COMPUTING THE CASSELS-TATE PAIRING ON THE 2-SELMER GROUP OF A GENUS 2 JACOBIAN

TOM FISHER AND JIALI YAN

Abstract. We describe a method for computing the Cassels-Tate pairing on the 2-Selmer group of the Jacobian of a genus 2 curve. This can be used to improve the upper bound coming from 2-descent for the rank of the group of rational points on the Jacobian. Our method remains practical regardless of the Galois action on the Weierstrass points of the genus 2 curve. It does however depend on being able to find a rational point on a certain twisted Kummer surface. The latter does not appear to be a severe restriction in practice. In particular, we have used our method to unconditionally determine the ranks of all genus 2 Jacobians in the L-functions and modular forms database (LMFDB).

Contents

1. Introduction 2
2. Explicit 2-descent on genus 2 Jacobians 5
2.1. The Kummer surface and its dual 5
2.2. The desingularised Kummer 8
2.3. The Selmer and fake Selmer groups 10
2.4. Models for 2-coverings 11
2.5. Recovering the Selmer group element 14
2.6. Twisted Kummer surfaces 16
3. The Cassels-Tate pairing on the 2-Selmer group 18
3.1. Definition of the Cassels-Tate pairing 20
3.2. A formula for the Cassels-Tate pairing 21
3.3. Remnants of the group law 24
3.4. The Heisenberg group 25
3.5. A formula for the untwisted $(2, 2, 2)$-form 27
3.6. A formula for the twisted $(2, 2, 2)$-form 29
4. Implementation and Examples 33
4.1. Controlling the bad primes 36
4.2. First examples over $\mathbb{Q}$ 37
4.3. Examples from an experiment of Bruin and Stoll 41
4.4. Examples from the LMFDB 44
References 47

Date: 14th September 2023.

1. Introduction

Let $\mathcal{C}$ be a smooth projective curve defined over a number field k. Its Jacobian $\mathcal{J} = \mathrm{Jac}(\mathcal{C})$ is a principally polarised abelian variety, also defined over k. We are interested in the group $\mathcal{J}(k)$ of k-rational points on $\mathcal{J}$. By the Mordell-Weil theorem this is a finitely generated abelian group. We may therefore write

$$\mathcal{J}(k) \cong \Delta \times \mathbb{Z}^r$$

where Δ is a finite abelian group, called the torsion subgroup, and r is a non-negative integer, called the rank.

We may compute an upper bound for the rank by carrying out a 2-descent. Specifically, there is a short exact sequence of $\mathbb{F}_2$-vector spaces

$$0 \to \mathcal{J}(k)/2\mathcal{J}(k) \to S^{(2)}(\mathcal{J}/k) \to Ш(\mathcal{J}/k)[2] \to 0 \tag{1}$$

where the 2-Selmer group $S^{(2)}(\mathcal{J}/k)$ is finite and effectively computable. Computing $S^{(2)}(\mathcal{J}/k)$ gives an upper bound for the rank, but this will only be sharp if the Tate-Shafarevich group $Ш(\mathcal{J}/k)$ contains no elements of order 2.

In principle, the upper bound for the rank can be improved by carrying out a 4-descent, that is, by computing the 4-Selmer group $S^{(4)}(\mathcal{J}/k)$. This sits in a commutative diagram with exact rows

$$\begin{tikzcd}
\mathcal{J}(k) \arrow[r, "\times 4"] \arrow[d, "\times 2"'] & \mathcal{J}(k) \arrow[r] \arrow[d, equal] & S^{(4)}(\mathcal{J}/k) \arrow[r] \arrow[d, "\alpha"'] & Ш(\mathcal{J}/k)[4] \arrow[r] \arrow[d, "\times 2"'] & 0 \\
\mathcal{J}(k) \arrow[r, "\times 2"] & \mathcal{J}(k) \arrow[r] & S^{(2)}(\mathcal{J}/k) \arrow[r] & Ш(\mathcal{J}/k)[2] \arrow[r] & 0
\end{tikzcd} \tag{2}$$

from which we read off the inclusions $\mathcal{J}(k)/2\mathcal{J}(k) \subset \mathrm{Im}(\alpha) \subset S^{(2)}(\mathcal{J}/k)$. However, by results of Cassels [C2] in the case of elliptic curves, generalised to abelian varieties by Tate [Ta], [Mi], there is a symmetric pairing of $\mathbb{F}_2$-vector spaces

$$\langle\ ,\ \rangle_{\mathrm{CT}} : S^{(2)}(\mathcal{J}/k) \times S^{(2)}(\mathcal{J}/k) \to \mathbb{F}_2$$

whose kernel is $\mathrm{Im}(\alpha)$. Thus a 2-descent followed by computing the Cassels-Tate pairing $\langle\ ,\ \rangle_{\mathrm{CT}}$ gives the same information (as regards bounding the rank) as a 4-descent, but with potentially very much less effort.

Cassels [C5] gave a practical method for computing the pairing in the case of elliptic curves (that is, when $\mathcal{C}$ has genus 1). His method involves solving a conic over the field of definition of each 2-torsion point of the elliptic curve. This was subsequently improved by Donnelly [Do], who found a method that only requires that we solve conics over the ground field.

The second author [Y2] generalised the method of Cassels to curves of genus 2. However the analogue of solving a conic is now the problem of finding an explicit isomorphism between an algebra given by structure constants and the algebra of 4×4 matrices. So even taking $k = \mathbb{Q}$ the method is only practical if the

genus 2 curve has all its Weierstrass points defined over $\mathbb{Q}$, or at least over a very small number field. In this paper we develop a new method that avoids these restrictions. To do this we generalise the method of Donnelly [Do], or more specifically the variant in [Fi2], to curves of genus 2.

Although we are able to compute the pairing for curves of genus 2 regardless of the Galois action on the Weierstrass points, our method depends on being able to find rational points on certain twisted Kummer surfaces. In general such points need not exist, as shown by Logan and van Luijk [LvL]. However this does not appear to be a severe restriction in practice. Indeed we have implemented our method in Magma [BCP], and in running our program on thousands of random examples, and on every genus 2 Jacobian in the *L-functions and modular forms database* [LMFDB] with non-trivial analytic order of Ш, we are yet to find an example where a lack of rational points on the twisted Kummer surfaces prevents us from computing the pairing.

There are also good theoretical reasons why the twisted Kummer surfaces should typically have rational points. The surfaces of interest are always everywhere locally soluble, and so have rational points if they satisfy the Hasse principle. However Kummer surfaces are examples of $K3$ surfaces, and for these it is conjectured that all counterexamples to the Hasse principle are explained by the Brauer-Manin obstruction. Moreover there is work of Harpaz and Skorobogatov [HS], and more recently Morgan [Mo], showing that if we assume the finiteness of all relevant Tate-Shafarevich groups, then twisted Kummer surfaces, satisfying certain additional mild assumptions, do indeed satisfy the Hasse principle.

Another approach to computing the Cassels-Tate pairing on the 2-Selmer group of a genus 2 Jacobian (in fact, more generally, of a hyperelliptic Jacobian) is currently being developed by Shukla and Stoll. This is based on the Albanese-Albanese definition of the Cassels-Tate pairing, due to Poonen and Stoll [PSt]. The practicality of their method is not yet clear, but unlike our method, it only applies to curves with a rational Weierstrass point.

In the case of elliptic curves, algorithms for 4-descent have been developed, but computing the Cassels-Tate pairing on the 2-Selmer group requires significantly less effort. For genus 2 Jacobians the contrast is even more stark as there is, to our knowledge, no practical way of carrying out a 4-descent. Computing the Cassels-Tate pairing on the 2-Selmer group therefore gives us information that could not otherwise be obtained. In particular we have used our methods to compute the ranks of some genus 2 Jacobians, taken from the LMFDB and from an experiment of Bruin and Stoll [BS], in cases where the rank had only previously been computed conditional on the Birch Swinnerton-Dyer conjecture. In fact prior to our work there were 69 genus 2 curves in the LMFDB that were unresolved in this sense, and we have resolved all of them.

This paper has its origins in Chapters 5 and 6 of the second author's PhD thesis [Y1]. However in the intervening two years we have succeeded in making

the method significantly more practical. Some of the main improvements concern explicit 2-descent on genus 2 Jacobians, by which we mean the problem of converting elements of the 2-Selmer group, represented algebraically (as units modulo squares in suitable étale algebras), to explicit equations for the corresponding 2-coverings. This problem was previously addressed by Flynn, Testa and van Luijk [FTvL], extending earlier work of Gordon and Grant [GG]. However we find it convenient to take a different approach, based on the observation that, at least over the complex numbers, the Jacobian of a genus 2 curve may be realised as the variety of lines on the intersection of two quadrics in $\mathbb{P}^5$. This "neoclassical approach" is discussed in the book of Cassels and Flynn [CF, Chapter 17], and has its origins in the geometric literature in works of Newstead [N], Narasimhan and Ramanan [NR], Reid [R] and Donagi [D]. More recently it has found important applications in arithmetic statistics; see for example the papers of Bhargava and Gross [BG], and of Shankar and Wang [SW].

The upshot for us is that by representing the 2-Selmer group elements as pairs of quadratic forms in 6 variables, we obtain simple elegant formulae for the 2-coverings in $\mathbb{P}^{15}$, the twisted Kummer surfaces in $\mathbb{P}^3$, the twisted desingularised Kummer surfaces in $\mathbb{P}^5$, the maps between these, and (various maps induced by) the covering map to the Jacobian. We have also found invariant-theoretic formulae, analogous to those in [Fi2], that allow us to directly compute the $(2,2,2)$-form that appears in our formula for the Cassels-Tate pairing.

We concentrate in this paper on giving practical methods for curves of genus 2. The question as to how much of our work generalises to hyperelliptic curves of higher genus is left to future work. One reason why such a generalisation might not be automatic is that we make implicit use of the exceptional isomorphism of Lie algebras $\mathfrak{so}_6 \cong \mathfrak{sl}_4$. The practicality of searching for rational points on higher dimensional Kummer varieties could also be a problem.

Throughout this paper $\mathcal{C}$ will be a genus 2 curve, defined over a field k of characteristic not 2, with equation

$$y^2 = f(x) = f_6x^6 + f_5x^5 + \ldots + f_1x + f_0. \tag{3}$$

We assume that $f_6 \neq 0$, noting that if $\deg f = 5$ and $|k| > 5$ then we can reduce to this case by applying a suitable Möbius map.

We have divided the paper into three main sections, each with its own introduction. Section 2 gives the background on 2-descent, including the refinements mentioned above. In Section 3 we develop our method for computing the Cassels-Tate pairing, and in Section 4 we give examples and applications.

We plan to make some Magma code accompanying this article (checking some of the formulae and examples) available from the first author's website.

Acknowledgements. We thank Brendan Creutz, Victor Flynn, Jef Laga, August Liu, Adam Morgan, Ross Paterson, Himanshu Shukla, Michael Stoll, Drew Sutherland and Jack Thorne for useful conversations.

2. Explicit 2-descent on genus 2 Jacobians

We give an account of 2-descent on the Jacobian of a genus 2 curve. The emphasis is on explicit formulae, some of which are taken from the existing literature and some of which are new.

In Sections 2.1 and 2.2 we give formulae relating to the Kummer surface, the dual Kummer surface, the desingularised Kummer, the embedding of the Jacobian in $\mathbb{P}^{15}$, and the action of the 2-torsion points. We are particularly interested in constructions that carry over to the twisted Kummer surfaces considered in Section 2.6. In Section 2.3 we briefly recall the standard algebraic description of the 2-Selmer group, and define its canonical element. Section 2.4 introduces the "neoclassical approach" where we represent Selmer group elements as pairs of quadratics forms. We call these pairs of quadratic forms *models*. In Section 2.5 we describe some methods for recovering a Selmer group element from a model. In Section 2.6 we explain how a model determines an equation for the corresponding twisted Kummer surface, and a wealth of other information.

2.1. **The Kummer surface and its dual.** Let $\mathcal{C}$ be a genus 2 curve with equation $y^2 = f(x)$ where f is a polynomial of degree 6, with coefficients labelled as in (3). Let $\mathcal{J}$ be the Jacobian of $\mathcal{C}$, and let $\mathcal{K} = \mathcal{J}/[-1]$ be its Kummer surface. We may represent points on $\mathcal{J}$ as

$$[(x, y) + (x', y') - \kappa]$$

where $(x, y), (x', y') \in \mathcal{C}$ and κ is the canonical divisor on $\mathcal{C}$. A point on $\mathcal{K}$ may therefore by represented by x, x' and a choice of square root of $f(x)f(x')$. It follows that $\mathcal{K}$ is the double cover of the projective plane $\mathbb{P}^2_{a,b,c}$ with equation

$$z^2 = \operatorname{Res}(ax^2 - bx + c, f(x)). \tag{4}$$

If we specialise a, b, c to $1, 2t, t^2$ then this resultant equals $f(t)^2$. This suggests putting

$$\begin{aligned} P_2(a, b, c) &= b^2 - 4ac, \\ P_3(a, b, c) &= 2(2f_0a^3 + f_1a^2b + 2f_2a^2c + f_3abc + 2f_4ac^2 + f_5bc^2 + 2f_6c^3), \end{aligned}$$

so that $P_2(1, 2t, t^2) = 0$ and $P_3(1, 2t, t^2) = 4f(t)$. We can then solve for the homogeneous polynomial $P_4(a, b, c)$ of degree 4 satisfying

$$P_3^2 - 4P_2P_4 = 16 \operatorname{Res}(ax^2 - bx + c, f(x)).$$

The equation (4) for the Kummer surface becomes

$$\mathcal{K} = \{P_2d^2 - P_3d + P_4 = 0\} \subset \mathbb{P}^3_{a,b,c,d}.$$

Renaming the coordinates a, b, c, d as $x_1, \ldots, x_4$ we have the following equation for $\mathcal{K} \subset \mathbb{P}^3$, in agreement with [CF, page 19].

$$\begin{aligned} F = {} & (x_2^2 - 4x_1x_3)x_4^2 - 2(2f_0x_1^3 + f_1x_1^2x_2 + 2f_2x_1^2x_3 + f_3x_1x_2x_3 + 2f_4x_1x_3^2 \\ & + f_5x_2x_3^2 + 2f_6x_3^3)x_4 + (f_1^2 - 4f_0f_2)x_1^4 - 4f_0f_3x_1^3x_2 - 2f_1f_3x_1^3x_3 \\ & - 4f_0f_4x_1^2x_2^2 + 4(f_0f_5 - f_1f_4)x_1^2x_2x_3 + (f_3^2 - 4f_0f_6 + 2f_1f_5 - 4f_2f_4)x_1^2x_3^2 \\ & - 4f_0f_5x_1x_2^3 + 4(2f_0f_6 - f_1f_5)x_1x_2^2x_3 + 4(f_1f_6 - f_2f_5)x_1x_2x_3^2 - 2f_3f_5x_1x_3^3 \\ & - 4f_0f_6x_2^4 - 4f_1f_6x_2^3x_3 - 4f_2f_6x_2^2x_3^2 - 4f_3f_6x_2x_3^3 + (f_5^2 - 4f_4f_6)x_3^4. \end{aligned} \tag{5}$$

This quartic surface is also the image of $\mathcal{J}$ by the linear system $|2\Theta|$, where Θ is the theta divisor.[1] It has exactly 16 nodes, these being the images of the 2-torsion points on $\mathcal{J}$.

The dual Kummer $\mathcal{K}^\vee \subset (\mathbb{P}^3)^\vee$ is obtained by mapping each smooth point on $\mathcal{K} \subset \mathbb{P}^3$ to its tangent plane. We write $x_1^*, \ldots, x_4^*$ for the coordinates on $(\mathbb{P}^3)^\vee$ dual to the coordinates $x_1, \ldots, x_4$ on $\mathbb{P}^3$. According to [CF, page 33], the dual Kummer has equation

$$\begin{vmatrix} 2f_0x_4^* & f_1x_4^* & x_1^* & x_2^* \\ f_1x_4^* & 2f_2x_4^* - 2x_1^* & f_3x_4^* - x_2^* & x_3^* \\ x_1^* & f_3x_4^* - x_2^* & 2f_4x_4^* - 2x_3^* & f_5x_4^* \\ x_2^* & x_3^* & f_5x_4^* & 2f_6x_4^* \end{vmatrix} = 0.$$

We identify $\operatorname{Pic}^d \mathcal{C}$ and $\operatorname{Pic}^{d+2} \mathcal{C}$ via addition of the canonical divisor, so that $\operatorname{Pic}^d \mathcal{C}$ only depends on the parity of d. It is a double cover of $\mathcal{K}$ if d is even and a double cover of $\mathcal{K}^\vee$ if d is odd. Adding a point $P \in \mathcal{C}$ defines a map $\operatorname{Pic}^d \mathcal{C} \to \operatorname{Pic}^{d+1} \mathcal{C}$. If $P = (\theta, 0)$ is a Weierstrass point then these maps descend to a pair of inverse maps $\mathcal{K} \to \mathcal{K}^\vee$ and $\mathcal{K}^\vee \to \mathcal{K}$. According to [CF, pages 38 and 184], the map $\mathcal{K} \to \mathcal{K}^\vee$ is given by

$$\begin{pmatrix} x_1^* \\ x_2^* \\ x_3^* \\ x_4^* \end{pmatrix} = \begin{pmatrix} 0 & h_5(\theta) & h_4(\theta) & \theta^2 \\ -h_5(\theta) & 0 & h_3(\theta) & -\theta \\ -h_4(\theta) & -h_3(\theta) & 0 & 1 \\ -\theta^2 & \theta & -1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \tag{6}$$

where

$$\begin{aligned} h_3(\theta) &= 2f_6\theta^3 + f_5\theta^2, \\ h_4(\theta) &= 2f_6\theta^4 + 2f_5\theta^3 + 2f_4\theta^2 + f_3\theta, \\ h_5(\theta) &= 2f_6\theta^5 + 2f_5\theta^4 + 2f_4\theta^3 + 2f_3\theta^2 + 2f_2\theta + f_1. \end{aligned} \tag{7}$$

[1] We abuse notation (suppressing the choice of Weierstrass point) as in [FTvL, page 397].

For $A = (A_{ij})$ a 4×4 skew symmetric matrix we put[2]

$$A^* = \begin{pmatrix} 0 & A_{43} & A_{24} & A_{32} \\ A_{34} & 0 & A_{41} & A_{13} \\ A_{42} & A_{14} & 0 & A_{21} \\ A_{23} & A_{31} & A_{12} & 0 \end{pmatrix}. \tag{8}$$

This is again a skew symmetric matrix. The Pfaffian $\mathrm{Pf}(A)$ then satisfies

$$AA^* = A^*A = \mathrm{Pf}(A)I_4. \tag{9}$$

We note that $\mathrm{Pf}(A)^2 = \det(A)$, $\mathrm{Pf}(A^*) = \mathrm{Pf}(A)$ and $A^{**} = A$. Moreover for any 4×4 matrix P we have

$$\mathrm{Pf}(P^T AP) = \det(P)\,\mathrm{Pf}(A). \tag{10}$$

Writing A for the matrix in (6), we have

$$\mathrm{Pf}(A) = h_5(\theta) + \theta h_4(\theta) + \theta^2 h_3(\theta) = f'(\theta). \tag{11}$$

Let f have roots $\theta_1, \ldots, \theta_6$, and write A_i for the matrix obtained by taking $\theta = \theta_i$ in (6). As explained in [CF, page 38], for $i \neq j$ the action of $T_{ij} = [(\theta_i, 0) + (\theta_j, 0) - \kappa] \in \mathcal{J}[2]$ by translation on $\mathcal{K} \subset \mathbb{P}^3$ is given by

$$A_i^* A_j = -A_j^* A_i. \tag{12}$$

Since $T_{12} + T_{34} + T_{56} = 0$ it follows that $A_1^* A_2 A_3^* A_4 A_5^* A_6 = \lambda I_4$ for some scalar λ. Squaring both sides and using (9), (11) and (12) shows that $\lambda^2 = f_6^6 \prod_{i<j}(\theta_i - \theta_j)^2$. Making the correct choice of square root it turns out that

$$A_1^* A_2 A_3^* A_4 A_5^* A_6 = f_6^3 \prod_{i<j}(\theta_i - \theta_j) I_4. \tag{13}$$

An alternative, less symmetric, way to write this identity is as

$$\frac{A_1 A_2^* A_3}{(\theta_1 - \theta_2)(\theta_2 - \theta_3)(\theta_3 - \theta_1)} = \frac{A_4 A_5^* A_6}{(\theta_4 - \theta_5)(\theta_5 - \theta_6)(\theta_6 - \theta_4)}. \tag{14}$$

Remark 2.1. The skew symmetric matrices A_i define 6 linear isomorphisms $\mathcal{K} \to \mathcal{K}^\vee$. A further 10 such isomorphisms are defined by the symmetric matrices of the form (14). These matrices are indexed by the $(1,5)$-partitions and $(3,3)$-partitions of the Weierstrass points.

[2]In basis free language, we are identifying the alternating square of a 4-dimensional vector space with its dual.

2.2. **The desingularised Kummer.** Blowing up the 16 nodes of $\mathcal{K}$ (or equally of $\mathcal{K}^\vee$) gives a surface $\widetilde{\mathcal{K}}$ called the desingularised Kummer. Equations for $\widetilde{\mathcal{K}}$ may be obtained as follows; see for example [FTvL, Section 4]. Let $L = k[x]/(f) = k[\theta]$ and define quadratic forms $Q_0, Q_1, \ldots, Q_5 \in k[u_0, u_1, \ldots, u_5]$ by

$$(u_0 + u_1\theta + \ldots + u_5\theta^5)^2 = Q_0 + Q_1\theta + \ldots + Q_5\theta^5. \tag{15}$$

Then $\widetilde{\mathcal{K}} = \{Q_3 = Q_4 = Q_5 = 0\} \subset \mathbb{P}^5$. The quadratic form Q_5 only involves the monomials u_iu_j with $i + j \geqslant 5$, and so has a 3-dimensional isotropic subspace given by $u_3 = u_4 = u_5 = 0$. This suggest making a change of coordinate on $\mathbb{P}^5$ transforming Q_5 to a scalar multiple of $u_0u_5 + u_1u_4 + u_2u_3$. Such a change of coordinates is given by replacing the basis $1, \theta, \ldots, \theta^5$ for $k[\theta]$ on the left hand side of (15) by the basis

$$1, \theta, \theta^2, h_3(\theta), h_4(\theta), h_5(\theta).$$

where the $h_j(\theta)$ were defined in (7). Making the same change of basis on the right hand side of (15), we find that $Q_5 = 2G$, $Q_4 = 2H$ and $Q_3 = 2S$ where

$$\begin{aligned}
G &= u_0u_5 + u_1u_4 + u_2u_3,\\
H &= u_0u_4 + u_1u_3 - f_0u_5^2 - f_1u_4u_5 - f_2u_4^2 - f_3u_3u_4 - f_4u_3^2 + \tfrac{1}{4}f_6^{-1}(u_2 - f_5u_3)^2,\\
S &= u_0u_3 - 2f_0u_4u_5 - f_1(u_3u_5 + u_4^2) - 2f_2u_3u_4 - f_3u_3^2\\
&\qquad + \tfrac{1}{2}f_6^{-1}(u_1 - f_3u_4 - 2f_4u_3)(u_2 - f_5u_3) - \tfrac{1}{4}f_6^{-2}f_5(u_2 - f_5u_3)^2.
\end{aligned}$$

The desingularised Kummer is now given by $\widetilde{\mathcal{K}} = \{G = H = S = 0\} \subset \mathbb{P}^5$.

Writing $\mathbf{G}$, $\mathbf{H}$, $\mathbf{S}$ for the symmetric matrices with $G(u) = \frac{1}{2}\mathbf{u}^T\mathbf{G}\mathbf{u}$ etc., where $\mathbf{u} = (u_0, \ldots, u_5)^T$, we find that $\mathbf{S} = \mathbf{H}\mathbf{G}^{-1}\mathbf{H}$ and

$$\det(x\mathbf{G} - \mathbf{H}) = -f_6^{-1}f(x).$$

In particular the 6×6 matrix $\theta\mathbf{G} - \mathbf{H}$ is singular. In fact this matrix has rank 5 and its kernel is spanned by the vector with entries

$$h_5(\theta), h_4(\theta), h_3(\theta), \theta^2, \theta, 1. \tag{16}$$

We may associate to each point $(x_1 : x_2 : x_3 : x_4) \in \mathbb{P}^3$ a 3-dimensional isotropic subspace for G spanned by the rows of the matrix

$$\Lambda = \begin{pmatrix} 0 & 0 & x_4 & 0 & x_3 & x_2 \\ 0 & -x_4 & 0 & x_3 & 0 & -x_1 \\ x_4 & 0 & 0 & -x_2 & -x_1 & 0 \\ -x_3 & x_2 & -x_1 & 0 & 0 & 0 \end{pmatrix}. \tag{17}$$

The "neoclassical approach" (see the introduction for references) suggests we look for lines contained in $\{G = H = 0\} \subset \mathbb{P}^5$. We obtain two such lines if the restriction of H to a 3-dimensional isotropic subspace for G has rank 2. This suggests that $\mathcal{K} \subset \mathbb{P}^3$ should be defined by the 3×3 minors of $B = \Lambda\mathbf{H}\Lambda^T$. This

is confirmed by a direct calculation, which more precisely shows that the equation F for $\mathcal{K}$ in (5) satisfies

$$-2f_6 \operatorname{Adj} B = F(x_1, \ldots, x_4)\mathbf{x}\mathbf{x}^T \tag{18}$$

where $\mathbf{x} = (x_1, x_2, x_3, x_4)^T$.

The equations for $\widetilde{\mathcal{K}}$ may be written in terms of Pfaffians. To do this we define skew symmetric matrices of linear forms in $u_0, \ldots, u_5$ by

$$Z = \begin{pmatrix} 0 & u_0 & u_1 & u_3 \\ & 0 & u_2 & -u_4 \\ & & 0 & u_5 \\ & & & 0 \end{pmatrix} \quad \text{and} \quad W = \begin{pmatrix} 0 & H_0 & H_1 & H_3 \\ & 0 & H_2 & -H_4 \\ & & 0 & H_5 \\ & & & 0 \end{pmatrix}^* \tag{19}$$

where $H_i = \partial H/\partial u_i$, and the superscript $*$ has the meaning explained in (8). Then for indeterminates λ and μ we have

$$\operatorname{Pf}(\lambda Z + \mu W) = \lambda^2 G - 2\lambda\mu H + \mu^2 S.$$

Remark 2.2. The birational map between $\mathcal{K} \subset \mathbb{P}^3$ and $\widetilde{\mathcal{K}} \subset \mathbb{P}^5$ may be described in the following ways.

(i) The graph of this map in $\mathbb{P}^3 \times \mathbb{P}^5$ is defined by the 8 bilinear forms

$$(x_1\ x_2\ x_3\ x_4)(Z|W) = 0.$$

(ii) The 4×4 matrix of quadratic forms ZW^* has rank at most 1 on $\widetilde{\mathcal{K}}$. Any row defines the map $\widetilde{\mathcal{K}} \to \mathcal{K}$ and any column defines the map $\widetilde{\mathcal{K}} \to \mathcal{K}^\vee$.

(iii) The 2×2 minors of B may be arranged in a 6×6 symmetric matrix of quartic forms that has rank at most 1 on $\mathcal{K}$. Any row or column defines the map $\mathcal{K} \to \widetilde{\mathcal{K}}$. Setting any diagonal entry of the 6×6 matrix equal to $-f_6$ times a square defines the double cover $\mathcal{J} \to \mathcal{K}$.

Remark 2.3. The previous remark is closely related to the 72 quadratic equations defining $\mathcal{J} \subset \mathbb{P}^{15}$, as originally computed by Flynn [F1], and revisited in [FTvL]. We write our coordinates on $\mathbb{P}^{15}$ as x_{ij} and z_{ij} where these are the entries of a generic 4×4 symmetric matrix X, and a generic 4×4 skew symmetric matrix Z. We identify the z_{ij} with the u_i via (19). Our first 21 quadratic equations are the 2×2 minors of X. Next the entries of XZ and XW give 32 quadratic equations, in fact only spanning a space of dimension 30, since these matrices have trace zero. Finally, generalising the last part of Remark 2.2(iii), there are 21 quadratic equations $-f_6 z_{ij} z_{kl} = B_{ik}B_{jl} - B_{il}B_{jk}$ where each quartic on the right is rewritten as a quadratic using $x_{rs} = x_r x_s$. In view of the first 21 equations, the choices here do not matter. In total this gives $21 + 30 + 21 = 72$ equations.

2.3. **The Selmer and fake Selmer groups.** We continue to take $\mathcal{C}$ a genus 2 curve with equation $y^2 = f(x)$ where $f \in k[x]$ is a polynomial of degree 6. We now suppose that k is a number field. Let $\mathcal{J}$ be the Jacobian of $\mathcal{C}$. The 2-Selmer group is

$$S^{(2)}(\mathcal{J}/k) = \ker\left(H^1(k, \mathcal{J}[2]) \to \prod_v H^1(k_v, \mathcal{J})\right). \tag{20}$$

Let W be the set of Weierstrass points on $\mathcal{C}$, that is, the points $(\theta, 0)$ where θ is a root of f. Let Φ be the set of all ways of partitioning W into two subsets. There is a natural Galois action on Φ induced by the Galois action on W, and a group law given by symmetric difference, equivalently by pointwise addition of indicator functions in $\mathrm{Map}(W, \mathbb{F}_2)/\mathbb{F}_2$. We write $\Phi = \Phi_0 \sqcup \Phi_1$ where Φ_0 (resp. Φ_1) is the set of decompositions into subsets of even (resp. odd) size. It is well known that Φ_0 is isomorphic to $\mathcal{J}[2]$ as a Galois module. It follows that Φ_1 is a torsor under $\mathcal{J}[2]$. We write $c \in H^1(k, \mathcal{J}[2])$ for the class of Φ_1.

Lemma 2.4. *The canonical element c belongs to $S^{(2)}(\mathcal{J}/k)$.*

Proof. The canonical element c is represented by the cocycle $\sigma \mapsto [\sigma P - P]$ where $P \in \mathcal{C}$ is a Weierstrass point. It follows that the natural map $H^1(k, \mathcal{J}[2]) \to H^1(k, \mathcal{J})$ sends c to the class of $\mathrm{Pic}^1 \mathcal{C}$. The lemma is therefore equivalent to showing that $\mathcal{C}$ admits a k_v-rational divisor class of degree 1 for each place v of k. As noted by Poonen and Stoll [PSt, Lemma 1] this is a consequence of Tate local duality, and is originally due to Lichtenbaum [L, Theorem 7]. □

Definition 2.5. The fake Selmer group is $S^{(2)}_{\mathrm{fake}}(\mathcal{J}/k) = S^{(2)}(\mathcal{J}/k)/\langle c \rangle$.

The analogue of (20) is

$$S^{(2)}_{\mathrm{fake}}(\mathcal{J}/k) = \ker\left(\frac{H^1(k, \mathcal{J}[2])}{\langle c \rangle} \to \prod_v H^1(k_v, \mathcal{J})\right).$$

Let $L = k[x]/(f) = k[\theta]$ be the étale algebra of W. As shown by Poonen and Schaefer [PSc] there is an isomorphism

$$\frac{H^1(k, \mathcal{J}[2])^{\cup c = 0}}{\langle c \rangle} \cong \ker\left(L^\times/(k^\times (L^\times)^2) \xrightarrow{N_{L/k}} k^\times/(k^\times)^2\right) \tag{21}$$

where the superscript $\cup c = 0$ indicates the subgroup of elements that pair trivially with c under the pairing

$$H^1(k, \mathcal{J}[2]) \times H^1(k, \mathcal{J}[2]) \to \mathrm{Br}(k)$$

given by cup product and the Weil pairing. The composite of the connecting map $\mathcal{J}(k)/2\mathcal{J}(k) \to H^1(k, \mathcal{J}[2])$ and (21) is the Cassels map (see e.g. [C4], [FPS]),

given for $yy' \neq 0$ by

$$[(x,y)+(x',y')-\kappa] \mapsto (x-\theta)(x'-\theta). \tag{22}$$

The fake Selmer group $S^{(2)}_{\text{fake}}(\mathcal{J}/k)$ naturally arises as the subgroup of the right hand side of (21) consisting of elements that are everywhere locally in the image of the Cassels map. This group can be computed in Magma [BCP], using programs originally due to Stoll [S2].

It is easy to compute the dimension of $S^{(2)}(\mathcal{J}/k)$ as an $\mathbb{F}_2$-vector space from that of $S^{(2)}_{\text{fake}}(\mathcal{J}/k)$, simply by adding 0 or 1 according as the canonical element c is trivial or non-trivial. However we shall need a more explicit way of representing elements of $S^{(2)}(\mathcal{J}/k)$. As explained by Stoll and van Luijk [SvL], this is given by augmenting elements of the right hand side of (21) with a choice of square root of the norm. Thus $S^{(2)}(\mathcal{J}/k)$ is a subgroup of

$$H^1(k,\mathcal{J}[2])^{\cup c=0} \cong \frac{\{(\xi,m)\in L^\times \times k^\times | N_{L/k}(\xi)=m^2\}}{\{(r\nu^2, r^3 N_{L/k}(\nu)) | r\in k^\times, \nu\in L^\times\}}. \tag{23}$$

2.4. **Models for 2-coverings.** Following the "neoclassical approach" (see the introduction for references) we explain how elements of the 2-Selmer group $S^{(2)}(\mathcal{J}/k)$ may be represented by certain pairs of quadratic forms, which we call *models*.

We only need the following proposition in the case $n=6$, but the extra generality costs us nothing.

Proposition 2.6. *Let $f(x)=f_nx^n+\ldots+f_1x+f_0\in k[x]$ be a square-free polynomial of degree n. Let $L=k[\theta]=k[x]/(f)$ and fix $\xi\in L^\times$. Consider the quadratic forms $Q_j\in k[u_0,\ldots,u_{n-1}]$ defined by*

$$\xi(u_0+u_1\theta+\ldots+u_{n-1}\theta^{n-1})^2=\sum_{j=0}^{n-1} Q_j(u_0,\ldots,u_{n-1})\theta^j. \tag{24}$$

(i) *There are $n\times n$ symmetric matrices $\mathbf{G}$ and $\mathbf{H}$, with $\mathbf{G}$ invertible, such that*

$$Q_j(u_0,\ldots,u_{n-1})=f_n^{-1}\sum_{i=j+1}^{n} f_i\mathbf{u}^T\mathbf{G}(\mathbf{G}^{-1}\mathbf{H})^{i-j-1}\mathbf{u}$$

for all $0\leqslant j\leqslant n-1$, where $\mathbf{u}=(u_0,\ldots,u_{n-1})^T$.

(ii) *We have*

$$\det(x\mathbf{G}-\mathbf{H})=(-1)^{\binom{n}{2}}f_n^{-1}N_{L/k}(\xi)f(x).$$

(iii) *If $\mathbf{v}=\mathbf{G}^{-1}(1,\theta,\ldots,\theta^{n-1})^T$ then $(\theta\mathbf{G}-\mathbf{H})\mathbf{v}=0$ and $\mathbf{v}^T\mathbf{G}\mathbf{v}=f_n^{-1}f'(\theta)/\xi$.*

(iv) *We have*

$$\left(\frac{1}{2^n}\frac{\partial(Q_0,\ldots,Q_{n-1})}{\partial(u_0,\ldots,u_{n-1})}\right)^2=(-1)^{\binom{n}{2}}(\det\mathbf{G})N_{L/k}\left(\sum_{j=0}^{n-1}Q_j(u_0,\ldots,u_{n-1})\theta^j\right).$$

Proof. Let $\theta_1, \ldots, \theta_n$ be the roots of f. A well known identity that is used in the theory of the different (see for example [Sw, page 45]) states that

$$\sum_{r=1}^{n} \frac{f(x)}{x-\theta_r} \frac{\theta_r^i}{f'(\theta_r)} = x^i.$$

for all $0 \leqslant i \leqslant n-1$. The proof is simply that each side is a polynomial of degree less than n taking the same values at $\theta_1, \ldots, \theta_n$. Writing

$$f(x) = (x-\theta)(\beta_{n-1}x^{n-1} + \ldots + \beta_1 x + \beta_0) \tag{25}$$

it follows that the θ^i and $\beta_i/f'(\theta)$ are dual bases for L with respect to the trace pairing $(x,y) \mapsto \mathrm{Tr}_{L/k}(xy)$. In particular for any $a \in L$ we have

$$N_{L/k}(a) = \det\left(\mathrm{Tr}_{L/k}\left(\frac{a\theta^i\beta_j}{f'(\theta)}\right)_{i,j=0,\ldots,n-1}\right) \tag{26}$$

and (24) is satisfied with

$$Q_j(u_0, \ldots, u_{n-1}) = \mathrm{Tr}_{L/k}\left(\frac{\xi\beta_j(u_0 + \ldots + u_{n-1}\theta^{n-1})^2}{f'(\theta)}\right). \tag{27}$$

(i) Let $\mathbf{G}$ represent the pairing $(x,y) \mapsto \mathrm{Tr}_{L/k}(f_n\xi xy/f'(\theta))$, and $\mathbf{\Theta}$ represent the multiplication-by-θ map, both with respect to the basis $1, \theta, \ldots, \theta^{n-1}$. Comparing coefficients in (25) shows that $\beta_j = \sum_{i=j+1}^{n} f_i\theta^{i-j-1}$. Rewriting (27) using this notation and putting $\mathbf{H} = \mathbf{G}\mathbf{\Theta}$ gives the stated formula.
(ii) We have $\det(x\mathbf{G} - \mathbf{H}) = \det \mathbf{G} \det(xI_n - \mathbf{\Theta})$ where

$$\det \mathbf{G} = N_{L/k}(\xi)\Delta(1, \theta, \ldots, \theta^{n-1})/N_{L/k}(f_n^{-1}f'(\theta)) = (-1)^{\binom{n}{2}}N_{L/k}(\xi) \tag{28}$$

and $\det(xI_n - \mathbf{\Theta}) = f_n^{-1}f(x)$.
(iii) We have $\mathbf{v}^T(\theta\mathbf{G} - \mathbf{H}) = (1, \theta, \ldots, \theta^{n-1})(\theta I_n - \mathbf{\Theta}) = 0$. On the other hand $\mathbf{G}\mathbf{v} = (1, \theta, \ldots, \theta^{n-1})^T$ and $\mathbf{v} = (f_n\xi)^{-1}(\beta_0, \beta_1, \ldots, \beta_{n-1})^T$. Therefore

$$\mathbf{v}^T\mathbf{G}\mathbf{v} = (\beta_0 + \beta_1\theta + \ldots + \beta_{n-1}\theta^{n-1})/(f_n\xi) = f'(\theta)/(f_n\xi).$$

(iv) We differentiate (27) to get

$$\frac{\partial Q_j}{\partial u_i}(u_0, \ldots, u_{n-1}) = \mathrm{Tr}_{L/k}\left(\frac{2\xi\theta^i\beta_j(u_0 + \ldots + u_{n-1}\theta^{n-1})}{f'(\theta)}\right).$$

It follows by (26) that

$$\frac{\partial(Q_0, \ldots, Q_{n-1})}{\partial(u_0, \ldots, u_{n-1})} = N_{L/k}\left(2\xi(u_0 + u_1\theta + \ldots + u_{n-1}\theta^{n-1})\right).$$

Squaring both sides and then using (24) and (28) gives the stated formula. □

We now return to considering a genus 2 curve $\mathcal{C}$ with equation $y^2 = f(x)$ where $f \in k[x]$ is a polynomial of degree 6. Let $\mathcal{J}$ be the Jacobian of $\mathcal{C}$.

Definition 2.7. (i) A *model* (*for a* 2*-covering of* $\mathcal{J}$) is a pair of quadratic forms (G, H) in variables $u_0, \ldots, u_5$, where $G = u_0u_5+u_1u_4+u_2u_3$ and the corresponding symmetric matrices (given by $G(\mathbf{u}) = \frac{1}{2}\mathbf{u}^T\mathbf{G}\mathbf{u}$ and $H(\mathbf{u}) = \frac{1}{2}\mathbf{u}^T\mathbf{H}\mathbf{u}$) satisfy

$$\det(x\mathbf{G} - \mathbf{H}) = -f_6^{-1}f(x). \tag{29}$$

Since G is fixed, we sometimes refer to the model (G, H) simply as H.
(ii) Two models are *k-equivalent* if they are in the same orbit for the action of $\mathrm{PGL}_4(k)$ defined as follows. We identify the 4×4 skew symmetric matrices Z with the column vectors $\mathbf{u} = (u_0, \ldots, u_5)^T$ via (19), so that $G = \mathrm{Pf}(Z)$. Then the action of $P \in \mathrm{GL}_4$ on the space of such matrices via $Z \mapsto PZP^T$ is described by a matrix $\wedge^2 P \in \mathrm{GL}_6$. We let $P \in \mathrm{GL}_4$ act on a model (G, H) first by changing coordinates using $\wedge^2 P$ and then dividing both G and H by $\det P$. By (10) this preserves G. Since the scalar matrices act trivially, this is an action of PGL_4.

Remark 2.8. (i) If we change our equation $y^2 = f(x)$ for $\mathcal{C}$ by applying a Möbius map to the x-coordinate then, provided f still has degree 6, we may update our models by applying the inverse Möbius map to the transformation $\mathbf{\Theta} = \mathbf{G}^{-1}\mathbf{H}$ in the proof of Proposition 2.6.
(ii) Any model for a 2-covering of $\mathcal{J} = \mathrm{Jac}(\mathcal{C})$ is also a model for a 2-covering of $\mathcal{J}_d = \mathrm{Jac}(\mathcal{C}_d)$ where $\mathcal{C}_d : dy^2 = f(x)$ is any quadratic twist of $\mathcal{C}$.

Starting from $(\xi, m) \in S^{(2)}(\mathcal{J}/k)$ we compute a model as follows. First, analogous to (15), we define quadratic forms $Q_0, Q_1, \ldots, Q_5 \in k[u_0, u_1, \ldots, u_5]$ by

$$\xi(u_0 + u_1\theta + \ldots + u_5\theta^5)^2 = Q_0 + Q_1\theta + \ldots + Q_5\theta^5. \tag{30}$$

If ξ is in the image of the Cassels map (22) then, after multiplying by a square, it is quadratic in θ. This motivates our interest in rational points on the twisted desingularised Kummer surface $\{Q_3 = Q_4 = Q_5 = 0\} \subset \mathbb{P}^5$. As suggested by Proposition 2.6(i) with $n = 6$ (see also [CF, page 167] or [FTvL, page 403]), we rewrite our equations for this surface as

$$\begin{aligned} G &= Q_5/2, \\ H &= (f_6Q_4 - f_5Q_5)/(2f_6), \\ S &= (f_6^2Q_3 - f_5f_6Q_4 + (f_5^2 - f_4f_6)Q_5)/(2f_6^2), \end{aligned}$$

The corresponding symmetric matrices (with $G(\mathbf{u}) = \frac{1}{2}\mathbf{u}^T\mathbf{G}\mathbf{u}$ etc.) are then related by $\mathbf{S} = \mathbf{H}\mathbf{G}^{-1}\mathbf{H}$. By Proposition 2.6(ii) we have

$$\det(x\mathbf{G} - \mathbf{H}) = -f_6^{-1}N_{L/k}(\xi)f(x). \tag{31}$$

If ξ is in the image of the Cassels map (22) then, after multiplying by a square, it is quadratic in θ. If we further take $u_2 = u_3 = u_4 = u_5 = 0$ then the left hand side of (30) has no term θ^5. It follows that the quadratic form G has a

2-dimensional isotropic subspace, and is therefore the orthogonal direct sum of two hyperbolic planes and a binary quadratic form. As a special case of (31) we have $\det \mathbf{G} = -N_{L/k}(\xi)$. Since $N_{L/k}(\xi) = m^2$ the binary quadratic form has discriminant a square. Therefore G has a 3-dimensional isotropic subspace.[3]

We are interested in (ξ, m) representing an element of the Selmer group. This means that ξ is everywhere locally in the image of the Cassels map. The previous paragraph shows that G has a 3-dimensional isotropic subspace everywhere locally. By a suitable form on the the Hasse principle (for example, the weak Hasse principle in [C3, Chapter 6]) it follows that G has a 3-dimensional isotropic subspace globally. In the case $k = \mathbb{Q}$ we use the existing function `IsotropicSubspace` in Magma [BCP] to find such a subspace. It is then easy to find a change of coordinates putting G in the standard form specified in Definition 2.7(i). We can and do choose this change of coordinates so that it has determinant m (rather than $-m$). This gives the desired model (G, H).

It is shown in [CF, Lemma 17.1.1] that the 3-dimensional isotropic subspaces of G fall into two algebraic families. This may conveniently be seen as follows. We write $G = \mathrm{Pf}(Z)$ as in Definition 2.7(ii). Setting all entries in the jth row and column to zero makes G vanish, as does setting all entries outside the jth row and column to zero. Repeating these observations for linear combinations of the rows and columns we see that the 3-dimensional isotropic subspaces of G are parametrised by $\mathbb{P}^3 \sqcup (\mathbb{P}^3)^\vee$.

Following [FH, Section 19.1], the subgroup $\mathrm{PO}(G) \subset \mathrm{PGL}_6$ preserving G up to scalars sits in an exact sequence

$$0 \to \mathrm{PSO}(G) \to \mathrm{PO}(G) \to \{\pm 1\} \to 0$$

where $\mathrm{PGL}_4 \cong \mathrm{PSO}(G)$ via $P \mapsto \wedge^2 P$, and $\{\pm 1\}$ swaps over the two families of isotropic subspaces. It follows that our procedure (noting in particular the condition on the determinant of the change of coordinates) associates to each Selmer group element (ξ, m) a unique equivalence class of models.

Remark 2.9. If we started with an arbitrary pair (ξ, m) in (23), not necessarily a Selmer group element, then the 3-dimensional isotropic subspaces of G would be parametrised by $S \sqcup S^\vee$, where S is a 3-dimensional Brauer-Severi variety, and $S^\vee$ is its dual. The obstruction map $H^1(k, \mathcal{J}[2]) \to \mathrm{Br}(k)$, as defined in [Cl, Section 5], is then realised by $(\xi, m) \mapsto [S]$.

2.5. **Recovering the Selmer group element.** We explain how to recover a Selmer group element (ξ, m) from a model (G, H). This not only helps us check that the models we computed in the last section are correct, but is also useful for testing equivalence of models, and for realising the group law.

[3]Our argument is specific to curves of genus 2. However corresponding results are known for hyperelliptic curves in general; see [T1], [Wa].

As in Section 2.2 the matrix $\theta\mathbf{G}-\mathbf{H}$ has rank 5. We pick a vector spanning its kernel, and rewrite it using (19) as a 4×4 skew symmetric matrix A with entries in $L=k[x]/(f)=k[\theta]$. We claim that

$$\xi \equiv \mathrm{Pf}(A)/f'(\theta) \mod k^\times (L^\times)^2. \tag{32}$$

In the untwisted case (i.e., when $\xi=1$) this claim follows by (6), (11) and (16). It is also easy to see that the class (32) only depends on the equivalence class of (G,H). Indeed picking a different basis for the kernel of $\theta\mathbf{G}-\mathbf{H}$ has the effect of multiplying A by an element of $L^\times$ and hence $\mathrm{Pf}(A)$ by an element of $(L^\times)^2$. By (10) the only further effect of replacing (G,H) by an equivalent model is to multiply $\mathrm{Pf}(A)$ by an element of $k^\times$.

If we take $\xi=\mathrm{Pf}(A)/f'(\theta)$ then the matrix A also determines a square root m of $N_{L/k}(\xi)$ via the formula

$$A_1^*A_2A_3^*A_4A_5^*A_6 = mf_6^3\prod_{i<j}(\theta_i-\theta_j)I_4, \tag{33}$$

which generalises (13).

Proposition 2.6(iii) shows that the class of ξ in $L^\times/k^\times(L^\times)^2$ is given by evaluating the quadratic form G at a vector in the kernel of $\theta\mathbf{G}-\mathbf{H}$, and then dividing by $f'(\theta)$. Since in computing a model we change coordinates so that G becomes the Pfaffian, this proves (32). Following this proof gives another formula for m, which improves on (33) in that it avoids the need for field extensions. Indeed we may take $m=(\det N)/(2f_6)^3$ where N is the 6×6 matrix that writes the entries of A above the diagonal in terms of the basis $1,\theta,\dots,\theta^5$ for L.

Remark 2.10. If we change (G,H) by reversing the coordinates $u_0,\dots,u_5$ then A is replaced by A^*. Since $\mathrm{Pf}(A)=\mathrm{Pf}(A^*)$ this does not change ξ, but using (12) and (33), or the formula in the last paragraph, it does change the sign of m. This in turn corresponds to adding the canonical element c (as defined in Section 2.3).

The following alternative way to recover a Selmer group element (ξ,m) from a model (G,H) will be useful in Sections 2.6 and 3.6.

Lemma 2.11. *Let (G,H) be a model and let $Q_0,\dots,Q_5$ be the quadratic forms defined by the formula in Proposition 2.6(i). Then the forms*

$$\Xi(u_0,\dots,u_5)=\sum_{j=0}^{5}Q_j(u_0,\dots,u_5)\theta^j \quad \textit{and} \quad M(u_0,\dots,u_5)=\frac{1}{2^6}\frac{\partial(Q_0,\dots,Q_5)}{\partial(u_0,\dots,u_5)}$$

satisfy $N_{L/k}(\Xi)=M^2$. Moreover specialising these forms at any $a\in k^6$ with $M(a)\neq 0$ gives a pair (ξ,m) representing the equivalence class of the model.

Proof. The first statement is proved by checking that Proposition 2.6(iv) is invariant under all changes of coordinates, and then noting that for G in the standard

form (as specified in Definition 2.7(i)) we have $\det \mathbf{G} = -1$. The second statement follows by (24). $\square$

2.6. **Twisted Kummer surfaces.** We may also represent elements of the 2-Selmer group as 2-coverings. In fact any $\varepsilon \in H^1(k, \mathcal{J}[2])$ may be represented by a 2-covering $(\mathcal{J}_\varepsilon, \pi_\varepsilon)$. By definition this fits in a commutative diagram

$$\begin{tikzcd} \mathcal{J}_\varepsilon \arrow[d, "\phi_\varepsilon"'] \arrow[dr, "\pi_\varepsilon"] & \\ \mathcal{J} \arrow[r, "\times 2"'] & \mathcal{J} \end{tikzcd} \tag{34}$$

where ϕ_ε is an isomorphism defined over $\overline{k}$. We emphasise that ϕ_ε is not part of the data defining the 2-covering. Indeed we are free to change it by composing with translation by T for any $T \in \mathcal{J}[2]$.

We give $\mathcal{J}_\varepsilon$ the structure of principal homogeneous space under $\mathcal{J}$ via

$$\begin{aligned} \mathcal{J} \times \mathcal{J}_\varepsilon &\to \mathcal{J}_\varepsilon \\ (P, Q) &\mapsto \phi_\varepsilon^{-1}(P + \phi_\varepsilon(Q)). \end{aligned} \tag{35}$$

This action is independent of the choice of ϕ_ε and hence defined over k. The natural map $H^1(k, \mathcal{J}[2]) \to H^1(k, \mathcal{J})$ is then realised by $(\mathcal{J}_\varepsilon, \pi_\varepsilon) \mapsto \mathcal{J}_\varepsilon$.

The isomorphism ϕ_ε identifies the map $[-1]$ on $\mathcal{J}$ with an involution ι_ε on $\mathcal{J}_\varepsilon$. Again it may be checked that $\iota_\varepsilon = \phi_\varepsilon^{-1} \circ [-1] \circ \phi_\varepsilon$ is independent of the choice of ϕ_ε and hence defined over k.

We have $\mathcal{J}/[-1] \cong \mathcal{K} \subset \mathbb{P}^3$, where $\mathcal{K}$ is the Kummer surface as described in Section 2.1. Twisting by $\varepsilon \in S^{(2)}(\mathcal{J}/k)$ gives $\mathcal{J}_\varepsilon/\iota_\varepsilon \cong \mathcal{K}_\varepsilon \subset \mathbb{P}^3$ where $\mathcal{K}_\varepsilon$ is a twisted Kummer surface. (To recap Remark 2.9: For general $\varepsilon \in H^1(k, \mathcal{J}[2])$ we might need to replace $\mathbb{P}^3$ by a Brauer-Severi variety S, but for Selmer group elements the local-global principle for the Brauer group shows that $S \cong \mathbb{P}^3$.)

We record this set-up in a commutative diagram

$$\begin{tikzcd} \mathcal{J}_\varepsilon \arrow[r] \arrow[d, "\phi_\varepsilon"'] & \mathcal{K}_\varepsilon \arrow[d, "\psi_\varepsilon"] \\ \mathcal{J} \arrow[r, "|2\Theta|"] & \mathcal{K} \end{tikzcd} \tag{36}$$

where ϕ_ε is as in (34) and $\psi_\varepsilon \in \mathrm{GL}_4(\overline{k})$. The divisor H_ε on $\mathcal{J}_\varepsilon$ obtained by pulling back a hyperplane section on $\mathcal{K}_\varepsilon \subset \mathbb{P}^3$ therefore satisfies

$$H_\varepsilon \sim \phi_\varepsilon^*(2\Theta) \tag{37}$$

where Θ is the theta divisor on $\mathcal{J}$.

In [Y1, Chapter 3] the second author gave two different methods for computing the twisted Kummer surface $\mathcal{K}_\varepsilon$, both of which worked by first computing the change of coordinates ψ_ε. This is typically defined over a degree 16 number field.

Using the models introduced in Section 2.4 we are now able to compute an equation for $\mathcal{K}_\varepsilon$ without making any field extensions. We start by finding a model (G, H) that represents ε. We then put $B = \Lambda \mathbf{H} \Lambda^T$ where Λ is defined by (17). Then, exactly as in Section 2.2, a quartic form defining $\mathcal{K}_\varepsilon \subset \mathbb{P}^3$ is obtained as the GCD of the 3×3 minors of B. Moreover all the formulae we gave in that section for $\mathcal{K}$, $\mathcal{K}^\vee$, $\widetilde{\mathcal{K}}$, $\mathcal{J}$ and the maps between them carry over immediately to their twisted counterparts $\mathcal{K}_\varepsilon$, $(\mathcal{K}_\varepsilon)^\vee$, $\widetilde{\mathcal{K}}_\varepsilon$ and $\mathcal{J}_\varepsilon$. In particular the double cover $\mathcal{J}_\varepsilon \to \mathcal{K}_\varepsilon$ is defined by setting any leading 2×2 minor of B equal to $-f_6$ times a square. As mentioned in the introduction, we find these formulae more convenient to use than those in [FTvL].

Remark 2.12. The model (G, H) that represents ε also determines a 4×4 skew symmetric matrix $A = A_\varepsilon$ as in Section 2.5. Just as in the untwisted case (see Section 2.1) this matrix defines an isomorphism $\mathcal{K}_\varepsilon \to (\mathcal{K}_\varepsilon)^\vee$. In the context of testing equivalence of models, these matrices help us solve for the corresponding transformation when the models are equivalent. This is analogous to the treatment of 3-coverings of elliptic curves in [Fi1]. The matrices A_ε also give, by means of the formula (12), the matrices M_T describing the action of $T \in \mathcal{J}[2]$ on $\mathcal{K}_\varepsilon \subset \mathbb{P}^3$. As explained in Remark 4.3 below, this is useful for reduction.

Remark 2.13. Let $c \in S^{(2)}(\mathcal{J}/k)$ be the canonical element defined in Section 2.3. Then continuing with Remark 2.10 we see that $(\mathcal{K}_\varepsilon)^\vee \cong \mathcal{K}_{\varepsilon+c}$.

The covering map $\pi_\varepsilon : \mathcal{J}_\varepsilon \to \mathcal{J}$ in (34) induces a map $\mathcal{K}_\varepsilon \to \mathcal{K}$, which we also call the covering map. We now explain how to compute this map explicitly. Starting with a model (G, H) we use the formula in Proposition 2.6(i) to define quadratic forms $Q_0, \ldots, Q_5$. Then Lemma 2.11 gives a formula for the covering map from the twisted desingularised Kummer $\widetilde{\mathcal{K}}_\varepsilon = \{Q_3 = Q_4 = Q_5 = 0\} \subset \mathbb{P}^5$ to the Kummer surface $\mathcal{K}$ written as a double cover of $\mathbb{P}^2$ as in (4).

We modify this to give the covering map $\mathcal{K}_\varepsilon \to \mathcal{K}$ where both surfaces are quartic surfaces in $\mathbb{P}^3$. As suggested by Remark 2.2(iii) our construction involves the 2×2 minors of $B = \Lambda \mathbf{H} \Lambda^T$. For $Q = \sum c_{ijkl} z_{ij} z_{kl}$ a quadratic form we put

$$Q \star H = \sum c_{ijkl}(B_{ik}B_{jl} - B_{il}B_{jk}).$$

Then we define quartic forms $E_r = \mathrm{Adj}(\Lambda \mathbf{G}(\mathbf{G}^{-1}\mathbf{H})^r \Lambda^T)_{44}/x_4^2$ and

$$\begin{aligned}
F_0 &= (2f_6)^{-1} E_1, \\
F_1 &= Q_2 \star H - 2f_4 F_0, \\
F_2 &= -Q_1 \star H + f_3 F_0 = -E_2 - f_3 F_0, \\
F_3 &= Q_0 \star H, \\
F_4 &= f_6 E_3 - (f_2 Q_2 - f_3 Q_1 + f_4 Q_0) \star H - (f_1 f_5 - 4 f_2 f_4 + 2 f_3^2) F_0.
\end{aligned}$$

The quartic forms $F_i = F_i(H)$ are covariants of the model H. By this we mean that for some integers $d_0, \ldots, d_4$ we have

$$F_i(\lambda H \circ \wedge^2 P) = \lambda^{d_i} (\det P)^{d_i+1} F_i(H) \circ P^{-T}$$

for all $\lambda \in k^\times$ and $P \in \mathrm{GL}_4(k)$. In fact $(d_0, \ldots, d_4) = (3, 5, 6, 7, 9)$. The next lemma shows that these covariants define the covering map. This generalises an observation of Weil [We] in the case of 2-coverings of elliptic curves.

Lemma 2.14. *Let $\varepsilon \in S^{(2)}(\mathcal{J}/k)$ be represented by a model (G, H) and let the $F_i = F_i(H)$ be the quartic polynomials defined above.*

(i) *$\mathcal{K}_\varepsilon \subset \mathbb{P}^3$ has equation $F_0 = 0$.*

(ii) *Let the matrices M_T be as defined in Remark 2.12. Then $F_0, \ldots, F_4$ are a basis for the space of Heisenberg invariant quartics*

$$\{F \in k[x_1, \ldots, x_4]_4 : F \circ M_T = \det(M_T) F \text{ for all } T \in \mathcal{J}[2]\}.$$

(iii) *The covering map $\mathcal{K}_\varepsilon \to \mathcal{K}$ is given by*

$$(x_1 : \ldots : x_4) \mapsto (F_1 : \ldots : F_4).$$

Proof. Since we are free to extend our field, and the F_i are covariants, it suffices to prove this for H as given in Section 2.2. We already checked (i) in Section 2.2. For (ii) we checked by computer algebra that $F_0, \ldots, F_4$ are linearly independent and then used Lemmas 3.11 and 3.13 below. See Proposition 3.19 below for further details of the proof of (iii). □

Remark 2.15. For the purposes of Lemma 2.14 it would not make any difference if we changed $F_1, \ldots, F_4$ by adding multiples of F_0. The reason for making the choices we did is to simplify the statement of Proposition 3.19 below.

3. The Cassels-Tate pairing on the 2-Selmer group

Let $\mathcal{A}$ be an abelian variety defined over a number field k. The Cassels-Tate pairing is a bilinear map

$$Ш(\mathcal{A}/k) \times Ш(\mathcal{A}^\vee/k) \to \mathbb{Q}/\mathbb{Z}. \tag{38}$$

It has the property that for any integer $n \geqslant 2$ the image of multiplication-by-n on $Ш(\mathcal{A}/k)$ and kernel of multiplication-by-n on $Ш(\mathcal{A}^\vee/k)$ are exact annihilators. This follows from [Mi, Chapter I, Theorem 6.13] or more directly from the injectivity of the middle vertical map in the diagram on page 88 of [Mi]. Flach [Fl] showed that if we identify $\mathcal{A} = \mathcal{A}^\vee$ using a principal polarisation, then the pairing is skew-symmetric.

We take $\mathcal{A} = \mathcal{J}$ a genus 2 Jacobian, and identify $\mathcal{J} = \mathcal{J}^\vee$ using the principal polarisation

$$X \mapsto [\tau_X^* \Theta - \Theta]. \tag{39}$$

By composing with the map $S^{(2)}(\mathcal{J}/k) \to Ш(\mathcal{J}/k)[2]$ in (1), the pairing (38) lifts to a pairing of $\mathbb{F}_2$-vector spaces

$$\langle\ ,\ \rangle_{\mathrm{CT}} : S^{(2)}(\mathcal{J}/k) \times S^{(2)}(\mathcal{J}/k) \to \mathbb{F}_2. \tag{40}$$

Specialising the results cited in the last paragraph, we see that this pairing is symmetric and bilinear and, by chasing around the diagram (2), has kernel the image of the natural map $S^{(4)}(\mathcal{J}/k) \to S^{(2)}(\mathcal{J}/k)$. The pairing is not in general alternating, but rather has the following properties.

Lemma 3.1 (Poonen and Stoll)**.** *Let $c \in S^{(2)}(\mathcal{J}/k)$ be the canonical element as defined in Section 2.3. Then*

(i) $\langle x, x + c\rangle_{\mathrm{CT}} = 0$ *for all* $x \in S^{(2)}(\mathcal{J}/k)$.
(ii) $\langle c, c\rangle_{\mathrm{CT}} = 0$ *if and only if the number of deficient places is even, where a place v is* deficient *if $\mathcal{C}$ has no k_v-rational divisor of degree* 1.
(iii) *The rank of the pairing $\langle\ ,\ \rangle_{\mathrm{CT}}$ is even if and only if $\langle c, c\rangle_{\mathrm{CT}} = 0$.*

Proof. (i) and (ii). See [PSt, Theorem 5 and Corollary 12]. Note that Poonen and Stoll write c for what in our notation is the image of c in $Ш(\mathcal{J}/k)$.
(iii) This follows by (i) and linear algebra. □

One consequence of Lemma 3.1 is that if the number of deficient places is odd then the upper bound for rank $\mathcal{J}(k)$ coming from 2-descent improves by 1, without even having to compute the pairing. Our focus in Section 4 is therefore in giving examples where the rank bound improves by 2 or more.

Remark 3.2. Further partial information about the pairing is given by work of Creutz [Cr] who (assuming there are no deficient places) gave a criterion for whether the canonical element c is in the kernel of the pairing, equivalently, for whether the pairing on $S^{(2)}(\mathcal{J}/k)$ is alternating. More generally, Creutz and Viray [CV, Proposition 6.6] gave a formula for $\langle c, x\rangle_{\mathrm{CT}}$ for arbitrary $x \in S^{(2)}(\mathcal{J}/k)$, provided that the genus 2 curve is everywhere locally soluble.

Remark 3.3. More generally, fixing a prime p, we may write S_m for the image of the p^m-Selmer group in the p-Selmer group. Then, exactly following Cassels' treatment [C1] in the case of elliptic curves, we have inclusions of $\mathbb{F}_p$-vector spaces

$$\mathcal{J}(k)/p\mathcal{J}(k) \subset \ldots \subset S_3 \subset S_2 \subset S_1 = S^{(p)}(\mathcal{J}/k)$$

and a skew-symmetric pairing on each S_m with kernel S_{m+1}. It is interesting to note (paraphrasing the work of Poonen and Stoll) that all of these pairings are

alternating, except for the one we compute in this paper, that is, the pairing on S_1 when $p = 2$. In particular, assuming finiteness of $Ш(\mathcal{J}/k)[2^\infty]$, the rank bounds we compute (by a combination of 2-descent and computing the pairing (40)) always have the same parity as the true rank.

In Section 3.1 we briefly review the definition of the Cassels-Tate pairing (38) that is relevant to our work. Then in Section 3.2 we give our new formula for the pairing (40). In outline it works as follows. Given $\varepsilon, \eta \in S^{(2)}(\mathcal{J}/k)$ we compute equations for the twisted Kummer surfaces $\mathcal{K}_\varepsilon \subset \mathbb{P}^3$ and $\mathcal{K}_\eta \subset \mathbb{P}^3$. If we can find a k-point on $\mathcal{K}_\eta$ then the image of η in $Ш(\mathcal{J}/k)$ splits over a quadratic extension. We can then represent η as a Brauer class on $\mathcal{K}_\varepsilon$ split by the same quadratic extension. We evaluate this Brauer class at suitable local points on $\mathcal{K}_\varepsilon$, and then compute $\langle \varepsilon, \eta \rangle_{\mathrm{CT}}$ as the sum of the local invariants.

To turn this formula into a practical method for computing the pairing, we must compute a rational function on $\mathcal{K}_\varepsilon$ that represents the required Brauer class. In the case of elliptic curves, the first author's solution to this problem [Fi2], was based on the well known formulae relating the x-coordinates of the points $P, Q, P+Q, P-Q$ on an elliptic curve. The analogue of these formulae in genus 2 are the biquadratic forms computed by Flynn [F2]. These describe remnants of the group law on $\mathcal{J}$ on the Kummer surface $\mathcal{K} = \mathcal{J}/[-1]$. This leads in Section 3.3 to the definition of a $(2,2,2)$-form on $\mathbb{P}^3 \times \mathbb{P}^3 \times (\mathbb{P}^3)^\vee$, a twisted version of which specialises to the rational function we need. In Sections 3.4–3.6 we give equations for the twisted $(2,2,2)$-form in terms of our invariant-theoretic formulae for the 2-covering map. Interestingly, we discover that the coefficients of the original $(2,2,2)$-form may be viewed as the structure constants for an étale algebra.

3.1. **Definition of the Cassels-Tate pairing.** We briefly review the homogeneous space definition of the Cassels-Tate pairing (38), following Poonen and Stoll [PSt] and Milne [Mi, Chapter 1, Remark 6.11].

We start with $a \in Ш(\mathcal{A}/k)$ and $b \in Ш(\mathcal{A}^\vee/k)$. Let X be a (locally trivial) principal homogeneous space over k representing a. When we write $\mathrm{Div}^0(X)$ and $\mathrm{Pic}^0(X)$ we shall mean these groups for X over $\overline{k}$. Since $\mathrm{Pic}^0(X)$ is canonically isomorphic as a $\mathrm{Gal}(\overline{k}/k)$-module to $\mathrm{Pic}^0(\mathcal{A}) = \mathcal{A}^\vee(\overline{k})$, the element $b \in Ш(\mathcal{A}^\vee/k) \subset H^1(k, \mathcal{A}^\vee)$ corresponds to an element of $H^1(k, \mathrm{Pic}^0(X))$.

The short exact sequence of Galois modules

$$0 \to \overline{k}(X)^\times/\overline{k}^\times \to \mathrm{Div}^0(X) \to \mathrm{Pic}^0(X) \to 0,$$

induces a long exact sequence of Galois cohomology

$$\ldots \to H^1(k, \mathrm{Pic}^0(X)) \to H^2(k, \overline{k}(X)^\times/\overline{k}^\times) \to \ldots \tag{41}$$

Let $b' \in H^2(k, \overline{k}(X)^\times/\overline{k}^\times)$ be the image of b. Next we consider the short exact sequence

$$0 \to \overline{k}^\times \to \overline{k}(X)^\times \to \overline{k}(X)/\overline{k}^\times \to 0,$$

and its associated long exact sequence

$$\ldots \to H^2(k,\overline{k}^\times) \to H^2(k,\overline{k}(X)^\times) \to H^2(k,\overline{k}(X)^\times/\overline{k}^\times) \to H^3(k,\overline{k}^\times) \to \ldots \tag{42}$$

Since k is a number field we have $H^3(k,\overline{k}^\times) = 0$. Therefore b' lifts to some $f' \in H^2(k,\overline{k}(X)^\times)$. In the local analogue of (42), each f'_v maps to zero (since b is locally trivial) and so is the image of some $c_v \in H^2(k_v,\overline{k}_v^\times) = \mathrm{Br}(k_v)$. The Cassels-Tate pairing is defined by

$$(a,b) \mapsto \sum_v \mathrm{inv}_v(c_v) \in \mathbb{Q}/\mathbb{Z}.$$

Remark 3.4. (i) Although the sum is over all places v of k, it may be shown that only finitely many places contribute and so the sum is in fact finite.
(ii) We can compute c_v by evaluating f'_v at any local point $P_v \in X(k_v)$. Since b is locally trivial, the choice of P_v does not matter.
(iii) The pairing is independent of the choice of f' since by class field theory the sum of the local invariants of an element in $\mathrm{Br}(k)$ is always zero.

3.2. **A formula for the Cassels-Tate pairing.** In this section we give our new formula for the pairing (40). Accordingly, we start with $\varepsilon,\eta \in S^{(2)}(\mathcal{J}/k)$ and aim to compute $\langle\varepsilon,\eta\rangle_{\mathrm{CT}}$. We write $\mathcal{K}_\varepsilon$, $\mathcal{K}_\eta$ and $\mathcal{K}_{\varepsilon+\eta}$ for the corresponding twisted Kummer surfaces. Our method depends on finding a rational point $P \in \mathcal{K}_\eta(k)$. In general there is no guarantee that such a point exists, but as discussed in the introduction this does not appear to be a severe restriction in practice. Since $\mathcal{J}_\eta \to \mathcal{K}_\eta$ is a double cover, the point P lifts to a point defined over $k(\sqrt{a})$ for some $a \in k$. We may suppose that P is not a node, and that a is not a square, otherwise $\mathcal{J}_\eta$ is trivial as a homogeneous space, in which case η has trivial image in $Ш(\mathcal{J}/k)$ and $\langle\varepsilon,\eta\rangle_{\mathrm{CT}} = 0$. As in Section 2.6, we have $\mathcal{K}_\varepsilon = \mathcal{J}_\varepsilon/\iota_\varepsilon$.

Theorem 3.5. *Suppose that $P \in \mathcal{K}_\eta(k)$ lifts to a point on $\mathcal{J}_\eta$ defined over $k(\sqrt{a})$. Let H_ε and $H_{\varepsilon+\eta}$ be divisors on $\mathcal{J}_\varepsilon$ and $\mathcal{J}_{\varepsilon+\eta}$ obtained by pulling back hyperplane sections on $\mathcal{J}_\varepsilon \to \mathcal{K}_\varepsilon \subset \mathbb{P}^3$ and $\mathcal{J}_{\varepsilon+\eta} \to \mathcal{K}_{\varepsilon+\eta} \subset \mathbb{P}^3$. Then*

(i) *The point P determines an isomorphism $\phi : \mathcal{J}_\varepsilon \to \mathcal{J}_{\varepsilon+\eta}$ defined over $k(\sqrt{a})$.*
(ii) *There is a k-rational function g on $\mathcal{J}_\varepsilon$ with divisor*

$$\mathrm{div}(g) = \phi^* H_{\varepsilon+\eta} + \iota_\varepsilon^*(\phi^* H_{\varepsilon+\eta}) - 2H_\varepsilon.$$

(iii) *The Cassels-Tate pairing (40) is given by*

$$\langle\varepsilon,\eta\rangle_{\mathrm{CT}} = \sum_v (a, g(P_v))_v$$

where for each place v of k we pick a local point $P_v \in \mathcal{J}_\varepsilon(k_v)$, avoiding the zeros and poles of g, and $(\ ,\ )_v : k_v^\times/(k_v^\times)^2 \times k_v^\times/(k_v^\times)^2 \to \mathbb{F}_2$ is the Hilbert norm residue symbol.

Remark 3.6. (i) The theorem is only useful if we have a practical method for computing the rational function g. This is the subject of Sections 3.3–3.6.
(ii) The scaling of g is not important for the same reason as in Remark 3.4(iii).
(iii) Since g factors via $\mathcal{K}_\varepsilon$ we may evaluate it at local points on $\mathcal{K}_\varepsilon$, provided that we are careful to choose local points that can be lifted to local points on $\mathcal{J}_\varepsilon$.

We start the proof of Theorem 3.5 by describing a twisted form of the group law on $\mathcal{J}$.

Lemma 3.7. *Let $\varepsilon, \eta \in H^1(k, \mathcal{J}[2])$. Let $\phi_\varepsilon : \mathcal{J}_\varepsilon \to \mathcal{J}$, $\phi_\eta : \mathcal{J}_\eta \to \mathcal{J}$ and $\phi_{\varepsilon+\eta} : \mathcal{J}_{\varepsilon+\eta} \to \mathcal{J}$ be isomorphisms defined over $\overline{k}$ making the diagram* (34) *and its analogues for η and $\varepsilon + \eta$ commute. Then, after possibly adjusting our choice of $\phi_{\varepsilon+\eta}$, there is a morphism μ defined over k making the following diagram commute*

$$\begin{tikzcd} \mathcal{J}_\varepsilon \arrow[d, "\phi_\varepsilon"] & \times & \mathcal{J}_\eta \arrow[r, "\mu"] \arrow[d, "\phi_\eta"] & \mathcal{J}_{\varepsilon+\eta} \arrow[d, "\phi_{\varepsilon+\eta}"] \\ \mathcal{J} & \times & \mathcal{J} \arrow[r, "+"] & \mathcal{J}. \end{tikzcd}$$

Proof. We know that ε is represented by a cocycle $(\sigma \mapsto \varepsilon_\sigma)$ where $\sigma(\phi_\varepsilon)\phi_\varepsilon^{-1}$ is translation by $\varepsilon_\sigma \in \mathcal{J}[2]$. The corresponding statements hold for η and $\varepsilon + \eta$. Since the cocycles $(\sigma \mapsto (\varepsilon + \eta)_\sigma)$ and $(\sigma \mapsto \varepsilon_\sigma + \eta_\sigma)$ differ by a coboundary, we may adjust our choice of $\phi_{\varepsilon+\eta}$ so that $(\varepsilon + \eta)_\sigma = \varepsilon_\sigma + \eta_\sigma$ for all $\sigma \in \mathrm{Gal}(\overline{k}/k)$.

Let $\mu : \mathcal{J}_\varepsilon \times \mathcal{J}_\eta \to \mathcal{J}_{\varepsilon+\eta}$ be the morphism that makes the diagram in the statement of the lemma commute. For any $P \in \mathcal{J}_\varepsilon$, $Q \in \mathcal{J}_\eta$ and $\sigma \in \mathrm{Gal}(\overline{k}/k)$ we have

$$\begin{aligned} \sigma(\mu(P, Q)) &= \sigma(\phi_{\varepsilon+\eta}^{-1}(\phi_\varepsilon(P) + \phi_\eta(Q))) \\ &= \phi_{\varepsilon+\eta}^{-1}(\sigma(\phi_\varepsilon(P)) + \sigma(\phi_\eta(Q)) - \varepsilon_\sigma - \eta_\sigma) \\ &= \phi_{\varepsilon+\eta}^{-1}(\phi_\varepsilon(\sigma P) + \phi_\eta(\sigma Q)) \\ &= \mu(\sigma P, \sigma Q). \end{aligned}$$

This proves that μ is defined over k. □

Remark 3.8. We are still free to replace $\phi_{\varepsilon+\eta}$ by $P \mapsto \phi_{\varepsilon+\eta}(P) + T$ for $T \in \mathcal{J}(k)[2]$, and for this reason there are $\#\mathcal{J}(k)[2]$ choices for the map μ.

Proof of Theorem 3.5. Let $\{Q, Q'\} \subset \mathcal{J}_\eta$ be the inverse image of $P \in \mathcal{K}_\eta$, and let μ be as defined in Lemma 3.7. Then $\phi = \mu(-, Q)$ is an isomorphism $\mathcal{J}_\varepsilon \to \mathcal{J}_{\varepsilon+\eta}$ defined over $k(Q) = k(\sqrt{a})$. This proves (i). From Lemma 3.7 we also get a

commutative diagram

$$\begin{tikzcd} \mathcal{J}_\varepsilon \arrow[r, "\phi"] \arrow[d, "\phi_\varepsilon"'] & \mathcal{J}_{\varepsilon+\eta} \arrow[d, "\phi_{\varepsilon+\eta}"] \\ \mathcal{J} \arrow[r, "\tau_R"] & \mathcal{J}, \end{tikzcd} \tag{43}$$

where τ_R is translation by $R = \phi_\eta(Q)$.

Let $\psi : \mathcal{J}_\eta \to \mathcal{J}$ be the isomorphism given by $X \mapsto X - Q$. Then $\sigma(\psi)\psi^{-1}$ is translation by $Q - \sigma(Q)$. By (35) we have $Q - \sigma(Q) = \phi_\eta(Q) - \phi_\eta(\sigma(Q))$. Since $\phi_\eta(Q) = R$ and ι_η swaps over Q and Q' we have $\phi_\eta(Q') = -R$. It follows that the image of η in $H^1(k, \mathcal{J})$ is represented by the cocycle

$$\sigma \mapsto \begin{cases} 0_{\mathcal{J}} & \text{if } \sigma(\sqrt{a}) = \sqrt{a}, \\ 2R & \text{if } \sigma(\sqrt{a}) = -\sqrt{a}. \end{cases}$$

We follow the definition of the Cassels-Tate pairing in Section 3.1, with a and b the images of ε and η in $Ш(\mathcal{J}/k)$ and $Ш(\mathcal{J}^\vee/k)$, in the latter case using the principal polarisation (39). Now b corresponds to the element in $H^1(k, \operatorname{Pic}^0 \mathcal{J}_\varepsilon)$ represented by the cocycle

$$\sigma \mapsto \begin{cases} \mathrm{id} & \text{if } \sigma(\sqrt{a}) = \sqrt{a}, \\ [\phi_\varepsilon^*(\tau_{2R}^*\Theta - \Theta)] & \text{if } \sigma(\sqrt{a}) = -\sqrt{a}. \end{cases}$$

Next we claim that

$$\phi_\varepsilon^*(\tau_{2R}^*\Theta - \Theta) \sim \phi_\varepsilon^*(\tau_R^*(2\Theta) - 2\Theta) \sim \phi^* H_{\varepsilon+\eta} - H_\varepsilon.$$

Indeed the first linear equivalence follows from the fact the polarisation (39) is a group homomorphism, whereas the second follows from (37) and (43).

To apply the connecting homomorphism in (41) we lift to a cochain

$$\sigma \mapsto \begin{cases} \mathrm{id} & \text{if } \sigma(\sqrt{a}) = \sqrt{a}, \\ \phi^* H_{\varepsilon+\eta} - H_\varepsilon & \text{if } \sigma(\sqrt{a}) = -\sqrt{a}, \end{cases}$$

and then take its differential to get

$$(\sigma_1, \sigma_2) \mapsto \begin{cases} \phi^* H_{\varepsilon+\eta} + \sigma_1(\phi^* H_{\varepsilon+\eta}) - 2H_\varepsilon & \text{if } \sigma_1(\sqrt{a}) = \sigma_2(\sqrt{a}) = -\sqrt{a}, \\ \mathrm{id} & \text{otherwise.} \end{cases}$$

For any $\sigma_1 \in \operatorname{Gal}(\overline{k}/k)$ with $\sigma_1(\sqrt{a}) = -\sqrt{a}$ we have $\sigma_1(\phi) = \iota_{\varepsilon+\eta} \circ \phi \circ \iota_\varepsilon$ and hence $\sigma_1(\phi^* H_{\varepsilon+\eta}) = \iota_\varepsilon^*(\phi^* H_{\varepsilon+\eta})$. Thus there exists a k-rational function g on $\mathcal{J}_\varepsilon$ as specified in (ii), and we can take $c_v \in H^2(k_v, \overline{k}_v^\times) = \operatorname{Br}(k_v)$ to be the class of

$$(\sigma_1, \sigma_2) \mapsto \begin{cases} g(P_v) & \text{if } \sigma_1(\sqrt{a}) = \sigma_2(\sqrt{a}) = -\sqrt{a}, \\ 1 & \text{otherwise,} \end{cases}$$

where $P_v \in \mathcal{J}_\varepsilon(k_v)$ is any local point avoiding the zeros and poles of g.

By [Se, Chapter XIV, Section 2, Proposition 5] the element $c_v \in \mathrm{Br}(k_v)$ is represented by the quaternion algebra $(a, g(P_v))$. In particular its local invariant is 0 or 1/2 according as the Hilbert symbol $(a, g(P_v))_v$ is 1 or -1. By abuse of notation, we let the Hilbert symbol take values in $\mathbb{F}_2$. The Cassels-Tate pairing is then given by summing the Hilbert symbols $(a, g(P_v))_v$ as claimed. □

3.3. **Remnants of the group law.** In this section we explain how the rational function g in Theorem 3.5 can be computed by specialising a certain $(2,2,2)$-form. In later sections we explain how to compute this $(2,2,2)$-form.

The Kummer surface $\mathcal{K} = \mathcal{J}/[-1]$ retains some remnants of the group law on $\mathcal{J}$. As usual we embed $\mathcal{K} \subset \mathbb{P}^3$ with coordinates $x_1, \dots, x_4$. Flynn [F2] computed biquadratic forms Φ_{ij} such that for all $P, Q \in \mathcal{J}$ we have

$$\begin{aligned} &\Phi_{ij}(x_1(P), \dots, x_4(P); x_1(Q), \dots, x_4(Q)) \\ &\qquad \propto \big(x_i(P+Q)x_j(P-Q) + x_i(P-Q)x_j(P+Q)\big) \end{aligned} \tag{44}$$

where the constant of proportionality is independent of $1 \leqslant i, j \leqslant 4$. We package these biquadratic forms as a $(2,2,2)$-form on $\mathbb{P}^3 \times \mathbb{P}^3 \times (\mathbb{P}^3)^\vee$. Explicitly, we put $\mathbf{x} = (x_1, \dots, x_4)$, $\mathbf{y} = (y_1, \dots, y_4)$, $\mathbf{z} = (z_1, \dots, z_4)$ and define

$$\Phi(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \sum_{i,j=1}^{4} \Phi_{ij}(\mathbf{x}, \mathbf{y}) z_i z_j.$$

Since the Φ_{ij} are symmetric, i.e., $\Phi_{ij}(\mathbf{x}, \mathbf{y}) = \Phi_{ij}(\mathbf{y}, \mathbf{x})$, we have $\Phi(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \Phi(\mathbf{y}, \mathbf{x}, \mathbf{z})$. If $P, Q \in \mathcal{J}$ then by (44) we have

$$\begin{aligned} &\Phi(x_1(P), \dots, x_4(P); x_1(Q), \dots, x_4(Q); c_1, c_2, c_3, c_4) \\ &\qquad \propto \big(\textstyle\sum_{i=1}^4 c_i x_i(P+Q)\big)\big(\textstyle\sum_{j=1}^4 c_j x_j(P-Q)\big). \end{aligned} \tag{45}$$

where the constant of proportionality is independent of $c_1, \dots, c_4$. We note for later use the immediate consequence that for fixed $Q \in \mathcal{J}$ and $(c_1 : \dots : c_4) \in (\mathbb{P}^3)^\vee$ the left hand side of (45) is a non-zero function of P.

Just as the $(2,2,2)$-form Φ corresponds to the group law on $\mathcal{J}$, there is a twisted $(2,2,2)$-form $\Phi_{\varepsilon,\eta}$ corresponding to the twisted group law

$$\mu : \mathcal{J}_\varepsilon \times \mathcal{J}_\eta \to \mathcal{J}_{\varepsilon+\eta}$$

defined in Lemma 3.7. The analogue of (45) is that if $P \in \mathcal{J}_\varepsilon$ and $Q \in \mathcal{J}_\eta$ then

$$\begin{aligned} &\Phi_{\varepsilon,\eta}(x_1(P), \dots, x_4(P); x_1(Q), \dots, x_4(Q); c_1, c_2, c_3, c_4) \\ &\qquad \propto \big(\textstyle\sum_{i=1}^4 c_i x_i(\mu(P,Q))\big)\big(\textstyle\sum_{j=1}^4 c_j x_j(\mu(P, \iota_\eta(Q)))\big). \end{aligned} \tag{46}$$

The next theorem computes the rational function g in Theorem 3.5.

Theorem 3.9. *Let $Q \in \mathcal{J}_\eta$ and let $\phi = \mu(-, Q) : \mathcal{J}_\varepsilon \to \mathcal{J}_{\varepsilon+\eta}$. Let H_ε and $H_{\varepsilon+\eta}$ be the divisors on $\mathcal{J}_\varepsilon$ and $\mathcal{J}_{\varepsilon+\eta}$ obtained by pulling back the hyperplane sections $\{x_1 = 0\}$ and $\{c_1x_1 + \ldots + c_4x_4 = 0\}$ on $\mathcal{J}_\varepsilon \to \mathcal{K}_\varepsilon \subset \mathbb{P}^3$ and $\mathcal{J}_{\varepsilon+\eta} \to \mathcal{K}_{\varepsilon+\eta} \subset \mathbb{P}^3$. Then*

$$g = \Phi_{\varepsilon,\eta}(x_1, \ldots, x_4; x_1(Q), \ldots, x_4(Q); c_1, c_2, c_3, c_4)/x_1^2$$

is a rational function on $\mathcal{J}_\varepsilon$ with divisor

$$\operatorname{div}(g) = \phi^* H_{\varepsilon+\eta} + \iota_\varepsilon^*(\phi^* H_{\varepsilon+\eta}) - 2H_\varepsilon. \tag{47}$$

Proof. Let $P \in \mathcal{J}_\varepsilon$ and $P' = \phi(P) = \mu(P, Q) \in \mathcal{J}_{\varepsilon+\eta}$. If $c_1x_1(P') + \ldots + c_4x_4(P') = 0$ then by (46) we have $g(P) = 0$. Therefore g vanishes on $\phi^* H_{\varepsilon+\eta}$. Since g factors via the double cover $\mathcal{J}_\varepsilon \to \mathcal{K}_\varepsilon$ it also vanishes on $\iota_\varepsilon^*(\phi^* H_{\varepsilon+\eta})$.

By the observation following (45) we know that g does not vanish identically on $\mathcal{J}_\varepsilon$. Assuming that $\phi^* H_{\varepsilon+\eta}$ and $\iota_\varepsilon^*(\phi^* H_{\varepsilon+\eta})$ are distinct and irreducible it follows that

$$\operatorname{div}(g) = \phi^* H_{\varepsilon+\eta} + \iota_\varepsilon^*(\phi^* H_{\varepsilon+\eta}) + E - 2H_\varepsilon \tag{48}$$

for some effective divisor E. By considering the quotient of g and the rational function of the same name in Theorem 3.5(ii), it follows that $E = 0$.

This completes the proof under the assumption in the last paragraph. We showed in [Y1, Section 5.2.3] that the assumption is satisfied for generic choices of $Q \in \mathcal{J}$ and $(c_1 : \ldots : c_4) \in (\mathbb{P}^3)^\vee$, and from this we were able to deduce that the theorem holds in general. □

In [Y1] the second author computed the twisted $(2, 2, 2)$-form $\Phi_{\varepsilon,\eta}$ from the untwisted $(2, 2, 2)$-form Φ by directly making the changes of coordinates ψ_ε, ψ_η and $\psi_{\varepsilon+\eta}$ as defined in (36). Since these 4×4 matrices are typically defined over (different) degree 16 number fields, this method is rather slow. Our improved method for computing the twisted Kummer surfaces (see Section 2.6) also means we do not have these matrices to hand, although it would be possible to compute them in hindsight by matching up the nodes on $\mathcal{K}$ and $\mathcal{K}_\varepsilon$.

In Section 3.6 we give a formula, analogous to that in [Fi2], that enables us to compute the twisted $(2, 2, 2)$-form $\Phi_{\varepsilon,\eta}$ without working in field extensions of such large degree.

3.4. **The Heisenberg group.** In this section we describe some of the geometry behind our method for computing the $(2, 2, 2)$-forms.

Definition 3.10. The *standard level* 2 *Heisenberg group* is the subgroup $H_2 \subset \mathrm{GL}_4$ generated by the matrices

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

It is a non-abelian group of order 2^5 and sits in an exact sequence

$$0 \to \{\pm 1\} \to H_2 \to \overline{H}_2 \to 0,$$

where $\overline{H}_2 \cong (\mathbb{Z}/2\mathbb{Z})^4$ is the image of H_2 in PGL_4.

Lemma 3.11. *Let $\mathcal{K} \subset \mathbb{P}^3$ be a Kummer surface defined over an algebraically closed field of characteristic not 2. We may change coordinates on $\mathbb{P}^3$ so that*

(i) *the isomorphisms $\mathcal{K} \to \mathcal{K}$ corresponding to a $(2,4)$-partition of the Weierstrass points (equivalently to translation by some $0 \neq T \in \mathcal{J}[2]$) are given by the non-trivial elements of $\overline{H}_2$, and*
(ii) *the isomorphisms $\mathcal{K} \to \mathcal{K}^\vee$ corresponding to a $(1,5)$, respectively $(3,3)$, partition of the Weierstrass points are given by the skew-symmetric, respectively symmetric, matrices in $\overline{H}_2$.*

Proof. The existence of a change of coordinates satisfying (i) is a special case of [BL, Example 6.7.4]. Since all the matrices are orthogonal, the conclusion in (i) for $\mathcal{K}$ also holds for the dual Kummer $\mathcal{K}^\vee$. The claims in (ii) follow by Remark 2.1 and the fact that $\overline{H}_2$ is its own centraliser inside PGL_4. □

Lemma 3.12. *Let $\mathcal{K} \subset \mathbb{P}^3$ be a Kummer surface defined over a field of characteristic not 2. Let $B_1, \ldots, B_{10}$ be 4×4 symmetric matrices whose images in PGL_4 correspond to the $(3,3)$-partitions of the Weierstrass points. If we define quadratic forms by $Q_i(x_1, \ldots, x_4) = \frac{1}{2}\mathbf{x}^T B_i \mathbf{x}$ and $Q_i^*(y_1, \ldots, y_4) = \frac{1}{2}\mathbf{y}^T B_i^{-1} \mathbf{y}$ then*

$$\sum_{i=1}^{10} Q_i(x_1, \ldots, x_4) Q_i^*(y_1, \ldots, y_4) = \left(\sum_{j=1}^{4} x_j y_j \right)^2. \tag{49}$$

Proof. The conclusions of the lemma are unchanged if we extend our field, rescale the matrices B_i, or make a change of coordinates on $\mathbb{P}^3$. By Lemma 3.11 we may therefore assume that the B_i are (lifts to GL_4 of) the symmetric matrices in $\overline{H}_2$.

The left hand side of (49) is now

$$\begin{aligned}\frac{1}{4}\sum_{u,v\in\{\pm1\}}&(x_1^2+ux_2^2+vx_3^2+uvx_4^2)(y_1^2+uy_2^2+vy_3^2+uvy_4^2)\\&+\sum_{u\in\{\pm1\}}(x_1x_2+ux_3x_4)(y_1y_2+uy_3y_4)\\&+\sum_{u\in\{\pm1\}}(x_1x_3+ux_2x_4)(y_1y_3+uy_2y_4)\\&+\sum_{u\in\{\pm1\}}(x_1x_4+ux_2x_3)(y_1y_4+uy_2y_3).\end{aligned}$$

Expanding this out gives the right hand side of (49). □

Lemma 3.13. *The space of quartic forms invariant under the natural action of the standard level* 2 *Heisenberg group* H_2 *is* 5*-dimensional, spanned by*

$$x_1^4+x_2^4+x_3^4+x_4^4,\quad x_1^2x_2^2+x_3^2x_4^2,\quad x_1^2x_3^2+x_2^2x_4^2,\quad x_1^2x_4^2+x_2^2x_3^2,\quad x_1x_2x_3x_4.$$

Up to scalars, there are exactly 10 *quartic forms in this space that factor as the square of a quadratic form. These are the squares of the quadratic forms corresponding to the symmetric matrices in* $\overline{H}_2$.

Proof. The lemma may be proved either by a brute force calculation, or by decomposing the 2nd and 4th symmetric powers of the standard representation of H_2 into irreducible representations. □

3.5. **A formula for the untwisted** $(2,2,2)$**-form.** As usual let $\mathcal{C}$ be the genus 2 curve with equation $y^2=f(x)$, where the coefficients of f are labelled as in (3). We recall that Flynn [F2] computed the biquadratic forms $\Phi_{ij}(\mathbf{x},\mathbf{y})$, with coefficients in $\mathbb{Z}[f_0,\ldots,f_6]$, and in Section 3.3 we packaged these as a $(2,2,2)$-form

$$\Phi(\mathbf{x},\mathbf{y},\mathbf{z})=\sum_{i,j=1}^{4}\Phi_{ij}(\mathbf{x},\mathbf{y})z_iz_j. \tag{50}$$

A generic calculation shows that

$$\Phi(\mathbf{x};\mathbf{x};z_1,z_2,z_3,0)=2(z_2^2-z_1z_3)F(\mathbf{x}) \tag{51}$$

where F is the equation (5) for $\mathcal{K}\subset\mathbb{P}^3$.

In this section we give a new formula for the $(2,2,2)$-form Φ, and in the next section we modify it to give a formula for the twisted $(2,2,2)$-form $\Phi_{\varepsilon,\eta}$. Both formulae involve working with the étale algebra of degree 10, say L_{10}, corresponding to the $(3,3)$-partitions of the Weierstrass points.

Remark 3.14. As explained in [S2, Lemma 5.3], after possibly replacing $f(x)$ by $f(x+n)$ for some $n \in \mathbb{Z}$, we can take L_{10} to be defined by the degree 10 polynomial specified in [CF, page 56]. If L_{10} is a field and f has roots $\theta_1, \ldots, \theta_6$ then this is the minimal polynomial of $\theta_1\theta_2\theta_3 + \theta_4\theta_5\theta_6$.

Supposing that f factors as the product of two cubics, say,

$$f(x) = f_6(x^3 + r_2x^2 + r_1x + r_0)(x^3 + s_2x^2 + s_1x + s_0), \tag{52}$$

we define a column vector

$$\lambda = (\lambda_1, \ldots, \lambda_4)^T = (f_6(r_0s_2 + r_2s_0), f_6(r_0 + s_0), f_6(r_1 + s_1), 1)^T \tag{53}$$

and a symmetric matrix

$$A = f_6 \begin{pmatrix} r_2 - s_2 & -r_1 + s_1 & r_0 - s_0 \\ -r_1 + s_1 & r_0 + r_1s_2 - r_2s_1 - s_0 & -r_0s_2 + r_2s_0 \\ r_0 - s_0 & -r_0s_2 + r_2s_0 & r_0s_1 - r_1s_0 \end{pmatrix}.$$

Lemma 3.15. *If f factors as in* (52) *as the product of two cubic polynomials, then the* $(2,2,2)$*-form* Φ *has the following properties.*

(i) $\Phi(\mathbf{x}, \mathbf{y}, \lambda) = (\mathbf{x}^T B\mathbf{y})^2$ *where*

$$B = \lambda\lambda^T + \begin{pmatrix} \operatorname{Adj} A & 0 \\ 0 & 0 \end{pmatrix}.$$

(ii) *If we put $b_{ii} = B_{ii}$ and $b_{ij} = 2B_{ij}$ for $i \neq j$ then*

$$b_{ij}b_{kl} = \sum_{m \leqslant n} \operatorname{coeff}(\Phi_{mn} | x_ix_jy_ky_l) b_{mn}$$

for all $1 \leqslant i, j, k, l \leqslant 4$.

Proof. We checked this by computer algebra, using Flynn's formulae for the biquadratic forms $\Phi_{ij}(\mathbf{x}, \mathbf{y})$ specialised to f of the form (52). □

Remark 3.16. The b_{ij} are unchanged when we swap over the two cubic factors in (52), and are therefore elements of L_{10}. In fact they form a basis. Lemma 3.15(iii) then says that the 10^3 coefficients of the $(2,2,2)$-form Φ are the structure constants for the degree 10 étale algebra L_{10} with respect to this basis.

The first part of the following proposition is an explicit form of a result of Stoll [S1, Lemma 5.2].

Proposition 3.17. *Let $\lambda_1, \lambda_2, \lambda_3 \in L_{10}$ be given by* (53)*. Then the quartic form*

$$P(x_1, \ldots, x_4) = 2(\lambda_2^2 - \lambda_1\lambda_3)F(\mathbf{x}) + 2\sum_{i=1}^{3} \lambda_i \Phi_{i4}(\mathbf{x}, \mathbf{x}) + \Phi_{44}(\mathbf{x}, \mathbf{x})$$

factors as $P = Q^2$ where $Q \in L_{10}[x_1, x_2, x_3, x_4]$ is a quadratic form. If we scale Q so that the coefficient of x_4^2 is 1 and write Q^* for the dual quadratic form (in the sense of Lemma 3.12) then the $(2, 2, 2)$-form is given by

$$\Phi(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \mathrm{Tr}_{L_{10}/k}(Q(\mathbf{x})Q(\mathbf{y})Q^*(\mathbf{z})).$$

Proof. By (50) and (51) we have $\Phi(\mathbf{x}, \mathbf{x}, \lambda) = P(x_1, \ldots, x_4)$. By Lemma 3.15(i) this factors as $P = Q^2$ where $Q(\mathbf{x}) = \sum_{i \leqslant j} b_{ij} x_i x_j$ and the coefficient of x_4^2 is 1. By Lemma 3.15(ii) we have

$$Q(\mathbf{x})Q(\mathbf{y}) = \left(\sum_{i \leqslant j} b_{ij} x_i x_j\right)\left(\sum_{k \leqslant l} b_{kl} y_k y_l\right) = \sum_{m \leqslant n} \Phi_{mn}(\mathbf{x}, \mathbf{y}) b_{mn}. \tag{54}$$

On the other hand by Lemma 3.12 we have

$$\mathrm{Tr}_{L_{10}/k}(b_{mn} Q^*(\mathbf{z})) = \begin{cases} z_m z_n & \text{if } m = n, \\ 2 z_m z_n & \text{if } m \neq n. \end{cases} \tag{55}$$

Combining (54) and (55) gives

$$\mathrm{Tr}_{L_{10}/k}(Q(\mathbf{x})Q(\mathbf{y})Q^*(\mathbf{z})) = \sum_{m,n=1}^{4} \Phi_{mn}(\mathbf{x}, \mathbf{y}) z_m z_n = \Phi(\mathbf{x}, \mathbf{y}, \mathbf{z}). \qquad \square$$

Remark 3.18. As noted in [CF, page 24], the doubling map on the Kummer surface $\mathcal{K} = \{F = 0\} \subset \mathbb{P}^3$ is given by

$$(x_1 : x_2 : x_3 : x_4) \mapsto (\Phi_{14}(\mathbf{x}, \mathbf{x}) : \Phi_{24}(\mathbf{x}, \mathbf{x}) : \Phi_{34}(\mathbf{x}, \mathbf{x}) : \tfrac{1}{2}\Phi_{44}(\mathbf{x}, \mathbf{x})).$$

The quartic form P in Proposition 3.17 is a linear combination of the Heisenberg invariant quartics $F, \Phi_{14}(\mathbf{x}, \mathbf{x}), \ldots, \Phi_{44}(\mathbf{x}, \mathbf{x})$ that factors as the square of a quadratic form. By Lemma 3.13 this quadratic form Q corresponds to a $(3, 3)$-partition of the Weierstrass points. In particular, an alternative way to compute Q is as the quadratic form defined by the symmetric matrix (14).

3.6. **A formula for the twisted $(2, 2, 2)$-form.** In the last section we gave a formula for the untwisted $(2, 2, 2)$-form Φ. We now modify this to compute the twisted $(2, 2, 2)$-form $\Phi_{\varepsilon,\eta}$.

Proposition 3.19. *Let $\lambda_1, \ldots, \lambda_4 \in L_{10}$ be given by (53). Let $\varepsilon \in S^{(2)}(\mathcal{J}/k)$ be represented by a model (G, H), and let $F_0, \ldots, F_4 \in k[x_1, \ldots, x_4]$ be the associated quartic forms, as defined in Section 2.6. Then the quartic form*

$$P_\varepsilon(x_1, \ldots, x_4) = (\lambda_2^2 - \lambda_1\lambda_3)F_0(x_1, \ldots, x_4) + \sum_{i=1}^{4} \lambda_i F_i(x_1, \ldots, x_4) \tag{56}$$

factors as

$$P_\varepsilon(x_1, \ldots, x_4) = \alpha_\varepsilon\, Q_\varepsilon(x_1, \ldots, x_4)^2 \tag{57}$$

where $\alpha_\varepsilon \in L_{10}^\times$ and $Q_\varepsilon \in L_{10}[x_1, \ldots, x_4]$ is a quadratic form.

Proof. For the proof we are free to extend our field k. Since the F_i are covariants we may then reduce to the case where H is as given in Section 2.2. In this case we find that $F_0, \ldots, F_4$ are (up to an overall scaling) the quartics

$$2F,\ 2\Phi_{14}(\mathbf{x}, \mathbf{x}),\ 2\Phi_{24}(\mathbf{x}, \mathbf{x}),\ 2\Phi_{34}(\mathbf{x}, \mathbf{x}),\ \Phi_{44}(\mathbf{x}, \mathbf{x}).$$

We are done by the first part of Proposition 3.17. □

Theorem 3.20. *Let $\varepsilon, \eta \in S^{(2)}(\mathcal{J}/k)$. The twisted $(2, 2, 2)$-form is given by*

$$\Phi_{\varepsilon,\eta}(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \mathrm{Tr}_{L_{10}/k}(\mu Q_\varepsilon(\mathbf{x}) Q_\eta(\mathbf{y}) Q^*_{\varepsilon+\eta}(\mathbf{z}))$$

for some $s \in k^\times$ and $\mu \in L_{10}^\times$ satisfying $\alpha_\varepsilon\alpha_\eta/\alpha_{\varepsilon+\eta} = s\mu^2$.

Proof. Let $\psi_\varepsilon \in \mathrm{GL}_4(\overline{k})$ be the matrix in (36) scaled so that the quartic forms in Propositions 3.17 and 3.19 are related by $P \circ \psi_\varepsilon = P_\varepsilon$. The corresponding quadratic forms are then related by $Q \circ \psi_\varepsilon = \sqrt{\alpha_\varepsilon}\, Q_\varepsilon$. We have the same relations with ε replaced by η or $\varepsilon + \eta$.

We write Tr for the trace from $\overline{L}_{10} = L_{10} \otimes_k \overline{k}$ to $\overline{k}$. First by definition and then using Proposition 3.17, the twisted $(2, 2, 2)$-form $\Phi_{\varepsilon,\eta}$ is a scalar multiple of

$$\begin{aligned}\Phi(\psi_\varepsilon\, \mathbf{x}, \psi_\eta\, \mathbf{y}, \psi_{\varepsilon+\eta}^{-T}\, \mathbf{z}) &= \mathrm{Tr}\left((Q \circ \psi_\varepsilon)(\mathbf{x})\, (Q \circ \psi_\eta)(\mathbf{y})\, (Q \circ \psi_{\varepsilon+\eta})^*(\mathbf{z})\right) \\ &= \mathrm{Tr}\left(\sqrt{\alpha_\varepsilon\alpha_\eta/\alpha_{\varepsilon+\eta}}\, Q_\varepsilon(\mathbf{x})\, Q_\eta(\mathbf{y})\, Q^*_{\varepsilon+\eta}(\mathbf{z})\right).\end{aligned}$$

Viewing the trace as a sum over conjugates, this last formula writes $\Phi_{\varepsilon,\eta}$ as a linear combination of 10 $(2, 2, 2)$-forms. It may be checked using Lemma 3.11 that these 10 forms are linearly independent. Since $\Phi_{\varepsilon,\eta}$ is defined over k this forces $\sqrt{\alpha_\varepsilon\alpha_\eta/\alpha_{\varepsilon+\eta}} = s_0\mu$ for some $s_0 \in \overline{k}^\times$ and $\mu \in L_{10}^\times$. Squaring both sides then shows that $s_0^2 \in k$. □

Remark 3.21. Theorem 3.20 is not always sufficient to compute the twisted $(2, 2, 2)$-form since the equation $\alpha_\varepsilon\alpha_\eta/\alpha_{\varepsilon+\eta} = s\mu^2$ does not determine s and μ uniquely. This is not a problem if for example $\mathrm{Gal}(f) = S_6$. In this case L_{10} is a

field, and it has no quadratic subfields. It follows that μ is uniquely determined up to multiplication by an element of $k^\times$. This is sufficient for computing the twisted $(2,2,2)$-form, again up to multiplication by an element of $k^\times$, but as explained in Remark 3.6(ii) this scaling is not important.

In order to handle arbitrary Galois actions on the Weierstrass points it remains to compute μ in a more systematic way. Our answer depends on the scaling of the quadratic forms Q_ε, Q_η and $Q_{\varepsilon+\eta}$, and indeed such a dependence is necessary since in (57) we are free to multiply Q_ε by any element of $\mu_2(L_{10})$ without changing α_ε.

Let W be the set of Weierstrass points, and Γ the set of $(3,3)$-partitions of W. Let $X = \{x \in \mathrm{Map}(W,\mu_2) : \prod_{\theta\in W} x(\theta) = 1\}$. There is a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \mu_2 \arrow[r] \arrow[d, equal] & X \arrow[r] \arrow[d, "\iota"'] & \mathcal{J}[2] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mu_2 \arrow[r] & \mathrm{Map}(\Gamma,\mu_2) \arrow[r] & \mathrm{Map}(\Gamma,\mu_2)/\mu_2 \arrow[r] & 0
\end{tikzcd}$$

where the middle vertical map is given by $\iota(x)(\gamma_1|\gamma_2) = \prod_{\theta\in\gamma_1} x(\theta)$. Taking Galois cohomology gives another commutative diagram with exact rows

$$\begin{tikzcd}
k^\times/(k^\times)^2 \arrow[r] \arrow[d, equal] & H^1(k,X) \arrow[r] \arrow[d, "\iota_*"'] & H^1(k,\mathcal{J}[2]) \arrow[r, "\cup c"] \arrow[d] & \mathrm{Br}(k) \arrow[d, equal] \\
k^\times/(k^\times)^2 \arrow[r] & L_{10}^\times/(L_{10}^\times)^2 \arrow[r] & H^1(k,\mu_2(\overline{L}_{10})/\mu_2) \arrow[r] & \mathrm{Br}(k)
\end{tikzcd} \tag{58}$$

We identify

$$H^1(k,X) \cong \frac{\{(\xi,m) \in L^\times \times k^\times | N_{L/k}(\xi) = m^2\}}{\{(\nu^2, N_{L/k}(\nu)) | \nu \in L^\times\}}.$$

so that the top row (where the first map is now $r \mapsto (r, r^3)$) gives us the isomorphism (23).

Definition 3.22. For $(\xi,m) \in L^\times \times k^\times$ with $N_{L/k}(\xi) = m^2$, let $w(\xi,m) \in L_{10} = \mathrm{Map}_k(\Gamma,\overline{k})$ be given by

$$(\theta_1\theta_2\theta_3|\theta_4\theta_5\theta_6) \mapsto \xi(\theta_1)\xi(\theta_2)\xi(\theta_3) + \xi(\theta_4)\xi(\theta_5)\xi(\theta_6) + 2m$$

and likewise under all permutations of $\theta_1,\dots,\theta_6$.

Lemma 3.23. *The map $\iota_* : H^1(k,X) \to L_{10}^\times/(L_{10}^\times)^2$ sends $(\xi,m) \mapsto w(\xi,m)$, provided that $w(\xi,m)$ is a unit.*

Proof. Let $(\xi,m) \in L^\times \times k^\times$ with $N_{L/k}(\xi) = m^2$, and let $w = w(\xi,m)$. We pick square roots $\sqrt{\xi(\theta)}$ in such a way that $\prod_{\theta\in W}\sqrt{\xi(\theta)} = m$. We can then take $\sqrt{\xi} \in$

$\mathrm{Map}(W,\overline{k}) = L \otimes_k \overline{k}$ to be given by $\theta \mapsto \sqrt{\xi(\theta)}$, and $\sqrt{w} \in \mathrm{Map}(\Gamma,\overline{k}) = L_{10} \otimes_k \overline{k}$ to be given by

$$(\gamma_1|\gamma_2) \mapsto \prod_{\theta\in\gamma_1} \sqrt{\xi(\theta)} + \prod_{\theta\in\gamma_2} \sqrt{\xi(\theta)}$$

We find that $\sigma\sqrt{w}/\sqrt{w} = \iota(\sigma\sqrt{\xi}/\sqrt{\xi})$ for all $\sigma \in \mathrm{Gal}(\overline{k}/k)$, and from this the lemma follows. □

Proposition 3.24. *Let $\varepsilon \in S^{(2)}(\mathcal{J}/k)$ be represented by a model (G,H). Let $\mathbf{G}$ and $\mathbf{H}$ be the 6×6 symmetric matrices corresponding to G and H, and let S be the quadratic form defined by $\mathbf{H}\mathbf{G}^{-1}\mathbf{H}$. Let Z and W be the 4×4 skew symmetric matrices defined in* (19)*, and let Y be the analogue of W where H is replaced by S. Let*

$$A_{ij}(u_0,\dots,u_5) = (W^*ZY^*)_{ij} + (W^*ZY^*)_{ji}.$$

Then the forms Ξ and M in Lemma 2.11 satisfy

$$-f_6 w(\Xi, M) = \alpha_\varepsilon \left(\sum c_{ij}A_{ij}\right)^2 \tag{59}$$

where α_ε and $Q_\varepsilon = \sum c_{ij}x_ix_j$ are as given in Proposition 3.19.

Proof. Since $P_\varepsilon \in L_{10}[x_1,\dots,x_4]$ is a quartic form, we may write

$$P_\varepsilon(x_1,\dots,x_4) = \widetilde{P}_\varepsilon(x_1^2, x_1x_2, \dots, x_4^2)$$

where $\widetilde{P}_\varepsilon$ is a quadratic form in 10 variables. This does not determine $\widetilde{P}_\varepsilon$ uniquely, but in view of (57) there is a canonical choice, namely the one for which the associated symmetric bilinear form sends

$$(x_1^2, x_1x_2, \dots, x_4^2; y_1^2, y_1y_2, \dots, y_4^2) \mapsto \alpha_\varepsilon Q_\varepsilon(x_1,\dots,x_4)Q_\varepsilon(y_1,\dots,y_4).$$

The proof of (59) is now reduced to showing that

$$-f_6 w(\Xi, M) = \widetilde{P}_\varepsilon(A_{11}, A_{12}, \dots, A_{44}).$$

Each side is a form of degree 6 in $u_0,\dots,u_5$ whose coefficients have degree 15 in the coefficients h_{ij} of the model. We checked this by computer algebra for the model (G,H) in Section 2.2. The general case follows by carefully keeping track of the effect of a change of coordinates. □

We solve for s and μ in Theorem 3.20 as follows. First we pick $(\xi_\varepsilon, m_\varepsilon)$ by specialising the forms (Ξ, M) in Lemma 2.11. Specialising (59) at the same point gives $-f_6 w(\xi_\varepsilon, m_\varepsilon) = \alpha_\varepsilon\chi_\varepsilon^2$ for some explicit $\chi_\varepsilon \in L_{10}$, which is a unit if we specialised at a sufficiently general point. We repeat everything with ε replaced by η or $\varepsilon+\eta$. By (23) we have

$$(\xi_\varepsilon\xi_\eta\xi_{\varepsilon+\eta}, m_\varepsilon m_\eta m_{\varepsilon+\eta}) = (r\nu^2, r^3 N_{L/k}(\nu)), \tag{60}$$

for some $r \in k^\times$ and $\nu \in L^\times$. We then use the next lemma to solve for s and μ satisfying $\alpha_\varepsilon \alpha_\eta / \alpha_{\varepsilon+\eta} = s\mu^2$.

Lemma 3.25. *Let $(\xi_i, m_i) \in L^\times \times k^\times$ with $N_{L/k}(\xi_i) = m_i^2$ for $i = 1, 2, 3$. If*

$$(\xi_1\xi_2\xi_3, m_1m_2m_3) = (r\nu^2, r^3 N_{L/k}(\nu))$$

then

$$\prod_{i=1}^{3} w(\xi_i, m_i) = s\mu^2$$

for some $s \in k$ and $\mu \in L_{10}$. Moreover we may take $s = r^3$ and

$$\mu(\gamma_1|\gamma_2) = \left(\prod_{\theta\in\gamma_1} \nu(\theta)\right) \prod_{i=1}^{3} \left(1 + \frac{m_i}{\prod_{\theta\in\gamma_1} \xi_i(\theta)}\right). \tag{61}$$

Proof. If the $w(\xi_i, m_i)$ are units, then the existence of s and μ follows from Lemma 3.23 and the commutative diagram (58). To prove the result in general and to give explicit formulae we proceed as follows. By Definition 3.22 we have

$$w(\xi_i, m_i)(\gamma_1|\gamma_2) = \left(\prod_{\theta\in\gamma_1} \xi_i(\theta)\right) \left(1 + \frac{m_i}{\prod_{\theta\in\gamma_1} \xi_i(\theta)}\right)^2.$$

It follows that $\prod_{i=1}^{3} w(\xi_i, m_i) = s\mu^2$ where s and μ are as given in the statement of the lemma. A calculation then shows that (61) is unchanged when we swap $\gamma_1 \leftrightarrow \gamma_2$ and so defines an element of L_{10}. □

We have now reduced the problem of solving for s and μ in Theorem 3.20 to that of solving for r and ν in (60). This still does not have a unique solution, but our choices for ν are more limited than they were for μ. Indeed ν is unique up to multiplying by elements of $k^\times$ (which do not matter) and elements of

$$\frac{\{\nu \in L^\times | \nu^2 \in k^\times, N_{L/k}(\nu) = \nu^6\}}{k^\times} \cong \mathcal{J}[2](k).$$

This leaves us with $\#\mathcal{J}[2](k)$ choices. Since this is the same as the number of choices we had in defining the twisted group law (see Remark 3.8), and so in defining the twisted $(2, 2, 2)$-form, all of these choices work.

4. Implementation and Examples

Let $\mathcal{C}$ be a genus 2 curve defined over a number field k, and let $\mathcal{J}$ be its Jacobian. We have written a program in Magma [BCP] for computing the Cassels-Tate pairing

$$\langle\ ,\ \rangle_{\mathrm{CT}} : S^{(2)}(\mathcal{J}/k) \times S^{(2)}(\mathcal{J}/k) \to \mathbb{F}_2$$

in the case $k = \mathbb{Q}$. We have also worked out some first examples when k is a small quadratic field. The main steps are as follows.

(i) We compute the fake 2-Selmer group $S^{(2)}_{\mathrm{fake}}(\mathcal{J}/k)$ using the Magma function `TwoSelmerGroup`. This calls programs of Stoll (when $k = \mathbb{Q}$) and Bruin (when $k \neq \mathbb{Q}$). Our insistence that $\mathcal{C}$ has an equation $y^2 = f(x)$ where f has degree 6 can slow these programs down, so in the presence of a rational Weierstrass point it may be better to work with a degree 5 model and then convert the fake 2-Selmer group elements back to a degree 6 model.

(ii) We compute the 2-Selmer group $S^{(2)}(\mathcal{J}/k)$ from the fake Selmer group, representing its elements as pairs (ξ, m) where $N_{L/k}(\xi) = m^2$ as in (23). Although this is simply a matter of extracting square roots of the norms, we must be careful to keep track of the group structure.

(iii) We convert each 2-Selmer group element (ξ, m) to a model (G, H) as described in Section 2.4. This involves solving for a 3-dimensional isotropic subspace of a quadratic form in 6 variables. When $k = \mathbb{Q}$ we use the existing function `IsotropicSubspace` in Magma [BCP]. This uses techniques of minimisation and reduction based on a paper of Simon [Si]. When k is a small quadratic field we find that similar ideas work reasonably well in practice.

(iv) We use the action of $\mathrm{PGL}_4(k)$ on the space of models to simplify our list of models. This is achieved by a combination of minimisation and reduction. The algorithm we used for minimisation is described in joint work of the first author and Mengzhen (August) Liu [FL]. See Remark 4.3 below for details of the method we used for reduction.

(v) We select elements $\varepsilon, \eta \in S^{(2)}(\mathcal{J}/k)$ and aim to compute $\langle \varepsilon, \eta \rangle_{\mathrm{CT}}$. If the value of the pairing can be inferred from earlier values computed, or from the properties of the pairing listed at the start of Section 3 (specifically, it is symmetric, bilinear and satisfies Lemma 3.1), then there is no need for the following steps (other than for testing purposes). The deficient places may be computed using the algorithm in [S2, Section 7], as implemented in the Magma function `IsDeficient`.

(vi) Starting from our models representing ε, η and $\varepsilon+\eta$ we use (18) to compute equations for the twisted Kummer surfaces $\mathcal{K}_\varepsilon$, $\mathcal{K}_\eta$ and $\mathcal{K}_{\varepsilon+\eta}$. As described in Section 2.6, computing 2×2 minors instead of 3×3 minors (and scaling by $-f_6$) gives us pushout forms for $\mathcal{K}_\varepsilon$ and $\mathcal{K}_\eta$, i.e., quartic forms that when set equal to a square define the double covers $\mathcal{J}_\varepsilon \to \mathcal{K}_\varepsilon$ and $\mathcal{J}_\eta \to \mathcal{K}_\eta$. Since we need them in Step (viii) below, we also compute the covariants describing the covering maps $\mathcal{K}_\varepsilon \to \mathcal{K}$, $\mathcal{K}_\eta \to \mathcal{K}$ and $\mathcal{K}_{\varepsilon+\eta} \to \mathcal{K}$.

(vii) We search for k-points on $\mathcal{K}_\eta \subset \mathbb{P}^3$. When $k = \mathbb{Q}$ we use the function `PointSearch` in Magma, slightly modified to allow for the fact that Kummer surfaces are always singular. When $k \neq \mathbb{Q}$ we took an ad hoc approach (intersecting with random lines) which could doubtless be improved.

(viii) Assuming we found a rational point $P \in \mathcal{K}_\eta(k)$, we compute $a \in k^\times/(k^\times)^2$ by evaluating the pushout form describing $\mathcal{J}_\eta \to \mathcal{K}_\eta$ at this point P. We then compute the rational function g on $\mathcal{K}_\varepsilon$ using Theorems 3.9 and 3.20. There is no need to compute the $(2,2,2)$-form in full, since we immediately specialise the second and third sets of variables. These are specialised to the coordinates of $P \in \mathcal{K}_\eta \subset \mathbb{P}^3$ and an arbitrary point on $(\mathbb{P}^3)^\vee$. For the latter we take $(c_1, c_2, c_3, c_4) = (1, 0, 0, 0)$.

(ix) We compute $\langle \varepsilon, \eta \rangle_{\mathrm{CT}}$ using Theorem 3.5(iii). We are careful to pick local points on $\mathcal{K}_\varepsilon$ that lift to local points on $\mathcal{J}_\varepsilon$. The sum over all places is reduced to a finite sum as explained in Section 4.1 below.

(x) We repeat Steps (v) to (ix) until we have computed the matrix of the Cassels-Tate pairing $\langle\ ,\ \rangle_{\mathrm{CT}}$ relative to a basis for $S^{(2)}(\mathcal{J}/k)$ as an $\mathbb{F}_2$-vector space.

Remark 4.1. For our methods to work, we do not need to find rational points on all of the twisted Kummer surfaces. Accordingly, in Step (vii) we use a relatively small search bound, and only return to search again if we do not succeed with other choices of η. For this reason it is recommended to give our program the full 2-Selmer group as input, and not some subgroup or just a pair of elements.

Remark 4.2. The main obstacles to generalising to number fields of larger degree are the need to carry out minimisation and reduction in Steps (iii) and (iv), and the point search in Step (vii). We found it particularly helpful if the ring of integers of k is a Euclidean domain since then our code for minimisation over $\mathbb{Q}$ (which calls the Magma function `SmithForm`) could be adapted relatively easily.

Remark 4.3. For simplicity we take $k = \mathbb{Q}$. In the reduction part of Step (iv) we are looking for a matrix in $\mathrm{GL}_4(\mathbb{Z})$ representing a change of coordinates that simplifies our equation for the twisted Kummer surface $\mathcal{K}_\varepsilon \subset \mathbb{P}^3$. The same matrix, acting as described in Definition 2.7(ii), may then be used to simplify the model (G, H). To find this matrix in $\mathrm{GL}_4(\mathbb{Z})$ we use the natural generalisation of [CFS, Corollary 6.3], namely we embed $\overline{\mathbb{Q}} \subset \mathbb{C}$ and perform lattice reduction with respect to the Gram matrix

$$\sum_{T \in \mathcal{J}[2]} \frac{M_T^\dagger M_T}{|\det M_T|^{1/2}}$$

where the matrices M_T were computed in Remark 2.12, and the superscript $\dagger$ denotes complex conjugate transpose. An alternative method would be to run Magma's `ReduceCluster` on the set of nodes of $\mathcal{K}_\varepsilon$, but the need to numerically solve for the nodes makes this method less efficient.

Both of these methods are specific to curves of genus 2. A method that works for 2-coverings of hyperelliptic Jacobians in general is currently being developed by Jack Thorne [T2].

Presented with the output of a long and complicated program, it is natural to wonder whether the answers computed are correct. We used the methods in Section 2.5 to check that the models computed in Step (iii) do indeed correspond to the Selmer elements claimed. For computing the pairing itself, we used all of the following checks. The first was the most important for catching bugs.

- In applying Theorem 3.5(iii) we may compute many k_v-points on $\mathcal{K}_\varepsilon$ and check that each makes the same local contribution to the pairing.
- In Step (viii) we may make different choices of P, of $(c_1, \ldots, c_4)$, and of the overall scaling of g, and check that the pairing does not change.
- We may check that the pairing as computed is symmetric, bilinear and satisfies Lemma 3.1.
- We may check that the image of the map $\mathcal{J}(k)/2\mathcal{J}(k) \to S^{(2)}(\mathcal{J}/k)$ is contained in the kernel of the pairing.
- We may check that our answers are consistent with Remark 3.2.

In Section 4.1 we explain how the sum over all places in our formula for the pairing reduces to a finite sum. In Section 4.2 we give some examples over $k = \mathbb{Q}$ where our methods improve the upper bound for the rank of $\mathcal{J}(\mathbb{Q})$ coming from 2-descent by 2 or more. In Section 4.3 we explain how our methods compare to the visibility method employed by Bruin and Stoll, and how the methods can be combined. Finally in Section 4.4 we explain how we used our methods to unconditionally determine the rank of every genus 2 Jacobian in the LMFDB.

4.1. **Controlling the bad primes.** We work over a number field k with ring of integers $\mathcal{O}_k$. Let $\mathcal{C}$ be a genus 2 curve with equation $y^2 = f(x) = f_6x^6 + f_5x^5 + \ldots + f_1x + f_0$ where the f_i are in $\mathcal{O}_k$. Let S_0 be a finite set of places of k containing all the infinite places and all the primes dividing $2f_6 \operatorname{disc}(f)$.

Theorem 4.4. *Let $v \notin S_0$ be a place of k. Suppose that*

(i) *$\mathcal{K}_\varepsilon$ arises from a model (G, H) (see Definition 2.7) and H has v-adically integral coefficients.*
(ii) *$a \in k^\times$ is a v-adic unit.*
(iii) *$g = \gamma(x_1, \ldots, x_4)/x_1^2$ where $\gamma \in k[x_1, \ldots, x_4]$ is a quadratic form, with all coefficients v-adically integral and at least one a v-adic unit.*

Then the local contribution at v in Theorem 3.5(iii) is trivial.

Proof. Replacing the local field k_v by an unramified extension of odd degree we may assume that the order of the residue field (q say) is arbitrarily large. Under the assumptions in the statement of the theorem, the construction of $\mathcal{K}_\varepsilon \subset \mathbb{P}^3$ and

the double cover $\mathcal{J}_\varepsilon \to \mathcal{K}_\varepsilon$ from the model (G, H) carries over to the residue field. By the Lang-Weil estimates there are $\Omega(q^2)$ smooth points on the reduction of $\mathcal{K}_\varepsilon$ mod v that lift to $\mathbb{F}_q$-points on the reduction of $\mathcal{J}_\varepsilon$ mod v. The reduction of γ mod v cannot be identically zero on the surface (it is a quadratic form, whereas the surface has degree 4) and so vanishes at $O(q)$ of these points. Since q is large there are some points left over. Hensel lifting any one of these (and noting that for $v \nmid 2\infty$ the Hilbert symbol of two v-adic units is trivial) shows that the local contribution at v is trivial. □

4.2. **First examples over $\mathbb{Q}$.** Our first example was chosen as a genus 2 curve with equation $y^2 = f(x)$ where f has small integer coefficients and Galois group S_6, and a 2-descent does not appear to give a sharp upper bound for the rank of the Jacobian.

Example 4.5. Let $\mathcal{C}$ be the genus 2 curve with equation

$$y^2 = -3x^6 + 3x - 15.$$

Let $L = \mathbb{Q}[\theta] = \mathbb{Q}[x]/(x^6 - x + 5)$. We represent elements of the 2-Selmer group $S^{(2)}(\mathcal{J}/\mathbb{Q})$ as pairs $(\xi, m) \in L^\times \times \mathbb{Q}^\times$ where $N_{L/\mathbb{Q}}(\xi) = m^2$. Magma computes that $S^{(2)}(\mathcal{J}/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^3$ is generated by

$$\begin{aligned} c &= (1, -1), \\ \varepsilon &= (\theta^5 - 3\theta^4 - 2\theta^3 + 5\theta^2 + 4\theta - 9, 1), \\ \eta &= (\theta^5 - 2\theta^4 + 2\theta^3 - \theta^2 + 1, 1). \end{aligned}$$

We find that the Selmer group elements ε, η, $\varepsilon + \eta$ are represented by models $(G, \frac{1}{2}H_1)$, $(G, \frac{1}{2}H_2)$, $(G, \frac{1}{2}H_3)$ where $G = u_0u_5 + u_1u_4 + u_2u_3$ and

$$\begin{aligned} H_1 &= u_0u_1 - 2u_0u_2 - u_1u_2 + u_1u_3 - 2u_1u_5 - 2u_2u_5 - 2u_3u_4 - 2u_4u_5 + 2u_5^2, \\ H_2 &= u_0u_2 - 2u_0u_3 - 2u_1^2 - u_1u_2 + u_2^2 - u_2u_4 + 3u_2u_5 + 2u_3^2 + 2u_3u_5 - 4u_4u_5, \\ H_3 &= -2u_0u_3 + u_1u_2 + u_1u_4 - 2u_1u_5 - u_2u_3 + 2u_2u_4 - u_3u_4 + 4u_4u_5 + 2u_5^2. \end{aligned}$$

The identity element is represented by (G, H) as given in Section 2.2, and the remaining four elements of $S^{(2)}(\mathcal{J}/\mathbb{Q})$ are given by reversing the order of the variables $u_0, u_1, \ldots, u_5$. (As noted in Remark 2.10 this corresponds to adding c.) It may be checked using the formulae in Section 2.5 that these models do indeed correspond to the pairs (ξ, m) we started with.

The procedure in Section 2.6 shows that $\mathcal{K}_\varepsilon \subset \mathbb{P}^3$ has equation $F_\varepsilon = 0$ where

$$\begin{aligned} F_\varepsilon = {} & 2x_1^3x_2 + 4x_1^3x_3 + 4x_1^3x_4 - 18x_1^2x_2^2 + 22x_1^2x_2x_3 + 2x_1^2x_2x_4 - 8x_1^2x_3^2 \\ & - 4x_1^2x_3x_4 - 2x_1^2x_4^2 + 6x_1x_2^3 + 6x_1x_2^2x_3 + 7x_1x_2^2x_4 - 6x_1x_2x_3^2 \\ & - 24x_1x_2x_3x_4 - 6x_1x_2x_4^2 + 4x_1x_3^3 + 6x_1x_4^3 - x_2^4 + 3x_2^3x_3 + 3x_2^3x_4 \\ & - 3x_2^2x_3x_4 - 5x_2^2x_4^2 + 2x_2x_3^3 - 2x_2x_3^2x_4 + 2x_2x_4^3 - 2x_3^2x_4^2 + 2x_3x_4^3 + x_4^4. \end{aligned}$$

We likewise find equations for $\mathcal{K}_\eta \subset \mathbb{P}^3$ and $\mathcal{K}_{\varepsilon+\eta} \subset \mathbb{P}^3$. On $\mathcal{K}_\eta$ we find the rational point $P = (1 : 0 : -1 : -1)$ whose inverse image in $\mathcal{J}_\eta$ is defined over $\mathbb{Q}(\sqrt{-3})$. Since $\mathrm{Gal}(f) = S_6$, computing the twisted $(2,2,2)$-form is simplified as described in Remark 3.21. Taking $(c_1, c_2, c_3, c_4) = (1, 0, 0, 0)$ in Theorem 3.9 we find that $g = \gamma(x_1, \ldots, x_4)/x_1^2$ where $\gamma = 12x_1x_2 - 2x_2^2 + 6x_2x_3 + 3x_2x_4$. According to Theorem 3.5 the Cassels-Tate pairing is given by

$$\langle \varepsilon, \eta \rangle_{\mathrm{CT}} = \sum_v (-3, \gamma(P_v))_v$$

where for each place v of $\mathbb{Q}$ we choose a local point $P_v \in \mathcal{K}_\varepsilon(\mathbb{Q}_v)$ that lifts to $\mathcal{J}_\varepsilon(\mathbb{Q}_v)$ and satisfies $\gamma(P_v) \neq 0$. As before, our convention is that the Hilbert symbol $(\ ,\ )_v$ takes values in $\mathbb{F}_2$.

By Theorem 4.4 the only places that could contribute to the pairing are the primes dividing the discriminant $-2^8 \cdot 3^{10} \cdot 5^6 \cdot 7 \cdot 31 \cdot 43$, together with ∞. For each of these places v we specify a local point $P_v \in \mathcal{K}_\varepsilon(\mathbb{Q}_v)$ whose first three coordinates are exact, and whose last coordinate is either exact or given to sufficient precision to determine the point uniquely. It is important to note that we have chosen local points that lift to $\mathcal{J}_\varepsilon(\mathbb{Q}_v)$. The third column lists $\gamma(P_v)$ as an element of $\mathbb{Q}_v^\times/(\mathbb{Q}_v^\times)^2$.

place v	local point P_v on $\mathcal{K}_\varepsilon$	$\gamma(P_v)$	$(-3, \gamma(P_v))_v$
2	$(3 : 4 : 1 : 2^2 + O(2^3))$	-2	1
3	$(1 : -1 : 0 : -3^2 + O(3^3))$	1	0
5	$(0 : 1 : 1 : 1)$	2	0
7	$(0 : 1 : 0 : 1)$	1	0
31	$(0 : 1 : 0 : 1)$	1	0
43	$(0 : 1 : 0 : 1)$	1	0
∞	$(0 : 1 : 1 : 1)$	1	0

Adding up the entries in the right hand column shows that $\langle \varepsilon, \eta \rangle_{\mathrm{CT}} \neq 0$.

Since $\mathcal{C}$ has an even number of deficient places (these are 3 and ∞) we know by Lemma 3.1 that the Cassels-Tate pairing on $S^{(2)}(\mathcal{J}/\mathbb{Q})$ has even rank. Since we have shown that this pairing is non-zero, this improves the upper bound $\operatorname{rank}\mathcal{J}(\mathbb{Q}) \leqslant 3$ coming from 2-descent to $\operatorname{rank}\mathcal{J}(\mathbb{Q}) \leqslant 1$.

Further calculations show that the pairing is given by

$\langle\ ,\ \rangle_{\mathrm{CT}}$	c	ε	η
c	0	1	1
ε	1	1	1
η	1	1	1

Since the kernel of the pairing is 1-dimensional, spanned by $\varepsilon+\eta$, this suggests we should look for rational points on $\mathcal{J}_{\varepsilon+\eta}$. We find that the point $(1:-2:-2:0)$ on $\mathcal{K}_{\varepsilon+\eta}$ lifts to a $\mathbb{Q}$-point on $\mathcal{J}_{\varepsilon+\eta}$. Using the formulae for the covering map in Section 2.6, this point maps to the point $(124:238:199:3607)$ on $\mathcal{K}$, which in turn lifts to a point of infinite order in $\mathcal{J}(\mathbb{Q})$, represented by a pair of points on $\mathcal{C}$ with x-coordinates satisfying $124x^2-238x+199=0$. It follows that $\operatorname{rank}\mathcal{J}(\mathbb{Q})=1$ and $Ш(\mathcal{J}/\mathbb{Q})[2]\cong(\mathbb{Z}/2\mathbb{Z})^2$. Our calculations further show that the Cassels-Tate pairing on $Ш(\mathcal{J}/\mathbb{Q})[2]$ is non-degenerate, and hence $Ш(\mathcal{J}/\mathbb{Q})[2^\infty]\cong(\mathbb{Z}/2\mathbb{Z})^2$.

Next we give an example where the rank of $\mathcal{J}(\mathbb{Q})$ had previously only been computed conditional on the Birch Swinnerton-Dyer conjecture. We discuss further such examples in Sections 4.3 and 4.4.

Example 4.6. Let $\mathcal{C}$ be the genus 2 curve with equation

$$y^2=-3x^6-4x^5-10x^4-51x^2+80x-28,$$

and LMFDB label `49471.a.49471.1`. Since the right hand side factors as the product of two cubics, the canonical element of the 2-Selmer group is trivial. It follows by Lemma 3.1 that the Cassels-Tate pairing on $S^{(2)}(\mathcal{J}/\mathbb{Q})\cong(\mathbb{Z}/2\mathbb{Z})^2$ is alternating. A calculation similar to that in the previous example shows that the pairing is non-zero. Therefore $\operatorname{rank}\mathcal{J}(\mathbb{Q})=0$ and $Ш(\mathcal{J}/\mathbb{Q})[2^\infty]\cong(\mathbb{Z}/2\mathbb{Z})^2$.

Our next example is taken from a paper of Logan and van Luijk [LvL].

Example 4.7. Let $\mathcal{C}$ be the genus 2 curve with equation

$$y^2=-6(x^2+1)(x^2-2x-1)(x^2+x-1).$$

We have $\mathcal{J}(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$. We find that $S^{(2)}(\mathcal{J}/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^4$ is generated by

$$\begin{aligned} c &= (1, -1), \\ \varepsilon &= (\theta^4 - \theta^3 - \theta^2 - 2\theta - 2, 18), \\ \eta &= (5\theta^3 - 14\theta^2 + 1, 900), \\ \nu &= (\theta^4 + \theta^3 + 5\theta^2 - 3, 270), \end{aligned}$$

and the Cassels-Tate pairing on $S^{(2)}(\mathcal{J}/\mathbb{Q})$ is given by

$\langle\ ,\ \rangle_{\mathrm{CT}}$	c	ε	η	ν
c	0	1	0	0
ε	1	1	0	0
η	0	0	0	0
ν	0	0	0	0

It follows that $\operatorname{rank} \mathcal{J}(\mathbb{Q}) = 0$ and $Ш(\mathcal{J}/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^2$.

We were able to compute the pairing in this example despite the result of Logan and van Luijk [LvL, Proposition 3.33] that $\mathcal{K}_\varepsilon(\mathbb{Q}) = \emptyset$. This illustrates the point we made in Remark 4.1. In fact, in this example we find that of the 15 twisted Kummer surfaces (associated to the non-zero elements of $S^{(2)}(\mathcal{J}/\mathbb{Q})$) all except $\mathcal{K}_\varepsilon$ and $\mathcal{K}_{\varepsilon+c} \cong (\mathcal{K}_\varepsilon)^\vee$ have rational points of small height.

We end this section with an example where the pairing has higher rank.

Example 4.8. Let $\mathcal{C}$ be the genus 2 curve with equation

$$y^2 = f(x) = 3x^6 + 10x^5 - 16x^4 + 18x^3 + 23x^2 - 54x - 17.$$

We have $\mathrm{Gal}(f) = S_6$ and so the Jacobian $\mathcal{J}$ has no rational 2-torsion. We find that $S^{(2)}(\mathcal{J}/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^5$ is generated by

$$\begin{aligned} c &= (1, -1), \\ \varepsilon &= (3\theta^2 - 8\theta + 10, 2041), \\ \eta &= (2\theta^2 - 4\theta + 15, 16657/3), \\ \nu &= (6\theta^3 + 14\theta^2 - 16\theta - 31, 37503), \\ \phi &= (2\theta^4 + 9\theta^3 - 3\theta^2 - 5\theta + 1, 2925), \end{aligned}$$

and the Cassels-Tate pairing on $S^{(2)}(\mathcal{J}/\mathbb{Q})$ is given by the rank 3 matrix

$\langle\ ,\ \rangle_{\mathrm{CT}}$	c	ε	η	ν	ϕ
c	1	0	0	0	1
ε	0	0	1	1	0
η	0	1	0	0	1
ν	0	1	0	0	1
ϕ	1	0	1	1	1

The points $(11 : -98 : 78 : -2217)$ and $(44 : 72 : 124 : -245)$ on the Kummer surface $\mathcal{K}$ lift to independent points of infinite order in $\mathcal{J}(\mathbb{Q})$. It follows that $\operatorname{rank} \mathcal{J}(\mathbb{Q}) = 2$ and $Ш(\mathcal{J}/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^3$.

4.3. **Examples from an experiment of Bruin and Stoll.** Bruin and Stoll conducted an experiment [BS] where they attempted to determine the existence of rational points on all genus 2 curves $y^2 = f_6x^6 + f_5x^5 + \ldots + f_1x + f_0$ where the f_i are integers with $|f_i| \leqslant 3$. They reduced this to the determination of the ranks of 47 genus 2 Jacobians, of which 36 are expected to have rank 0, a further 10 are expected to have rank 1, and one is expected to have rank 2.

We start by considering one of the cases where the rank is expected to be 1.

Example 4.9. Let $\mathcal{C}$ be the genus 2 curve with equation

$$y^2 = -x^6 + 2x^5 + 3x^4 + 2x^3 - x - 3.$$

Magma computes that $S^{(2)}(\mathcal{J}/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^3$ is generated by

$$\begin{aligned} c &= (1, -1), \\ \varepsilon &= (\theta^2 + \theta + 1, 4), \\ \eta &= (\theta^3 - 4\theta^2 + 3\theta - 1, 8). \end{aligned}$$

We find that the Selmer group elements ε, η, $\varepsilon + \eta$ are represented by the models $(G, \frac{1}{2}H_1)$, $(G, \frac{1}{2}H_2)$, $(G, \frac{1}{2}H_3)$, where $G = u_0u_5 + u_1u_4 + u_2u_3$ and

$$\begin{aligned} H_1 &= u_0u_2 - u_0u_4 + 2u_1u_3 - 2u_1u_5 + 2u_2^2 + 2u_2u_3 + 4u_3^2 - 10u_3u_5 - 2u_4u_5, \\ H_2 &= 2u_0^2 + 2u_0u_1 + 2u_0u_4 + 4u_1u_5 + 2u_2^2 + 2u_2u_3 + 4u_2u_5 - u_3u_4 + 3u_3u_5, \\ H_3 &= u_0u_4 + 2u_1u_2 - 2u_1u_3 + 4u_1u_4 - 2u_2u_3 + 8u_3u_5 - u_4^2 - 6u_4u_5 - 2u_5^2. \end{aligned}$$

Using these models we compute that the Cassels-Tate pairing is given by

$\langle\ ,\ \rangle_{\mathrm{CT}}$	c	ε	η
c	0	0	0
ε	0	0	1
η	0	1	0

Since the point $(9536 : -5312 : 5008 : 53113)$ on $\mathcal{K}$ lifts to a point of infinite order in $\mathcal{J}(\mathbb{Q})$ it follows that $\operatorname{rank}\mathcal{J}(\mathbb{Q}) = 1$.

Remark 4.10. Let d be a squarefree integer. We write $\mathcal{C}_d$ for the quadratic twist of $\mathcal{C}$ by d, and $\mathcal{J}_d$ for its Jacobian. It is well known that

$$\operatorname{rank}\mathcal{J}(\mathbb{Q}(\sqrt{d})) = \operatorname{rank}\mathcal{J}(\mathbb{Q}) + \operatorname{rank}\mathcal{J}_d(\mathbb{Q}). \tag{62}$$

Bruin (see [BF], [BS]) observed that the upper bound for the rank of $\mathcal{J}(\mathbb{Q})$ coming from 2-descent can sometimes be improved by carrying out a 2-descent over $\mathbb{Q}(\sqrt{d})$. Indeed, this gives an upper bound for the rank of $\mathcal{J}(\mathbb{Q}(\sqrt{d}))$ which, when combined with (62) and a lower bound for the rank of $\mathcal{J}_d(\mathbb{Q})$, gives an upper bound for the rank of $\mathcal{J}(\mathbb{Q})$. When this method succeeds it is because there are elements in $Ш(\mathcal{J}/\mathbb{Q})[2]$ that are in the kernel of the restriction map

$$Ш(\mathcal{J}/\mathbb{Q}) \to Ш(\mathcal{J}/\mathbb{Q}(\sqrt{d})).$$

One way to think about this kernel is as the elements of $Ш(\mathcal{J}/\mathbb{Q})$ that are visible (in the sense defined by Mazur) in the restriction of scalars of $\mathcal{J}$. Accordingly Bruin calls his method *visibility*.

Bruin and Stoll [BS] were already able to show that $\operatorname{rank}\mathcal{J}(\mathbb{Q}) = 1$ in Example 4.9 by taking $d = -1$ in Remark 4.10. In fact this is just one of 5 curves on their list for which the same thing happens, that is, by computing the Cassels-Tate pairing we are able to prove that $\operatorname{rank}\mathcal{J}(\mathbb{Q}) = 1$, but Bruin and Stoll already proved this using visibility. Likewise the conclusion $\operatorname{rank}\mathcal{J}(\mathbb{Q}) = 1$ in Example 4.5 can be proved by taking $d = -3$ in Remark 4.10. However our method has the advantage that we only had to carry out a 2-descent over $\mathbb{Q}$ instead of $\mathbb{Q}(\sqrt{d})$, and so only had to verify a class group calculation in a degree 6 rather than a degree 12 number field.

In the remaining 42 examples we find that the Cassels-Tate pairing on $S^{(2)}(\mathcal{J}/\mathbb{Q})$ is identically zero. This is consistent with the calculations of Bruin and Stoll, who showed in each case that $Ш(\mathcal{J}/\mathbb{Q})$ has analytic order (approximately) 16, and so is expected to be isomorphic to $(\mathbb{Z}/4\mathbb{Z})^2$. Visibility was not sufficient for Bruin and Stoll to compute the ranks in these cases, except in 4 cases where they obtained results conditional on GRH. However by combining visibility with computing the

Cassels-Tate pairing over a quadratic field $\mathbb{Q}(\sqrt{d})$, we are able to prove that in all but 4 of the 42 examples the Jacobian does have the expected rank. For this we took $d \in \{-1, \pm 2, \pm 3, 5, -7\}$. In the unresolved cases[4] the expected rank is 0, and the problem is the apparent lack of a suitable small d.

We give further details for the final curve on their list.

Example 4.11. Let $\mathcal{C}$ be the genus 2 curve

$$y^2 = f(x) = 3x^6 + 3x^5 + x^4 - 3x^3 - 3x^2 + x - 3.$$

Since $\mathrm{Gal}(f) = S_6$ there are no 2-torsion points on $\mathcal{J} = \mathrm{Jac}(\mathcal{C})$, even over a quadratic extension. It is easy to find two independent $\mathbb{Q}$-points of infinite order on both $\mathcal{J}$ and its quadratic twist by -3. Let $k = \mathbb{Q}(\zeta)$ where $\zeta = (-1+\sqrt{-3})/2$. Magma computes[5] that $S^{(2)}(\mathcal{J}/k) \cong (\mathbb{Z}/2\mathbb{Z})^6$ is generated by

$$\begin{aligned}
\alpha_1 &= (1, -1),\\
\alpha_2 &= (\theta^2 + \theta, 1),\\
\alpha_3 &= (3\theta^4 - 3\theta^2 + 1, 169/3),\\
\alpha_4 &= (3\theta^5 + 3\theta^4 + \theta^3 + 3\theta^2 + 1, 9),\\
\varepsilon &= (3(1+\zeta)\theta^4 - 10\theta^2 - 8\zeta\theta - 5 - 2\zeta, -1543 - 2462\zeta),\\
\eta &= (3(2+\zeta)\theta^3 - 2(2+\zeta)\theta, -171),
\end{aligned}$$

where as usual θ is a root of f. In fact $S^{(2)}(\mathcal{J}/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^4$ is generated by $\alpha_1, \ldots, \alpha_4$, but the Cassels-Tate pairing on this Selmer group is trivial. We represent the Selmer group elements ε, η, $\varepsilon + \eta$ by the models $(G, \lambda^{-1}H_1)$, $(G, \lambda^{-1}H_2)$, $(G, \lambda^{-1}H_3)$ where $G = u_0u_5 + u_1u_4 + u_2u_3$, $\lambda = 4(1-\zeta)$ and

$$\begin{aligned}
H_1 &= (2+\zeta)u_0^2 - 2(1-\zeta)u_0u_4 - 2(1-\zeta)u_0u_5 + 2u_1^2 - 4u_1u_3 + 5(1+2\zeta)u_2^2\\
&\quad + 6(3+2\zeta)u_2u_4 + 4(7+8\zeta)u_2u_5 - 2u_3^2 + 8u_3u_4 + 2u_4^2 + 18u_4u_5 + (29+16\zeta)u_5^2,\\
H_2 &= 2u_0u_2 + 2(1-\zeta)u_0u_3 - \zeta u_1^2 - 2(1-\zeta)u_1u_4 - 4u_2^2 + 4u_2u_4 + 8u_2u_5\\
&\quad - 4(1-\zeta)u_3u_4 - 8(1-\zeta)u_3u_5 - u_4^2 + 8(1+3\zeta)u_4u_5 - 16u_5^2,\\
H_3 &= 4u_0^2 + 8u_0u_1 + 4u_0u_2 - 4\zeta u_0u_3 - 8\zeta u_0u_4 + (3-\zeta)u_1^2 + 4(1+\zeta)u_1u_2\\
&\quad - 2(1-\zeta)u_1u_4 + 2\zeta u_2^2 + 2(1+2\zeta)u_2u_5 - 2(1-2\zeta)u_3^2 - 4u_3u_4 + 2(2+\zeta)u_3u_5\\
&\quad - (1-3\zeta)u_4^2.
\end{aligned}$$

On $\mathcal{K}_\eta$ we find the point $(\zeta : 1 : 2+2\zeta : 2-4\zeta)$. This lifts to a point on $\mathcal{J}_\eta$ defined over $k(\sqrt{a})$ where $a = 7 + 4\zeta$. Using Theorem 3.9 with $(c_1, \ldots, c_4) = (1, 0, 0, 0)$

[4]These were numbers 2, 21, 23, 33 on Bruin and Stoll's list. In particular we were able to resolve the 22nd curve on their list, making the main result of [FJ] unconditional.

[5]This takes a few seconds assuming GRH, and still less than 10 minutes without.

we compute that $g = \gamma(x_1, \ldots, x_4)/x_1^2$ where

$$\begin{aligned}\gamma = &-(233+446\zeta)x_1^2 - (276-308\zeta)x_1x_2 + (178-316\zeta)x_1x_3 \\ &+ (118+260\zeta)x_1x_4 + (228-196\zeta)x_2^2 - (4+188\zeta)x_2x_3 \\ &+ (84-300\zeta)x_2x_4 + (227+34\zeta)x_3^2 - (6-36\zeta)x_3x_4 - (17+82\zeta)x_4^2.\end{aligned}$$

According to Theorem 3.5 the Cassels-Tate pairing is given by

$$\langle \varepsilon, \eta \rangle_{\mathrm{CT}} = \sum_v (a, \gamma(P_v))_v$$

where for each place v of k we choose a local point $P_v \in \mathcal{K}_\varepsilon(k_v)$ that lifts to $\mathcal{J}_\varepsilon(k_v)$ and satisfies $\gamma(P_v) \neq 0$.

Since $\mathcal{C}$ has discriminant $2^8 \cdot 3^4 \cdot 13 \cdot 17 \cdot 89 \cdot 6229$, the norm of a is 37, the coefficients of γ generate the unit ideal in $\mathbb{Z}[\zeta]$, and k has no real places, it follows by Theorem 4.4 that the only places that could contribute to the pairing are the primes dividing $2, 3, 13, 17, 37, 89$ and 6229. For each of these primes $\mathfrak{p}$, except (2), it is easy to find a smooth point on the reduction of $\mathcal{K}_\varepsilon$ mod $\mathfrak{p}$ where the pushout form defining the double cover $\mathcal{J}_\varepsilon \to \mathcal{K}_\varepsilon$ takes a non-zero square value, and γ takes a non-zero value. Moreover if $\mathfrak{p}$ is the prime dividing a, then γ takes a non-zero square value. Taking as our local point any Hensel lift of this mod $\mathfrak{p}$ point shows that these primes make no contribution to the pairing. It remains to compute the contribution at the prime (2). In this case we choose the local point

$$P_2 = (1 : 0 : 1 : 2^2 + (1+\zeta)2^3 + O(2^5)) \in \mathcal{K}_\varepsilon(k_2)$$

which lifts to $\mathcal{J}_\varepsilon(k_2)$, and satisfies $\gamma(P_2) \equiv 2^2(-1+2\zeta) \pmod{2^5}$. Since the Hilbert symbol $(a, -1+2\zeta)_2$ is non-trivial it follows that $\langle \varepsilon, \eta \rangle_{\mathrm{CT}} \neq 0$.

Since $\mathcal{C}$ has no deficient places, we know by Lemma 3.1 that the Cassels-Tate pairing on $S^{(2)}(\mathcal{J}/k)$ has even rank. In view of the points of infinite order we found earlier, and (62), it follows that $\operatorname{rank} \mathcal{J}(k) = 4$ and $\operatorname{rank} \mathcal{J}(\mathbb{Q}) = 2$.

4.4. **Examples from the LMFDB.** The *L-functions and modular forms database* [LMFDB] contains a database of genus 2 curves defined over $\mathbb{Q}$, as described in the accompanying paper [BSSVY]. The database (accessed May 2023) contains 66,158 genus 2 curves in 65,534 isogeny classes, and contains all known genus 2 curves with absolute discriminant at most 10^6.

Amongst the data listed (for each genus 2 curve $\mathcal{C}$ with Jacobian $\mathcal{J}$) is the analytic order of the Tate–Shafarevich group $Ш(\mathcal{J}/\mathbb{Q})$. We restrict attention to the 4161 curves where this order is even. In all 4161 cases we were able to compute the Cassels-Tate pairing on $S^{(2)}(\mathcal{J}/\mathbb{Q})$. In particular the fact that our method depends on finding rational points on certain twisted Kummer surfaces was not a problem in practice.

In 4088 of the 4161 cases we find that the Cassels-Tate pairing on $Ш(\mathcal{J}/\mathbb{Q})[2]$ is non-degenerate, and hence a 2-descent followed by our methods are sufficient to compute the rank of $\mathcal{J}(\mathbb{Q})$ unconditionally. In such examples it also follows that $Ш(\mathcal{J}/\mathbb{Q})[2^\infty]$ is 2-torsion. These examples, broken down by $r = \operatorname{rank} \mathcal{J}(\mathbb{Q})$ and $s = \dim_{\mathbb{F}_2} Ш(\mathcal{J}/\mathbb{Q})[2]$, were distributed as follows.

	$s=1$	$s=2$	$s=3$	$s=4$	total
$r=0$	1125	1387	38	9	2559
$r=1$	1004	406	7	2	1419
$r=2$	106	3	0	0	109
$r=3$	1	0	0	0	1
total	2236	1796	45	11	4088

We recall (see Lemma 3.1) that a place v is deficient if $\mathcal{C}$ has no $\mathbb{Q}_v$-rational divisor of degree 1. The same examples, broken down by the number t of deficient places and $s = \dim_{\mathbb{F}_2} Ш(\mathcal{J}/\mathbb{Q})[2]$, were distributed as follows.

	$s=1$	$s=2$	$s=3$	$s=4$	total
$t=0$	0	1782	0	10	1792
$t=1$	2232	0	45	0	2277
$t=2$	0	14	0	1	15
$t=3$	4	0	0	0	4
total	2236	1796	45	11	4088

This is in accordance with the result of Poonen and Stoll (see Lemma 3.1) that the rank of the pairing has the same parity as the number of deficient places. The pairing was alternating (equivalently, the canonical element c was in the kernel of the pairing) in 486 cases with $s = 2$, and 3 cases with $s = 4$.

We now compute the rank of $\mathcal{J}(\mathbb{Q})$ in the remaining $4161 - 4088 = 73$ cases. We divide these curves into lists A, B, C and D according to the method we use. These lists contain 17, 30, 15 and 11 curves respectively.

The Jacobians in list A are isogenous over $\mathbb{Q}$ to a product of elliptic curves. Since the elliptic curves all have small conductor (at most 25840), it is easy to compute the rank of $\mathcal{J}(\mathbb{Q})$ (it is either 0 or 1) as the sum of the ranks of the elliptic curves. In contrast the Jacobians in lists B, C and D are absolutely simple. In these cases it is expected that $\operatorname{rank} \mathcal{J}(\mathbb{Q}) = 0$. The Birch Swinnerton-Dyer conjecture (together with a 2-descent and Lemma 3.1) further predicts that $Ш(\mathcal{J}/\mathbb{Q}) \cong (\mathbb{Z}/4\mathbb{Z})^2$ or $(\mathbb{Z}/8\mathbb{Z})^2$, the latter only for the curve with LMFDB label `108737.a.108737.1` in list C.

We say that genus 2 curves are isogenous if their Jacobians are isogenous. For each curve in list B we found an isogenous curve whose Jacobian has no elements of order 2 in its Tate-Shafarevich group. A 2-descent was therefore sufficient to prove that the rank is 0. For each curve in list C we likewise found an isogenous curve whose Jacobian has no elements of order 4 in its Tate-Shafarevich group. Computing the Cassels-Tate pairing on the 2-Selmer group was therefore sufficient to prove that the rank is 0.

In processing lists B and C, we found the isogenous curves using the Magma function `TwoPowerIsogenies`. In all but two cases (`111989.a.111989.2` and `276083.a.276083.2`, both in list C) the isogenous curve we used is *not* listed in the LMFDB, since it has absolute discriminant greater than 10^6. The isogenies that are relevant here are typically "double Richelot isogenies". These are isogenies defined over $\mathbb{Q}$ that are the composite of two Richelot isogenies defined over a cubic number field.

There are 11 curves in list D, in 10 isogeny classes. We were able to prove that the rank is 0 in each of these cases using our method from Section 4.3, that is, we combine visibility with computing the Cassels-Tate pairing over a quadratic field $\mathbb{Q}(\sqrt{d})$. We used the following values of d, ignoring the first curve since it is isogenous to the second (in fact via a double Richelot isogeny).

LMFDB label	d	LMFDB label	d	LMFDB label	d
`65563.d.65563.1`		`300429.a.300429.1`	-3	`876096.a.876096.1`	-3
`65563.d.65563.2`	-7	`438837.b.438837.1`	-3	`881669.a.881669.1`	5
`106015.b.742105.1`	-3	`681797.a.681797.1`	-3	`913071.a.913071.1`	-3
`270438.a.270438.1`	-3	`711917.a.711917.1`	-3		

This completes the unconditional determination of the ranks of all genus 2 Jacobians in the LMFDB.

Remark 4.12. Prior to our work, the LMFDB listed[6] 69 genus 2 curves for which the rank of the Jacobian was only known conditionally. In 45 of these cases (the first being that in Example 4.6) we have $Ш(\mathcal{J}/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^2$. These are therefore included in the 4088 cases analysed above. These are all cases where the canonical element of $S^{(2)}(\mathcal{J}/\mathbb{Q})$ is trivial, there are no deficient places, and $\operatorname{rank} \mathcal{J}(\mathbb{Q}) = 0$ or 1 (the latter only for `776185.a.776185.1`). The remaining 24 cases comprise all but 2 curves in list C, and all curves in list D. There are no curves in lists A and B since our methods in these cases are already used by Stoll's Magma function `MordellWeilGroupGenus2`. The two curves in list C that were already resolved are `38267.a.38267.1` and `523925.a.523925.1`. These

[6] `https://www.lmfdb.org/api/g2c_curves/?mw_rank_proved=0`

are isogenous to curves where Lemma 3.1 and Remark 3.2 already give sufficient information about the pairing to conclude.

References

[BG] M. Bhargava and B.H. Gross, The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point, in *Automorphic representations and L-functions*, D. Prasad, C.S. Rajan, A. Sankaranarayanan and J. Sengupta (eds), 23–91, Tata Inst. Fundam. Res. Stud. Math., **22**, Tata Inst. Fund. Res., Mumbai, 2013.

[BL] C. Birkenhake and H. Lange, *Complex abelian varieties*, Second edition, Grundlehren der mathematischen Wissenschaften, **302**, Springer-Verlag, Berlin, 2004.

[BSSVY] A.R. Booker, J. Sijsling, A.V. Sutherland, J. Voight, and D. Yasaki, A database of genus 2 curves over the rational numbers, Twelfth Algorithmic Number Theory Symposium (ANTS XII), *LMS Journal of Computation and Mathematics* **19** (2016), 235–254.

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

[BF] N. Bruin and E.V. Flynn, Exhibiting SHA[2] on hyperelliptic Jacobians, *J. Number Theory* **118** (2006), no. 2, 266–291.

[BS] N. Bruin and M. Stoll, Deciding existence of rational points on curves: an experiment, *Experiment. Math.* **17** (2008), no. 2, 181–189.

[C1] J.W.S. Cassels, Arithmetic on curves of genus 1, III. The Tate-Šafarevič and Selmer groups, *Proc. London Math. Soc.* (3) **12** (1962), 259–296.

[C2] J.W.S. Cassels, Arithmetic on curves of genus 1, IV. Proof of the Hauptvermutung. *J. reine angew. Math.* **211** (1962), 95–112.

[C3] J.W.S. Cassels, *Rational quadratic forms*, London Mathematical Society Monographs, **13**, Academic Press, London-New York, 1978.

[C4] J.W.S. Cassels, The Mordell-Weil group of curves of genus 2, in *Arithmetic and geometry, Vol. I*, M. Artin and J Tate (eds), 27–60, Progr. Math., 35, Birkhäuser, Boston, Mass., 1983.

[C5] J.W.S. Cassels, Second descents for elliptic curves, *J. reine angew. Math.* **494** (1998), 101–127.

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

[Cl] P.L. Clark, *The period-index problem in WC-groups II: abelian varieties*, preprint 2004, `arXiv:math/0406135[math.NT]`

[CFS] 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.

[Cr] B. Creutz, Improved rank bounds from 2-descent on hyperelliptic Jacobians, *Int. J. Number Theory* **14** (2018), no. 6, 1709–1713.

[CV] B. Creutz and B. Viray, Two torsion in the Brauer group of a hyperelliptic curve, *Manuscripta Math.* **147** (2015), no. 1-2, 139–167.

[D] R. Donagi, Group law on the intersection of two quadrics, *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)* **7** (1980), no. 2, 217–239.

[Do] S. Donnelly, *Algorithms for the Cassels-Tate pairing*, preprint, 2015.

[Fi1] T.A. Fisher, Testing equivalence of ternary cubics, in *Algorithmic number theory*, 333–345, Lecture Notes in Comput. Sci., **4076**, Springer, Berlin, 2006.

[Fi2] T.A. Fisher, On binary quartics and the Cassels-Tate pairing, *Res. Number Theory* **8** (2022), no. 4, Paper No. 74, 13 pp.

[FL] T.A. Fisher and M. Liu, *Minimisation of* 2*-coverings of genus* 2 *Jacobians*, preprint 2023, `arXiv:2309.06220[math.NT]`

[Fl] M. Flach, A generalisation of the Cassels-Tate pairing, *J. reine angew. Math.* **412** (1990), 113–127.

[F1] E.V. Flynn, The Jacobian and formal group of a curve of genus 2 over an arbitrary ground field, *Math. Proc. Cambridge Philos. Soc.* **107** (1990), no. 3, 425–441.

[F2] E.V. Flynn, The group law on the Jacobian of a curve of genus 2, *J. reine angew. Math.* **439** (1993), 45–69.

[FPS] E.V. Flynn, B. Poonen and E.F. Schaefer, Cycles of quadratic polynomials and rational points on a genus-2 curve, *Duke Math. J.* **90** (1997), no. 3, 435–463.

[FTvL] E.V. Flynn, D. Testa and R. van Luijk, Two-coverings of Jacobians of curves of genus 2, *Proc. Lond. Math. Soc.* (3) **104** (2012), no. 2, 387–429.

[FJ] S. Frei and L. Ji, *A threefold violating a local-to-global principle for rationality*, preprint 2023, `arXiv:2304.09306[math.AG]`

[FH] W. Fulton and J. Harris, *Representation theory, A first course*, Graduate Texts in Mathematics, **129**, Springer-Verlag, New York, 1991.

[GG] D.M. Gordon and D. Grant, Computing the Mordell-Weil rank of Jacobians of curves of genus two, *Trans. Amer. Math. Soc.* **337** (1993), no. 2, 807–824.

[HS] Y. Harpaz and A.N. Skorobogatov, Hasse principle for Kummer varieties, *Algebra & Number Theory* **10** (2016), no. 4, 813–841.

[LMFDB] The LMFDB Collaboration, The L-functions and Modular Forms Database, (online; accessed May 2023), `https://www.lmfdb.org/`

[L] S. Lichtenbaum, Duality theorems for curves over p-adic fields, *Invent. Math.* **7** (1969), 120–136.

[LvL] A. Logan and R. van Luijk, Nontrivial elements of Sha explained through K3 surfaces, *Math. Comp.* **78** (2009), no. 265, 441–483.

[Mi] J.S. Milne, *Arithmetic duality theorems*, Second edition, BookSurge, LLC, Charleston, SC, 2006.

[Mo] A. Morgan, *Hasse principle for Kummer varieties in the case of generic 2-torsion*, preprint 2023, `arXiv:2309.02374[math.NT]`

[NR] M.S. Narasimhan and S. Ramanan, Moduli of vector bundles on a compact Riemann surface, *Ann. of Math.* (2) **89** (1969), 14–51.

[N] P.E. Newstead, Stable bundles of rank 2 and odd degree over a curve of genus 2, *Topology* **7** (1968), 205–215.

[PSc] B. Poonen and E.F. Schaefer, Explicit descent for Jacobians of cyclic covers of the projective line, *J. reine angew. Math.* **488** (1997), 141–188.

[PSt] B. Poonen and M. Stoll, The Cassels-Tate pairing on polarized abelian varieties, *Ann. of Math.* (2) **150** (1999), no. 3, 1109–1149.

[R] M. Reid, *The complete intersection of two or more quadrics*, PhD thesis, University of Cambridge, 1972.

[Se] J.-P. Serre, *Local fields*, Graduate Texts in Mathematics, **67**, Springer-Verlag, New York-Berlin, 1979.

[SW] A. Shankar and X. Wang, Rational points on hyperelliptic curves having a marked non-Weierstrass point, *Compos. Math.* **154** (2018), no. 1, 188–222.

[Si] D. Simon, *Quadratic equations in dimensions 4, 5 and more*, preprint, 2005, `https://simond.users.lmno.cnrs.fr/`

[S1] M. Stoll, On the height constant for curves of genus two, *Acta Arith.* **90** (1999), no. 2, 183–201.

[S2] M. Stoll, Implementing 2-descent for Jacobians of hyperelliptic curves, *Acta Arith.* **98** (2001), no. 3, 245–277.

[SvL] M. Stoll and R. van Luijk, Explicit Selmer groups for cyclic covers of $\mathbb{P}^1$, *Acta Arith.* **159** (2013), no. 2, 133–148.

[Sw] H.P.F. Swinnerton-Dyer, *A brief guide to algebraic number theory*, London Mathematical Society Student Texts, **50**, Cambridge University Press, Cambridge, 2001.

[Ta] J. Tate, Duality theorems in Galois cohomology over number fields, *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)* pp. 288–295, Inst. Mittag-Leffler, Djursholm, 1963.

[T1] J.A. Thorne, A remark on the arithmetic invariant theory of hyperelliptic curves, *Math. Res. Lett.* **21** (2014), no. 6, 1451–1464.

[T2] J.A. Thorne, *Reduction theory for stably graded Lie algebras*, in preparation.

[Wa] X. Wang, Maximal linear spaces contained in the based loci of pencils of quadrics, *Algebr. Geom.* **5** (2018), no. 3, 359–397.

[We] A. Weil, Remarques sur un mémoire d'Hermite, *Arch. Math. (Basel)* **5** (1954), 197–202.

[Y1] J. Yan, *Computing the Cassels-Tate pairing for Jacobian varieties of genus two curves*, PhD thesis, University of Cambridge, 2021, `https://doi.org/10.17863/CAM.72729`

[Y2] J. Yan, *Computing the Cassels-Tate pairing for genus two Jacobians with rational two torsion points*, preprint, 2021, `arXiv:2109.08258[math.NT]`

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

Email address: `T.A.Fisher@dpmms.cam.ac.uk`

Email address: `jialiyan.lele@gmail.com`