^2\big)\big(3bs^4 + 18cs^3 - 6b^2s^2 - 6bcs - b^3 - 9c^2\big)^3} X^2
\end{aligned}
\tag{C.1}
$$

$$+\frac{3\left(s^3+bs+c\right)^2\left(3s^4+6bs^2+12cs-b^2\right)J(b,c,s)}{16\left(3bs^4+18cs^3-6b^2s^2-6bcs-b^3-9c^2\right)^3}X$$
$$+\frac{-\left(s^3+bs+c\right)J(b,c,s)K(b,c,s)}{64\left(3bs^4+18cs^3-6b^2s^2-6bcs-b^3-9c^2\right)^3}$$

and where

$$\begin{aligned}
E(b,c,s) &= 9cs^7-26b^2s^6-171bcs^5+34b^3s^4-333c^2s^4+155b^2cs^3-6b^4s^2\\
&\quad +126bc^2s^2+7b^3cs+144c^3s-2b^5-17b^2c^2\\
G(b,c,s) &= 7s^6+23bs^4+68cs^3-11b^2s^2-4bcs-3b^3-20c^2\\
H(b,c,s) &= 27cs^{11}+6b^2s^{10}+585bcs^9-402b^3s^8+2349c^2s^8-3330b^2cs^7+460b^4s^6\\
&\quad -6156bc^2s^6+1410b^3cs^5-7776c^3s^5+140b^5s^4+4230b^2c^2s^4+23b^4cs^3\\
&\quad +3024bc^3s^3+46b^6s^2+516b^3c^2s^2+3024c^4s^2+5b^5cs-48b^2c^3s+6b^7\\
&\quad +85b^4c^2+288bc^4\\
J(b,c,s) &= s^6+5bs^4+20cs^3-5b^2s^2-4bcs-b^3-8c^2\\
K(b,c,s) &= 27cs^9-54b^2s^8-324bcs^7+36b^3s^6-891c^2s^6+378b^2cs^5-72b^4s^4\\
&\quad +81bc^2s^4-36b^3cs^3+324c^3s^3-36b^5s^2-297b^2c^2s^2-45b^4cs-324bc^3s\\
&\quad -2b^6-45b^3c^2-216c^4.
\end{aligned}$$

Acknowledgments We would like to thank Everett Howe for directing us to Oskar Bolza's 1887 result [1] described in Appendix A. We are also very thankful for the comments of and correspondence with an anonymous referee. Particularly his insistence on a precise definition of the notion of (n,n)-splitting greatly clarified the exposition and ultimately helped us arrive at a correct and complete result.

References

[1] O. Bolza, *Ueber die Reduction hyperelliptischer Integrale erster Ordnung und erster Gattung auf elliptische durch eine Transformation vierten Grades.* Math. Ann. **28**(1886), no. 3, 447–456.

[2] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models.* Ergebnisse der Mathematik und ihrer Grenzgebiete (3), 21, Springer-Verlag, Berlin, 1990.

[3] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language.* Computational algebra and number theory (London, 1993), J. Symbolic Comput. **24**(1997), no. 3–4, 235–265. doi:10.1006/jsco.1996.0125

[4] J.-B. Bost and J.-F. Mestre, *Moyenne arithmético-géométrique et périodes des courbes de genre* 1 *et* 2. Gaz. Math. **38**(1988), 36–64.

[5] N. Bruin and K. Doerksen, *Electronic resources.* http://www.cecm.sfu.ca/~nbruin/splitigusa.

[6] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2. London Mathematical Society Lecture Note Series, 230, Cambridge University Press, Cambridge, 1996.

[7] R. Donagi and R. Livné, *The arithmetic-geometric mean and isogenies for curves of higher genus.* Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **28**(1999), no. 2, 323–339.

https://doi.org/10.4153/CJM-2011-039-3 Published online by Cambridge University Press

[8] G. Frey, *On elliptic curves with isomorphic torsion structures and corresponding curves of genus* 2. In: Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), Ser. Number Theory, I, Int. Press, Cambridge, MA, 1995, pp. 79–98.

[9] G. Frey and E. Kani, *Curves of genus* 2 *covering elliptic curves and an arithmetical application.* In: Arithmetic algebraic geometry (Texel, 1989), Progr. Math., 89, Birkhäuser Boston, Boston, MA, 1991, pp. 153–176.

[10] P. Gaudry and É. Schost, *On the invariants of the quotients of the Jacobian of a curve of genus 2.* In: Applied algebra, algebraic algorithms and error-correcting codes (Melbourne, 2001), Lecture Notes in Comput. Sci., 2227, Springer, Berlin, 2001, pp. 373–386.

[11] J.-i. Igusa, *Arithmetic variety of moduli for genus two.* Ann. of Math. (2) **72**(1960), 612–649. doi:10.2307/1970233

[12] ———, *On Siegel modular forms of genus two.* Amer. J. Math. **84**(1962), 175–200. doi:10.2307/2372812

[13] E. Kani, *Elliptic curves on abelian surfaces.* Manuscripta Math. **84**(1994), no. 2, 199–223. doi:10.1007/BF02567454

[14] ———, *Hurwitz spaces of genus 2 covers of an elliptic curve.* Collect. Math. **54**(2003), no. 1, 1–51.

[15] L.-C. Kappe and B. Warren, *An elementary test for the Galois group of a quartic polynomial.* Amer. Math. Monthly **96**(1989), no. 2, 133–137. doi:10.2307/2323198

[16] A. Krazer, *Lehrbuch der Thetafunktionen*, Tuebner, 1903, http://hdl.handle.net/2027/miun.acq9458.0001.001.

[17] R. M. Kuhn, *Curves of genus* 2 *with split Jacobian.* Trans. Amer. Math. Soc. **307**(1988), no. 1, 41–49.

[18] K. Magaard, T. Shaska, and H. Völklein, *Genus 2 curves that admit a degree 5 map to an elliptic curve.* Forum Math. **21**(2009), no. 3, 547–566. doi:10.1515/FORUM.2009.027

[19] J. S. Milne, *Abelian varieties.* In: Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150.

[20] N. Murabayashi, *The moduli space of curves of genus two covering elliptic curves.* Manuscripta Math. **84**(1994), no. 2, 125–133. doi:10.1007/BF02567449

[21] T. Shaska, *Genus 2 curves with* $(3,3)$*-split Jacobian and large automorphism group.* In: Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., 2369, Springer, Berlin, 2002, pp. 205–218.

[22] ———, *Genus 2 fields with degree 3 elliptic subfields.* Forum Math. **16**(2004), no. 2, 263–280. doi:10.1515/form.2004.013

[23] A. Silverberg, *Explicit families of elliptic curves with prescribed mod N representations.* In: Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 447–461.

[24] B. Smith, *Explicit endomorphisms and correspondences.* Ph.D. thesis, University of Sydney, 2005, http://hdl.handle.net/2123/1066.

Department of Mathematics, Simon Fraser University, Burnaby, BC V5A 1S6
e-mail: nbruin@sfu.ca kdoerkse@sfu.ca

https://doi.org/10.4153/CJM-2011-039-3 Published online by Cambridge University Press