An Explicit Formula for the Arithmetic–Geometric Mean in Genus 3

D. Lehavi and C. Ritzenthaler

CONTENTS

The arithmetic–geometric mean algorithm for calculating elliptic integrals of the first type was introduced by Gauss. The analogous algorithm for abelian integrals of genus 2 was introduced by Richelot (1837) and Humbert (1901). We present the analogous algorithm for abelian integrals of genus 3.

1. INTRODUCTION

The arithmetic–geometric mean (AGM) was discovered by Lagrange in 1785 and independently by Gauss in 1791. It is described as follows: given two positive numbers a and b, define $M(a,b)$ as the limit of the following convergent sequences:

$$a_0 := a, \qquad b_0 = b,$$
$$a_{n+1} = \frac{a_n + b_n}{2}, \qquad b_{n+1} = \sqrt{a_n b_n}.$$

During the period 1791–1799, Gauss discovered a relation between the AGM and elliptic curves:

Theorem 1.1. (Gauss.) [Cox 84], [Bost and Mestre 88]. *For each pair of positive real numbers in the AGM double sequence $a_n > b_n > 0$, define*

$$e_{n1} := \frac{1}{3}(a_n^2 + b_n^2), \quad e_{n2} := e_{n1} - b_n^2, \quad e_{n3} := e_{n1} - a_n^2.$$

Denote by E_n the elliptic curve given by the equation

$$y_n^2 = 4(x_n - e_{n1})(x_n - e_{n2})(x_n - e_{n3}).$$

Then the sequence

$$0 \to \{0, (e_{n1}, 0) - \infty\} \to E_n \to E_{n+1} \to 0$$

of abelian groups is exact for all n. Moreover, identifying E_n, E_{n+1} with their respective Picard groups, the map $E_n \to E_{n+1}$ is given by $\frac{dx_n}{y_n} \mapsto \frac{dx_{n+1}}{y_{n+1}}$.

2000 AMS Subject Classification: Primary: 14H40, 14H45, 14Q05
Keywords: Prym varieties, arithmetic geometric mean

1058-6458/2007 $0.50 per page
Experimental Mathematics **16**:4, page 421

It is easy to see that we create in this way a sequence of 2-isogenous elliptic curves. Gauss generalized the definition of the AGM to the complex numbers; in this case there is a choice involved in taking the square root. Gauss described the resulting correspondence [Cox 84] for the description.

Recall that the real points in the Picard group of a curve that is defined over $\mathbb{R}$ are the divisor classes that are invariant under the action of the group $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ (see [Gross and Harris 81, Sections 1–5]). Gauss proved that if the 2-torsion points of $\mathrm{Pic}(E)$ are real, then there is a unique $\alpha \in \mathrm{Pic}(E)[2]$ such that the 2-torsion points of $\mathrm{Pic}(E'_\alpha)$ are real. Applying this property iteratively, one gets an algorithm for calculating elliptic integrals (see [Cox 84, Bost and Mestre 88]) of the form

$$\int_{e_3}^{e_2} \frac{dx}{\sqrt{(x-e_1)(x-e_2)(x-e_3)}}.$$

This iterative algorithm is applied in numerical evaluations of certain types of abelian integrals (see [Borwein and Borwein 88]).

In genera higher than 1 one can hope for an isogeny between the Jacobians of the curves. Before stating results in higher genera, we recall some facts on polarized abelian varieties. A pair (A, Θ), where A is an abelian variety and Θ is an effective divisor of A, is called a *polarized* abelian variety. The divisor Θ is called the *theta divisor* of the polarized abelian variety, and the map $A \to \mathrm{Pic}^0(A)$ defined by $a \mapsto T_a^{-1}(\Theta) - \Theta$, where T_a is the translation by a, is called the *polarization* of the pair (A, Θ).

Since the kernel of the polarization is a finite abelian group whose dimension as a $\mathbb{Z}$ module is bounded by twice the genus of A, we describe its isomorphism type by two copies of a monotonic sequence of $\mathrm{genus}(A)$ natural numbers. We will abuse notation and denote, for instance, the sequence $(2,2,2,2,1,1),(2,2,2,2,1,1)$ by $2^4 1^2$.

If the polarization type is trivial, we say that the polarization is *principal*; in this case (principal polarization) we say that A is a principally polarized abelian variety or PPAV. The translates of Θ that contain 0 are called the *theta characteristics* of A. The theta characteristics are called even or odd if their multiplicity at 0 is even or odd. The theta characteristics of an abelian variety A induce a symplectic structure on the $\mathbb{F}_2$-vector space $A[2]$ (the group of 2-torsion points in A) in the following way: Let θ be a theta characteristic of A. Then the map

$$q : A[2] \to \mathbb{F}_2,$$
$$a \mapsto h^0(\theta + a) + h^0(\theta) \pmod 2,$$

is a quadratic form over $\mathbb{F}_2$. The quadratic form q induces the following symplectic pairing on the group $A[2]$:

$$\langle a, b\rangle = q(a+b) - q(a) - q(b) \pmod 2.$$

This pairing is called the *Weil pairing*. If G is a subgroup of $A[2]$, we will use the notation

$$G^\perp := \{a \in A[2] | \langle a, g\rangle = 0 \text{ for all } g \in G\}.$$

If A is a PPAV and G is a subgroup of the group $A[2]$, then $\mathrm{Pic}^0(A/G)$ is naturally isomorphic to $\mathrm{Pic}^0(A)/G^\perp$, whence the abelian variety A/G is principally polarized only if G is 0, $A[2]$, or a maximal isotropic group of $A[2]$ with respect to the Weil pairing. Finally, recall that a Jacobian of a smooth curve C is principally polarized by the theta divisor Θ_C, the image of $\mathrm{Sym}^{g-1} C$ in $\mathrm{Jac}(C)$ under the Abel map.

The dimension of the moduli space of principally polarized abelian varieties of genus g is $g(g+1)/2$, while the dimension of the moduli space of curves of genus $g \geq 2$ is $3g-3$. Thus if C is a general curve of genus $g \leq 3$ and L is a maximal isotropic subgroup of $\mathrm{Jac}(C)[2]$, then $\mathrm{Jac}(C)/L$ is a Jacobian of some curve C'. This motivates the following questions:

- Is this an algebraic correspondence?
- Does there exist a curve C' for *every* pair C, L in genera $2, 3$ (and not only generically)?
- If C is a real curve, are there "distinguished" maximal subgroups?
- What is the situation for genera higher then 3?

In the case $g = 2$, the first three questions were settled by Richelot [Richelot 37] and Humbert [Humbert 01]. Both Richelot and Humbert observed that for curves of genus 2 with six real Weierstrass points there are distinguished maximal isotropic subgroups; they used the distinguished maximal groups to describe an iterative integration algorithm for differentials on the components of real curves of genus 2 with six real Weierstrass points. Richelot described *algebraically* the curve C' in terms of the curve C, and Humbert described the isomorphism

$$H^0(C, K_C) \longrightarrow H^0(C', K_{C'}).$$

See [Donagi and Livné 99, Section 4] for a modern review of the construction and [Bost and Mestre 88] for the resulting integration identities and the iterative integration algorithm resulting in the real case. Using modern tools

(namely GAGA), the answer to the first question is immediately positive in all genera. Donagi and Livné solved the second question for genus $g = 3$, and answered negatively the last question:

Theorem 1.2. [Donagi and Livné 99] *Let C be a smooth curve of genus g over a base field of characteristic different from $2, 3$. Let $L \subset \mathrm{Jac}(C)[2]$ be a maximal isotropic subgroup (with respect to the Weil pairing).*

(i) *If $g = 3$ then there exists a curve C' such that $\mathrm{Jac}(C') \cong \mathrm{Jac}(C)/L$. The curve C' can be described algebraically in terms of the curve C and the maximal isotropic subgroup L.*

(ii) *If $g > 3$, then generically there is no curve C' such that $\mathrm{Jac}(C') \cong \mathrm{Jac}(C)/L$.*

The proof that Donagi and Livné presented for genus 3 is constructive in the set-theoretic sense. However, as a basis for explicit work it has drawbacks: it is not clear how to give coordinates to the spaces and functions involved or how one can track the canonical classes.

The object of this paper is to extend Gauss's original work on curves of genus 1 to the case of genus 3. In Section 2 we use the Coble–Recillas construction to give an alternative construction to the one proposed in [Donagi and Livné 99]; we describe the curve C' in terms of the pair (C, L), where the curve C is a general curve. In Section 3 we describe the isomorphism between the canonical linear systems $|K_C|$ and $|K_{C'}|$.

In Section 4 we derive the formulas describing the curve C' in terms of the curve C and the isomorphism $H^0(C, K_C) \cong H^0(C', K_{C'})$. We also show how to iterate the construction. In Section 5 we concentrate on real curves: assuming the curve C is a real M-curve (i.e., a real curve with four components), we present a distinguished maximal isotropic subgroup of $\mathrm{Jac}(C)[2]$; we also analyze the map between the first homology with integer coefficients of the real part of $\mathrm{Jac}(C)$ and $\mathrm{Jac}(C')$. The combined result of Sections 3 and 5 is an iterative integration algorithm on any of the components of C, where C is an M-curve.

Although our construction is stated over the complex numbers, it is mostly algebraic. The complex structure is used in one crucial point: we use a result (due to Jordan in [Jordan 70, Section 332], or see Harris's modern approach in [Harris 79]) stating that the Galois group of the bitangents of a smooth plane quartic over the complex numbers is $\mathrm{SP}_6(2)$. In the rest of the paper we require only that the characteristic of the base field be the one arising from the bigonal and trigonal constructions; the characteristic of the base field K is not 2 or 3 (see the discussion in the introduction to [Donagi and Livné 99]).

Some of the proofs in Sections 4 and 5 are computer-aided proofs. The Mathematica and MAGMA programs that generated the computer part of the proofs appear in [Lehavi and Ritzenthaler 06].

We remark that the AGM has a nice application in the area of curves over finite fields: Mestre observed that the theta-function identities involved in the AGM over p-adic fields can be used to study the number of points in curves over finite fields. See [Mestre 00, Lercier and Lubicz 03] for elliptic and hyperelliptic results and [Ritzenthaler 03] for results on nonhyperelliptic genus-3 curves.

2. THE CONSTRUCTION

The idea behind our construction is to filter the level-2 data and perform the construction in three steps, using nonprincipally polarized abelian varieties to keep track of the level data. Throughout this paper we fix a *generic* curve C of genus 3, and a maximal isotropic flag $\mathcal{L} = (\langle\alpha\rangle = L_1 \subsetneq L_2 \subsetneq L_3)$ with respect to the Weil pairing on $\mathrm{Jac}(C)[2]$. Let C' be a curve such that $\mathrm{Jac}(C') \cong \mathrm{Jac}(C)/L_3$. The flag $\mathcal{L}$ induces a dual isotropic flag $\mathcal{L}' = (L_1' \subsetneq L_2' \subsetneq L_3')$ in $\mathrm{Jac}(C')[2]$ in the following way: L_1' (respectively L_2', respectively L_3') is the image of $L_2^\perp$ (respectively $L_1^\perp$, respectively $\mathrm{Jac}(C)[2]$) under the map $\mathrm{Jac}(C) \to \mathrm{Jac}(C)/L_3$. We denote by α (respectively α') the nontrivial element in L_1 (respectively L_1'). Using the Coble–Recillas construction we will introduce ramified double covers $Y \longrightarrow E$ and $Y' \longrightarrow E'$ such that there are natural isomorphisms

$$\mathrm{Prym}(Y/E) \cong \mathrm{Jac}(C)/L_1^\perp,$$
$$\mathrm{Prym}(Y'/E') \cong \mathrm{Jac}(C')/{L_1'}^\perp.$$

Using a bigonal construction (see [Donagi 92, pp. 68–69] for an overview of the bigonal construction) we will prove that the polarized abelian varieties $\mathrm{Prym}(Y'/E')$ and $\mathrm{Prym}(Y/E)$ are dual to one another, up to finite data arising from L_2.

Before describing the geometry of the construction (in Sections 2.5–2.10), we describe the finite symplectic algebra involved: the level-2 structure of the curve C. Define the following $\mathrm{SP}_6(2)$ equivariant surjective map:

$$D : \{^{\text{unordered pairs of distinct}}_{\text{odd theta characteristics of } C}\} \longrightarrow \mathrm{Jac}(C)[2] \smallsetminus \{0\},$$
$$\{\theta_1, \theta_2\} \mapsto \theta_1 - \theta_2$$

(recall that the group $\mathrm{SP}_6(2)$ acts on the odd theta characteristics via the monodromy action; see [Harris 79]). Since the group $\mathrm{SP}_6(2)$ acts transitively on the set $\mathrm{Jac}(C)[2] \smallsetminus \{0\}$, all the fibers of the map D are of the same order: $\binom{28}{2}/63 = 6$. For any 2-torsion point γ in $\mathrm{Jac}(C)$ we define the *Steiner system*

$$\Sigma_\gamma := \bigcup_{x \in D^{-1}(\gamma)} \{x\}.$$

Since the pairs in a fiber of the map D do not intersect, the order of all the Steiner systems is 12. In Propositions 2.1 and 2.2 below we discuss the relation between the symplectic structure on the vector space $\mathrm{Jac}(C)[2]$ and the combinatorics of the 63 Steiner systems.

Proposition 2.1. *Let γ, γ' be two distinct elements in $\mathrm{Jac}(C)[2] \smallsetminus \{0\}$. Then $\#(\Sigma_\gamma \cap \Sigma_{\gamma'})$ is 4 if $\langle \gamma, \gamma' \rangle = 0$, and 6 otherwise.*

Proof: Since the group $\mathrm{SP}_6(2)$ acts transitively on pairs of distinct elements in $\mathrm{Jac}(C)[2] \smallsetminus \{0\}$ with the same Weil pairing, the order of the set $\Sigma_\gamma \cap \Sigma_{\gamma'}$ depends only on the Weil pairing $\langle \gamma, \gamma' \rangle$. We denote the two possible intersection orders by n_0, n_1. Any odd theta characteristic sits on $28 - 1 = 27$ different Σ_γ's, and the number of $\gamma \in \mathrm{Jac}(C)[2] \smallsetminus \{0, \alpha\}$ such that $\langle \gamma, \alpha \rangle = 0$ (respectively 1) is 30 (respectively 32). So we get

$$\begin{aligned} 12 \cdot 27 &= \sum_{\alpha \neq 0} \#\{\theta \mid \theta \in \Sigma_\alpha \cap \Sigma_\gamma\} \\ &= \#\Sigma_\alpha \\ &\quad + \#\{\alpha \mid \langle \gamma, \alpha \rangle = 0\} n_0 + \#\{\alpha \mid \langle \gamma, \alpha \rangle = 0\} n_1 \\ &= 12 + 30 n_0 + 32 n_1, \end{aligned}$$

and the unique nonnegative integer solution of this equation is $n_1 = 6$, $n_0 = 4$. □

Proposition 2.2. *The following properties hold:*

(i) *Let γ be a 2-torsion point in $\mathrm{Jac}(C)$. Then the map*

$$D_\gamma : \{^{\text{unordered pairs of distinct}}_{\text{classes in } \Sigma_\gamma/\gamma}\} \longrightarrow \mathrm{Jac}(C)[2]/\gamma, \quad \{a_i, a_j\} \mapsto a_i - a_j,$$

is an isomorphism on $(\gamma^\perp/\gamma) \smallsetminus \{0\}$. Moreover, the map D_γ maps the intersection pairing to the Weil pairing.

(ii) *Let H be an isotropic subgroup of $\mathrm{Jac}(C)[2]$ of order 4. Then there is a unique theta characteristic θ such that for all $\alpha \in H$, $\theta + \alpha$ is an odd theta characteristic. Denoting the set $\{\theta + \alpha, \alpha \in H\}$ by Γ_H, one has $\Gamma_H = \bigcap_{\gamma \in H \smallsetminus \{0\}} \Sigma_\gamma$.*

(iii) *A maximal isotropic subgroup of $\mathrm{Jac}(C)[2]$ containing α is represented by a partition of Σ_α/α into three pairs.*

(iv) *If seven Steiner systems intersect at mutually distinct 4-tuples, then there is a maximal isotropic subgroup $G \subset \mathrm{Jac}(C)[2]$ such that these seven Steiner systems are the Steiner systems of the nonzero elements of G.*

Proof: Let $G_\gamma \subset \mathrm{SP}_6(2)$ be the stabilizer of γ Then the G_γ orbits of $\mathrm{Jac}(C)[2]/\gamma$ are the sets

$$\{0\}, \quad (\gamma^\perp/\gamma) \smallsetminus \{0\}, \quad (\mathrm{Jac}(C)[2] \smallsetminus \gamma^\perp)/\gamma,$$

which are of orders $1, 15, 16$ respectively. Since the map D_γ is a nontrivial G_γ-equivariant map, and since the order of the set of unordered pairs of distinct points in Σ_γ is $\binom{6}{2} = 15$, the map D_γ is a one-to-one map on the projective space $(\gamma^\perp/\gamma) \smallsetminus \{0\}$. By a similar counting argument we prove the claim for the Weil pairing. The last three assertions follow from Proposition 2.1. □

Using the description of *one* maximal isotropic flag in terms of odd theta characteristics, we describe the combinatorics of *two* isotropic flags: $\mathcal{L}' = (\langle \alpha' \rangle = L'_1 \subsetneq L'_2 \subsetneq L'_3)$ (see the beginning of Section 2) and $\tilde{\mathcal{L}} = (\langle \tilde{\alpha} \rangle = \tilde{L}_1 \subset \tilde{L}_2 \subset \tilde{L}_3)$ in $\mathrm{Jac}(C')[2]$ such that

$$\tilde{L}_1 \oplus L'_3 = L'^\perp_2, \quad \tilde{L}_2 \oplus L'_3 = L'^\perp_1, \quad \tilde{L}_3 \oplus L'_3 = \mathrm{Jac}(C')[2].$$

Such a description is essential for iterating the algorithm, since the pair $(C', \tilde{\mathcal{L}})$ should be the starting point of the second iteration, playing the same role that the pair $(C, \mathcal{L})$ played in the first iteration. Note that $\tilde{\mathcal{L}}$ is not uniquely defined. For further uses, we will need the following lemma:

Lemma 2.3. *For any subgroup $H \subset \tilde{L}_3$ of order 4 one has $\#\Gamma_H \cap \Sigma_{\alpha'} = 0$ if $H = \tilde{L}_2$ and $\#\Gamma_H \cap \Sigma_{\alpha'} = 2$ otherwise.*

Proof: Since we have $\tilde{L}_2 \subset L'^\perp_1$, the Weil pairings of the nontrivial elements in $\tilde{L}_2/\tilde{L}_1, (L'_1 \oplus \tilde{L}_1)/\tilde{L}_1$ are all 0. By Proposition 2.2 the intersection

$$D_{\tilde{\alpha}}^{-1}(\tilde{L}_2/\tilde{L}_1) \cap D_{\tilde{\alpha}}^{-1}((L'_1 \oplus \tilde{L}_1)/\tilde{L}_1)$$

is empty, whence the intersection

$$\Gamma_{\tilde{L}_2} \cap \Sigma_{\alpha'} = \Gamma_{\tilde{L}_2} \cap (\Sigma_{\alpha'} \cap \Sigma_{\tilde{\alpha}}) = \Gamma_{\tilde{L}_2} \cap \Gamma_{L'_1 \oplus \tilde{L}_1}$$

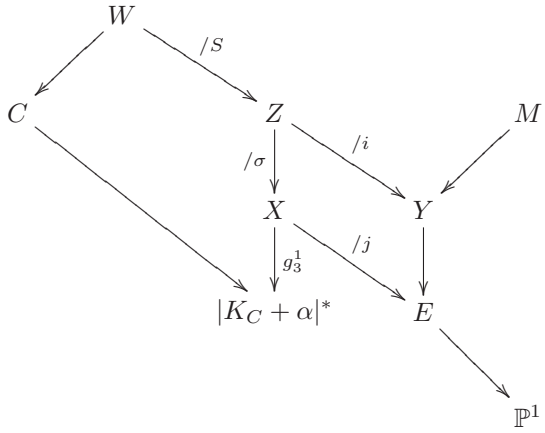
is also empty. Reasoning in the same way, for any subgroup $H \subset \tilde{L}_3$ of order 4 such that $H \neq \tilde{L}_2$, we have that H is not a subset of ${L'}_1^{\perp}$. By Proposition 2.2,

$$\#(D_{\tilde{\alpha}}^{-1}(H/\tilde{L}_1) \cap D_{\tilde{\alpha}}^{-1}((L'_1 \oplus \tilde{L}_1)/\tilde{L}_1)) = 1,$$

and therefore the cardinality of the intersection $\Gamma_H \cap \Sigma_{\alpha'}$ is 2. □

We now move to the geometric part of the construction. Recall that C is a generic genus-3 curve and that $\mathcal{L} = (\langle\alpha\rangle = L_1 \subsetneq L_2 \subsetneq L_3)$ is a full isotropic flag in $\mathrm{Jac}(C)[2]$. We start with the Coble–Recillas construction. Next we construct the double cover $Y \longrightarrow E$ mentioned above and review its properties. Finally, we describe the AGM construction through the bigonal construction.

Notation. If $V \to U$ is a cover without specific name for the morphism, we denote the morphism by $\pi_{V/U}$. In the following diagram we summarize some constructions and notation that will be introduced afterward. Note that this diagram admits a symmetry with respect to the vertical axis passing through the right term. These symmetric objects, which are related to $(C', \mathcal{L}')$ under those constructions, will be indicated by $'$.



The left construction is the Coble–Recillas trigonal construction, and the right construction is (half of) a bigonal construction (see [Donagi 92, pp. 68–69]).

Let us recall some elements of the theory of the trigonal construction (see, for instance, [Recillas 74, **?**, Lehavi 05]). Define

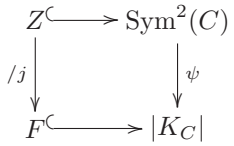
$$\begin{aligned} W &:= \overline{C \times_{|K_C+\alpha|^*} C \smallsetminus \Delta_C} \\ &= \{(p_1, p_2) \in C \times C \mid p_1 + p_2 < K_C + \alpha\} \end{aligned}$$

(where by Δ_C we denote the diagonal). The curve W admits a natural involution, the switching of coordinates, which we denote by S. The curve $Z = W/S$ can be viewed as the subset of $\mathrm{Sym}^2(C)$ defined by $\{p_1 + p_2 \mid p_1 + p_2 < K_C + \alpha\}$. The curve Z admits three natural nontrivial involutions:

- $\sigma : p_1 + p_2 \mapsto p_3 + p_4$ such that $p_1 + p_2 + p_3 + p_4 \sim K_C + \alpha$; define $X := Z/\sigma$.
- $i : p_1 + p_2 \mapsto p_3 + p_4$ such that $p_3 + p_4 \sim p_1 + p_2 + \alpha$; define $Y := Z/i$.
- $j = \sigma \circ i$; define $F := Z/j$.

Remark 2.4. The curve Z has a "theta divisor interpretation": the Abel map $\mathrm{Sym}^2 C \longrightarrow \mathrm{Pic}^2 C$ induces an isomorphism $Z \cong \Theta_C \cap (\Theta_C + \alpha)$ (see, e.g., [Lehavi 05, 3.1–3.4]). In particular, Z is generically a smooth curve of genus 7. Note that the involution i is then $d \mapsto d + \alpha$, j is $d \mapsto K_C - d$, and σ is $d \mapsto K_C + \alpha - d$.

Let us denote by ψ the morphism from $\mathrm{Sym}^2(C)$ to $|K_C|$ defined by sending $p_1 + p_2$ to the line $\overline{p_1 p_2}$. Since the supports of $p_1 + p_2$ and $j(p_1 + p_2)$ as points on $C \subset |K_C|^*$ lie on the same line, ψ induces a morphism from $F = Z/j$ to $|K_C|$ making the following diagram commutative:



It is classical that bitangents to C are in one-to-one correspondence with odd theta characteristics. Moreover, if l is a bitangent corresponding to an element $\theta \in \Sigma_\alpha$, it defines a point on Z (still denoted by θ): indeed, if $l \cdot C = 2(p_1 + p_2)$ and if $\theta + \alpha$ corresponds to a bitangent with divisor $2(p_3 + p_4)$, one gets $(p_1 + p_2) - (p_3 + p_4) \sim \alpha$, so

$$p_1 + p_2 + p_3 + p_4 \sim 2(p_1 + p_2) + \alpha \sim K_C + \alpha.$$

Thus $p_1 + p_2 < K_C + \alpha$.

By definition of Z and j, the morphism j is ramified exactly at the 12 elements of the Steiner system Σ_α. Since Z is of genus 7, F is of genus 1, and by the preceding embedding the 12 bitangents (viewed as points in $|K_C|$) are points on F. Note that $F \subset |K_C|$ is a cubic: the degree of the map $F \longrightarrow |K_C|$ is 3, since $\deg(\psi) = 6$, and the map is nondegenerate because the points of $\psi(\Sigma_\alpha)$ are not collinear.

Since i is fixed-point-free and commutes with j, it defines a fixed-point-free involution i_F on F exchanging the points $\theta, \theta+\alpha \in \Sigma_\alpha$. This involution defines a point $\alpha_F \in \mathrm{Pic}^0(F)[2]$ such that for all $p \in F$, $p + \alpha_F \sim i_F(p)$. The quotient of F by the involution i_F is the curve $E = X/j$ (because $(Z/\sigma)/j = (Z/j)/i$). Hence E is naturally embedded in $|K_C|^*$ by the image of $\pi_{F/E} : p \mapsto p \cap (p + \alpha_F)$.

Theorem 2.5. (A. Coble.) See [Coble 61, Sections 47–49] or [Lehavi 05]. *The images of the points of $\Sigma_\alpha \subset F$ under the map $\pi_{F/E}$ sit on a unique conic $Q \subset |K_C|^*$. They are the intersection points of the bitangents $\theta, \theta+\alpha \in \Sigma_\alpha$. The locus $Q \cap E$ is the ramification locus of the map $\pi_{Y/E} : Y \to E$.*

The following results are mostly due to Coble and to Recillas.

Proposition 2.6. *Let α_E be the unique nonzero element in $(\pi_{F/E})_*(\mathrm{Pic}(F)[2]) \subset \mathrm{Pic}(E)[2]$. Given the double cover $Y \longrightarrow E$ and the 2-torsion point α_E, one can reconstruct the curve C and the linear system $|K_C + \alpha|$ in the following way. We have $F \simeq E/\alpha_E$. The curve Z is isomorphic to the fibered product $Y \times_E F$. This construction induces two commuting involutions i, j on Z. Since the double cover $\pi_{F/E}$ is unramified, the involutions i, j on Z are fixed-point-free.*

The genera of the curves Z, X, Y are then $7, 4, 4$ respectively. The curve X is a bielliptic curve of genus 4 that has only one g^1_3 up to the bielliptic involution. Thus we are back in the trigonal construction setting. Note that C and the linear system $|K_C + \alpha|$ are invariant under the choice of the g^1_3. On our way to $(C', \mathcal{L}')$, we have now expressed $(\mathrm{Jac}(C), \alpha)$ in terms of the double cover Z/X.

The second step in the construction (see Theorem 2.9) is to interpret the symplectic data through the quotient i. Our main tool for analysis of nonprincipally polarized abelian varieties is Lemmas 2.7 and 2.8 below.

Lemma 2.7. [Donagi and Livné 99, Lemma 1] *Let $\tilde{V} \longrightarrow V$ be an admissible double cover of curves, and let $\nu\tilde{V} \longrightarrow \nu V$ be its partial normalization at $r > 1$ points $x_1, \ldots, x_r \in V$. Let g be the arithmetic genus of the partial normalization νV, so the arithmetic genus of V is $g + r$. Then $\mathrm{Prym}(\tilde{V}/V)$ has a principal polarization, $\mathrm{Prym}(\nu\tilde{V}/\nu V)$ has a polarization of type $2^g 1^{r-1}$, and the pullback map*

$$\nu^* : \mathrm{Prym}(\tilde{V}/V) \longrightarrow \mathrm{Prym}(\nu\tilde{V}/\nu V)$$

is an isogeny of degree 2^{r-1}.

Lemma 2.8. (The monodromy argument.) *Let $V' \longrightarrow V$ be a finite cover such that the Galois group of the Galois closure of V'/V is 2-transitive on the cover. Then the only section of the cover $V' \times_V V' \longrightarrow V$ is the diagonal.*

We will apply Lemma 2.8 with the covers $\mathcal{A}^1_3 \to \mathcal{A}_3$ and $\mathcal{A}^F_3 \to \mathcal{A}_3$, where $\mathcal{A}^1_3$ (respectively $\mathcal{A}^F_3$) is the moduli space of PPAVs of dimension 3 with a 2-torsion point (respectively with a maximal isotropic group).

Theorem 2.9. *The quotient by i induces an isogeny of abelian varieties:*

$$\phi : \mathrm{Prym}(Z/X) \longrightarrow \mathrm{Prym}(Y/E).$$

Identifying the principally polarized abelian varieties $\mathrm{Jac}(C)$ and $\mathrm{Prym}(Z/X)$ as in [Donagi 92, Theorem 2.11]*, the kernel of ϕ is $\alpha^\perp$.*

Proof: The proof consists of three steps:

Step 1: The map $\phi : \mathrm{Prym}(Z/X) \longrightarrow \mathrm{Prym}(Y/E)$ is an isogeny. To prove this claim it suffices to prove that the induced map on the tangent spaces at 0 is an isomorphism. We do this by considering the space $M := H^0(Z, \Omega^1_Z)$ as a $\mathrm{Gal}(Z/E)$ module and calculating the module decomposition to irreducible representations. We denote by M_- the irreducible representation corresponding to the character whose kernel is the subgroup $\langle - \rangle \subset \mathrm{Gal}(Z/E)$, and by M_1 the irreducible representation corresponding to the trivial character. Using this notation we have

$$\begin{aligned}
&H^0(Z, \Omega^1_Z) = M_1 \oplus M_i \oplus M_j \oplus M_\sigma, \quad H^0(E, \Omega^1_E) = M_1,\\
&H^0(F, \Omega^1_F) = M_1^j \oplus M_i^j \oplus M_j^j \oplus M_\sigma^j = M_1 \oplus M_j,\\
&H^0(Y, \Omega^1_Y) = M_1^i \oplus M_i^i \oplus M_j^i \oplus M_\sigma^i = M_1 \oplus M_i,\\
&H^0(X, \Omega^1_X) = M_1^\sigma \oplus M_i^\sigma \oplus M_j^\sigma \oplus M_\sigma^\sigma = M_1 \oplus M_\sigma.
\end{aligned}$$

However, since E and F are both of genus 1, the map $H^0(F, \Omega^1_F) \longrightarrow H^0(E, \Omega^1_E)$ is an isomorphism. Thus we have $M_j = 0$, and our claim holds.

Step 2: The kernel of the isogeny ϕ is a subset of $\mathrm{Prym}(Z/X)[2]$. Denoting by $[2]_A$ the multiplication by 2 on an abelian variety A, we have

$$\pi_{Z/Y\,*}\pi^*_{Z/Y} : \mathrm{Jac}(Y) \longrightarrow \mathrm{Jac}(Y) = [2]_{\mathrm{Jac}(Y)}.$$

Denote by μ_*, μ^* the restrictions of maps $\pi_{Z/Y\,*}, \pi^*_{Z/Y}$ to the abelian varieties $\mathrm{Prym}(Y/E), \mathrm{Prym}(Z/X)$ respectively. Note that $\phi = \mu^*$. We have $\mu^*\mu_* = [2]_{\mathrm{Prym}(Z/X)}$.

Step 3: Computation of the kernel of ϕ. By applying Lemma 2.7 to some degeneration of the cover Y/E along

its ramification locus $Q \cap E$, one finds that the polarization type of the variety $\mathrm{Prym}(Y/E)$ is $2^1 1^5$. Thus, the order of the kernel of ϕ is 32.

By [Donagi 92, Theorem 2.11], the norms in the trigonal construction induce an isomorphism $\mathrm{Jac}(C) \cong \mathrm{Prym}(Z/X)$. The kernel of ϕ can thus be identified with $\beta^\perp$ for some $\beta \in \mathrm{Jac}(C)[2]$. The map $(\mathrm{Jac}(C), \alpha) \to (\mathrm{Jac}(C), \beta)$ gives a endomorphism of $\mathcal{A}_3^1$ and then a section from $\mathcal{A}_3^1$ to $\mathcal{A}_3^1 \times_{\mathcal{A}_3} \mathcal{A}_3^1$. By Lemma 2.8 this section maps into the diagonal component, so $\alpha = \beta$. □

Denote by $q_1, \ldots, q_6$ the intersection points of E and Q. In Proposition 2.2 we identified pairs of q_i's with the nonzero points of the symplectic space $\alpha^\perp/\alpha$. This identification induces bijections between the sets of data shown in Table 1.

We let $\{q_1, q_2\}, \{\{q_3, q_4\}, \{q_5, q_6\}\}$ be the partition of the q_i's that corresponds to the full isotropic flag $\mathcal{L}$. Denote by $\pi_{E/\mathbb{P}^1}$ the linear system $|q_1 + q_2|$ on the curve E and by B the ramification locus of $\pi_{E/\mathbb{P}^1}$. Note that the symmetric construction introduces a set B'. Using these definitions we are ready to prove the correctness of our construction:

Theorem 2.10. *Let us assume that the ramification pattern of the tower $Y \longrightarrow E \longrightarrow \mathbb{P}^1$ is generic. Denote by $\tilde{H} \longrightarrow H \longrightarrow \mathbb{P}^1$ the image of the tower $Y \longrightarrow E \longrightarrow \mathbb{P}^1$ by the bigonal construction. Then the tower $Y' \longrightarrow E' \longrightarrow \mathbb{P}^1$ is the normalization of the tower $\tilde{H} \longrightarrow H \longrightarrow \mathbb{P}^1$. Moreover, there is a one-to-one correspondence between points $b \in Q \cap E \smallsetminus \{q_1, q_2\}$ and points $b' \in B'$, given by*

$$\pi_{E/\mathbb{P}^1}(b) = \pi_{E'/\mathbb{P}^1}(b').$$

Proof: The ramification pattern of the bigonal construction on $Y \longrightarrow E \longrightarrow \mathbb{P}^1$ is the following (see [Donagi 92, pp. 68–69]):

- If $\pi_{E/\mathbb{P}^1}^{-1}(a) = \{q_1, q_2\}$, then Y/E is ramified over both q_1 and q_2, $\pi_{H/\mathbb{P}^1}^{-1}(a)$ is a node, and over this node the curve $\tilde{H}$ is a gluing of two ramified sheets (symbolically, $\subset\subset / = | \supset\subset / \times$) .
- If $\pi_{E/\mathbb{P}^1}^{-1}(a) = 2b$ for some $b \in B$, then Y/E is étale over b, $\pi_{H/\mathbb{P}^1}$ is étale over a, and $\tilde{H}$ is ramified over one of the points in $\pi_{H/\mathbb{P}^1}^{-1}(a)$ and étale over the other one (symbolically, $\subset\subset / \subset | \subset= / =$).
- If $\pi_{E/\mathbb{P}^1}^{-1}(a) \ni q$ for some $q \in Q \cap E \smallsetminus \{q_1, q_2\}$, then Y/E is ramified over q and étale over the other point in $\pi_{E/\mathbb{P}^1}^{-1}(a)$. Moreover, $\pi_{H/\mathbb{P}^1}$ is ramified at a, and $\tilde{H}/H$ is étale over both branches (symbolically, $\subset= / = | \subset\subset / \subset$).
- In all other points the ramification patterns of the towers $Y/E/\mathbb{P}^1$ and $\tilde{H}/H/\mathbb{P}^1$ are generic (i.e., unramified).

Denote by $\nu\tilde{H}, \nu H$ the normalizations of the curves $\tilde{H}, H$ respectively. By the Riemann–Hurwitz formula, the genera of the curves $\nu\tilde{H}, \nu H$ are $4, 1$ respectively. The ramification pattern over the points $\pi_{E/\mathbb{P}^1}(q_3), \pi_{E/\mathbb{P}^1}(q_4)$, $\pi_{E/\mathbb{P}^1}(q_5), \pi_{E/\mathbb{P}^1}(q_6)$ in the tower $Y \longrightarrow E \longrightarrow \mathbb{P}^1$ is $\subset= / =$. Thus, the partition $\{\{q_3, q_4\}, \{q_5, q_6\}\}$ induces a partition into two pairs of the four ramification points of the map $\nu H \longrightarrow \mathbb{P}^1$, which induces a choice of a 2-torsion point in $\mathrm{Pic}^0(\nu H)$. Applying the reconstruction technique from Proposition 2.6 to the double cover $\nu\tilde{H} \longrightarrow \nu H$ and the 2-torsion point, we get a smooth curve C'' of genus 3. We claim that we have the following degrees for the isogenies:

$$\mathrm{Jac}(C) \xrightarrow{2} \mathrm{Prym}(\tilde{H}/H) \xrightarrow{2} \mathrm{Prym}(\nu\tilde{H}/\nu H) \xrightarrow{2} \mathrm{Jac}(C'').$$

By [Pantazis 86, Proposition 3.1], the abelian variety $\mathrm{Prym}(\tilde{H}/H)$ is isomorphic to the dual of the abelian variety $\mathrm{Prym}(Y/E)$. Since $\mathrm{Prym}(Y/E)$ is isomorphic to $\mathrm{Jac}(C)/\alpha^\perp$, we have (see the discussion on PPAVs) that $\mathrm{Prym}(\tilde{H}/H) \simeq \mathrm{Jac}(C)/\alpha$. The second arrow is a consequence of Lemma 2.7 for the normalization of $\tilde{H}/H$ over the point of type $\supset\subset / \times$. The third arrow follows from Theorem 2.9.

Thus we have obtained an isogeny of degree 2^3. By our observation in the discussion on PPAVs, this isogeny is given by a maximal isotropic group $L \in \mathrm{Jac}(C)[2]$. In the same spirit as in the proof of 2.9 we can use the monodromy argument of Lemma 2.8 for L_3 and L to prove that $L = L_3$. Thus $C'' \simeq C'$, and we get

$$\nu\tilde{H} \simeq Y', \quad \nu H \simeq E'.$$

The ramification patterns prove the last assertion of the theorem. □

Remark 2.11. In the same way, one can describe analogous results for the other nongeneric ramification patterns of the tower $Y \longrightarrow E \longrightarrow \mathbb{P}^1$, but this effort is redundant: in Section 4 we will find a formula that gives C' in terms of a generic pair (C, L); since C' is continuous in the pair (C, L), the formula will be correct for all pairs (C, L) for which the denominators in the formula are non zero.

Data on isotropic subgroups in $\mathrm{Jac}(C)[2]$ that contain α.	Data on isotropic subgroups of $\alpha^\perp/\alpha$	Partitions of the points $\{q_i\}_{i=1,\dots,6}$
Isotropic subgroups of order 4	Isotropic subgroups of order 2	$2+4$
Maximal Isotropic subgroups	Maximal Isotropic subgroups	$2+2+2$
Full isotropic flags	Full isotropic flags	$2+(2+2)$

TABLE 1. Symplectic algebra and the Steiner system dictionary.

3. THE ISOMORPHISM BETWEEN THE CANONICAL CLASSES

In this section we describe the isomorphism $k : |K_{C'}|^* \longrightarrow |K_C|^*$ between the duals of the canonical linear systems of the curves C and C'. In Section 4, this description is used to calculate the equation of the canonical embedding of the curve C' in terms of the canonical embedding of the curve C and to describe $\overline{k} : H^0(K_C) \to H^0(K_{C'})$.

We describe the isomorphism k by considering the images and preimages (under the map k) of the sets B, B' (recall the definition following Theorem 2.9) and the points defined below:

$$p := E \cap \overline{q_1 q_2} \smallsetminus \{q_1, q_2\}, \quad p' := E' \cap \overline{q_1' q_2'} \smallsetminus \{q_1', q_2'\}.$$

The resulting description is encoded in the following theorem:

Theorem 3.1. *The isomorphism k is completely determined by the following identities:*

$$\begin{aligned} k(Q' \cap E' \smallsetminus \{q_1', q_2'\}) &= B, \\ k(\overline{q_1' q_2'}) &= \overline{q_1 q_2}, \\ k(B') &= Q \cap E \smallsetminus \{q_1, q_2\}, \\ k(p') &= p, \end{aligned}$$

where the identifications of $Q' \cap E' \smallsetminus \{q_1', q_2'\}$ with B and of B' with $Q \cap E \smallsetminus \{q_1, q_2\}$ are those from Theorem 2.10.

Proof: The theorem follows from Theorem 3.3 and two applications of Theorem 3.2 below. □

To describe the isomorphism k we present it as a composition of three isomorphisms. Denote by j_Y (respectively J_Y) the involution on the curve Y (respectively the homology group $H^0(K_Y)$) induced from the double cover $Y \longrightarrow E$. Denote by $H^0(K_Y)_{\mathrm{odd}}$ (respectively $H^0(K_Y)_{\mathrm{even}}$) the odd (respectively even) part of $H^0(K_Y)$ with respect to the involution J_Y. We denote by $|K_Y|_{\mathrm{odd}}$ (respectively $|K_Y|_{\mathrm{even}}$) the projectivization of the vector space $H^0(K_Y)_{\mathrm{odd}}$ (respectively $H^0(K_Y)_{\mathrm{even}}$). We use the analogous notation for subspaces of $|K_{Y'}|$. The involution J_Y induces an involution on the dual of the canonical system $|K_Y|^*$. The fixed set under this involution is the union of the projective plane $|K_Y|^*_{\mathrm{odd}}$ and a point p_Y, the projectivization of the space $H^0(K_Y)_{\mathrm{even}}$.

By Theorem 2.10 we have a sequence of isogenies of abelian varieties

$$\mathrm{Jac}(C) \xrightarrow{/\alpha^\perp} \mathrm{Prym}(Y/E) \longrightarrow \mathrm{Prym}(Y'/E') \xleftarrow{/\alpha'^\perp} \mathrm{Jac}(C').$$

Taking the tangents spaces at 0 of these varieties, we get the sequence of isomorphisms

$$H^0(K_C) \xrightarrow{\overline{\phi}} H^0(K_Y)_{\mathrm{odd}} \xrightarrow{\overline{\psi}} H^0(K_{Y'})_{\mathrm{odd}} \xleftarrow{\overline{\phi'}} H^0(K_{C'}). \tag{3–1}$$

Taking the duals, inverses, and projectivizations of the spaces and morphisms in (3–1), we get another sequence of isomorphisms,

$$|K_C|^* \xrightarrow{\phi} |K_Y|^*_{\mathrm{odd}} \xrightarrow{\psi} |K_{Y'}|^*_{\mathrm{odd}} \xleftarrow{\phi'} |K_{C'}|^*.$$

By construction, these two morphisms have interpretation in terms of the trigonal and bigonal constructions. With the notation of the trigonal construction "dictionary," the morphism ϕ is induced by $\pi_{W/Y\,*}\pi^*_{W/C}$. In the same way, denoting by M the normalization of the Galois closure of the tower $Y \longrightarrow E \longrightarrow \mathbb{P}^1$, the isomorphism ψ is defined as the composition $\pi_{M/Y'\,*} \circ \pi^*_{M/Y}$.

We discuss the morphism ϕ in Theorem 3.2 below. Our analysis is based on the two views of the set $\{q_i\}_{i=1,\dots,6}$ presented in Theorem 2.5:

- The q_i's are in natural one-to-one correspondence with intersection points of pairs of bitangents that lie in $|K_C|^*$.
- The q_i's are in natural one-to-one correspondence with the fixed points in Y of the involution j_Y, i.e., with the points of $Y \cap |K_Y|^*_{\mathrm{odd}} \subset |K_Y|^*$.

We interpret the relation between these views using the norms in the trigonal construction. If $\pi_{V/U} : V \longrightarrow U$ is one of the covers arising in our construction, we denote the ramification divisor of the map $\pi_{V/U}$ by $R_{V/U}$. We will make repetitive use of the following version of the

Riemann–Hurwitz theorem (see [Hartshorne 77, Proposition IV.2.1]): Let ω be a differential on U. Then the zero divisor of the differential $\pi^*_{V/U}\omega$ is $\pi^*_{V/U}((\omega)_0) + R_{V/U}$.

Theorem 3.2. *The map $\phi : |K_C|^* \longrightarrow |K_Y|^*_{\text{odd}}$ takes each of the q_i's to the corresponding point in $Y \cap |K_Y|^*_{\text{odd}} \subset |K_Y|^*$. Moreover, this property defines ϕ.*

Proof: To avoid confusion between the points of W, Z, Y and divisors, we denote here a point of W by (p_1, p_2), a point on Z by $(p_1 + p_2)$, and a point of Y by $\{(p_1 + p_2), (p_3 + p_4)\}$ if $p_3 + p_4 = j(p_1 + p_2) \in Z$.

Let $\{p_1+p_2, p_3+p_4\}$ be the pair of theta characteristics in Σ_α that represent one of the q_i's (see the discussion following Theorem 2.9). Let $\omega \in H^0(K_C)$ be a differential such that $\omega_0 = 2(p_1 + p_2)$. Then

$$\begin{aligned}(\pi^*_{W/C}(\omega))_0 - R_{W/C} &= \pi^*_{W/C}(\omega_0)\\ &= 2((p_1, p_2) + (p_2, p_1) + \sum_{\substack{1\le i\le 2\\ 3\le j\le 4}} (p_i, p_j)).\end{aligned}$$

So $(\pi^*_{W/C}(\omega)) \ge 2((p_1, p_2) + (p_2, p_1)) + R_{W/C}$.

By the properties of the trigonal construction (see [Donagi 92, p. 74]) we have $R_{W/C} \ge R_{W/Z}$. So we get

$$(\pi^*_{W/C}(\omega) + S\pi^*_{W/C}(\omega))_0 \ge 2((p_1, p_2) + (p_2, p_1)) + R_{W/Z}.$$

The left summand is precisely the pullback of $\pi_{W/Z\,*}\pi^*_{W/C}(\omega)$, so we finally get

$$(\pi_{W/Z\,*}\pi^*_{W/C}(\omega))_0 \ge 2(p_1 + p_2).$$

Now,

$$\begin{aligned}\pi_{Z/Y\,*}\pi_{W/Z\,*}\pi^*_{W/C}(\omega) &= \pi_{W/Y\,*}\pi^*_{W/C}(\omega)\\ &= \overline{\phi}(\omega) \in H^0(K_Y)_{\text{odd}}.\end{aligned}$$

So by invariance under J_Y,

$$(\overline{\phi}(\omega))_0 = (\pi_{W/Y\,*}\pi^*_{W/C}(\omega))_0 \ge 2\{(p_1 + p_2), (p_3 + p_4)\}.$$

Since the q_i's are the intersection points of the two bitangents supported by $(p_1, p_2), (p_3, p_4)$, the last inequality implies

$$\phi(q_i) = \{(p_1 + p_2), (p_3 + p_4)\}.$$

Since the q_i's are six noncollinear points, this property completely describes the map ϕ. □

It remains to analyze the isogeny ψ induced from the bigonal construction relating the double covers $Y \longrightarrow E$ and $Y' \longrightarrow E'$ (see the proof of Theorem 2.10). We make the identifications of Theorem 3.2 (so ψ becomes k). Since the linear system $|p + q_1 + q_2|$ spans the space $|K_Y|^*_{\text{odd}}$ (and the same with the symmetric notation $'$), we reduce the description of the map $\mathbb{P}\psi$ to a description of a natural isomorphism between these linear systems on the curves E, E'.

Theorem 3.3. *The isomorphism ψ is determined by the following identities:*

$$\begin{aligned}\psi(Q' \cap E' \smallsetminus \{q'_1, q'_2\}) &= B,\\ \psi(\overline{q'_1 q'_2}) &= \overline{q_1 q_2},\\ \psi(B') &= Q \cap E \smallsetminus \{q_1, q_2\},\\ \psi(p') &= p,\end{aligned}$$

where the identifications of $Q' \cap E' \smallsetminus \{q'_1, q'_2\}$ with B and of B' with $Q \cap E \smallsetminus \{q_1, q_2\}$ are those from Theorem 2.10.

Proof: The theorem follows from the following two claims:

1. Let t be a point in $\mathbb{P}^1$ and let ω be a differential in $H^0(K_Y)_{\text{odd}}$ such that $\frac{1}{2}\pi_{Y/E\,*}((\omega)_0) = p + \pi^*_{E/\mathbb{P}^1}(t)$. Then the image of ω under $\overline{\psi}$ satisfies $\frac{1}{2}\pi_{Y'/E'\,*}((\overline{\psi}(\omega))_0) = p' + \pi^*_{E'/\mathbb{P}^1}(t)$.
2. Let b be a point in the set $B \subset E$ and let q'_i be the corresponding point (in the sense of Theorem 2.10) in the set $Q' \cap E'$. Let ω be a differential in $H^0(K_Y)_{\text{odd}}$ such that $\pi_{Y'/E'\,*}(\omega)_0 \ge 2b$. Then the image of ω under $\overline{\psi}$ satisfies $(\overline{\psi}(\omega))_0 \ge 2q'_i$.

As in the proof of Theorem 3.2, we make repetitive use of the Riemann–Hurwitz theorem.

Proof of Claim 1: Let ω be a differential as in the first claim above. Since the zero divisor of the differential ω is moving with t, the intersection $(\pi^*_{M/Y}(\omega))_0 \cap R_{M/Y}$ is generically empty. By the definition of the bigonal construction,

$$\begin{aligned}(\overline{\psi}(\omega))_0 &= (\pi_{M/Y'\,*}\pi^*_{M/Y}(\omega))_0\\ &= \frac{1}{2}\pi_{M/Y'\,*}((\pi^*_{M/Y}(\omega))_0 - R_{M/Y})\\ &= \frac{1}{2}\pi_{M/Y'\,*}\pi^*_{M/Y}(\pi_{Y/\mathbb{P}^1}{}^*(t) + \pi_{Y/E}{}^*(p)).\end{aligned}$$

Then

$$\begin{aligned}&\frac{1}{2}\pi_{Y'/E'\,*}\left((\overline{\psi}(\omega))_0\right)\\ &\quad= \frac{1}{2}(\pi_{M/E'\,*}\pi^*_{M/\mathbb{P}^1}(t) + \pi_{M/E'\,*}\pi^*_{M/E}(p))\\ &\quad= \pi^*_{E/\mathbb{P}^1}(t) + p'.\end{aligned}$$

Proof of Claim 2: Define the objects ω, b, q_i' as in the second claim above. By the definition of the point b we have $(\pi_{M/Y}^*(\omega))_0 \geq \pi_{M/\mathbb{P}^1}^*(\pi_{E/\mathbb{P}^1}(b))$, whence

$$\begin{aligned}(\overline{\psi}(\omega))_0 &= (\pi_{M/Y'*}\pi_{M/Y}^*(\omega))_0 \\ &= \frac{1}{2}\pi_{M/Y'*}((\pi_{M/Y}^*(\omega))_0 - R_{M/Y'}) \\ &\geq \frac{1}{2}\pi_{M/Y'*}(\{t \in \pi_{M/\mathbb{P}^1}^*(\pi_{E/\mathbb{P}^1}(b)) | t \notin R_{M/Y'}\}).\end{aligned}$$

To prove the inequality $(\overline{\psi}(\omega))_0 \geq 2q_i$ it suffices to show that $R_{M/Y'} \cap \pi_{M/Y'}^* R_{Y'/E'} = \varnothing$. By the bigonal construction dictionary (see Theorem 2.10), if the cover $Y \longrightarrow \mathbb{P}^1$ is ramified over a point t, then the cover $E' \longrightarrow \mathbb{P}^1$ is étale over t. Since the curve M can be defined as the product $E' \times_{\mathbb{P}^1} Y$, there are no multiple points in the ramification divisor $R_{M/\mathbb{P}^1}$. This proves that $R_{M/Y'} \cap \pi_{M/Y'}^* R_{Y'/E'} = \varnothing$. □

4. A SMALL MATTER OF PROGRAMMING

In the previous sections we presented an explicit construction of the AGM in genus 3. In this section we close the gap between "explicit" and a formula. We tackle five problems: describing the pair (C, α), describing the intermediate data $(E, Q), (E', Q')$ in terms of (C, L_2), describing the pair $(C', \mathcal{L}')$ in terms of the pair $(C, \mathcal{L})$, describing the isomorphism $\overline{k} : H^0(C, K_C) \longrightarrow H^0(C', K_{C'})$, and describing a flag $\tilde{\mathcal{L}}$ in terms of $E', Q', \mathcal{L}'$. We solve these problems by a "coordinification" of the proof of Theorem 3.1. We identify the two spaces $|K_C|^*$ and $|K_{C'}|^*$ under the isomorphism k. We denote the coordinates on this space by x, y, z (we describe a precise choice of coordinates).

Notation. 4.1. To write the equations, we use the lexicographic order on the dual coordinates of x, y, z. That is, instead of writing $ax^2 + bxy + cxz + dy^2 + eyz + fz^2$, we will write (a, b, c, d, e, f). When we talk about the corresponding curve, we will use the projective coordinates $(a : b : c : d : e : f)$. Finally, we will abuse notation by using the name of a curve in $\mathbb{P}^2$ for its defining equation.

The data (C, α): Let us consider the natural bilinear map

$$\begin{aligned}H^0(K_C + \alpha) \times H^0(K_C + \alpha) &\longrightarrow H^0(2K_C) \\ &= H^0(\mathcal{O}_{|K_C|}(2)), \\ ((as_1 + bs_2), (cs_1 + ds_2)) &\mapsto acA_1 + (bc + ad)A_3 + bdA_2,\end{aligned}$$

defined by the tensor multiplication of the sections s_i. Identifying $|K_C + \alpha|$ with $\mathbb{P}^1$, we also get a map

$$m : \mathbb{P}^1 \times \mathbb{P}^1 \to |2K_C|.$$

We simplify the conics A_i by a special choice of our sections s_i: let $\theta_i, \theta_i + \alpha \in \Sigma_\alpha$ for $i = 1, 2$; we assume below that the pair $(\theta_i, \theta_i + \alpha)$ corresponds to the points q_i by Theorem 2.5. Note that the choice of a distinguished pair $\{q_1, q_2\}$ is equivalent to the choice of L_2 in $\mathrm{Jac}(C)[2]$ as described in the trigonal construction "dictionary."

Let l_{1i} (respectively l_{2i}) denote the bitangents corresponding to θ_i (respectively $\theta_i + \alpha$), and let D_{ji} denote the effective divisor of degree 2 such that $2D_{ji} = (l_{ji})_0$. Then we have

$$\begin{aligned}K_C + \alpha &\sim D_{1i} + \sigma(D_{1i}) \sim D_{1i} + i \circ j(D_{1i}) \\ &\sim D_{1i} + i(D_{1i}) \sim D_{1i} + D_{2i}.\end{aligned}$$

We denote by s_i the sections of $H^0(K_C + \alpha)$ corresponding to $D_{1i} + D_{2i}$. With this choice of sections, we have $A_1 = l_{11}l_{21}$ and $A_2 = l_{12}l_{22}$. We now fix the coordinates $(x : y : z)$ of $|K_C|^*$ such that $A_1 = (y - z)(y + z)$ and $A_2 = (x - z)(x + z)$. The following proposition is now a particular case of a classical result (see [Dolgachev 07]).

Proposition 4.2. *The quartic C is given by $A_3^2 - A_1A_2 = 0$. Assume that the quadrics A_1, A_2, A_3 are respectively given by*

$$(0, 0, 0, 1, 0, -1), \quad (1, 0, 0, 0, 0, -1), \quad (a, b, c, d, e, f).$$

Then the coordinates of $C \in |\mathcal{O}_{|K_C|^*}(4)|$ are

$$\begin{aligned}&(a^2 : 2ab : 2ac : b^2 + 2ad - 1 : 2bc + 2ae : 1 + c^2 + 2af \\ &: 2bd : 2cd + 2be : 2ce + 2bf : 2cf : d^2 : 2de : 1 + e^2 + 2df \\ &: 2ef : f^2 - 1).\end{aligned}$$

Below we find the equations for the intermediate data $(E, Q), (E', Q')$.

Theorem 4.3. *Assume that the quadrics A_1, A_2, A_3 are as in Proposition 4.2. The coordinates of the curves $E, E' \in |\mathcal{O}_{|K_C|^*}(3)|$ are*

$$\begin{aligned}E &= (0 : c : b : e : 2(a + d + f) : e : 0 : b : c : 0), \\ E' &= (-2ac : -2ae : b^2 - c^2 - 4af - 1 - 4a^2 : 2cd \\ &\quad : 4b(d - a) : 2be - 4ac - 2cf : 2de \\ &\quad : 1 - b^2 + 4d^2 + e^2 + 4df : 2e(2d + f) - 2bc \\ &\quad : e^2 - c^2).\end{aligned}$$

The coordinates of the conics $Q, Q' \in |\mathcal{O}_{|K_C|^*}(2)|$ *are*

$$\begin{aligned} Q = (&0 : ce(b^2 - 1 + 4ad) - 2b(c^2d + e^2a) \\ &: b(-2bcd - e + b^2e) + 2a(b^2c + ce^2 - 2bef) - 4a^2be \\ &: 0 : b^3c + 2c^2de + 2b^2(d-a)e - bc(1 + 4d^2 + 4df) \\ &: c^2e^2 + b^2(c^2 + e^2) - 2bce(a + d + f)), \\ Q' = (&-a(e^2 - c^2) : 0 : (d-a)(c(a + d + f) - be) \\ &: d(c^2 - e^2) : 2(a-d)(e(a + d + f) - bc) \\ &: (d-a)(c^2 - e^2)). \end{aligned}$$

The essence of the proof is to convert the problem into a sequence of "steps" of the following form: *find a pencil that is spanned by two known forms and contains another form that we have to calculate.* We perform these steps explicitly using a computer. Let us stress, though, that in most cases, two of the three forms involved in the computation are divisible by a known linear form. Thus, the obstinate reader could still check the computations below, up to and including Theorem 4.9, by hand.

The curve E: Recall (see the trigonal construction "dictionary") that to any point $p_1+p_2 \in Z$ one associates a point $q \in E \subset |K_C|^*$ as $\overline{p_1p_2} \cap \overline{p_3p_4}$, where $i(p_1+p_2) = p_3+p_4 \in Z$. Denote by A the conic given by the product of the lines $\overline{p_1p_2}$ and $\overline{p_3p_4}$. Note that the singular point of A is q.

Lemma 4.4. *There exists a unique pair of sections (up to permutation)* $(t_1, t_2) \in H^0(K_C+\alpha)^{\otimes 2}$ *such that* $t_1t_2 = A$. *Conversely, the singular point of each singular conic in* $m(\mathbb{P}^1 \times \mathbb{P}^1)$ *is on* E.

Proof: Let us prove the first assertion. By definition of j, the zero divisor of A is $2K_C \sim p_1 + p_2 + j(p_1 + p_2) + p_3 + p_4 + j(p_3 + p_4)$. Since $p_3 + p_4 = i(p_1 + p_2)$, one gets

$$(A)_0 = p_1 + p_2 + j \circ i(p_1 + p_2) + i(p_1 + p_2) + \sigma \circ i(p_1 + p_2).$$

Since $p_1 + p_2 + \sigma(p_1 + p_2) \in |K_C + \alpha|$ (respectively $i(p_1 + p_2) + \sigma \circ i(p_1 + p_2) \in |K_C + \alpha|$), the divisor defines a unique section t_1 (respectively t_2) in $H^0(K_C + \alpha)$. □

To account for the permutation of the two lines in Lemma 4.4, we introduce the map

$$\begin{aligned} v_2 : \mathbb{P}^1 \times \mathbb{P}^1 &\to \mathbb{P}^2 \simeq \mathrm{Sym}^2 \mathbb{P}^1 \\ (\lambda, \mu), (\lambda', \mu') &\mapsto (\lambda\lambda', \mu\mu', \lambda\mu' + \mu\lambda'). \end{aligned}$$

Let $(X : Y : Z)$ be the coordinates in $v_2(\mathbb{P}^1 \times \mathbb{P}^1)$. Lemma 4.4 can be reformulated to say that the curve E can be seen as the locus $(x : y : z)$ of singular points in the net of conics $XA_1 + YA_2 + ZA_3$. If $M = X_0A_1 + Y_0A_2 + Z_0A_3$ is such a conic, it is singular at q_0 if and only if

$$\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} M_x(q_0) \\ M_y(q_0) \\ M_z(q_0) \end{pmatrix} = \begin{pmatrix} (A_1)_x(q_0) & (A_1)_y(q_0) & (A_1)_z(q_0) \\ (A_2)_x(q_0) & (A_2)_y(q_0) & (A_2)_z(q_0) \\ (A_3)_x(q_0) & (A_3)_y(q_0) & (A_3)_z(q_0) \end{pmatrix}^t \times \begin{pmatrix} X_0 \\ Y_0 \\ Z_0 \end{pmatrix}.$$

Denote by $\mathrm{Jac}(A_1, A_2, A_3)$ the previous matrix. Thus the curve E is given by $\det(\mathrm{Jac}(A_1, A_2, A_3)) = 0$.

The curve Q: It is easy to check algebraically that the point $o := (0 : 0 : 1)$ lies on E (see Lemma 4.8 for a geometric explanation). Let $\hat{q_1} := \overline{oq_1} \cap E \smallsetminus \{o, q_1\}$ and $\hat{q_2} := \overline{oq_2} \cap E \smallsetminus \{o, q_2\}$. Let

$$\hat{Q} := \mathrm{Nulls}\left(4\frac{\partial A_3}{\partial x}\frac{\partial A_3}{\partial y} - \frac{\partial A_1}{\partial y}\frac{\partial A_2}{\partial x}\right).$$

Proposition 4.5. *The cubics* E, $Q\overline{\hat{q_1}\hat{q_2}}$, $\hat{Q}\overline{q_1q_2}$ *lie in the same pencil. Moreover,* $p \in \overline{\hat{q_1}\hat{q_2}}$.

Proof: See Figure 1 for a "graphical demonstration." Recall that the intersection points q_i of $Q \cap E$ are the intersection points of the pairs of bitangents θ_i, $\theta_i + \alpha$. With the notation of the previous proof, if $p_1 + p_2$ is the divisor associated to θ_i, the divisor associated to the product of the two lines is $2(p_1+p_2)+2i(p_1+p_2)$. So $t_1 = t_2$, and the

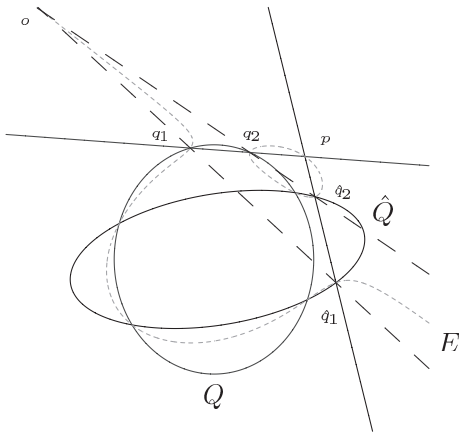


FIGURE 1. The geometry of Proposition 4.5.

points q_i correspond to singular points of singular conics of the form $m((\lambda:\mu),(\lambda:\mu))$, i.e.,

$$Q\cap E=\{(x:y:z)\mid \operatorname{Jac}(A_1,A_2,A_3)^t\cdot(\lambda^2,\mu^2,2\lambda\mu)^t=0 \text{ for one } (\lambda:\mu)\in\mathbb{P}^1\}.$$

Since $\frac{\partial A_2}{\partial x}=\frac{\partial A_1}{\partial y}=0$, the points of $Q\cap E$ are the $(x:y:z)$ coordinates for which the following system admits a solution:

$$\begin{aligned}\frac{\partial A_2}{\partial x}\mu^2+2\frac{\partial A_3}{\partial x}\lambda\mu=0,\\ \frac{\partial A_1}{\partial y}\lambda^2+2\frac{\partial A_3}{\partial y}\lambda\mu=0,\\ \frac{\partial A_1}{\partial z}\lambda^2+\frac{\partial A_2}{\partial z}\mu^2+2\frac{\partial A_3}{\partial z}\lambda\mu=0,\\ (\lambda,\mu)\neq(0,0).\end{aligned}$$

If $\lambda=0$ (respectively $\mu=0$), this system admits q_1 (respectively q_2) as a solution. If $\lambda\mu\neq 0$, then a solution satisfies

$$\left(\frac{\partial A_2}{\partial x}:-2\frac{\partial A_3}{\partial x}\right)=(\lambda:\mu)=\left(-2\frac{\partial A_3}{\partial y}:\frac{\partial A_1}{\partial y}\right),$$

so it belongs to $\hat{Q}$. Hence the intersection points of $\hat{Q}$ and Q are $E\cdot Q\setminus\{q_1,q_2\}=B'$ (see Theorem 3.1).

It follows from the definition of $\hat{q}_i$ that $\hat{q}_i\in\hat{Q}$ for $i=1,2$. We compute the intersections:

$$\begin{aligned}E\cdot(Q\overline{\hat{q}_1\hat{q}_2})&>(B'+q_1+q_2)+\hat{q}_1+\hat{q}_2,\\ E\cdot(\hat{Q}\overline{q_1q_2})&>(B'+\hat{q}_1+\hat{q}_2)+(q_1+q_2+p).\end{aligned}$$

These three cubics thus have eight points in common, so they lie in the same pencil. Moreover, their last intersection point is the same, too, so $p\in\overline{\hat{q}_1\hat{q}_2}$. □

The curve E': For the purpose of describing the isotropic subgroup L_3, as well as for technical reasons, we set the following notation: Denote by Q_p the unique conic such that $Q_p\cdot E=2p+B$, and by Q'_p the unique conic such that $Q'_p\cdot E'=2p+B'$ (the notation B,B',p was defined following Theorem 2.9 and at the beginning of Section 3). Recall that under the identification of the linear system given by k, we have $E\cap Q\cap Q'_p=B'$ and $E'\cap Q'\cap Q_p=B$.

Proposition 4.6. *The plane cubics E, $QT_p(E)$, $\overline{q_1q_2}Q'_p$ lie in the same pencil.*

Proof: See Figure 2 for a "graphical demonstration." As in the previous proof, this follows after the intersections

$$\begin{aligned}E\cdot(Q+T_p(E))&>(B'+q_1+q_2)+2p,\\ E\cdot(\overline{q_1q_2}Q'_p)&>(q_1+q_2+p)+(B'+p),\end{aligned}$$

are calculated. □

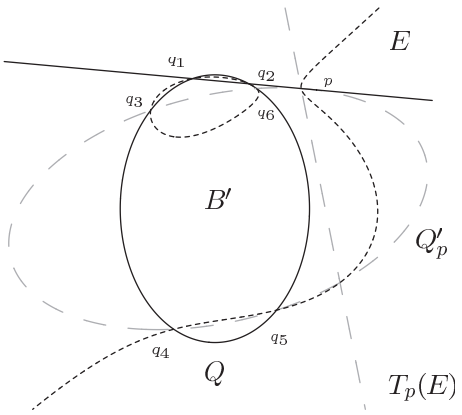


FIGURE 2. The geometry of Proposition 4.6.

Let $J=\cup_{b\in B'}\overline{pb}$; we compute the quartic defining J using the following procedure:

1. Since $p=(-e:c:0)$, the lines passing through p are given by linear forms $cx+ey-\alpha z=0$ for some $\alpha\in\mathbb{C}$. Thus $J=\prod_{i=1}^4(cx+ey-\alpha_i)$, where the α_i's are defined by the property $cx_i+ey_i=\alpha_i$ for each of the four points $(x_i:y_i:1)\in B'$.

2. Let $Y=cx+ey$. Then $Y_i:=cx_i+ey_i$ are the roots of the polynomial $R(Y)=\big(\text{Resultant}(Q(x,(Y-cx)/e,1),\ Q'_p(x,Y-cx)/e,1),x\big)$. So by definition, in *affine* coordinates, $J=R(cx+ey)$.

Proposition 4.7. *The plane quartics $E'T_p(Q'_p),{Q'_p}^2,J$ lie in the same pencil.*

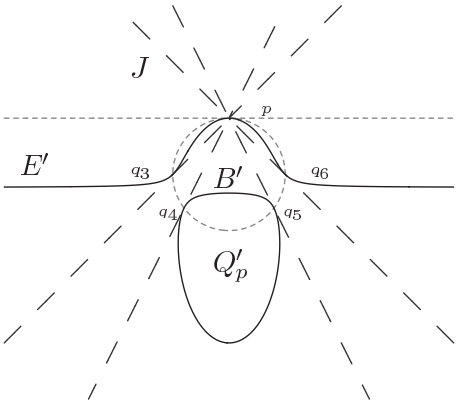


FIGURE 3. The geometry of Proposition 4.7.

Proof: See Figure 3 for a "graphical demonstration." By the definition of J, Q'_p we have

$$Q'^{\,2}_p \cdot J = 2(B' + 4p)$$

and

$$Q'^{\,2}_p \cdot (E' + T_p(Q'_p)) = 2((B' + 2p) + 2p).$$

So the three quartics belong to the same pencil. □

The curve Q': We compute Q' using Proposition 4.6 and symmetry. To compute the conic Q_p, one notes that $Q_p \cdot E = 2p + B$. By the definition of B following Theorem 2.9, $b \in B$ if and only if $T_b(E) \cdot E = 2b + p$. It is then classical (see, for instance, [Salmon 79]) that Q_p is the polar conic of p with respect to E; recall that if $p = (x_0 : y_0 : z_0) \in E$, then the polar conic of p with respect to E is given by the equation $x_0E_x + y_0E_y + z_0E_z = 0$.

To complete the calculation of $(C', \mathcal{L}')$ from $(C, \mathcal{L})$ we still have to make a final choice: the partition of the set B' to the two pairs $\{\{q_3, q_4\}, \{q_5, q_6\}\}$. Geometrically, this is the choice of the singular conic $\overline{q_3q_4} \cup \overline{q_5q_6}$ among the three singular conics in the pencil spanned by the conics Q, Q'_p. We start with a lemma on the symmetric situation:

Lemma 4.8. *The following equality holds:*

$$\overline{q'_3q'_4} \cap \overline{q'_5q'_6} = p + \alpha_E = o,$$

where the addition is in $\mathrm{Pic}(E)$.

Proof: To see the first equality, note that $2q'_i + p$ is a line section of $E \subset |K_C|^*$ for all $i = 3, \dots, 6$. By the proof of Theorem 2.10 and the symmetry on the construction, we also have $q'_3 - q'_4 = q'_5 - q'_6 = \alpha_E$. Setting $\tilde{o} := p + \alpha_E$, we see that $q_3 + q_4 + \tilde{o} = 2q_3 + p$ and $q_5 + q_6 + \tilde{o} = 2q_5 + p$ are both line sections. To see the second equality, note that $T_pE \cap T_oE$ lies on E, which means that $\gamma := p - o$ is in $\mathrm{Pic}(E)[2]$. However, by a monodromy argument on maximal isotropic flags on $\mathrm{Jac}(C')[2]$ containing L'_2, we have $\gamma = \alpha_E$. □

In order to find an equation for (C', α') in the form $A'^2_3 = A'_1A'_2$, we apply a projective transformation to mimic the form of the pair (E, Q). Denote by T a projective transformation of $|K_C|^*$ that sends q'_1, q'_2, and $\overline{q_3q_4} \cap \overline{q_5q_6}$ to the points $(1 : 0 : 0)$, $(0 : 1 : 0)$, and $(0 : 0 : 1)$ respectively. Define $T(E') = (e_1, \dots, e_{10})$ and $T(Q') = (d_1, \dots, d_6)$. Finally, define T_2 to be the transformation that operates by multiplication of the x-axis by $\sqrt{e_2/e_9}$ and multiplication of the y-axis by $\sqrt{e_4/e_6}$.

Theorem 4.9. *The coordinates of the quadratic forms $T(A'_1), T(A'_2)$ are given by*

$$(0, 0, 0, e_4/e_6, 0, -1), \quad (e_2/e_9, 0, 0, 0, 0, -1),$$

while the coordinates of the quadric form $T(A'_3)$ are given by

$$\begin{aligned}\frac{1}{X}\big(&e_2e_6(e_2d_3 - e_3d_2),\ 2e_2e_3e_4d_6,\ 2e_2^2e_6d_6,\\ &e_4(e_2e_6d_5 - e_3e_9d_2),\ 2e_2e_4e_6d_6,\\ &-e_6(-e_2e_5d_6 + e_2e_6d_5 + e_2e_9d_3 - 2e_3e_9d_2)\big),\end{aligned}$$

where X is given by

$$\sqrt{\begin{aligned}&4e_6e_9(e_6e_2e_5d_6e_3d_2 + e_6^2e_2^2d_3d_5 - e_6^2e_2e_3d_2d_5\\ &- e_9e_6e_2d_3e_3d_2 + e_9e_6e_3^2d_2^2 - e_6e_2^2e_3d_5d_6\\ &- e_6^2e_2^2d_2d_6 + e_2e_3^2e_4d_6^2 - e_2e_3e_4e_6d_3d_6)\end{aligned}}.$$

Proof: Let us assume that we have taken A'_1 (respectively A'_2) such that $T_2 \circ T(A'_1)$ (respectively $T_2 \circ T(A'_1)$) is the conic $y^2 - z^2$ (respectively $x^2 - z^2$). Let $T_2 \circ T(A'_3) = (a', b', c', d', e', f')$. By Theorem 4.3, if we call (E_2, Q_2) the data (E, Q) associated to these transformations of A'_1, A'_2, A'_3, we have

$$\begin{aligned}E_2 = \big(&0 : c' : b' : 0 : e' : 2(a' + d' + f') : e' : 0 : b' : c' : 0\big),\\ Q_2 = \big(&0 : c'e'(b'^2 - 1 + 4a'd') - 2b'(c'^2d' + e'^2a');\\ &b'(-2b'c'd' - e' + b'^2e')\\ &+ 2a'(b'^2c' + c'e'^2 - 2b'e'f') - 4a'^2b'e' : 0;\\ &b'^3c' + 2c'^2d'e' + 2b'^2(d' - a')e'\\ &- b'c'(1 + 4d'^2 + 4d'f');\\ &c'^2e'^2 + b'^2(c'^2 + e'^2) - 2b'c'e'(a' + d' + f')\big).\end{aligned}$$

If we let $T_2 \circ T(E') = (0, \hat{c}, \hat{b}, \hat{e}, \hat{g}, \hat{e}, 0, \hat{b}, \hat{c}, 0)$ and $T_2 \circ T(Q') = (0, \delta_1, \delta_2, 0, \delta_3, \delta_4)$, there exists a constant ξ such that

$$b' = \hat{b}/\xi, \quad c' = \hat{c}/\xi, \quad e' = \hat{e}/\xi, \quad a' + d' + f' = \hat{g}/(2\xi),$$

and

$$\begin{aligned}&\begin{pmatrix} -2\hat{b}\hat{c}^2 & -2\hat{b}\hat{e}^2 & \hat{c}\hat{e} \\ -2\hat{b}^2\hat{c} & 2\hat{b}^2\hat{c} + 2c\hat{e}^2 - 2\hat{b}\hat{e}\hat{g} & \hat{b}\hat{e} \\ 2\hat{b}^2\hat{e} + 2\hat{c}^2\hat{e} - 2\hat{b}\hat{c}\hat{g} & -2\hat{b}^2\hat{e} & \hat{b}\hat{c} \end{pmatrix}\\ &\times \begin{pmatrix} d'\xi \\ a'\xi \\ 4a'd'\xi^2 - \xi^2 \end{pmatrix} + \hat{b}^2 \begin{pmatrix} \hat{c}\hat{e} \\ \hat{b}\hat{e} \\ \hat{b}\hat{c} \end{pmatrix}\\ &= \frac{\hat{c}^2\hat{e}^2 + \hat{b}^2(\hat{c}^2 + \hat{e}^2) - \hat{b}\hat{c}\hat{e}\hat{g}}{\delta_4} \begin{pmatrix} \delta_1 \\ \delta_2 \\ \delta_3 \end{pmatrix}.\end{aligned}$$

By the geometry of the configuration and the coordinates we chose, the only solutions a', d', ξ to the system above arise from solutions of the quadric $T_2 \circ T(A_3')$. Since the quadric A_3' is determined up to a sign, the matrix equation above has only one solution, and this solution determines a', d', ξ up to a choice of sign. We apply then the transformation T_2^{-1} to obtain the expression of $T(A_3)$ in terms of e_i, d_i. □

Remark 4.10. Note that the transformation T_2 and the square roots $\sqrt{e_2/e_9}$, $\sqrt{e_4/e_6}$ served merely as technical aids in the proof above, and indeed vanished in the final result. The situation is different with the root we take to distinguish between q_1' and q_2'. Recall that when performing the trigonal construction, one has to take a degree-2 field extension in order to construct W' from the tower $Z'/X'/\mathbb{P}^1$, and one has to construct W' in order to construct C'.

Since after distinguishing between q_1' and q_2' we can construct C', the root we take when we distinguish between these points generates the field extension of the function field of W' over the function field of Z'. This carries little significance when one is working over an algebraically closed field, but in working over a nonalgebraically closed field, it reflects the fact that in order to find the isogeny $\mathrm{Prym}(Z/X) \cong \mathrm{Jac}(C)$ we may have to make a degree-2 field extension of the base field.

Corollary 4.11. *Let $\mathcal{M}$ be the moduli of a, b, c, d, e, f and a root of the cubic form (in t)* $\mathrm{Hessian}(tQ_p' + Q)$. *Then:*

- *The space $\mathcal{M}$ is birational to a finite cover of the moduli of $(C, \mathcal{L})$ with monodromy group naturally isomorphic to D_4.*
- *The map $T_2 \circ T$ is defined globally over $\mathcal{M}$. Moreover, as a map on quadrics in x, y, z with parameters in $\mathcal{M}$, the map $T_2 \circ T$ is an involution that lifts the involution $(C, \mathcal{L}) \longrightarrow (C', \mathcal{L}')$.*
- *Using affine coordinates on $|K_C|^*$ (by setting $z = 1$), the map $\overline{k}$ is given by the formula*

$$T_2 \circ T\left(\frac{l\,dx}{\partial(A_1'A_2' - {A_3'}^2)/\partial y}\right) = \pm\overline{k}^{-1}\left(\frac{l\,dx}{\partial(A_1A_2 - A_3^2)/\partial y}\right),$$

where l is any linear form.

Proof: The first assertion follows from the choice of coordinates we use (see Theorem 4.3) and the fact that the singular conics in the pencil of conics spanned by Q_p', Q are in one-to-one correspondence with the roots of the cubic $\mathrm{Hessian}(tQ_p' + Q)$. The dihedral group is the symmetry group acting on the nested partition of linear forms $\{\{x - z, x + z\}, \{y - z, y + z\}\}$.

The second assertion follows from the definition of T and T_2, and from Theorem 4.9.

It is well known that a basis of regular differentials on a genus-3 nonhyperelliptic curve C can be given by $\left(\frac{l\,dx}{\partial(C)/\partial y}\right)$. With the identifications we have made during the construction on the coordinates

$$(x : y : z), \quad (x' : y' : z')$$

(see the beginning of Section 4), the map $\overline{k}$ with this choice of bases is given by the transformation $(T_2 \circ T)^{-1}$ up to a constant. However, since $T_2 \circ T$ is an involution on $\mathcal{M}$, the square of this constant is 1. □

Our final objective in this section is to show how one iterates the construction. Following the discussion below Proposition 2.2, we use a tilde ($\sim$) to indicate the objects related to $(C', \tilde{\mathcal{L}})$.

Our first task is to find an $\tilde{\alpha}$. By our analysis of the symplectic pairings in Proposition 2.2 and following Theorem 2.9, we have

$$\#D_{\alpha'}^{-1}(\tilde{\alpha}) \cap \{q_1', q_2'\} = 0 \iff \tilde{\alpha} \in L_2'^{\perp} \smallsetminus L_2',$$
$$\#D_{\alpha'}^{-1}(\tilde{\alpha}) \cap \{q_5', q_6'\} = 1 \iff \tilde{\alpha} \notin L_3'.$$

So we can assume that $D_{\alpha'}^{-1}(\tilde{\alpha}) = \{q_3', q_5'\}$. The situation can be represented as in Figure 4.

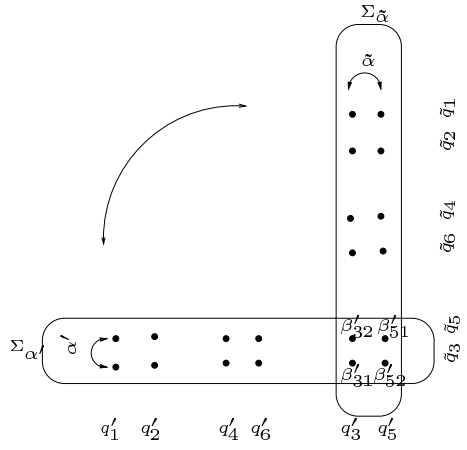


FIGURE 4. Calculation of data on the "new" curve.

Thus, the four bitangents β'_{31}, β'_{32} (lying over q'_3), β'_{51}, β'_{52} (lying over q'_5) in $\Gamma_{\alpha'\oplus\alpha} = \Sigma_{\alpha'} \cap \Sigma_{\tilde{\sigma}}$ (Proposition 2.1) can be grouped as $(\beta'_{31}, \beta'_{52})$ and $(\beta'_{51}, \beta'_{32})$ to give a possible $\tilde{\alpha}$ (the other grouping corresponds to an $\tilde{\alpha}+\alpha'$). Let us set $\tilde{q}_3 = \beta'_{31} \cap \beta'_{52}$ and $\tilde{q}_5 = \beta'_{51} \cap \beta'_{32}$. Let $\tilde{E}$, $\tilde{Q}$ be the cubic and conic associated to $(C', \tilde{\alpha})$. We define $\{\tilde{q}_i\}_{i=1}^6 = \tilde{Q} \cap \tilde{E}$.

The second step is to find $\tilde{L}_2$. By Proposition 2.2, a maximal isotropic group that contains α' (respectively $\tilde{\alpha}$) is equivalent to the partition of $\Sigma_{\alpha'}/\alpha'$ (respectively $\Sigma_{\tilde{\alpha}}/\tilde{\alpha}$) into three pairs. There are three different maximal isotropic spaces containing $\alpha' \oplus \tilde{\alpha}$, given by the nonzero points in $(\alpha' \oplus \tilde{\alpha})^\perp/(\alpha' \oplus \tilde{\alpha})$. These maximal flags are in bijection with partitions into two pairs of the points $\{q'_1, q'_2, q'_4, q'_6\}$, and also with partitions into two pairs of the points $\{\tilde{q}_1, \tilde{q}_2, \tilde{q}_4, \tilde{q}_6\}$.

One of the three maximal isotropic groups containing $\tilde{\alpha}\oplus\alpha'$ is $\tilde{\alpha}\oplus L'_2$. The two others correspond to $\alpha' \oplus \tilde{L}_2$ for the two different choices of $\tilde{L}_2$. Thus, in order to choose $\tilde{L}_2$, we first choose the maximal isotropic group $\alpha' \oplus \tilde{L}_2$, and in making this choice, we exclude the partition corresponding to the group $\tilde{\alpha} \oplus L'_2$.

The partition of $\{q'_1, q'_2, q'_4, q'_6\}$ that corresponds to $\alpha' \oplus \tilde{L}_2$ is simply the partition $\{q'_1, q'_2\}, \{q'_4, q'_6\}$, but in order to proceed we will have to find the corresponding partition of $\{\tilde{q}_1, \tilde{q}_2, \tilde{q}_4, \tilde{q}_6\}$. To do this we will describe explicitly the natural isomorphism between the three partitions into two pairs of these 4-tuples. This isomorphism is geometric in nature, and to describe it we will interpret these partitions as singular conics defined by the partitions.

To describe the isomorphism we need some more notation. If $\alpha_1, \alpha_2 \in \mathrm{Jac}(C')[2]$ such that $\langle \alpha_1, \alpha_2 \rangle = 0$, one denotes by $A_{3,\alpha_i}, E_{\alpha_i}, Q_{\alpha_i}, p(\alpha_i)$ the elements A_3, E, Q, p relative to the construction starting from (C', α_i). Also, we denote by $E_{\alpha_i\oplus\alpha_j}$ and $Q_{p(\alpha_i),\alpha_j}$ the curve E' and the conic Q'_p constructed from the data $(C', \alpha_i \subset \alpha_i \oplus \alpha_j)$, and by $'$ the symmetric constructions. Note that

$$E_{\alpha_i\oplus\alpha_j} = E'_{(\alpha_i\oplus\alpha_j)^\perp/L} = E_{\alpha_j\oplus\alpha_i}$$

for any maximal isotropic group L containing $\alpha_i \oplus \alpha_j$. However, $Q_{p(\alpha_i),\alpha_j} \neq Q_{p(\alpha_j),\alpha_i}$.

Lemma 4.12. *The identification of a singular conic through $\{q'_1, q'_2, q'_4, q'_6\}$ (respectively $\{\tilde{q}_1, \tilde{q}_2, \tilde{q}_4, \tilde{q}_6\}$) with a root of*

$$\mathrm{Hessian}(Q_{\alpha'} + uQ_{p(\alpha'),\tilde{\alpha}}),$$

respectively

$$\mathrm{Hessian}(Q_{\tilde{\alpha}} + uQ_{p(\tilde{\alpha}),\alpha'}),$$

defines a natural transformation $\mu : \mathbb{P}^1 \to \mathbb{P}^1$ that fixes ∞ and maps the two triple of roots bijectively.

Proof: We have $E_{\alpha'\oplus\tilde{\alpha}} = E_{\tilde{\alpha}\oplus\alpha'}$. Let t be the translation on $E_{\tilde{\alpha}\oplus\alpha'}$ by $p(\tilde{\alpha}) - p(\alpha')$. Let $s_{Q_{p(\alpha'),\tilde{\alpha}}}, s_{Q_{\alpha'}}$ (respectively $s_{Q_{p(\tilde{\alpha}),\alpha'}}, s_{Q_{\tilde{\alpha}}}$) denote the sections of the bundle of $E_{\alpha'\oplus\tilde{\alpha}}$ defined by the divisor $q'_1+q'_2+q'_4+q'_6$ (respectively $\tilde{q}_1, \tilde{q}_2, \tilde{q}_4, \tilde{q}_6$) and corresponding to the subscript objects. Since $Q_{p(\alpha'),\tilde{\alpha}}$ (respectively $Q_{p(\tilde{\alpha}),\alpha'}$) is *the* polar conic of $p(\alpha')$ (respectively $p(\tilde{\alpha})$), there exists $a \in K$ such that

$$t^*(s_{Q_{p(\alpha'),\tilde{\alpha}}}) = as_{Q_{p(\tilde{\alpha}),\alpha'}}.$$

Thus t maps the points $\{q'_1, q'_2, q'_4, q'_6\}$ onto $\{\tilde{q}_1, \tilde{q}_2, \tilde{q}_4, \tilde{q}_6\}$. Since $t^*(s_{Q_{\alpha'}})$ contains the points $\{\tilde{q}_1, \tilde{q}_2, \tilde{q}_4, \tilde{q}_6\}$, there are also two constants b, c such that $t^*(s_{Q_{\alpha'}}) = bs_{Q_{\tilde{\alpha}}} + cs_{Q_{p(\tilde{\alpha}),\alpha'}}$. Thus any section in the pencil $s_{Q_{\alpha'}} + us_{Q_{p(\alpha'),\tilde{\alpha}}}$ is mapped through t onto $bs_{Q_{\tilde{\alpha}}} + (au + c)s_{Q_{p(\tilde{\alpha}),\alpha'}}$. Hence there is an affine transformation μ that maps a conic $Q_{\alpha'} + uQ_{p(\alpha'),\tilde{\alpha}}$ to $Q_{\tilde{\alpha}'} + \mu(u)Q_{p(\tilde{\alpha}),\alpha'}$. In particular, a singular conic is mapped to a singular conic, which means that μ maps the three roots of $\mathrm{Hessian}(Q_{\alpha'} + uQ_{p(\alpha'),\tilde{\alpha}})$ to the three roots of $\mathrm{Hessian}(Q_{\tilde{\alpha}} + uQ_{p(\tilde{\alpha}),\alpha'})$.

To identify the transformation μ, we work on the generic case C' given by (a', b', c', d', e', f'), and we are looking for a continuous affine transformation. We assume that the bitangents β'_{31}, β'_{32}, β'_{51}, β'_{52} are $y - z$, $y + z$, $x - z$, $x + z$ respectively.

Denote by

$$T := \frac{1}{2}\begin{pmatrix} -1 & 1 & 2 \\ 1 & -1 & 2 \\ 1 & 1 & 0 \end{pmatrix}$$

the transformation that sends $y - z$, $y + z$, $x - z$, $x + z$ to $y - z$, $x + z$, $x - z$, $y + z$ respectively. This projective transformation defines a linear transformation $T_{\tilde{\alpha}}$ on the coefficients of $A_{3,\alpha'}$ given by (a', b', c', d', e', f') maps to the coefficients of $A_{3,\tilde{\alpha}}$:

$$\Big(\frac{1}{4}(a' - b' - c' + d' + e' + f'),\ \frac{1}{2}(-a' + b' - d' + f'),\ \frac{1}{2}(-2a' + c' + 2d' + e'),\ \frac{1}{4}(a' - b' + c' + d' - e' - f'),\ \frac{1}{2}(2a' + c' - 2d' + e'),\ a' + b' + d'\Big).$$

Using Theorem 4.3, we can compute the different objects involved, and we obtain

$$\begin{aligned}\mu(u) = {} & (2a' - c' - 2d' - e') \cdot (2a' + c' - 2d' + e') \\ & \cdot (2a'b'e'^2 - 4a'c'd'e' - b'^2c'e' + 2b'c'^2d' + c'e')u \\ & + 2e' \cdot c' \cdot a' \\ & \cdot (4a'^2b' - 8a'b'd' - 2a'c'e' - b'c'^2 + 4b'd'^2 - be'^2 \\ & - 2c'd'e' + 2c'e'f').\end{aligned}$$

Let us say a few words about the computation: We are comparing the coefficients of two monic cubic forms in u under the transformation $u \mapsto (\mu_0 u + \mu_1)$. Thus we get the equation

$$\begin{aligned}\epsilon(u^3 + a_2u^2 + a_1u + a_0) = {} & (\mu_0u + \mu_1)^3 + b_2(\mu_0u + \mu_1)^2 \\ & + b_1(\mu_0u + \mu_1) + b_0.\end{aligned}$$

Comparing the u coefficients, we get a system of equations in μ_0, μ_1:

$$\begin{aligned}3\mu_1 + b_2 - \mu_0a_2 &= 0, \\ 3\mu_1^2 + 2b_2\mu_1 + b_1 - \mu_0^2a_1 &= 0, \\ \mu_1^3 + b_2\mu_1^2 + b_1\mu + b_0 - \mu_0^3a_0 &= 0.\end{aligned}$$

We solve the system by finding the two solutions of the first two equations and checking which of the two solutions solves the third equation. □

By a projective transformation one can send the bitangents β'_{31}, β'_{32}, β'_{51}, β'_{52} to $y - z$, $y + z$, $x - z$, $x + z$ respectively. Using the previous lemma, one can then identify the value u_0 of u corresponding to $\tilde{\alpha} + L'_2$ (i.e., to the singular conic whose one component is $\overline{q'_1q'_2}$) and then exclude the singular conic $Q_{\tilde{\alpha}} + \mu(u_0)Q_{p(\tilde{\alpha}),\alpha'}$. Let us denote this one by $\overline{\tilde{q}_1\tilde{q}_2} \cup \overline{\tilde{q}_4\tilde{q}_6}$, and then $\tilde{L}_2$ is represented, for instance, by $\overline{\tilde{q}_4\tilde{q}_6}$.

The last task is to identify $\tilde{L}_3$: by Lemma 2.3, it has to contain one of the points $\tilde{q}_3$, $\tilde{q}_5$, so it is given by any choice of a pair $\{\tilde{q}_2, \tilde{q}_5\}$ or $\{\tilde{q}_2, \tilde{q}_3\}$.

5. REAL CURVES

In this section we show that if C is a real M-curve of genus 3 (i.e., a curve with four components), then the *topology* of the real structure induces a distinguished isotropic flag $L_1 \subset L_3$ in $\mathrm{Jac}(C)[2]$ such that the curve C' is an M-curve.

In Theorem 5.1 we establish a bijection between partitions of the four components of the curve C into two pairs and the set of full flags $\mathcal{L}$ containing the flag $L_1 \subset L_3$.

Following Proposition 5.2 we show how to find the *topologically* distinguished flag $\tilde{\mathcal{L}}'$ on the curve C' using the data $C', \mathcal{L}'$ (one calculates the pair $(C', \mathcal{L}')$ from the pair $(C, \mathcal{L})$) by taking square roots as described below Corollary 4.11, thus getting an iterative process.

We will show that the choice of these square roots is uniquely determined by the topology.

Finally, we describe the iterative integration algorithm.

Let C be a real plane quartic with four components C_1, C_2, C_3, C_4. We denote by $\mathrm{Jac}_{\mathbb{R}}(C)$ the real part of the Jacobian of the curve C, and by $\mathrm{Jac}_{\mathbb{R}}(C)_0$ the 0-component of $\mathrm{Jac}_{\mathbb{R}}(C)$; see [Gross and Harris 81, p. 159]. Recall that since the degree of the curve C is even, each of the C_i's is null homotopic in $\mathbb{PR}^2$ (see, e.g., [Gross and Harris 81]). Therefore, the set $\mathbb{RP}^2 \smallsetminus C_i$ is a union of a disk and a Möbius strip. Recall also that the quotient $\mathrm{Jac}_{\mathbb{R}}(C)[2]/\mathrm{Jac}_{\mathbb{R}}(C)_0[2]$ is naturally isomorphic to the vector space $\mathbb{F}_2[C_1, C_2, C_3, C_4]/\mathbb{F}_2$, where $\mathbb{F}_2$ acts by adding $1_{\mathbb{F}_2}$ to all the coordinates.

Let $\{\{C_1, C_3\}, \{C_2, C_4\}\}$ be a partition of the four components into two pairs. Denote by c_i a point in the trivial component of $\mathbb{PR}^2 \smallsetminus C_i$, and choose the infinity line l_∞ in $\mathbb{PR}^2$ such that the four points c_1, c_2, c_3, c_4 admit a cyclic order in $\mathbb{PR}^2 \smallsetminus l_\infty$ (formally, this means that c_1, c_2, c_3, c_4 sit on an ellipse in $\mathbb{PR}^2 \smallsetminus l_\infty$ in the order $1, 2, 3, 4$). We assume that the order induced on c_1, c_2, c_3, c_4 from the choice of the line l_∞ is counterclockwise. Note that there is a natural isomorphism

$$\begin{aligned}\mathcal{H} &:= H_1(\mathbb{PR}^2 \smallsetminus \{c_1, c_2, c_3, c_4\}, \mathbb{F}_2) \\ &\cong \mathbb{F}_2[l_\infty] \oplus \mathbb{F}_2[C_1, C_2, C_3, C_4]/\mathbb{F}_2.\end{aligned}$$

Since the bitangents are lines, the classes of the bitangents in $\mathcal{H}$ have nontrivial l_∞ coordinate. In fact, a much stronger result holds:

Theorem 5.1. *For any $i \in \{1, \dots, 4\}$ there is a Steiner system Σ_i such that the bitangents in Σ_i have exactly four representatives in each of the following homology classes in $\mathcal{H}$:*

$$l_\infty + C_i, \quad l_\infty + C_i + C_{i+1 \,(\mathrm{mod}\, 4)}, \quad l_\infty + C_{i-1 \,(\mathrm{mod}\, 4)}.$$

Proof: All additions of indices in the proof are modulo 4. For any $i < j$ consider a one-parameter degeneration of the curve C to a curve $\overline{C}_{ij}$ such that on $\overline{C}_{ij}$, the ovals C_i, C_{i-1} are connected with a node, and the ovals C_j, C_{j-1} are connected with a node; see Figure 5.

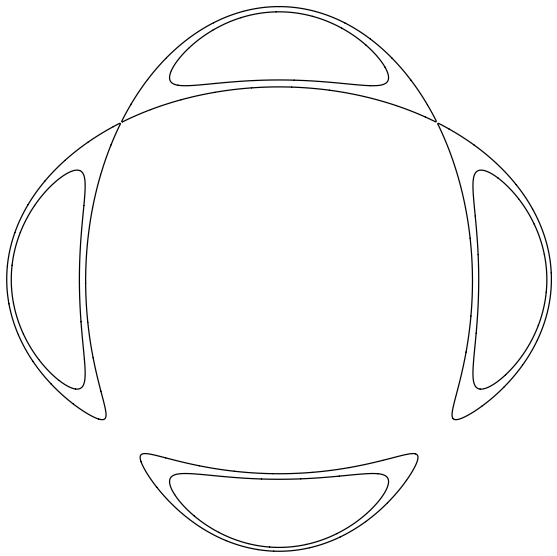


FIGURE 5. The geometry of Theorem 5.1.

By [Beauville 77], the degeneration of each of the two nodes degenerates a 2-torsion point in the Jacobian variety $\mathrm{Jac}(C)$; we mark these points by γ_i, γ_j. Under the degeneration from C to $\overline{C}_{ij}$, any of the six pairs of bitangents in the Steiner system Σ_{γ_i} degenerates to one double line through the node corresponding to γ_i; the same property holds also for j. Moreover, the intersection of the Steiner systems $\Sigma_{\gamma_i} \cap \Sigma_{\gamma_j}$ is then the quadruple line through the two nodes of $\overline{C}_{ij}$.

Thus by Proposition 2.2, the Weil pairing $\langle \gamma_i, \gamma_j \rangle$ is 0, and all the bitangents in $\Gamma_{\gamma_i \oplus \gamma_j}$ have the same homology class in $\mathcal{H}$: if $j = i + 1$, this class is $l_\infty + C_i$, and if $j = i + 2$, this class is $l_\infty + C_i + C_{i+1}$. □

Note that for any i there is a bitangent to the pair of components C_i, C_{i+1} in the homology class of l_∞. Thus the 24 bitangents from Theorem 5.1 together with these 4 bitangents exhaust the list of 28 bitangents of C. By Proposition 2.2 we have also identified a distinguished flag given by the following partition data:

- four bitangents in the class of l_∞;
- four bitangents in each of the classes $l_\infty, l_\infty + C_1 + C_3, l_\infty + C_2 + C_4$; by the combinatorial structure we described and by Proposition 2.2, this is a Steiner system;
- four bitangents in each of the classes in $\mathcal{H}$ with nontrivial line coordinate except the class $l_\infty + C_1 + C_3$.

Finally, recall (see [Huisman 02]) that since C is an M-curve, the variety $\mathrm{Jac}_{\mathbb{R}}(C)_0$ is naturally isomorphic to a product of any three (= genus(C)) of the components. Since the group $\mathrm{Jac}_{\mathbb{R}}(C)_0[2]$ is spanned by any two subgroups of order 4 in it, and since four of the order-4 subgroups we built above sit in the product of three components of the curve, the maximal group in the flag we built is $\mathrm{Jac}_{\mathbb{R}}(C)_0[2]$. Note that the quotient $\mathrm{Jac}_{\mathbb{R}}(C)/L_3$ is the Jacobian of an M-curve if and only if this quotient has 2^3 components, which means that $L_3 = \mathrm{Jac}_{\mathbb{R}}(C)_0[2]$. Thus the choice of a distinguished L_3 we made above is indeed the unique choice that will enable iteration.

Proposition 5.2. *Denote by C' the M-curve whose Jacobian is $\mathrm{Jac}(C)/L_3$, where L_3 is chosen following Theorem 5.1; denote by C'_i the components of C'. Then $H_1(\mathrm{Jac}(C)^0_{\mathbb{R}}, \mathbb{Z})$ (respectively $H_1(\mathrm{Jac}(C')^0_{\mathbb{R}}, \mathbb{Z})$) is generated by the C_i's (respectively C'_i's). Moreover, the morphism $H_1(\mathrm{Jac}(C)^0_{\mathbb{R}}, \mathbb{Z}) \to H_1(\mathrm{Jac}(C')^0_{\mathbb{R}}, \mathbb{Z})$ induced from the construction is a composition of two maps: multiplication by 2, and an isomorphism that sends each of the C_i's to one of the C'_j's.*

Proof: We start by proving that the deck group of the space of M-curves of genus 3 plus a choice of a component covering the space of M-curves is either the alternating group A_4 or the symmetric group S_4. To prove this claim we consider a moduli point with many automorphisms: the action of the automorphism group of

$$\{(x : y : z :) | (x^2 - z^2) + (y^2 - z^2) = \epsilon\}$$

on the components is via the A_4 action of projective automorphisms.

Using [Huisman 02] we have

$$H_1(\mathrm{Jac}(C)^0_{\mathbb{R}}) \cong \mathbb{Z}[C_1, C_2, C_3].$$

Applying the monodromy argument to the scenario above, we have $\sum C_i = 0$ in $H_1(\mathrm{Jac}(C)^0_{\mathbb{R}})$. Thus we can make the natural identifications

$$H_1(\mathrm{Jac}(C)^0_{\mathbb{R}}, \mathbb{Z}) \cong \mathbb{Z}[C_1, C_2, C_3, C_4] / \sum C_i,$$
$$H_1(\mathrm{Jac}(C')^0_{\mathbb{R}}, \mathbb{Z}) \cong \mathbb{Z}[C'_1, C'_2, C'_3, C'_4] / \sum C'_i.$$

Note that the map $\mathrm{Jac}(C)^0_{\mathbb{R}} \to \mathrm{Jac}(C')^0_{\mathbb{R}}$ is a covering map whose kernel is isomorphic to $\mathbb{F}_2^3$. Since the first homotopy group and the first homology groups of tori are naturally isomorphic, and since the rank of the homotopy groups in our case is 3, it follows that the induced map on the homology groups is indeed a composition of

multiplication by 2 and some isomorphism I. To find the isomorphism I we apply the monodromy argument from above again: the isomorphism I is given by a matrix in $\mathrm{SL}(\mathbb{Z}^4)$ whose class in $\mathrm{SL}(\mathrm{coker}(\mathbb{Z}^4 \overset{x\mapsto\|x\|_1}{\longrightarrow} \mathbb{Z}))$ is invariant under the action of A_4 on $\mathbb{Z}^4$. However, the only class of this type is the identity class. □

To complete the description of an iterative algorithm, we have to solve two problems: initiating the algorithm and performing an iterative step. In the discussion of these problems we will apply several times the following proposition.

Proposition 5.3. *The symplectic-algebraic properties of a configuration of bitangents to a real M-curve of genus 3 as points on the odd part of an affine symplectic space are determined by the homotopy classes of the bitangents in $\mathbb{PR}^2 \smallsetminus \{c_i\}_{i=2}^4$ and the intersection pattern of the bitangents with the components of C.*

Proof: This follows from the following facts:

- Bitangents are continuous on families. Thus, the homology classes of bitangents in $\mathbb{RP}^2 \smallsetminus \{c_i\}_1^4$ is constant on families.
- Level structure is continuous on families.
- The moduli space of M-curves is irreducible.

□

We will apply Proposition 5.3 several times to study the configuration of bitangents arising from the discussion following Corollary 4.11. We will describe real algebrogeometric data on the moduli of configurations of bitangents that defines several nonzero real algebraic functions. To show that some real configuration is associated with a distinguished flag (in the sense of Theorem 5.1) we will present one curve for which our function is positive on the distinguished configuration and negative on the others. The conceptual calculations appear below. The related numeric calculations appear in [Lehavi and Ritzenthaler 06].

Initiating the algorithm: To initiate the algorithm one essentially has to solve, in a Galois theory sense, the bitangents of the curve C. Since the Galois group acting on the bitangents is generically unsolvable, this problem is generically unsolvable in radicals.

However, there are still other computationally useful problems that we will answer: Determine whether on a given M-curve of genus 3 and quadrics A_1, A_2, A_3, the flag $L_1 \subset L_2$ induced from A_1, A_2, A_3 is a subflag of a distinguished flag (in the sense of Theorem 5.1). To check this, it suffices to verify that the curve C lies in one component of $\mathbb{PR}^2 \smallsetminus \mathrm{Nulls}(A_1A_2)$. It suffices to check this on an infinitesimal neighborhood of the four bitangents determined by the conics A_1, A_2.

Given an M-curve C in the form $A_1A_2 - A_3^2$ such that the induced flag is a subflag of a distinguished flag, mark the choice of the distinguished group L_3. Note that the quartic form $(x^2 - z^2)(y^2 - z^2)$ separates the real projective plane into three positive components and four negative components. Thus, if the form A_3', calculated as in Theorem 4.9, is purely imaginary, then the curve C' is an M-curve, and thus the choice of L_3 is the distinguished choice. Note also that A_3' is purely imaginary if and only if the expression under the square root in Theorem 4.9 is negative. By Proposition 5.3, it suffices to show one example of a curve C with purely imaginary A_3'. We do this in [Lehavi and Ritzenthaler 06].

Describing the iterative step: Recall that during the calculation of the iterative step in the discussion following Corollary 4.11, the field extensions were geometrically described by several times making choices of the following type: given three lines l_1, l_2, l_3 and two pairs of points $p_{i1}, p_{i2} \in l_i \smallsetminus (l_i \cap (l_{3-i} \cup l_3))$, find a partition into two pairs of the four points $p_{11}, p_{12}, p_{21}, p_{22}$ that is not the one arising from the lines l_1, l_2.

This choice boils down to a positivity question: we consider the pencil of conics throughput the four points $p_{11}, p_{12}, p_{21}, p_{22}$. There are three singular conics in this pencil, one of which is given by $l_1 \cup l_2$. Moreover, $l_1 \cup l_2$ cuts $\mathbb{PR}^2$ into two components, and the two nodes of the two other singular conics in the pencil, which are $\overline{p_{11}p_{21}} \cup \overline{p_{22}p_{12}}, \overline{p_{11}p_{22}} \cup \overline{p_{12}p_{21}}$, appear one in each of the two components of $\mathbb{PR}^2 \smallsetminus (l_1 \cup l_2)$.

We calculate the choices that bring us to a distinguished configuration on C' (in the sense of Theorem 5.1 in [Lehavi and Ritzenthaler 06]). We plot in Figure 6 one step of the computation: finding the distinguished topological configuration of $\Gamma_{L_1' \oplus \tilde{L}_1}$ (see the discussion following Corollary 4.11). The set $\Gamma_{L_2'}$ is plotted in dashed lines, and the set $\Gamma_{\tilde{L}_1 \oplus L_1'}$ is plotted in dotted lines.

We conclude this section with a description of the integration algorithm. By Proposition 5.2 (and the previous sections in which we established the isomorphism of the canonical linear systems) we know how to express C' and the differentials on it in terms of C and the differentials on it; and we know how to express the integrals of differentials on C on the C_i's in terms of integrals of differentials on C' on the C_i''s.

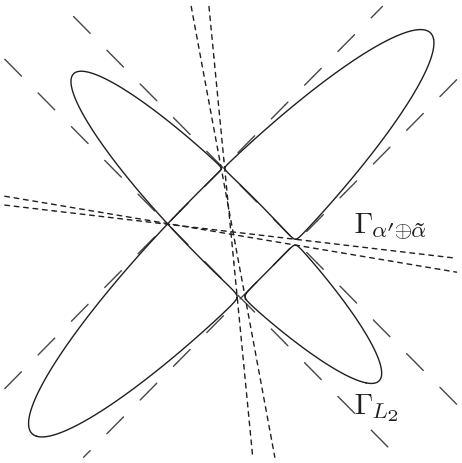


FIGURE 6. Preparing the data for the second iteration.

Let us consider now the period matrices of the curves in the iterations of the algorithm. In each iteration we divide the period matrix by 2. Since the bitangents are gradients of the theta functions (with characteristics) in these period matrices, and since theta functions are exponential in the period matrix of C, the distances between the bitangents in each of the distinguished 4-tuples are decreasing exponentially. That is, the limit curve of this process is a union of four lines in $\mathbb{PR}^2$, and the convergence rate of the curves to the configuration of four lines is exponential. Using this method and Corollary 4.11 we reduced the calculation of integrals of cycles on $\mathrm{Jac}_{\mathbb{R}}(C)$ to a calculation of integrals of rational functions on line segments.

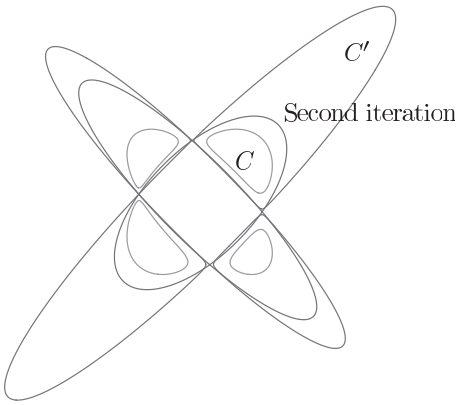


FIGURE 7. Two iterations.

In Figure 7, which is computed in the final step of [Lehavi and Ritzenthaler 06], we plot two iterations of our algorithm, where the canonical classes of the curves C, C' and the next curve in the iterative process are identified.

From a numerical-analytic point of view there is an obstacle that we did not tackle in this paper: the stability of the solution. From a theta-function-theoretic point of view it is the stability, in the sense of singular values decomposition, of the period matrix of C. From an algebraic point of view it is the stability of the formulas developed in Section 4.

ACKNOWLEDGMENTS

Sections 2 and 3 of this paper were part of the first author's Ph.D. thesis, written under the supervision of R. Livné, who suggested the series of questions above. I. Dolgachev kindly gave the first author an early copy of his preprint [Dolgachev 07] and introduced him to the works of A. Coble.

D. Lehavi was partially supported by Israel–US BSF grant 1998265. C. Ritzenthaler acknowledges the financial support provided through the European Community's Human Potential Programme under contract HPRN-CT-2000-00114, GTEM.

REFERENCES

[Beauville 77] A. Beauville. "Prym Varieties and the Schottky Problem." *Invent. Math.* 41 (1977), 149–196.

[Borwein and Borwein 88] J. M. Borwein and P. B. Borwein. *Pi and the AGM: A Study in Analytic Number Theory and Computational Complexity*. New York: John Wiley and Sons, 1988.

[Bost and Mestre 88] J.-B. Bost and J.-F. Mestre. "Moyenne Arithmetico-geometrique et Périodes des Courbes de genere 1 et 2." *Gaz. Math.* 38 (1988), 36–64.

[Coble 61] A. Coble. *Algebraic Geometry and Theta Functions*, revised printing, American Mathematical Society Colloquium Publication, X. Providence: American Mathematical Society, 1961.

[Cox 84] D. A. Cox. "The Arithmetic–Geometric Mean of Gauss." *Enseign. Math. (2)* 30 (1984), 275–330.

[Dolgachev 07] I. Dolgachev. "Topics in Classical Algebraic Geometry." Manuscript, 2007.

[Donagi 92] R. Donagi. "The Fibers of the Prym Map." In *Curves, Jacobians, and Abelian Varieties (Amherst, MA, 1990)*, pp. 55–125, Contemp. Math. 136. Providence: Amer. Math. Soc., 1992.

[Donagi and Livné 99] 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), 323–339.

[Gross and Harris 81] B. Gross and J. Harris. "Real Algebraic Curves." *Ann. Sci. École Norm. Sup. (4)* 14 (1981), 157–182.

[Harris 79] J. Harris. "Galois Groups of Enumerative Problems." *Duke Math. J.* 46 (1979), 685–724.

[Hartshorne 77] R. Hartshorne. *Algebraic Geometry*, GTM 52. New York: Springer-Verlag, 1977.

[Huisman 02] J. Huisman. "A Group Law on Smooth Real Quartics Having at Least 3 Real Branches." *J. Théor. Nombres Bordeaux* 14 (2002), 249–256.

[Humbert 01] G. Humbert. "Sur la transformation ordinaire des fonctions abeliennes." *J. de math. (5)* 7 (1901), 359–417.

[Jordan 70] M. C. Jordan. *Traité des substitutions et des équations algébriques*. Paris: Gauthier-Villars, 1870.

[Lehavi 05] D. Lehavi. "A Smooth Plane Quartic Can Be Reconstructed from Its Bitangents." *Isr. J. Math.* 146 (2005), 371–379.

[Lehavi and Ritzenthaler 06] D. Lehavi and C. Ritzenthaler. "A Proof of the Arithmetic Geometric Mean Formula in Genus 3: A Computer Program." Available online (http://www.math.princeton.edu/~dlehavi), 2006.

[Lercier and Lubicz 03] R. Lercier and D. Lubicz. "Counting Points on Elliptic Curves over Finite Fields of Small Characteristic in Quasi Quadratic Time." In *Advances in Cryptology—EUROCRPYT 2003: International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4–8, 2003*, pp. 360–373, Lecture Notes in Computer Science 2656. Berlin: Springer, 2003.

[Mestre 00] J.-F. Mestre. "Lettre adressée à Gaudry et Harley, Décembre 2000." Available online (http://www.math.jussieu.fr/~mestre/), 2000.

[Pantazis 86] S. Pantazis. "Prym Varieties and the Geodesic Flow on SO(n)." *Math. Ann.* 273 (1986), 297–315.

[Recillas 74] S. Recillas. "Jacobians of Curves with g_4^1's Are the Pryms of Trigonal Curves." *Bol. Soc. Mat. Mexicana (2)* 19 (1974), 9–13.

[Richelot 37] F. Richelot. "De transformatione integralium Abelianorum primi ordinis comentatio." *J. Reine Angew. Math.* 16 (1837), 221–341.

[Ritzenthaler 03] C. Ritzenthaler. "Problèmes arithmétiques relatifs à certaines familles de courbes sur les corps nis." Thèse de Doctorat, Université Paris 7, 2003.

[Salmon 79] G. Salmon. *A Treatise on the Higher Plane Curves*, Third edition. New York: Chelsea, 1879.

D. Lehavi, Correlix Ltd., 6 Galgaley Haplada Street, POB 12607, Herzelia Pituah, Isreal 46733
(dlehavi@gmail.com)

C. Ritzenthaler, Institut de Mathématiques de Luminy, 163 Avenue de Luminy, Case 907, 13288 Marseille, France
(ritzenth@iml.univ-mrs.fr)

Received March 10, 2004; accepted in revised form August 9, 2006.