Compositio Math. 144 (2008) 317–338
doi:10.1112/S0010437X07003314

The arithmetic of Prym varieties in genus 3

Nils Bruin

Abstract

Given a curve of genus 3 with an unramified double cover, we give an explicit description of the associated Prym variety. We also describe how an unramified double cover of a non-hyperelliptic genus 3 curve can be mapped into the Jacobian of a curve of genus 2 over its field of definition and how this can be used to perform Chabauty- and Brauer–Manin-type calculations for curves of genus 5 with an fixed-point-free involution. As an application, we determine the rational points on a smooth plane quartic and give examples of curves of genus 3 and 5 violating the Hasse principle. The methods are, in principle, applicable to any genus 3 curve with a double cover. We also show how these constructions can be used to design smooth plane quartics with specific arithmetic properties. As an example, we give a smooth plane quartic with all 28 bitangents defined over $\mathbb{Q}(t)$. By specialization, this also gives examples over $\mathbb{Q}$.

1. Introduction

In this article, we investigate the arithmetic of unramified double covers of non-hyperelliptic curves of genus 3. This research is inspired by the recent success in applying the theory of unramified double covers of hyperelliptic curves to the problem of determining the set of rational points on such curves [Bru02, Bru03, BF05, Wet97]. Combined with explicit Chabauty methods, this has yielded very practical methods for obtaining often sharp bounds on the number of rational points on a hyperelliptic curve. In the hyperelliptic case, the construction of unramified covers is particularly easy to make explicit using Kummer theory. There has been some limited work investigating how these ideas may be generalized to unramified covers of higher degree of hyperelliptic curves [BF03].

In this article, we generalize in a different direction. We derive the general form of a curve C of genus 3 over a field K of characteristic zero that allows an unramified double cover $\pi : D \to C$ defined over K. A non-hyperelliptic curve of genus 3 with an unramified double cover allows a smooth plane projective model of the form

$$C : Q_1(u,v,w)Q_3(u,v,w) = Q_2(u,v,w)^2,$$

where $Q_1, Q_2, Q_3 \in K[u,v,w]$ are quadratic forms, such that the unramified double cover of C has a canonical model in $\mathbb{P}^4$ of the form

$$D : \begin{cases} Q_1(u,v,w) = r^2, \\ Q_2(u,v,w) = rs, \\ Q_3(u,v,w) = s^2. \end{cases}$$

Received 2 June 2006, accepted in final form 16 July 2007, published online 14 March 2008.
2000 Mathematics Subject Classification 11G30 (primary), 14H40 (secondary).
Keywords: Prym varieties, Chabauty methods, rational points on curves, covering techniques, Brauer–Manin, smooth plane quartics.
The research in this paper is partially supported by NSERC.

We also describe how the associated Prym variety (the connected component of the kernel of $\pi_* : \mathrm{Jac}(D) \to \mathrm{Jac}(C)$ that contains the origin O of $\mathrm{Jac}(D)$) can be described explicitly as $\mathrm{Jac}(F)$ of some genus 2 curve F over K:

$$F : y^2 = -\det(M_1 + 2xM_2 + x^2M_3),$$

where M_i is the symmetric 3×3 matrix such that

$$(u, v, w)M_i \begin{pmatrix} u \\ v \\ w \end{pmatrix} = Q_i(u, v, w).$$

Combined with earlier work, this gives a complete description of how principally polarized Abelian surfaces arise as Prym varieties in genus 3 over base fields of characteristic zero which are not necessarily algebraically closed (see Theorem 5.1).

The description of $\mathrm{Prym}(D/C)$ as $\mathrm{Jac}(F)$ over $\mathbb{C}$ can already be found in [ACGH85, Exercise VI.F]. For arithmetic applications, we need the result in a more general setting. If C has a rational point, then the *trigonal construction* gives a Galois-theoretic way of describing the Prym variety as the Jacobian of some curve (see [Don92] and [Rec74]). Here, we refine the description to arbitrary characteristic zero base fields. The results should generalize to base fields of arbitrary odd characteristic.

We show how D can be mapped into $\mathrm{Prym}(D/C)$ over K, without an explicit rational degree one divisor class on D (see Proposition 6.2). We can thus use Chabauty-like methods on genus 5 curves in Abelian surfaces to obtain what is, in practice, often a sharp bound on the number of rational points on D. This can, in turn, be used to obtain a corresponding bound on the number of rational points on C. As an example, we prove the following.

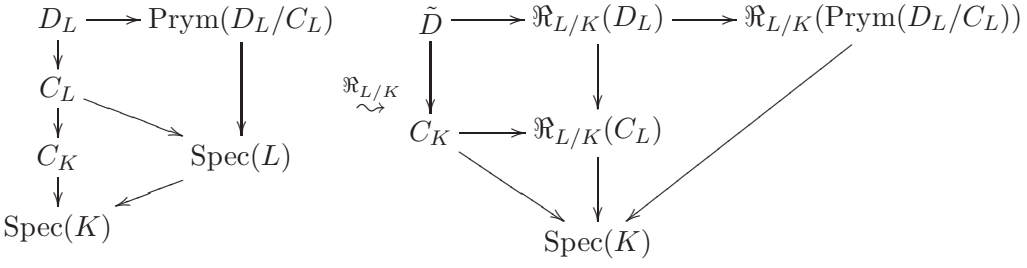
Proposition 1.1. *For the curve*

$$C : (4u^2 - 4vw + 4w^2)(2u^2 + 4uv + 4v^2) = (2u^2 + 2uw - 4vw + 2w^2)^2$$

we have $C(\mathbb{Q}) = \{(0 : 1 : 0)\}$.

The proof avoids computing the Mordell–Weil group of $\mathrm{Jac}(C)$. Instead, it uses the computationally more accessible Mordell–Weil group of the associated Prym variety, which is an Abelian surface.

Remark 1.2. The method does not put restrictions on the geometry of C. Indeed, let L be a field extension of K such that the group scheme $\mathrm{Jac}(C)[2]$ has a non-trivial rational point. Let $d = [L : K]$. We can use the construction above to obtain an unramified double cover D_L/C_L and a corresponding map $D_L \to \mathrm{Prym}(D_L/C_L)$. In complete analogy to the treatment of genus 2 in [Bru03], we take Weil restrictions and obtain a finite étale cover of dimension d varieties $\Re_{L/K}(D_L) \to \Re_{L/K}(C_L)$ and a map $\Re_{L/K}(D_L) \to \Re_{L/K}(\mathrm{Prym}(D_L/C_L))$. Inside $\Re_{L/K}(C_L)$ we have $C = C_K$ and we can take its preimage $\tilde{D} \subset \Re_{L/K}(D_L)$. This will give a degree 2^d unramified cover of C, which could consist of multiple components, depending on the linear dependencies between the L/K-conjugates of the 2-torsion point in $\mathrm{Jac}(C)[2]$ corresponding to D_L/C_L.



https://doi.org/10.1112/S0010437X07003314

In any case, we end up with an unramified cover $\tilde{D}/C$ over K that maps non-trivially into an Abelian variety of dimension $2d$, which has a Mordell–Weil group that is computationally relatively accessible, because it is isomorphic to $\mathrm{Prym}(D_L/C_L)(L)$. We can then apply Chabauty-like methods to determine $\tilde{D}(K)$ and $C(K)$. The group $\Re_{L/K}(\mathrm{Prym}(D/C_L))(K) \simeq \mathrm{Prym}(D/C_L)(L)$ would be the hardest ingredient to obtain and it should be noted that the computations involved would probably be prohibitive, except for very low degree L.

Since the mapping of D into $\mathrm{Prym}(D/C)$ does not require a rational point on D, we can apply this construction to prove in examples that $D(\mathbb{Q})$ is empty, even if D does have points everywhere locally. In our computations, we show in certain examples that the image of $D(\mathbb{A}_\mathbb{Q})$ in $\mathrm{Prym}(D/C)(\mathbb{A}_\mathbb{Q})$ misses the closure of $\mathrm{Prym}(D/C)(\mathbb{Q})$ by combining the local information at a finite number of primes.

It is reassuring that, at least conjecturally, our computations correspond to determining part of the Brauer–Manin obstruction of D. By this we mean that if the argument above succeeds in showing that D has no rational points, then subject to standard conjectures, there is a Brauer–Manin obstruction to having rational points, i.e. $D(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}}$ is empty. The explanation below is of no relevance for the rest of this paper, but may be of interest to experts.

Suppose that D is a curve of genus at least 2, defined over a number field K, with points everywhere locally. Since D is naturally a subvariety of $\underline{\mathrm{Pic}^1}(D)$, the scheme representing the functor $X \mapsto \mathrm{Pic}^1(D/X)$, it follows that $\underline{\mathrm{Pic}^1}(D)$ has points everywhere locally as well. Since $\underline{\mathrm{Pic}^1}(D)$ is a torsor under $\mathrm{Jac}(D)$, it follows that $\underline{\mathrm{Pic}^1}$ represents an element of $Ш(\mathrm{Jac}(D)/K) \subset H^1(K, \mathrm{Jac}(D))$. Manin has proved (see [Sko01, Theorem 6.2.3]) that if $Ш(\mathrm{Jac}(D)/K)$ is finite, then the failure of any $X \in Ш(\mathrm{Jac}(D)/K)$ to have points globally, can be explained by the Brauer–Manin obstruction.

If $\underline{\mathrm{Pic}^1}(D)$ does have a rational point then it is isomorphic to $\mathrm{Jac}(D)$ and hence D can be considered as a subvariety of $\mathrm{Jac}(D)$ (via the Abel–Jacobi map). In this case, Scharaschkin [Sch99] proves that if $Ш(\mathrm{Jac}(D)/K)$ has trivial divisible subgroup, then $D(\mathbb{A}_K)^{\mathrm{Br}}_\bullet$ is a subset of $D(\mathbb{A}_K)_\bullet \cap \overline{\mathrm{Jac}(D)(K)}_\bullet$. Here, the $\bullet$ symbol means taking the quotient by the connected component. This only makes a difference at the archimedean components of adelic point sets.

If D does have a degree one divisor, then our map $2(\iota_* - \mathrm{id}_*) : D \to \mathrm{Prym}(D/C)$ differs by a translation over a rational point of $\mathrm{Prym}(D/C)$ from twice the map obtained via the obvious projection $J(D) \to \mathrm{Prym}(D/C)$. Hence, if $2(\iota_* - \mathrm{id}_*)D(\mathbb{A}_K)_\bullet \cap \overline{\mathrm{Prym}(D/C)(\mathbb{Q})}_\bullet$ is empty, then so is $D(\mathbb{A}_K)_\bullet \cap \overline{\mathrm{Jac}(D)(K)}_\bullet$ and, therefore, D conjecturally has a non-trivial Brauer–Manin obstruction to having rational points.

Proposition 1.3. *The genus* 5 *curve*

$$D : \begin{cases} (v^2 + vw - w^2) = r^2 \\ (u^2 - v^2 - w^2) = rs \\ (uv + w^2) = s^2 \end{cases}$$

and the genus 3 *curve*

$$C : (v^2 + vw - w^2)(uv + w^2) = (u^2 - v^2 - w^2)^2$$

over $\mathbb{Q}$ *both have points everywhere locally, but they have no rational points.*

For this example, we find $\mathrm{Prym}(D/C)(\mathbb{Q}) \simeq \mathbb{Z} \times \mathbb{Z}$. This illustrates that the method used is not a special case of a Chabauty-type argument.

Also note that while, at least conjecturally, the curve D in Proposition 1.3 has a non-trivial Brauer–Manin obstruction to having points, the same does not immediately follow for C. Hence, the proof of Proposition 1.3 does not suggest that $C(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}}$ is empty, although undoubtedly it is.

https://doi.org/10.1112/S0010437X07003314

In addition, we investigate the arithmetic implications of the geometric description of the fibres of the Prym map between moduli spaces, corresponding to the functor Prym : $\{\pi : D \to C\} \mapsto \{\mathrm{Prym}(D/C)\}$, given in [Ver87]. For a general principally polarized Abelian surface A we denote the standard map $\mathbb{Z} \to \mathrm{End}(A)$ by $n \mapsto [n]$. Kummer surface $\mathcal{K} = A/\langle[-1]\rangle$ has a singular quartic model in $\mathbb{P}^3$, with a singular locus consisting of 16 points, corresponding to $A[2]$. Translation by $A[2]$ induces automorphisms on $\mathcal{K}$, given by linear transformations on $\mathbb{P}^3$. We write $\widehat{\mathbb{P}}^3$ for the space of planes in $\mathbb{P}^3$. Verra [Ver87] shows that over $\mathbb{C}$, the fibre of Prym over a principally polarized surface A is birational to $\widehat{\mathbb{P}}^3/A[2]$. In fact, he gives a very precise description of the fibre as a blow-up of this space, where the exceptional components contain the moduli points corresponding to hyperelliptic or degenerate curves C.

In particular, a non-hyperelliptic genus 3 curve C over $\mathbb{C}$ which has a double cover D such that $\mathrm{Prym}(D/C) = A$ can be obtained as a plane section of $\mathcal{K}$, with D the pull-back of C to A. Any two such plane sections of $\mathcal{K}$ in the same $A[2]$-orbit give isomorphic covers D/C.

In this article we explain how, given a genus 2 curve F over a number field K and a genus 3 plane section C of $\mathcal{K} = \mathrm{Jac}(F)/\langle\pm 1\rangle$, we can obtain a model for C of the type $Q_1Q_3 = (Q_2)^2$. Since a sufficiently general plane section of $\mathcal{K}$ is non-singular and thus of genus 3, it shows that any Jacobian of a genus 2 curve over K can be realized as a Prym variety of a non-hyperelliptic genus 3 curve *over* K. In fact, this particular construction certainly works over any odd characteristic base field with sufficiently many elements. We can phrase this in entirely elementary terms as follows.

Proposition 1.4. *Let k be an infinite field of odd characteristic and let $f \in k[x]$ be a square-free polynomial of degree 5 or 6. Then there exist symmetric matrices $M_1, M_2, M_3 \in \mathbb{Q}^{3\times 3}$ such that*

$$f = \det(M_1 + xM_2 + x^2M_3).$$

We use this construction to obtain a systematic way of constructing curves of genus 3 with all 28 bitangents defined over a non-algebraically closed field, for instance $\mathbb{Q}(t)$ (see § 7). By specialization of t, this gives infinitely many examples of curves over $\mathbb{Q}$ with rational bitangents. This strengthens a result in [Edg94], where an example is given with all bitangents defined over $\mathbb{R}$. See [Sch98] or [Cay79] for an approach via interpolation.

Finally, it should be noted that not all covers $\pi : D \to C$ defined over K with $\mathrm{Prym}(D/C) = A$ and C non-hyperelliptic, have C occurring as a plane section of the associated Kummer surface $\mathcal{K}$ defined over K, since not all rational points of $\widehat{\mathbb{P}}^3/A[2]$ are covered by rational points of $\widehat{\mathbb{P}}^3$. This follows, for instance, from the fact that this does not even hold for the quotient by one 2-torsion point, i.e.

$$\mathbb{P}^3 \Big/ \left\langle \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \right\rangle$$

has rational points that do not lift to $\mathbb{P}^3$.

2. Preliminaries

First we fix some notation. Let K be a field and let C be a complete, absolutely irreducible algebraic curve over K. We write κ_C for a canonical divisor on C over K. For a divisor $\mathfrak{D} \in \mathrm{Div}(C)$, we write $[\mathfrak{D}]$ for its class in $\mathrm{Pic}(C)$ and $|\mathfrak{D}|$ for the complete linear system corresponding to $\mathfrak{D}$ and $l(\mathfrak{D}) = \dim|\mathfrak{D}|$. We say that a divisor $\mathfrak{D}$ on C is a g^r_d if $\deg(\mathfrak{D}) = d$ and $l(\mathfrak{D}) > r$. We write $W^r_d \subset \mathrm{Pic}^d(C)$ for the classes of all such g^r_d. By abuse of notation, we also write W^r_d for the corresponding subscheme of the scheme representing the functor $\mathrm{Pic}^d(C)$.

https://doi.org/10.1112/S0010437X07003314

2.1 Unramified double covers and Prym varieties

Let $\pi : D \to C$ be an unramified finite morphism of degree two between curves over a field K and let $\iota : D \to D$ be the non-trivial involution of D over C. It follows by the Riemann–Hurwitz theorem that $g(C) > 0$ and that

$$g(D) = 2g(C) - 1.$$

The kernel of $\pi_* : \mathrm{Jac}(D) \to \mathrm{Jac}(C)$ has two connected components. The component that contains 0 coincides with the image of $(\mathrm{id}_* - \iota_*) : \mathrm{Jac}(D) \to \mathrm{Jac}(D)$.

Definition 2.1. Let $\pi : D \to C$ be an unramified finite morphism of degree two between curves over a field K. We write $\mathrm{Prym}(\pi) = \mathrm{Prym}(D/C)$ for the connected component of the identity-element of $\ker(\pi_* : \mathrm{Jac}(D) \to \mathrm{Jac}(C))$. We call this the *Prym variety* of D/C.

Thus, $\mathrm{Prym}(D/C)$ is an Abelian subvariety of $\mathrm{Jac}(D)$. The principal polarization on $\mathrm{Jac}(D)$ restricts to a principal polarization on $\mathrm{Prym}(D/C)$. Historically, Prym varieties were considered interesting primarily because they give examples of principally polarized Abelian varieties that are not Jacobian varieties. However, if $\dim(\mathrm{Prym}(D/C)) \leqslant 2$, then $\mathrm{Prym}(D/C)$ generally is a Jacobian variety.[1] See [ACGH85, VI-C] or [Mum74] for details.

2.2 Prym varieties in the hyperelliptic case

In contrast to the general situation, the Prym variety associated to an unramified double cover of a hyperelliptic curve is closely related to a Jacobian variety. In fact, the Prym variety is isomorphic to the product of Jacobian varieties of subcovers, which themselves are again hyperelliptic.

Let us first assume that C is a double cover of a $\mathbb{P}^1$ defined over a field K of odd characteristic. Then C has an affine model of the form

$$C : y^2 = f(x)$$

where $f \in K[x]$ is a square-free polynomial of degree $2g(C)+2$. Kummer theory tells us exactly what the unramified degree two extensions of $K(C)$ are. For any factorization $f = f_1 f_2$, with $f_1, f_2 \in K[x]$ and of even degree, we have a curve D given by the affine model

$$\begin{cases} y_1^2 = f_1(x) \\ y_2^2 = f_2(x) \end{cases}$$

and an unramified morphism of degree two:

$$\begin{array}{ccccc} \pi & : & D & \to & C \\ & & (x, y_1, y_2) & \mapsto & (x, y_1 y_2) \quad = (x, y). \end{array}$$

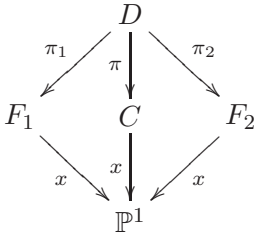
Then there are the two obvious curves

$$F_1 : y_1^2 = f_1(x)$$
$$F_2 : y_2^2 = f_2(x)$$

[1] It can also be the product of two elliptic curves, in which case it is a Jacobian of a reducible curve.

https://doi.org/10.1112/S0010437X07003314

with the obvious projections $\pi_1 : D \to F_1$ and $\pi_2 : D \to F_2$. This yields the familiar diagram associated to biquadratic extensions.



In addition, if f_1, f_2 are quadratic conjugate over some quadratic extension L over K then this construction will also yield an unramified double cover D over C, defined over K, because the construction of D is symmetric in F_1, F_2.

Proposition 2.2. *Let $C, D, F_1, F_2, \pi, \pi_1, \pi_2$ be defined as above. Then*

$$\pi_1^* + \pi_2^* : \mathrm{Jac}(F_1) \times \mathrm{Jac}(F_2) \to \mathrm{Prym}(D/C)$$

is an isomorphism of Abelian varieties.

Proof. First, we prove that π_1^* indeed maps $\mathrm{Jac}(F_1)$ into $\mathrm{Prym}(D/C)$. To that end, take the generic point $(x_1, y_1) \in F_1$. We have $\pi_1^*(x_1, y_1) = (x_1, y_1, \sqrt{f_2(x_1)}) + (x_1, y_1, -\sqrt{f_2(x_1)})$. Under π, this maps to the divisor cut out by $x = x_1$. This shows that $\pi_* \pi_1^* : \mathrm{Jac}(F_1) \to \mathrm{Jac}(C)$ is constant and, hence, $(\pi_* \pi_1^*)|_{\mathrm{Jac}(F_1)}$ is the zero map. By symmetry it follows that $\mathrm{Jac}(F_1) \times \mathrm{Jac}(F_2)$ lands in the kernel of π_* under $\pi_1^* + \pi_2^*$ and, since it is connected and covers $0 \in \mathrm{Jac}(D)$, lands in $\mathrm{Prym}(D/C)$.

The fact that $(\pi_i)_* \circ \pi_i^* = [2]$ for $i = 1, 2$ already assures that $\mathrm{Jac}(F_1) \times \mathrm{Jac}(F_2)$ is isogenous to $\mathrm{Prym}(D/C)$. A quick way to see that they are actually isomorphic is by noting that F_1 and F_2 can be arbitrary hyperelliptic curves and that, by construction, the isogeny would have to depend functorially on F_1 and F_2. In general, $\mathrm{Jac}(F_1) \times \mathrm{Jac}(F_2)$ has no non-trivial polarization-preserving isogenies and hence there are no other candidates for $\mathrm{Prym}(D/C)$. □

Remark 2.3. The result in Proposition 2.2 is easily extended to the situation where f_1, f_2 are quadratic conjugate over some quadratic extension L over K. Then, over L we still have $\mathrm{Jac}(F_1) \to \mathrm{Prym}(D/C)$ and by taking Weil restrictions we see that $\Re_{L/K}\mathrm{Jac}(F_1) = \mathrm{Prym}(D/C) = \Re_{L/K}\mathrm{Jac}(F_2)$.

Remark 2.4. In general, a hyperelliptic curve C over K is a double cover of a curve L of genus 0. We can express $K(L)$ as some quadratic extension of $K(\mathbb{P}^1)$. Relative Kummer theory allows us to describe $\mathrm{Prym}(D/C)$ in terms of Jacobians of subcovers of D/L in exactly the same way as above.

2.3 Linear subspaces on quadrics

It is well known that on a non-singular quadric in $\mathbb{P}^3$, there are two rulings of lines with the property that a line from one ruling intersects a unique line from the opposite ruling and that two lines from the same ruling do not intersect. We need a simple lemma that classifies whether the two rulings are split or quadratic conjugates.

Lemma 2.5. *Let K be a field of characteristic different from two and let $M \in K^{4\times 4}$ be a symmetric matrix describing a non-singular quadric $Q \subset \mathbb{P}^3$. The two rulings of lines on Q are individually defined over K exactly if* $\det(M)$ *is a square in K. Otherwise, they are quadratic conjugate.*

Proof. First assume we have a point $\mathbf{x}_0 \in Q(K)$. Let $V = \{\mathbf{x} : \mathbf{x}_0{}^t M \mathbf{x} = 0\}$ be the plane tangent to Q at $\mathbf{x}$. The intersection $V \cap Q$ consists of exactly two lines through $\mathbf{x}_0$, one from each of the rulings. With a change of basis, we can assume that $\mathbf{x}_0 = (1 : 0 : 0 : 0)$ and that the points $\mathbf{x}_1 = (0 : 1 : 0 : 0)$

https://doi.org/10.1112/S0010437X07003314

and $\mathbf{x}_2 = (0:0:1:0)$ lie on V as well. It follows that

$$M = \begin{pmatrix} 0 & 0 & 0 & d \\ 0 & a & b & * \\ 0 & b & c & * \\ d & * & * & * \end{pmatrix}; \quad \det(M) = d^2(b^2 - ac).$$

We see that Q intersected with the line through $\mathbf{x}_1, \mathbf{x}_2$ is described by the equation $ax_1^2 + 2bx_1x_2 + cx_2^2 = 0$, which is split exactly if $b^2 - ac$ is a square. The lemma follows.

If $Q(K)$ is empty, then we base change to $K(Q)$, where we have the generic point $(x_0 : x_1 : x_2 : x_3) \in Q(K(Q))$. Since K is algebraically closed in $K(Q)$, the pair of rulings (defined over K) is split over $K(Q)$ if and only if they are split over K. Furthermore, $\det(M)$ is a square in K if and only if it is in $K(Q)$. □

3. Non-hyperelliptic curves of genus 5 with an unramified involution

Let K be a field of characteristic zero and let D be a non-hyperelliptic curve of genus 5 with a fixed-point-free involution ι over K. Let $\pi : D \to C = D/\langle\iota\rangle$ be the quotient map by the action of ι. The Riemann–Hurwitz formula yields that C is of genus 3. Let κ_C be a canonical divisor on C and let $\langle u, v, w\rangle = |\kappa_C|$ be coordinates on the associated canonical model of C. Note that we do not insist that C is non-hyperelliptic. By abuse of notation, we also write u, v, w for the pull-backs $u \circ \pi, v \circ \pi, w \circ \pi$. We write $\kappa_D = \pi^*(\kappa_C)$, which is again canonical. There are functions r, s on D with $r + r \circ \iota = s + s \circ \iota = 0$ such that $\langle u, v, w, r, s\rangle = |\kappa_D|$.

We identify D with the canonical model associated to κ_D, being the image of $(u : v : w : r : s) : D \to \mathbb{P}^4$. In this notation,

$$\iota : (u : v : w : r : s) \mapsto (u : v : w : -r : -s).$$

We let Λ be the linear system of quadrics containing $D \subset \mathbb{P}^4$. A simple comparison of the dimensions $l(\kappa_D) = 5$ and $l(2\kappa_D) = 12$ yields that $\Lambda \simeq \mathbb{P}^2$. We let $(\lambda_1 : \lambda_2 : \lambda_3)$ be coordinates on Λ such that $Q_1, Q_2, Q_3 \in \Lambda(K)$ correspond to $(1:0:0)$, $(0:1:0)$, $(0:0:1)$, respectively.

Note that $|\kappa_D|$ has a decomposition into the $+1$-eigenspace $\langle u, v, w\rangle$ and the -1-eigenspace $\langle r, s\rangle$ of ι. The involution ι acts identically on the corresponding linear subspaces $\{r = s = 0\}, \{u = v = w = 0\} \subset \mathbb{P}^4$.

We recall that a curve is called *trigonal* if it admits a degree three map to $\mathbb{P}^1$.

LEMMA 3.1. *With the notation above, D is not a trigonal curve.*

Proof. Since a trigonal curve remains trigonal upon base extension, it suffices to prove the lemma for algebraically closed K. Suppose that D were trigonal.

We argue following [ACGH85, p. 207]. The fibers of the degree three map $D \to \mathbb{P}^1$ form a base-point-free linear system of degree three. Let $\mathfrak{D}$ be the divisor corresponding to one such fiber. Then $\mathfrak{D}$ is a g^1_3. Note that if $\mathfrak{D}$ were a g^2_3, then removing a point from $\mathfrak{D}$ would yield a g^1_2 and, hence, D would be hyperelliptic, which we assumed not to be the case. Hence, $|\mathfrak{D}| \simeq \mathbb{P}^1$.

As is argued in [ACGH85, p. 207] (using the Brill–Noether residue theorem; see, for instance, [Ful69, ch. 8]), a curve of genus 5 can have at most one divisor class of type g^1_3. Therefore, $\iota_* : \mathrm{Div}(D) \to \mathrm{Div}(D)$ induces an involution on $|\mathfrak{D}|$. Since an involution on $\mathbb{P}^1$ has two fixed points, there are two effective degree three divisors that are fixed under ι_*. It follows that ι has a fixed point on D, which contradicts our assumption. □

LEMMA 3.2. *With the notation above, $D = Q_1 \cap Q_2 \cap Q_3$. Furthermore, the Q_i can be chosen to be non-singular and D misses the singular locus of any quadric containing D.*

https://doi.org/10.1112/S0010437X07003314

Proof. First note that if the statement of the lemma is false, then it is also false over the algebraic closure of K. Therefore, it suffices to prove the lemma for algebraically closed K. By Petri's theorem [ACGH85, p. 131], a canonical model of a non-hyperelliptic, non-trigonal curve of genus 5 is the intersection of quadrics.

Next we show that a quadric $Q \in \Lambda$ cannot be singular at D. Suppose that $P_0 \in D$ is a singular point of some quadric $Q \in \Lambda$. Note that, if $\mathrm{rk}Q < 3$, then there is a $\mathbb{P}^3 \subset Q$. Since $D \subset Q$ too, we have that $D \cap \mathbb{P}^3$ is a curve. The space Λ restricted to that $\mathbb{P}^3$ would be at most a pencil of quadrics and hence contain an intersection of two quadrics. This would imply that D has a component of genus at most one, which contradicts that D is a curve of genus 5.

Hence, Q is of rank three or four, which implies that Q contains a $\mathbb{P}^1$ of planes through the singular point $P_0 \in D$. On each such plane V, the restriction of Λ is a pencil of conics and, hence, has a base locus of degree four. Since $P_0 \in V \cap D$ is contained in that base locus, this realizes D as a degree three cover of that $\mathbb{P}^1$. This contradicts that D is non-trigonal.

By Bertini's theorem [Har77, Chapter III, Remark 10.9.2] it follows that a general member of Λ is non-singular and hence we can choose the Q_i to be non-singular. □

Lemma 3.3. *With the notation above, we have that ι acts trivially on Λ. Equivalently, for $Q \in \Lambda$, we can find quadratic forms $Q^+ \in K[u,v,w]$ and $Q^- \in K[r,s]$ such that Q is given by the equation*

$$Q^+(u,v,w) + Q^-(r,s) = 0.$$

Proof. First note that ι preserves D and, hence, preserves Λ. Suppose that there is $Q \in \Lambda(\overline{K})$ such that $Q \neq \iota(Q)$. Then $Q - \iota(Q) \in \Lambda(\overline{K})$ is not zero. On the other hand, since ι acts trivially on $\{r = s = 0\}$, we have that $Q - \iota(Q)$ restricted to $\{r = s = 0\}$ is zero. Hence, Λ restricted to $\{r = s = 0\}$ is a pencil of plane conics and has a base locus of degree four. This yields four points on D that are fixed points of ι, which contradicts the assumptions.

For an equation of any quadric in $\Lambda(\overline{K})$, this means that the monomials $ur, vr, \ldots, ws$ cannot occur. □

4. Special divisor classes of degree four

As in the previous section, let D be a non-hyperelliptic curve of genus 5 over a field K of characteristic zero with an unramified involution $\iota : D \to D$. We also adopt the other notation from the previous section. We consider the scheme of special divisors

$$W_4^1(D) = \{\mathcal{D} \in \mathrm{Pic}^4(D) : l(\mathcal{D}) \geqslant 2\}.$$

From the Riemann–Roch formula it follows that the residuation map $\mathcal{D} \mapsto [\kappa_D] - \mathcal{D}$ defines an involution on W_4^1.

We denote the locus of singular quadrics in Λ by

$$\Gamma = \{Q \in \Lambda : \det(Q) = 0\}.$$

By Lemma 3.3 we have a decomposition $\Gamma = \Gamma^+ \cup \Gamma^-$, with equations

$$\Gamma^+ : \det(\lambda_1 Q_1^+ + \lambda_2 Q_2^+ + \lambda_3 Q_3^+) = 0,$$
$$\Gamma^- : \det(\lambda_1 Q_1^- + \lambda_2 Q_2^- + \lambda_3 Q_3^-) = 0.$$

From the definition it is clear that Γ is at least one-dimensional and, by Lemma 3.2, Γ is at most one-dimensional too. In fact, it is straightforward to check that

$$\Gamma' = \{Q \in \Lambda : \mathrm{rk}Q = 3\} \tag{1}$$

is zero-dimensional and is the singular locus of Γ.

https://doi.org/10.1112/S0010437X07003314

Lemma 4.1. *Let $\mathfrak{D}, \mathfrak{D}' \in \mathrm{Div}(D)$ be effective divisors of degree four with $l(\mathfrak{D}) = 2$. Then the following hold.*

(i) *There is a unique 2-plane $V_{\mathfrak{D}}$ such that $\mathfrak{D} = D \cdot V_{\mathfrak{D}}$.*
(ii) *There is a unique quadric $Q_{\mathfrak{D}} \in \Lambda$ which vanishes on $V_{\mathfrak{D}}$. In fact, $Q_{\mathfrak{D}} \in \Gamma$.*
(iii) *If $V_{\mathfrak{D}}$ and $V_{\mathfrak{D}'}$ meet in a line, then $[\mathfrak{D} + \mathfrak{D}'] = [\kappa_D]$.*
(iv) *If $Q_{\mathfrak{D}} = Q_{\mathfrak{D}'}$, then $[\mathfrak{D}' + \mathfrak{D}] = [\kappa_D]$ or $[\mathfrak{D} - \mathfrak{D}'] = 0$.*
(v) *If $Q_{\mathfrak{D}} \neq Q_{\mathfrak{D}'}$, then $[\mathfrak{D}' + \mathfrak{D}] \neq [\kappa_D]$ and $[\mathfrak{D} - \mathfrak{D}'] \neq 0$.*

Proof. (i) The geometric formulation of the Riemann–Roch theorem [ACGH85, p. 12] states that, for a divisor $P_1 + \cdots + P_r$ with $r \leqslant g$, we have

$$l(P_1 + \cdots + P_r) = r + 1 - \mathrm{rk}\langle P_1, \ldots, P_r \rangle,$$

so one can take $V_{\mathfrak{D}}$ to be the plane spanned by the support of $\mathfrak{D}$ over $\overline{K}$.

(ii) Since the restriction of Λ to $V_{\mathfrak{D}}$ has a base locus of degree four, it is a pencil of conics. Hence, there is a unique quadric $Q_{\mathfrak{D}} \in \Lambda$ that vanishes on $V_{\mathfrak{D}}$. Since a quadric in $\mathbb{P}^4$ containing a 2-plane is necessarily singular, it follows that $Q_{\mathfrak{D}} \in \Gamma$.

(iii) Two 2-planes meeting in a line lie in a 3-plane, say W. Since $\mathfrak{D} + \mathfrak{D}'$ is effective of degree eight it equals the hyperplane section $D \cdot W$. Hyperplane sections of canonical models are canonical divisors. If $\mathfrak{D}$ and $\mathfrak{D}'$ have intersecting support, then replace $\mathfrak{D}'$ by a linearly equivalent effective divisor $\mathfrak{D}''$. The divisors $\mathfrak{D}'$ and $\mathfrak{D}''$ certainly have disjoint support, since otherwise $\mathfrak{D}' - \mathfrak{D}''$ would be the divisor of a function of degree at most three, contradicting Lemma 3.1.

(iv) First suppose that $Q_{\mathfrak{D}}$ is of rank four. Then $Q_{\mathfrak{D}}$ is a cone over a non-singular quadric in $\mathbb{P}^3$. The two line rulings on that quadric give rise to two plane 'rulings' on $Q_{\mathfrak{D}}$. Planes in opposite rulings meet in a line and planes in the same ruling meet only in the singular point of $Q_{\mathfrak{D}}$. Hence, if $V_{\mathfrak{D}}$ and $V_{\mathfrak{D}'}$ belong to opposite rulings, then by part (iii) we have $[\mathfrak{D} + \mathfrak{D}'] = [\kappa_D]$. If $V_{\mathfrak{D}}$ and $V_{\mathfrak{D}'}$ belong to the same ruling, then both $\mathfrak{D}$ and $\mathfrak{D}'$ are residual to an arbitrary divisor from the opposite ruling and, hence, linearly equivalent.

If $Q_{\mathfrak{D}}$ is of rank three, then $Q_{\mathfrak{D}}$ is a cone over a singular quadric in $\mathbb{P}^3$, so there is one ruling of planes on $Q_{\mathfrak{D}}$ and any two of these meet in a line. It follows by part (iii) that $[\mathfrak{D} + \mathfrak{D}'] = [\kappa_D]$. Since this holds for any $\mathfrak{D}'$ with $Q_{\mathfrak{D}'} = Q_{\mathfrak{D}}$, it follows that $[\mathfrak{D} - \mathfrak{D}'] = 0$.

(v) Given $V_{\mathfrak{D}}$, there is a map

$$\mathbb{P}^1 \to \{\text{planes in } Q_{\mathfrak{D}}\}$$

parametrizing the ruling on $Q_{\mathfrak{D}}$ containing $V_{\mathfrak{D}}$. Each of the planes V in the image of this map cuts out an effective divisor $\mathfrak{D}'$ equivalent to $\mathfrak{D}$. By construction, $Q_{\mathfrak{D}'} = Q_{\mathfrak{D}}$. This gives an explicit realization of $\mathbb{P}^1 \simeq |\mathfrak{D}|$, so this accounts for all divisors linearly equivalent to $\mathfrak{D}$. □

Corollary 4.2. *The map*

$$\begin{array}{rccc} \lambda: & W_4^1(D) & \to & \Gamma \\ & [\mathfrak{D}] & \mapsto & Q_{\mathfrak{D}} \end{array}$$

is well defined and realizes $W_4^1(D)$ as a double cover of Γ, ramified over Γ'. The involution of $W_4^1(D)$ over Γ corresponds to the residuation map $\mathcal{D} \mapsto [\kappa_D] - \mathcal{D}$.

5. The Prym variety in genus 3

We write F for the union of components of $W_4^1(D)$ above Γ^-. If $\mathcal{D} \in F$, then $Q_{\mathcal{D}}$ has a singular point on $\{u = v = w = 0\}$. If the plane $V_{\mathcal{D}}$ would not contain that singular point, then $Q_{\mathcal{D}}$ would

https://doi.org/10.1112/S0010437X07003314

contain a $\mathbb{P}^3$, but this contradicts that $\mathrm{rk}(Q_{\mathcal{D}}) \geqslant 3$ (by Lemma 3.2). Hence, $\pi(V_{\mathcal{D}})$ is a line and $\pi_*(\mathcal{D}) = [\kappa_C]$. It follows that the map

$$\begin{array}{rccc} j: & F \times F & \to & \mathrm{Pic}^0(D) \\ & \mathcal{D}_1, \mathcal{D}_2 & \mapsto & \mathcal{D}_1 + \mathcal{D}_2 - [\kappa_D] \end{array} \tag{2}$$

maps $F \times F$ into $\ker(\pi_*)$.

Depending on the type of Γ^-, this gives us different descriptions of $\mathrm{Prym}(D/C)$. The case numbering is in correspondence with Table 1.

Case 0: Γ^- *is a doubled line.* This case does not occur because assuming that it does, leads to a contradiction. By choosing coordinates appropriately, Γ^- is described by the equation $\lambda_1^2 = 0$. It follows that $Q_1^- + \lambda_2 Q_2^- + \lambda_3 Q_3^-$ is non-singular for all λ_2, λ_3. It follows that $Q_2^- = Q_3^- = 0$. Therefore, D has an intersection with $\{u = v = w = 0\}$ and thus ι would be ramified.

Case 2: Γ^- *is a split singular conic, i.e.* $L_1 \cup L_2$*, for lines* L_1, L_2 *over* K. In that situation, F consists of two components E_1 and E_2, covering L_1 and L_2, respectively. Each of these covers is ramified at a degree four locus: the intersection of L_i with the other components of Γ. Hence, E_1 and E_2 are curves of genus 1. In fact, each has a rational point above $L_1 \cap L_2$, so we can identify them with their Jacobians. We have the map

$$\begin{array}{ccc} E_1 \times E_2 & \to & \mathrm{Jac}(D) \\ (\mathcal{D}_1, \mathcal{D}_2) & \mapsto & \mathcal{D}_1 + \mathcal{D}_2 - [\kappa_D]. \end{array}$$

Note that $(\mathcal{D}_1, \mathcal{D}_2)$ only maps to O if $Q_{\mathcal{D}_1} = Q_{\mathcal{D}_2}$. This can only happen above the (ramified) point $L_1 \cap L_2$, so the map is an injection. Since $E_1 \times E_2$ is connected and contains the origin, the image is contained in $\mathrm{Prym}(D/C)$ and because $E_1 \times E_2$ is an Abelian surface itself, we have the equality

$$\mathrm{Prym}(D/C) \cong E_1 \times E_2.$$

Case 3: Γ^- *is a non-split singular conic.* Then, over some quadratic extension $K(\sqrt{d})$ of K, the conic Γ^- splits and the analysis above applies. It follows that in that situation E_1 and E_2 are elliptic curves that are conjugate with respect to $K(\sqrt{d})/K$. By Weil restriction, it follows that

$$\mathrm{Prym}(D/C) \cong \Re_{K(\sqrt{d})/K}(E_1).$$

Case 4: Γ^- *is a non-singular conic.* In that case, Q_1^-, Q_2^-, Q_3^- are K-linearly independent and therefore span the space of quadratic forms in r, s. Without loss of generality, we can assume

$$\begin{aligned} Q_1 : Q_1^+(u, v, w) &= r^2, \\ Q_2 : Q_2^+(u, v, w) &= rs, \\ Q_3 : Q_3^+(u, v, w) &= s^2. \end{aligned}$$

It follows that Γ^- is given by the equation $4\lambda_1\lambda_3 = \lambda_2^2$ and we have a parametrization

$$\begin{array}{ccc} \mathbb{P}^1 & \to & \Gamma^- \\ (x:1) & \mapsto & (1:2x:x^2). \end{array}$$

The curve F is a double cover of Γ^-, ramified above $\Gamma^+ \cap \Gamma^-$. Using the parametrization above we obtain an equation of the form

$$\det(Q_1^+ + 2xQ_2^+ + x^2 Q_3^+) = \delta y^2$$

for some $\delta \in K^*$. Note that $\Gamma^+ \cap \Gamma^-$ has no multiple points, since those would correspond to conics in Λ of rank smaller than three, which contradicts Lemma 3.2. It follows that F is branched over six points and, hence, is of genus 2.

https://doi.org/10.1112/S0010437X07003314

TABLE 1. Structure of the Prym variety.

Case	C	D	Γ^-	$\mathrm{Prym}(D/C)$
1	Hyperelliptic	Hyperelliptic	—	$\mathrm{Jac}(F)$
2	Hyperelliptic	Non-hyperelliptic	Split singular	$E_1 \times E_2$
3	Hyperelliptic	Non-hyperelliptic	Non-split singular	$\Re_{K(\sqrt{d})/K}(E)$
4	Non-hyperelliptic	Non-hyperelliptic	Non-singular	$\mathrm{Jac}(F)$

In order to determine the correct value of δ, suppose that we have $\mathcal{D} \in F$ such that $2\mathcal{D} \neq [\kappa_D]$. Then $\mathcal{D}$ is cut out by a system of planes on $Q = \lambda(\mathcal{D})$, as defined in Corollary 4.2. If $\mathcal{D}$ is rational over K, then Q and the system of planes must be as well (but note that $\mathcal{D}$ itself does not need to contain rational divisors, nor does the system need to contain any planes rational over K).

If no rational $\mathcal{D}$ is available, then we base extend to $K(F)$ to ensure there is. We only want to determine the value of δ modulo squares and since K is algebraically closed in $K(F)$, our results will be valid as long as we find $\delta \in K$.

Using the parametrization of Γ^-, there is an $(x : 1) \in \mathbb{P}^1(K)$ such that

$$Q^- = -(r^2 + 2xrs + x^2 s^2).$$

It follows that $(0 : 0 : 0 : x : -1)$ is the singular point of Q and that Q is a cone over the quadric in $\mathbb{P}^3 = \{s = 0\} \subset \mathbb{P}^4$ with coordinates $(u : v : w : r)$ given by

$$Q^+(u, v, w) - r^2 = 0.$$

According to Lemma 2.5, this quadric has two rational systems of lines (and, therefore, a cone over it has two rational systems of planes) if

$$-\det Q^+ = -\det(Q_1^+ + 2xQ_2^+ + x^2 Q_3^+)$$

is a square in K. It follows that F is isomorphic to

$$F : y^2 = -\det(Q_1^+ + 2xQ_2^+ + x^2 Q_3^+).$$

The map $j : F \times F \to \mathrm{Pic}^0(D)$ defined in (2) gives rise to an isomorphism

$$\mathrm{Prym}(D/C) \simeq \mathrm{Jac}(F).$$

In Cases 2 and 3 above, the Jacobian of D contains elliptic curves E_1, E_2. In these cases, D is in fact a double cover of genus 1 curves C_1 and C_2 with $\mathrm{Jac}(C_i) \cong E_i$.

The cover can be constructed explicitly in the following way. A linear system of singular quadrics has a fixed singularity. Therefore, the $Q \in L_i \subset \Gamma^-$ have a fixed singularity P_i on the line $\{u = v = w = 0\}$. When we project D from P_i, we obtain an intersection of two quadrics in $\mathbb{P}^3$. Thus, this presents D as a double cover of a genus 1 curve C_i.

Let $\sigma_i \in \mathrm{Aut}_{\overline{K}}(D)$ denote the involution of D over C_i. We have $\iota = \sigma_1\sigma_2$. In fact, the projection $(u : v : w : r : s) \to (u : v : w)$ corresponds to $D \to D/\langle\sigma_1, \sigma_2\rangle$. This shows that the canonical model of C is, in fact, of genus 0 and, hence, that C is hyperelliptic. This places us in the situation of § 2.2.

THEOREM 5.1. *Let K be a field of characteristic zero and let C be a curve of genus 3 over K with an unramified double cover D/C. Then $\mathrm{Prym}(D/C)$ can be described as given in Table 1 depending on the nature of C and D. Models of the curves involved can be described as in Table 2. For hyperelliptic curves, it is assumed they are hyperelliptic over a $\mathbb{P}^1$ over K.*

https://doi.org/10.1112/S0010437X07003314

Table 2. Models of involved curves.

Case	Models
1	C: $y^2 = Q(x)R(x)$ where $\deg(Q) = 2, \deg(F) = 6$ D: $y_1^2 = Q(x)$ and $y_2^2 = R(x)$ F: $y_2^2 = R(x)$
2	C: $y^2 = R_1(x)R_2(x)$ where $\deg(R_1) = \deg(R_2) = 4$ D: $y_1^2 = R_1(x)$ and $y_2^2 = R_2(x)$ E_1: $\mathrm{Jac}(y_1^2 = R_1(x))$ E_2: $\mathrm{Jac}(y_2^2 = R_2(x))$
3	C: $y^2 = N_{K(\sqrt{d})[x]/K[x]}R(x)$ where $\deg(R) = 4$ D: (x, y_0, y_1) satisfying $(y_0 + y_1\sqrt{d})^2 = R(x)$ E: $\mathrm{Jac}(y^2 = R(x))$
4	C: $Q_1^+(u,v,w)Q_3^+(u,v,w) = Q_2^+(u,v,w)^2$ with Q_i^+ quadratic forms D: $\begin{cases} Q_1^+(u,v,w) = r^2 \\ Q_2^+(u,v,w) = rs \\ Q_3^+(u,v,w) = s^2 \end{cases}$ F: $y^2 = -\det(Q_1^+ + 2xQ_2^+ + x^2Q_3^+)$

6. Mapping D into $\mathrm{Prym}(D/C)$

As was shown in § 5, if C is hyperelliptic, then D is a cover of the curves that span $\mathrm{Prym}(D/C)$. Hence, it is obvious how to map D into $\mathrm{Prym}(D/C)$. In this section we show how D can be mapped into $\mathrm{Prym}(D/C)$ if C is non-hyperelliptic.

First, if we have a rational point $P_0 \in D(K)$, we can embed D in $\mathrm{Jac}(D)$ via the *Abel–Jacobi map*

$$\begin{array}{ccc} D & \to & \mathrm{Jac}(D) \\ P & \mapsto & [P - P_0]. \end{array}$$

When we combine this map with the projection map $(\mathrm{id}_* - \iota_*) : \mathrm{Jac}(D) \to \mathrm{Prym}(D/C)$, we obtain the *Abel–Prym map*

$$\begin{array}{ccc} D & \to & \mathrm{Prym}(D/C) \\ P & \mapsto & [P - \iota(P)] - [P_0 - \iota(P_0)]. \end{array}$$

In general, we do not have a rational base point P_0 at our disposal. We give an alternative map, based on the description of $\mathrm{Prym}(D/C)$ as $\mathrm{Jac}(F)$ for some component F of $W_4^1(D)$. This map turns out to correspond to $2(\iota_* - \mathrm{id}_*) : \mathrm{Pic}^1(D) \to \mathrm{Prym}(D/C)$. Thus, the image of D is a translation of twice an Abel–Prym embedding of D.

Let P_0 be a point on D and let L be the tangent line of C at $\pi(P)$. Then $L \cdot C$, being a linear section of a canonical model, determines an effective canonical divisor on C. Consequently, for some $P_1, P_2 \in D$ we have that $\pi^*(L \cdot C) = 2P_0 + 2\iota(P_0) + P_1 + \iota(P_1) + P_2 + \iota(P_2)$ is an effective canonical divisor on D.

We use the notation from § 3. Furthermore, we write $\mathrm{Tang}_D(P)$ for the tangent line of D at P and for a quadric $Q \subset \mathbb{P}^n$ and $T_1, T_2 \in \mathbb{P}^n$ we write $T_1^t Q T_2$ for the matrix product, where Q is identified with its representing $(n+1) \times (n+1)$ symmetric matrix and T_1, T_2 are interpreted as $(n+1)$-dimensional column vectors of projective coordinates.

https://doi.org/10.1112/S0010437X07003314

Lemma 6.1. *With the notation as above, let P be a point in $D(\overline{K})$.*

(i) *There are two divisors $\mathfrak{D}_1, \mathfrak{D}_2$ on D (with $\mathfrak{D}_1 = \mathfrak{D}_2$ in degenerate cases) such that $\mathfrak{D}_i \geqslant 2P$ and $[\mathfrak{D}_i] \in F(\overline{K}) \subset W_4^1(\overline{K})$.*

(ii) *Let P_1, P_2 be the points on D such that $\mathfrak{D}_1 = 2P + P_1 + P_2$. Then $\mathfrak{D}_2 = 2P + \iota(P_1) + \iota(P_2)$.*

(iii) *Let $T \in \mathrm{Tang}_D(P)$ with $T \neq P$. If $\mathfrak{D} \in F$ with $D = 2P + P_1 + P_2$, then $x = x_*(\mathfrak{D})$ satisfies*

$$(T^t \cdot Q_1 \cdot T) + 2x(T^t \cdot Q_2 \cdot T) + x^2(T^t \cdot Q_3 \cdot T) = 0.$$

(iv) *The map*

$$\begin{array}{rccc} \varphi: & D(\overline{K}) & \to & \mathrm{Div}^2(F/\overline{K}) \\ & P & \mapsto & [\mathfrak{D}_1] + [\mathfrak{D}_2] \end{array}$$

is defined over K.

Proof. (iii) Note that $\mathfrak{D} \in F$ implies $l(\mathfrak{D}) = 2$. By Lemma 4.1 we have $\mathrm{Tang}_D(P) \subset V_{\mathfrak{D}} \subset Q_{\mathfrak{D}}$. This implies that $T \in Q_{\mathfrak{D}}$ for some (and, hence, for all) $T \in \mathrm{Tang}_D(P)$ with $T \neq P$. Using that $\Gamma^- \simeq \mathbb{P}^1$ via $(1 : 2x : x^2) \mapsto (x : 1)$, we get the desired equation.

(i) From part (iii), we know that there are two quadrics $Q \in \Gamma^-$ containing $\mathrm{Tang}_D(P)$. We show that such a quadric is $Q_{\mathfrak{D}}$ for some $\mathfrak{D} \in F$ such that $\mathfrak{D} \geqslant 2P$. Consider the plane V spanned by $\mathrm{Tang}_D(P)$ and a singular point $(0 : 0 : 0 : x : -1)$ of Q. Then $V \subset Q$. The proof of Lemma 4.1(v) points out that then $\mathfrak{D} = V \cdot D$ represents a divisor class in $W_4^1(D)$ and that $Q = Q_{\mathfrak{D}}$. By construction, we have $\mathfrak{D} \geqslant 2P$.

If there is another divisor $\mathfrak{D}' \geqslant 2P$ with $Q_{\mathfrak{D}'} = Q$, then $\mathfrak{D} - \mathfrak{D}'$ or $\mathfrak{D} - \iota_*(\mathfrak{D}')$ is principal. Taking the image under π_* would give a divisor of a degree two function on C, which contradicts that C is not hyperelliptic.

(ii) Note that $\pi_*(\mathfrak{D}_2) = \pi_*(\mathfrak{D}_1) = C \cdot \mathrm{Tang}_C(\pi(P))$. If $\mathfrak{D}_2 = 2P + P_1 + \iota(P_2)$, then $2P + P_1$ must lie on the line $V_{\mathfrak{D}_1} \cap V_{\mathfrak{D}_2}$. Since D is canonical, it follows that $l(2P + P_1) = 2$. This contradicts Lemma 3.1. It follows that $\mathfrak{D}_2$ must be as stated.

(iv) Verify that ${}^{\sigma}(\varphi(P)) = \varphi({}^{\sigma}P)$ for $\sigma \in \mathrm{Gal}(\overline{K}/K)$ via direct computation. □

Proposition 6.2. *Let C be a non-hyperelliptic genus 3 curve over a field K of characteristic zero and let D/C be an unramified double cover with $\iota : D \to D$ the associated involution. Let F be the genus 2 curve given by Theorem 5.1 such that $\mathrm{Jac}(F) = \mathrm{Prym}(D/C)$ and let $\varphi : D \to \mathrm{Div}^2(F)$ be the map defined in Lemma 6.1. Then we have*

$$\begin{array}{rccc} 2(\iota_* - \mathrm{id}_*): & D(\overline{K}) & \to & \mathrm{Prym}(D/C)(\overline{K}) \\ & P & \mapsto & [\varphi(P) - \kappa_F]. \end{array}$$

Proof. Using Lemma 6.1(ii), we have $\varphi(P) = 4P + P_1 + P_2 + \iota(P_1) + \iota(P_2)$. Using that $[\kappa_D] = [2P + 2\iota(P) + P_1 + P_2 + \iota(P_1) + \iota(P_2)]$, we have $[\varphi(P) - \kappa_D] = 2P - 2\iota(P)$ as an element of $\mathrm{Pic}(D)$. Note that $[\kappa_D] = [\mathfrak{D} + \iota(\mathfrak{D})]$ for any $[\mathfrak{D}] \in F \subset W_4^1(D)$, so identifying $\mathrm{Pic}(F) \subset \mathrm{Pic}(D)$, we get $[\kappa_F] = [\kappa_D]$. This proves the proposition. □

Remark 6.3. It is worth noting that the map $(\iota_* - \mathrm{id}_*) : D \to \ker(\pi_*)$ does not map D to $\mathrm{Prym}(D/C)$. To see this, note that $\mathrm{Prym}(D/C) = \mathrm{Jac}(F)$ for some genus 2 curve F. Any degree zero divisor class on F can be represented as the difference of two points on F, so we have that $\mathrm{Prym}(D/C) = F - F$. If $P \in D(\overline{K})$ has $[\iota(P) - P] \in \mathrm{Prym}(D/C)$, then we can find $[\mathfrak{D}_1], [\mathfrak{D}_2] \in F(\overline{K})$ such that $[\iota(P) - P] = [\mathfrak{D}_1 - \mathfrak{D}_2]$. Since $F \subset W_4^1(D)$, we can choose effective representatives $\mathfrak{D}_1, \mathfrak{D}_2$ with a given point in the support. Hence, we can assume that $\mathfrak{D}_1 = \iota(P) + P_2 + P_3 + P_4$ and $\mathfrak{D}_2 = P + P_5 + P_6 + P_7$. Note that P_2, P_3, P_4 are not collinear, because if they were, then the geometric formulation of the

https://doi.org/10.1112/S0010437X07003314

Riemann–Roch theorem [ACGH85, p. 12] would imply that $l(P_2+P_3+P_4)=2$, so D would be trigonal or hyperelliptic.

Therefore, P_2, P_3, P_4 already determine the plane $V_{\mathfrak{D}_1}$. If $P_5+P_6+P_7 = P_2+P_3+P_4$, then we would have that both P and ιP lie in the same plane $V_{\mathfrak{D}_1}$, which would yield a g^2_5 on D. However, then the Riemann–Roch theorem tells us that $\kappa_D - P - \iota(P) - P_2 - P_3 - P_4$ would be a g^1_3 and therefore D would be trigonal.

It follows that the non-zero divisor $P_2+P_3+P_4-P_5-P_6-P_7$ is linearly equivalent to zero, so D is hyperelliptic or trigonal, contradicting Lemma 3.1.

Lemma 6.1 together with Proposition 6.2 provide an explicit way of mapping D into an Abelian surface $\mathrm{Prym}(D/C) \simeq \mathrm{Jac}(F)$. By slight abuse of notation, we write $\varphi : D \to \mathrm{Jac}(F)$.

For explicit computations, Abelian surfaces have proven to be rather unwieldy. In many cases, enough of the group variety structure remains in the associated Kummer surface $\mathcal{K} = \mathrm{Jac}(F)/\langle -1\rangle$. The surface $\mathcal{K}$ is naturally expressed as a quartic surface in $\mathbb{P}^3$. We use the map[2] from [CF96, 3.1]

$$\begin{array}{rccc} k: & \mathrm{Jac}(F) & \to & \mathcal{K} \\ & [(x_1,y_1)+(x_2,y_2)-\kappa_F] & \mapsto & (1 : x_1+x_2 : x_1x_2 : \dots) = (k_1 : k_2 : k_3 : k_4) \end{array}$$

which expresses $\mathrm{Jac}(F)$ as a double cover of $\mathcal{K}$, ramified at $\mathrm{Jac}(F)[2]$, which maps to the singular locus of $\mathcal{K}$. The equation of $\mathcal{K}$ is of the form

$$\mathcal{K} : (k_2^2 - 4k_1k_3)k_4^2 + K_3(k_1,k_2,k_3)k_4 + K_4(k_1,k_2,k_3) = 0,$$

where K_3 and K_4 are homogeneous forms of degrees three and four, respectively (see [CF96] for explicit formulae). Hence, $\mathcal{K}$ is itself a double cover of the projective plane with coordinates $(k_1 : k_2 : k_3)$ outside the point $(0:0:0:1)$.

Since $\iota_* \circ 2(\iota_* - \mathrm{id}_*) = -1 \circ 2(\iota_* - \mathrm{id}_*)$, we see that $D \to k\varphi(D)$ factors through $D/\langle\iota\rangle = C$. Furthermore, if $\mathfrak{D} \in \mathrm{Div}^2(F)$ is effective and $(k_1 : k_2 : k_3 : k_4) = k([\mathfrak{D} - \kappa_F])$, then $x_*(\mathfrak{D})$ satisfies

$$k_3 - k_2x + k_1x^2 = 0.$$

This gives us a procedure to compute many pointwise images for $k\varphi$.

(1) Choose an extension L and a point $P \in D(L)$ (since D is given as a degree eight curve, there is an abundance of suitable degree eight extensions).

(2) Following Lemma 6.1, choose $T \in \mathrm{Tang}_D(P)$ and set

$$(k_1,k_2,k_3) = (T^t \cdot Q_1 \cdot T, -2T^t \cdot Q_2 \cdot T, T^t \cdot Q_3 \cdot T).$$

(3) If $k_3 - k_2x + k_1x^2$ is irreducible of degree two over L, then there is a unique point $(k_1 : k_2 : k_3 : k_4) \in \mathcal{K}(L)$ that has an L-rational preimage in $\mathrm{Jac}(F)$. This is the desired image.

The irreducibility in the last step corresponds to P_1, P_2 from Lemma 6.1(ii) being quadratic conjugate over L. In that case, the divisor $P_1 + \iota(P_2)$ is not L-rational and, hence, rationality tells which divisor to pick. If P_1, P_2 are themselves L-rational, then the above procedure does not compute sufficient information to distinguish between $2P + P_1 + P_2$ and $P + \iota(P) + P_1 + \iota(P_2)$.

The procedure above yields a way to compute the equations of $k\varphi(D)$. First, one gathers many pointwise images for points over extensions L and then one interpolates for low degree rational forms vanishing on those points. As we will see, $k\varphi(D)$ is the intersection of $\mathcal{K}$ with another degree four surface.

[2] If F is given by the equation $y^2 = f_0 + f_1x + f_2x^2 + \cdots + f_6x^6$, then

$$k_4 = \frac{2f_0 + f_1k_2 + 2f_2k_3 + f_3k_2k_3 + 2f_4k_3^2 + f_5k_2k_3^2 + 2f_6k_3^3 - 2y_1y_2}{(x_1-x_2)^2}.$$

https://doi.org/10.1112/S0010437X07003314

Lemma 6.4. *With the notation above, the image of D under $k \circ \varphi$ is of degree at most* 16.

Proof. We compute the degree of the image by computing the degree of the intersection with $k_1 = 0$. By change of basis we can assume that Q_3 is of rank four. According to Lemma 6.1(iii), a point $P \in D$ has $k_1 = 0$ if Q_3 contains the plane $V_{\mathfrak{D}}$ for some $\mathfrak{D} \geqslant 2P$. The two plane rulings on Q_3 give rise to two degree four covers $D \to \mathbb{P}^1$, where the fibres are the divisors cut out by the $V_{\mathfrak{D}}$ in the ruling. From Riemann–Hurwitz it follows that for each ruling there are 16 ramified fibres, i.e. $\mathfrak{D}$ of the form $2P + P_1 + P_2$. Hence, we see that there are 32 points on D (counted with appropriate multiplicity) that land on $k_1 = 0$. Note that the image of D under $k\varphi$ factors through $D/\langle\iota\rangle$, so the degree of $k\varphi(D)$ is at most 16. □

The procedure above has been implemented as a routine for the computer algebra system MAGMA [BCP97]. See [Bru04].

7. The fibre of the Prym map in genus 3

Given a genus 2 curve F, we have an Abelian variety $\mathrm{Jac}(F)$ and a quartic surface $\mathrm{Jac}(F)/\langle -1\rangle = \mathcal{K} \subset \mathbb{P}^3$, with a singular locus consisting of the image of $\mathrm{Jac}(F)[2]$. There is an obvious way of realizing $\mathrm{Jac}(F)$ as a Prym variety of a non-hyperelliptic curve of genus 3. Pick a plane $V \subset \mathbb{P}^3$ such that $C := V \cap \mathcal{K}$ is a non-singular quartic curve. It follows that C stays away from the singular points of $\mathcal{K}$ and thus does not meet the ramification locus of $k : \mathrm{Jac}(F) \to \mathcal{K}$. Therefore, $D = k^{-1}(C)$ is an unramified cover of C. Either D is connected and, hence, of genus 5 or D is the disjoint union of two copies of C. Note, however, that C is of genus 3 and, hence, has to be special to fit in an Abelian surface.

In fact, as Verra [Ver87] proves, over an algebraically closed field, essentially any occurrence of $\mathrm{Jac}(F)$ as $\mathrm{Prym}(D/C)$ occurs for C isomorphic to a linear section of $\mathcal{K}$. The addition of $\mathrm{Jac}(F)[2]$ induces automorphisms of $\mathcal{K}$ which are induced by linear transformations of $\mathbb{P}^3$. He shows that the fibre of the Prym map $(D/C) \mapsto \mathrm{Prym}(D/C)$ over $\mathrm{Jac}(F)$ is a blow-up of $\widehat{\mathbb{P}}^3/\mathrm{Jac}(F)[2]$, where $\widehat{\mathbb{P}}^3$ is the space of plane sections of $\mathcal{K}$.

Verra also proves that genus 5 curves $D \subset \mathrm{Jac}(F)$ of the form above are, up to translation by a 2-torsion point, Abel–Prym embeddings. We give a short description of a procedure to recover

$$C : Q_1^+(u,v,w)Q_3^+(u,v,w) = Q_2^+(u,v,w)^2$$

from a plane section of the Kummer surface $\mathcal{K} = \mathrm{Jac}(F)/\langle -1\rangle$ for a curve F of genus 2.

First we review some of the basic geometry of Jacobians of curves of genus 2. Let F be a curve of genus 2. In [CF96], Cassels and Flynn define a projective model of $\mathrm{Jac}(F)$ in $\mathbb{P}^{15}$ with coordinates $(z_0 : \cdots : z_{15})$ with (among others) the following properties.

- There is a symmetric theta divisor Θ on $\mathrm{Jac}(F)$ such that
$$\langle k_1, \ldots, k_4\rangle = |2\Theta|$$
and
$$\langle z_0, \ldots, z_{15}\rangle = |4\Theta|$$
with
$$(k_1 : k_2 : k_3 : k_4) = (z_{14} : z_{13} : z_{12} : z_5).$$
- The coordinates $(k_1 : k_2 : k_3 : k_4)$ provide a model of the Kummer surface $\mathcal{K} = \mathrm{Jac}(F)/\langle -1\rangle$.
- With respect to the action of $[-1] \in \mathrm{Aut}(\mathrm{Jac}(F))$ on $|4\Theta|$, we have that
$$\langle z_0, z_3, z_4, z_5, z_{10}, \ldots, z_{15}\rangle = \langle k_1^2, k_1k_2, \ldots, k_4^2\rangle$$

https://doi.org/10.1112/S0010437X07003314

is the $+1$-eigenspace and

$$\langle g_0, \ldots, g_5 \rangle := \langle z_1, z_2, z_6, z_7, z_8, z_9 \rangle$$

is the -1-eigenspace.

Let $V = \{k_4 = v_1 k_1 + v_2 k_2 + v_3 k_3\} \subset \mathbb{P}^3$ be a plane such that $C = \mathcal{K} \cap V$ is a non-singular plane section and let $(u : v : w) = (k_1 : k_2 : k_3)$ be coordinates on V (since $(0 : 0 : 0 : 1)$ is a singular point of $\mathcal{K}$, assuming this suggested form of V is not a restriction). On V, we have that $k_4 = k_4(u, v, w)$ is a linear form in u, v, w. The curve C is a non-singular degree four plane curve. It follows that C is of genus 3 and that $(u : v : w)$ gives a canonical model of C, i.e. that $\langle u|_C, v|_C, w|_C \rangle = |\kappa_C|$ for some canonical divisor κ_C of C. Let D be the pull-back of C along $\mathrm{Jac}(F) \to \mathcal{K}$ and let κ_D be the pull-back of κ_C. It is a straightforward computation to check that the restriction of $\langle z_0, \ldots, z_{15} \rangle$ to D gives a linear system contained in $|\kappa_D|$ and that generically it gives the complete linear system.

Using the quadratic relations between the z_i (see [CF96], [Fly96] and [Fly90] for the explicit formulae), we can express any $g_i g_j$ as a degree four form in $k_1, \ldots, k_4$. Hence, we obtain that

$$(a_0 g_0 + \cdots + a_5 g_5)^2 = G(a_0, \ldots, a_5; k_1, \ldots, k_4),$$

where G is homogeneous of degrees two and four in the a_i and the k_j, respectively.

Insisting that

$$G(a_0, \ldots, a_5; u, v, w, k_4(u, v, w)) = u^2 Q(u, v, w)$$

for some quadratic form Q gives nine quadratic equations in $a_0, \ldots, a_5$. However, a solution to these equations corresponds exactly to a form $Q(u, v, w)$ on C that becomes a square when pulled back to D. We know that this happens for exactly two forms $Q_1^+(u, v, w) = r^2$ and $Q_3^+(u, v, w) = s^2$, so these equations determine a degree two locus in $(a_0 : \cdots : a_5)$.

Solving these equations allows us to determine $Q_1^+(u, v, w)$ and $Q_3^+(u, v, w)$ up to a scalar. The quadratic form $Q_2^+(u, v, w)$ is then easily determined up to a scalar because this corresponds to the conic through the intersection of $Q_1^+(u, v, w)Q_3^+(u, v, w) = 0$ with C. It is then straightforward to find scalars λ, μ such that

$$\lambda Q_1^+(u, v, w)Q_3^+(u, v, w) - \mu Q_2^+(u, v, w)^2$$

equals the equation for C or, equivalently, that

$$\lambda Q_1^+(u, v, w)\mu Q_3^+(u, v, w) - (\mu Q_2^+(u, v, w))^2$$

defines the curve C.

Note that we may find Q_i^+ that are quadratic conjugate over the base field we are working with, because of the arbitrary coordinate choice we made when insisting that $G = u^2 Q(u, v, w)$. The analysis from § 3 guarantees us that by change of basis (corresponding to $\mathrm{Aut}(\Gamma^-)$ or, equivalently, fractional linear transformations of x) we can in fact obtain rational Q_1^+, Q_3^+. This yields the following amusing result, which is equivalent to saying that all Jacobians of genus 2 curves over $\mathbb{Q}$ occur as Prym varieties of non-hyperelliptic curves of genus 3 over $\mathbb{Q}$.

Proof of Proposition 1.4. Take the curve of genus 2

$$F : y^2 = f(x)$$

and take a sufficiently general plane section of the associated Kummer surface. Using the construction above, we obtain a cover $D \to C$ such that $\mathrm{Prym}(D/C) = \mathrm{Jac}(F)$. Section 3 tells us that F must be of the described form and the outline above explains how one can find the representation explicitly. □

In fact, the model of C as a plane section of a Kummer surface $\mathcal{K}$ completely encodes the 28 bitangents of C as well. The 16 tropes of $\mathcal{K}$ cut out bitangents on C. The remaining 12 bitangents come in pairs, making up the six singular conics in the family $Q_1^+ + 2xQ_2^+ + x^2Q_3$.

This gives us a way to search for genus 3 curves with all bitangents rational. First, start with a Kummer surface $\mathcal{K}$ with 16 rational tropes (i.e. the Kummer surface of the Jacobian of a genus 2 curve with six rational Weierstraß points). Then, select a plane V such that $C := V \cap \mathcal{K}$ is of the form

$$Q_1^+(u,v,w)Q_3^+(u,v,w) = Q_2^+(u,v,w)^2,$$

where the singular conics in $Q_1^+ + 2xQ_2^+ + x^2Q_3$ are split.

Remark 7.1. These conics are all split or non-split simultaneously. In order to see that, we have to look a bit closer to the relation between $\mathrm{Jac}(C)[2]$ and pairs of bitangents. Each of the 63 non-trivial 2-torsion points can be represented by a pair of bitangents in six ways. Furthermore, the bitangents of C split over the same extension as $\mathrm{Jac}(C)[2]$.

The 16 tropes give rise to at least $\binom{16}{2}/6 = 20$ non-trivial rational points in $\mathrm{Jac}(C)[2]$. Thus, $\mathrm{Jac}(C)[2](K) \supset (\mathbb{Z}/2)^5$ and has index at most two in $\mathrm{Jac}(C)[2](\overline{K})$. It follows that the action of Galois on $\mathrm{Jac}(C)[2](\overline{K})$ factors through a group of order at most two. Hence, if not all bitangents are rational over K, then they must be conjugate over the one quadratic extension corresponding to this group of order two.

Example

A curve of genus 3 *with all* 28 *bitangents rational.* Take

$$F : y^2 = x(x-2)(x-1)(x+1)(x+3).$$

The corresponding Kummer surface is

$$\begin{aligned}\mathcal{K} : 36k_1^4 + 84k_1^3k_3 - 24k_1^2k_2k_3 - 12k_1^2k_2k_4 + 65k_1^2k_3^2 + 4k_1^2k_3k_4 - 24k_1k_2^2k_3 + 4k_1k_2k_3^2 \\ + 14k_1k_2k_3k_4 + 14k_1k_3^3 - 4k_1k_3^2k_4 - 4k_1k_3k_4^2 + k_2^2k_4^2 - 2k_2k_3^2k_4 + k_3^4 = 0.\end{aligned}$$

We take the plane section

$$V : k_1 + k_2 + tk_3 + k_4 = 0.$$

Projecting onto $(u : v : w) = (k_1 : k_2 : k_3)$, we obtain

$$C : Q_1^+(u,v,w)Q_3^+(u,v,w) = Q_2^+(u,v,w)^2,$$

where

$$\begin{aligned}Q_1^+ &= (36t-82)u^2 + (6t-80)uv + (-11t+14)uw + (6t+2)v^2 + (t+14)vw + tw^2,\\ Q_2^+ &= (-3t+40)u^2 + \left(-\frac{1}{2}t - 9\right)uv + \left(-6t^2 + \frac{11}{2}t + 51\right)uw + \left(-\frac{1}{2}t - 7\right)v^2\\ &\quad + \left(-\frac{1}{2}t^2 - 2t + 2\right)vw + \left(-t^2 + \frac{1}{2}t + 7\right)w^2,\\ Q_3^+ &= (6t+2)u^2 + (t+14)uv + (t^2+2t-4)uw + tv^2 + (2t^2 - t - 14)vw + (t^3 - t^2 - 8t + 2)w^2.\end{aligned}$$

The 16 bitangents coming from the tropes are given by the polynomials

$$\begin{aligned}&u, \quad w, \quad 4u - 2v + w, \quad 5u + 3v + (t+1)w, \quad 4u + v + (t+2)w, \quad u + 7v + (t-1)w,\\ &u - v + w, \quad 7u + v + (-t-3)w, \quad 9u + 3v + w, \quad 7u + v + (t+1)w,\\ &5u - v + (-t+1)w, \quad u - v + (-t+3)w, \quad 2u - 4v + (-t+2)w,\\ &10u - 2v + (t-4)w, \quad u + v + w, \quad 2u + 2v + tw.\end{aligned}$$

https://doi.org/10.1112/S0010437X07003314

The remaining 12 bitangents come from the six singular quadrics. They are split if $196+20t-23t^2$ is a square. Therefore, we substitute

$$t := \frac{4s^2-10s-6}{2s^2+s+3}$$

and obtain the bitangents given by the polynomials

$$\begin{aligned}
&(s+21)u+(7s+3)v+(s-3)w, \quad (10s+11)u+(-2s+5)v+(-2s-1)w,\\
&(8s^3+2s^2+11s-3)u+(2s^3+5s^2+5s+6)v+(8s^3+17s^2-s-6)w,\\
&(10s^3-s^2+12s-9)u+(-2s^3-7s^2-6s-9)v+(-2s^3+5s^2+30s-9)w,\\
&(4s^3+4s^2+7s+3)u+(2s^2+s+3)v+(2s^2+3s-3)w,\\
&(2s^3-5s^2-9)u+(-2s^3-3s^2-4s-3)v+(2s^3+7s^2+4s-1)w,\\
&(2s^3+7s^2+6s+9)u+(2s^3+s^2+3s)v+(2s^3+s^2-3s)w,\\
&(4s^3+10s^2+10s+12)u+(-2s^3+s^2-2s+3)v+(s^3+4s^2-5s)w,\\
&(4s^3+16s^2+13s+21)u+(-4s^3-5s+3)v+(4s^3+16s^2-3s-3)w,\\
&(10s^3+23s^2+24s+27)u+(6s^3+s^2+8s-3)v+(6s^3-5s^2-20s+7)w,\\
&(14s^3+13s^2+24s+9)u+(2s^3-5s^2-9)v+(-10s^3-35s^2+9)w,\\
&(4s^3-8s^2+s-15)u+(4s^3+4s^2+7s+3)v+(4s^3-8s^2-23s+9)w.
\end{aligned}$$

8. Applications to finding rational points on curves of genus 3

In this section, we will apply the concepts of *covering collections* (see [Bru02, BF05, CW32, Wet97]) and *Chabauty methods* (see [Col85, Fly97]) to a curve C of genus 3 with an unramified double cover D. We end up determining the rational points on a curve of genus 5 inside the Jacobian of a curve F of genus 2. The hardest piece of information we need is the Mordell–Weil group of $\mathrm{Jac}(F)$. Computationally, this is much more attractive than applying Chabauty methods directly to an embedding of C in its own Jacobian. In the latter case, we would have to analyze the Mordell–Weil group of $\mathrm{Jac}(C)$.

In addition, the techniques we present here do not depend on the existence of an embedding of C in $\mathrm{Jac}(C)$. As a result, we see that we can even use the construction to exhibit part of a local–global obstruction for C and D having rational points.

Let K be a number field and let C be a non-hyperelliptic curve of genus 3 with an unramified double cover D over K. As we have seen in § 3, it follows that there exists a smooth plane model of C of the form

$$Q_1(u,v,w)Q_3(u,v,w) = Q_2(u,v,w)^2,$$

where $Q_1, Q_2, Q_3 \in K[u,v,w]$ are quadratic forms. Without loss of generality, we can assume that Q_1, Q_2, Q_3 have integral coefficients. Furthermore, we have a collection of twists of D, each covering C, of the form

$$D_\delta : \begin{cases} Q_1(u,v,w) = \delta r^2, \\ Q_2(u,v,w) = \delta rs, \\ Q_3(u,v,w) = \delta s^2. \end{cases}$$

We write $\mathcal{O} = \mathcal{O}_K$ for the ring of integers of K and we consider the projective $\mathcal{O}_K$-scheme X corresponding to the ideal $I = (Q_1, Q_3, Q_1Q_3 - Q_2^2)\mathcal{O}_K[u,v,w]$. Since C is non-singular as a curve over K, we have that $X \times_{\mathcal{O}_K} \mathrm{Spec}(K)$ is empty. Let S be a finite set of primes of $\mathcal{O}$ containing all primes of even residue characteristic such that for any prime $\mathfrak{p}$ of $\mathcal{O}_K$ not in S, we have that

https://doi.org/10.1112/S0010437X07003314

$X \times_{\mathcal{O}_K} \mathrm{Spec}(\mathcal{O}_K/\mathfrak{p})$ is empty. Such a set S is easily computed. Let $\mathrm{Res}_v(P,Q)$ be the resultant of the polynomials P, Q with respect to the variable v. Compute

$$\mathrm{Res}_u(\mathrm{Res}_v(Q_1,Q_3),\mathrm{Res}_v(Q_1,Q_2)) = \lambda w^{16}.$$

One can take S to be the set of prime divisors of λ, together with the primes above two. One may obtain a smaller set by intersecting such sets S obtained from all different combinations in which such resultants could be taken. It is straightforward to check that for any point $P \in C(K)$ and any $\mathfrak{p} \notin S$ we have that $\nu_\mathfrak{p}(Q_1(P)) \in 2\mathbb{Z}$ or $\nu_\mathfrak{p}(Q_3(P)) \in 2\mathbb{Z}$, because otherwise P would reduce to a point on $X \times_{\mathcal{O}_K} \mathrm{Spec}(\mathcal{O}_K/\mathfrak{p})$. We recall the definition

$$K(S,2) := \{\delta \in K^* : v_\mathfrak{p}(\delta) \equiv 0 \bmod 2 \text{ for all primes of } K \text{ satisfying } \mathfrak{p} \notin S\}/K^{*2}.$$

This is a finite subgroup of K^*/K^{*2} and we will identify its elements with a finite set of representatives in K^*.

We obtain the standard lemma, which determines to the twists D_δ to which rational points of C may lift.

Lemma 8.1. *Let C and Q_1, Q_2, Q_3 and S be as above. If $(u_0 : v_0 : w_0) \in C(K)$, then there exists $\delta \in K(S,2)$ and $r_0, s_0 \in K$ such that*

$$(u_0 : v_0 : w_0 : r_0 : s_0) \in D_\delta(K).$$

Thus, in order to determine the rational points of C, it suffices to determine the rational points of D_δ for all $\delta \in K(S,2)$. From § 4 we know that for

$$F_\delta : y^2 = -\delta \det(Q_1 + 2xQ_2 + x^2Q_3),$$

we have $\mathrm{Prym}(D_\delta/C) \simeq \mathrm{Jac}(F_\delta)$ and Proposition 6.2 gives an explicitly computable map $\varphi : D_\delta \to \mathrm{Jac}(F_\delta)$. We can then proceed to determine $\varphi(D_\delta(\mathbb{Q})) \cap \mathrm{Jac}(F_\delta)(\mathbb{Q})$ or rather, as it turns out, $k(\mathrm{Jac}(F_\delta)(\mathbb{Q})) \cap k\varphi(D_\delta)(\mathbb{Q})$.

Example

Chabauty using Prym varieties.

Proof of Proposition 1.1. See [Bru04] for a transcript of the computer calculations. Applying the method described above we verify that we can take $S = \{1,2,5\}$ and local considerations show that $D_\delta(\mathbb{Q}) = \emptyset$ for $\delta \neq -1$. We find

$$F : y^2 = x^5 + 8x^4 - 7x^3 - \tfrac{7}{2}x^2 + 5x - 1$$

and

$$\mathrm{Jac}(F)(\mathbb{Q}) = \langle \mathcal{D} \rangle = \langle [(2\sqrt{2} - 2, 17\sqrt{2} - 25) + (-2\sqrt{2} - 2, -17\sqrt{2} - 25) - 2\infty] \rangle.$$

The equation of the associated Kummer surface is

$$\begin{aligned}\mathcal{K} : {} & 11k_1^4 - 28k_1^3k_2 + 70k_1^3k_3 + 4k_1^3k_4 + 32k_1^2k_2^2 - 164k_1^2k_2k_3 - 10k_1^2k_2k_4 + 171k_1^2k_3^2 \\ & + 14k_1^2k_3k_4 + 4k_1k_2^3 - 20k_1k_2^2k_3 + 14k_1k_2k_3^2 + 14k_1k_2k_3k_4 + 14k_1k_3^3 - 32k_1k_3^2k_4 \\ & - 4k_1k_3k_4^2 + k_2^2k_4^2 - 2k_2k_3^2k_4 + k_3^4 = 0\end{aligned}$$

and, using the interpolation procedure described in § 6, we find that the model of C in $\mathcal{K}$ given by $k\varphi(D)$ is given by the polynomial equation

$$\begin{aligned}\psi = {} & 429\,136k_1^4 + 1\,330\,784k_1^3k_3 + 567\,232k_1^3k_4 - 159\,200k_1^2k_2^2 - 2\,866\,016k_1^2k_2k_3 + 33\,440k_1^2k_2k_4 \\ & + 4\,248\,768k_1^2k_3^2 + 27\,552k_1^2k_3k_4 + 881\,664k_1^2k_4^2 + 288\,072k_1k_2^3 - 777\,432k_1k_2^2k_3 - 256\,928k_1k_2^2k_4 \\ & + 244\,832k_1k_2k_3^2 + 907\,424k_1k_2k_3k_4 - 745\,472k_1k_2k_4^2 + 593\,152k_1k_3^3 - 991\,488k_1k_3^2k_4\end{aligned}$$

https://doi.org/10.1112/S0010437X07003314

$$+357\,440k_1k_3k_4^2+573\,440k_1k_4^3+34\,895k_2^4-69\,720k_2^3k_3+1120k_2^3k_4+151\,704k_2^2k_3^2$$
$$-364\,448k_2^2k_3k_4+226\,032k_2^2k_4^2-251\,552k_2k_3^3+569\,376k_2k_3^2k_4+10\,752k_2k_3k_4^2-315\,392k_2k_4^3$$
$$+156\,704k_3^4-167\,552k_3^3k_4-283\,136k_3^2k_4^2+200\,704k_3k_4^3+114\,688k_4^4=0.$$

Using that $\varphi : D \to \mathrm{Jac}(F)$ is defined over $\mathbb{Q}$ and that $\mathrm{Jac}(F)(\mathbb{Q}) = \langle \mathcal{D} \rangle$, we find that a rational point $P \in \varphi(D)(\mathbb{Q})$ must be of the form $P = n\mathcal{D}$ for some $n \in \mathbb{Z}$. Furthermore, considering F and $\mathcal{K}$ over $\mathbb{F}_{13}$, we find that any such point must have $n \equiv \pm 1 \bmod 10$.

Since $\mathrm{Jac}(F)$ is an algebraic group, we can pick a set of local coordinates z_1, z_2 on $\mathrm{Jac}(F)$ around the origin O. We can find formal power series vectors $\mathrm{Log}(z_1, z_2) \in \mathbb{Q}[[z_1, z_2]]^2$ and $\mathrm{Exp}(l_1, l_2) \in \mathbb{Q}[[l_1, l_2]]^2$ such that for any two points $P, Q \in \mathrm{Jac}(F)(\mathbb{Q}[[z_1, z_2]])$ we have

$$(z_1(P+Q), z_2(P+Q)) = \mathrm{Exp}(\mathrm{Log}(z_1(P), z_2(P)) + \mathrm{Log}(z_1(Q), z_2(Q))).$$

Furthermore, if $p > 2$ is a prime of good reduction then for points in the kernel of reduction

$$\mathrm{Jac}(F)(\mathbb{Q}_p)^{(1)} = \ker(\mathrm{Jac}(F)(\mathbb{Q}_p) \to \mathrm{Jac}(F)(\mathbb{F}_p)),$$

these power series actually converge and yield an isomorphism

$$\mathrm{Jac}(F)(\mathbb{Q}_p)^{(1)} \simeq (p\mathbb{Z}_p)^2.$$

Using this, we obtain a power series

$$\psi(N) = \psi(k((1+10N)\mathcal{D})) = \psi(k(\mathcal{D} + \mathrm{Exp}(N\mathrm{Log}(10\mathcal{D})))),$$

say,

$$\psi(N) = \psi_0 + \psi_1 N + \psi_2 N^2 + \cdots \in \mathbb{Z}_{13}[\![N]\!],$$

with $\psi_i \equiv 0 \bmod 13^i$ such that, if $P = (1+10N)\mathcal{D}$ is a point on $\varphi(D)(K)$, then $\psi(N) = 0$.

Note that the values of $\psi(k(\mathcal{D})), \psi(k(11\mathcal{D}))$ determine $\psi_0, \psi_1 \bmod 13^2$, so one does not need an explicit description of the formal group law on $\mathrm{Jac}(F)$ to obtain an approximation to $\psi(N)$.

Since $\psi(k(\mathcal{D})) = 0$ and $\psi(k(11\mathcal{D})) \not\equiv 0 \bmod 13^2$, it follows that $\psi_1 \not\equiv 0 \bmod 13^2$. From Straßmann's lemma it follows that $\psi(N)$ has at most one zero for $N \in \mathbb{Z}_{13}$ (i.e. $N = 0$). This implies that $\varphi(D)$ has only one rational point which reduces to $\mathcal{D}$ modulo 13. By symmetry, it follows that there is also only one rational point reducing to $-\mathcal{D}$ modulo 13. On the other hand, the computation over $\mathbb{F}_{13}$ shows that all rational points of $\varphi(D)$ reduce to $\pm\mathcal{D}$ modulo 13. Hence, it follows that

$$\varphi(D)(K) = \{\mathcal{D}, -\mathcal{D}\}$$

and that C has only one rational point, being $(0:1:0)$. □

Example

Computations in the Brauer–Manin obstruction. Since the embedding of D in $\mathrm{Prym}(D/C)$ is independent of D having any rational points, we can also apply this construction to curves D that have no rational points, but do have rational points everywhere locally. Using information obtained from the reduction of $\mathrm{Jac}(F)$ at various primes, we might actually succeed in *proving* that $D(\mathbb{Q})$ is empty. Under the assumption that $\mathrm{Jac}(D)$ has a finite Tate–Shafarevich group, this corresponds to computing part of the Brauer–Manin obstruction according to [Sch99].

We consider the curve

$$C : (v^2 + vw - w^2)(uv + w^2) = (u^2 - v^2 - w^2)^2.$$

It is easily checked that C has points everywhere locally. Furthermore, the set of primes S described above can be taken to be $\{2\}$ and D_δ only has points everywhere locally for $\delta = 1$.

https://doi.org/10.1112/S0010437X07003314

Proof of Proposition 1.3. See [Bru04] for a transcript of the computer calculations. The fact that $D(\mathbb{Q}_p)$ and $D(\mathbb{R})$ are all non-empty can be verified with a straightforward computation. To prove that $D(\mathbb{Q}) = \emptyset$ we map D into $\mathrm{Prym}(D/C) = \mathrm{Jac}(F)$, where

$$F : y^2 = x^6 + 2x^5 + 15x^4 + 40x^3 - 10x.$$

We write ∞^+ and ∞^- for the two points above $x = \infty$ on the desingularization of F. We find that

$$\mathrm{Jac}(F)(\mathbb{Q}) = \langle \mathcal{D}_1, \mathcal{D}_2 \rangle \simeq \mathbb{Z} \times \mathbb{Z},$$

where

$$\mathcal{D}_1 = [\infty^+ - \infty^-],$$
$$\mathcal{D}_2 = \left[\left\{ x^2 + \frac{2}{5}x + \frac{1}{41} = 0, y = \frac{4683}{2050}x - \frac{281}{410} \right\} \cdot F - \kappa_F \right].$$

Considering $\mathrm{Jac}(F)$ modulo 7, we find

$$\varphi(D)(\mathbb{Q}) \subset \{\pm 9\mathcal{D}_1, \pm 22\mathcal{D}_1, \pm 23\mathcal{D}_1\} + \langle 55\mathcal{D}_1, \mathcal{D}_2 - 15\mathcal{D}_1 \rangle$$

and considering $\mathrm{Jac}(F)$ modulo 11, we find

$$\varphi(D)(\mathbb{Q}) \subset \{\pm 33\mathcal{D}_1\} + \langle 93\mathcal{D}_1, \mathcal{D}_2 + 46\mathcal{D}_1 \rangle.$$

Considering $\mathrm{Jac}(F)$ modulo 11^2, we find that the two residue classes modulo 11 lift to 11 residue class modulo

$$\langle 11 \cdot 93\mathcal{D}_1, 11 \cdot (\mathcal{D}_2 + 46\mathcal{D}_1) \rangle.$$

We combine the information modulo 11^2 and 7 and express it as congruences modulo

$$\langle 55\mathcal{D}_1, \mathcal{D}_2 - 15\mathcal{D}_1, 11 \cdot 93\mathcal{D}_1, 11 \cdot (\mathcal{D}_2 + 46\mathcal{D}_1) \rangle = \langle 11\mathcal{D}_1, \mathcal{D}_2 - 4\mathcal{D}_1 \rangle.$$

We obtain

$$\begin{array}{lcccccc} \text{from } 7 & : & \varphi(D)(\mathbb{Q}) & \subset & \{0, \pm\mathcal{D}_1, \pm 2\mathcal{D}_1\} & + & \langle 11\mathcal{D}_1, \mathcal{D}_2 - 4\mathcal{D}_1 \rangle \\ \text{from } 11^2 & : & \varphi(D)(\mathbb{Q}) & \subset & \{\pm 4\mathcal{D}_1\} & + & \langle 11\mathcal{D}_1, \mathcal{D}_2 - 4\mathcal{D}_1 \rangle. \end{array}$$

It follows that $D(\mathbb{Q}) = \emptyset$ and therefore that $C(\mathbb{Q})$ is empty as well. □

Acknowledgements

I would like to thank MSRI for their 2000 Fall special semester on explicit methods in number theory for bringing me into contact with many mathematicians. I have greatly benefited from the discussions I had with them. In particular, I would like to thank, Armand Brumer, J. Merriman, Ed Schaefer, Michael Stoll and Joe Wetherell. Furthermore, I would like to thank the anonymous referee for many constructive comments.

References

ACGH85 E. Arbarello, M. Cornalba, P. A. Griffiths and J. Harris, *Geometry of algebraic curves*, Vol. I, *Grundlehren der Mathematischen Wissenschaften*, vol. 267 (Springer, New York, 1985).

BCP97 W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, in *Computational algebra and number theory*, London, 1993, J. Symbolic Comput. **24** (1997), 235–265.

Bru02 N. R. Bruin, *Chabauty methods and covering techniques applied to generalized Fermat equations*, of CWI Tract, vol. 133 (Stichting Mathematisch Centrum Centrum voor Wiskunde en Informatica, Amsterdam, 2002).

Bru03 N. Bruin, *Chabauty methods using elliptic curves*, J. reine angew. Math. **562** (2003), 27–49.

https://doi.org/10.1112/S0010437X07003314

Bru04 N. Bruin, *Routines and transcript of computations*, http://www.cecm.sfu.ca/~bruin/g3prym (2004).

BF05 N. Bruin and E. V. Flynn, *Towers of* 2*-covers of hyperelliptic curves*, Trans. Amer. Math. Soc. **357** (2005), 4329–4347 (electronic).

BF03 N. Bruin and E. V. Flynn, *n-covers of hyperelliptic curves*, Math. Proc. Cambridge Philos. Soc. **134** (2003), 397–405.

CF96 J. W. S. Cassels and E. V. Flynn, *Prolegomena to a Middlebrow arithmetic of curves of genus 2*, London Mathematical Society, Lecture Notes Series, vol. 230 (Cambridge University Press, Cambridge, 1996).

Cay79 A Cayley, *On the bitangents of a quartic*, in *A treatise on the higher plane curves* (Chelsea, New York, 1879), 387—389.

CW32 C. Chevalley and A. Weil, *Un théorème d'arithmétiques sur les courbes algébriques*, C. R. Math. Acad. Sci. Paris **195** (1932), 570–572.

Col85 R. F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), 765–770.

Don92 R. Donagi, *The fibers of the Prym map*, in *Curves, Jacobians, and abelian varieties*, Amherst, MA, 1990, Contemporary Mathematics, vol. 136 (American Mathematical Society, Providence, RI, 1992), 55–125.

Edg94 W. L. Edge, 28 *real bitangents*, Proc. Roy. Soc. Edinburgh Sect. A **124** (1994), 729–736.

Fly90 E. V. Flynn, *The jacobian and formal group of a curve of genus* 2 *over an arbitrary ground field*, Math. Proc. Cambridge Philos. Soc. **107** (1990), 425–441.

Fly96 E. V. Flynn, *Electronic resources for curves of genus* 2, ftp://ftp.liv.ac.uk/pub/genus2/ (1996).

Fly97 E. V. Flynn, *A flexible method for applying Chabauty's theorem*, Compositio Math. **105** (1997), 79–94.

Ful69 W. Fulton, *Algebraic curves. An introduction to algebraic geometry*, Notes written with the collaboration of Richard Weiss, Mathematics Lecture Notes Series (Benjamin, New York, 1969).

Har77 R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, vol. 52 (Springer, New York, 1977).

Mum74 D. Mumford, *Prym varieties. I*, in *Contributions to analysis (a collection of papers dedicated to Lipman Bers)* (Academic Press, New York, 1974), 325–350.

Rec74 S. Recillas, *Jacobians of curves with* g_4^1*'s are the Prym's of trigonal curves*, Bol. Soc. Mat. Mexicana (2) **19** (1974), 9–13.

Sch98 E. F. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann. **310** (1998), 447–471.

Sch99 V. Scharaschkin, *Local–global problems and the Brauer–Manin obstruction*, PhD thesis, University of Michigan (1999).

Sko01 A. Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics (Cambridge University Press, Cambridge, 2001).

Ver87 A. Verra, *The fibre of the Prym map in genus three*, Math. Ann. **276** (1987), 433–448.

Wet97 J. L. Wetherell, *Bounding the number of rational points on certain curves of high rank*, PhD thesis, U. C. Berkeley, 1997.

Nils Bruin bruin@member.ams.org

Department of Mathematics, Simon Fraser University, Burnaby, BC, Canada V5A 1S6