Computing low-degree isogenies in genus 2 with the Dolgachev-Lehavi method

Benjamin Smith

COMPUTING LOW-DEGREE ISOGENIES IN GENUS 2 WITH THE DOLGACHEV–LEHAVI METHOD

BENJAMIN SMITH

ABSTRACT. Let ℓ be a prime, and $\mathscr{H}$ a curve of genus 2 over a field $\Bbbk$ of characteristic not 2 or ℓ. If S is a maximal Weil-isotropic subgroup of $\mathscr{J}_{\mathscr{H}}[\ell]$, then $\mathscr{J}_{\mathscr{H}}/S$ is isomorphic to the Jacobian $\mathscr{J}_{\mathscr{X}}$ of some (possibly reducible) curve $\mathscr{X}$. We investigate the Dolgachev–Lehavi method for constructing the curve $\mathscr{X}$, simplifying their approach and making it more explicit. The result, at least for $\ell = 3$, is an efficient and easily programmable algorithm suitable for number-theoretic calculations.

1. INTRODUCTION

Let $\ell \geq 3$ be prime, and let $\mathscr{H}$ be a curve of genus 2 over a perfect field $\Bbbk$ of characteristic not 2 or ℓ. Let $\mathscr{J}_{\mathscr{H}}$ be the Jacobian of $\mathscr{H}$, and let S be a maximal ℓ-Weil isotropic subgroup of $\mathscr{J}_H[\ell]$; since ℓ is prime, $S \cong (\mathbb{Z}/\ell\mathbb{Z})^2$. The quotient $\mathscr{J}_{\mathscr{H}}/S$ is isomorphic (as a principally polarized abelian variety) to a Jacobian $\mathscr{J}_{\mathscr{X}}$, where $\mathscr{X}$ is some curve of genus 2 (see [14]); hence, there exists an isogeny

$$\phi : \mathscr{J}_{\mathscr{H}} \to \mathscr{J}_{\mathscr{X}}$$

with kernel S (note that $\mathscr{X}$ may be reducible, in which case $\mathscr{J}_{\mathscr{X}}$ is a product of elliptic curves). Our aim is to compute an explicit form for $\mathscr{X}$ given $\mathscr{H}$ and S.

In the case $\ell = 2$, the problem is resolved by the well-known Richelot construction (see [3] and [5, Chapter 9]). For $\ell \neq 2$ and $\Bbbk$ finite, we can apply the explicit theta function-based approach of Lubicz and Robert [10], implemented in the freely-available `avIsogenies` package [1].

Alternatively, there is the algebraic-geometric approach described by Dolgachev and Lehavi [7], which computes the image of the theta divisor on $\mathscr{J}_{\mathscr{H}}$ in the Kummer surface of $\mathscr{J}_{\mathscr{X}}$. As presented in [7], this approach has two drawbacks:

(1) it is not effective for $\ell \neq 3$, and
(2) for $\ell = 3$, where theta structures are involved, it assumes $\Bbbk \subset \mathbb{C}$.

In this work, we render the kernel of the Dolgachev–Lehavi method completely explicit, with a view to computations in number theory. Our intention is to provide a sort of "user's guide" to the algorithm and its concrete implementation. For $\ell = 3$ we obtain a simple, efficient, and easily-programmable algorithm (that does not require $\Bbbk \subset \mathbb{C}$). Our algorithm retains the pleasing geometric flavour of the original, but is better-suited to everyday calculations.

2. AN OVERVIEW OF THE DOLGACHEV–LEHAVI CONSTRUCTION

We begin by briefly recalling the Dolgachev–Lehavi construction, before treating it in detail in the following sections. Suppose $\mathscr{H}/\Bbbk$, S, ϕ, and $\mathscr{X}$ are as above; we assume we are given an explicit form for $\mathscr{H}$ and S, and we want to compute an explicit form for $\mathscr{X}$. Dolgachev and Lehavi observe that if $\Theta_{\mathscr{H}}$ and $\Theta_{\mathscr{X}}$ are theta divisors on $\mathscr{J}_{\mathscr{H}}$ and $\mathscr{J}_{\mathscr{X}}$, respectively, then $\phi(\Theta_{\mathscr{H}})$ is in $|\ell\Theta_{\mathscr{X}}|$ (see [7, Proposition 2.4]); and as such the image of $\phi(\Theta_{\mathscr{H}})$ in the Kummer surface $\mathscr{K}_{\mathscr{X}} = \mathscr{J}_{\mathscr{X}}/\langle\pm 1\rangle$ is a degree-2ℓ rational curve[1] in $\mathbb{P}^3$ of arithmetic genus $(\ell^2-1)/2$ and with $(\ell^2-1)/2$ ordinary double points corresponding to the nonzero elements of S, up to sign [7, Proposition 3.1]. For $\ell = 3$ we can compute this curve *without* knowing ϕ. We express the map $\Phi : \mathscr{H} \cong \Theta_{\mathscr{H}} \to \mathscr{J}_{\mathscr{X}} \to \mathscr{K}_{\mathscr{X}} \subset \mathbb{P}^3$ as the composition of a double cover $\rho_{2\ell}$ of a rational normal curve in $\mathbb{P}^{2\ell}$ with a projection $\pi : \mathbb{P}^{2\ell} \to \mathbb{P}^3$, whose centre depends on certain secants corresponding, up to sign, to the nonzero elements of S. The images under Φ of the Weierstrass points of $\mathscr{H}$ lie on a conic $\mathscr{Q}$ in a hyperplane of $\mathbb{P}^3$; that is, a trope of $\mathscr{K}_{\mathscr{X}}$. The double cover of $\mathscr{Q}$ ramified over the Weierstrass point images is then (a quadratic twist of) $\mathscr{X}$.

3. THE DOMAIN CURVE

We suppose that $\mathscr{H}/\Bbbk$ is presented as a nonsingular projective model

$$\mathscr{H} : Y^2 = F(X,Z) = \sum_{i=0}^{6} F_i X^i Z^{6-i} \subset \mathbb{P}(1,3,1), \tag{1}$$

where F is a squarefree homogeneous sextic over $\Bbbk$ (such a model always exists when $\Bbbk$ is perfect and has characteristic not 2: see [5, §1.3]). The hyperelliptic involution of $\mathscr{H}$ is

$$\iota_{\mathscr{H}} : (X : Y : Z) \longmapsto (X : -Y : Z).$$

The divisor at infinity on $\mathscr{H}$ is

$$D_\infty = \left(1 : \sqrt{F_6} : 0\right) + \left(1 : -\sqrt{F_6} : 0\right);$$

we observe that D_∞ is defined over $\Bbbk$, fixed by $\iota_{\mathscr{H}}$, and equal to $2(1:0:0)$ if $F_6 = 0$.

The six Weierstrass points of $\mathscr{H}$ are the fixed points of $\iota_{\mathscr{H}}$; they correspond to the projective roots of the sextic F. The Weierstrass divisor $W_{\mathscr{H}}$ of $\mathscr{H}$ is the effective divisor cut out by $Y = 0$; if $F(X,Z) = \prod_{i=1}^{6}(z_i X - x_i Z)$ over $\overline{\Bbbk}$, then

$$W_{\mathscr{H}} = (x_1 : 0 : z_1) + \cdots + (x_6 : 0 : z_6).$$

Note that $W_{\mathscr{H}}$ is defined over $\Bbbk$. Finally, we fix a canonical divisor on $\mathscr{H}$, defining

$$K_{\mathscr{H}} = W_{\mathscr{H}} - 2D_\infty.$$

4. THE KERNEL OF THE ISOGENY

When defining their method for $\ell = 3$, Dolgachev and Lehavi state "unfortunately, we do not know how to input explicitly the pair $(\mathscr{H}, S)$. Instead we consider $\mathscr{H}$ with an odd theta structure." We will take a rather more middlebrow approach to the problem: we suppose that $\mathscr{H}$ is presented in the form (1), and that S is given as a collection of divisor classes on $\mathscr{H}$ expressed using an extended Mumford representation (detailed below).

Our motivation for this choice is simple: this is precisely how one computes with hyperelliptic Jacobians in computational algebra systems such as Magma [11, 2] and SAGE [13]. This choice also radically simplifies the algorithm: we can omit the theta structure calculations, and pass directly to the secant computations (short-circuiting the first four steps of the algorithm in [7, §5.1]).

Points on $\mathscr{J}_{\mathscr{H}}$ correspond to divisor classes of degree zero on $\mathscr{H}$. The Riemann–Roch theorem tells us that every nonzero degree-0 class has a unique representative in the form $P + Q - D_\infty$ (this representation fails to be unique for the trivial class, because $[P + \iota_{\mathscr{H}}(P) - D_\infty] = 0$ for every P in $\mathscr{H}(\overline{\Bbbk})$).

---

[1] By "rational curve" we mean a curve of genus 0. In all other contexts, "rational" means "defined over $\Bbbk$".

Let e be a point of $\mathcal{J}_{\mathcal{H}}$, corresponding to the divisor class $[P+Q-D_\infty]$. The effective divisor $P+Q$ is cut out by an ideal in the form $(A(X,Z), Y-B(X,Z))$, where B is a homogeneous cubic and A a homogeneous polynomial of degree $d \le 2$. The triple

$$\langle a(x), b(x), d\rangle := \langle A(x,1), B(x,1), d\rangle$$

then encodes the point e. Note that if L is an extension of $\Bbbk$, then $e = \langle a,b,d\rangle$ is in $\mathcal{J}_{\mathcal{H}}(L)$ if and only if a and b have coefficients in L.

Conversely, given a triple $\langle a,b,d\rangle$, we recover the corresponding point of $\mathcal{J}_{\mathcal{H}}$ by computing the effective divisor cut out by $(A(X,Z), Y-B(X,Z))$, where B is the degree-3 homogenization of b and A is the degree-d homogenization of a, and then subtracting $(d/2)D_\infty$. If $\mathcal{H}$ has two points at infinity (that is, if $F_6 \ne 0$) then d must be either 2 or 0. In the case where $\mathcal{H}$ has a single point at infinity (that is, when $F_6 = 0$) we always have $d = \deg a$, and the pair $\langle a, b \bmod a\rangle$ is the standard Mumford representation. The advantage of the extended representation above is that it gracefully handles the general case where there are two points at infinity.

Example 4.1. Consider the following points on the Jacobian of $\mathcal{H} : Y^2 = X^6 - Z^6$.

- 0 is represented by $\langle 1,0,0\rangle$.
- $[(1:0:1)+(-1:0:1)-D_\infty]$ is represented by $\langle x^2-1,0,2\rangle$.
- $[(1:1:0)-(1:-1:0)] = [2(1:1:0)-D_\infty]$ is represented by $\langle 1,x^3,2\rangle$.

In this article, we will assume that the points of S are all $\Bbbk$-rational. This simplifies the exposition and the computations; however, all of our calculations are symmetric in the elements of S. The algorithm should therefore be easily adapted to the case where S is rational but its elements are not.

5. The rational normal curve

The Riemann–Roch space $L(2\ell K_{\mathcal{H}})$ is a direct sum of subspaces

$$L(2\ell K_{\mathcal{H}}) = L(2\ell K_{\mathcal{H}})^+ \oplus L(2\ell K_{\mathcal{H}})^-,$$

where $\iota_{\mathcal{H}}$ acts as $+1$ on the elements of $L(2\ell K_{\mathcal{H}})^+$ and -1 on the elements of $L(2\ell K_{\mathcal{H}})^-$; writing $x = X/Z$ and $y = Y/Z^3$, we have

$$L(2\ell K_{\mathcal{H}})^+ = \left\langle x^i/y^{2\ell}\right\rangle_{i=0}^{2\ell} \quad\text{and}\quad L(2\ell K_{\mathcal{H}})^- = \left\langle x^i/y^{2\ell-1}\right\rangle_{i=0}^{2\ell-3}.$$

The space $L(2\ell K_{\mathcal{H}})^+$ corresponds to the linear system $|2\ell K_{\mathcal{H}}|^{\langle\iota_{\mathcal{H}}\rangle}$; we see immediately that it is $2\ell+1$-dimensional, and therefore defines a map

$$\rho_{2\ell} : \mathcal{H} \longrightarrow \mathcal{R}_{2\ell} \subset \mathbb{P}^{2\ell}$$

onto a curve $\mathcal{R}_{2\ell}$ in $\mathbb{P}^{2\ell}$. Fixing coordinates on $\mathbb{P}^{2\ell}$, we take $\rho_{2\ell}$ to be defined by

$$\rho_{2\ell} : (X:Y:Z) \longmapsto (U_0 : \cdots : U_{2\ell}) = (X^0 Z^{2\ell} : X Z^{2\ell-1} : \cdots : X^{2\ell-1} Z : X^{2\ell}).$$

We see that $\mathcal{R}_{2\ell}$ is a rational normal curve of degree 2ℓ in $\mathbb{P}^{2\ell}$, and $\rho_{2\ell}$ is a double cover:

$$\rho_{2\ell}(P) = \rho_{2\ell}(Q) \iff \big(P = Q \quad\text{or}\quad P = \iota_{\mathcal{H}}(Q)\big). \tag{2}$$

(Essentially, $\rho_{2\ell}$ is a composition of the canonical map of $\mathcal{H}$ and an ℓ-uple embedding.)

6. THE SECANT LINES

We adopt the following convention: if S is a set of points in some projective space $\mathbb{P}^n$, then $\langle S\rangle$ denotes the linear subspace of $\mathbb{P}^n$ generated by S.

For any pair of points P and Q on $\mathscr{H}$, we define $\mathscr{L}_{P,Q}$ to be the line in $\mathbb{P}^{2\ell}$ intersecting $\mathscr{R}_{2\ell}$ in $\rho_{2\ell}(P)+\rho_{2\ell}(Q)$; that is,

$$\mathscr{L}_{P,Q} := \begin{cases} \left\langle \rho_{2\ell}(P), \rho_{2\ell}(Q)\right\rangle & \text{if } P \notin \{Q, \iota_{\mathscr{H}}(Q)\} \\ T_{\rho_{2\ell}(P)}(\mathscr{R}_{2\ell}) & \text{otherwise.}\end{cases}$$

We can also define secant lines corresponding to nonzero Jacobian elements: if e is a nonzero point on $\mathscr{J}_{\mathscr{H}}$, then we define

$$\mathscr{L}_e := \mathscr{L}_{P,Q} \quad \text{where } e = [P+Q-D_\infty].$$

Observe that $\mathscr{L}_{P,Q} = \mathscr{L}_{P,\iota_{\mathscr{H}}(Q)} = \mathscr{L}_{\iota_{\mathscr{H}}(P),Q} = \mathscr{L}_{\iota_{\mathscr{H}}(P),\iota_{\mathscr{H}}(Q)}$ for all P and Q on $\mathscr{H}$, so

$$\mathscr{L}_e = \mathscr{L}_{-e}$$

for all e in $\mathscr{J}_{\mathscr{H}} \setminus \{0\}$.

Remark 6.1. Dolgachev and Lehavi define the secant $l_e = \left\langle \rho_{2\ell}(P_1), \rho_{2\ell}(P_2)\right\rangle$ for each nontrivial point $e = [P_1 - P_2]$ in $\mathscr{J}_{\mathscr{H}}$ (see [7, Theorem 1.1]). Our secant $\mathscr{L}_e$ is equal to l_e, because $[P_1-P_2] = [P_1 + \iota_{\mathscr{H}}(P_2) - D_\infty]$ and $\mathscr{L}_{P_1,P_2} = \mathscr{L}_{P_1,\iota_{\mathscr{H}}(P_2)}$.

The following lemma gives explicit and rational formulæ for the secants $\mathscr{L}_e$ and their intersection with arbitrary hyperplanes in $\mathbb{P}^2$. These formulæ are central to the explicit Dolgachev–Lehavi method.

Lemma 6.2. *Let $e = \langle a,b,d\rangle$ be a nonzero point of $\mathscr{J}_{\mathscr{H}}$. Let $H : \sum_{i=0}^{2\ell} H_i U_i$ be a hyperplane in $\mathbb{P}^{2\ell}$, and write $h(x) := \sum_{i=0}^{2\ell} H_i x^i$.*

(1) *If $a = 1$ and $d = 2$, then*
$$\mathscr{L}_e = \left\langle (0:\cdots:0:1:0), (0:\cdots:0:0:1)\right\rangle.$$
  (a) *If $H_{2\ell} = H_{2\ell-1} = 0$, then $\mathscr{L}_e \subset H$.*
  (b) *Otherwise, $\mathscr{L}_e \cap H = (0:\cdots:0:H_{2\ell}:-H_{2\ell-1})$.*

(2) *If $a(x) = x-\alpha$, then*
$$\mathscr{L}_e = \left\langle (0:\cdots:0:1), (1:\cdots:\alpha^{2\ell})\right\rangle.$$
  (a) *If $h(\alpha) = 0$ and $H_{2\ell} = 0$, then $\mathscr{L}_e \subset H$.*
  (b) *Otherwise, $\mathscr{L}_e \cap H = \left(H_{2\ell} : H_{2\ell}\alpha : \cdots : H_{2\ell}\alpha^{2\ell-1} : H_{2\ell}\alpha^{2\ell} - h(\alpha)\right)$.*

(3) *If $a(x) = x^2 + a_1 x + a_0$ with $a_1^2 \neq 4a_0$, then*
$$\mathscr{L}_e = \left\langle (\pi_0:\cdots:\pi_{2\ell}), (-a_1 : a_2\pi_0 : a_2\pi_1 : \cdots : a_2\pi_{2\ell-1})\right\rangle$$
  where $\pi_0 = 2$, $\pi_1 = -a_1$, and $\pi_i = -a_1\pi_{i-1} - a_2\pi_{i-2}$ for $i > 1$.
  (a) *If $a(x)$ divides $h(x)$, then $\mathscr{L}_e \subset H$.*
  (b) *Otherwise, $\mathscr{L}_e \cap H = (\gamma_0 : \cdots : \gamma_{2\ell})$ where*
$$\gamma_i = \sum_{0\le j\le 2\ell} H_j (a_2^j \sigma_{i-j} - a_2^i \sigma_{j-i})$$
  with $\sigma_k = 0$ for $k < 1$, $\sigma_1 = 1$, and $\sigma_k = -a_1\sigma_{k-1} - a_2\sigma_{k-2}$ for $k > 1$.

(4) *If $a(x) = x^2 + a_1 x + a_0$ with $a_1^2 = 4a_0$, then writing α for $-a_1/2$, we have*
$$\mathscr{L}_e = \left\langle (1:\alpha:\cdots:\alpha^{2\ell}), (0:1:2\alpha:\cdots:2\ell\alpha^{2\ell-1})\right\rangle.$$
  (a) *If $a(x)$ divides $h(x)$, then $\mathscr{L}_e \subset H$.*
  (b) *Otherwise, $\mathscr{L}_e \cap H = (\gamma_0 : \cdots : \gamma_{2\ell})$ where $\gamma_i = i\alpha^{i-1}h(\alpha) - \alpha^i h'(\alpha)$.*

Proof. In general, given points $\alpha = (\alpha_0 : \cdots : \alpha_{2\ell})$ and $\beta = (\beta_0 : \cdots : \beta_{2\ell})$ in $\mathbb{P}^{2\ell}$, we have

$$H \cap \mathscr{L}_{\alpha,\beta} = (A\beta_0 - B\alpha_0 : \cdots : A\beta_{2\ell} - B\alpha_{2\ell})$$

where $A = \sum_{i=0}^{2\ell} H_i\alpha_i$ and $B = \sum_{i=0}^{2\ell} H_i\beta_i$; if $A = B = 0$, then $\mathscr{L}_{\alpha,\beta} \subset H$ (and the point above is not defined). In the following, we suppose $e = [P + Q - D_\infty]$; we have $e \neq 0$, so we can suppose $P \neq \iota_{\mathscr{H}}(Q)$.

In case (1), both P and Q are at infinity; hence $\rho_{2\ell}(P) = \rho_{2\ell}(Q) = (0 : \cdots : 0 : 1)$, and our expression for $\mathscr{L}_e$ gives generators for the tangent to $\mathscr{R}_{2\ell}$ at $(0 : \cdots : 0 : 1)$. The intersection formula follows immediately.

In case (2), we have $P = (1 : 0 : 0)$ and $Q = (\alpha : \pm\sqrt{F(\alpha,1)} : 1)$, so $\rho_{2\ell}(P) = (0 : \cdots : 0 : 1)$ and $\rho_{2\ell}(Q) = (1 : \alpha : \cdots : \alpha^{2\ell})$. The intersection formula follows immediately.

In case (3), we have $P = (\alpha : \pm\sqrt{F(\alpha,1)} : 1)$ and $Q = (\beta : \pm\sqrt{F(\beta,1)} : 1)$ with $\alpha \neq \beta$, $\alpha + \beta = -a_1$, and $\alpha\beta = a_2$; so $\rho_{2\ell}(P) = (1 : \alpha : \cdots : \alpha^{2\ell})$ and $\rho_{2\ell}(Q) = (1 : \beta : \cdots : \beta^{2\ell})$. If we take

$$T = (2 : \alpha + \beta : \cdots : \alpha^{2\ell} + \beta^{2\ell}) \quad \text{and} \quad S = (\alpha + \beta : 2\beta\alpha : \cdots : \alpha\beta^{2\ell} + \beta\alpha^{2\ell}),$$

then we easily verify that $\mathscr{L}_{P,Q} = \mathscr{L}_{T,S}$; it is a straightforward exercise with symmetric polynomials to show that $\alpha^i + \beta^i = \pi_i$ for $0 \leq i \leq 2\ell$ and $\alpha\beta^i + \beta\alpha^i = a_2\pi_{i-1}$ for $i > 0$, whence our formula for $\mathscr{L}_e$. The intersection $H \cap \mathscr{L}_e$ is

$$H \cap \mathscr{L}_{P,Q} = (h(\alpha) - h(\beta) : h(\alpha)\beta - h(\beta)\alpha : \cdots : h(\alpha)\beta^{2\ell} - h(\beta)\alpha^{2\ell});$$

it is another straightforward exercise to show that

$$\alpha^j\beta^i - \beta^j\alpha^i = (\beta - \alpha)(a_2^j\sigma_{i-j} - a_2^i\sigma_{j-i}),$$

so $h(\alpha)\beta^i - h(\beta)\alpha^i = \sum_{j=0}^{2\ell} H_j(\beta-\alpha)(a_2^j\sigma_{i-j} - a_2^i\sigma_{j-i}) = (\beta-\alpha)\gamma_i$ for $0 \leq i \leq 2\ell$, and thus $H \cap \mathscr{L}_e = (\gamma_0 : \cdots : \gamma_{2\ell})$.

In case (4), we have $P = Q = (\alpha : \pm\sqrt{F(\alpha,1)} : 1)$; our expression for $\mathscr{L}_e$ gives generators for the tangent to $\mathscr{R}_{2\ell}$ at $\rho_{2\ell}(P) = (1 : \alpha : \cdots : \alpha^{2\ell})$. The intersection formula follows. □

7. THE WEIERSTRASS SUBSPACE

Since $\mathscr{R}_{2\ell}$ is a rational normal curve of degree 2ℓ, any $2\ell + 1$ distinct points on $\mathscr{R}_{2\ell}$ are linearly independent. In particular, the images of the six Weierstrass points of $\mathscr{H}$ under $\rho_{2\ell}$ are linearly independent because $\ell \geq 3$. In view of (2) the images are distinct, so the subspace

$$W := \langle \rho_{2\ell}(W_{\mathscr{H}}) \rangle \subset \mathbb{P}^{2\ell}$$

is five-dimensional.

Definition 7.1. For each $0 \leq i \leq 2\ell - 6$, we define

$$W_i := \sum_{j=0}^{6} F_j U_{i+j}.$$

Lemma 7.2. *The space W is*

$$W = \bigcap_{i=0}^{2\ell-6} V(W_i) = V(\{W_i : 0 \leq i \leq 2\ell - 6\}).$$

Proof. Each hyperplane $V(W_i)$ contains W, since $W_i \circ \rho_{2\ell} = X^i Z^{2\ell-6-i} F(X,Z)$. But the W_i are linearly independent, so the intersection $\bigcap_{i=0}^{2\ell-6} V(W_i)$ is 5-dimensional, and hence equal to W. □

8. The theorem of Dolgachev and Lehavi

We are now ready to state the main theorem behind the Dolgachev–Lehavi method.

Theorem 8.1 ([7, Theorem 1.1])**.** *There exists a unique hyperplane $H \subset \mathbb{P}^{2\ell}$ such that*

1. *H contains W, and*
2. *the intersection points of H with the secants $\mathscr{L}_e$ for each nonzero e in S are contained in a subspace N of codimension 3 in H.*

The image of the Weierstrass divisor under the projection $\mathbb{P}^{2\ell} \to \mathbb{P}^3$ with centre N lies on a conic $\mathscr{Q}$ (which may be reducible), and the double cover of $\mathscr{Q}$ ramified over this divisor is a stable curve $\mathscr{X}$ of arithmetic genus 2 such that $\mathscr{J}_{\mathscr{X}} \cong \mathscr{J}_{\mathscr{H}}/S$.

It is crucial to note that Theorem 8.1 is not constructive: it does not in itself yield the hyperplane H, nor the centre N of the projection to $\mathbb{P}^3$. In [7, §3.4] it is noted that H is defined by $\phi^*(\Theta_{\mathscr{X}})$, but in our application we do not yet have an expression for ϕ or $\Theta_{\mathscr{X}}$.

In the case $\ell = 3$, we are saved by a happy coincidence: $2\ell - 1 = 5$, so $H = W$ (we return to this case in §11 below). For $\ell > 3$, we must compute H in some other way; Lemma 8.2, an easy corollary of Lemma 7.2, characterizes the possible hyperplanes.

Lemma 8.2. *The linear system of all hyperplanes in $\mathbb{P}^{2\ell}$ containing W is generated by the $2\ell-5$ hyperplanes $V(W_i)$ for $0 \le i \le 2\ell-6$. That is, if $H \supset W$ is a hyperplane in $\mathbb{P}^{2\ell}$, then*

$$H = V(\alpha_0 W_0 + \cdots + \alpha_{2\ell-6} W_{2\ell-6})$$

for some $(\alpha_0 : \cdots : \alpha_{2\ell-6})$ in $\mathbb{P}^{2\ell-6}(\Bbbk)$.

In view of Lemma 8.2, a naïve approach to computing H for $\ell > 3$ could involve taking a generic $H = V\left(\sum_{i=0}^{2\ell-6} \alpha_i W_i\right)$, and computing its intersection with the secants $\mathscr{L}_e$. This yields $(\ell^2-1)/2$ points whose coordinates are linear expressions in the α_i. We could then solve for the values of α_i by computing the zero locus of the $(2\ell-2)\times(2\ell-2)$ minors of the matrix formed by the intersections $H \cap \mathscr{L}_e$; but each minor is still a degree-$(2\ell-2)$ polynomial in $2\ell-5$ variables, and the number of minors is exponential in ℓ. Alternatively, we could take a generic set of linear equations determining N inside the generic H; requiring that this centre intersects any one of the $(\ell^2-1)/2$ secants imposes $O(\ell^4)$ quartic polynomial conditions on the $O(\ell)$ unknowns.

In each approach the system is highly overdetermined, and with a clever choice of minors we might hope to get lucky and find a solutions for toy examples. However, both approaches already represent a significant undertaking for $\ell = 5$, even over finite fields; they are totally impractical for larger ℓ and for infinite fields.

We continue the treatment for general ℓ in §9 and §10, supposing that an equation for H has been found; without such an equation, the `avIsogenies` package [1] represents a much more sensible approach for $\ell \ge 5$. For $\ell = 3$, the Dolgachev–Lehavi method is as highly practical as it is interesting; we specialize to this case in §11 and §12.

9. From theory to practice

To compute $\mathscr{X}$ via Theorem 8.1, we must compute the map

$$\Phi := \pi \circ \rho_{2\ell} : \mathscr{H} \to \mathbb{P}^3,$$

where $\pi : \mathbb{P}^{2\ell} \to \mathbb{P}^3$ is the projection with centre N. Suppose that we have an equation

$$H : \sum_i \alpha_i W_i = 0$$

for H. We can then apply Lemma 6.2 to compute the centre $N = \langle \mathscr{L}_e \cap H : e \in S \setminus \{0\}\rangle$. Since $N \subset H$, we may compute $v_{0,0},\ldots,v_{0,2\ell},v_{1,0},\ldots,v_{1,2\ell},v_{2,0},\ldots,v_{2,2\ell}$ in $\Bbbk$ such that

$$N = V\left(\sum_{i=0}^{2\ell} v_{0,i}U_i,\ \sum_{i=0}^{2\ell} v_{1,i}U_i,\ \sum_{i=0}^{2\ell} v_{2,i}U_i,\ \sum_{i=0}^{2\ell-6} \alpha_i W_i\right).$$

(This amounts to computing the kernel of the matrix whose rows are formed by the coordinates of the $\mathscr{L}_e \cap H$; the choice of $\sum_{i=0}^{6} \alpha_i W_i$ is convenient later in the procedure.) Fixing coordinates on $\mathbb{P}^3$, the projection π with centre N is defined by

$$\pi : (U_0 : \cdots : U_{2\ell}) \longmapsto (V_0 : V_1 : V_2 : V_3) = \left(\sum_{i=0}^{2\ell} v_{0,i}U_i,\ \sum_{i=0}^{2\ell} v_{1,i}U_i,\ \sum_{i=0}^{2\ell} v_{2,i}U_i,\ \sum_{i=0}^{2\ell-6} \alpha_i W_i\right),$$

and the composed map $\Phi = \pi \circ \rho_{2\ell}$ is

$$\Phi : (X : Y : Z) \longmapsto (V_0 : V_1 : V_2 : V_3) = \big(\Phi_0(X,Z) : \Phi_1(X,Z) : \Phi_2(X,Z) : \Phi_3(X,Z)\big),$$

where

$$\Phi_0 := \sum_{i=0}^{2\ell} v_{0,i}X^iZ^{2\ell-i}, \quad \Phi_2 := \sum_{i=0}^{2\ell} v_{1,i}X^iZ^{2\ell-i}, \quad \Phi_2 := \sum_{i=0}^{2\ell} v_{2,i}X^iZ^{2\ell-i},$$

and

$$\Phi_3 := \sum_{i=0}^{2\ell-6} \alpha_i X^i Z^{2\ell-6-i} F(X,Z).$$

The image of Φ is a rational curve of degree 2ℓ in $\mathbb{P}^3$. It lies on the Kummer surface $\mathscr{K}_{\mathscr{X}}$ of the unknown codomain Jacobian $\mathscr{J}_{\mathscr{X}}$, and is therefore the intersection of a quadric and a cubic hypersurface in $\mathbb{P}^3$ (see [9, Chapter XIII]):

$$\Phi(\mathbb{P}^1) = \tilde{\mathscr{Q}} \cap \tilde{\mathscr{C}} \quad \text{where} \quad \tilde{\mathscr{Q}} = V\big(\tilde{Q}(V_0,V_1,V_2,V_3)\big) \quad \text{and} \quad \tilde{\mathscr{C}} = V\big(\tilde{C}(V_0,V_1,V_2,V_3)\big)$$

for some forms $\tilde{Q}$ and $\tilde{C}$ of degree 2 and 3, respectively. The forms $\tilde{Q}$ and $\tilde{C}$ generate the elimination ideal

$$\big(\tilde{Q},\tilde{C}\big) = (V_0 - \Phi_0, V_1 - \Phi_1, V_2 - \Phi_2, V_3 - \Phi_3) \cap \Bbbk[V_0,V_1,V_2,V_3];$$

note that $\tilde{Q}$ is uniquely determined, and $\tilde{C}$ is determined modulo (V_0Q, V_1Q, V_2Q, V_3Q).

The Weierstrass points of $\mathscr{H}$ map into the hyperplane $V_3 = 0$, which we identify with $\mathbb{P}^2$. (This simplification motivates our choice of Φ_3.) Theorem 8.1 asserts that a conic $\mathscr{Q}$ passes through the six images, and indeed

$$\mathscr{Q} = V(Q(V_0,V_1,V_2)) \subset \mathbb{P}^2, \quad \text{where} \quad Q(V_0,V_1,V_2) = \tilde{Q}(V_0,V_1,V_2,0).$$

The image of the Weierstrass divisor under Φ is therefore $\mathscr{Q} \cap \mathscr{C}$, where

$$\mathscr{C} = V(C(V_0,V_1,V_2)) \subset \mathbb{P}^2 \quad \text{with} \quad C(V_0,V_1,V_2) = \tilde{C}(V_0,V_1,V_2,0).$$

We are more interested in the forms Q and C than in $\tilde{Q}$ and $\tilde{C}$, and it is a simple matter to interpolate them. For Q, we compute the six quintic polynomials $\Phi_i\Phi_j(x,1) \bmod F(x,1)$ for $0 \le i \le j \le 2$; the unique linear relation between them (and between the $v_{i,0}v_{j,0}$ if $F_6 = 0$) yields the coefficients of Q. Similarly, to find C we compute the ten quintics $\Phi_i\Phi_j\Phi_k(x,1) \bmod F(x,1)$ for $0 \le i \le j \le k \le 2$; any one of the linear relations between them (and the $v_{i,0}v_{j,0}v_{k,0}$ if $F_6 = 0$) gives an equation for a valid cubic C.

10. THE CODOMAIN CURVE

The data $(\mathscr{Q}, \mathscr{Q} \cap \mathscr{C})$ specifies a genus 2 curve $\mathscr{X}$ (up to a quadratic twist) as a double cover of $\mathscr{Q}$ ramified over the six points of $\mathscr{Q} \cap \mathscr{C}$. This is the output of the Dolgachev–Lehavi algorithm and of Theorem 8.1, and it is sufficient for computing isomorphism invariants of $\mathscr{X}$ (see, for example, [4] and [12]).

In some situations, however, we would like to derive a defining equation for $\mathscr{X}$ itself. When $\mathscr{Q}$ is nonsingular, we recover a hyperelliptic curve; in the degenerate case where $\mathscr{Q}$ is singular, we recover a union of two elliptic curves $\mathscr{X}_+$ and $\mathscr{X}_-$, which are generally defined over a quadratic extension of $\Bbbk$ (in which case they are Galois conjugates). The procedure is essentially standard (cf. [4, §2]), but we recall it here for completeness.

Algorithm 10.1. Computes a (possibly reducible) genus 2 curve representing a double cover of a given plane conic ramified over the intersection with a plane cubic.

Input: A plane conic $\mathscr{Q} : Q(V_0, V_1, V_2) = 0$ and cubic $\mathscr{C} : C(V_0, V_1, V_2) = 0$.

Output: A genus 2 curve $\mathscr{X}$ forming a double cover of $\mathscr{Q}$ ramified over $\mathscr{Q} \cap \mathscr{C}$. If $\mathscr{Q}$ is singular, then $\mathscr{X}$ will be a one-point union of elliptic curves $\mathscr{X}_+$ and $\mathscr{X}_-$, with $\mathscr{X}_\pm$ ramified over P_0 and $\mathscr{C} \cap \mathscr{L}_\pm$ where $\mathscr{Q} = \mathscr{L}_+ + \mathscr{L}_-$ and $P_0 = \mathscr{L}_+ \cap \mathscr{L}_-$.

1: Let M be the matrix defined by

$$M := \begin{pmatrix} 2q_{0,0} & q_{0,1} & q_{0,2} \\ q_{0,1} & 2q_{1,1} & q_{1,2} \\ q_{0,2} & q_{1,2} & 2q_{2,2} \end{pmatrix}, \quad \text{where} \quad \sum_{0 \le i \le j \le 2} q_{i,j} V_i V_j = Q(V_0, V_1, V_2).$$

2: If $\det(M) = 0$, then $\mathscr{Q}$ is singular.

2a: Compute a diagonal matrix $D = \operatorname{diag}(a, b, 0)$ and an invertible matrix T such that $M = TDT^{-1}$.

2b: Set $\delta = \sqrt{-a/b}$, and define homogeneous cubics $C_+(X,Z)$ and $C_-(X,Z)$ by $C_\pm := C\big((t_{00} \pm \delta t_{01})Z + t_{02}X, (t_{10} \pm \delta t_{11})Z + t_{12}X, (t_{20} \pm \delta t_{21})Z + t_{22}X\big)$ where

$$\begin{pmatrix} t_{00} & t_{01} & t_{02} \\ t_{10} & t_{11} & t_{12} \\ t_{20} & t_{21} & t_{22} \end{pmatrix} = T.$$

2c: Define elliptic curves $\mathscr{X}_+$ and $\mathscr{X}_-$ over $\Bbbk(\delta)$ in $\mathbb{P}(2,3,2)$ by

$$\mathscr{X}_+ : Y^2 = C_+(X,Z) \quad \text{and} \quad \mathscr{X}_- : Y^2 = C_-(X,Z),$$

and return the union of $\mathscr{X}_+$ and $\mathscr{X}_-$ identifying the points at infinity.

3: Otherwise, $\mathscr{Q}$ is nonsingular.

3a: Compute a rational point $P = (\alpha_0 : \alpha_1 : \alpha_2)$ in $\mathscr{Q}(\Bbbk)$ (see Remark 10.2).

3b: Let $\pi : \mathbb{P}^1 \to \mathscr{Q}$ be the corresponding rational parametrization, defined by

$$\pi : (X : Z) \longmapsto (V_0 : V_1 : V_2) = (P_0(X,Z) : P_1(X,Z) : P_2(X,Z))$$

(the P_i are quadratic forms).

3c: Return $\mathscr{X} : Y^2 = C(P_0(X,Z), P_1(X,Z), P_2(X,Z))$.

Remark 10.2. Step 3a of Algorithm 10.1 requires us to compute a $\Bbbk$-rational point P on the conic $\mathscr{Q}$. If $\mathscr{H}$ has a rational Weierstrass point W_0, then we may take $P = \Psi(W_0)$. Generically, however, $\mathscr{H}$ has no rational Weierstrass points, and then we are obliged to search for a rational point on $\mathscr{Q}$. We are guaranteed that such a rational point exists (cf. [12, Lemme 1]). Over a finite field, finding a rational point is straightforward; over the rationals, we can apply (for example) the Cremona–Rusin algorithm [6].

11. THE ALGORITHM FOR $\ell = 3$

Consider the special case $\ell = 3$. The map $\rho_6 : \mathscr{H} \to \mathscr{R}_6 \subset \mathbb{P}^6$ is defined by

$$\rho_6 : (X : Y : Z) \longmapsto (U_0 : U_1 : \cdots : U_5 : U_6) = \left(Z^6 : XZ^5 : \cdots : X^5 Z : X^6\right).$$

The hyperplane H of Theorem 8.1 contains $W = \langle \rho_6(W_{\mathscr{H}}) \rangle$ by definition; but $\dim H = \dim W = 5$, so $H = W$. Applying Lemma 7.2, we find

$$H = V(W_0) = V\left(\sum_{i=0}^{6} F_i U_i\right) \subset \mathbb{P}^6. \tag{3}$$

This allows us to simplify Lemma 6.2 for the case $\ell = 3$.

Proposition 11.1. *If $e = \langle a, b, d\rangle$ is a nonzero 3-torsion point of $\mathscr{J}_{\mathscr{H}}$, then*

$$H \cap \mathscr{L}_e = \left(\gamma_0(e) : \cdots : \gamma_6(e)\right),$$

where the γ_i are defined as follows:

(1) *If $a = 1$, then $\gamma_i(e) = 0$ for $0 \le i < 5$, with $\gamma_5(e) = F_6$ and $\gamma_6(e) = -F_5$.*
(2) *If a is linear, then $\gamma_i(e) = 0$ for $0 \le i < 6$, and $\gamma_6(e) = 1$.*
(3) *If $a(x) = x^2 + a_1 x + a_0$ with $a_1^2 \ne 4a_0$, then*

$$\gamma_i(e) = \sum_{j=0}^{6} F_j (a_2^j \sigma_{i-j} + a_2^i \sigma_{j-i}) \quad \text{for } 0 \le i \le 6$$

with $\sigma_k = 0$ for $k < 1$, $\sigma_1 = 1$, and $\sigma_k = -a_1\sigma_{k-1} - a_2\sigma_{k-2}$ for $k > 1$.
(4) *If $a(x) = x^2 + a_1 x + a_0$ with $a_1^2 = 4a_0$, then*

$$\gamma_i(e) = \sum_{j=0}^{6} (i-j) F_j (-a_1/2)^{i+j-1} \quad \text{for } 0 \le i \le 6.$$

Proof. This follows immediately from Lemma 6.2 on setting $H = V\left(\sum_{i=0}^{6} F_i U_i\right)$ and noting that $a(x)$ cannot divide $h(x) = \sum_{i=0}^{6} F_i x^i$ (since otherwise e would have order 2). □

We are now ready to present a version of the Dolgachev–Lehavi algorithm for $\ell = 3$ based on the extended Mumford representation. The algorithm requires only elementary matrix algebra and polynomial arithmetic, and should be easily implemented in most computational algebra systems.

Algorithm 11.2. A streamlined Dolgachev–Lehavi-style algorithm for $\ell = 3$.

Input: A genus 2 curve $\mathscr{H} : Y^2 = F(X, Z) = \sum_{i=0}^{6} F_i X^i Z^{6-i}$ over $\mathbb{k}$ and a maximal Weil-isotropic subgroup S of $\mathscr{J}_{\mathscr{H}}[3]$, its elements defined over $\mathbb{k}$ and presented as in §4.

Output: A genus 2 curve $\mathscr{X}/\mathbb{k}$ such that there exists an isogeny $\phi : \mathscr{J}_{\mathscr{H}} \to \mathscr{J}_{\mathscr{X}}$ with kernel S (the curve $\mathscr{X}$ is computed up to a quadratic twist, so the isogeny may only be defined over a quadratic extension of $\mathbb{k}$).

1: Compute a minimal subset $S^{\pm}$ of S such that $S = \{e : e \in S^{\pm}\} \cup \{-e : e \in S^{\pm}\} \cup \{0\}$ (then $\{\mathscr{L}_e : e \in S^{\pm}\} = \{\mathscr{L}_e : e \in S \setminus \{0\}\}$; this avoids redundancy in Steps 2 and 3).

2: For each e in $S^{\pm}$, compute the vector $v_e = (\gamma_0(e), \ldots, \gamma_6(e))$ using the formulæ in Proposition 11.1.

3: Compute vectors $n_i = (v_{i,0}, \ldots, v_{i,6})$ such that $\{n_0, n_1, n_2, (F_j : 0 \le j \le 6)\}$ is a basis for the (left) kernel of the 7×4 matrix $(v_e^t : e \in S^{\pm})$. Set

$$\Phi_i = \sum_{j=0}^{6} v_{i,j} X^j Z^{6-j} \quad \text{for } 0 \le i \le 2.$$

4: For each $0 \le i \le j \le 2$, compute the vector $r_{i,j}$ of length 6 whose n^{th} entry is the coefficient of x^{n-1} in $(\Phi_i\Phi_j)(x,1) \bmod F(x,1)$. If $F_6 = 0$, then we take the 6^{th} entry to be $v_{i,0}v_{j,0}$: this allows us to correctly interpolate through the image of the Weierstrass point at infinity.

5: Compute a generator $(q_{i,j} : 0 \le i \le j \le 2)$ for the (left) kernel of the 6×6 matrix whose rows are the $r_{i,j}$ for $0 \le i \le j \le 2$. Set

$$Q(V_0,V_1,V_2) := q_{0,0}V_0^2 + q_{0,1}V_0V_1 + q_{0,2}V_0V_2 + q_{1,1}V_1^2 + q_{1,2}V_1V_2 + q_{2,2}V_2^2.$$

6: For each $0 \le i \le j \le k \le 2$, compute the vector $s_{i,j,k}$ of length 6 whose n^{th} entry is the coefficient of x^{n-1} in $(\Phi_i\Phi_j\Phi_k)(x,1) \bmod F(x,1)$. If $F_6 = 0$, then we take the 6^{th} entry to be $v_{i,0}v_{j,0}v_{k,0}$.

7: Compute any nontrivial element $(c_{i,j,k} : 0 \le i \le j \le k \le 2)$ of the (left) kernel of the 10×6 matrix whose rows are the $s_{i,j,k}$ for $0 \le i \le j \le k \le 2$, and set

$$C(V_0,V_1,V_2) := \sum_{0\le i\le j\le k\le 2} c_{i,j,k}V_iV_jV_k.$$

8: Return the result $\mathscr{X}$ of Algorithm 10.1 applied to $\mathscr{Q} = V(Q)$ and $\mathscr{C} = V(C)$.

12. THE ALGORITHM IN PRACTICE

We conclude with an example for $\ell = 3$. To avoid a visually overwhelming mass of coefficients, we will work over a small finite field; the curve was chosen at random.

Consider the genus 2 curve over $\mathbb{F}_{997}$ defined by

$$\mathscr{H} : Y^2 = X^6 + 113X^5Z + 99X^4Z^2 + 363X^3Z^3 + 64X^2Z^4 + 503XZ^5 + 630Z^6.$$

Computing the zeta function of $\mathscr{H}$ (using Magma), we see that its Weil polynomial is

$$P(T) = T^4 - 31T^3 + 54T^2 - 30907T + 994009,$$

so $\mathscr{J}_{\mathscr{H}}$ is absolutely simple by the Howe–Zhu criterion [8, Theorem 6]. The elements $D_1 = \langle x^2 + 392x + 208, 579x + 603, 2\rangle$ and $D_2 = \langle x^2 + 48x + 527, 918x + 832, 2\rangle$ of $\mathscr{J}_{\mathscr{H}}$ have order 3, and $S = \langle D_1, D_2\rangle$ is a maximal 3-Weil isotropic subgroup of $\mathscr{J}_{\mathscr{H}}[3]$.

Applying Algorithm 11.2, we may take

$$S^{\pm} = \left\{ \begin{matrix} \langle x^2+392x+208, 579x+603, 2\rangle, \langle x^2+48x+527, 918x+832, 2\rangle, \\ \langle x^2+428x+880, 252x+901, 2\rangle, \langle x^2+348x+292, 596x+269, 2\rangle \end{matrix} \right\}$$

in Step 1. Equation (3) shows that the hyperplane $H \subset \mathbb{P}^6$ is defined by

$$H : 630U_0 + 503U_1 + 64U_2 + 363U_3 + 99U_4 + 113U_5 + U_6 = 0,$$

so the matrix in Step 3 is

$$\begin{pmatrix} 234 & 319 & 906 & 896 \\ 780 & 16 & 29 & 754 \\ 500 & 565 & 703 & 398 \\ 680 & 329 & 823 & 248 \\ 324 & 68 & 779 & 868 \\ 742 & 416 & 468 & 392 \\ 664 & 395 & 698 & 952 \end{pmatrix};$$

computing kernel vectors, we take

$$\begin{aligned} \Phi_0 &= 121X^6 + 742X^5Z + 549X^4Z^2 + XZ^5, \\ \Phi_1 &= 285X^6 + 642X^5Z + 332X^4Z^2 + X^2Z^4, \\ \Phi_2 &= 889X^6 + 701X^5Z + 454X^4Z^2 + X^3Z^3. \end{aligned}$$

The quadratic form of Step 5 is

$$Q(V_0,V_1,V_2) = V_0^2 + 52V_0V_1 + 361V_1^2 + 548V_0V_2 + 715V_1V_2 + 296V_2^2,$$

and we may take the cubic form in Step 7 to be

$$C(V_0,V_1,V_2) = V_0^3 + 167V_1^3 + 149V_0V_1V_2 + 836V_1^2V_2 + 885V_0V_2^2 + 538V_1V_2^2 + 294V_2^3.$$

We now apply Algorithm 10.1 to $\mathscr{Q} : Q(V_0,V_1,V_2) = 0$ and $\mathscr{C} : C(V_0,V_1,V_2) = 0$. The conic $\mathscr{Q}$ is nonsingular, and $\mathscr{H}$ has a rational Weierstrass point $(-76:0:1)$ mapping to the point $(-36:-80:1)$ on $\mathscr{Q}$. The associated parametrization $\mathbb{P}^1 \to \mathscr{Q}$ is defined by

$$(X:Z) \longmapsto (36X^2 + 781XZ + 109Z^2 : 80X^2 + 865XZ + 17Z^2 : 996X^2 + 945XZ + 636Z^2);$$

substituting its defining polynomials into C, we find that $\mathscr{X}$ has a model

$$\mathscr{X} : Y^2 = 118X^5Z + 183X^4Z^2 + 613X^3Z^3 + 35X^2Z^4 + 174XZ^5 + 474Z^6.$$

In fact, this is the quadratic twist of the true $\mathscr{X}$: explicit calculation shows that its Weil polynomial is $P(-T)$.

REFERENCES

[1] G. Bisson, R. Cosset, and D. Robert, *avIsogenies: a library for computing isogenies between abelian varieties.* Available from `http://avisogenies.gforge.inria.fr/`

[2] W. Bosma, C. Playoust, and J. J. Cannon, *The Magma algebra system. I. The user language.* J. Symbolic Comput. **24** (1997), 235–265

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

[4] G. Cardona and J. Quer, *Field of moduli and field of definition for curves of genus 2.* In *Computational aspects of algebraic curves*, Lecture Notes Ser. Comput. **13**, 71–83. World Sci. Publ., Hackensack, NJ, 2005.

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

[6] J. E. Cremona and D. Rusin, *Efficient solution of rational conics.* Math. Comp. **72** issue 473 (2003), 1417–1441

[7] I. Dolgachev and D. Lehavi, *On isogenous principally polarized Abelian surfaces.* In *Curves and abelian varieties*, Contemp. Math. **465** (2008), 51–69

[8] E. W. Howe and H. J. Zhu, *On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field.* J. Number Theory **92** (2002), 139–163

[9] R. W. H. T. Hudson, *Kummer's quartic surface.* Cambridge University Press, Cambridge (1990)

[10] D. Lubicz and D. Robert, *Computing isogenies between Abelian Varieties.* Preprint (2010), available from `http://hal.inria.fr/hal-00446062/en`

[11] The Magma computational algebra system. `http://magma.maths.usyd.edu.au`

[12] J.-F. Mestre, *Construction de courbes de genre 2 à partir de leurs modules.* In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, Progr. Math. **94**, 313–334. BirkhÃd'user Boston, Boston, MA, 1991.

[13] W. A. Stein et al., *Sage Mathematics Software.* The Sage Development Team, `http://www.sagemath.org/`

[14] A. Weil, *Zum Beweis des Torellischen Satzes.* Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa. **1957** (1957), 33–53

INRIA SACLAY–ÎLE-DE-FRANCE AND LABORATOIRE D'INFORMATIQUE DE L'ÉCOLE POLYTECHNIQUE (LIX), 91128 PALAISEAU CEDEX, FRANCE