MINIMISATION OF 2-COVERINGS OF GENUS 2 JACOBIANS

TOM FISHER AND MENGZHEN LIU

Abstract. An important problem in computational arithmetic geometry is to find changes of coordinates to simplify a system of polynomial equations with rational coefficients. This is tackled by a combination of two techniques, called minimisation and reduction. We give an algorithm for minimising certain pairs of quadratic forms, subject to the constraint that the first quadratic form is fixed. This has applications to 2-descent on the Jacobian of a genus 2 curve.

1. Introduction

1.1. **Models for 2-coverings.** We work over a field K with $\mathrm{char}(K) \neq 2$. Let C be a smooth curve of genus 2 with equation $y^2 = f(x) = f_6x^6 + f_5x^5 + \ldots + f_1x + f_0$ where $f \in K[x]$ is a polynomial of degree 6. We fix throughout the polynomial

$$G = z_{12}z_{34} - z_{13}z_{24} + z_{23}z_{14}.$$

The following two definitions are based on those in [FY, Section 2.4].

Definition 1.1. A *model* (for a 2-covering of the Jacobian of C) is a pair (λ, H) where $\lambda \in K^\times$ and $H \in K[z_{12}, z_{13}, z_{23}, z_{14}, z_{24}, z_{34}]$ is a quadratic form satisfying

$$\det(\lambda x\mathbf{G} - \mathbf{H}) = -\lambda^6 f_6^{-1} f(x)$$

where $\mathbf{G}$ and $\mathbf{H}$ are the matrices of second partial derivatives of G and H.

We identify the space of column vectors of length 6 and the space of 4×4 alternating matrices via the map

$$A : z = \begin{pmatrix} z_{12} \\ z_{13} \\ z_{23} \\ z_{14} \\ z_{24} \\ z_{34} \end{pmatrix} \mapsto \begin{pmatrix} 0 & z_{12} & z_{13} & z_{14} \\ & 0 & z_{23} & z_{24} \\ & - & 0 & z_{34} \\ & & & 0 \end{pmatrix}$$

Date: 12th September 2023.

so that $G(z)$ is the Pfaffian of $A(z)$. Then each 4×4 matrix P uniquely determines a 6×6 matrix $\wedge^2 P$ such that

$$PA(z)P^T = A((\wedge^2 P)z)$$

for all column vectors z. For $F\in K[x_1,\dots,x_n]$ and $M\in \mathrm{GL}_n(K)$ we write $F\circ M$ for the polynomial satisfying $(F\circ M)(x) = F(Mx)$ for all columns vectors x. The Pfaffian $\mathrm{Pf}(A)$ of an alternating matrix A has the properties that $\mathrm{Pf}(A)^2 = \det(A)$ and $\mathrm{Pf}(PAP^T) = (\det P)\,\mathrm{Pf}(A)$. The latter tells us that $G\circ\wedge^2 P = (\det P)G$. It is also not hard to show that $\det(\wedge^2 P) = (\det P)^3$.

Definition 1.2. Two models are K-*equivalent* if they are in the same orbit for the action of $K^\times \times \mathrm{PGL}_4(K)$ via

$$(c,P) : (\lambda, H) \mapsto \left(c\lambda, \frac{c}{\det P} H\circ \wedge^2 P\right).$$

It may be checked using the above observations that this is a well defined (right) group action on the space of models (for a fixed choice of genus 2 curve C).

Example 1.3. Let $C/\mathbb{Q}$ be the genus 2 curve given by $y^2 = f(x)$ where

$$f(x) = -28x^6 + 84x^5 - 323x^4 + 506x^3 - 471x^2 + 232x - 60.$$

One of the elements of the 2-Selmer group of $\mathrm{Jac}\, C$ is represented by the model

$$\begin{aligned}(\lambda_1, H_1) = (42336,\ & 25128z_{12}^2 + 24480z_{12}z_{13} + 14031z_{12}z_{23} + 15408z_{12}z_{14} \\ & + 13959z_{12}z_{24} + 25407z_{12}z_{34} + 2232z_{13}^2 - 16407z_{13}z_{23} + 4464z_{13}z_{14} \\ & - 22815z_{13}z_{24} + 1161z_{13}z_{34} + 2329z_{23}^2 + 15282z_{23}z_{14} + 7687z_{23}z_{24} \\ & - 19547z_{23}z_{34} - 2304z_{14}^2 - 17838z_{14}z_{24} - 22590z_{14}z_{34} - 134z_{24}^2 \\ & + 41978z_{24}z_{34} - 99584z_{34}^2).\end{aligned}$$

Applying the transformation (c,P) with $c = 1/3024$ and

$$P = \begin{pmatrix} 2 & -19 & 2 & 5 \\ 4 & 4 & -31 & 38 \\ 2 & 2 & 37 & 40 \\ -7 & -7 & -14 & 7 \end{pmatrix} \tag{1}$$

gives the $\mathbb{Q}$-equivalent model

$$\begin{aligned}(\lambda_2, H_2) = (14,\ & z_{12}z_{23} + 2z_{12}z_{14} - z_{12}z_{24} + 8z_{12}z_{34} - 7z_{13}^2 - 13z_{13}z_{23} \\ & - 12z_{13}z_{14} - 15z_{13}z_{24} - 20z_{13}z_{34} - 5z_{23}^2 - 2z_{23}z_{14} - 25z_{23}z_{24} \\ & - 59z_{23}z_{34} - 4z_{14}^2 - 14z_{14}z_{24} - 18z_{14}z_{34} + 17z_{24}^2 - 37z_{24}z_{34} - 11z_{34}^2).\end{aligned}$$

1.2. **Relation to previous work.** The change of coordinates (1) was found by a combination of two techniques, called minimisation and reduction. *Minimisation* seeks to remove prime factors from a suitably defined invariant (usually the discriminant). The prototype example is using Tate's algorithm to compute a minimal Weierstrass equation for an elliptic curve. *Reduction* seeks to a make a final unimodular substitution so that the coefficients are as small as possible. The prototype example is the reduction algorithm for positive definite binary quadratic forms.

Algorithms for minimising and reducing 2-, 3-, 4- and 5-coverings of elliptic curves are given by Cremona, Fisher and Stoll [CFS], and Fisher [F], building on earlier work of Birch and Swinnerton-Dyer [BSD] for 2-coverings. Algorithms for minimising some other representations associated to genus 1 curves are given by Fisher and Radicevic [FR]. A general framework for minimising hypersurfaces is described by Kollar [K], and this has been refined by Elsenhans and Stoll [ES]; in particular they give practical algorithms for plane curves (of arbitrary degree) and for cubic surfaces. Algorithms for minimising Weierstrass equations for general hyperelliptic curves are given by Q. Liu [L].

In this paper we give an algorithm for minimising 2-coverings of genus 2 Jacobians. These are represented by pairs of quadratic forms (see Definition 1.1) where the first quadratic form is fixed. We only consider minimisation and not reduction, since the latter is already treated in [FY, Remark 4.3].

Our minimisation algorithm plays a key role in the work of the first author and Jiali Yan [FY] on computing the Cassels-Tate pairing on the 2-Selmer group of a genus 2 Jacobian. Indeed the method presented in *loc. cit.* for computing the Cassels-Tate pairing relies on being able to find rational points on certain twisted Kummer surfaces. Minimising and reducing our representatives for the 2-Selmer group elements simplifies the equations for these surfaces, and so makes it more likely that we will be able to find such rational points.

Earlier works on minimisation (see in particular [CFS]) considered both minimisation theorems (i.e., general bounds on the minimal discriminant) and minimisation algorithms (i.e., practical methods for finding a minimal model equivalent to a given one). For 2-coverings of hyperelliptic Jacobians, some minimisation theorems have already been proved; see the papers of Bhargava and Gross [BG, Section 8], and Shankar and Wang [SW, Section 2.4]. We will not revisit these results, as our focus is on the minimisation algorithms.

Remark 1.4. As noted in [CF, Lemma 17.1.1], [FH, Section 19.1] and [FY, Section 2.4] the quadratic form $G = z_{12}z_{34} - z_{13}z_{24} + z_{23}z_{14}$ has two algebraic families of 3-dimensional isotropic subspaces. Moreover, the transformations considered in Definition 1.2 do not describe the full projective orthogonal group of G, but only the index 2 subgroup that preserves (rather than swaps over) these two algebraic families. Restricting attention to this index 2 subgroup (when defining equivalence) makes no difference to the minimisation problem (see Remark 3.2), but as explained in [FY, Sections 2.4 and 2.5] it is important in the context of 2-descent, since it means we can distinguish between elements of the 2-Selmer group with the same image in the fake 2-Selmer group.

Some Magma [BCP] code accompanying this article, including an implementation of our algorithm, will be made available from the first author's website.

Acknowledgements. This work originated as a summer project carried out by the second author and supervised by the first author. We thank the Research in the CMS Programme for their support.

2. Statement of the algorithm

We keep the notation of Section 1.1, but now let K be a field with discrete valuation $v : K^\times \to \mathbb{Z}$, valuation ring $\mathcal{O}_K$, uniformiser π, and residue field k. If F is a polynomial with coefficients in K then we write $v(F)$ for the minimum of the valuations of its coefficients.

Definition 2.1. A model (λ, H) is *integral* if $v(H) \geqslant 0$. It is *minimal* if $v(\lambda)$ is minimal among all K-equivalent integral models.

Using the action of $K^\times$ (see Definition 1.2) to clear denominators it is clear that any model is K-equivalent to an integral model. By Definition 1.1 we have $v(\lambda) \geqslant (v(f_6) - v(f_i))/(6-i)$ for all $i = 0, 1, \ldots, 5$. We cannot have $f_0 = \ldots = f_5 = 0$ since C is a smooth curve of genus 2. Therefore $v(\lambda)$ is bounded below, and minimal models exist.

It also follows from Definition 1.1 that if $v(f_6) = v(\operatorname{disc} f) = 0$ then any integral model (λ, H) has $v(\lambda) \geqslant 0$. Therefore, in global applications, minimality is automatic at all but a finite set of primes, which we may determine by factoring.

Returning to the local situation, there is an evident recursive algorithm for computing minimal models if we can solve the following problem.

Minimisation problem. Given an integral quadratic form $H \in \mathcal{O}_K[z_{12}, \ldots, z_{34}]$ determine whether there exists $P \in \mathrm{PGL}_4(K)$ such that

$$v\left(\frac{1}{\det P} H \circ \wedge^2 P\right) > 0$$

and find such a matrix P if it exists.

Our solution to this problem (see Algorithm 2.4) is an iterative procedure that computes the required transformation as a composition of simpler transformations. These simpler transformations are either given by a matrix in $\mathrm{GL}_4(\mathcal{O}_K)$, in which case we call the transformation an *integral change of coordinates*, or given by one of the following operations, corresponding to $P = \mathrm{Diag}(1,1,1,\pi), \mathrm{Diag}(1,1,\pi,\pi)$ or $\mathrm{Diag}(1,\pi,\pi,\pi)$.

Definition 2.2. We define the following three operations on quadratic forms H:

- Operation 1. Replace H by $\frac{1}{\pi}H(z_{12}, z_{13}, z_{23}, \pi z_{14}, \pi z_{24}, \pi z_{34})$,
- Operation 2. Replace H by $H(\pi^{-1}z_{12}, z_{13}, z_{23}, z_{14}, z_{24}, \pi z_{34})$,
- Operation 3. Replace H by $\frac{1}{\pi}H(z_{12}, z_{13}, \pi z_{23}, z_{14}, \pi z_{24}, \pi z_{34})$,

The following algorithm suggests some transformations that we might try applying to H. In applications $W \subset k^6$ will be a subspace determined by the reduction of H mod π. We write $e_{12}, e_{13}, e_{23}, e_{14}, e_{24}, e_{34}$ for the standard basis of k^6, and identify the dual basis with $z_{12}, z_{13}, z_{23}, z_{14}, z_{24}, z_{34}$.

Algorithm 2.3. (Subalgorithm to suggest some transformations.) We take as input an integral quadratic form $H \in \mathcal{O}_K[z_{12}, \ldots, z_{34}]$ and a vector space $W \subset k^6$ that is isotropic for G. When we make an integral change of coordinates we apply the same transformation (or rather its reduction mod π) to W. The output is either one or two transformations $P \in \mathrm{PGL}_4(K)$.

- If $\dim W = 1$ then make an integral change of coordinates so that $W = \langle e_{12} \rangle$. Then apply Operation 2.
- If $\dim W = 2$ then make an integral change of coordinates so that $W = \langle e_{12}, e_{13} \rangle$. Then apply either Operation 1 or Operation 3.
- If $\dim W = 3$ then either make an integral change of coordinates so that $W = \langle e_{12}, e_{13}, e_{23} \rangle$ and apply Operation 1, or make an integral change of coordinates so that $W = \langle e_{12}, e_{13}, e_{14} \rangle$ and apply Operation 3.

We write $\overline{H} \in k[z_{12}, \ldots, z_{34}]$ for the reduction of H mod π. If $\mathrm{char}(k) \neq 2$ then the rank and kernel of $\overline{H}$ are defined as the rank and kernel of the corresponding 6×6 symmetric matrix. If $\mathrm{char}(k) = 2$ then we assume that k is perfect, so that

$$\overline{H} = \frac{\partial \overline{H}}{\partial z_{12}} = \ldots = \frac{\partial \overline{H}}{\partial z_{34}} = 0$$

defines a k-vector space, which we call $\ker \overline{H}$. We then define

$$\mathrm{rank}\, \overline{H} = 6 - \dim \ker \overline{H}.$$

We continue to write G for the reduction of G mod π, as it should always be clear from the context which of these we mean.

Algorithm 2.4. (Minimisation algorithm.) We take as input an integral quadratic form $H \in \mathcal{O}_K[z_{12}, \ldots, z_{34}]$. The output is `TRUE/FALSE` according as whether there exists $P \in \mathrm{PGL}_4(K)$ such that

$$v\left(\frac{1}{\det P} H \circ \wedge^2 P\right) > 0.$$

Step 1. Compute $r = \operatorname{rank} \overline{H}$. If $r = 0$ then return `TRUE`.

Step 2. If $r = 1$ then try making an integral change of coordinates so that $\overline{H} = z_{34}^2$. If the reductions of G and $\pi^{-1}H(z_{12}, \ldots, z_{24}, 0) \bmod \pi$ have a common 3-dimensional isotropic subspace $W \subset \ker \overline{H}$, then (since running Algorithm 2.3 on any such subspace W gives $v(H) > 0$) return `TRUE`.

Step 3. If $r = 2$ then try running Algorithm 2.3 on each codimension 1 subspace $W \subset \ker \overline{H}$ that is isotropic for G. If one of the suggested transformations gives $v(H) > 0$ then return `TRUE`.

Step 4. If $r \in \{1, 2\}$ and $\overline{H}$ factors as a product of linear forms defined over k, say $\overline{H} = \ell_1 \ell_2$, then for each $i = 1, 2$ try making an integral change of coordinates so that $\ell_i = z_{34}$ and then apply Operation 2. If at least one of these transformations gives $v(H) \geqslant 0$ then select one with $\operatorname{rank} \overline{H}$ as small as possible and go to Step 1.

Step 5. If $r \in \{2, 3, 4, 5\}$ then try running Algorithm 2.3 on $W = \ker \overline{H}$ if this subspace is isotropic for G, and otherwise on each codimension 1 subspace $W \subset \ker \overline{H}$ that is isotropic for G. If at least one of the suggested transformations gives $v(H) \geqslant 0$ then select one with $\operatorname{rank} \overline{H}$ as small as possible and go to Step 1.

Step 6. If this step is reached, or if after visiting Step 1 the first time and returning to it a further 4 times we still do not have $v(H) > 0$, then return `FALSE`.

There is no difficulty in modifying the algorithm so that when it returns `TRUE` the corresponding transformation $P \in \mathrm{PGL}_4(K)$ is also returned. In Section 3 we give further details of the implementation, in particular explaining how we make the integral changes of coordinates, and giving further details of Step 2. In Sections 4 and 5 we prove that Algorithm 2.4 is correct.

3. Remarks on implementation

In Algorithms 2.3 and 2.4 we are asked to try making various integral changes of coordinates. It is important to realise that we are restricted to considering matrices of the form $\wedge^2 P$ for $P \in \mathrm{GL}_4(\mathcal{O}_K)$, and not general elements of $\mathrm{GL}_6(\mathcal{O}_K)$. Therefore some care is required both in determining whether a suitable transformation exists, and in finding one when it does.

Since the natural map $\mathrm{GL}_4(\mathcal{O}_K) \to \mathrm{GL}_4(k)$ is surjective, we may concentrate on the mod π situation here. Notice however that in the global application with

$K = \mathbb{Q}$ and $v = v_p$ it is better to use the surjectivity of $\mathrm{SL}_4(\mathbb{Z}) \to \mathrm{SL}_4(\mathbb{Z}/p\mathbb{Z})$, so that minimisation at p does not interfere with minimisation at other primes.

Let k^4 have basis $e_1, \ldots, e_4$. We identify $\wedge^2 k^4 = k^6$ via $e_i \wedge e_j \mapsto e_{ij}$. Each linear subspace $W \subset k^6$ determines a linear subspace $V_0 \subset k^4$ given by

$$V_0 = \{v \in k^4 \mid v \wedge w = 0 \text{ for all } w \in W\}$$

where $\wedge$ is the natural map $k^4 \times \wedge^2 k^4 \to \wedge^3 k^4$. Let V_1 be the analogue of V_0 when W is replaced by its orthogonal complement with respect to G.

Lemma 3.1. *Let $W \subset k^6$ be a subspace, and let $P \in \mathrm{GL}_4(k)$.*

(i) *If $\dim W = 1$ then $\wedge^2 P$ sends W to $\langle e_{12} \rangle$ if and only if P sends V_0 to $\langle e_1, e_2 \rangle$.*
(ii) *If $\dim W = 2$ or 3 then $\wedge^2 P$ sends W to a subspace of $\langle e_{12}, e_{13}, e_{14} \rangle$ if and only if P sends V_0 to $\langle e_1 \rangle$.*
(iii) *If $\dim W = 5$ then $\wedge^2 P$ sends W to $\langle e_{12}, e_{13}, e_{14}, e_{23}, e_{24} \rangle$ if and only if P sends V_1 to $\langle e_1, e_2 \rangle$.*

Proof. In (i) we have $W = \langle e_{12} \rangle$ if and only if $V_0 = \langle e_1, e_2 \rangle$, and in (ii) we have $W \subset \langle e_{12}, e_{13}, e_{14} \rangle$ if and only if $V_0 = \langle e_1 \rangle$. Since the definition of V_0 in terms of W behaves well under all changes of coordinates this proves (i) and (ii). As noted in Section 1.1, all transformations of the form $\wedge^2 P$ preserve G (up to a scalar multiple). Therefore (iii) follows from (i) on replacing W by its orthogonal complement with respect to G. $\square$

Remark 3.2. Let $\mathbf{G}$ be the matrix of second partial derivatives of G, i.e., the 6×6 matrix with entries $1, -1, 1, 1, -1, 1$ on the antidiagonal. A direct calculation shows that for any 4×4 matrix P we have

$$\wedge^2(\mathrm{adj}(P)^T) = (\det P)\mathbf{G}(\wedge^2 P)\mathbf{G}.$$

Letting PGL_4 act on the space of quadratic forms via $P : H \mapsto \frac{1}{\det P} H \circ \wedge^2 P$, this tells us that applying P to a quadratic form $H(z_{12}, z_{13}, z_{23}, z_{14}, z_{24}, z_{34})$ has the same effect as applying P^{-T} to its *dual quadratic form* which we define to be $H(z_{34}, -z_{24}, z_{14}, z_{23}, -z_{13}, z_{12})$. We note that the substitution used to replace H by its dual swaps over the two families of isotropic subspaces in Remark 1.4.

We find the changes of coordinates in Algorithm 2.3 by using Lemma 3.1(i) and (ii), and the analogue of (ii) after passing to the dual as in Remark 3.2. We find the changes of coordinates in Steps 2 and 4 of Algorithm 2.4 using Lemma 3.1(iii).

Remark 3.3. In Step 2 of Algorithm 2.4 we must find if possible a 3-dimensional subspace $W \subset \langle e_{12}, e_{13}, e_{14}, e_{23}, e_{24} \rangle$ that is isotropic for both G and $\overline{H}_1$ where

$$H_1(z_{12}, \ldots, z_{24}) = \pi^{-1} H(z_{12}, \ldots, z_{24}, 0).$$

To be isotropic for G we need that $\langle e_{12} \rangle \subset W$. So such a subspace W can only exist if $\overline{H}_1(1, 0, \ldots, 0) = 0$. We assume that this is the case and write

$$\overline{H}_1(z_{12}, \ldots, z_{24}) = z_{12} h_1(z_{13}, z_{23}, z_{14}, z_{24}) + h_2(z_{13}, z_{23}, z_{14}, z_{24})$$

where h_i is a homogeneous polynomial of degree i. Our problem reduces to that of finding a line contained in

$$\{z_{13}z_{24} - z_{23}z_{14} = h_1 = h_2 = 0\} \subset \mathbb{P}^3.$$

The well known description of the lines on $\{z_{13}z_{24} - z_{23}z_{14} = 0\} \subset \mathbb{P}^3$ suggests that we substitute $(z_{13}, z_{23}, z_{14}, z_{24}) = (x_1y_1, x_1y_2, x_2y_1, x_2y_2)$ into h_1 and h_2, take the GCD, and factor into irreducibles. The lines of interest now correspond to linear factors of the form $\alpha x_1 + \beta x_2$ or $\gamma y_1 + \delta y_2$.

Remark 3.4. In Steps 3 and 5 of Algorithm 2.4, when $\ker \overline{H}$ is not itself isotropic for G, we must find all codimension 1 subspaces of $\ker \overline{H}$ that are isotropic for G. Since the restriction of G to $\ker \overline{H}$ is a non-zero quadratic form, it can have at most two linear factors. There are therefore at most two codimension 1 subspaces we need to consider. In particular, the number of times that Algorithm 2.4 applies one of the operations in Definition 2.2 is uniformly bounded.

4. Weights and Admissibility

Let $H \in \mathcal{O}_K[u_0, \ldots, u_5]$ be an integral quadratic form and suppose that there exists $P \in \mathrm{GL}_4(K)$ such that

$$v\left(\frac{1}{\det P} H \circ \wedge^2 P\right) > 0.$$

Then P is equivalent to a matrix in Smith normal form, say

$$P = U \mathrm{Diag}(\pi^{w_1}, \pi^{w_2}, \pi^{w_3}, \pi^{w_4}) V$$

for some $U, V \in \mathrm{GL}_4(\mathcal{O}_K)$ and $w_1, w_2, w_3, w_4 \in \mathbb{Z}$. We say that the weight $w = (w_1, w_2, w_3, w_4)$ is *admissible* for H. It is clear that permuting the entries of w, or adding the same integer to all entries, has no effect on admissibility.

Definition 4.1. The weight $w = (w_1, w_2, w_3, w_4)$ *dominates* the weight $w' = (w_1', w_2', w_3', w_4')$ if

$$\begin{aligned} &\max(1 + w_1 + w_2 + w_3 + w_4 - w_i - w_j - w_k - w_l, 0) \\ &\qquad \geqslant \max(1 + w_1' + w_2' + w_3' + w_4' - w_i' - w_j' - w_k' - w_l', 0) \end{aligned} \tag{2}$$

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

This definition is motivated by the fact that if w dominates w' and w is admissible for H then w' is admissible for H. Our next lemma shows that (for the purpose of proving that Algorithm 2.4 is correct) it suffices to consider finitely many (in fact 12) weights.

Lemma 4.2. *Every weight $w = (0, a, b, c) \in \mathbb{Z}^4$ with $0 \leqslant a \leqslant b \leqslant c$ dominates one of the following weights*

$$\begin{gathered}(0,0,0,0),\ (0,0,0,1),\ (0,1,1,1),\ (0,0,1,1),\ (0,0,1,2),\ (0,1,2,2),\\ (0,1,1,2),\ (0,1,1,3),\ (0,2,2,3),\ (0,1,2,3),\ (0,1,2,4),\ (0,2,3,4).\end{gathered}$$

Proof. We list the pairs (i, j) and (k, l) in Definition 4.1 in the order $(1, 2)$, $(1, 3)$, $(2, 3)$, $(1, 4)$, $(2, 4)$, $(3, 4)$. Taking $w = (0, a, b, c)$, the left hand side of (2) is $\max(\xi, 0)$ where ξ runs over the entries of the following symmetric matrix.

$$\begin{bmatrix} 1+b+c-a & 1+c & 1+c-a & 1+b & 1+b-a & 1 \\ 1+c & 1+a+c-b & 1+c-b & 1+a & 1 & 1+a-b \\ 1+c-a & 1+c-b & 1+c-a-b & 1 & 1-a & 1-b \\ 1+b & 1+a & 1 & 1+a+b-c & 1+b-c & 1+a-c \\ 1+b-a & 1 & 1-a & 1+b-c & 1+b-a-c & 1-c \\ 1 & 1+a-b & 1-b & 1+a-c & 1-c & 1+a-b-c \end{bmatrix}$$

We divide into 8 cases according as to which of the inequalities $0 \leqslant a \leqslant b \leqslant c$ are equalities. In fact we make the following more precise claims.

- If $0 = a = b = c$ then $w = (0, 0, 0, 0)$.
- If $0 = a = b < c$ then w dominates $(0, 0, 0, 1)$.
- If $0 = a < b = c$ then w dominates $(0, 0, 1, 1)$.
- If $0 = a < b < c$ then w dominates $(0, 0, 1, 2)$.
- If $0 < a = b = c$ then w dominates $(0, 1, 1, 1)$.
- If $0 < a = b < c$ then w dominates $(0, 1, 1, 3)$, $(0, 1, 1, 2)$ or $(0, 2, 2, 3)$.
- If $0 < a < b = c$ then w dominates $(0, 1, 2, 2)$.
- If $0 < a < b < c$ then w dominates $(0, 1, 2, 4)$, $(0, 1, 2, 3)$ or $(0, 2, 3, 4)$.

In each case where we list three possibilities, we further claim that these correspond to the subcases $a + b < c$, $a + b = c$ and $a + b > c$ (in that order).

Since the proofs are very similar, we give details in just one case. So suppose that $0 < a < b < c$ and $a + b = c$. Then we have $a \geqslant 1$, $b \geqslant 2$, $c \geqslant 3$, $b - a \geqslant 1$, $c - a \geqslant 2$ and $c - b \geqslant 1$. Listing the pairs (i, j) and (k, l) in the same order as before, the left hand side of (2) is at least

$$\begin{bmatrix} 5 & 4 & 3 & 3 & 2 & 1 \\ 4 & 3 & 2 & 2 & 1 & 0 \\ 3 & 2 & 1 & 1 & 0 & 0 \\ 3 & 2 & 1 & 1 & 0 & 0 \\ 2 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

with equality if $(a, b, c) = (1, 2, 3)$. Therefore w dominates $(0, 1, 2, 3)$. $\square$

Our next remark further reduces the number of weights we must consider.

Remark 4.3. It is clear from Remark 3.2 that if $w \in \mathbb{Z}^4$ is admissible for H then $-w$ is admissible for the dual of H. We say that the weights w and $-w$ (or any weights equivalent to these, in the sense of permuting the entries, or adding the same integer to all entries) are *dual*. The list of 12 weights in Lemma 4.2 consists of 4 dual pairs $(0, a, b, c)$ and $(0, c - b, c - a, c)$ with $a + b \neq c$, and 4 self-dual weights $(0, a, b, a + b)$.

5. Completion of the proof

In this section we complete the proof that Algorithm 2.4 is correct.

We first note that if H and H' are related by an integral change of coordinates, and the algorithm works for H then it works for H'. This is because before applying Operations 1, 2 or 3 we always make an integral change of coordinates that, by Lemma 3.1, is unique up to an element of $\mathrm{GL}_4(\mathcal{O}_K)$ whose reduction mod π preserves a suitable subspace of k^4. The following elementary lemma then shows that the transformed quadratic forms are again related by an integral change of coordinates.

Lemma 5.1. *Let* $\alpha = \mathrm{Diag}(I_r, \pi I_{4-r})$ *and* $P \in \mathrm{GL}_4(\mathcal{O}_K)$. *Then* $P \in \alpha \, \mathrm{GL}_4(\mathcal{O}_K)\alpha^{-1}$ *if and only if the reduction of* P *mod* π *preserves the subspace* $\langle e_1, \ldots, e_r \rangle$.

Proof. This is [CFS, Lemma 4.1]. $\square$

Let $H \in \mathcal{O}_K[z_{12}, \ldots, z_{34}]$ be a quadratic form. If there exists $P \in \mathrm{PGL}_4(K)$ such that

$$v\left(\frac{1}{\det P} H \circ \wedge^2 P\right) > 0, \tag{3}$$

then, as explained in Section 4, one of the 12 weights in Lemma 4.2 is admissible for H. Since the analysis for dual weights (see Remark 4.3) is essentially identical, we only need to consider one weight from each dual pair. It therefore suffices to consider the 8 weights listed in the table below.

In the case of weight $(w_1, \ldots, w_4)$ we may suppose, by an integral change of coordinates, that (3) holds with $P = \mathrm{Diag}(\pi^{w_1}, \ldots, \pi^{w_4})$. This implies certain lower bounds on the valuations of the coefficients of H. To specify these (in a way that is valid even when $\mathrm{char}(k) = 2$), we relabel the variables $z_{12}, z_{13}, z_{23}, z_{14}, z_{24}, z_{34}$ as $z_1, \ldots, z_6$ and write $H = \sum_{i \leqslant j} H_{ij} z_i z_j$. We also put $H_{ji} = H_{ij}$. Then the lower bounds on the $v(H_{ij})$ are as recorded in the table.

Case 1: $(0,0,0,0)$ $\begin{bmatrix} 1&1&1&1&1&1\\ 1&1&1&1&1&1\\ 1&1&1&1&1&1\\ 1&1&1&1&1&1\\ 1&1&1&1&1&1\\ 1&1&1&1&1&1 \end{bmatrix}$ $r=0$	**Case 2:** $(0,0,0,1)$ $\begin{bmatrix} 2&2&2&1&1&1\\ 2&2&2&1&1&1\\ 2&2&2&1&1&1\\ 1&1&1&0&0&0\\ 1&1&1&0&0&0\\ 1&1&1&0&0&0 \end{bmatrix}$ $r=1,2,3$	**Case 3:** $(0,0,1,1)$ $\begin{bmatrix} 3&2&2&2&2&1\\ 2&1&1&1&1&0\\ 2&1&1&1&1&0\\ 2&1&1&1&1&0\\ 2&1&1&1&1&0\\ 1&0&0&0&0&0 \end{bmatrix}$ $r=1,2$	**Case 4:** $(0,1,1,2)$ $\begin{bmatrix} 3&3&2&2&1&1\\ 3&3&2&2&1&1\\ 2&2&1&1&0&0\\ 2&2&1&1&0&0\\ 1&1&0&0&0&0\\ 1&1&0&0&0&0 \end{bmatrix}$ $r=1,2,3,4$
Case 5: $(0,0,1,2)$ $\begin{bmatrix} 4&3&3&2&2&1\\ 3&2&2&1&1&0\\ 3&2&2&1&1&0\\ 2&1&1&0&0&0\\ 2&1&1&0&0&0\\ 1&0&0&0&0&0 \end{bmatrix}$ $r=3,4$	**Case 6:** $(0,1,1,3)$ $\begin{bmatrix} 4&4&3&2&1&1\\ 4&4&3&2&1&1\\ 3&3&2&1&0&0\\ 2&2&1&0&0&0\\ 1&1&0&0&0&0\\ 1&1&0&0&0&0 \end{bmatrix}$ $r=3,4$	**Case 7:** $(0,1,2,3)$ $\begin{bmatrix} 5&4&3&3&2&1\\ 4&3&2&2&1&0\\ 3&2&1&1&0&0\\ 3&2&1&1&0&0\\ 2&1&0&0&0&0\\ 1&0&0&0&0&0 \end{bmatrix}$ $r=3,4$	**Case 8:** $(0,1,2,4)$ $\begin{bmatrix} 6&5&4&3&2&1\\ 5&4&3&2&1&0\\ 4&3&2&1&0&0\\ 3&2&1&0&0&0\\ 2&1&0&0&0&0\\ 1&0&0&0&0&0 \end{bmatrix}$ $r=5$

In our analysis of each case, we will assume we are not in an earlier case. The possibilities for $r = \mathrm{rank}\, \overline{H}$ will be justified below, but are recorded in the table for convenience. We complete the proof that Algorithm 2.4 is correct by going through the 8 cases. In fact we show that if the cases are grouped as

Case 1	Case 2	Case 4	Case 5	Case 7
	Case 3		Case 6	Case 8

then at each iteration of the algorithm we move at least one column to the left. Therefore, if after visiting Step 1 the first time and returning to it a further 4 times we still do not have $v(H) > 0$ then the algorithm is correct to return `FALSE`.

Case 1: $w = (0,0,0,0)$. In this case we already have $v(H) > 0$, so $r = 0$ and we are done by Step 1.

Case 2: $w = (0,0,0,1)$. We see from the table that $\langle e_{12}, e_{13}, e_{23} \rangle \subset \ker \overline{H}$ and so $r \leqslant 3$. We cannot have $r = 0$, otherwise we would be in Case 1. If $r = 1$ then we are done by Step 2. If $r = 2$ then we are done by Step 3. If $r = 3$ then Step 5 directly applies Operation 1. (By "directly" we mean that there is no preliminary integral change of coordinates.) Since this gives $v(H) > 0$ we are in Case 1 on the next iteration.

Case 3: $w = (0,0,1,1)$. We see from the table that $\overline{H} = \ell z_{34}$ for some linear form ℓ. One of the transformations considered in Step 4 is to directly apply Operation 2. Since this gives $v(H) > 0$ we are in Case 1 on the next iteration.

Case 4: $w = (0,1,1,2)$. We see from the table that $\langle e_{12}, e_{13} \rangle \subset \ker \overline{H}$ and so $r \leqslant 4$. If $r = 4$ then Step 5 directly applies Operation 1 or Operation 3. Then on the next iteration either $(0,0,0,1)$ or $(0,1,1,1)$ is admissible, which means we are in Case 2 or its dual. If $r \leqslant 3$ then by applying a block diagonal element of $\mathrm{GL}_4(\mathcal{O}_K)$ with blocks of sizes 1, 2 and 1, we may suppose that $H_{35} \equiv H_{45} \equiv 0 \pmod{\pi}$. If $r = 3$ then $\ker \overline{H} = \langle e_{12}, e_{13}, a e_{23} + b e_{14} \rangle$ for some $a, b \in k$. If $a = 0$ or $b = 0$ then $\ker \overline{H}$ is isotropic for G. Otherwise $\langle e_{12}, e_{13} \rangle$ is the unique codimension 1 isotropic subspace. Either way, Step 5 directly applies Operation 1 or Operation 3, and we are done as before.

We now suppose that $r \leqslant 2$ and divide into the following cases.

- Suppose that $H_{36} \not\equiv 0 \pmod{\pi}$ and $H_{46} \not\equiv 0 \pmod{\pi}$. Since $r \leqslant 2$ we have $\overline{H} = \ell z_{34}$ for some linear form ℓ. Since there is no integral change of coordinates taking ℓ to z_{34} the only possible outcome of Step 4 is to directly apply Operation 2. This brings us to Case 3.
- Suppose that $H_{36} \equiv 0 \pmod{\pi}$ and $H_{46} \not\equiv 0 \pmod{\pi}$. Then $v(H_{33}) = 1$, otherwise we would be in Case 2. We again have $\overline{H} = \ell z_{34}$ for some linear form ℓ. Although there does now exist an integral change of coordinates taking ℓ to z_{34}, following this up with Operation 2 does not preserve that $v(H) \geqslant 0$. So again the only possible outcome of Step 4 is to directly apply Operation 2. This brings us to Case 3.
- Suppose that $H_{36} \not\equiv 0 \pmod{\pi}$ and $H_{46} \equiv 0 \pmod{\pi}$. This is essentially the same as the previous case by duality.
- Suppose that $H_{36} \equiv H_{46} \equiv 0 \pmod{\pi}$. Then $\overline{H}$ is a quadratic form in z_{24} and z_{34} only. If this factors over k then either of the transformations in Step 4 brings us to Case 3. Otherwise we proceed to Step 5 which directly

applies Operation 1 or Operation 3. As before, this brings us to Case 2 or its dual.

Case 5: $w = (0,0,1,2)$. Applying a block diagonal element of $\mathrm{GL}_4(\mathcal{O}_K)$ with blocks of sizes 2, 1 and 1, we may suppose that $H_{26} \equiv 0 \pmod{\pi}$. Then $H_{36} \not\equiv 0 \pmod{\pi}$ (otherwise we would be in Case 2) and H_{44}, H_{45}, H_{55} cannot all vanish mod π (otherwise we would be in Case 3). Therefore $\langle e_{12}, e_{13} \rangle \subset \ker \overline{H}$ and $r = 3$ or 4. The only 3-dimensional isotropic subspaces for G that contain $\langle e_{12}, e_{13} \rangle$ are $\langle e_{12}, e_{13}, e_{23} \rangle$ and $\langle e_{12}, e_{13}, e_{14} \rangle$. Therefore one of the transformations considered in Step 5 is to directly apply Operation 1 or Operation 3 (the latter only being a possibility if $H_{44} \equiv 0 \pmod{\pi}$). It follows that at the next iteration we have $r \leqslant 2$, and so are in Case 4 or earlier.

Case 6: $w = (0,1,1,3)$. Applying a block diagonal element of $\mathrm{GL}_4(\mathcal{O}_K)$ with blocks of sizes 1, 2 and 1, we may suppose that $H_{15} \equiv 0 \pmod{\pi^2}$. We have $H_{44} \not\equiv 0 \pmod{\pi}$ (otherwise we would be in Case 4) and $H_{35} \not\equiv 0 \pmod{\pi}$ (otherwise we would be in Case 5). Therefore $\langle e_{12}, e_{13} \rangle \subset \ker \overline{H}$ and $r = 3$ or 4. Exactly as in Case 5 we find that at the next iteration we have $r \leqslant 2$, and so are in Case 4 or earlier.

Case 7: $w = (0,1,2,3)$. We have $H_{26} \not\equiv 0 \pmod{\pi}$ (otherwise we would be in Case 4), and H_{35}, H_{45}, H_{55} cannot all vanish mod π (otherwise we would be in Case 3). Therefore $r = 3$ or 4, and $\langle e_{12} \rangle \subset \ker \overline{H} \subset \langle e_{12}, e_{13}, e_{23}, e_{14} \rangle$.

If $r = 4$ then $\ker \overline{H} = \langle e_{12}, ae_{13} + be_{23} + ce_{14} \rangle$ for some $a, b, c \in k$. If $b, c \neq 0$ then $\langle e_{12} \rangle$ is the unique codimension 1 subspace of $\ker \overline{H}$ that is isotropic for G. Therefore, Step 5 directly applies Operation 2, which brings us to Case 4. If $b = 0$ then $c \neq 0$, and by applying a block diagonal element of $\mathrm{GL}_4(\mathcal{O}_K)$ with blocks of sizes 1, 1 and 2, we may suppose that $a = 0$. Then the 3-dimensional isotropic subspaces for G containing $\ker \overline{H} = \langle e_{12}, e_{14} \rangle$ are $\langle e_{12}, e_{13}, e_{14} \rangle$ and $\langle e_{12}, e_{14}, e_{24} \rangle$. Step 5 applies either $\mathrm{Diag}(1, \pi, \pi, \pi)$ or $\mathrm{Diag}(1, 1, \pi, 1)$ bringing us to Case 5 or Case 6. The case $c = 0$ is similar by duality.

If $r = 3$ then $\ker \overline{H} = \langle e_{12}, e_{23} + ae_{13}, e_{14} + be_{13} \rangle$ for some $a, b \in k$. By applying a block diagonal element of $\mathrm{GL}_4(\mathcal{O}_K)$ with blocks of sizes 2 and 2, we may suppose that $a = b = 0$. Then $H_{35} \equiv H_{36} \equiv H_{45} \equiv H_{46} \equiv 0 \pmod{\pi}$ and $H_{55} \not\equiv 0 \pmod{\pi}$. The codimension 1 subspaces of $\ker \overline{H} = \langle e_{12}, e_{23}, e_{14} \rangle$ that are isotropic for G are $\langle e_{12}, e_{23} \rangle$ and $\langle e_{12}, e_{14} \rangle$. The 3-dimensional isotropic subspaces for G containing one of these spaces are

$$\langle e_{12}, e_{13}, e_{23} \rangle, \quad \langle e_{12}, e_{13}, e_{14} \rangle, \quad \langle e_{12}, e_{23}, e_{24} \rangle, \quad \langle e_{12}, e_{14}, e_{24} \rangle.$$

The first two of these correspond to directly applying Operation 1 or Operation 3, which brings us to Case 5 or its dual. The last two correspond to transformations which fail to preserve that $v(H) \geqslant 0$, and so cannot be selected by Step 5.

Case 8: $w = (0, 1, 2, 4)$. We have $H_{35} \not\equiv 0 \pmod{\pi}$ (otherwise we would be in Case 5), $H_{26} \not\equiv 0 \pmod{\pi}$ (otherwise we would be in Case 6), and $H_{44} \not\equiv 0 \pmod{\pi}$ (otherwise we would be in Case 7). Therefore $r = 5$ and $\ker \overline{H} = \langle e_{12} \rangle$. Step 5 directly applies Operation 2 which brings us to Case 6.

Example 5.2. We give three examples where Algorithm 2.4 takes the maximum of 4 iterations to give $v(H) > 0$. The first two examples start in Case 7, with $\operatorname{rank} \overline{H} = 3$ or 4, and the final one starts in Case 8. In the first two examples there are two choices on the first iteration. We made an arbitrary choice in each case, but in fact with the other choices the algorithm would still have taken 4 iterations.

Let $K = \mathbb{Q}$ and $v = v_p$ for any choice of prime number p. An arrow labelled $(w_1, \ldots, w_4)$ indicates that we replace H by $\frac{1}{\det P} H \circ \wedge^2 P$ where $P = \operatorname{Diag}(p^{w_1}, \ldots, p^{w_4})$.

$$\begin{aligned} p^5 z_{12}^2 + z_{13}z_{34} + p z_{23}^2 + p z_{14}^2 + z_{24}^2 &\xrightarrow{(0,0,0,1)} p^4 z_{12}^2 + z_{13}z_{34} + z_{23}^2 + p^2 z_{14}^2 + p z_{24}^2 \\ &\xrightarrow{(0,0,1,0)} p^3 z_{12}^2 + p z_{13}z_{34} + p z_{23}^2 + p z_{14}^2 + z_{24}^2 \\ &\xrightarrow{(0,1,0,1)} p^3 z_{12}^2 + z_{13}z_{34} + p z_{23}^2 + p z_{14}^2 + p^2 z_{24}^2 \\ &\xrightarrow{(0,0,1,1)} p(z_{12}^2 + z_{13}z_{34} + z_{23}^2 + z_{14}^2 + p z_{24}^2). \end{aligned}$$

$$\begin{aligned} p^5 z_{12}^2 + z_{13}z_{34} + p z_{23}^2 + z_{14}z_{24} &\xrightarrow{(0,0,0,1)} p^4 z_{12}^2 + z_{13}z_{34} + z_{23}^2 + p z_{14}z_{24} \\ &\xrightarrow{(0,0,1,0)} p^3 z_{12}^2 + p z_{13}z_{34} + p z_{23}^2 + z_{14}z_{24} \\ &\xrightarrow{(0,1,0,1)} p^3 z_{12}^2 + z_{13}z_{34} + p z_{23}^2 + p z_{14}z_{24} \\ &\xrightarrow{(0,0,1,1)} p(z_{12}^2 + z_{13}z_{34} + z_{23}^2 + z_{14}z_{24}). \end{aligned}$$

$$\begin{aligned} p^6 z_{12}^2 + z_{13}z_{34} + z_{23}z_{24} + z_{14}^2 &\xrightarrow{(0,0,1,1)} p^4 z_{12}^2 + p z_{13}z_{34} + z_{23}z_{24} + z_{14}^2 \\ &\xrightarrow{(0,0,0,1)} p^3 z_{12}^2 + p z_{13}z_{34} + z_{23}z_{24} + p z_{14}^2 \\ &\xrightarrow{(0,1,0,1)} p^3 z_{12}^2 + z_{13}z_{34} + p z_{23}z_{24} + p z_{14}^2 \\ &\xrightarrow{(0,0,1,1)} p(z_{12}^2 + z_{13}z_{34} + z_{23}z_{24} + z_{14}^2). \end{aligned}$$

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 Institute of Fundamental Research, Stud. Math. **22**, Mumbai, 2013.

[BSD] B.J. Birch and H.P.F. Swinnerton-Dyer, Notes on elliptic curves. I, *J. reine angew. Math.* **212** (1963), 7–25.

[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/`

[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.

[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.

[ES] A.-S. Elsenhans and M. Stoll, *Minimization of hypersurfaces*, preprint, 2021, `https://arxiv.org/abs/2110.04625`

[F] T.A. Fisher, Minimisation and reduction of 5-coverings of elliptic curves, *Algebra & Number Theory* **7** (2013), no. 5, 1179–1205.

[FR] T.A. Fisher and L. Radičević, Some minimisation algorithms in arithmetic invariant theory, *J. Théor. Nombres Bordeaux* **30** (2018), no. 3, 801–828.

[FY] T.A. Fisher and J. Yan, *Computing the Cassels-Tate pairing on the 2-Selmer group of a genus 2 Jacobian*, preprint, 2023, `https://arxiv.org/abs/2306.06011`

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

[K] J. Kollár, Polynomials with integral coefficients, equivalent to a given polynomial, *Electron. Res. Announc. Amer. Math. Soc.* **3** (1997), 17–27.

[L] Q. Liu, *Computing minimal Weierstrass equations*, preprint, 2022, `https://arxiv.org/abs/2209.00469`

[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.

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

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

Harvard University, Department of Mathematics, Science Center Room 325, 1 Oxford Street, Cambridge, MA 02138, USA

Email address: `aliu@math.harvard.edu`