INVARIANT THEORY FOR THE ELLIPTIC NORMAL QUINTIC, I. TWISTS OF X(5)

TOM FISHER

Abstract. A genus one curve of degree 5 is defined by the 4×4 Pfaffians of a 5×5 alternating matrix of linear forms on $\mathbb{P}^4$. We describe a general method for investigating the invariant theory of such models. We use it to explain how we found our algorithm for computing the invariants [12] and to extend our method in [14] for computing equations for visible elements of order 5 in the Tate-Shafarevich group of an elliptic curve. As a special case of the latter we find a formula for the family of elliptic curves 5-congruent to a given elliptic curve in the case the 5-congruence does *not* respect the Weil pairing. We also give an algorithm for doubling elements in the 5-Selmer group of an elliptic curve, and make a conjecture about the matrices representing the invariant differential on a genus one normal curve of arbitrary degree.

1. Introduction

A genus one normal curve $C \subset \mathbb{P}^{n-1}$ of degree $n \geq 3$ is a genus one curve embedded by a complete linear system of degree n. If $n \geq 4$ then the homogeneous ideal of C is generated by a vector space of quadrics of dimension $n(n-3)/2$.

Definition 1.1. A *genus one model* (of degree 5) is a 5×5 alternating matrix of linear forms on $\mathbb{P}^4$. We write $C_\phi \subset \mathbb{P}^4$ for the subvariety defined by the 4×4 Pfaffians of ϕ, and say that ϕ is *non-singular* if C_ϕ is a smooth curve of genus one.

It is a classical fact that (over $\mathbb{C}$) every genus one normal curve of degree 5 is of the form C_ϕ for some ϕ. Importantly for us, the proof using the Buchsbaum-Eisenbud structure theorem [5],[6] shows that this is still true over an arbitrary ground field.

There is a natural action of $\mathrm{GL}_5 \times \mathrm{GL}_5$ on the space of genus one models. The first factor acts as $M : \phi \mapsto M\phi M^T$ and the second factor by changing co-ordinates on $\mathbb{P}^4$. To describe this situation we adopt the following notation. Let V and W be 5-dimensional vector spaces with bases $v_0, \ldots, v_4$ and $w_0, \ldots, w_4$. The dual bases for V^* and W^* will be denoted $v_0^*, \ldots, v_4^*$ and $w_0^*, \ldots, w_4^*$. We identify the space of genus one models with $\wedge^2 V \otimes W$ via

$$\phi = (\phi_{ij}) \longleftrightarrow \textstyle\sum_{i<j} (v_i \wedge v_j) \otimes \phi_{ij}(w_0, \ldots, w_4).$$

Date: 14th October 2011.

With this identification the action of $\mathrm{GL}_5 \times \mathrm{GL}_5$ becomes the natural action of $\mathrm{GL}(V) \times \mathrm{GL}(W)$ on $\wedge^2 V \otimes W$. By squaring and then identifying $\wedge^4 V \cong V^*$ there is a natural map

$$P_2 : \wedge^2 V \otimes W \to V^* \otimes S^2 W = \mathrm{Hom}(V, S^2 W). \tag{1}$$

Explicitly $P_2(\phi) = (v_i \mapsto p_i(w_0, \ldots, w_4))$ where $p_0, \ldots, p_4$ are the 4×4 Pfaffians of ϕ. Thus V may be thought of as the space of quadrics defining C_ϕ and W as the space of linear forms on $\mathbb{P}^4$. Despite this clear geometric distinction, we show in this paper that certain covariants that mix up the roles of V and W have interesting arithmetic applications.

We work over a perfect field K with characteristic not equal to 2, 3 or 5. The co-ordinate ring $K[\wedge^2 V \otimes W]$ is a polynomial ring in 50 variables.

Theorem 1.2. *The ring of invariants for* $\mathrm{SL}(V) \times \mathrm{SL}(W)$ *acting on* $K[\wedge^2 V \otimes W]$ *is generated by invariants* c_4 *and* c_6 *of degrees* 20 *and* 30*. If we scale them as specified in* [12] *and put* $\Delta = (c_4^3 - c_6^2)/1728$ *then*

(i) *A genus one model* ϕ *is non-singular if and only if* $\Delta(\phi) \neq 0$.

(ii) *If* ϕ *is non-singular then* C_ϕ *has Jacobian elliptic curve*

$$y^2 = x^3 - 27c_4(\phi)x - 54c_6(\phi).$$

Proof: See [12, Theorem 4.4]. □

The invariants c_4 and c_6 are too large to write down as explicit polynomials. Nonetheless we gave an algorithm for evaluating them in [12, Section 8]. By Theorem 1.2 this gives an algorithm for computing the Jacobian. In [14] we studied a covariant we call the Hessian. Explicitly it is a 50-tuple of homogeneous polynomials of degree 11 defining a map $H : \wedge^2 V \otimes W \to \wedge^2 V \otimes W$. Again rather than write down these polynomials we gave an algorithm for evaluating them. The Hessian allows us to compute certain twists of the universal family of elliptic curves parametrised by $X(5)$. We used it to find equations for visible elements of order 5 in the Tate-Shafarevich group of an elliptic curve, and to recover the formulae of Rubin and Silverberg [20] for families of 5-congruent elliptic curves. However in both these applications we were restricted to 5-congruences that respect the Weil pairing. In this paper we remove this restriction.

In Sections 2, 3, 4 we explain a general method for investigating the covariants associated to a genus one model. In particular we explain how we found the algorithm for computing the invariants in [12, Section 8]. One key result on the existence of covariants is left to a sequel to this paper [16]. Our account is still however self-contained, since in Section 8 we give explicit constructions of each of the covariants used in the second half of this paper. In Section 5 we use the covariants to write down families of 5-congruent elliptic curves. In Section 6 we give a formula for doubling in the 5-Selmer group of an elliptic curve and extend our method in [14] for computing visible elements of the Tate-Shafarevich group.

In particular we check local solubility for each of the visible elements of order 5 in the Weil-Châtelet group that were considered in [8]. In Section 7 we study a covariant that describes the invariant differential. This is needed not only for some of the constructions in Section 8, but also leads us to make a conjecture about the matrices representing the invariant differential on a genus one normal curve of arbitrary degree.

2. Covariants

We recall that a *rational representation* of a linear algebraic group G is a morphism of group varieties $\rho_Y : G \to \mathrm{GL}(Y)$.

Definition 2.1. Let Y be a rational representation of $\mathrm{GL}(V) \times \mathrm{GL}(W)$. A *covariant* (for Y) is a polynomial map $F : \wedge^2 V \otimes W \to Y$ such that $F \circ g = \rho_Y(g) F$ for all $g \in \mathrm{SL}(V) \times \mathrm{SL}(W)$.

The covariants in the case $Y = K$ is the trivial representation are the invariants as described in Theorem 1.2. For general Y the covariants form a module over the ring of invariants. In all our examples Y will be *homogeneous* by which we mean there exist integers r and s such that

$$\rho_Y(\lambda I_V, \mu I_W) = \lambda^r \mu^s I_Y$$

for all $\lambda, \mu \in K^\times$. A polynomial map $F : \wedge^2 V \otimes W \to Y$ is *homogeneous* of degree d if $F(\lambda \phi) = \lambda^d F(\phi)$ for all $\lambda \in K$, equivalently F is represented by a tuple of homogeneous polynomials of degree d.

Lemma 2.2. *Let $F : \wedge^2 V \otimes W \to Y$ be a covariant and suppose that both Y and F are homogeneous. Then there exist integers p and q called the* weights *of F such that*

$$F \circ g = (\det g_V)^p (\det g_W)^q \rho_Y(g) \circ F$$

for all $g = (g_V, g_W) \in \mathrm{GL}(V) \times \mathrm{GL}(W)$. Moreover if Y has degree (r, s) then

$$\begin{aligned} 2 \deg F &= 5p + r \\ \deg F &= 5q + s. \end{aligned} \tag{2}$$

Proof: The only 1-dimensional rational representations of GL_n are integer powers of the determinant. This proves the first statement. The second statement follows from the special case where g_V and g_W are scalar matrices. □

The first example of a covariant is the identity map

$$U : \wedge^2 V \otimes W \to \wedge^2 V \otimes W.$$

It has degree 1 and weights $(p, q) = (0, 0)$. The Pfaffian map P_2 defined in (1) is a covariant of degree 2 with weights $(p, q) = (1, 0)$. Subject to picking a basis for V, $\phi \in \wedge^2 V \otimes W$ is a 5×5 alternating matrix of linear forms and $P_2(\phi)$ is its vector of 4×4 Pfaffians. The determinant of the Jacobian matrix of these 5 quadrics defines a covariant

$$S_{10} : \wedge^2 V \otimes W \to S^5 W. \tag{3}$$

It has degree 10 and weights $(p, q) = (4, 1)$. It is shown in [19, VIII.2.5] that if $\phi \in \wedge^2 V \otimes W$ is non-singular then $S_{10}(\phi)$ is an equation for the secant variety of $C_\phi \subset \mathbb{P}^4$.

Our initial motivation for studying the covariants was that by constructing a large enough supply of covariants we might eventually arrive at an algorithm for computing the invariants, and so by Theorem 1.2 an algorithm for computing the Jacobian. This programme was successful, leading to the algorithm in [12]. We have subsequently found that some of the covariants have interesting arithmetic applications in their own right.

In the next two sections we explain our methods for studying the covariants. The key idea is that although the covariants are routinely too large to write down, their restrictions to the Hesse family, i.e. the universal family of elliptic curves over $X(5)$, are much easier to write down and are (nearly) characterised by their invariance properties under an appropriate action of $\mathrm{SL}_2(\mathbb{Z}/5\mathbb{Z})$. Thus our work resolves, albeit in one particular case, what is described in [1, Chapter V,§22] as the "mysterious role of invariant theory".

3. The extended Heisenberg group

We take $n \geq 5$ an odd integer. In this section we work over an algebraically closed field K of characteristic not dividing n, and let $\zeta_n \in K$ be a primitive nth root of unity. We write $E[n]$ for the n-torsion subgroup of an elliptic curve E and $e_n : E[n] \times E[n] \to \mu_n$ for the Weil pairing.

Definition 3.1. (i) The modular curve $Y(n) = X(n) \setminus \{\text{cusps}\}$ parametrises triples (E, P_1, P_2) where E is an elliptic curve and P_1, P_2 are a basis for $E[n]$ with $e_n(P_1, P_2) = \zeta_n$.
(ii) Let $Z(n) \subset \mathbb{P}^{n-1}$ be the subvariety defined by $a_0 = 0$, $a_{n-i} = -a_i$ and $\mathrm{rank}(a_{i-j}a_{i+j}) \leq 2$ where $(a_0 : \ldots : a_{n-1})$ are co-ordinates on $\mathbb{P}^{n-1}$ and the subscripts are read mod n.

There is an action of $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ on $Y(n)$ given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : (E, P_1, P_2) \mapsto (E, dP_1 - cP_2, -bP_1 + aP_2).$$

Let $S = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ be the usual generators for $\mathrm{SL}_2(\mathbb{Z})$. By abuse of notation we also write S and T for their images in $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.

Theorem 3.2. *There is an embedding $X(n) \subset \mathbb{P}^{n-1}$ such that*

(i) *$X(n) \subset Z(n)$ with equality if n is prime.*

(ii) *The action of* $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ *on* $X(n)$ *is given by* $\overline{\rho} : \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{PGL}_n(K)$ *where*

$$\overline{\rho}(S) \propto (\zeta_n^{ij})_{i,j=0,\ldots,n-1} \qquad \overline{\rho}(T) \propto \mathrm{Diag}(\zeta_n^{i^2/2})_{i=0,\ldots,n-1}$$

Moreover $\overline{\rho}$ *lifts uniquely to a representation* $\rho : \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{SL}_n(K)$.

Proof: The condition for equality in (i) is due to Vélu [26]. The remaining statements are proved in [15, Section 2]. Proofs that $\overline{\rho}$ lifts in the case $n = 5$ may also be found in [18], [22]. □

The Heisenberg group of level n is

$$H_n = \langle \sigma, \tau | \sigma^n = \tau^n = [\sigma,[\sigma,\tau]] = [\tau,[\sigma,\tau]] = 1 \rangle.$$

It is a non-abelian group of order n^3. The centre is a cyclic group of order n generated by $\zeta = [\sigma,\tau] = \sigma\tau\sigma^{-1}\tau^{-1}$. We write $\overline{H}_n$ for the quotient of H_n by its centre and identify $\overline{H}_n \cong (\mathbb{Z}/n\mathbb{Z})^2$ via $\overline{\sigma} \mapsto (1,0)$ and $\overline{\tau} \mapsto (0,1)$. Since each automorphism of H_n induces an automorphism of $\overline{H}_n$ there is a natural group homomorphism $\beta : \mathrm{Aut}(H_n) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. The kernel of β is $\overline{H}_n$ acting as the group of inner automorphisms. We may thus identify $\mathrm{Aut}(H_n)$ as a group of affine transformations. Let $\iota \in \mathrm{Aut}(H_n)$ be the involution given by $\iota(\sigma) = \sigma^{-1}$ and $\iota(\tau) = \tau^{-1}$. (Any involution ι with $\beta(\iota) = -I$ would do, but we have picked one for definiteness.) Since n is odd there is a unique section s_β for β with $s_\beta(-I) = \iota$. (This means that $s_\beta : \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{Aut}(H_n)$ is a group homomorphism with $\beta \circ s_\beta = \mathrm{id}$.) Indeed the image of s_β is the centraliser of ι in $\mathrm{Aut}(H_n)$.

Definition 3.3. The extended Heisenberg group is the semi-direct product

$$H_n^+ = H_n \ltimes \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}),$$

with group law $(h,\gamma)(h',\gamma') = (h\, s_\beta(\gamma)h', \gamma\gamma')$.

Remark 3.4. (i) The map s_β is explicitly given by

$$s_\beta((\begin{smallmatrix} a & b \\ c & d \end{smallmatrix})) : \sigma \mapsto \zeta^{-ac/2}\sigma^a\tau^c ;\; \tau \mapsto \zeta^{-bd/2}\sigma^b\tau^d.$$

(ii) The group H_5^+ was used by Horrocks and Mumford [18] in their construction of an indecomposable rank 2 vector bundle on $\mathbb{P}^4$. In fact the order of H_5^+ appears in the title of their paper.

We now identify H_n as a subgroup of $\mathrm{SL}_n(K)$ via the Schrödinger representation $\theta : H_n \to \mathrm{SL}_n(K)$ where

$$\theta(\sigma) = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \zeta_n & 0 & \cdots & 0 \\ 0 & 0 & \zeta_n^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & \zeta_n^{n-1} \end{pmatrix}, \quad \theta(\tau) = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}. \tag{4}$$

Since $\theta(\zeta) = \zeta_n I_n$ this identifies the centre of H_n with μ_n. Let N_n be the normaliser of H_n in $\mathrm{SL}_n(K)$. It may be checked that the automorphisms of $\overline{H}_n$ induced by conjugation by elements of N_n are precisely those that preserve the commutator pairing $\overline{H}_n \times \overline{H}_n \to \mu_n$. This proves the surjectivity of the map α in the following commutative diagram with exact rows and columns.

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & & \\
 & \mu_n \arrow[r, equal] \arrow[d] & \mu_n \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & H_n \arrow[r] \arrow[d] & N_n \arrow[r, "\alpha"] \arrow[d] & \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \overline{H}_n \arrow[r] \arrow[d] & \mathrm{Aut}(H_n) \arrow[r, "\beta"] \arrow[d] & \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \arrow[r] \arrow[d, "\det"] & 0 \\
 & 0 & (\mathbb{Z}/n\mathbb{Z})^\times \arrow[r, equal] \arrow[d] & (\mathbb{Z}/n\mathbb{Z})^\times \arrow[d] & \\
 & & 0 & 0 &
\end{tikzcd}$$

The restriction of s_β to $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ defines a projective representation

$$\overline{\rho} : \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{PGL}_n(K).$$

Comparison with the proof of Theorem 3.2 shows that this is the same as the projective representation considered there.

Lemma 3.5. *The following objects are in natural 1-1 correspondence.*

(i) *Sections s_α for α compatible with s_β.*
(ii) *Lifts of $\overline{\rho} : \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{PGL}_n(K)$ to $\rho : \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{SL}_n(K)$.*
(iii) *Extensions of $\theta : H_n \to \mathrm{SL}_n(K)$ to $\theta^+ : H_n^+ \to \mathrm{SL}_n(K)$.*

Proof. The projective representation $\overline{\rho}$ is defined by the requirement

$$\overline{\rho}(\gamma)\, h\, \overline{\rho}(\gamma)^{-1} = s_\beta(\gamma) h \quad \text{for all } h \in H_n,\ \gamma \in \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}).$$

But to say that s_α is a section for α compatible with s_β means

$$s_\alpha(\gamma)\, h\, s_\alpha(\gamma)^{-1} = s_\beta(\gamma) h \quad \text{for all } h \in H_n,\ \gamma \in \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}). \tag{5}$$

The correspondence between (i) and (ii) is clear. Now given s_α compatible with s_β we define $\theta^+(h,\gamma) = h s_\alpha(\gamma)$ and check using (5) that θ^+ is a homomorphism. Conversely, given θ^+ we set $s_\alpha(\gamma) = \theta^+(1,\gamma)$. This gives the correspondence between (i) and (iii). □

From the final statement of Theorem 3.2 we immediately deduce

Theorem 3.6. *The Schrödinger representation* $\theta : H_n \to \mathrm{SL}_n(K)$ *extends uniquely to a representation* $\theta^+ : H_n^+ \to \mathrm{SL}_n(K)$. *Moreover the normaliser of* $\theta(H_n)$ *in* $\mathrm{SL}_n(K)$ *is* $\theta^+(H_n^+)$.

Remark 3.7. The Schrödinger representation has $\phi(n)$ conjugates obtained by either changing our choice of ζ_n or precomposing with an automorphism of H_n. We may apply Theorem 3.6 to any one of these representations. This is important for our applications and explains why we were careful to define H_n^+ before introducing the Schrödinger representation.

4. Discrete covariants

In this section we work over an algebraically closed field of characteristic not equal to 2, 3 or 5. The Hesse family of elliptic normal quintics (studied for example in [14], [19]) is given by

$$\begin{array}{rccl} u: & \mathbb{A}^2 & \to & \wedge^2 V \otimes W \\ & (a,b) & \mapsto & a\sum(v_1 \wedge v_4)w_0 + b\sum(v_2 \wedge v_3)w_0 \end{array}$$

where the sums are taken over all cyclic permutations of the subscripts mod 5. The models $u(a,b)$, called the *Hesse models*, are representative of all genus one models in the following sense.

Lemma 4.1. *Every non-singular genus one model is* $\mathrm{GL}(V) \times \mathrm{GL}(W)$*-equivalent to a Hesse model.*

Proof: See [14, Proposition 4.1] □

The Hesse models are invariant under the following actions of the Heisenberg group H_5 on V and W.

$$\begin{array}{llll} \theta_V : H_5 \to \mathrm{SL}(V)\,; & \sigma : v_i \mapsto \zeta_5^{2i} v_i\,; & \tau : v_i \mapsto v_{i+1} \\ \theta_W : H_5 \to \mathrm{SL}(W)\,; & \sigma : w_i \mapsto \zeta_5^{i} w_i\,; & \tau : w_i \mapsto w_{i+1}. \end{array} \tag{6}$$

Our definition of the Hesse family differs from that in [14, Section 4] by a change of co-ordinates. This is to make the formulae (6) more transparent than those immediately preceding [14, Lemma 7.7].

Since θ_V and θ_W are conjugates of the Schrödinger representation they extend by Theorem 3.6 to representations of H_5^+. By abuse of notation we continue to write these representations as θ_V and θ_W. Let Y be a rational representation of $\mathrm{GL}(V) \times \mathrm{GL}(W)$. Then θ_V and θ_W define an action θ_Y of H_5^+ on Y. We write Y^{H_5} for the subspace of Y fixed by H_5. Since H_5^+ sits in an exact sequence

$$0 \longrightarrow H_5 \longrightarrow H_5^+ \longrightarrow \Gamma \longrightarrow 0$$

there is an action of $\Gamma = \mathrm{SL}_2(\mathbb{Z}/5\mathbb{Z})$ on Y^{H_5}. In the case $Y = \wedge^2 V \otimes W$ we find (by using Lemma 4.4 below to compute $\dim Y^{H_5}$) that $\mathrm{Im}(u) = (\wedge^2 V \otimes W)^{H_5}$.

The action of Γ is then described by a representation $\chi_1 : \Gamma \to \mathrm{GL}_2(K)$ with the defining property that

$$u \circ \chi_1(\gamma) = \theta_{\wedge^2 V \otimes W}(\gamma) \circ u \tag{7}$$

for all $\gamma \in \Gamma$.

Definition 4.2. Let $\pi : \Gamma \to \mathrm{GL}(Z)$ be a representation. A *discrete covariant* (for Z) is a polynomial map $f : \mathbb{A}^2 \to Z$ satisfying

$$u \circ \chi_1(\gamma) = \pi(\gamma) \circ u$$

for all $\gamma \in \Gamma$.

Theorem 4.3. *Let $F : \wedge^2 V \otimes W \to Y$ be a covariant. Then $f = F \circ u : \mathbb{A}^2 \to Y^{H_5}$ is a discrete covariant. Moreover F is uniquely determined by f.*

Proof: Since F is a covariant it is $\mathrm{SL}(V) \times \mathrm{SL}(W)$-equivariant (by definition) and therefore H_5^+-equivariant. So its restriction to $(\wedge^2 V \otimes W)^{H_5}$ takes values in Y^{H_5} and this restriction is Γ-equivariant.

If F_1 and F_2 restrict to the same discrete covariant f then by Lemma 4.1 they agree on all non-singular models. By Theorem 1.2 the non-singular models are Zariski dense in $\wedge^2 V \otimes W$ and from this we deduce that $F_1 = F_2$. □

For any given Y it is easy to compute the discrete covariants using invariant theory for the finite groups H_5 and Γ. We say that a discrete covariant $f : \mathbb{A}^2 \to Y^{H_5}$ *is a covariant* if it arises from a covariant $F : \wedge^2 V \otimes W \to Y$ as described in Theorem 4.3. It is important to note that not every discrete covariant is a covariant. We give examples below.

We recall the character table of H_p for p an odd prime. There are p^2+p-1 conjugacy classes with representatives ζ^i and $\sigma^j\tau^k$ for $i, j, k \in \mathbb{Z}/p\mathbb{Z}$ with $(j,k) \neq (0,0)$. There are p^2 one-dimensional characters indexed by $(r,s) \in (\mathbb{Z}/p\mathbb{Z})^2$. The remaining $p-1$ irreducible characters are conjugates of the Schrödinger representation. These are indexed by $t \in (\mathbb{Z}/p\mathbb{Z})^\times$.

	ζ^i	$\sigma^j\tau^k$
$\lambda_{r,s}$	1	ζ_p^{jr+ks}
θ_t	$p\zeta_p^{it}$	0

The dual of θ_t is θ_{-t}. From the character table we also deduce

Lemma 4.4. *Let $t, t' \in (\mathbb{Z}/p\mathbb{Z})^\times$.*

(i) $\theta_t \otimes \theta_{t'} \cong \begin{cases} p\theta_{t+t'} & \textit{if } t+t' \not\equiv 0 \pmod p \\ \bigoplus_{r,s} \lambda_{r,s} & \textit{if } t+t' \equiv 0 \pmod p \end{cases}$

(ii) $\wedge^d \theta_t \cong \begin{cases} \lambda_{0,0} & \textit{if } d = 0 \textit{ or } d = p \\ \frac{1}{p}\binom{p}{d}\theta_{dt} & \textit{if } 1 \le d \le p-1 \end{cases}$

(iii) $$S^d\theta_t \cong \begin{cases} \frac{1}{p}\binom{p+d-1}{d}\theta_{dt} & \textit{if } d \not\equiv 0 \pmod p \\ \lambda_{0,0} \oplus \frac{1}{p^2}\left(\binom{p+d-1}{d} - 1\right)\bigoplus_{r,s}\lambda_{r,s} & \textit{if } d \equiv 0 \pmod p. \end{cases}$$

By (6) the representations W, V, V^*, W^* are equivalent to θ_t for $t = 1,2,3,4$. In the examples at the end of this section we use Lemma 4.4 to compute the dimension of Y^{H_5} and then find a basis by inspection.

The representation $\chi_1 : \Gamma \to \mathrm{GL}_2(K)$ defined by (7) works out as

$$\begin{array}{rccl} \chi_1(S): & (a,b) & \mapsto & (\varphi a + b, a - \varphi b)/(\zeta_5^4 - \zeta_5) \\ \chi_1(T): & (a,b) & \mapsto & (\zeta_5^2 a, \zeta_5^3 b). \end{array}$$

where $\varphi = 1 + \zeta_5 + \zeta_5^4$. To fix our notation for the other irreducible characters we recall the character table for $\Gamma = \mathrm{SL}_2(\mathbb{Z}/5\mathbb{Z})$. In the first row we list the sizes of the conjugacy classes. The same symbols are used to denote both a representation and its character. We have written $\overline{\varphi} = 1 - \varphi$.

	1	1	20	20	30	12	12	12	12
	I	$-I$	ST	$-ST$	S	T	$-T$	T^2	$-T^2$
ψ_1	1	1	1	1	1	1	1	1	1
ψ_2	4	4	1	1	0	-1	-1	-1	-1
ψ_3	5	5	-1	-1	1	0	0	0	0
ψ_4	3	3	0	0	-1	φ	φ	$\overline{\varphi}$	$\overline{\varphi}$
ψ_5	3	3	0	0	-1	$\overline{\varphi}$	$\overline{\varphi}$	φ	φ
χ_1	2	-2	-1	1	0	$-\varphi$	φ	$-\overline{\varphi}$	$\overline{\varphi}$
χ_2	2	-2	-1	1	0	$-\overline{\varphi}$	$\overline{\varphi}$	$-\varphi$	φ
χ_3	4	-4	1	-1	0	-1	1	-1	1
χ_4	6	-6	0	0	0	1	-1	1	-1

The discrete covariants in the case $Y = K$ is the trivial representation form the ring of *discrete invariants* $R = K[a,b]^\Gamma$. This ring was already studied by Klein. We noted in [14, Section 3] that R is generated by

$$\begin{aligned} & D = ab(a^{10} - 11a^5b^5 - b^{10}) \\ (8) \qquad & c_4 = a^{20} + 228a^{15}b^5 + 494a^{10}b^{10} - 228a^5b^{15} + b^{20} \\ & c_6 = -a^{30} + 522a^{25}b^5 + 10005a^{20}b^{10} + 10005a^{10}b^{20} - 522a^5b^{25} - b^{30} \end{aligned}$$

subject only to the relation $c_4^3 - c_6^2 = 1728D^5$. The discrete invariants c_4 and c_6 are the restrictions of the invariants c_4 and c_6 in Theorem 1.2. Our use of the same notation for both a covariant and its restriction to the Hesse family should not cause any confusion in view of the uniqueness statement in Theorem 4.3.

For an arbitrary representation $\pi : \Gamma \to \mathrm{GL}_m(K)$ the discrete covariants form an R-module M_π. We write $M_\pi = \oplus_{d\geq 0} M_{\pi,d}$ for the grading by degree. For any given π and d it is easy to compute a basis for $M_{\pi,d}$ by linear algebra.

Lemma 4.5. *Let $\pi : \Gamma \to \mathrm{GL}_m(K)$ be a representation. Then*

(i) *M_π is a free $K[D, c_4]$-module of rank $2m$.*
(ii) *M_π is a free $K[D, c_6]$-module of rank $3m$.*
(iii) *M_π is a free $K[c_4, c_6]$-module of rank $5m$.*

Moreover if $M_\pi(r) \subset M_\pi$ is the direct sum of the graded pieces $M_{\pi,d}$ with $d \equiv r \pmod 5$, then $M_\pi(r)$ is a free $K[c_4, c_6]$-module of rank m.

Proof. In [14, Lemma 5.3] we showed that M_{χ_1} is a free $K[c_4, c_6]$-module. Since the same method (recalled from [3]) works in general it only remains to compute the ranks. Let $\mathbb{K} = K(a, b)^\Gamma$ be the field of fractions of R. By the normal basis theorem the $\mathbb{K}[\Gamma]$-module $K(a, b)$ is a copy of the regular representation. So if Γ acts on $Z = K^m$ via π then

$$\mathbb{K} \otimes Z \cong (K(a, b) \otimes Z)^\Gamma = \mathbb{K} \otimes M_\pi.$$

In particular $\dim_{\mathbb{K}}(\mathbb{K} \otimes M_\pi) = m$. Statements (i)-(iii) follow since

$$[\mathbb{K} : K(D, c_4)] = 2, \qquad [\mathbb{K} : K(D, c_6)] = 3, \qquad [\mathbb{K} : K(c_4, c_6)] = 5.$$

Finally we observe that the $M_\pi(r)$ for $r \in \mathbb{Z}/5\mathbb{Z}$ are free $K[c_4, c_6]$-modules with ranks m_r (say) adding up to $5m$. Multiplication by D shows that $m_r \le m_{r+2}$ for all r. Therefore $m_0 = \ldots = m_4 = m$ as required. □

The Hilbert series of M_π can be computed using Molien's theorem:

$$h(M_\pi, t) = \sum_{d=0}^{\infty} (\dim M_{\pi,d}) t^d = \frac{1}{|\Gamma|} \sum_{\gamma \in \Gamma} \frac{\operatorname{Tr} \pi(\gamma)}{1 - \operatorname{Tr} \chi_1(\gamma) t + t^2}. \tag{9}$$

For example taking $\pi = \chi_1$ we find

$$\begin{aligned} h(M_{\chi_1}, t) &= \frac{t + t^{11} + t^{19} + t^{29}}{(1 - t^{12})(1 - t^{20})} \\ &= \frac{t + t^{11} + t^{19} + t^{21} + t^{29} + t^{39}}{(1 - t^{12})(1 - t^{30})} \\ &= \frac{(t + t^{11}) + (t^{13} + t^{23}) + (t^{25} + t^{35}) + (t^{37} + t^{47}) + (t^{19} + t^{29})}{(1 - t^{20})(1 - t^{30})}. \end{aligned}$$

The numerators of these three expression give the degrees of the generators in each part of Lemma 4.5.

There are essentially two ways in which a discrete covariant can fail to be a covariant. The first is that the weights computed using (2) might fail to be integers. For example the discrete invariant D has weights $(p, q) = (24/5, 12/5)$ and so cannot be an invariant. (However Theorem 1.2 tells us that c_4, c_6 and $\Delta = D^5$ are invariants.) Likewise taking $Y = S^5 W$ the discrete covariant

$$(a, b) \mapsto ab \sum w_0^5 - 5b^2 \sum w_0^3 w_1 w_4 + 5a^2 \sum w_0^3 w_2 w_3 - 30ab \prod w_0.$$

has weights $(p, q) = (4/5, -3/5)$ and so cannot be a covariant. The second is that the discrete covariant f might arise from a *fractional covariant* by which we mean an $\mathrm{SL}(V) \times \mathrm{SL}(W)$-equivariant rational map $F : \wedge^2 V \otimes W \dashrightarrow Y$. It can happen that f is regular even when F is not. For example decomposing $(S^{10}W)^{H_5}$ as a Γ-module we find it contains a copy of the trivial representation. So there is a discrete covariant of degree 0. But there are clearly no covariants $\wedge^2 V \otimes W \to S^{10}W$ of degree 0.

In [16] we prove that these are the only two obstructions. More precisely we show that if $f : \mathbb{A}^2 \to Y^{H_5}$ is an integer weight discrete covariant then $\Delta^k f$ is a covariant for some integer $k \geq 0$. Moreover we give a practical method for determining the least such k.

If Y is homogeneous of degree (r, s) and $Y^{H_5} \neq 0$ then the action of the centre of H_5 shows that $2r + s \equiv 0 \pmod 5$. We see by (2) that p is an integer if and only if q is an integer. So the integer weight condition is just a congruence mod 5 on the degree of a covariant. In particular Lemma 4.5 shows that the $K[c_4, c_6]$-module of integer weight discrete covariants is a free module of rank $m = \dim Y^{H_5}$.

In this article we are primarily concerned with the rational representations Y in the following table. In each case Lemma 4.4 shows that $\dim Y^{H_5} = 2$ or 3. We list a basis for Y^{H_5} (the sums are taken over all cyclic permutations of the subscripts mod 5) followed by its character as a Γ-module. In the final column we list the degrees of the generators for the $K[c_4, c_6]$-module of integer weight discrete covariants, as computed using Molien's theorem.

Table 4.6

Y	basis for Y^{H_5}	character	degrees
$\wedge^2 V \otimes W$	$\sum (v_1 \wedge v_4) w_0$, $\sum (v_2 \wedge v_3) w_0$	χ_1	$1, 11$
$V^* \otimes \wedge^2 W$	$\sum v_0^* (w_1 \wedge w_4)$, $\sum v_0^* (w_2 \wedge w_3)$	χ_2	$7, 17$
$V \otimes \wedge^2 W^*$	$\sum v_0 (w_1^* \wedge w_4^*)$, $\sum v_0 (w_2^* \wedge w_3^*)$	χ_2	$13, 23$
$\wedge^2 V^* \otimes W^*$	$\sum (v_1^* \wedge v_4^*) w_0^*$, $\sum (v_2^* \wedge v_3^*) w_0^*$	χ_1	$19, 29$
$V^* \otimes S^2 W$	$\sum v_0^* w_0^2$, $\sum v_0^* w_1 w_4$, $\sum v_0^* w_2 w_3$	ψ_4	$2, 12, 22$
$S^2 V^* \otimes W^*$	$\sum v_0^{*2} w_0^*$, $\sum v_1^* v_4^* w_0^*$, $\sum v_2^* v_3^* w_0^*$	ψ_5	$14, 24, 34$
$S^2 V \otimes W$	$\sum v_0^2 w_0$, $\sum v_1 v_4 w_0$, $\sum v_2 v_3 w_0$	ψ_5	$6, 16, 26$
$V \otimes S^2 W^*$	$\sum v_0 w_0^{*2}$, $\sum v_0 w_1^* w_4^*$, $\sum v_0 w_2^* w_3^*$	ψ_4	$18, 28, 38$

Checking the conditions in [16] it turns out that each of these discrete covariants is a covariant. In [14] we gave an alternative proof in the cases $Y = \wedge^2 V \otimes W$ and $Y = \wedge^2 V^* \otimes W^*$ using evectants. The explicit constructions in Section 8 also show that each of these covariants exists at least as a fractional covariant.

The discrete covariant of degree 2 for $Y = V^* \otimes S^2 W$ is $P_2 = \sum v_i^* p_i$ where

$$p_i = ab w_i^2 + b^2 w_{i-1} w_{i+1} - a^2 w_{i-2} w_{i+2} \tag{10}$$

and the discrete covariant of degree 6 for $Y = S^2 V \otimes W$ is

$$Q_6 = \sum (5a^3 b^3 v_0^2 + a(a^5 - 3b^5) v_1 v_4 - b(3a^5 + b^5) v_2 v_3) w_0.$$

Substituting $v_i = p_i$ in Q_6 gives a covariant of degree 10 for $Y = S^5W$ which turns out to be (a scalar multiple of) the secant variety covariant (3). This suggested to us the algorithm for computing Q_6 in [12, Section 8] that is the key step in our algorithm for computing the invariants.

In the remainder of this article we are concerned with arithmetic applications of the covariants in Table 4.6 and in algorithms for evaluating them on (non-singular) genus one models.

5. Families of 5-congruent elliptic curves

From now on K will be a field of characteristic 0 with algebraic closure $\overline{K}$.

Definition 5.1. (i) Elliptic curves E and E' over K are n-congruent if $E[n]$ and $E'[n]$ are isomorphic as Galois modules.
(ii) The modular curve $Y_E^{(r)}(n) = X_E^{(r)}(n) \setminus \{\text{cusps}\}$ parametrises the family of elliptic curves n-congruent to E via an isomorphism ψ with $e_n(\psi S, \psi T) = e_n(S,T)^r$ for all $S, T \in E[n]$.

The curves $X_E^{(r)}(n)$ depend only on the class of $r \in (\mathbb{Z}/n\mathbb{Z})^\times$ modulo squares. In the cases $r = \pm 1$ we denote them $X_E(n)$ and $X_E^-(n)$. Rubin and Silverberg [20], [21], [23] computed formulae for the families of elliptic curves parametrised by $Y_E(n)$ for $n = 2, 3, 4, 5$. In [14] we gave a new proof of their result and extended to $Y_E^-(n)$ for $n = 3, 4, 5$. In the case $n = 5$ this is not so interesting since -1 is a square mod 5. In Theorem 5.8 below we remedy this by giving a formula for the family of elliptic curves parametrised by $Y_E^{(2)}(5)$.

First we need some preliminaries on Heisenberg groups. Since we have dropped our earlier assumption that K is algebraically closed our point of view is slightly different from that in Section 3.

Definition 5.2. A *Heisenberg group* is a Galois invariant subgroup $H \subset \mathrm{SL}_n(\overline{K})$ such that

(i) H is the inverse image of a subgroup $\Delta \subset \mathrm{PGL}_n(\overline{K})$ with $\Delta \cong (\mathbb{Z}/n\mathbb{Z})^2$.
(ii) Taking commutators in H induces a non-degenerate pairing $\Delta \times \Delta \to \mu_n$.

Let $C \subset \mathbb{P}^{n-1}$ be a genus one normal curve of degree n. The Heisenberg group defined by C is the group of all matrices in $\mathrm{SL}_n(\overline{K})$ that act on C as translation by an n-torsion point of its Jacobian E. In this case the commutator pairing is the Weil pairing $e_n : E[n] \times E[n] \to \mu_n$. If C is a curve of degree $n = 5$ then there is another Heisenberg group determined by C coming instead from the action of $E[5]$ on the space of quadrics defining C.

Lemma 5.3. *Let $\phi \in \wedge^2 V \otimes W$ be non-singular and let $E = \mathrm{Jac}(C_\phi)$. Then there are projective representations $\chi_V : E[5] \to \mathrm{PGL}(V)$ and $\chi_W : E[5] \to \mathrm{PGL}(W)$ such that*

(i) *The action of* $E[5]$ *on* $C_\phi \subset \mathbb{P}(W^*)$ *is given by* χ_W *and*
(ii) $(\chi_V(T), \chi_W(T))\phi \propto \phi$ *for all* $T \in E[5]$.

Proof: If $g_W \in \mathrm{GL}(W)$ describes an automorphism of C_ϕ then by [14, Lemma 7.6] there exists $g_V \in \mathrm{GL}(V)$, unique up to sign, such that $(g_V, g_W)\phi = \phi$. So once we have used (i) to define χ_W, condition (ii) uniquely determines χ_V. □

The projective representations χ_V and χ_W determine Heisenberg groups

$$H_1 \subset \mathrm{SL}(W^*) \quad H_2 \subset \mathrm{SL}(V^*) \quad H_3 \subset \mathrm{SL}(V) \quad H_4 \subset \mathrm{SL}(W) \tag{11}$$

where the first of these is the Heisenberg group defined by C_ϕ. It follows by (6) that the commutator pairing on $E[5]$ induced by H_r is the rth power of the Weil pairing.

Theorem 5.4. *Let* $\phi \in \wedge^2 V \otimes W$ *be a non-singular genus one model determining Heisenberg groups* $H_1, \ldots, H_4$ *as above. Then the genus one normal curves with Heisenberg group* H_r *are the* $C_{\phi'}$ *for* ϕ' *a non-singular member of the pencil spanned by* $F_1(\phi)$ *and* $F_2(\phi)$ *where* F_1 *and* F_2 *are a basis for the* $K[c_4, c_6]$*-module of covariants* $\wedge^2 V \otimes W \to Y$ *and*

$$Y = \begin{cases} \wedge^2 V \otimes W & \text{if } r = 1 \\ V \otimes \wedge^2 W^* & \text{if } r = 2 \\ V^* \otimes \wedge^2 W & \text{if } r = 3 \\ \wedge^2 V^* \otimes W^* & \text{if } r = 4. \end{cases}$$

Proof: This generalises [14, Theorem 8.2] where we treated the case $r = 1$.

For the proof we may assume that K is algebraically closed. By Lemma 4.1 and the covariance of F_1 and F_2 we may assume that $\phi = u(a, b)$ is a Hesse model. Then each H_r is the standard Heisenberg group generated by the matrices (4). By [14, Lemma 7.5] the genus one normal curves with this Heisenberg group are the $C_{\phi'}$ for ϕ' a non-singular Hesse model. Splitting into the cases $r = 1, 2, 3, 4$ we checked by computing the discrete covariants (see Remark 5.5 below for the case $r = 3$) that $F_1(\phi)$ and $F_2(\phi)$ are linearly independent. They therefore span the space of Hesse models. □

In [14] we studied the cases $r = 1, 4$. We now work out explicit formulae in the case $r = 3$. According to the table at the end of Section 4 the $K[c_4, c_6]$-module of covariants for $Y = V^* \otimes \wedge^2 W$ is generated by covariants Ψ_7 and Ψ_{17} of degrees 7 and 17. The corresponding discrete covariants are

$$(a, b) \mapsto f_d(a, b) \sum v_0^*(w_1 \wedge w_4) + g_d(a, b) \sum v_0^*(w_2 \wedge w_3) \tag{12}$$

where

$$f_7(a, b) = b^2(7a^5 - b^5), \qquad f_{17}(a, b) = b^2(17a^{15} + 187a^{10}b^5 + 119a^5b^{10} + b^{15}),$$
$$g_7(a, b) = a^2(a^5 + 7b^5), \qquad g_{17}(a, b) = -a^2(a^{15} - 119a^{10}b^5 + 187a^5b^{10} - 17b^{15}).$$

Remark 5.5. Direct calculation shows that $f_7 g_{17} - g_7 f_{17} = -24D^2$. We deduce that if ϕ is non-singular then $\Psi_7(\phi)$ and $\Psi_{17}(\phi)$ are linearly independent. In [16] we generalise this to arbitrary Y.

We recall that the ring of discrete invariants $K[a,b]^\Gamma$ is generated by the polynomials D, c_4 and c_6 in (8).

Lemma 5.6. *There are polynomials $\mathbf{D}(\lambda,\mu)$, $\mathbf{c}_4(\lambda,\mu)$ and $\mathbf{c}_6(\lambda,\mu)$ with coefficients in $K[c_4,c_6]$ such that*

$$\begin{aligned} \mathbf{D}(\lambda,\mu) &= 27 \cdot D(\lambda f_7 + \mu f_{17}, \lambda g_7 + \mu g_{17})/D(a,b)^2 \\ \mathbf{c}_4(\lambda,\mu) &= 54^2 \cdot c_4(\lambda f_7 + \mu f_{17}, \lambda g_7 + \mu g_{17}) \\ \mathbf{c}_6(\lambda,\mu) &= 54^3 \cdot c_6(\lambda f_7 + \mu f_{17}, \lambda g_7 + \mu g_{17}) \end{aligned}$$

Proof: The coefficients are discrete invariants of degree a multiple of 5. We can then therefore write them as polynomials in c_4 and c_6. (The factors 27, 54^2, 54^3 are included to make $\mathbf{D}$, $\mathbf{c}_4$, $\mathbf{c}_6$ primitive polynomials in $\mathbb{Z}[c_4,c_6,\lambda,\mu]$.) □

The polynomials $\mathbf{D}(\lambda,\mu)$, $\mathbf{c}_4(\lambda,\mu)$ and $\mathbf{c}_6(\lambda,\mu)$ are easily computed from the description in Lemma 5.6. We find

$$\begin{aligned} \mathbf{D}(\lambda,\mu) = &-(125c_4^3 + 64c_6^2)\lambda^{12} - 1620c_4^2c_6\lambda^{11}\mu - 66(25c_4^4 + 56c_4c_6^2)\lambda^{10}\mu^2 \\ &- 220(11c_4^3c_6 + 16c_6^3)\lambda^9\mu^3 + 1485(5c_4^5 + 4c_4^2c_6^2)\lambda^8\mu^4 + 792(53c_4^4c_6 + 28c_4c_6^3)\lambda^7\mu^5 \\ &+ 660(9c_4^6 + 164c_4^3c_6^2 + 16c_6^4)\lambda^6\mu^6 + 2376(19c_4^5c_6 + 44c_4^2c_6^3)\lambda^5\mu^7 \\ &+ 495(27c_4^7 + 104c_4^4c_6^2 + 112c_4c_6^4)\lambda^4\mu^8 + 220(81c_4^6c_6 + 136c_4^3c_6^3 + 80c_6^5)\lambda^3\mu^9 \\ &- 594(9c_4^8 - 32c_4^5c_6^2 - 16c_4^2c_6^4)\lambda^2\mu^{10} - 60(135c_4^7c_6 - 328c_4^4c_6^3 + 112c_4c_6^5)\lambda\mu^{11} \\ &- (729c_4^9 + 108c_4^6c_6^2 - 2896c_4^3c_6^4 + 1600c_6^6)\mu^{12}, \end{aligned}$$

$$\mathbf{c}_4(\lambda,\mu) = \frac{-1}{11^2 \cdot 12^2} \begin{vmatrix} \frac{\partial^2 \mathbf{D}}{\partial \lambda^2} & \frac{\partial^2 \mathbf{D}}{\partial \lambda \partial \mu} \\ \frac{\partial^2 \mathbf{D}}{\partial \lambda \partial \mu} & \frac{\partial^2 \mathbf{D}}{\partial \mu^2} \end{vmatrix} \quad \text{and} \quad \mathbf{c}_6(\lambda,\mu) = \frac{-1}{12 \cdot 20} \begin{vmatrix} \frac{\partial \mathbf{D}}{\partial \lambda} & \frac{\partial \mathbf{D}}{\partial \mu} \\ \frac{\partial \mathbf{c}_4}{\partial \lambda} & \frac{\partial \mathbf{c}_4}{\partial \mu} \end{vmatrix}.$$

These polynomials satisfy the relation

$$\mathbf{c}_4(\lambda,\mu)^3 - \mathbf{c}_6(\lambda,\mu)^2 = (c_4^3 - c_6^2)^2\, \mathbf{D}(\lambda,\mu)^5.$$

We have contributed them to Magma [4] as `HessePolynomials(5,2,[c4,c6])`.

Lemma 5.7. *The $K[c_4,c_6]$-module of covariants $\wedge^2 V \otimes W \to V^* \otimes \wedge^2 W$ is generated by covariants Ψ_7 and Ψ_{17} satisfying*

$$\begin{aligned} c_4(\lambda\Psi_7 + \mu\Psi_{17}) &= \mathbf{c}_4(\lambda,\mu)/54^2 \\ c_6(\lambda\Psi_7 + \mu\Psi_{17}) &= \mathbf{c}_6(\lambda,\mu)/54^3. \end{aligned}$$

Proof: By Lemma 4.1 and the covariance of Ψ_7 and Ψ_{17} it suffices to check these identities on the Hesse family. But in that case we are done by the definitions of $\mathbf{c}_4$ and $\mathbf{c}_6$ in Lemma 5.6. □

We say that elliptic curves E and E' are *indirectly* 5-*congruent* if there is an isomorphism of Galois modules $\psi : E[5] \cong E'[5]$ with $e_5(\psi S, \psi T) = e_5(S,T)^r$ for some $r \in \{2,3\}$. In the notation introduced at the start of this section the elliptic curves indirectly 5-congruent to E are parametrised by $Y_E^{(2)}(5)$.

Theorem 5.8. *Let E be an elliptic curve over K with Weierstrass equation*

$$y^2 = x^3 - 27c_4 x - 54c_6.$$

Then the family of elliptic curves parametrised by $Y_E^{(2)}(5)$ is

$$E_{\lambda,\mu} : \quad y^2 = x^3 - 12\mathbf{c}_4(\lambda,\mu)x - 16\mathbf{c}_6(\lambda,\mu)$$

where the coefficients of $\mathbf{c}_4(\lambda,\mu)$ and $\mathbf{c}_6(\lambda,\mu)$ are evaluated at $c_4, c_6 \in K$.

PROOF: We embed $E \subset \mathbb{P}^4$ via the complete linear system $|5.0_E|$. The image is defined by some $\phi \in \wedge^2 V \otimes W$ with invariants c_4 and c_6. Let $H_1, \ldots, H_4$ be the Heisenberg groups (11) determined by ϕ.
(i) Suppose that $\phi' = \lambda\Psi_7(\phi) + \mu\Psi_{17}(\phi)$ is non-singular. By Theorem 5.4 the genus one normal curves $C_\phi \subset \mathbb{P}^4$ and $C_{\phi'} \subset \mathbb{P}^4$ have Heisenberg groups H_1 and H_3. By Theorem 1.2 and Lemma 5.7 the Jacobians of these curves are E and $E_{\lambda,\mu}$. Since the Heisenberg group carries the information of both the action of Galois on the 5-torsion of the Jacobian, and the Weil pairing (via the commutator), it follows that E and $E_{\lambda,\mu}$ are indirectly 5-congruent.
(ii) Let E' be an elliptic curve indirectly 5-congruent to E. By [9, Theorem 5.2] there is a genus one normal curve $C' \subset \mathbb{P}^4$ with Jacobian E' and Heisenberg group H_3. Then Theorem 5.4 shows that $C' = C_{\phi'}$ for some $\phi' = \lambda\Psi_7(\phi) + \mu\Psi_{17}(\phi)$. Taking Jacobians gives $E' \cong E_{\lambda,\mu}$. □

We also worked out formulae corresponding to the case $r = 2$ of Theorem 5.4. We omit the details since the family of elliptic curves obtained is the same as that in Theorem 5.8. (We encountered a similar situation in [14] with the cases $r = \pm 1$.)

Example 5.9. Let $F/\mathbb{Q}$ be the elliptic curve $y^2 + xy = x^3 - 607x + 5721$ labelled $2834c1$ in Cremona's tables [7]. The invariants of this Weierstrass equation are $c_4 = 29137$ and $c_6 = -4986649$. Substituting into the above expression for $\mathbf{D}$ and then making a change of variables[1] to simplify we obtain

$$\begin{aligned}\mathfrak{D}(\xi,\eta) &= \frac{1}{2^{89} \cdot 3^{15} \cdot 13^9}\mathbf{D}(1663\xi + 2850\eta, 7\xi + 18\eta) \\ &= -60647\xi^{12} + 74183\xi^{11}\eta - 366344\xi^{10}\eta^2 - 965800\xi^9\eta^3 \\ &\quad + 1640430\xi^8\eta^4 - 166188\xi^7\eta^5 + 1473362\xi^6\eta^6 - 1041216\xi^5\eta^7 \\ &\quad + 1224300\xi^4\eta^8 + 816860\xi^3\eta^9 - 474188\xi^2\eta^{10} + 22692\xi\eta^{11} - 51256\eta^{12}.\end{aligned}$$

[1] This change of variables was found by minimising to make the numerical factor on the right hand side of (13) a small integer, and reducing as described in [24].

By Theorem 5.8 the family of elliptic curves indirectly 5-congruent to F is $y^2 = x^3 - 27\mathfrak{c}_4(\xi,\eta)x - 54\mathfrak{c}_6(\xi,\eta)$ where

$$\mathfrak{c}_4(\xi,\eta) = \frac{-1}{11^2}\begin{vmatrix} \frac{\partial^2 \mathfrak{D}}{\partial \xi^2} & \frac{\partial^2 \mathfrak{D}}{\partial \xi \partial \eta} \\ \frac{\partial^2 \mathfrak{D}}{\partial \xi \partial \eta} & \frac{\partial^2 \mathfrak{D}}{\partial \eta^2} \end{vmatrix} \quad \text{and} \quad \mathfrak{c}_6(\xi,\eta) = \frac{-1}{20}\begin{vmatrix} \frac{\partial \mathfrak{D}}{\partial \xi} & \frac{\partial \mathfrak{D}}{\partial \eta} \\ \frac{\partial \mathfrak{c}_4}{\partial \xi} & \frac{\partial \mathfrak{c}_4}{\partial \eta} \end{vmatrix}.$$

These polynomials satisfy the relation

$$\mathfrak{c}_4(\xi,\eta)^3 - \mathfrak{c}_6(\xi,\eta)^2 = 2 \cdot 13 \cdot 109^2 \cdot 1728\, \mathfrak{D}(\xi,\eta)^5. \tag{13}$$

We specialise ξ, η to integers with $\max(|\xi|,|\eta|) \leq 100$ and sort by conductor to obtain a list of elliptic curves that begins

ξ	η	conductor	$[a_1,\ldots,a_6]$
3	2	2834	$[1,-1,1,-8109,-279017]$
0	1	18157438	$[1,-1,1,68377761,119969009527]$
1	0	171873598	$[1,0,0,895245563,21917334070263]$
2	1	205326134	$[1,0,0,-637387852699482,-6550975667615204649116]$
1	1	1506404198	$[1,0,0,-793652608607,-207340288851298727]$
1	-1	6582143542	$[1,0,0,-2705846635122,-1178369764561303100]$

The first curve in this list is the elliptic curve E labelled $2834d1$ in Cremona's tables. We discuss the elliptic curves E and F further in Example 6.7.

6. Doubling in the 5-Selmer group and visibility

Let E/K be an elliptic curve. In [9] we interpreted the group $H^1(K, E[n])$ as parametrising Brauer-Severi diagrams $[C \to S]$ as twists of $[E \to \mathbb{P}^{n-1}]$. We also studied the obstruction map $\mathrm{Ob}_n : H^1(K,E[n]) \to \mathrm{Br}(K)[n]$ that sends the class of $[C \to S]$ to the class of the Brauer-Severi variety S. The diagrams with trivial obstruction, i.e. $S \cong \mathbb{P}^{n-1}$, are genus one normal curves of degree n. Strictly speaking a diagram includes the choice of an action of E on C. So in general a genus one normal curve of degree n with Jacobian E represents a pair of inverse elements in $H^1(K,E[n])$.

In the case $n = 5$ we obtain the following partial interpretation of $H^1(K,E[5])$ in terms of genus one models. We say that genus one models are *properly equivalent* if they are related by $(g_V, g_W) \in \mathrm{GL}(V) \times \mathrm{GL}(W)$ with $(\det g_V)^2 \det g_W = 1$.

Theorem 6.1. *Let c_4 and c_6 be the invariants of a Weierstrass equation for E. Then the genus one models over K with invariants c_4 and c_6, up to proper K-equivalence, are parametrised by* $\ker(\mathrm{Ob}_5) \subset H^1(K,E[5])$.

Proof: This is analogous to the case $n = 3$ treated in [11, Theorem 2.5]. The proof given there relies on a statement about invariant differentials which is generalised to the case $n = 5$ in [12, Proposition 5.19]. □

The obstruction map is not a group homomorphism and its kernel is not a group. So given two genus one models with the same invariants, their sum in $H^1(K,E[5])$

need not be represented by a genus one model. However the obstruction map is quadratic and in particular satisfies $\mathrm{Ob}_n(a\xi) = a^2\mathrm{Ob}_n(\xi)$ for $a \in \mathbb{Z}$. If ϕ is a genus one model representing $\xi \in \ker(\mathrm{Ob}_5)$ then $-\phi$ (which has the same invariants) represents $-\xi$. In this section we show how to find a model ϕ' representing $\pm 2\xi$. It turns out that $C_{\phi'}$ sits inside an ambient space $\mathbb{P}^4$ that is naturally the dual of the ambient space for C_ϕ.

First we need to recall another of the interpretations of $H^1(K, E[n])$ given in [9]. A *theta group* for $E[n]$ is a central extension of $E[n]$ by $\mathbb{G}_m$ with commutator given by the Weil pairing. The base theta group $\Theta_E \subset \mathrm{GL}_n(\overline{K})$ is the set of all matrices that act on the base diagram $[E \to \mathbb{P}^{n-1}]$ as translation by an n-torsion point of E. Then $H^1(K, E[n])$ parametrises the theta groups for $E[n]$ as twists of Θ_E.

In Section 5 we saw that a non-singular genus one model ϕ determines Heisenberg groups $H_1, \ldots, H_4$. We write Θ_r for the theta group generated by H_r and the scalar matrices. Writing $E = \mathrm{Jac}(C_\phi)$ we see that Θ_r is a theta group for $E[5]$ where the latter is equipped with the rth power of the Weil pairing.

Lemma 6.2. *Let $\phi, \phi' \in \wedge^2 V \otimes W$ be non-singular genus one models determining theta groups $\Theta_1, \ldots, \Theta_4$ and $\Theta'_1, \ldots, \Theta'_4$. If $\mathrm{Jac}(C_\phi) = \mathrm{Jac}(C_{\phi'}) = E$ then there exists $\xi \in H^1(K, E[5])$ and isomorphisms $\gamma_r : \Theta_r \cong \Theta'_r$ such that*

$$\sigma(\gamma_r)\gamma_r^{-1} : x \mapsto e_5(\xi_\sigma, x)^r x \qquad (14)$$

for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$ and $r \in (\mathbb{Z}/5\mathbb{Z})^\times$.

PROOF: The curves C_ϕ and $C_{\phi'}$ are isomorphic over $\overline{K}$. So by [12, Proposition 4.6] there exists $g = (g_V, g_W) \in \mathrm{GL}(V) \times \mathrm{GL}(W)$ with $g\phi = \phi'$. In fact we can choose g so that it induces the identity map on the Jacobian E. The isomorphisms $\gamma_1, \ldots, \gamma_4$ are conjugation by $g_W^{-T}, g_V^{-T}, g_V, g_W$ where the superscript $-T$ indicates inverse transpose. Then $\sigma(\gamma_r)\gamma_r^{-1}$ is conjugation by an element of Θ'_r above $\xi_\sigma \in E[5]$, with ξ_σ independent of r. The conclusion (14) follows since the commutator pairing for Θ_r is the rth power of the Weil pairing. □

Theorem 6.3. *Let E and F be elliptic curves over K and $\psi : E[5] \cong F[5]$ an isomorphism of Galois modules with $e_5(\psi S, \psi T) = e_5(S,T)^r$ for some $r \in (\mathbb{Z}/5\mathbb{Z})^\times$. Let $\Theta_1, \ldots, \Theta_4$ be the theta groups determined by a non-singular genus one model $\phi \in \wedge^2 V \otimes W$ with $\mathrm{Jac}(C_\phi) = E$. If Θ_1 is the twist of Θ_E by $\xi \in H^1(K, E[5])$ then Θ_r is the twist of Θ_F by $\psi_*(\xi) \in H^1(K, F[5])$*

PROOF: We first prove the case $\xi = 0$. We claim that if ϕ describes the image of $E \subset \mathbb{P}^4$ embedded by $|5.0_E|$ then $\Theta_r \to E[5]$ has a Galois equivariant section $T \mapsto M_T$ with $M_S M_T = e_5(S,T)^{r/2} M_{S+T}$. We recall the proof of this in the case $r = 1$ from [9, Lemma 3.11]. The $[-1]$-map on E lifts to $\iota \in \mathrm{PGL}_5(K)$. Then there is a unique scaling of M_T such that $M_T^5 = I$ and $\iota M_T \iota^{-1} = M_T^{-1}$. The uniqueness ensures that $T \mapsto M_T$ is Galois equivariant. Now if $M_S M_T = \lambda M_{S+T}$

then conjugating by ι gives $M_S^{-1}M_T^{-1} = \lambda M_{S+T}^{-1}$ and so $\lambda^2 = M_S M_T M_S^{-1} M_T^{-1} = e_5(S,T)$. This proves the claim when $r = 1$. The cases $r = 2, 3, 4$ are similar using that the $[-1]$-map induces involutions in $\mathrm{PGL}(V)$ and $\mathrm{PGL}(W)$. Applying the claim to both E and F we see that if $\Theta_1 \cong \Theta_E$ then $\Theta_r \cong \Theta_F$. This proves the theorem in the case $\xi = 0$. The general case follows by Lemma 6.2. □

According to Table 4.6 the $K[c_4, c_6]$-module of covariants for $Y = \wedge^2 V^* \otimes W^*$ is generated by covariants Π_{19} and Π_{29} of degrees 19 and 29. The corresponding discrete covariants are

$$(a,b) \mapsto \tfrac{1}{\deg c_k} \left(\tfrac{\partial c_k}{\partial a} \sum (v_1^* \wedge v_4^*) w_0^* + \tfrac{\partial c_k}{\partial b} \sum (v_2^* \wedge v_3^*) w_0^* \right) \tag{15}$$

for $k = 4, 6$. As noted in [14] these are the evectants of c_4 and c_6.

Theorem 6.4. *Let* $\Pi_{49} = \frac{1}{144}(c_6 \Pi_{19} - c_4 \Pi_{29})$ *be the covariant of degree* 49 *whose restriction to the Hesse family is*

$$(a,b) \mapsto D^4 \left(b \sum (v_1^* \wedge v_4^*) w_0^* - a \sum (v_2^* \wedge v_3^*) w_0^* \right)$$

If $\phi \in \wedge^2 V \otimes W$ *is non-singular and* $\phi' = \Pi_{49}(\phi)$ *then*

(i) C_ϕ *and* $C_{\phi'}$ *have the same Jacobian elliptic curve* E, *and*
(ii) *the class of* $[C_{\phi'} \to \mathbb{P}^4]$ *is twice the class of* $[C_\phi \to \mathbb{P}^4]$ *in* $H^1(K, E[5])$.

Proof: (i) By considering ϕ a Hesse model we deduce

$$c_4(\phi') = \Delta(\phi)^{16} c_4(\phi)$$
$$c_6(\phi') = \Delta(\phi)^{24} c_6(\phi)$$

It follows by Theorem 1.2 that the Jacobians are isomorphic.
(ii) We apply Theorem 6.3 in the case $\psi : E[5] \to E[5]$ is multiplication by 2. This shows that the double of $[C_\phi \to \mathbb{P}^4]$ has theta group Θ_4. By (i) and Theorem 5.4 this double is $[C_{\phi'} \to \mathbb{P}^4]$. □

Remarks 6.5. (i) Whether Theorem 6.4 is a formula for doubling or tripling in $H^1(K, E[5])$ depends on the choice of isomorphism $\mathrm{Jac}(C_\phi) \cong \mathrm{Jac}(C_{\phi'})$. We have not attempted to resolve these sign issues.
(ii) If K is a number field then the n-Selmer group $S^{(n)}(E/K)$ is by definition a subgroup $H^1(K, E[n])$. It is well known that $S^{(n)}(E/K) \subset \ker(\mathrm{Ob}_n)$. Thus Theorem 6.4 gives a formula for doubling/tripling in the 5-Selmer group.
(iii) Let $g = (g_V, g_W) \in \mathrm{GL}(V) \times \mathrm{GL}(W)$ be any element defined over K with $(\deg g_V)^2 (\det g_W) = \Delta(\phi)^4$, for example a pair of diagonal matrices. Then in terms of Theorem 6.1 the double/triple of ϕ is $\pm g^{-1} \Pi_{49}(\phi)$.

Example 6.6. Wuthrich [27] constructed an element of order 5 in the Tate-Shafarevich group of the elliptic curve $E/\mathbb{Q}$ with Weierstrass equation

$$y^2 + xy + y = x^3 + x^2 - 3146x + 39049.$$

His example (also discussed in [12, Section 9]) is defined by the 4×4 Pfaffians of

$$\begin{pmatrix} 0 & 310x_1 + 3x_2 + 162x_5 & -34x_1 - 5x_2 - 14x_5 & 10x_1 + 28x_4 + 16x_5 & 80x_1 - 32x_4 \\ & 0 & 6x_1 + 3x_2 + 2x_5 & -6x_1 + 7x_3 - 4x_4 & -14x_2 - 8x_3 \\ & & 0 & -x_3 & 2x_2 \\ & - & & 0 & -4x_1 \\ & & & & 0 \end{pmatrix}$$

The algorithms in [17] suggest making a change of co-ordinates

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} \leftarrow \begin{pmatrix} 0 & 4 & -8 & 4 & 8 \\ 0 & 0 & 0 & 0 & 16 \\ 0 & -4 & 4 & 0 & 12 \\ 4 & 5 & -15 & 2 & 7 \\ 4 & -12 & 20 & -12 & -8 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix}$$

so that Wuthrich's example becomes

$$\begin{pmatrix} 0 & x_2 + x_5 & -x_5 & -x_1 + x_2 & x_4 \\ & 0 & x_2 - x_3 + x_4 & x_1 + x_2 + x_3 - x_4 - x_5 & x_1 - x_2 - x_3 - x_4 - x_5 \\ & & 0 & x_1 - x_2 + 2x_3 - x_4 - x_5 & -x_2 - x_4 + x_5 \\ & - & & 0 & -x_3 - x_4 - 2x_5 \\ & & & & 0 \end{pmatrix}$$

Our Magma function `DoubleGenusOneModel` uses the algorithms in Section 8 to evaluate Π_{19} and Π_{29} and then returns $\Pi_{49} = \frac{1}{144}(c_6\Pi_{19} - c_4\Pi_{29})$. Running it on the above model ϕ gives a model ϕ' with entries

$$\phi'_{12} = 3534132778x_1 + 3583651940x_2 - 881947110x_3 - 323014538x_4 + 3395115339x_5$$
$$\phi'_{13} = 5079379222x_1 - 2965539950x_2 + 11022202860x_3 + 12821590868x_4 + 640276471x_5$$
$$\phi'_{14} = -10098238458x_1 - 1274966110x_2 - 7873816170x_3 - 3456923272x_4 - 62353929x_5$$
$$\phi'_{15} = -12929747724x_1 - 6790511810x_2 - 11113305270x_3 - 15161763156x_4 + 3241937033x_5$$
$$\phi'_{23} = -3381247332x_1 + 3810679160x_2 + 5919634530x_3 + 75326852x_4 - 1245085426x_5$$
$$\phi'_{24} = -3572860258x_1 - 5569480730x_2 - 953739600x_3 - 2138046812x_4 - 858145244x_5$$
$$\phi'_{25} = -4674149266x_1 - 943631490x_2 - 6754488160x_3 + 751535046x_4 + 117685567x_5$$
$$\phi'_{34} = -1851228934x_1 + 5238146110x_2 - 165588410x_3 - 2070411506x_4 + 678105748x_5$$
$$\phi'_{35} = -6992835070x_1 - 3744630360x_2 + 3130208220x_3 - 4523781310x_4 + 433739425x_5$$
$$\phi'_{45} = 780078472x_1 + 2039763820x_2 - 450062790x_3 - 7105731722x_4 + 1625466111x_5$$

The algorithms in [17] suggest making a change of co-ordinates

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} \leftarrow \begin{pmatrix} 92 & -36 & -153 & 129 & -131 \\ -54 & 84 & 5 & -206 & 139 \\ -63 & -174 & -60 & -79 & 53 \\ -111 & 106 & 206 & -115 & -162 \\ 314 & -466 & 158 & -328 & -12 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix}$$

whereupon the model ϕ' simplifies to

$$\begin{pmatrix} 0 & -x_4 + x_5 & x_3 - x_4 + x_5 & x_2 - x_5 & x_1 - x_2 + x_3 - x_4 - 2x_5 \\ & 0 & x_1 + x_5 & -x_2 - x_3 & -x_2 + x_5 \\ & & 0 & x_4 & -x_1 \\ & - & & 0 & x_1 + x_4 - x_5 \\ & & & & 0 \end{pmatrix}$$

This is the double in $Ш(E/\mathbb{Q})[5]$ of Wuthrich's example. If we double again then we get back to the original example. Moreover the matrices needed to minimise and reduce are the transposes of those used above.

Let E and F be a pair of n-congruent elliptic curves. In terminology introduced by Mazur [8] the *visible subgroup* of $H^1(K,E)$ explained by $F(K)$ is the image of the composite

$$\frac{F(K)}{nF(K)} \xrightarrow{\delta} H^1(K,F[n]) \cong H^1(K,E[n]) \xrightarrow{\iota} H^1(K,E)[n]$$

where the maps δ and ι come from the Kummer exact sequences for E and F, and the middle isomorphism is induced by the congruence. Our interest is in using visibility to compute explicit elements of $H^1(K,E)$. In [14] we gave examples in the cases $n = 2,3,4,5$ assuming in the case $n = 5$ that the congruence $E[5] \cong F[5]$ respects the Weil pairing. Using Theorems 5.4 and 6.3 and the explicit constructions in Section 8 we may now remove this restriction.

Example 6.7. We start with the pair of elliptic curves $E = 2834d1$ and $F = 2834c1$ taken from [8, Table 1]. We have already seen in Example 5.9 that E and F are indirectly 5-congruent. Alternatively this may be checked as follows. Let $\mathbf{c}_4(\lambda,\mu)$ and $\mathbf{c}_6(\lambda,\mu)$ be the polynomials defined in Section 5 with coefficients specialised to the invariants $c_4 = 29137$ and $c_6 = -4986649$ of F. Then writing $j_E = -389217^3/(2 \cdot 13 \cdot 109^3)$ for the j-invariant of E we find that the binary form of degree 60

$$(1728 - j_E)\mathbf{c}_4(\lambda,\mu)^3 + j_E \mathbf{c}_6(\lambda,\mu)^2 = 0$$

has a unique $\mathbb{Q}$-rational root. Substituting this root $(\lambda : \mu) = (3563 : 19)$ into Theorem 5.8 confirms that E and F are indirectly 5-congruent.

Our method is now the same as that in [14, Section 15] except that in place of the Hessian we use the covariants

$$\Psi_7, \Psi_{17} : \wedge^2 V \otimes W \to V^* \otimes \wedge^2 W.$$

We have $F(\mathbb{Q}) \cong \mathbb{Z}^2$ generated by $P_1 = (-10, 109)$ and $P_2 = (-28, 45)$. If we embedding $F \subset \mathbb{P}^4$ via the complete linear system $|4.0_F + P|$ with $P = P_1$ then the image is defined by a genus one model ϕ. Our Magma function `GenusOneModel(5,P)` computes such a model

$$\begin{pmatrix} 0 & x_2 + 2x_4 - 3x_5 & 3x_1 - x_2 + 8x_3 + 2x_4 - 3x_5 & x_1 - 2x_4 + 3x_5 & x_3 - x_4 + x_5 \\ & 0 & 3x_2 + 2x_3 + 2x_4 + 3x_5 & x_2 + x_3 & x_5 \\ & & 0 & x_3 + 2x_4 + 2x_5 & x_4 + x_5 \\ & - & & 0 & 0 \\ & & & & 0 \end{pmatrix}$$

with the same invariants as F. The algorithms in Section 8 for evaluating Ψ_7 and Ψ_{17} are implemented in our Magma function `HesseCovariants(phi,2)`. We use them to compute $\phi' = 3563\Psi_7(\phi) + 19\Psi_{17}(\phi)$. The algorithms in [17] suggest making a change of co-ordinates

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} \leftarrow \begin{pmatrix} -16 & 16 & -9 & -4 & -8 \\ 0 & 0 & -2 & -4 & 0 \\ 24 & 0 & 7 & -4 & 8 \\ 8 & 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix}$$

so that ϕ' becomes

$$\begin{pmatrix} 0 & -x_2 + x_3 & x_1 - x_5 & x_2 - 2x_5 & x_2 - x_4 - x_5 \\ & 0 & -x_1 + x_2 + x_3 + 2x_5 & -x_2 + x_4 + x_5 & -x_1 - x_2 \\ & & 0 & -x_1 + x_2 + x_4 & x_3 + x_4 \\ & - & & 0 & x_1 \\ & & & & 0 \end{pmatrix}.$$

This genus one model has the same invariants as E. In particular its 4×4 Pfaffians define a curve $C \subset \mathbb{P}^4$ with good reduction at all primes $p \neq 2, 13, 109$. For $p = 2, 13, 109$ we checked directly that $C(\mathbb{Q}_p) \neq \emptyset$. Since $E(\mathbb{Q}) = 0$ it follows that C represents a non-trivial element of $Ш(E/\mathbb{Q})[5]$. Repeating for $P = r_1 P_1 + r_2 P_2$ for $0 \le r_1, r_2 \le 4$ we similarly find equations for all elements in a subgroup of $Ш(E/\mathbb{Q})$ isomorphic to $(\mathbb{Z}/5\mathbb{Z})^2$.

The following corollary was already proved in many (but not all) cases in the appendix to [2].

Corollary 6.8. *Let (E, F, n) be any of the triples listed in* [8, Table 1]. *Then E and F are n-congruent, and the visible subgroup of $H^1(\mathbb{Q}, E)$ explained by $F(\mathbb{Q})$ is contained in* $Ш(E/\mathbb{Q})$.

Proof: The examples in this table all have $n = 3$ or 5. Using the methods in [14] and in this paper, we verified the congruences and computed equations for all relevant elements of $H^1(\mathbb{Q}, E)$. We then checked directly that these curves are everywhere locally soluble. □

7. The invariant differential

The following definition is suggested by the discussion in [12, Section 2].

Definition 7.1. Let $C \subset \mathbb{P}^{n-1}$ be a genus one normal curve with hyperplane section H. An Ω-*matrix* for C is an $n \times n$ alternating matrix of quadratic forms representing the linear map

$$\wedge^2 \mathcal{L}(H) \to \mathcal{L}(2H) \, ; \quad f \wedge g \mapsto \frac{f dg - g df}{\omega}$$

where ω is an invariant differential on C.

Since the natural map $S^2\mathcal{L}(H) \to \mathcal{L}(2H)$ is surjective it is clear that Ω-matrices exist. However for $n > 3$ their entries are only determined up to the addition of quadrics vanishing on C. Nonetheless we claim in Conjecture 7.4 below that there is a canonical choice.

From an Ω-matrix we may recover the invariant differential ω using the rule

$$\omega = \frac{x_j^2 d(x_i/x_j)}{\Omega_{ij}} \qquad \text{for any } i \neq j.$$

We may also characterise Ω-matrices as alternating matrices of quadratic forms such that

$$\begin{pmatrix} \partial f/\partial x_0 & \cdots & \partial f/\partial x_{n-1} \end{pmatrix} \Omega = 0$$

in $K(C)$ for all $f \in I(C)$, and Ω has rank 2 at all points on C.

Returning to the case $n = 5$ this suggests looking for covariants in the case $Y = \wedge^2 W^* \otimes S^2 W$. By Lemma 4.4 we have $\wedge^2\theta_4 \otimes S^2\theta_1 \cong 2\theta_3 \otimes 3\theta_2 \cong 6\sum_{r,s}\lambda_{r,s}$ and so $\dim Y^{H_5} = 6$. A basis for Y^{H_5} is

$$\begin{array}{ccc} \sum(x_1^* \wedge x_4^*)x_0^2, & \sum(x_1^* \wedge x_4^*)x_1x_4, & \sum(x_1^* \wedge x_4^*)x_2x_3, \\ \sum(x_2^* \wedge x_3^*)x_0^2, & \sum(x_2^* \wedge x_3^*)x_1x_4, & \sum(x_2^* \wedge x_3^*)x_2x_3. \end{array}$$

Since $-I, T \in \Gamma$ act on Y^{H_5} with traces -6 and 1 it is easy to see from the character table for Γ that Y^{H_5} has character $\chi_4 = S^5\chi_1$. The $K[c_4, c_6]$-module of integer weight discrete covariants is generated in degrees $5, 15, 15, 25, 25, 35$. Checking the conditions in [16] shows that all of these are covariants.

The discrete covariant of degree 5 is

$$\Omega_5 = \begin{pmatrix} 0 & \alpha_3 & \beta_1 & -\beta_4 & -\alpha_2 \\ -\alpha_3 & 0 & \alpha_4 & \beta_2 & -\beta_0 \\ -\beta_1 & -\alpha_4 & 0 & \alpha_0 & \beta_3 \\ \beta_4 & -\beta_2 & -\alpha_0 & 0 & \alpha_1 \\ \alpha_2 & \beta_0 & -\beta_3 & -\alpha_1 & 0 \end{pmatrix}$$

where

$$\begin{aligned} \alpha_i &= 5a^4bw_i^2 - 10a^3b^2w_{i-1}w_{i+1} + (a^5 - 3b^5)w_{i-2}w_{i+2} \\ \beta_i &= 5ab^4w_i^2 - (3a^5 + b^5)w_{i-1}w_{i+1} + 10a^2b^3w_{i-2}w_{i+2}. \end{aligned} \tag{16}$$

Proposition 7.2. *If $\phi \in \wedge^2 V \otimes W$ is non-singular then $\Omega_5(\phi)$ is an Ω-matrix for $C_\phi \subset \mathbb{P}^4$.*

Proof: By Lemma 4.1 and the covariance of Ω_5 it suffices to prove this for ϕ a Hesse model. Let $p_0, \ldots, p_4$ be the quadrics (10) defining C_ϕ and $J = (\partial p_i/\partial w_j)$ the Jacobian matrix. We checked by direct calculation that all the entries of $J\Omega_5$ belong to the homogeneous ideal $I(C_\phi) = (p_0, \ldots, p_4)$. Since $C_\phi \subset \mathbb{P}^4$ is a smooth curve the Jacobian matrix J has rank 3 at all points of C_ϕ. So Ω_5 has rank at most 2 on C_ϕ. Since an alternating matrix always has even rank it only remains to show that Ω_5 is non-zero on C_ϕ. By (10) and (16) it suffices to show that

$$\det \begin{pmatrix} ab & b^2 & -a^2 \\ 5a^4b & -10a^3b^2 & a^5 - 3b^5 \\ 5ab^4 & -3a^5 - b^5 & 10a^2b^3 \end{pmatrix} = 18D \tag{17}$$

is non-zero. Since $\Delta = D^5$ this is clear by Theorem 1.2 and our assumption that ϕ is non-singular. □

Taking the 4×4 Pfaffians of Ω_5 and identifying $\wedge^4 W^* = W$ gives a covariant for $Y = W \otimes S^4 W$. This is a scalar multiple of the vector of partial derivatives of the secant variety covariant (3). This observation not only gives an algorithm for computing Ω_5 (used in Section 8) but also suggested to us the following conjecture about Ω-matrices for genus one normal curves of arbitrary degree. The rth *higher secant variety* $\mathrm{Sec}^r C$ of a curve C is the Zariski closure of the locus of all $(r-1)$-planes spanned by r points on C. Thus the usual secant variety is $\mathrm{Sec}^2 C$.

Lemma 7.3. *Let $C \subset \mathbb{P}^{n-1}$ be a genus one normal curve of degree $n \geq 3$.*

(a) *If $n = 2r + 1$ is odd then $\mathrm{Sec}^r C \subset \mathbb{P}^{n-1}$ is a hypersurface $\{F = 0\}$ of degree n.*

(b) *If $n = 2r + 2$ is even then $\mathrm{Sec}^r C \subset \mathbb{P}^{n-1}$ is a complete intersection $\{F_1 = F_2 = 0\}$ where F_1 and F_2 each have degree $n/2$.*

Proof: See [10] or [25]. □

Let $R = K[x_0, \ldots, x_{n-1}]$ be the co-ordinate ring of $\mathbb{P}^{n-1}$ and write $R = \oplus_{d \geq 0} R_d$ for its usual grading by degree. We require that morphisms of graded R-modules have degree 0 and write $R(d)$ for the R-module with eth graded piece R_{d+e}.

Conjecture 7.4. *Let $C \subset \mathbb{P}^{n-1}$ be a genus one normal curve of degree $n \geq 3$, and let F, respectively F_1 and F_2, be as in Lemma 7.3.*

(a) *If n is odd then there is a minimal free resolution*

$$0 \longrightarrow R(-2n) \xrightarrow{P^T} R(-n-1)^n \xrightarrow{\Omega} R(-n+1)^n \xrightarrow{P} R$$

where Ω is an alternating matrix of quadratic forms and

$$P = \begin{pmatrix} \partial F/\partial x_0 & \cdots & \partial F/\partial x_{n-1} \end{pmatrix}.$$

Moreover P is (a scalar multiple of) the vector of $(n-1) \times (n-1)$ Pfaffians of Ω, and Ω is an Ω-matrix for C.

(b) *If n is even then there is a minimal free resolution*

$$0 \longrightarrow R(-n)^2 \xrightarrow{P^T} R(\tfrac{-n+2}{2})^n \xrightarrow{\Omega} R(\tfrac{-n+2}{2})^n \xrightarrow{P} R^2$$

where Ω is an alternating matrix of quadratic forms and

$$P = \begin{pmatrix} \partial F_1/\partial x_0 & \cdots & \partial F_1/\partial x_{n-1} \\ \partial F_2/\partial x_0 & \cdots & \partial F_2/\partial x_{n-1} \end{pmatrix}.$$

Moreover the 2×2 minors of P are (a fixed scalar multiple of) the $(n-2) \times (n-2)$ Pfaffians of Ω, and Ω is an Ω-matrix for C.

Remarks 7.5. (i) If $n = 3, 4$ then the equations in Lemma 7.3 are the equations for $\mathrm{Sec}^1 C = C$. The conjecture reduces to some well known formulae for the invariant differential.
(ii) If $n = 2r + 1$ is odd then it is known (see [25, Section 8]) that $\mathrm{Sec}^r C$ has singular locus $\mathrm{Sec}^{r-1} C$ and the latter is Gorenstein of codimension 3. It follows by the Buchsbaum-Eisenbud structure theorem [5], [6] that a minimal free resolution of the stated form exists. The content of the conjecture is that the alternating matrix constructed in this way is an Ω-matrix.
(iii) If $n = 5$ then it suffices to take $C = C_\phi$ with ϕ a Hesse model. We have already observed that the 4×4 Pfaffians of $\Omega_5(\phi)$ are the partial derivatives of $F = S_{10}(\phi)$. Combined with (ii) this proves the conjecture in the case $n = 5$.
(iv) We have tested the conjecture in some numerical examples over finite fields for $n = 6, 7, 8, 10, 12$.

8. Explicit constructions

We give evaluation algorithms for each of the covariants in Table 4.6 (as reproduced below). This is mainly of interest for the covariants Π_{19} and Π_{29} used in Example 6.6 and the covariants Ψ_7 and Ψ_{17} used in Example 6.7.

Y	degrees	covariants
$\wedge^2 V \otimes W$	$1, 11$	U, H
$V^* \otimes \wedge^2 W$	$7, 17$	Ψ_7, Ψ_{17}
$V \otimes \wedge^2 W^*$	$13, 23$	Ξ_{13}, Ξ_{23}
$\wedge^2 V^* \otimes W^*$	$19, 29$	Π_{19}, Π_{29}
$V^* \otimes S^2 W$	$2, 12, 22$	P_2, P_{12}, P_{22}
$S^2 V \otimes W$	$6, 16, 26$	Q_6, Q_{16}, Q_{26}
$V \otimes S^2 W^*$	$18, 28, 38$	R_{18}, R_{28}, R_{38}
$S^2 V^* \otimes W^*$	$14, 24, 34$	S_{14}, S_{28}, S_{38}

We fix our choice of generators by specifying them on the Hesse family. The covariant U is the identity map, whereas the Hessian is given by

$$H = -\tfrac{\partial D}{\partial b} \sum (v_1 \wedge v_4) w_0 + \tfrac{\partial D}{\partial a} \sum (v_2 \wedge v_3) w_0.$$

The corresponding formulae for $\Psi_7, \Psi_{17}, \Pi_{19}$ and Π_{29} are given in (12) and (15). We put

$$\Xi_d = f_d(a,b) \sum v_0 (w_1^* \wedge w_4^*) + g_d(a,b) \sum v_0 (w_2^* \wedge w_3^*)$$

where $f_{13}(a,b) = b^3(26a^{10} + 39a^5b^5 - b^{10})$, $g_{13}(a,b) = a^3(a^{10} + 39a^5b^5 - 26b^{10})$ and

$$f_{23}(a,b) = -b^3(46a^{20} + 1173a^{15}b^5 - 391a^{10}b^{10} + 207a^5b^{15} + b^{20}),$$
$$g_{23}(a,b) = a^3(a^{20} - 207a^{15}b^5 - 391a^{10}b^{10} - 1173a^5b^{15} + 46b^{20}).$$

We recall that P_2 is the map taking a genus one model to its vector of 4×4 Pfaffians. The remaining generators in the above table are uniquely determined by the following "Pfaffian identities".

$$\begin{aligned} P_2(\lambda U + \mu H) &= \lambda^2 P_2 + 2\lambda\mu P_{12} + \mu^2 P_{22} \\ P_2(\lambda \Psi_7 + \mu \Psi_{17}) &= \lambda^2 S_{14} + 2\lambda\mu S_{24} + \mu^2 S_{34} \\ P_2(\lambda \Xi_{13} + \mu \Xi_{23}) &= \lambda^2 Q_{26} - \lambda\mu(c_6 Q_6 + c_4 Q_{16}) + \mu^2(c_4^2 Q_6 + c_6 Q_{16} - c_4 Q_{26}) \\ P_2(\lambda \Pi_{19} + \mu \Pi_{29}) &= \lambda^2(c_4 R_{18} + R_{38}) + \lambda\mu(c_6 R_{18} + c_4 R_{28}) + \mu^2(c_6 R_{28} - c_4 R_{38}) \end{aligned}$$

The evaluation algorithms below are justified by checking them on the Hesse family, and then appealing to Lemma 4.1 and the appropriate covariance properties to show that they work for all non-singular models. (We do not consider the case where the input is singular.)

Lemma 8.1. *Let $(F, G) = (P_2, P_{12})$ or (Q_6, Q_{16}). If $\phi \in \wedge^2 V \otimes W$ is non-singular and $F(\phi)$ and $G(\phi)$ are represented by quadratic forms $f_0, \ldots, f_4$ and $g_0, \ldots, g_4$ in variables $x_0, \ldots, x_4$ then the 75 quintic forms $\{(f_i g_j + f_j g_i) x_k : i \leq j\}$ are linearly independent.*

Proof: It suffices to check this for $\phi = u(a,b)$ a Hesse model.

We arrange the coefficients of the quintic forms in a 75×126 matrix. The entries are homogeneous polynomials in $\mathbb{Q}[a,b]$. In principle we could finish the proof by computing the GCD of the 75×75 minors. In practice we first decompose the space of quintic forms into its eigenspaces for the action of $x_i \mapsto \zeta_5^i x_i$. This leaves us with one 15×26 matrix and four 15×25 matrices. Rather than compute all 15×15 minors we compute just those that correspond to sets of monomials that are invariant under cyclic permutations of the x_i. In each case we find that the GCD of these minors divides a power of the discriminant. □

We gave algorithms for evaluating the invariants c_4 and c_6 in [12, Section 8] and the Hessian H in [14, Section 11]. We compute P_2, P_{12} and P_{22} by taking 4×4 Pfaffians of linear combinations of U and H as indicated in the first of the Pfaffian identities above. We compute Q_6 as described in [12, Section 8]. Lemma 8.1 shows that we can solve for Q_{16} and $Q'_{26} = 5(4Q_{26} + 3c_4Q_6)$ using the identities

$$\begin{aligned} Q_{16}(P_2, P_{12}) &= Q_6(P_{12}, P_{12}), \\ Q'_{26}(P_2, P_{12}) &= Q_6(P_{12}, P_{22}) + 4Q_{16}(P_{12}, P_{12}). \end{aligned}$$

Next we use the determinant map $V \otimes (V \otimes W) \to S^5V$ to compute some covariants taking values in S^5V:

$$\begin{aligned} \det(\lambda U + \mu Q_6) &= \lambda^4 \mu M_{10} - 2\lambda^2\mu^3 M_{20} + \mu^5 M_{30}, \\ \det(\lambda H + \mu Q_6) &= \lambda^4 \mu M_{50} + 2\lambda^2\mu^3 M_{40} + \mu^5 M_{30}, \\ \det(\lambda U + \mu Q_{16}) &= \lambda^4 \mu M_{20} + 2\lambda^2\mu^3 M'_{50} + \mu^5 M_{80}. \end{aligned}$$

Lemma 8.1 shows that we can solve for R_{18} and R_{28} using the identities

$$\begin{aligned} R_{18}(Q_6, Q_{16}) &= \tfrac{-1}{18}(5c_6M_{10} + 14c_4M_{20} + M_{40}), \\ R_{28}(Q_6, Q_{16}) &= \tfrac{-1}{792}(9c_4^2M_{10} + 620c_6M_{20} - 270c_4M_{30} + M_{50} - 216M'_{50}). \end{aligned}$$

Then we compute Π_{19} and Π_{29} using the natural map

$$\begin{aligned} (\wedge^2V \otimes W) \times (V \otimes S^2W^*) &\to \wedge^2V^* \otimes W^* \\ (U, R_{18}) &\mapsto 2\Pi_{19} \\ (U, R_{28}) &\mapsto 2\Pi_{29}. \end{aligned}$$

In Section 7 we constructed a covariant $\Omega_5 : \wedge^2V \otimes W \to \wedge^2W^* \otimes S^2W$. Conjecture 7.4 (which is a theorem in the case $n = 5$) gives an algorithm for computing Ω_5 (up to sign) using minimal free resolutions. We may represent P_{12} and P_{22} as 5-tuples of quadrics and Ω_5 as a 5×5 alternating matrix of quadrics. Then Ψ_7 and Ψ_{17} tell us how to write the quadrics in P_{12} and P_{22} as linear combinations of the quadrics in Ω_5. In basis-free language there is a natural map

$$\begin{aligned} (V^* \otimes \wedge^2W) \times (\wedge^2W^* \otimes S^2W) &\to V^* \otimes S^2W \\ (\Psi_7, \Omega_5) &\mapsto P_{12} \\ (\Psi_{17}, \Omega_5) &\mapsto \tfrac{1}{2}(P_{22} + c_4P_2). \end{aligned}$$

The proof of Proposition 7.2 shows that if ϕ is non-singular then the entries of $\Omega_5(\phi)$ above the diagonal are linearly independent. We can therefore solve for Ψ_7 and Ψ_{17} by linear algebra. We then compute Ξ_{13} and Ξ_{23} using the natural map

$$\begin{aligned}(V^* \otimes \wedge^2 W) \times (S^2 V \otimes W) &\to V \otimes \wedge^2 W^* \\ (\Psi_7, Q_6) &\mapsto 2\,\Xi_{13} \\ (\Psi_7, Q_{16}) &\mapsto -2\,\Xi_{23}.\end{aligned}$$

Since we only computed Ω_5 up to sign we have only computed Ψ_7, Ψ_{17}, Ξ_{13} and Ξ_{23} up to sign. Fortunately this does not matter for our applications. (See Example 6.7.)

The remaining covariants S_{14}, S_{24}, S_{34} and R_{38} may be computed using the Pfaffian identities.

References

[1] A. Adler and S. Ramanan, *Moduli of abelian varieties*, Lect. Notes in Math. 1644, Springer (1996).

[2] A. Agashé and W. Stein, Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero, with an appendix by J. Cremona and B. Mazur, *Math. Comp.* 74 (2005), no. 249, 455–484.

[3] D.J. Benson, *Polynomial invariants of finite groups,* London Mathematical Society, Lecture Note Series 190, Cambridge University Press, Cambridge, 1993.

[4] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: The user language, *J. Symb. Comb.* 24, 235-265 (1997). See also `http://magma.maths.usyd.edu.au/magma/`

[5] D.A. Buchsbaum and D. Eisenbud, Gorenstein ideals of height 3, *Seminar D. Eisenbud/B. Singh/W. Vogel*, Vol. 2, pp. 30–48, Teubner-Texte zur Math., 48, Teubner, Leipzig, 1982.

[6] D.A. Buchsbaum and D. Eisenbud, Algebra structures for finite free resolutions, and some structure theorems for ideals of codimension 3, *Amer. J. Math.* 99 (1977) 447-485.

[7] J.E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, Cambridge, 1997. See also `http://www.warwick.ac.uk/~masgaj/ftp/data/`

[8] J.E. Cremona and B. Mazur, Visualizing elements in the Shafarevich-Tate group, *Experiment. Math.* 9 (2000), no. 1, 13–28.

[9] 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.

[10] T.A. Fisher, *The higher secant varieties of an elliptic normal curve*, preprint.

[11] T.A. Fisher, Testing equivalence of ternary cubics, in *Algorithmic number theory (ANTS-VII)*, F. Hess, S. Pauli, M. Pohst (eds.), Lecture Notes in Comput. Sci. 4076, Springer, 2006, 333-345.

[12] T.A. Fisher, The invariants of a genus one curve, *Proc. Lond. Math. Soc.* (3) 97 (2008), no. 3, 753–782.

[13] T.A. Fisher, Pfaffian presentations of elliptic normal curves, *Trans. Amer. Math. Soc.* 362 (2010), no. 5, 2525–2540.

[14] T.A. Fisher, *The Hessian of a genus one curve*, to appear in Proc. Lond. Math. Soc.

[15] T.A. Fisher, *On families of n-congruent elliptic curves*, preprint.

[16] T.A. Fisher, *Invariant theory for the elliptic normal quintic, II. The covering map*, preprint.

[17] T.A. Fisher, *Minimisation and reduction of* 5*-coverings of elliptic curves*, in preparation.

[18] G. Horrocks and D. Mumford, A rank 2 vector bundle on $\mathbb{P}^4$ with $15,000$ symmetries, *Topology* 12 (1973), 63–81.

[19] K. Hulek, *Projective geometry of elliptic curves*, Soc. Math. de France, Astérisque 137 (1986).

[20] K. Rubin and A. Silverberg, Families of elliptic curves with constant mod p representations, in *Elliptic curves, modular forms & Fermat's last theorem* (Hong Kong, 1993), J. Coates and S.-T. Yau (eds.), Ser. Number Theory I, Int. Press, Cambridge, MA, (1995) 148–161.

[21] K. Rubin and A. Silverberg, Mod 2 representations of elliptic curves, *Proc. Amer. Math. Soc.* 129 (2001), no. 1, 53–57.

[22] N.I. Shepherd-Barron and R. Taylor, Mod 2 and mod 5 icosahedral representations, *J. Amer. Math. Soc.* 10 (1997), no. 2, 283–298.

[23] A. Silverberg, Explicit families of elliptic curves with prescribed mod N representations, in *Modular forms and Fermat's last theorem* (Boston, MA, 1995), G. Cornell, J.H. Silverman and G. Stevens (eds.), Springer-Verlag, New York, (1997) 447–461.

[24] M. Stoll and J.E. Cremona, On the reduction theory of binary forms. *J. reine angew. Math.* 565 (2003), 79–99.

[25] H.-Chr. Graf v. Bothmer and K. Hulek, Geometric syzygies of elliptic normal curves and their secant varieties, *Manuscripta Math.* 113 (2004), no. 1, 35–68.

[26] J. Vélu, Courbes elliptique munies d'un sous-group $\mathbb{Z}/n\mathbb{Z} \times \mu_n$, *Bull. Math. Soc. math. France*, Mémoire 57 (1978)

[27] C. Wuthrich, Une quintique de genre 1 qui contredit le principe de Hasse, *Enseign. Math.* (2) 47 (2001), no. 1-2, 161–172.

University of Cambridge, DPMMS, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, UK

E-mail address: T.A.Fisher@dpmms.cam.ac.uk