LMS J. Comput. Math. 17 (Special issue A) (2014) 112–127 © 2014 Author
doi:10.1112/S1461157014000217

Minimal models for 6-coverings of elliptic curves

Tom Fisher

Abstract

In this paper we give a new formula for adding 2-coverings and 3-coverings of elliptic curves that avoids the need for any field extensions. We show that the 6-coverings obtained can be represented by pairs of cubic forms. We then prove a theorem on the existence of such models with integer coefficients and the same discriminant as a minimal model for the Jacobian elliptic curve. This work has applications to finding rational points of large height on elliptic curves.

1. *Introduction*

Let E be an elliptic curve defined over a number field K. For each $n \geqslant 2$ there is an exact sequence

$$0 \to E(K)/nE(K) \to \mathrm{Sel}^{(n)}(E/K) \to Ш(E/K)[n] \to 0$$

where the n-Selmer group $\mathrm{Sel}^{(n)}(E/K)$ is finite and effectively computable. It gives information about both the Mordell–Weil group $E(K)$ and the Tate–Shafarevich group $Ш(E/K)$. Elements of the Selmer group may be represented by n-coverings of E. Coverings $\pi : C \to E$ and $\pi' : C' \to E$ are isomorphic if there is an isomorphism $\alpha : C \to C'$ with $\pi = \pi' \circ \alpha$. An n-covering $\pi : C \to E$ is then, by definition, a twist of the trivial n-covering $[n] : E \to E$, where $[n]$ is multiplication-by-n on E. In particular, C is a smooth curve of genus 1 defined over K. The n-Selmer group $\mathrm{Sel}^{(n)}(E/K)$ is the set of K-isomorphism classes of n-coverings for which C has points everywhere locally. A theorem of Cassels [**10**] tells us that every such n-covering admits a K-rational divisor of degree n, and so (for $n \geqslant 3$) may be embedded in $\mathbb{P}^{n-1}$ as a curve of degree n.

If m and n are coprime integers then it is immediate that

$$\mathrm{Sel}^{(mn)}(E/K) \cong \mathrm{Sel}^{(m)}(E/K) \times \mathrm{Sel}^{(n)}(E/K).$$

Moreover, if we are given an m-covering $C_m \to E$ and an n-covering $C_n \to E$ then the fibre product $C_{mn} = C_m \times_E C_n$ is an mn-covering. We would like to realize these constructions explicitly, that is, given equations for C_m and C_n as curves of degree m and n in $\mathbb{P}^{m-1}$ and $\mathbb{P}^{n-1}$, find equations for C_{mn} as a curve of degree mn in $\mathbb{P}^{mn-1}$. This problem has applications to finding generators of $E(K)$ of large height. The solution in [**14**] in the case $(m, n) = (2, 3)$ involves calculations in an extension of the number field K, typically of degree 9. In § 2 we give a new formula that removes the need for any field extensions.

For the application to point searching, it is important that we give equations for our n-coverings with respect to a good choice of coordinates on $\mathbb{P}^{n-1}$. This is both to make the equations have smaller coefficients, and the rational points we are searching for have smaller height. This problem can be solved by a combination of minimisation and reduction, as described in [**13**] in the cases $n = 2, 3, 4$ and [**17**] in the case $n = 5$. By minimisation we mean changing coordinates so that the data defining our n-covering still has integer coefficients, yet prime factors are removed where possible from some suitably defined discriminant.

Received 27 February 2014; revised 23 May 2014.

2010 Mathematics Subject Classification 11G05, 14H52 (primary).

Contributed to the Algorithmic Number Theory Symposium XI, GyeongJu, Korea, 6–11 August 2014.

https://doi.org/10.1112/S1461157014000217 Published online by Cambridge University Press

In this paper we represent 6-coverings $C \subset \mathbb{P}^5$ by pairs of cubic forms defining the secant variety $\operatorname{Sec} C$. We then define a discriminant function, and prove results on minimisation analogous to those in the papers cited above. It turns out that if we add minimal models for a 2-covering and a 3-covering, using the formula in § 2, then the model we get for a 6-covering is *not* minimal. Therefore in numerical examples we should still make a change of coordinates before searching for rational points.

In a remarkable series of papers [2–5], Bhargava and Shankar have shown for $n = 2, 3, 4, 5$ that the average number of elements in $\mathrm{Sel}^{(n)}(E/\mathbb{Q})$ of order n is exactly n, when elliptic curves $E/\mathbb{Q}$ are ordered by naive height. (The average size of $\mathrm{Sel}^{(n)}(E/\mathbb{Q})$ is then the sum of the divisors of n.) They conjecture that the same is true for all integers $n \geqslant 2$, and indeed proving this for larger n would improve the upper bound they give for the average rank of an elliptic curve. Their method relies on counting orbits of lattice points in an affine space, under the action of a suitable linear algebraic group. The representations and invariants required for $n = 2, 3, 4$ are classical: see [1, 26, 28, 29]. The corresponding results for $n = 5$ were obtained in [15, 18]. We think it is unlikely there is any directly analogous construction for $n > 5$ for the following reasons.

(1) In the cases $n = 2, 3, 4, 5$ the n-coverings are represented by collections of forms of degree $6-n$. The representations studied have dimension $10n/(6-n)$, and the rings of invariants are generated in degrees $4n/(6-n)$ and $6n/(6-n)$.
(2) The modular curve $X(n)$ has genus 0 for $n = 2, 3, 4, 5$ but not for $n > 5$.
(3) In [18] the cases $n = 2, 3, 4, 5$ are related to the exceptional Lie groups G_2, F_4, E_7, E_8.
(4) None of the representations studied in [6] appear to be suitable.

However, one might still hope that some construction can be made to tackle the above conjecture, say for $n = 6$. Put more simply, we would like to know how to write down genus-one curves of degree 6 at random. We do not know a good answer to this question, but our work might provide a useful starting point for further investigations.

In §§ 3 and 4 we study the secant variety of a genus-one curve of degree n, first in general, and then in the case $n = 6$. Some of the results are justified by explicit formulae recorded in § 5. One application of the invariants in the cases $n = 2, 3, 4, 5$ is that they give a formula for the Jacobian elliptic curve. In § 6 we prove an analogue of this in the case $n = 6$. We then present our results on minimisation in § 7, and finally give a numerical example in § 8 to illustrate the application of our work to finding rational points of large height on an elliptic curve.

We work throughout over a field K with $\operatorname{char} K \neq 2, 3$.

A *genus-one normal curve* is a smooth curve $C \subset \mathbb{P}^{n-1}$ of genus 1 embedded by a complete linear system of degree n. This last condition is equivalent to demanding that C has degree n, and is not contained in a hyperplane. We write $(x_1 : \ldots : x_n)$ for our coordinates on $\mathbb{P}^{n-1}$. We also write $\mathcal{L}(D)$ for the Riemann–Roch space of a divisor D on C, and H for the divisor of a hyperplane section. We may identify $\mathcal{L}(H)$ with the space of linear forms on $\mathbb{P}^{n-1}$, and more generally $S^d\mathcal{L}(H)$ with the space of forms (that is, homogeneous polynomials) of degree d in $K[x_1, \ldots, x_n]$. The word 'normal' in the definition of a genus-one normal curve refers to the fact that these curves are projectively normal, that is, the natural map $S^d\mathcal{L}(H) \to \mathcal{L}(dH)$ is surjective for all $d \geqslant 1$. Taking $d = 2$ shows that the space of quadrics vanishing on C has dimension $n(n+1)/2-2n = n(n-3)/2$. If $n \geqslant 4$ then these quadrics generate the homogeneous ideal $I(C)$, and so, in particular, define C. Proofs of these standard facts may be found, for example, in [7, 15, 22, 23].

2. *Adding 2-coverings and 3-coverings*

In this section we give an explicit formula for adding a 2-covering and a 3-covering of an elliptic curve, to give a 6-covering. We assume that the 2-covering is represented by a binary quartic,

https://doi.org/10.1112/S1461157014000217 Published online by Cambridge University Press

and the 3-covering is represented by a ternary cubic. In other words, we assume that these curves have trivial obstruction, in the sense of [11, 12, 24]. This hypothesis is always satisfied by Selmer group elements (by the result of Cassels [10] cited above), and more generally in all cases where the 6-covering we are trying to compute has trivial obstruction.

First we need to review some classical invariant theory of binary quartics and ternary cubics. See, for example, [1, 13, 15, 26, 28, 29]. For f a form in n variables, say $x_1, \dots, x_n$, and M an $n \times n$ matrix, we write $f \circ M$ for the form obtained by substituting $x_i \leftarrow \sum_{j=1}^{n} m_{ij} x_j$.

The invariants of the binary quartic

$$F(x,z) = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4$$

are

$$\begin{aligned} c_4 &= 2^4(12ae - 3bd + c^2), \\ c_6 &= 2^5(72ace - 27ad^2 - 27b^2e + 9bcd - 2c^3), \end{aligned}$$

and $\Delta = (c_4^3 - c_6^2)/1728$. These are invariants of weight 4, 6 and 12, in the sense that

$$\begin{aligned} c_4(F \circ M) &= (\det M)^4 c_4(F), \\ c_6(F \circ M) &= (\det M)^6 c_6(F), \\ \Delta(F \circ M) &= (\det M)^{12} \Delta(F), \end{aligned}$$

for all $M \in \mathrm{GL}_2$. More generally the invariants of $y^2 + A(x,z)y = B(x,z)$, where A and B are forms of degree 2 and 4, are the invariants of $\frac{1}{4}A^2 + B$. These are integer coefficient polynomials in the coefficients of A and B. The Hessian $\mathcal{H} = \mathcal{H}(F)$ is the binary quartic obtained as $\frac{1}{3}$ times the determinant of the matrix of second partial derivatives of F. Explicitly,

$$\begin{aligned} \mathcal{H} = {} & (8ac - 3b^2)x^4 + (24ad - 4bc)x^3z + (48ae + 6bd - 4c^2)x^2z^2 \\ & + (24be - 4cd)xz^3 + (8ce - 3d^2)z^4. \end{aligned}$$

It satisfies the covariance property $\mathcal{H}(F \circ M) = (\det M)^2(\mathcal{H} \circ M)$ for all $M \in \mathrm{GL}_2$.

The invariants of the ternary cubic

$$G(x,y,z) = ax^3 + by^3 + cz^3 + a_2x^2y + a_3x^2z + b_1xy^2 + b_3y^2z + c_1xz^2 + c_2yz^2 + mxyz$$

are certain polynomials c_4, c_6 and $\Delta = (c_4^3 - c_6^2)/1728$ in $\mathbb{Z}[a, b, c, \dots, m]$. They are again invariants of weights 4, 6 and 12. The Hessian $\mathcal{H}' = \mathcal{H}'(G)$ is the ternary cubic obtained as $-\frac{1}{2}$ times the determinant of the matrix of second partial derivatives of G. The invariants may be computed from the relation

$$\mathcal{H}'(\lambda G + \mu\mathcal{H}') = 3(c_4\lambda^2\mu + 2c_6\lambda\mu^2 + c_4^2\mu^3)G + (\lambda^3 - 3c_4\lambda\mu^2 - 2c_6\mu^3)\mathcal{H}'.$$

The contravariants $P = P(G)$ and $Q = Q(G)$ are the ternary cubics determined by

$$P = (-1/xyz) \times \begin{vmatrix} \frac{\partial G}{\partial x}(0,z,-y) & \frac{\partial G}{\partial y}(0,z,-y) & \frac{\partial G}{\partial z}(0,z,-y) \\ \frac{\partial G}{\partial x}(-z,0,x) & \frac{\partial G}{\partial y}(-z,0,x) & \frac{\partial G}{\partial z}(-z,0,x) \\ \frac{\partial G}{\partial x}(y,-x,0) & \frac{\partial G}{\partial y}(y,-x,0) & \frac{\partial G}{\partial z}(y,-x,0) \end{vmatrix}$$

and

$$P(\lambda G + \mu\mathcal{H}') = (\lambda^3 + 3c_4\lambda\mu^2 + 4c_6\mu^3)P + 3(\lambda^2\mu - c_4\mu^3)Q.$$

We write M^{-T} for the inverse transpose of M. Then P and Q have the covariance properties $P(G \circ M) = (\det M)^4(P \circ M^{-T})$ and $Q(G \circ M) = (\det M)^6(Q \circ M^{-T})$ for all $M \in \mathrm{GL}_3$.

https://doi.org/10.1112/S1461157014000217 Published online by Cambridge University Press

A binary quartic F, or ternary cubic G, with non-zero discriminant Δ defines a smooth curve of genus 1. This is either a double cover $C_2 \to \mathbb{P}^1$ with equation $y^2 = F(x,z)$, or a plane cubic $C_3 \subset \mathbb{P}^2$ with equation $G(x,y,z) = 0$. With c_4 and c_6 defined as above, the Jacobian is the elliptic curve E with Weierstrass equation $y^2 = x^3 - 27c_4x - 54c_6$.

For f a polynomial which is homogeneous of degree d in each of the sets of variables x_1, x_2 and y_1, y_2, y_3, we write $\{f\}$ for the polynomial in $z_{11}, z_{12}, z_{13}, z_{21}, z_{22}, z_{23}$ obtained by substituting

$$x_{i_1} \dots x_{i_d} y_{j_1} \dots y_{j_d} \mapsto \sum_{\sigma \in S_d} z_{i_1 j_{\sigma(1)}} \dots z_{i_d j_{\sigma(d)}}.$$

Let $\mathcal{H}$ be the Hessian of a binary quartic F. Let P and Q be the contravariants of a ternary cubic G. Then for $i = 1, 2$ we put

$$e_i = \left\{\frac{\partial F}{\partial x_i}(x_1,x_2)P(y_1,y_2,y_3)\right\}, \quad f_i = \left\{\frac{\partial F}{\partial x_i}(x_1,x_2)Q(y_1,y_2,y_3)\right\},$$
$$g_i = \left\{\frac{\partial \mathcal{H}}{\partial x_i}(x_1,x_2)P(y_1,y_2,y_3)\right\}, \quad h_i = \left\{\frac{\partial \mathcal{H}}{\partial x_i}(x_1,x_2)Q(y_1,y_2,y_3)\right\}.$$

THEOREM 2.1. *Suppose that F and G have the same invariants c_4, c_6 and Δ. Then:*

(i) *the partial derivatives of $f_1 - g_1$ and $f_2 - g_2$ define a genus-one normal curve $C_6 \subset \mathbb{P}^5$ with $C_6 \cong C_2 \times_E C_3$;*

(ii) *the morphism $C_6 \to C_3$ is given by the 2×2 minors of the matrix (z_{ij}), that is,*

$$(z_{12}z_{23} - z_{13}z_{22} : z_{13}z_{21} - z_{11}z_{23} : z_{11}z_{22} - z_{12}z_{21});$$

(iii) *the composite of the morphism $C_6 \to C_2$ and the double cover $C_2 \to \mathbb{P}^1$ is given by*

$$(-e_2 : e_1) = (-f_2 : f_1) = (-g_2 : g_1) = (-h_2 : h_1)$$

where it is possible that some (but not all) of these pairs of forms vanish identically on C_6.

Proof. We write 2 and 3 for the standard representations of GL_2 and GL_3. Then as representations of $\mathrm{GL}_2 \times \mathrm{GL}_3$ we have

$$S^2(2 \otimes 3) \cong (\wedge^2 2 \otimes \wedge^2 3) \oplus (S^2 2 \otimes S^2 3).$$

In other words, the 21-dimensional space of quadrics in $z_{11}, z_{12}, z_{13}, z_{21}, z_{22}, z_{23}$ naturally decomposes into subspaces of dimensions 3 and 18. The first of these is spanned by the 2×2 minors in (ii). We may project onto the second factor by substituting $z_{ij} = x_i y_j$, and a section for this map, respecting the action of $\mathrm{GL}_2 \times \mathrm{GL}_3$, is given by $f \mapsto \frac{1}{2}\{f\}$.

The curve C_6 in (i) is defined by the nine quadrics

$$\left\{\frac{\partial^2 F}{\partial x_i \partial x_j}(x_1,x_2)\frac{\partial Q}{\partial y_k}(y_1,y_2,y_3) - \frac{\partial^2 \mathcal{H}}{\partial x_i \partial x_j}(x_1,x_2)\frac{\partial P}{\partial y_k}(y_1,y_2,y_3)\right\} \tag{1}$$

for $1 \leqslant i \leqslant j \leqslant 2$ and $1 \leqslant k \leqslant 3$.

By the covariance properties of $F, \mathcal{H}, P$ and Q we are free to change coordinates by any pair of matrices in $\mathrm{GL}_2 \times \mathrm{GL}_3$ with the same determinant. We are also free to extend our field K. We may therefore reduce to the case where $C_2 \to \mathbb{P}^1$ and $C_3 \subset \mathbb{P}^2$ are copies of the same elliptic curve E, and the maps to projective space are via the complete linear systems $|2.0_E|$ and $|3.0_E|$. If E has Weierstrass equation $y^2 = x^3 + ax + b$ then

$$F(x,z) = x^3 z + axz^3 + bz^4,$$
$$\mathcal{H}(x,z) = -3(x^4 - 2ax^2z^2 - 8bxz^3 + a^2z^4),$$

https://doi.org/10.1112/S1461157014000217 Published online by Cambridge University Press

and

$$\begin{aligned} G(x,y,z) &= y^2z - x^3 - axz^2 - bz^3, \\ P(y_1,y_2,y_3) &= 2(ay_1^3 + 9by_1y_2^2 + 3y_1y_3^2 - 6ay_2^2y_3), \\ Q(y_1,y_2,y_3) &= 24(2by_1^3 - ay_1^2y_3 - 2a^2y_1y_2^2 - 9by_2^2y_3 + y_3^3). \end{aligned}$$

By direct calculation, the quadrics (1) define the image of E embedded in $\mathbb{P}^5$ via

$$\begin{pmatrix} z_{11} & z_{12} & z_{13} \\ z_{21} & z_{22} & z_{23} \end{pmatrix} = \begin{pmatrix} x^3 + 3ax + 4b & -2xy & ax^2 + 6bx - a^2 \\ -3x^2 - a & -2y & x^3 - ax - 2b \end{pmatrix}. \tag{2}$$

We checked, using the discriminant condition $4a^3 + 27b^2 \neq 0$, that the rational functions on the right are a basis for the Riemann–Roch space $\mathcal{L}(6.0_E)$. The image is therefore a genus-one normal curve.

Since the fibre product of the trivial 2-covering and the trivial 3-covering is the trivial 6-covering, it only remains to prove that the maps in (ii) and (iii) are $[2]_E$ and $[3]_E$, where $[n]_E$ is multiplication-by-n on E. For the first of these we simply checked that the 2×2 minors of (2) define $[2]_E$. The x-coordinate of $[3]_E(x,y)$ is given by θ_3/ψ_3^2 where

$$\begin{aligned} \theta_3 &= x^9 - 12ax^7 - 96bx^6 + \ldots + 3(3a^4 + 32ab^2)x + 8(a^3b + 8b^3), \\ \psi_3 &= 3x^4 + 6ax^2 + 12bx - a^2. \end{aligned}$$

After making the substitution (2) we find

$$\begin{aligned} (e_1,e_2) &= (-48a\psi_3^2, 48a\theta_3), \quad (f_1,f_2) = (-864b\psi_3^2, 864b\theta_3), \\ (g_1,g_2) &= (-864b\psi_3^2, 864b\theta_3), \quad (h_1,h_2) = (2304a^2\psi_3^2, -2304a^2\theta_3). \end{aligned}$$

Since the numerical factors are of the form 2^r3^s, and we cannot have $a = b = 0$, this proves (iii). □

3. *Secant varieties*

In this section we work over an algebraically closed field and review some geometric facts about secant varieties of genus-one normal curves. Many of the results have been generalized to higher secant varieties; see, for example, [9].

Let $C \subset \mathbb{P}^{n-1}$ be a genus-one normal curve of degree n. We write H for the divisor of a hyperplane section, and identify the Riemann–Roch space $\mathcal{L}(H)$ with the space of linear forms on $\mathbb{P}^{n-1}$. If D is an effective divisor on C of degree $d < n$ then the subspace $\mathcal{L}(H-D) \subset \mathcal{L}(H)$ defines a linear subvariety $\overline{D} \subset \mathbb{P}^{n-1}$ of dimension $d-1$. For example, if D is the sum of two points $P, Q \in C$ then $\overline{D}$ is the secant line PQ if $P \neq Q$, and the tangent line T_PC if $P = Q$. The secant variety $\operatorname{Sec} C$ is the Zariski closure of the union of all secant lines, equivalently the union of all lines $\overline{D}$ for D a degree-2 effective divisor on C. If $n \geqslant 5$ and $P \in \overline{D}$ for two such divisors D, then it is easy to show (see [16, Lemma 2.6]) that $P \in C$.

LEMMA 3.1. *If $n \geqslant 5$ then $\operatorname{Sec} C \subset \mathbb{P}^{n-1}$ is an irreducible variety of dimension 3.*

Proof. See [20, Proposition 11.24]. □

We write $I(X)$ for the homogeneous ideal of a projective variety X. Suppose we know a basis for the space of quadrics in $I(C)$. The next lemma shows it is easy to solve for the cubic forms in $I(\operatorname{Sec} C)$ by linear algebra.

https://doi.org/10.1112/S1461157014000217 Published online by Cambridge University Press

LEMMA 3.2. *If $n \geqslant 6$ then $I(\operatorname{Sec} C)$ is generated by cubics. A cubic form f vanishes on $\operatorname{Sec} C$ if and only if it is singular at every point on C, equivalently $\partial f/\partial x_i \in I(C)$ for all $1 \leqslant i \leqslant n$.*

Proof. The first statement is a special case of results in [**9**, **19**].

Now let $P_1, \ldots, P_n$ be any points on C spanning $\mathbb{P}^{n-1}$. We choose coordinates so that $P_1 = (1 : 0 : \ldots : 0)$, $P_2 = (0 : 1 : \ldots : 0)$, etc. For each $1 \leqslant i < j \leqslant n$ the secant variety contains the line P_iP_j. So if $f \in I(\operatorname{Sec} C)$ is a form of degree d, then f can contain no monomials involving x_i and x_j only. Therefore $d \geqslant 3$. Moreover, if $d = 3$ then f is singular at P_1. Since $P_1 \in C$ was arbitrary, f is singular at every point of C.

Conversely, suppose f is singular at every point of C. Then for distinct points $P, Q \in C$ the restriction of f to the line PQ is a binary cubic with at least two double roots. Therefore f vanishes on the line PQ, and it follows that $f \in I(\operatorname{Sec} C)$. □

LEMMA 3.3. *If $n \geqslant 5$ then C is the singular locus of $\operatorname{Sec} C$.*

Proof. If $P \in C$ then the line PQ is contained in the tangent space $T_P \operatorname{Sec} C$ for every $Q \in C$. Since C spans $\mathbb{P}^{n-1}$ it follows that $T_P \operatorname{Sec} C = \mathbb{P}^{n-1}$. Since $\operatorname{Sec} C \subset \mathbb{P}^{n-1}$ is a proper subvariety (by Lemma 3.1) it follows that the singular locus of $\operatorname{Sec} C$ contains C. The reverse inclusion is proved in [**9**, Proposition 8.15] and [**19**, Proposition 5.1]. In fact if $P \in \overline{D}$ for D a degree-2 effective divisor on C, and $P \notin C$, then $T_P \operatorname{Sec} C = \overline{2D}$. □

The next two lemmas count the dimension of the space of cubics in $I(\operatorname{Sec} C)$. The exact statements are also of interest.

Let $P \in C$ be any point. We choose coordinates $x_1, \ldots, x_n$ so that $\mathcal{L}(H - iP)$ has basis $x_1, \ldots, x_{n-i}$ for $i = 0, 1, 2$. In other words, $P = (0 : \ldots : 0 : 1)$ and $T_PC = \{(0 : \ldots : 0 : \lambda : \mu)\}$. We write C' and C'' for the genus-one normal curves with hyperplane sections $H - P$ and $H - 2P$ obtained by projecting away from P and T_PC.

LEMMA 3.4.

(i) *If $f \in I(\operatorname{Sec} C)$ is a cubic then*

$$f(x_1, \ldots, x_n) = x_n g(x_1, \ldots, x_{n-2}) + h(x_1, \ldots, x_{n-1}) \tag{3}$$

for some quadric $g \in I(C'')$ and cubic h.

(ii) *The space of cubics vanishing on $\operatorname{Sec} C$ has dimension at most $n(n-4)(n-5)/6$.*

Proof. (i) We write $f(x_1, \ldots, x_n) = \sum x_{n-1}^r x_n^s g_{rs}(x_1, \ldots, x_{n-2})$. Since f vanishes on T_PC we have $g_{rs} = 0$ whenever $r + s = 3$. Since $\partial f/\partial x_i \in I(C)$ for all $1 \leqslant i \leqslant n-2$ we also have $g_{11} = g_{02} = 0$. Therefore f is of the form (3) and

$$g = \frac{\partial f}{\partial x_n} \in I(C) \cap K[x_1, \ldots, x_{n-2}] = I(C'').$$

(ii) In the case $n = 5$ it is known (see [**22**, VIII.2.5]) that $\operatorname{Sec} C \subset \mathbb{P}^4$ is a hypersurface of degree 5. So there are no cubic forms in $I(\operatorname{Sec} C)$. The proof is now by induction on $n \geqslant 6$. By (i), and the observation that

$$I(\operatorname{Sec} C) \cap K[x_1, \ldots, x_{n-1}] = I(\operatorname{Sec} C'),$$

the space of cubic forms in $I(\operatorname{Sec} C)$ has dimension at most

$$\frac{(n-1)(n-5)(n-6)}{6} + \frac{(n-2)(n-5)}{2} = \frac{n(n-4)(n-5)}{6},$$

https://doi.org/10.1112/S1461157014000217 Published online by Cambridge University Press

where the first term is our inductive upper bound for the dimension of the space of cubics in $I(\operatorname{Sec} C')$, and the second term is the dimension of the space of quadrics in $I(C'')$. □

As before, we identify the Riemann–Roch space $\mathcal{L}(H)$ with the space of linear forms on $\mathbb{P}^{n-1}$. Let D_1, D_2 be divisors on C with $D_1 + D_2 = H$. We write $\Phi(D_1, D_2)$ for the matrix of linear forms representing (with respect to some choices of bases for $\mathcal{L}(D_1)$ and $\mathcal{L}(D_2)$) the multiplication map

$$\mathcal{L}(D_1) \times \mathcal{L}(D_2) \to \mathcal{L}(H).$$

It is clear that $\Phi(D_1, D_2)$ has rank at most 1 on C, and hence rank at most 2 on $\operatorname{Sec} C$. So the 2×2 minors are quadrics in $I(C)$ and the 3×3 minors are cubics in $I(\operatorname{Sec} C)$.

LEMMA 3.5. *The space of cubics spanned by the 3×3 minors of the matrices $\Phi(D_1, D_2)$ has dimension at least $n(n-4)(n-5)/6$.*

Proof. See [**16**, Lemma 2.1]. □

Combining Lemmas 3.4 and 3.5 shows that the space of cubics in $I(\operatorname{Sec} C)$ has dimension exactly $n(n-4)(n-5)/6$.

4. *Pencils of cubic forms*

We drop our assumption that K is algebraically closed, and write $\overline{K}$ for the algebraic closure. The Hessian $\mathcal{H}(F)$ of a cubic form $F \in K[x_1, \dots, x_6]$ is the form of degree 6 obtained as the determinant of the 6×6 matrix of second partial derivatives of F. To avoid confusion with our earlier notation, we will now write $h = h(f)$ for the Hessian of a binary quartic.

THEOREM 4.1. *Let $C \subset \mathbb{P}^5$ be a genus-one normal curve of degree 6 with secant variety defined by cubic forms F_1 and F_2. Then, working over $\overline{K}$, there are exactly four 'special' cubics F in the pencil spanned by F_1 and F_2, with $\mathcal{H}(F)$ a scalar multiple of F^2. Moreover:*

(i) *each cubic in the pencil spanned by F_1 and F_2 has singular locus C, with the exception of the special cubics which have singular locus a Veronese surface;*

(ii) *there is a binary quartic $f \in K[s,t]$, with roots corresponding to the special cubics, and cubic forms $G_1, G_2 \in K[x_1, \dots, x_6]$ satisfying*

$$\begin{aligned}\mathcal{H}(sF_1 + tF_2) = {} & \frac{1}{3}h(s,t)(sF_1 + tF_2)^2 - 2f(s,t)(sF_1 + tF_2)(sG_1 + tG_2) \\ & - \frac{1}{3}f(s,t)\left(\frac{\partial^2 f}{\partial t^2}F_1^2 - 2\frac{\partial^2 f}{\partial s \partial t}F_1F_2 + \frac{\partial^2 f}{\partial s^2}F_2^2\right)\end{aligned} \tag{4}$$

where h is the Hessian of f, as defined in § 2;

(iii) *the covering map from C to its Jacobian factors via a quadratic twist of $y^2 = f(x,z)$.*

Proof. For the first part of the proof we may take $K = \overline{K}$. Let D_1 and D_2 be degree-3 divisors on C with $D_1 + D_2 = H$. Then $\det \Phi(D_1, D_2)$ is a cubic form vanishing on $\operatorname{Sec} C$ and so belongs to the pencil spanned by F_1 and F_2. By Lemmas 3.4 and 3.5 the pencil is spanned by cubics of this form. We now show that every cubic in the pencil is of this form. We say that divisor pairs (D_1, D_2) and (D_1', D_2') are *equivalent* if $D_1 \sim D_1'$ or $D_1 \sim D_2'$. It is shown in [**16**, Lemma 2.9], following [**25**, 9.22.1], that if (D_1, D_2) and (D_1', D_2') are inequivalent then $\operatorname{Sec} C = \{\det \Phi(D_1, D_2) = \det \Phi(D_1', D_2') = 0\} \subset \mathbb{P}^5$. In particular, these two cubic forms are linearly independent.

https://doi.org/10.1112/S1461157014000217 Published online by Cambridge University Press

We claim that the map $(D_1, D_2) \mapsto \det \Phi(D_1, D_2)$ is a bijection between the equivalence classes of divisor pairs and the pencil of cubics spanned by F_1 and F_2. To prove this let C be the image of an elliptic curve E embedded in $\mathbb{P}^5$ by $|6.0_E|$. Then writing

$$\det \Phi(2.0_E + P, 4.0_E - P) = s(P)F_1 + t(P)F_2,$$

for $P \in E$, we can see that s/t is a rational function on E. It therefore defines a morphism $(s : t) : E \to \mathbb{P}^1$. By the previous paragraph, this morphism is non-constant, and indeed has fibres of the form $\{P, -P\}$. It must therefore be surjective. This proves the claim.

By considering $P \in E[2]$ we see there are four cubics in the pencil of the form $\det \Phi(D_1, D_2)$ with $D_1 \sim D_2$. In these cases we may choose bases for $\mathcal{L}(D_1)$ and $\mathcal{L}(D_2)$ so that $\Phi(D_1, D_2)$ is a generic 3×3 symmetric matrix, say

$$M = \begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{12} & x_{22} & x_{23} \\ x_{13} & x_{23} & x_{33} \end{pmatrix}.$$

Then $F = \det M$ satisfies $\mathcal{H}(F) = -16F^2$. Moreover, the partial derivatives of F, equivalently the 2×2 minors of M, define a Veronese surface, that is, the image of the 2-uple embedding $\mathbb{P}^2 \to \mathbb{P}^5$.

The identity (4) is well behaved under the natural action of $\mathrm{GL}_2 \times \mathrm{GL}_6$. Specifically, if the identity is satisfied by (F_1, F_2) and f, then it is also satisfied by

$$(m_{11}F_1 + m_{21}F_2, m_{12}F_1 + m_{22}F_2) \quad \text{and} \quad \frac{1}{\det M}(f \circ M) \tag{5}$$

for any $M \in \mathrm{GL}_2$, and by

$$(F_1 \circ N, F_2 \circ N) \quad \text{and} \quad (\det N)f \tag{6}$$

for any $N \in \mathrm{GL}_6$. Therefore (ii) follows from any of the special cases computed in § 5.

To complete the proof of (i) it remains to show that if $(s : t) \in \mathbb{P}^1$ is not a root of f then $sF_1 + tF_2$ is not a special cubic, and its partial derivatives define C. Taking $s = 1$ in (4) and using Euler's identity, we have

$$\mathcal{H}(F_1 + tF_2) \equiv -4f(1, t)^2 F_2^2 \pmod{(F_1 + tF_2)}. \tag{7}$$

In particular, if $f(1, t) \neq 0$ then $F_1 + tF_2$ is not a special cubic, and indeed it does not even divide its own Hessian. If the partial derivatives of a cubic form F vanish at a point $P = (a_1 : \ldots : a_6)$, then by Euler's identity the vector $(a_1, \ldots, a_6)$ is in the kernel of the matrix of second partial derivatives of F evaluated at P. Therefore $\mathcal{H}(F)$ vanishes at P. If $f(1, t) \neq 0$ and P is singular on $\{F_1 + tF_2 = 0\} \subset \mathbb{P}^5$ it now follows by (7) that $F_2(P) = 0$. But then $P \in \operatorname{Sec} C$ and it follows by Lemma 3.3 that $P \in C$. This completes the proof of (i).

We now drop our assumption that K is algebraically closed. To complete the proof of (ii) we must show that G_1, G_2 and f have coefficients in K. However by a change of coordinates defined over K we may assume that C is of the form described in Theorem 2.1. We are then done by the last of the special cases computed in § 5. This also proves (iii). □

Remarks 4.2. (i) The identity (4) only defines f up to sign. It can be computed by using (7) to solve for $f(1, t)^2$ for several values of t and then interpolating.

(ii) The geometric interpretation of the cubic forms G_1, G_2 is that F_1, F_2, G_1, G_2 are a basis for the space of cubic forms vanishing on the tangent variety of C.

(iii) The set of special cubics is a torsor under $E[2]$, where E is the Jacobian of C. This can be seen either by considering the divisors D on C with $2D \sim H$, or as a consequence of Theorem 4.1(iii).

https://doi.org/10.1112/S1461157014000217 Published online by Cambridge University Press

(iv) It is shown in [**16**, Theorem 1.3] that if D_1, D_2 are degree-3 divisors on C with $D_1+D_2 = H$ and $D_1 \not\sim D_2$ then the 2×2 minors of $\Phi(D_1, D_2)$ generate $I(C)$.

5. *Explicit formulae*

We check the identity (4) first in the case of an elliptic curve E embedded via $|6.0_E|$, then for a binary quartic 3-uply embedded, then for a ternary cubic 2-uply embedded, and finally for the sum of a binary quartic and ternary cubic as computed using Theorem 2.1. (For the general definition of a d-uple embedding see [**21**, p. 13].)

Let E be the elliptic curve $y^2 = x^3 + ax + b$. The embedding of E in $\mathbb{P}^5$ via $|6.0_E|$ is given by $(x_1 : \ldots : x_6) = (1 : x : y : x^2 : xy : x^3)$ and has image $C \subset \mathbb{P}^5$ defined by quadrics

$$\begin{aligned} q_1 &= x_1x_4 - x_2^2, & q_6 &= x_1x_6 - x_2x_4,\\ q_2 &= x_2x_4 - x_3^2 + ax_1x_2 + bx_1^2, & q_7 &= x_2x_6 - x_4^2,\\ q_3 &= x_1x_5 - x_2x_3, & q_8 &= x_3x_6 - x_4x_5,\\ q_4 &= x_2x_5 - x_3x_4, & q_9 &= x_4x_6 - x_5^2 + ax_2x_4 + bx_2^2.\\ q_5 &= x_3x_5 - x_4^2 - ax_1x_4 - bx_1x_2. \end{aligned}$$

By Lemma 3.2 the cubics defining $\operatorname{Sec} C$ are

$$\begin{aligned} F_1 &= (x_6 + ax_2 + bx_1)q_1 - x_1x_5^2 + 2x_2x_3x_5 - x_3^2x_4,\\ F_2 &= x_6q_2 - x_2x_5^2 + 2x_3x_4x_5 - x_4^3 - x_1x_4(ax_4 + 2bx_2) + bx_2^3. \end{aligned}$$

These are of the form specified in Lemma 3.4, where $C'' \subset \mathbb{P}^3$ is the quadric intersection defined by q_1 and q_2. We remark that if $C' \subset \mathbb{P}^4$ is the genus-one normal curve of degree 5 defined by $q_1, \ldots, q_5$ then $\operatorname{Sec} C'$ is defined by the quintic form

$$2(q_2F_1 - q_1F_2) = \det\left(\frac{\partial q_i}{\partial x_j}\right)_{i,j=1,\ldots,5}.$$

By following the proof of Theorem 4.1 we find that F_1 and F_2 are the determinants of the matrices

$$\begin{pmatrix} x_1 & x_2 & x_3\\ x_2 & x_4 & x_5\\ x_3 & x_5 & x_6' \end{pmatrix} \quad\text{and}\quad \begin{pmatrix} x_2 & x_4 & x_3 + \sqrt{b}x_1\\ x_4 & x_6 & x_5 + \sqrt{b}x_2\\ x_3 - \sqrt{b}x_1 & x_5 - \sqrt{b}x_2 & x_4 + ax_1 \end{pmatrix}$$

where $x_6' = x_6 + ax_2 + bx_1$. Moreover (4) is satisfied with $f(s,t) = 4(s^3t + ast^3 - bt^4)$ and

$$\begin{aligned} G_1 &= 2(x_1x_6^2 + 2x_3^2x_6 + 2ax_1x_2x_6 + 2bx_1^2x_6 - 6x_2x_5^2 - 4ax_1x_3x_5 + 3x_4^3 + 6ax_2^2x_4\\ &\quad + a^2x_1^2x_4 - 4bx_1x_3^2 + 6bx_2^3 + 3a^2x_1x_2^2 + 8abx_1^2x_2 + 4b^2x_1^3),\\ G_2 &= 2(x_2x_6^2 - 4x_3x_5x_6 + 3x_4^2x_6 + 2ax_1x_4x_6 - 4bx_1x_2x_6 + a^2x_1^2x_6 + 2ax_1x_5^2 + 8bx_1x_3x_5\\ &\quad + 6ax_2x_4^2 + 12bx_1x_4^2 - 6ax_3^2x_4 + 2abx_1^2x_4 - 12bx_2x_3^2 + 3a^2x_2^3 + 6abx_1x_2^2 + 4b^2x_1^2x_2). \end{aligned}$$

More general formulae are obtained if we start with a binary quartic

$$F(x,z) = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4,$$

https://doi.org/10.1112/S1461157014000217 Published online by Cambridge University Press

defining a double cover $C_2 \to \mathbb{P}^1$, and then embed C_2 in $\mathbb{P}^5$ via

$$(x_0 : x_1 : x_2 : x_3 : y_0 : y_1) = (x^3 : x^2z : xz^2 : z^3 : xy : zy).$$

The image has secant variety defined by

$$\begin{aligned} F_1 &= (ax_0 + bx_1 + cx_2 + dx_3)(x_0x_2 - x_1^2) + e(x_0x_3^2 - 2x_1x_2x_3 + x_2^3) \\ &\quad - (x_0y_1^2 - 2x_1y_0y_1 + x_2y_0^2), \\ F_2 &= (bx_0 + cx_1 + dx_2 + ex_3)(x_1x_3 - x_2^2) + a(x_0^2x_3 - 2x_0x_1x_2 + x_1^3) \\ &\quad - (x_1y_1^2 - 2x_2y_0y_1 + x_3y_0^2). \end{aligned}$$

Moreover, the identity (4) is satisfied with $f(s,t) = 4F(-t,s)$, and G_1, G_2 certain cubic forms with coefficients in $\mathbb{Z}[a,b,c,d,e]$.

Alternatively, we start with a ternary cubic $G(x_1,x_2,x_3)$ defining $C_3 \subset \mathbb{P}^2$ and then embed C_3 in $\mathbb{P}^5$ via

$$(x_{11} : x_{12} : x_{13} : x_{22} : x_{23} : x_{33}) = (x_1^2 : x_1x_2 : x_1x_3 : x_2^2 : x_2x_3 : x_3^2).$$

The image has secant variety defined by

$$F_1 = \det \begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{12} & x_{22} & x_{23} \\ x_{13} & x_{23} & x_{33} \end{pmatrix},$$

$$F_2 = \frac{1}{6} \sum_{i,j,k,p,q,r=1}^{3} \frac{\partial^3 G}{\partial x_i \partial x_j \partial x_k} \frac{\partial^3 G}{\partial x_p \partial x_q \partial x_r} (3x_{ij}x_{pq} - x_{ip}x_{jq})x_{kr}.$$

Let $R_3 = \mathbb{Z}[a,b,c,\ldots]$ where $a,b,c,\ldots$ are the coefficients of G. Then F_1 and F_2 have coefficients in R_3 and (4) is satisfied with $f(s,t) = 4(s^3t - 3c_4st^3 - 2c_6t^4)$, where c_4 and c_6 are the invariants of G. If $b_2, b_4, b_6 \in R_3$ are as defined in [**13**] then $F_2' = \frac{1}{12}(F_2 + b_2F_1)$ has coefficients in R_3. Moreover, F_1 and F_2' satisfy (4) with

$$f(s,t) = 4s^3t + b_2s^2t^2 + 2b_4st^3 + b_6t^4.$$

Finally, we start with a generalized binary quartic $y^2 + A(x,z)y = B(x,z)$ and a ternary cubic $G(x,y,z)$ with the same invariants c_4, c_6 and Δ. We put $F(x,z) = \frac{1}{4}A(x,z)^2 + B(x,z)$, and define e_i, f_i, g_i, h_i as in § 2. Then putting

$$F_i = \tfrac{1}{72}(f_i - g_i) \quad \text{and} \quad G_i = \tfrac{1}{72}\Delta(c_4e_i - h_i)$$

for $i = 1, 2$, the identity (4) is satisfied with $f(s,t) = 4\Delta F(s,t)$. This is proved by a generic calculation, which is made feasible by reducing to the special case considered in the proof of Theorem 2.1. Suppose that the Weierstrass equations, computed using [**13**, Theorem 2.10], for the Jacobians of $y^2 + A(x,z)y = B(x,z)$ and $G(x,y,z) = 0$ are related by $x \leftarrow x + r$ and $y \leftarrow y + sx + t$. Then a generic calculation shows that the coefficients of F_1, F_2, G_1, G_2 are integer coefficient polynomials in r, s, t and the coefficients of A, B and G. The reason for introducing r, s, t is to avoid having denominators of the form 2^a3^b.

6. *Computing the Jacobian*

Suppose we are given equations for a genus-one curve C that is either a double cover of $\mathbb{P}^1$ (case $n = 2$) or a genus-one normal curve of degree $n \geqslant 3$. If $n = 2, 3, 4, 5$ then the invariants

https://doi.org/10.1112/S1461157014000217 Published online by Cambridge University Press

in [**1**, **15**] give a formula for the Jacobian of C. If $n = 6$ then Theorem 4.1(iii) and Remark 4.2(i), together with the invariants in the case $n = 2$, determine the Jacobian up to quadratic twist. In this section we explain how Theorem 2.1 can be used to compute the Jacobian exactly.

By Lemma 3.2 we may solve for cubic forms F_1 and F_2 defining $\operatorname{Sec} C$. We know by Lemma 3.3 that the partial derivatives of F_1 and F_2 define C. In fact, by the formulae in § 5, they generate $I(C)$. The 12 partial derivatives of F_1 and F_2, in the 9-dimensional space of quadrics vanishing on C, therefore satisfy three linear dependence relations.

By properties of the obstruction map, as cited in § 2, we know that C is of the form arising in Theorem 2.1, up to a change of coordinates on $\mathbb{P}^5$ defined over K. We now find this change of coordinates, up to the action of $\mathrm{GL}_2(K) \times \mathrm{GL}_3(K)$. The cubic forms $f_1 - g_1$ and $f_2 - g_2$ in Theorem 2.1 satisfy

$$\frac{\partial(f_1 - g_1)}{\partial z_{2k}} = \frac{\partial(f_2 - g_2)}{\partial z_{1k}}$$

for $k = 1, 2, 3$. Therefore substituting

$$x_i = \sum_{j=1}^{2} \sum_{k=1}^{3} a_{ijk} z_{jk}$$

into F_1 and F_2, for suitable constants a_{ijk}, gives cubic forms $F_1', F_2' \in K[z_{11}, \ldots, z_{23}]$ satisfying

$$\frac{\partial F_1'}{\partial z_{1k}} + \frac{\partial F_2'}{\partial z_{2k}} = 0$$

for $k = 1, 2, 3$. By the chain rule

$$\sum_{i=1}^{6} \sum_{j=1}^{2} a_{ijk} \frac{\partial F_j}{\partial x_i} = 0$$

for $k = 1, 2, 3$. The coefficients of the three linear dependence relations mentioned above are therefore exactly the numbers we need in order to write down the required change of coordinates on $\mathbb{P}^5$.

We have now reduced to the case where $C = C_6$ is as described in Theorem 2.1. In particular, the 2×2 minors of the matrix (z_{ij}) define a morphism $C_6 \to C_3$, where C_3 is a plane cubic. We can solve for an equation for C_3 by linear algebra. The Jacobian of C_6 is now the same as that of C_3, which may be computed using the classical formulae cited above.

7. *Minimal models*

We represent a genus-one normal curve of degree 6 by a pair of cubic forms defining its secant variety. In this section we define the *discriminant* of such a model. We then prove a result on the existence of models with the same discriminant as a minimal Weierstrass equation for the Jacobian elliptic curve.

DEFINITION 7.1. Let $F_1, F_2 \in K[x_1, \ldots, x_6]$ be cubic forms defining the secant variety of a genus-one normal curve of degree 6. The *discriminant* of (F_1, F_2) is

$$\Delta(F_1, F_2) = 2^{-12} \Delta(f)$$

where f is the binary quartic in Theorem 4.1, and $\Delta(f)$ is as defined in § 2.

Since Theorem 4.1 only determines f up to sign, Definition 7.1 relies on the fact that the discriminant of a binary quartic has even degree (in fact degree 6). Since f has distinct roots, we have $\Delta(F_1, F_2) \neq 0$.

https://doi.org/10.1112/S1461157014000217 Published online by Cambridge University Press

LEMMA 7.2. *If* $(M, N) \in \mathrm{GL}_2 \times \mathrm{GL}_6$ *then*

$$\Delta(m_{11}F_1' + m_{12}F_2', m_{21}F_1' + m_{22}F_2') = (\det M)^6(\det N)^6\Delta(F_1, F_2)$$

where $F_1' = F_1 \circ N$ *and* $F_2' = F_2 \circ N$.

Proof. This follows from (5), (6) and properties of the discriminant of a binary quartic, namely that it has degree 6 and weight 12. □

Let $\mathcal{O}_K$ be a discrete valuation ring with uniformizer π, discrete valuation v, residue field k, and field of fractions K. As usual, we assume $\mathrm{char}\, K \neq 2, 3$.

THEOREM 7.3. *Suppose that* F_1 *and* F_2 *have coefficients in* $\mathcal{O}_K$*, and that their reductions mod* π *(which we denote* $\overline{F}_1$ *and* $\overline{F}_2$*) are linearly independent over* k*. Then the binary quartic* f *has coefficients in* $\mathcal{O}_K$.

Proof. Suppose $\mathcal{H}(F_1) \equiv \alpha F_2^2 \pmod{F_1}$ for some $\alpha \in K$. If α is not in $\mathcal{O}_K$ then $\overline{F}_1$ divides $\overline{F}_2^2$. Then $\overline{F}_1$ and $\overline{F}_2$ have a common quadratic factor, and $\overline{F}_1 + \xi\overline{F}_2$ divides $\overline{F}_2^2$ for at most two $\xi \in k$. It follows by (7) that $2f(1, t) \in \mathcal{O}_K$ for all $t \in \mathcal{O}_K$, avoiding at most two residue classes mod π. If $|k| \geqslant 7$ we see by interpolation that $2f$ has coefficients in $\mathcal{O}_K$. In general we may reduce to this case by making an unramified extension.

A generic calculation shows that if F is a cubic form in $x_1, \ldots, x_6$ then the coefficients of $\frac{1}{4}\mathcal{H}(F)$ are integer coefficient polynomials in the coefficients of F. The above arguments then show that f has coefficients in $\mathcal{O}_K$. □

THEOREM 7.4. *Let* $C \subset \mathbb{P}^5$ *be a genus-one normal curve of degree* 6 *defined over* K*. Suppose that* $C(K) \neq \emptyset$*. Then, after a change of coordinates on* $\mathbb{P}^5$ *defined over* K*, the secant variety* $\mathrm{Sec}\, C$ *is defined by cubic forms* $F_1, F_2 \in \mathcal{O}_K[x_1, \ldots, x_6]$ *with* $\Delta(F_1, F_2) = \Delta_E$*, where* Δ_E *is the minimal discriminant of the Jacobian* E *of* C.

Proof. If C is an elliptic curve E embedded by $|6.0_E|$, or the 3-uple embedding of a binary quartic, or the 2-uple embedding of a ternary cubic, then the theorem already follows from the formulae in § 5, and the corresponding results for 2-coverings and 3-coverings in [**13**]. If, however, we use Theorem 2.1 to add a binary quartic and ternary cubic then we only get $F_1, F_2 \in \mathcal{O}_K[x_1, \ldots, x_6]$ with $\Delta(F_1, F_2) = \Delta_E^7$. In other words, adding a minimal 2-covering and a minimal 3-covering does not give a minimal 6-covering.

In general we argue as follows. We first observe that if $P \in C(K)$ then there is a unique point $Q \in C(K)$ such that C has hyperplane section $5P + Q$. The complete linear system $|P + Q|$ defines a morphism $C \to \mathbb{P}^1$. This gives an equation for C of the form $y^2 + A(x, z)y = B(x, z)$ where A and B are binary forms of degrees 2 and 4. By [**13**, Theorem 3.4] we may change coordinates on $\mathbb{P}^1$ (and make a substitution for y) so that $y^2 + A(x, z)y = B(x, z)$ has coefficients in $\mathcal{O}_K$, yet has discriminant Δ_E. Since $\mathrm{SL}_2(\mathcal{O}_K)$ acts transitively on $\mathbb{P}^1(K)$ we may assume that P and Q are the points on C above $(x : z) = (1 : 0)$. By a substitution $y \leftarrow y + \lambda x^2$ we may further assume that Q is the point $(x : z : y) = (1 : 0 : 0)$. Setting $z = 1$ gives an affine equation

$$y^2 + (lx^2 + mx + n)y = bx^3 + cx^2 + dx + e$$

where P and Q are now the points at infinity. We have $x \in \mathcal{L}(P + Q)$, $y \in \mathcal{L}(2P + Q)$ and $bx - ly \in \mathcal{L}(2P)$. The embedding $C \subset \mathbb{P}^5$ via $|5P + Q|$ is given by

$$(x_1 : \ldots : x_6) = (1 : x : y : (bx - ly)x : (bx - ly)y : (bx - ly)^2 x).$$

https://doi.org/10.1112/S1461157014000217 Published online by Cambridge University Press

The image differs from the curve we started with by a change of coordinates defined over K. It has secant variety defined by cubics

$$\begin{aligned}F_1 = {} & bex_1^2x_4 - lex_1^2x_5 - b^2ex_1x_2^2 + 2lbex_1x_2x_3 + bdx_1x_2x_4 - ldx_1x_2x_5 - l^2ex_1x_3^2 - nbx_1x_3x_4 \\ & + lnx_1x_3x_5 + cx_1x_4^2 - mx_1x_4x_5 + x_1x_4x_6 - x_1x_5^2 - b^2dx_2^3 + (2lbd + nb^2)x_2^2x_3 - bcx_2^2x_4 \\ & - (lc - mb)x_2^2x_5 - bx_2^2x_6 - (l^2d + 2lnb)x_2x_3^2 + 2lcx_2x_3x_4 + 2bx_2x_3x_5 + lx_2x_3x_6 \\ & - lx_2x_4x_5 + l^2nx_3^3 - (lm + b)x_3^2x_4 - lx_3^2x_5 + lx_3x_4^2\end{aligned}$$

and

$$\begin{aligned}F_2 = {} & -ex_1^2x_6 + 2bex_1x_2x_4 - dx_1x_2x_6 - 2lex_1x_3x_4 + nx_1x_3x_6 + dx_1x_4^2 - nx_1x_4x_5 - b^2ex_2^3 \\ & + 2lbex_2^2x_3 + nbx_2^2x_5 - cx_2^2x_6 - l^2ex_2x_3^2 - nbx_2x_3x_4 - lnx_2x_3x_5 + mx_2x_3x_6 + cx_2x_4^2 \\ & - x_2x_4x_6 + x_2x_5^2 + lnx_3^2x_4 + x_3^2x_6 - mx_3x_4^2 - 2x_3x_4x_5 + x_4^3.\end{aligned}$$

Moreover, the identity (4) is satisfied with $f(s,t) = A(s,t)^2 + 4B(s,t)$ and G_1, G_2 certain cubic forms with coefficients in $\mathbb{Z}[l,m,n,b,c,d,e]$. Then $\Delta(F_1,F_2) = \Delta_E$ as required. □

We say that pairs of cubic forms (F_1,F_2) and (F_1',F_2') are K-equivalent if they are related by the action of $\mathrm{GL}_2(K) \times \mathrm{GL}_6(K)$, as specified in (5) and (6).

Definition 7.5. Let $F_1, F_2 \in \mathcal{O}_K[x_1,\dots,x_6]$ be cubic forms defining the secant variety of a genus-one normal curve of degree 6. We say that (F_1,F_2) is *minimal* if $v(\Delta(F_1,F_2))$ is minimal among all pairs of cubics forms with coefficients in $\mathcal{O}_K$ that are K-equivalent to (F_1,F_2).

Corollary 7.6. *Let $C \subset \mathbb{P}^5$ be a genus-one normal curve of degree 6 defined over K. Let Δ_E be the minimal discriminant of the Jacobian elliptic curve E.*

(i) *If F_1 and F_2 have coefficients in $\mathcal{O}_K$ then $2^{12}\Delta(F_1,F_2) \in \mathcal{O}_K$.*
(ii) *A minimal model (F_1,F_2) for C exists. Moreover, $v(\Delta(F_1,F_2)) = v(\Delta_E) + 6\ell$ for some integer $\ell \geqslant -1 - 2v(2)$ we call the minimal level.*
(iii) *If $v(\Delta_E) < 6$ and $\mathrm{char}\,(k) \neq 2$ then $\ell \geqslant 0$. If, in addition, $C(K) \neq \emptyset$ then $\ell = 0$.*

Proof. (i) Since F_1 and F_2 are linearly independent over K, we can use Lemma 7.2 to reduce to the case where $\overline{F}_1$ and $\overline{F}_2$ are linearly independent over k. Then, by Theorem 7.3, f has coefficients in $\mathcal{O}_K$ and so $2^{12}\Delta(F_1,F_2) = \Delta(f) \in \mathcal{O}_K$. We expect that $\Delta(F_1,F_2) \in \mathcal{O}_K$. It may be possible to prove this by adapting the identity (4), so that f is replaced by a generalized binary quartic. This would be analogous to the proof of [**13**, Lemma 2.9] in the case $n = 4$.

(ii) By (i) we have $v(\Delta(F_1,F_2)) \geqslant -12v(2)$, and so minimal models exist. If f has coefficients in $\mathcal{O}_K$ then by [**13**, Lemma 3.2] and Theorem 4.1(iii) we have

$$v(\Delta(f)) \text{ or } v(\Delta(\pi f)) = v(\Delta_E) + 12m$$

for some integer $m \geqslant 0$. It follows that $\ell \geqslant -1 - 2v(2)$. We expect that $\ell \geqslant 0$ in all cases.

(iii) This is immediate from (i) and Theorem 7.4. In fact, arguing as in the proof of (ii), the condition $v(\Delta_E) < 6$ could be weakened to $v(\Delta_E) < v(\Delta_{E'})$ where E' is the quadratic twist of E by π. □

Our results have the following global application. A curve $C/\mathbb{Q}$ is said to be *everywhere locally soluble* if $C(\mathbb{R}) \neq \emptyset$ and $C(\mathbb{Q}_p) \neq \emptyset$ for all primes p.

Corollary 7.7. *Let $C/\mathbb{Q}$ be an everywhere locally soluble 6-covering of an elliptic curve $E/\mathbb{Q}$. Then C is isomorphic to a genus-one normal curve in $\mathbb{P}^5$ with secant variety defined by cubic forms $F_1, F_2 \in \mathbb{Z}[x_1,\dots,x_6]$ with $\Delta(F_1,F_2)$ equal to the minimal discriminant of E.*

https://doi.org/10.1112/S1461157014000217 Published online by Cambridge University Press

Proof. Cassels [10] showed that if an n-covering of an elliptic curve is everywhere locally soluble then it admits a $\mathbb{Q}$-rational divisor of degree n. We may therefore embed $C \subset \mathbb{P}^5$ as a genus-one normal curve of degree 6. The result now follows from Theorem 7.4 (with $K = \mathbb{Q}_p$) and strong approximation for $\mathrm{SL}_2 \times \mathrm{SL}_6$ over $\mathbb{Q}$. □

8. *Example*

Let $E/\mathbb{Q}$ be the elliptic curve

$$y^2 + y = x^3 + x^2 - 20404558x - 35483149947.$$

This is an elliptic curve with Mordell–Weil rank 2 and prime conductor $p = 1631859133$ taken from the Stein–Watkins database [27]. We used Magma [8] to compute everywhere locally soluble 2- and 3-coverings of E represented by the binary quartic

$$F = (733/4)x^4 + 181x^3z + 3979x^2z^2 + 1943xz^3 + 21117z^4,$$

and ternary cubic

$$G = 17x^3 - 14x^2y - 10x^2z - 57xy^2 + 36xyz + 41xz^2 - 43y^3 - 52y^2z - 104yz^2 - 5z^3.$$

Theorem 2.1 computes equations for the 6-covering of E that is the sum of F and G. The secant variety of this curve is defined by cubics

$$\begin{aligned} F_1 = {} & 41175z_{11}^3 - 12589z_{11}^2z_{12} + 17791z_{11}^2z_{13} - 1178025z_{11}^2z_{21} \\ & + 111252z_{11}^2z_{22} - 163938z_{11}^2z_{23} - 26576z_{11}z_{12}^2 + 6300z_{11}z_{12}z_{13} \\ & \qquad \vdots \qquad\qquad\qquad \vdots \\ & + 1633757z_{21}^2z_{23} - 2666032z_{21}z_{22}^2 + 649908z_{21}z_{22}z_{23} + 3188136z_{21}z_{23}^2 \\ & - 652977z_{22}^3 + 455246z_{22}^2z_{23} - 3402998z_{22}z_{23}^2 + 1121925z_{23}^3 \end{aligned}$$

and

$$\begin{aligned} F_2 = {} & -392675z_{11}^3 + 111252z_{11}^2z_{12} - 163938z_{11}^2z_{13} - 1887994z_{11}^2z_{21} \\ & + 175400z_{11}^2z_{22} - 260852z_{11}^2z_{23} + 268818z_{11}z_{12}^2 - 65625z_{11}z_{12}z_{13} \\ & \qquad \vdots \qquad\qquad\qquad \vdots \\ & + 3726130z_{21}^2z_{23} - 5804300z_{21}z_{22}^2 + 1394862z_{21}z_{22}z_{23} + 7094292z_{21}z_{23}^2 \\ & - 1502332z_{22}^3 + 1070278z_{22}^2z_{23} - 7608418z_{22}z_{23}^2 + 2490164z_{23}^3. \end{aligned}$$

The coefficients of F_1 and F_2 are integers with maximum absolute value 11718351. These cubics are linearly independent mod q for all primes q, and have discriminant $\Delta(F_1, F_2) = p^7$. The ad hoc methods for minimisation and reduction in [14, § 6.3] suggest making the substitution

$$\begin{pmatrix} z_{11} \\ z_{12} \\ z_{13} \\ z_{21} \\ z_{22} \\ z_{23} \end{pmatrix} = \begin{pmatrix} 18 & 16 & -6 & 3 & -34 & -19 \\ -4 & -7 & -15 & 16 & 23 & -32 \\ -21 & 2 & 5 & -17 & -4 & -4 \\ 18 & -1 & -23 & -4 & -2 & 36 \\ -12 & -27 & -3 & 12 & -8 & 1 \\ 10 & 1 & -2 & -31 & 11 & -18 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix}. \tag{8}$$

https://doi.org/10.1112/S1461157014000217 Published online by Cambridge University Press

The determinant of this matrix is p, and after making this substitution both cubics are divisible by p. The secant variety is now defined by

$$\begin{aligned} F_1' = {} & 15x_1^3 - 12x_1^2x_2 - 44x_1^2x_3 - 76x_1^2x_4 + 43x_1^2x_5 + 57x_1^2x_6 - 3x_1x_2^2 \\ & + 46x_1x_2x_3 - 39x_1x_2x_4 + 23x_1x_2x_5 - 77x_1x_2x_6 + 64x_1x_3^2 \\ & \qquad \vdots \qquad\qquad\qquad \vdots \\ & - 207x_3x_6^2 - 31x_4^3 + 76x_4^2x_5 - x_4^2x_6 - 29x_4x_5^2 + 55x_4x_5x_6 \\ & - 79x_4x_6^2 + 5x_5^3 - 52x_5^2x_6 + 15x_5x_6^2 + 122x_6^3 \end{aligned}$$

and

$$\begin{aligned} F_2' = {} & -27x_1^3 - 9x_1^2x_2 + 150x_1^2x_3 - 43x_1^2x_4 + 175x_1^2x_5 - 162x_1^2x_6 \\ & + 53x_1x_2^2 + 158x_1x_2x_3 - 9x_1x_2x_4 - 10x_1x_2x_5 - 245x_1x_2x_6 \\ & \qquad \vdots \qquad\qquad\qquad \vdots \\ & - 543x_3x_5x_6 - 123x_3x_6^2 + 143x_4^3 + 58x_4^2x_5 + 59x_4^2x_6 - 74x_4x_5^2 \\ & + x_4x_5x_6 - 247x_4x_6^2 + 7x_5^3 - 136x_5^2x_6 + 495x_5x_6^2 + 111x_6^3. \end{aligned}$$

The coefficients of F_1' and F_2' are integers with maximum absolute value 542. These cubics are linearly independent mod q for all primes q, and have discriminant $\Delta(F_1', F_2') = p$.

On the singular locus of $\{F_1' = F_2' = 0\} \subset \mathbb{P}^5$ the Magma function `PointSearch` finds the point

$$(3859214977 : -4307304051 : 6829067848 : -2044256038 : 1674518872 : 1893140020).$$

By the substitution (8) this corresponds to

$$\begin{pmatrix} z_{11} & z_{12} & z_{13} \\ z_{21} & z_{22} & z_{23} \end{pmatrix} = \begin{pmatrix} 139461472460 & 142496392463 & 35031066301 \\ 10314359739 & -13465342697 & -68341834433 \end{pmatrix}.$$

The 2×2 minors of this matrix define a point

$$(9266759548221841924682 : -9892375880512983270619 : 334765557307523787177 7)$$

on the plane cubic $\{G = 0\} \subset \mathbb{P}^2$. By the classical formulae for the 3-covering map (see [1]), this maps down to a point $P \in E(\mathbb{Q})$ with canonical height $\widehat{h}(P) \approx 307.45928$.

References

1. S. Y. An, S. Y. Kim, D. C. Marshall, S. H. Marshall, W. G. McCallum and A. R. Perlis, 'Jacobians of genus one curves', *J. Number Theory* 90 (2001) no. 2, 304–315.
2. M. Bhargava and A. Shankar, 'Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves', Preprint, 2013, arXiv:1006.1002v3 [math.NT].
3. M. Bhargava and A. Shankar, 'Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0', Preprint, 2013, arXiv:1007.0052v2 [math.NT].
4. M. Bhargava and A. Shankar, 'The average number of elements in the 4-Selmer groups of elliptic curves is 7', Preprint, 2013, arXiv:1312.7333 [math.NT].
5. M. Bhargava and A. Shankar, 'The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1', Preprint, 2013, arXiv:1312.7859 [math.NT].
6. M. Bhargava and W. Ho, 'Coregular spaces and genus one curves', Preprint, 2013, arXiv:1306.4424 [math.AG].
7. C. Birkenhake and H. Lange, *Complex abelian varieties*, 2nd edn, Grundlehren der Mathematischen Wissenschaften 302 (Springer, Berlin, 2004).

https://doi.org/10.1112/S1461157014000217 Published online by Cambridge University Press

8. W. Bosma, J. Cannon and C. Playoust, 'The Magma algebra system I: the user language', *J. Symbolic Comput.* 24 (1997) 235–265; see also the Magma home page at http://magma.maths.usyd.edu.au/magma/.
9. H.-C. Graf von Bothmer and K. Hulek, 'Geometric syzygies of elliptic normal curves and their secant varieties', *Manuscripta Math.* 113 (2004) no. 1, 35–68.
10. J. W. S. Cassels, 'Arithmetic on curves of genus 1, IV. Proof of the Hauptvermutung', *J. reine angew. Math.* 211 (1962) 95–112.
11. P. L. Clark, 'The period-index problem in WC-groups, I. Elliptic curves', *J. Number Theory* 114 (2005) no. 1, 193–208.
12. J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon and M. Stoll, 'Explicit n-descent on elliptic curves, I. Algebra', *J. reine angew. Math.* 615 (2008) 121–155.
13. J. E. Cremona, T. A. Fisher and M. Stoll, 'Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves', *Algebra Number Theory* 4 (2010) no. 6, 763–820.
14. T. A. Fisher, 'Finding rational points on elliptic curves using 6-descent and 12-descent', *J. Algebra* 320 (2008) no. 2, 853–884.
15. T. A. Fisher, 'The invariants of a genus one curve', *Proc. Lond. Math. Soc.* (3) 97 (2008) 753–782.
16. T. A. Fisher, 'Pfaffian presentations of elliptic normal curves', *Trans. Amer. Math. Soc.* 362 (2010) no. 5, 2525–2540.
17. T. A. Fisher, 'Minimisation and reduction of 5-coverings of elliptic curves', *Algebra Number Theory* 7 (2013) no. 5, 1179–1205.
18. B. H. Gross, 'On Bhargava's representation and Vinberg's invariant theory', *Frontiers of mathematical sciences* (eds B. Gu and S.-T. Yau; International Press, Somerville, MA, 2011) 317–321.
19. M. Gross and S. Popescu, 'Equations of $(1, d)$-polarized abelian surfaces', *Math. Ann.* 310 (1998) no. 2, 333–377.
20. J. Harris, *Algebraic geometry, a first course*, Graduate Texts in Mathematics 133 (Springer, New York, 1992).
21. R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics 52 (Springer, New York, 1977).
22. K. Hulek, 'Projective geometry of elliptic curves', *Astérisque* 137 (1986).
23. D. Mumford, 'Varieties defined by quadratic equations', *Questions on Algebraic Varieties (C.I.M.E., III Ciclo, Varenna, 1969)* (Edizioni Cremonese, Rome, 1970) 29–100.
24. C. O'Neil, 'The period-index obstruction for elliptic curves', *J. Number Theory* 95 (2002) no. 2, 329–339.
25. T. G. Room, *The geometry of determinantal loci* (Cambridge University Press, Cambridge, 1938).
26. G. Salmon, *A treatise on the higher plane curves*, 3rd edn (Hodges, Foster and Figgis, Dublin, 1879).
27. W. A. Stein and M. Watkins, 'A database of elliptic curves—first report', *Algorithmic number theory (Sydney 2002)*, Lecture Notes in Computer Science 2369 (Springer, Berlin, 2002) 267–275.
28. A. Weil, 'Remarques sur un mémoire d'Hermite', *Arch. Math. (Basel)* 5 (1954) 197–202.
29. A. Weil, 'Euler and the Jacobians of elliptic curves', *Arithmetic and geometry, Vol. I*, Progress in Mathematics 35 (eds M. Artin and J. Tate; Birkhäuser, Boston, 1983) 353–359.

Tom Fisher
University of Cambridge
DPMMS
Centre for Mathematical Sciences
Wilberforce Road
Cambridge
CB3 0WB
United Kingdom

T.A.Fisher@dpmms.cam.ac.uk

https://doi.org/10.1112/S1461157014000217 Published online by Cambridge University Press