MINIMISATION AND REDUCTION OF 2-, 3- AND 4-COVERINGS OF ELLIPTIC CURVES

J.E. CREMONA, T.A. FISHER, AND M. STOLL

ABSTRACT. In this paper we consider models for genus one curves of degree n for $n = 2$, 3 and 4, which arise in explicit n-descent on elliptic curves. We prove theorems on the existence of minimal models with the same invariants as the minimal model of the Jacobian elliptic curve and provide simple algorithms for minimising a given model, valid over general number fields. Finally, for genus one models defined over $\mathbb{Q}$, we develop a theory of reduction and again give explicit algorithms for $n = 2$, 3 and 4.

CONTENTS

Date: 12th August 2009.

1. Introduction

Let E be an elliptic curve defined over a number field K. An n-descent on E computes the n-Selmer group of E, which parametrises the everywhere locally soluble n-coverings of E up to isomorphism. An *n-covering of E* is a principal homogeneous space C for E, together with a map $\pi : C \to E$ that fits into a commutative diagram

$$\begin{tikzcd} C \arrow[d, dashed, "\psi"'] \arrow[dr, "\pi"] & \\ E \arrow[r, "\cdot n"] & E \end{tikzcd}$$

where $\psi : C \to E$ is an isomorphism defined over the algebraic closure $\overline{K}$, compatible with the structure of C as a principal homogeneous space. In a series of papers [CFOSS], it is shown how to produce explicit equations of covering curves from a more abstract representation of the Selmer group. (The latter is computed, at least for n prime, in [ScSt].)

In general, an n-covering C can be realised as a smooth curve of degree n inside a Severi-Brauer variety S of dimension $n-1$ (when $n=2$, we obtain a double cover of a conic instead of an embedding). If C has points everywhere locally, as will be the case when C represents an element of the n-Selmer group of E, then the same statement is true of S, and hence $S \cong \mathbb{P}^{n-1}$, so that C has a degree-n model in projective space. Thus, for $n = 2$, we get a double cover of $\mathbb{P}^1$ ramified in four points, for $n = 3$, we get a plane cubic curve, and for $n = 4$, we get an intersection of two quadrics in $\mathbb{P}^3$. For larger n, these models are no longer complete intersections, but can be given by a number of quadratic equations.

In this paper, we will focus on the problem of how to produce "nice" models of the covering curves, i.e., models given by equations with small integral coefficients, in the cases $n = 2$, 3 and 4. The advantage of having such a nice model is two-fold. On the one hand, rational points on the covering curve can be expected to be of smaller height on a model with small coefficients, and therefore will be found more easily. On the other hand, if no rational points are found, one would like to use the covering curve as the basis for a further descent, and the necessary computations are greatly facilitated when the given model is nice.

This problem naturally splits into two parts: *Minimisation* and *Reduction*. Minimisation makes the invariants of the model smaller by eliminating spurious bad primes and reducing the exponents of primes of bad reduction, to obtain a "minimal model". We prove the following theorem. (See Section 2 for the definitions of models for n-coverings and their invariants.)

Theorem 1.1. *Let $n = 2, 3$ or 4. Let K be a number field of class number one, and E an elliptic curve defined over K. If $\mathcal{C}$ is an n-covering of E which is everywhere locally soluble (i.e. $\mathcal{C}$ has points over all completions of K) then $\mathcal{C}$ has* *a model with integral coefficients and the same discriminant as a global minimal Weierstrass equation for E.*

By contrast, reduction attempts to reduce the size of the coefficients by an invertible integral (i.e., unimodular) linear change of coordinates, which leaves the invariants unchanged. Both processes are necessary to obtain a nice model: minimisation without reduction will provide a model with small invariants, but most likely rather large coefficients, whereas reduction without minimisation will not be able to make the coefficients really small, since the invariants will still be large.

After introducing the kinds of models we will be using and their invariants in Section 2, we state our main results on minimisation over local fields in Section 3.1, and discuss how they relate to earlier work. The most important of these results (the Minimisation Theorem, Theorem 3.4) is proved in Section 3.2. The proof is short and transparent, but is not algorithmic. We remedy this in Section 4 where we give practical algorithms for computing minimal models, that may be seen as generalising Tate's algorithm [Ta]. In Section 4.5 we deduce Theorem 1.1 from our local results, and explain how it may be generalised to arbitrary number fields. Moreover, as our local minimisation results make no restriction on the characteristic of the local field, they have more general global applications; in particular, one obtains results over function fields as well as number fields.

The algorithms of Section 4 may be combined with the Minimisation Theorem to prove the Strong Minimisation Theorem (Theorem 3.5 (i)). This states that if an n-covering of E (defined over a local field, and represented by a degree-n model) is soluble over the maximal unramified extension, then it has a model with integral coefficients and the same discriminant as a minimal Weierstrass equation for E. In Section 5 we prove the converse (Theorem 3.5 (ii)), thereby showing that the Strong Minimisation Theorem is best possible.

In Section 6 we discuss reduction for general n-coverings, and more specifically for $n = 2$, 3 and 4. Our results for reduction only cover the case where the ground field is $\mathbb{Q}$. A comparable theory of reduction over a general number field would be very useful in practice, but has not yet been sufficiently developed. We end in Section 7 by giving some examples of both minimisation and reduction (over $K = \mathbb{Q}$). All our algorithms (for $n = 2, 3, 4$ and $K = \mathbb{Q}$) have been implemented in (and contributed to) MAGMA (see [M]).

As stated earlier, the main application of our results is in explicit n-descent on elliptic curves over number fields. Minimisation and reduction of binary quartics is also used in the invariant theory method for 2-descent (see [BSD] and [Cr1]). For $n = 3$, Djabri and Smart in their ANTS III article [DS] consider the possibility of carrying out 3-descent using invariant theory in a similar way; one stumbling-block there was the inability to minimise plane cubic models for 3-coverings.

2. Genus one models

In this section, we specify the models of the covering curves that we will use, together with their invariants c_4, c_6, and Δ. For completeness and later reference we include the case $n = 1$. Note that we use the term "genus one model" to include singular models, which do not define curves of genus one.

Definition 2.1. A *Weierstrass equation*, or *genus one model of degree 1*, is an equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2.1}$$

The space of all Weierstrass equations with coefficients $a_1, \ldots, a_6$ in a ring R will be denoted $X_1(R)$. We say that two such models are *R-equivalent* if they are related by substitutions

$$x \leftarrow u^2x + r \qquad y \leftarrow u^3y + u^2sx + t \tag{2.2}$$

for some $u \in R^\times$ and $r, s, t \in R$. We write $\mathcal{G}_1(R)$ for the group of all transformations $[u; r, s, t]$ and define $\det([u; r, s, t]) = u^{-1}$. The invariants c_4, c_6 and Δ are certain primitive polynomials in $a_1, \ldots, a_6$ with integer coefficients, satisfying $c_4^3 - c_6^2 = 1728\Delta$ (see e.g. [Sil1, Chapter III]).

Definition 2.2. A *genus one model of degree 2*, or *generalised binary quartic*, is an equation of the form

$$y^2 + P(x, z)y = Q(x, z)$$

where P and Q are homogeneous polynomials of degrees 2 and 4. We sometimes abbreviate this as (P, Q). The space of all such models with coefficients in a ring R is denoted $X_2(R)$. Two such models are *R-equivalent* if they are related by substitutions $x \leftarrow m_{11}x+m_{21}z$, $z \leftarrow m_{12}x+m_{22}z$ and $y \leftarrow \mu^{-1}y+r_0x^2+r_1xz+r_2z^2$ for some $\mu \in R^\times$, $r = (r_0, r_1, r_2) \in R^3$ and $M = (m_{ij}) \in \mathrm{GL}_2(R)$. We write $\mathcal{G}_2(R)$ for the group of all such transformations $[\mu, r, M]$, and define $\det([\mu, r, M]) = \mu \det(M)$.

A generalised binary quartic $y^2+P(x_1, x_2)y = Q(x_1, x_2)$ over a field K defines a subscheme $\mathcal{C}_{(P,Q)} \subset \mathbb{P}(1, 1, 2)$, the ambient space being a weighted projective space with coordinates x_1, x_2, y. The model $\Phi = (P, Q)$ is *K-soluble* if $\mathcal{C}_\Phi(K) \neq \emptyset$.

The binary quartic $F(x, z) = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4$ has invariants $c_4(F) = 2^4I$ and $c_6(F) = 2^5J$, where I and J are given by

$$\begin{aligned} I &= 12ae - 3bd + c^2, \\ J &= 72ace - 27ad^2 - 27b^2e + 9bcd - 2c^3. \end{aligned}$$

The discriminant $\Delta = (c_4^3 - c_6^2)/1728$ is 16 times the usual discriminant of a quartic polynomial. The invariants of a generalised binary quartic are obtained by completing the square, *i.e.* $c_4(P,Q) = c_4(\frac{1}{4}P^2 + Q)$ and so on. We find that c_4, c_6 and Δ are primitive integer coefficient polynomials in the coefficients of P and Q, again satisfying $c_4^3 - c_6^2 = 1728\Delta$.

Earlier work on 2-coverings, including [BSD] and [SC1], used the more restrictive binary quartic models with $P = 0$. We use generalised binary quartics here, in order to obtain more uniform local results at places with residue characteristic 2.

Definition 2.3. A *genus one model of degree 3* is a ternary cubic. We write $X_3(R)$ for the space of all ternary cubics with coefficients in a ring R. Two such models are *R-equivalent* if they are related by multiplying by $\mu \in R^\times$ and then substituting $x_j \leftarrow \sum_{i=1}^3 m_{ij}x_i$ for some $M = (m_{ij}) \in \mathrm{GL}_3(R)$. We write $\mathcal{G}_3(R) = R^\times \times \mathrm{GL}_3(R)$ for the group of all such transformations $[\mu, M]$, and define $\det([\mu, M]) = \mu \det(M)$.

A ternary cubic $F(x,y,z)$ over a field K defines a subscheme $\mathcal{C}_F \subset \mathbb{P}^2$. The model F is *K-soluble* if $\mathcal{C}_F(K) \neq \emptyset$.

The invariants c_4 and c_6 may be defined as follows. Let

$$H(F) = \det \begin{pmatrix} F_{xx} & F_{xy} & F_{xz} \\ F_{yx} & F_{yy} & F_{yz} \\ F_{zx} & F_{zy} & F_{zz} \end{pmatrix}$$

be the *Hessian* of F, which is again a ternary cubic. Then we have

$$H(H(F)) = 48\, c_4(F)^2 F + 16\, c_6(F) H(F)\,;$$

the sign of $c_4(F)$ is fixed by requiring that $\Delta = (c_4^3 - c_6^2)/1728$ has integer coefficients. Then c_4, c_6 and Δ are primitive integer coefficient polynomials in the coefficients of F and satisfy $c_4^3 - c_6^2 = 1728\Delta$.

Definition 2.4. A *genus one model of degree 4*, or *quadric intersection*, is an ordered pair (Q_1, Q_2) of quadrics (homogeneous polynomials of degree 2) in four variables. The space of all such models with coefficients in a ring R is denoted $X_4(R)$. Quadric intersections (Q_1, Q_2) and (Q_1', Q_2') are *R-equivalent* if they are related by putting $Q_1' = m_{11}Q_1 + m_{12}Q_2$ and $Q_2' = m_{21}Q_1 + m_{22}Q_2$ for some $M = (m_{ij}) \in \mathrm{GL}_2(R)$ and then substituting $x_j \leftarrow \sum_{i=1}^4 n_{ij}x_i$ for some $N = (n_{ij}) \in \mathrm{GL}_4(R)$. We write $\mathcal{G}_4(R) = \mathrm{GL}_2(R) \times \mathrm{GL}_4(R)$ for the group of all such transformations $[M, N]$, and define $\det([M,N]) = \det(M)\det(N)$.

A quadric intersection $\Phi = (Q_1, Q_2)$ over a field K defines a subscheme $\mathcal{C}_\Phi \subset \mathbb{P}^3$. The model Φ is *K-soluble* if $\mathcal{C}_\Phi(K) \neq \emptyset$.

The invariants c_4 and c_6 may be defined as follows. Let A and B be the matrices of second partial derivatives of Q_1 and Q_2. Then $F(x,z) = \det(Ax + Bz)$

is a binary quartic. We define $c_4(Q_1, Q_2) = 2^{-4}c_4(F)$, $c_6(Q_1, Q_2) = 2^{-6}c_6(F)$ and $\Delta(Q_1, Q_2) = 2^{-12}\Delta(F)$. These scalings are chosen so that c_4, c_6 and Δ are primitive integer coefficient polynomials in the coefficients of Q_1 and Q_2. They satisfy $c_4^3 - c_6^2 = 1728\Delta$.

Earlier work on 4-coverings, including [Wo] and [Sik], used pairs of symmetric matrices rather than pairs of quadrics. We use quadrics here, in order to obtain more uniform local results at places with residue characteristic 2.

Remark 2.5. There is also a definition of *genus one model of degree* 5, see [Fi4]. The minimisation and reduction of these models (and possible extensions to larger n) will be the subject of future investigations.

Remark 2.6. There is a natural way in which we can re-write a Weierstrass equation (a genus one model of degree 1) as a genus one model of degree $n = 2, 3$ or 4 (see Lemma 3.11). We have normalised the invariants c_4, c_6 and Δ so that they agree with the usual formulae (see e.g. [Sil1, Chapter III]) when specialised to one of these 'Weierstrass models'.

Definition 2.7. Let K be a field and $\overline{K}$ its algebraic closure. Let $K[X_n]$ be the polynomial ring in the coefficients of a genus one model of degree n. A polynomial $F \in K[X_n]$ is an *invariant* of *weight* k if $F \circ g = \det(g)^k F$ for all $g \in \mathcal{G}_n(\overline{K})$.

For $n = 1, 2, 3, 4$ we defined polynomials $c_4, c_6, \Delta \in \mathbb{Z}[X_n]$ with $c_4^3 - c_6^2 = 1728\Delta$. These have the following properties.

Theorem 2.8. *Let* $n = 1, 2, 3$ *or* 4.

(i) *The polynomials* $c_4, c_6, \Delta \in K[X_n]$ *are invariants of weights* 4, 6 *and* 12.
(ii) *A genus one model* $\Phi \in X_n(K)$ *defines a smooth curve* $\mathcal{C}_\Phi$ *of genus one (over* $\overline{K}$*) if and only if* $\Delta(\Phi) \neq 0$.
(iii) *If* $\mathrm{char}(K) \neq 2, 3$ *then* c_4 *and* c_6 *generate the ring of invariants. Moreover if* $\Phi \in X_n(K)$ *with* $\Delta(\Phi) \neq 0$ *then the Jacobian of the curve* $\mathcal{C}_\Phi$ *has Weierstrass equation*

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

PROOF: The invariants c_4, c_6 and Δ were known to the nineteenth century invariant theorists. The observation that they give a formula for the Jacobian is due to Weil [We1], [We2]. See [AKM^{3}P] for a brief survey, or [Fi4] for a proof of the theorem exactly as it is stated here. □

As was first pointed out to us by Rodriguez-Villegas, it is possible to work back through Tate's formulaire (see e.g. [Sil1, Chapter III]) to write the invariants c_4 and c_6 in terms of polynomials $a_1, \ldots, a_6$.

Lemma 2.9. *There exist* $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}[X_n]$ *and* $b_2, b_4, b_6 \in \mathbb{Z}[X_n]$ *with*

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 & c_4 &= b_2^2 - 24b_4 \\ b_4 &= a_1 a_3 + 2a_4 & c_6 &= -b_2^3 + 36b_2b_4 - 216b_6. \\ b_6 &= a_3^2 + 4a_6 \end{aligned}$$

Proof: The lemma is proved by splitting into the cases $n = 2, 3, 4$ and giving explicit formulae for the a-invariants. (The case $n = 1$ is a tautology.)
Case $n = 2$. The a-invariants of the generalised binary quartic

$$y^2 + (lx^2 + mxz + nz^2)y = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4$$

are

$$\begin{aligned} a_1 &= m \\ a_2 &= c - ln \\ a_3 &= ld + nb \\ a_4 &= -4ae + bd - (l^2e + lnc + n^2a) \\ a_6 &= -4ace + ad^2 + b^2e - (l^2ce + m^2ae + n^2ac + lnbd) + lmbe + mnad. \end{aligned} \tag{2.3}$$

Case $n = 3$. The a-invariants of the ternary cubic

$$ax^3 + by^3 + cz^3 + a_2x^2y + a_3x^2z + b_1xy^2 + b_3y^2z + c_1xz^2 + c_2yz^2 + mxyz$$

are

$$\begin{aligned} a_1 &= m \\ a_2 &= -(a_2c_2 + a_3b_3 + b_1c_1) \\ a_3 &= 9abc - (ab_3c_2 + ba_3c_1 + ca_2b_1) - (a_2b_3c_1 + a_3b_1c_2) \\ a_4 &= -3(abc_1c_2 + acb_1b_3 + bca_2a_3) \\ &\quad + a(b_1c_2^2 + b_3^2c_1) + b(a_2c_1^2 + a_3^2c_2) + c(a_2^2b_3 + a_3b_1^2) \\ &\quad + a_2c_2a_3b_3 + b_1c_1a_2c_2 + a_3b_3b_1c_1 \\ a_6 &= -27a^2b^2c^2 + 9abc(ab_3c_2 + ca_2b_1 + ba_3c_1) + \ldots + abcm^3. \end{aligned} \tag{2.4}$$

These formulae in the case $n = 3$ were first given in [ARVT].
Case $n = 4$. Let $Q = \sum_{i \le j} c_{ij}x_ix_j$ be a quadric in 4 variables. Then

$$\det(\tfrac{\partial^2 Q}{\partial x_i \partial x_j}) = \mathrm{pf}(Q)^2 + 4\,\mathrm{rd}(Q)$$

where $\mathrm{pf}(Q) = c_{12}c_{34} + c_{13}c_{24} + c_{14}c_{23}$ and $\mathrm{rd}(Q) \in \mathbb{Z}[c_{11}, c_{12}, \ldots, c_{44}]$. We define the a-invariants of the quadric intersection (Q_1, Q_2) to be the a-invariants of the generalised binary quartic

$$y^2 + \mathrm{pf}(xQ_1 + zQ_2)y = \mathrm{rd}(xQ_1 + zQ_2).$$

$\square$

The polynomials a_i of Lemma 2.9 are far from unique. They can be modified by any transformation in $\mathcal{G}_1(\mathbb{Z}[X_n])$, i.e. by any transformation of the form $[\pm 1; r, s, t]$ with $r, s, t \in \mathbb{Z}[X_n]$. The following theorem extends Theorem 2.8(iii) to fields of arbitrary characteristic. (The reader only interested in applications over number fields and their completions, may safely skip this result.)

Theorem 2.10. *Let K be any field, and $n = 1, 2, 3$ or 4. For all $\Phi \in X_n(K)$ with $\Delta(\Phi) \neq 0$, the Jacobian of the curve $\mathcal{C}_\Phi$ has Weierstrass equation*

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \tag{2.5}$$

where $a_i = a_i(\Phi)$.

PROOF: For $n = 3$ this is a special case of a theorem of Artin, Rodriguez-Villegas and Tate [ARVT]. The cases $n = 2, 4$ may be proved using similar techniques. We sketch a simplified form of the proof, covering the cases $n = 2$, 3, and 4. (The case $n = 1$ is of course a tautology.)

Let C/S be the universal family over[1] $S = \mathrm{Spec}(\mathbb{Z}[X_n][\Delta^{-1}])$. By Theorem 2.8(ii) the fibres are smooth projective curves of genus one. Let J/S be the Jacobian of C/S, in the sense that J is the S-scheme representing the relative Picard functor $\mathrm{Pic}^0_{C/S}$; see [BLR, §9.3, Theorem 1]. Each fibre of J/S is the Jacobian of the corresponding fibre of C/S and hence an elliptic curve. By a generalisation of the usual procedure for putting an elliptic curve in Weierstrass form (see [De], or [ARVT, Theorem 2] for a further generalisation) J is defined as a subscheme of $\mathbb{P}^2_S$ by the homogenisation of

$$y^2 + a_1' xy + a_3' y = x^3 + a_2' x^2 + a_4' x + a_6' \tag{2.6}$$

for some $a_1', \dots, a_6' \in \mathbb{Z}[X_n][\Delta^{-1}]$. Thus for every field K, and every $\Phi \in X_n(K)$ with $\Delta(\Phi) \neq 0$, the Weierstrass equation (2.6) gives a model for the Jacobian of $\mathcal{C}_\Phi$.

It only remains to show that (2.5) and (2.6) are related by a transformation in $\mathcal{G}_1(R)$ where $R = \mathbb{Z}[X_n][\Delta^{-1}]$. By Theorem 2.8(iii) they are related by some $[u; r, s, t] \in \mathcal{G}_1(K)$ where $K = \mathbb{Q}(X_n)$. Since for any genus one model with $\Delta \neq 0$, (2.5) and (2.6) both specialise to a non-singular Weierstrass equation, it follows that $u \in R^\times$. Then, since R is integrally closed, a standard argument (see [Sil1, Chapter VII, Proposition 1.3]) shows that $r, s, t \in R$. □

We note that $a_1, \dots, a_6$ are not invariants in the sense of Definition 2.7. The ring of invariants when $\mathrm{char}(K) = 2$ or 3 is described in [Fi4, §10]. As is noted there, these do not give a formula for the Jacobian.

[1] In [ARVT] the authors work over $S = \mathrm{Spec}(\mathbb{Z}[X_3]) \setminus \{0\}$. This gives a more general result, but also makes the proof more difficult.

3. Minimisation theorems

3.1. **Statement of results.** Let K be a field with normalised discrete valuation $v : K^\times \to \mathbb{Z}$. We write $\mathcal{O}_K$ for the valuation ring (or ring of integers) of K and fix a uniformiser $\pi \in K$. We assume throughout that the residue field $k = \mathcal{O}_K/\pi\mathcal{O}_K$ is perfect. A field extension L/K is *unramified* if there is a (normalised) discrete valuation $w : L^\times \to \mathbb{Z}$ extending v. The strict Henselisation K^{sh} of K is an unramified extension of K that satisfies the conclusions of Hensel's lemma and has residue field $\overline{k}$, the algebraic closure of k. (See [Mi, Definition 4.18] for the precise definition.) If K is complete (with respect to v) then K^{sh} is the maximal unramified extension K^{nr} of K as defined in [Se, Chapter III, §5].

We work with genus one models of degree $n = 1, 2, 3$ or 4. The invariants c_4, c_6 and Δ of a genus one model were defined in Section 2.

Definition 3.1.

(i) A genus one model $\Phi \in X_n(K)$ is *non-singular* if $\Delta(\Phi) \neq 0$.
(ii) A genus one model $\Phi \in X_n(K)$ is *integral* if it has coefficients in $\mathcal{O}_K$.
(iii) A non-singular model $\Phi \in X_n(\mathcal{O}_K)$ is *minimal* if $v(\Delta(\Phi))$ is minimal among all integral models K-equivalent to Φ, otherwise Φ is *non-minimal*.

Algorithms for computing minimal models in the case $n = 1$ have been given by Tate [Ta], [Sil2, Chapter IV, §9] and Laska [La]. The latter can be refined using Kraus' conditions [Kr] as described in [Co, Chapter V] or [Cr1, §3.2]. (Laska's algorithm and its refinements are simpler than Tate's algorithm, but are only applicable when $\mathrm{char}(K) \neq 2, 3$.) In Section 4 we give algorithms for computing minimal models in the cases $n = 2, 3, 4$.

In the following lemma we define the *level* of a genus one model.

Lemma 3.2. *Let $\Phi \in X_n(K)$ be a non-singular model of degree n. Let Δ_E be the minimal discriminant of $E = \mathrm{Jac}(\mathcal{C}_\Phi)$. Then*

(i) *$v(\Delta(\Phi)) = v(\Delta_E) + 12\ell$ for some integer ℓ, called the* level *of Φ.*
(ii) *If $\mathrm{char}(k) \neq 2, 3$ then $\ell = \min\{\lfloor v(c_4(\Phi))/4 \rfloor, \lfloor v(c_6(\Phi))/6 \rfloor\}$.*
(iii) *The level of an integral model is always non-negative.*

Proof: If $\mathrm{char}(k) \neq 2, 3$ then this is clear by Theorem 2.8 and the standard formulae for transforming Weierstrass equations. In general (that is, to prove (iii) when $\mathrm{char}(k) = 2$ or 3, or even to define the level when $\mathrm{char}(K) = 2$ or 3) we use Lemma 2.9 and Theorem 2.10 instead. □

The level of $\Phi \in X_n(K)$ may be computed as $v(u)$ where $[u; r, s, t] \in \mathcal{G}_1(K)$ is a transformation that minimises the Weierstrass equation (2.5).

Definition 3.3. The *minimal level* of $\Phi \in X_n(K)$ is the minimum of the levels of all integral models K-equivalent to Φ. Thus an integral model Φ is minimal (see Definition 3.1) if and only if it has level equal to this minimal level.

If $n = 1$ then the minimal level is 0, for trivial reasons. So from now on we take $n = 2, 3$ or 4. The most important result on minimisation states that every K-soluble model has minimal level 0, or in other words, is K-equivalent to an integral model whose discriminant has the same valuation as the discriminant of a minimal model for the Jacobian elliptic curve.

Theorem 3.4 (Minimisation theorem). *Let $\Phi \in X_n(K)$ be non-singular. If $\mathcal{C}_\Phi(K) \neq \emptyset$ then Φ has minimal level 0.*

The following strengthening of the Minimisation Theorem shows that a non-singular model has minimal level 0 if and only if it is K^{sh}-soluble.

Theorem 3.5. *Let $\Phi \in X_n(K)$ be non-singular.*

(i) (Strong Minimisation Theorem). *If $\mathcal{C}_\Phi(K^{\mathrm{sh}}) \neq \emptyset$ then Φ has minimal level 0.*
(ii) (Converse Theorem). *If $\mathcal{C}_\Phi(K^{\mathrm{sh}}) = \emptyset$ then the minimal level is at least 1, and is equal to 1 if $\mathrm{char}(k) \nmid n$.*

Algorithms for minimising K-soluble binary quartics over $K = \mathbb{Q}_p$ are sketched by Birch and Swinnerton-Dyer [BSD, Lemmas 3,4,5], with details in the case $p \neq 2, 3$. Their algorithms give a proof of the Minimisation Theorem for $n = 2$, except when $p = 2$ (in which case further work is required to handle the "cross terms"). As pointed out in [SC1] this generalises immediately to any local field K with $\mathrm{char}(k) \neq 2, 3$. The authors extended these calculations to the case $n = 3$ in conjunction with their work on 3-descent [CFOSS]. The case $n = 4$ was treated by Womack in his PhD thesis [Wo, Section 2.5], using a method that goes via the results for $n = 2$.

In each case, the approach taken is to start with a K^{sh}-soluble model $\Phi \in X_n(\mathcal{O}_K)$ with $v(c_4(\Phi)) \geq 4$ and $v(c_6(\Phi)) \geq 6$, and then by a series of substitutions to show that Φ is K-equivalent to an integral model of smaller level. This leads to both a proof of the Strong Minimisation Theorem and a practical algorithm for minimising. However, this traditional approach suffers from the following drawbacks.

- It is necessary to split into a large number of (elementary yet tedious) cases, and the number of cases grows rapidly with n.
- The modifications required if $\mathrm{char}(k) = 2$ or 3 are somewhat involved. (The hypothesis that Φ has positive level has to made explicit using either Kraus' conditions [Kr] or the "a-invariants" defined in Lemma 2.9.)

We take a different approach, in which the tasks of proving the Minimisation Theorem and finding a practical algorithm for minimising are treated separately. A proof of the Minimisation Theorem for $n = 2, 3$ (in all residue characteristics) is given in [Fi2]. In Section 3.2 we simplify the proof and extend to the case $n = 4$. Unfortunately this approach does not lead to any readily implementable algorithm, nor does it prove the Strong Minimisation Theorem.

In Section 4.1 (case $n = 2$) and Section 4.2 (case $n = 3$) we specify a rather simple-minded procedure and show that, given any non-minimal integral model, iterating this procedure will eventually decrease the level. This gives an algorithm for computing minimal models. In Section 4.3 we give an algorithm in the case $n = 4$ based on the treatment in Womack's thesis. The algorithms for $n = 2, 4$ must be modified when the residue characteristic is 2, as described in Section 4.4. These modifications are required since, as noted in Section 2, our models for n-coverings differ slightly from those used previously in the literature. We have also defined the level, not in an absolute way, but by comparison with a minimal model for the Jacobian elliptic curve. The combined effect of these changes is that our results are much cleaner to state, in particular for residue characteristic 2, and can be proved uniformly, without assumptions on the ramification index.

As is the case for Tate's algorithm, it is clear from the form of our algorithms (for $n = 2, 3, 4$) that their success or otherwise is unchanged by an unramified field extension. We deduce the following.

Theorem 3.6. *The minimal level of a non-singular genus one model of degree $n = 2, 3$ or 4 is unchanged by an unramified field extension.*

The Strong Minimisation Theorem is then an immediate consequence of Theorem 3.6 and the Minimisation Theorem.

In Section 5 we show how to write down examples of minimal genus one models of positive level. We call the models arising in our construction *critical models*, see Definition 5.1 below. We show (for $n = 2, 3$) that any K^{sh}-insoluble model is K-equivalent to a critical model. There is a corresponding result for models of degree $n = 4$. The proof of the Converse Theorem (Theorem 3.5(ii)) is then reduced to a statement about the possible levels of a critical model (see Lemma 5.4).

Theorem 3.5 in the case $n = 2$ may already be found in [Liu, Remarque 21]. We claim that our proof is simpler, and in any case serves as a template for our generalisations to $n = 3, 4$. Liu also gives an algorithm for minimising [Liu, p.4594, Remarque 11] (still for $n = 2$), which although not made explicit appears to be the same as ours.

We remark that minimisations are not unique, in the sense that there can be more than one $\mathcal{O}_K$-equivalence class of minimal models K-equivalent to a given genus one model. Following on from our work and that of Liu, it will be explained in [Sa] how to compute the number of such classes.

For a more general, but necessarily less explicit, discussion of the problem of minimising homogeneous polynomials (of degree d in n variables) see [Ko].

3.2. **Proof of the minimisation theorem.** In this section only we relax our assumptions on $\mathcal{O}_K$ and K. It will only be necessary to assume that $\mathcal{O}_K$ is a principal ideal domain and K is its field of fractions. The definitions of a non-singular model and an integral model (see Definition 3.1) carry over as before. We consider models of degree $n = 2, 3$ or 4.

Let E be an elliptic curve over K, with identity $\mathcal{O}_E \in E(K)$, and let D be a K-rational divisor on E of degree n. We write $[D]$ for the linear equivalence class of D. We pick a basis $f_1, \ldots, f_n$ for the Riemann-Roch space $\mathcal{L}(D)$, and let $E \to \mathbb{P}^{n-1}$ be the morphism given by $P \mapsto (f_1(P) : \ldots : f_n(P))$. Then according as $n = 2, 3$ or 4, we find that E may be written as either a double cover of $\mathbb{P}^1$, a plane cubic, or an intersection of two quadrics in $\mathbb{P}^3$. It is therefore defined by a suitable genus one model $\Phi \in X_n(K)$. Moreover this model is uniquely determined up to K-equivalence by the pair $(E, [D])$: replacing D by an equivalent divisor or changing basis for the space $\mathcal{L}(D)$ only has the effect of a linear change of coordinates on $\mathbb{P}^{n-1}$, so only changes the genus one model by a K-equivalence. In this situation we say that the genus one model Φ *represents* the pair $(E, [D])$.

Similarly, we obtain a genus one model $\Phi \in X_n(K)$, well-defined up to K-equivalence, representing every pair $(\mathcal{C}, [D])$ where $\mathcal{C}$ is a genus one curve and D a divisor of degree n on $\mathcal{C}$; we have $\mathcal{C} \cong \mathcal{C}_\Phi$ (over K), and in particular, Φ is K-soluble if and only if $\mathcal{C}(K) \neq \emptyset$. Under this isomorphism, the divisor class $[D]$ on $\mathcal{C}$ maps to a distinguished divisor class $[D_\Phi]$ of degree n on $\mathcal{C}_\Phi$, namely the class of the fibres of the map $\mathcal{C}_\Phi \to \mathbb{P}^1$ if $n = 2$, or the hyperplane section if $n = 3, 4$.

The following is now immediate.

Lemma 3.7. *Every K-soluble non-singular genus one model represents a pair $(E, [D])$ in the manner described above.*

Proof: Let $\Phi \in X_n(K)$ be a non-singular genus one model. It is a tautology that Φ represents the pair $(\mathcal{C}_\Phi, [D_\Phi])$. Now if Φ is K-soluble then $\mathcal{C}_\Phi$ is a smooth curve of genus one with a rational point, and hence is an elliptic curve. □

The aim of this section is to prove the following theorem. The Minimisation Theorem (Theorem 3.4) is then an immediate consequence by Lemma 3.7.

Theorem 3.8. *Let E/K be an elliptic curve with integral Weierstrass equation*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{3.1}$$

and let $D \in \mathrm{Div}_K(E)$ be a divisor on E of degree $n = 2, 3$ or 4. Then $(E, [D])$ can be represented by an integral genus one model with the same discriminant as (3.1).

This theorem states that, in the K-equivalence class of genus one models representing $(E, [D])$, there is one which is integral and has the same discriminant as any given integral Weierstrass model for E. Our strategy for proving this starts with two observations.

Firstly, the claim really does only depend on the divisor class $[D]$ and not the given specific divisor D in that class, since the K-equivalence class of genus one models representing $(E, [D])$ only depends on the divisor class.

Secondly, if $\tau_Q : E \to E$ is translation by some point $Q \in E(K)$, then the pairs $(E, [D])$ and $(E, [\tau_Q^* D])$ determine K-equivalent genus one models. This follows from the fact that the map $E \to \mathbb{P}^{n-1}$ determined by $[\tau_Q^* D]$ is the composite of τ_Q and the map determined by $[D]$.

Using the classical facts that every K-rational divisor D of degree n is linearly equivalent to a unique divisor of the form $(n-1).\mathcal{O}_E + P$ for some $P \in E(K)$, and that divisors on an elliptic curve are linearly equivalent if and only if they have the same degree and the same sum, it suffices to prove Theorem 3.8 for such divisors as P runs over a set of coset representatives for $E(K)/nE(K)$.

In Lemmas 3.11 and 3.12 below, we show by means of explicit formulae that Theorem 3.8 holds in the cases $D = n.\mathcal{O}_E$ and $D = (n-1).\mathcal{O}_E + P$ where $P \in E(K)$ is an integral point, that is, a point with coordinates in $\mathcal{O}_K$. This is already enough to prove Theorem 3.8 in the case $\mathcal{O}_K$ is a complete discrete valuation ring with residue characteristic prime to n. Indeed, by the theory of formal groups, every non-zero element of $E(K)/nE(K)$ may then be represented by an integral point.

In general we rely on the following two lemmas, proved later in this section.

Lemma 3.9 (Unprojection lemma). *Let $D \in \mathrm{Div}_K(E)$ have degree 2 or 3, and let $P \in E(K)$. If Theorem 3.8 holds for D then it holds for $D + P$.*

Lemma 3.10 (Projection lemma). *Let $D \in \mathrm{Div}_K(E)$ have degree 3 or 4, and let $P \in E(K)$. If Theorem 3.8 holds for D then it holds for $D - P$.*

Theorem 3.8 may be deduced from these lemmas in more than one way. For example, if $n = 3$ or 4 then $D \sim (n-1).\mathcal{O}_E + P$ for some $P \in E(K)$. Then we quote the result for $D' = (n-1).\mathcal{O}_E$ and use the unprojection lemma. Likewise if $n = 2$ or 3 then $D \sim (n+1).\mathcal{O}_E - P$ for some $P \in E(K)$. Then we quote the result for $D' = (n+1).\mathcal{O}_E$ and apply the projection lemma to D'.

Theorem 3.8 in the case $D = n.\mathcal{O}_E$ follows from the formulae we used to normalise the invariants c_4, c_6 and Δ: see Remark 2.6.

Lemma 3.11. *Let E be an elliptic curve with Weierstrass equation*

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6. \tag{3.2}$$

Then the pair $(E, [n.\mathcal{O}_E])$ determines genus one models as follows:

$$\begin{aligned}
n = 2: &\quad y^2 + (a_1x_1x_2 + a_3x_2^2)y = x_1^3x_2 + a_2x_1^2x_2^2 + a_4x_1x_2^3 + a_6x_2^4;\\
n = 3: &\quad y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3 = 0;\\
n = 4: &\quad \left\{ \begin{array}{r} x^2 - zt = 0 \\ y^2 + a_1xy + a_3yz - xt - a_2x^2 - a_4xz - a_6z^2 = 0 \end{array} \right\}.
\end{aligned}$$

Moreover, each of these models has the same invariants c_4, c_6 and Δ as (3.2).

PROOF: In the case $n = 2$ we embed E in $\mathbb{P}(1, 1, 2)$ via $(x_1 : x_2 : y) = (X : 1 : Y)$. In the cases $n = 3, 4$ we embed E in $\mathbb{P}^{n-1}$ via $(z : x : y) = (1 : X : Y)$ and $(z : x : y : t) = (1 : X : Y : X^2)$ respectively. The statement about the invariants follows by direct calculation. □

Next we prove Theorem 3.8 in the case $D = (n - 1).\mathcal{O}_E + P$ where $P \in E(K)$ is an integral point. By a substitution $X \leftarrow X + X(P)$, $Y \leftarrow Y + Y(P)$ we may assume that P is the point $(0, 0)$.

Lemma 3.12. *Let E be an elliptic curve with Weierstrass equation*

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X \tag{3.3}$$

and let $P = (0, 0)$. Then the pair $(E, [(n - 1).\mathcal{O}_E + P])$ determines genus one models as follows:

$$\begin{aligned}
n = 2: &\quad y^2 + (-x_1^2 + a_1x_1x_2 + a_2x_2^2)y = -a_3x_1x_2^3 - a_4x_2^4;\\
n = 3: &\quad y^2z - x^2y + a_1xyz + a_2yz^2 + a_3xz^2 + a_4z^3 = 0;\\
n = 4: &\quad \left\{ \begin{array}{l} zt - xy + a_1yz + a_3z^2 = 0 \\ y^2 - xt + a_2yz + a_4z^2 = 0 \end{array} \right\}.
\end{aligned}$$

Moreover, each of these models has the same invariants c_4, c_6 and Δ as (3.3).

PROOF: The rational function

$$F = \frac{Y + a_1X + a_3}{X} = \frac{X^2 + a_2X + a_4}{Y}$$

belongs to the Riemann-Roch space $\mathcal{L}(\mathcal{O}_E + P)$. In the case $n = 2$ we embed E in $\mathbb{P}(1, 1, 2)$ via $(x_1 : x_2 : y) = (F : 1 : X)$. In the cases $n = 3, 4$ we embed E in $\mathbb{P}^{n-1}$ via $(z : x : y) = (1 : F : X)$ and $(z : x : y : t) = (1 : F : X : Y)$ respectively. The statement about the invariants follows by direct calculation. □

It remains to prove Lemmas 3.9 and 3.10. One observation that we use in the proofs is the following.

Lemma 3.13. *The group $\mathrm{SL}_n(\mathcal{O}_K)$ acts transitively on $\mathbb{P}^{n-1}(K)$.*

PROOF: Since $\mathcal{O}_K$ is a principal ideal domain this is standard. See for example [Ja, Exercise 6 on p.186]. □

The following lemma explains how to pass between results for generalised binary quartics (case $n = 2$) and ternary cubics (case $n = 3$).

Lemma 3.14. *Let $D \in \mathrm{Div}_K(E)$ be a divisor of degree 2 and let $P \in E(K)$. Let f_1, f_2, f_3 be binary forms over K with $\deg(f_i) = i$. The following statements are equivalent.*

(i) *The pair $(E, [D])$ is represented by the generalised binary quartic*

$$y^2 + f_2(x_1, x_2)y = f_1(x_1, x_2)f_3(x_1, x_2) \tag{3.4}$$

and P is the point defined by $f_1 = y = 0$.

(ii) *The pair $(E, [D + P])$ is represented by the ternary cubic*

$$f_1(X, Z)Y^2 - f_2(X, Z)Y - f_3(X, Z) = 0 \tag{3.5}$$

and P is the point $(X : Y : Z) = (0 : 1 : 0)$.

PROOF: We first show that the curves C_2 and C_3 defined by (3.4) and (3.5) are isomorphic. An isomorphism $\phi : C_2 \to C_3$ is given by

$$\begin{aligned}\phi : (x_1 : x_2 : y) \mapsto (X : Y : Z) &= (x_1 f_1(x_1, x_2) : y + f_2(x_1, x_2) : x_2 f_1(x_1, x_2)) \\ &= (x_1 y : f_3(x_1, x_2) : x_2 y)\end{aligned}$$

with inverse

$$\phi^{-1} : (X : Y : Z) \mapsto (x_1 : x_2 : y) = (X : Z : f_1(X, Z)Y - f_2(X, Z)).$$

The isomorphism identifies the points $\{f_1 = y = 0\} \in C_2(K)$ and $(0 : 1 : 0) \in C_3(K)$. To prove the equivalence of (i) and (ii) we note that if $D = P_1 + P_2$ is a fibre of the map $C_2 \to \mathbb{P}^1$; $(x_1 : x_2 : y) \mapsto (x_1 : x_2)$ then the points $\phi(P_1), \phi(P_2)$ and $(0 : 1 : 0)$ are collinear on $C_3 \subset \mathbb{P}^2$. □

There is an entirely analogous result for passing between ternary cubics (case $n = 3$) and quadric intersections (case $n = 4$).

Lemma 3.15. *Let $D \in \mathrm{Div}_K(E)$ be a divisor of degree 3 and let $P \in E(K)$. Let ℓ_1, ℓ_2, q_1, q_2 be ternary forms over K with $\deg(\ell_i) = 1$ and $\deg(q_i) = 2$. The following statements are equivalent.*

(i) *The pair $(E, [D])$ is represented by the ternary cubic*

$$\ell_1(x_1, x_2, x_3)q_2(x_1, x_2, x_3) - \ell_2(x_1, x_2, x_3)q_1(x_1, x_2, x_3) = 0 \tag{3.6}$$

and P is the point defined by $\ell_1 = \ell_2 = 0$.

(ii) *The pair* $(E, [D+P])$ *is represented by the quadric intersection*

$$\begin{aligned} \ell_1(x_1,x_2,x_3)x_4 + q_1(x_1,x_2,x_3) = 0 \\ \ell_2(x_1,x_2,x_3)x_4 + q_2(x_1,x_2,x_3) = 0 \end{aligned} \tag{3.7}$$

and P *is the point* $(x_1 : x_2 : x_3 : x_4) = (0 : 0 : 0 : 1)$.

Proof: We first show that the curves C_3 and C_4 defined by (3.6) and (3.7) are isomorphic. An isomorphism $\phi : C_3 \to C_4$ is given by

$$\phi : (x_1 : x_2 : x_3) \mapsto (x_1\ell_1 : x_2\ell_1 : x_3\ell_1 : -q_1) = (x_1\ell_2 : x_2\ell_2 : x_3\ell_2 : -q_2)$$

with inverse

$$\phi^{-1} : (x_1 : x_2 : x_3 : x_4) \mapsto (x_1 : x_2 : x_3).$$

This isomorphism identifies the points $\{\ell_1 = \ell_2 = 0\} \in C_3(K)$ and $(0 : 0 : 0 : 1) \in C_4(K)$. To prove the equivalence of (i) and (ii) we note that if $C_3 \subset \mathbb{P}^2$ meets some line in the divisor $D = P_1 + P_2 + P_3$ then the points $\phi(P_1), \phi(P_2), \phi(P_3)$ and $(0 : 0 : 0 : 1)$ are coplanar on $C_4 \subset \mathbb{P}^3$. □

A generic computation shows that the genus one models (3.4) and (3.5) in Lemma 3.14 have the same discriminant. Likewise the models (3.6) and (3.7) in Lemma 3.15 have the same discriminant.

Proof of Lemma 3.9: (i) Let $D \in \mathrm{Div}_K(E)$ be a divisor of degree 2, and suppose the pair $(E, [D])$ is represented by an integral generalised binary quartic of discriminant Δ. By Lemma 3.13 (with $n = 2$) we may assume that P is the point $(x_1 : x_2 : y) = (1 : 0 : \eta)$ for some $\eta \in K$. Since $\mathcal{O}_K$ is integrally closed it follows that $\eta \in \mathcal{O}_K$. By making a substitution $y \leftarrow y + \eta x_1^2$ we may assume that $\eta = 0$. Our model is now of the form (3.4) with $f_1(x_1, x_2) = x_2$. Then the ternary cubic (3.5) is an integral model of discriminant Δ representing the pair $(E, [D+P])$.
(ii) Let $D \in \mathrm{Div}_K(E)$ be a divisor of degree 3, and suppose the pair $(E, [D])$ is represented by an integral ternary cubic of discriminant Δ. By Lemma 3.13 (with $n = 3$) we may assume that P is the point $(x_1 : x_2 : x_3) = (0 : 0 : 1)$. Our model is now of the form (3.6) with $\ell_1 = x_1$ and $\ell_2 = x_2$. We may choose the quadratic forms q_1 and q_2 to have coefficients in $\mathcal{O}_K$. Then the quadric intersection (3.7) is an integral model of discriminant Δ representing the pair $(E, [D+P])$. □

Proof of Lemma 3.10: (i) Let $D \in \mathrm{Div}_K(E)$ be a divisor of degree 3, and suppose the pair $(E, [D])$ is represented by an integral ternary cubic of discriminant Δ. By Lemma 3.13 (with $n = 3$) we may assume that P is the point $(x_1 : x_2 : x_3) = (0 : 0 : 1)$. Our model is now of the form (3.5). Then the generalised binary quartic (3.4) is an integral model of discriminant Δ representing the pair $(E, [D-P])$.
(ii) Let $D \in \mathrm{Div}_K(E)$ be a divisor of degree 4, and suppose the pair $(E, [D])$ is represented by an integral quadric intersection of discriminant Δ. By Lemma 3.13

(with $n = 4$) we may assume that P is the point $(x_1 : x_2 : x_3 : x_4) = (0 : 0 : 0 : 1)$ Our model is now of the form (3.7) for some forms ℓ_1, ℓ_2, q_1, q_2 with coefficients in $\mathcal{O}_K$. Then the ternary cubic (3.5) is an integral model of discriminant Δ representing the pair $(E, [D - P])$. $\square$

Remark 3.16. In principle these proofs give an algorithm for minimising K-soluble models, but only once a K-rational point is explicitly known. Although it is easy to decide solubility over local fields, such an algorithm would require that we find a local point to sufficiently high precision. Hence our comment that this is not a readily implementable algorithm.

4. Minimisation algorithms

In this section we give algorithms for minimising binary quartics (case $n = 2$), ternary cubics (case $n = 3$) and quadric intersections (case $n = 4$). As in Section 3.1 we work over a field K which is the field of fractions of a discrete valuation ring $\mathcal{O}_K$. There is no need to assume that K is complete (or even Henselian). We fix a uniformiser π and write $k = \mathcal{O}_K/\pi\mathcal{O}_K$ for the residue field. In the cases $n = 2, 4$ we initially assume that $\mathrm{char}(k) \neq 2$, leaving the case $\mathrm{char}(k) = 2$ to Section 4.4.

Our algorithms for $n = 2, 3$ share some common features which we now elucidate. In these cases we specify a procedure that takes as input an integral genus one model of positive level, and returns a K-equivalent integral model of the same or smaller level. We then show that if the model is non-minimal then the level must decrease after finitely many iterations, and give a bound N on the number of iterations required. This also gives a test for minimality: if N iterations of the procedure fail to decrease the level, then the model must be minimal.

The proofs are by induction on the *slope*, which we define as the least valuation of the determinant of a matrix $M \in \mathrm{GL}_n(K)$ with entries in $\mathcal{O}_K$ that can be used to decrease the level. The slope of a minimal model is undefined. The arguments we use are incapable of proving the Minimisation Theorem, since we assume at the outset that the given model has a slope, *i.e.* is non-minimal.

The following lemma is used to show that our procedure gives a well-defined map on $\mathcal{O}_K$-equivalence classes. This is useful, since it means we are free to replace our model by an $\mathcal{O}_K$-equivalent one at any stage of the proof. We write I_m for the m by m identity matrix.

Lemma 4.1. *Let $\mathrm{GL}_n(K)$ act on $\mathbb{P}^{n-1}$ in the natural way (via left multiplication of column vectors by matrices). Let $\alpha = \mathrm{Diag}(I_r, \pi I_{n-r})$ for some $0 < r < n$. Then the subgroup of $\mathrm{GL}_n(\mathcal{O}_K)$ consisting of transformations whose reduction mod π preserves the subspace $\{x_{r+1} = \ldots = x_n = 0\}$ is*

$$\mathrm{GL}_n(\mathcal{O}_K) \cap \alpha\, \mathrm{GL}_n(\mathcal{O}_K)\alpha^{-1}$$

Proof: Identifying $\mathbb{P}^{n-1}(K)$ with the non-zero elements of K^n modular scalars, $\mathrm{GL}_n(\mathcal{O}_K)$ is the subgroup preserving $\mathcal{O}_K^n$ and we are interested in the subgroup which also preserves $\mathcal{O}_K^r \oplus (\pi\mathcal{O}_K)^{n-r} = \alpha(\mathcal{O}_K^n)$. The statement is now clear. □

This lemma is used as follows. Suppose that Φ and Ψ are $\mathrm{GL}_n(\mathcal{O}_K)$-equivalent models, and the matrix relating them is one whose reduction mod π preserves the subspace $\{x_{r+1} = \ldots = x_n = 0\}$. Then the models Φ' and Ψ' obtained by applying $\alpha = \mathrm{Diag}(I_r, \pi I_{n-r})$ to both Φ and Ψ, will again be $\mathrm{GL}_n(\mathcal{O}_K)$-equivalent.

4.1. **Minimisation of 2-coverings.** Let $F \in K[x,z]$ be a binary quartic, say

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

Viewing the set of these as a subset of $X_2(K)$, the group of K-equivalences between binary quartics is $K^\times \times \mathrm{GL}_2(K)$, where $[\mu, M]$ acts as $[\mu, (0,0,0), M] \in \mathcal{G}_2(K)$. Note that $[\pi^{-2}, \pi I_2]$ acts trivially, so we may if convenient assume that M has entries in $\mathcal{O}_K$, not all in $\pi\mathcal{O}_K$.

We say that an integral binary quartic F is *minimal* if $v(\Delta(F))$ is minimal among all integral binary quartics K-equivalent to F. If $\mathrm{char}(k) = 2$ then this need not be the same as being minimal as a generalised binary quartic. We define the valuation $v(F)$ to be the minimum of the valuations of the coefficients. If $v(F) \geq 2$, then F is not minimal, and indeed dividing through by π^2 gives a K-equivalent integral model of smaller level. The algorithm for minimising binary quartics is described in the following theorem.

Theorem 4.2. *Let $F \in \mathcal{O}_K[x,z]$ be a non-singular binary quartic. Suppose that $v(F) = 0$ or 1, but F has positive level. If $\mathrm{char}(k) = 2$ then further assume that F is non-minimal. Then*

(i) *The reduction mod π of $F_1(x,z) = \pi^{-v(F)}F(x,z)$ has either a triple or quadruple root defined over k.*
(ii) *The following procedure replaces F by a K-equivalent integral model of the same level.*
  - *Move the repeated root of $F_1(x,z)$ mod π to $(x:z) = (0:1)$.*
  - *Replace $F(x,z)$ by $\pi^{-2}F(\pi x, z)$.*

(iii) *If F is non-minimal then the procedure in (ii) gives $v(F) \geq 2$ after at most 2 iterations.*

Proof: We first prove the theorem in the case F is non-minimal. By hypothesis there exists $[\mu, M] \in K^\times \times \mathrm{GL}_2(K)$ with $v(\mu \det(M)) \leq -1$ such that the transform of F by $[\mu, M]$ is still integral. The slope s of F is the least possible valuation of $\det M$, for M such a matrix with entries in $\mathcal{O}_K$. By Lemma 4.1 we are free to replace F by any $\mathcal{O}_K$-equivalent binary quartic. So, putting M in Smith normal form, we may assume that

$$F(\pi^s x, z) \equiv 0 \pmod{\pi^{2s+2}}$$

where s is the slope. For $s \geq 2$, this condition works out as $\pi^2 \,|\, c$, $\pi^{s+2} \,|\, d$ and $\pi^{2s+2} \,|\, e$. So the only possible slopes are $s = 0, 1, 2$ (as if these conditions hold for some $s > 2$, then they also hold for $s = 2$, and s was defined to be minimal). If $s = 0$, then $v(F) \geq 2$ contrary to hypothesis. If $s = 1$, then the coefficients of F have valuations satisfying

$$\geq 0 \quad \geq 1 \quad \geq 2 \quad \geq 3 \quad \geq 4.$$

So either $v(F) = 0$ and $F(x, z) \bmod \pi$ has a quadruple root at $(x : z) = (0 : 1)$, or $v(F) = 1$ and $\pi^{-1}F(x, z) \bmod \pi$ has a triple or quadruple root at $(x : z) = (0 : 1)$. If $s = 2$, then the coefficients of F have valuations satisfying

$$\geq 0 \quad = 0 \quad \geq 2 \quad \geq 4 \quad \geq 6.$$

Then $F(x, z) \bmod \pi$ has a triple root at $(0 : 1)$. In each of the cases $s = 1, 2$ statements (i) and (ii) of the theorem are now clear. Moreover the procedure in (ii) returns a K-equivalent integral model of smaller slope. Hence at most 2 iterations are required to give $v(F) \geq 2$, establishing (iii).

It remains to prove (i) and (ii) in the case $\mathrm{char}(k) \neq 2$ and F has positive level (but could be minimal). Statement (i) follows from the fact that $F_1 \bmod \pi$ is a null form, *i.e.* both the invariants I and J vanish. (Since k is perfect the multiple root is defined over k.) For (ii) we must show that if $v(F) = 0$ and the reduction of $F \bmod \pi$ has a repeated root at $(x : z) = (0 : 1)$ then $\pi^2 \,|\, e$. But in this case there are smooth $\overline{k}$-points on the reduction of $\mathcal{C} \bmod \pi$ where $\mathcal{C} = \{y^2 = F(x, z)\}$. So after an unramified extension we may assume that $\mathcal{C}(K) \neq \emptyset$. Then Theorem 3.4 shows that F is non-minimal, and our earlier argument applies. $\square$

To give a satisfactory analogue of this algorithm when $\mathrm{char}(k) = 2$ we must work with generalised binary quartics. We give details in Section 4.4.

4.2. **Minimisation of 3-coverings.** The valuation $v(F)$ of a ternary cubic

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

is the minimum valuation of a coefficient. If $v(F) \geq 1$ then F is non-minimal, and indeed dividing through by π gives a K-equivalent integral model of smaller level. The algorithm for minimising ternary cubics is described in the following theorem.

Theorem 4.3. *Let $F \in X_3(\mathcal{O}_K)$ be a non-singular ternary cubic. Suppose $v(F) = 0$, but F has positive level. Then*

(i) *The singular locus of the reduction*

$$\mathcal{S} = \{(x : y : z) \in \mathbb{P}^2 \mid F \equiv \tfrac{\partial F}{\partial x} \equiv \tfrac{\partial F}{\partial y} \equiv \tfrac{\partial F}{\partial z} \equiv 0 \pmod{\pi}\}$$

is either a point or a line, and is defined over k.

(ii) *The following procedure replaces F by a K-equivalent integral ternary cubic of the same level.*
- *Make a $\mathrm{GL}_3(\mathcal{O}_K)$-transformation to move the singular locus $\mathcal{S}$ to the point $(1:0:0)$, respectively the line $\{z=0\}$.*
- *Replace $F(x,y,z)$ by $\pi F(\pi^{-1}x,y,z)$, respectively $\pi^{-1}F(x,y,\pi z)$.*

(iii) *If F is non-minimal then the procedure in (ii) gives $v(F) \geq 1$ after at most 4 iterations.*

Proof: We are given that F has positive level. It follows that its reduction mod π is a null-form, *i.e.* the invariants c_4, c_6 and Δ all vanish. The classification of singular ternary cubics (up to equivalence over an algebraically closed field) is well known. See for example [Do, §10.3] or [Po]. The possible null-forms are either a cuspidal cubic, a line touching a conic, three lines through a common point, a double line and a line, or a triple line. So over $\overline{k}$ the singular locus of the reduction is either a point or a line. Since k is perfect, this point or line is already defined over k. This proves (i).

Next we prove (ii) and (iii) in the case F is non-minimal. By hypothesis there exists $[\mu, M] \in \mathcal{G}_3(K) = K^\times \times \mathrm{GL}_3(K)$ with $v(\mu \det M) \leq -1$ such that the transform of F by $[\mu, M]$ is still integral. Since $[\pi^{-3}, \pi I_3]$ acts trivially, we may assume that M has entries in $\mathcal{O}_K$. The slope s of F is the least possible valuation of $\det M$, for M such a matrix with entries in $\mathcal{O}_K$. By Lemma 4.1 we are free to replace F by any $\mathcal{O}_K$-equivalent ternary cubic. So, putting M in Smith normal form, we may assume that

$$F(x, \pi^a y, \pi^b z) \equiv 0 \pmod{\pi^{a+b+1}} \tag{4.1}$$

for some $0 \leq a \leq b$ with $a+b=s$. If $a=b=0$, then $v(F) \geq 1$, contrary to hypothesis. If $a=0$ and $b \geq 1$, then the reduction of F mod π only involves the monomials xz^2, yz^2 and z^3. Hence $\mathcal{S}$ is the line $\{z=0\}$. If $a \geq 1$, then the coefficients of x^3, x^2y and x^2z all vanish mod π. Hence $\mathcal{S}$ is either the point $(1:0:0)$ or a line through this point. In each of these cases it is clear that the procedure in (ii) returns an integral model of the same level and smaller slope. Moreover it gives $v(F) \geq 1$ after a finite number of iterations (bounded by the initial slope). The next lemma shows that the only possible slopes are $0,1,2,3$ and 5. Hence at most 4 iterations are required, establishing (iii).

It remains to prove (ii) in the case F has positive level (but could be minimal). We must show that if $(1:0:0)$ is the only singular point on the reduction then $F(1,0,0) \equiv 0 \pmod{\pi^2}$. But in this case there are smooth $\overline{k}$-points on the reduction. So after an unramified extension we may assume that $\mathcal{C}_F(K) \neq \emptyset$. Then Theorem 3.4 shows that F is non-minimal, and our earlier argument applies. □

We say that a pair (a,b) is *admissible* for F if (4.1) holds.

Lemma 4.4. *If some pair* (a, b) *with* $0 \le a \le b$ *is admissible for* F *then at least one of the pairs* $(0, 0)$, $(0, 1)$, $(1, 1)$, $(1, 2)$ *or* $(2, 3)$ *is admissible for* F.

Proof: Suppose (a, b) is admissible for F. We make the observations:

- If $a = 0$ and $b \ge 1$ then $(0, 1)$ is admissible.
- If $a = b \ge 1$ then $(1, 1)$ is admissible.
- If $a \ge 1$ and $b \ge 2a$ then $(1, 2)$ is admissible.
- If $a \ge 2$ and $b \ge a + 1$ then $(2, 3)$ is admissible.

The only remaining possibility is $(a, b) = (0, 0)$. □

Example 4.5. We apply our algorithm to a cuspidal cubic. (Although this is singular, there are π-adically close smooth ternary cubics that are treated in the same way by our algorithm.) An arrow labelled $(0, a, b)$ indicates that we make the transformation $[\pi^{-a-b}, \mathrm{Diag}(1, \pi^a, \pi^b)]$.

$$\begin{aligned} xz^2 - y^3 &\xrightarrow{(0,1,1)} xz^2 - \pi y^3 \\ &\xrightarrow{(0,0,1)} \pi x z^2 - y^3 \\ &\xrightarrow{(0,1,0)} xz^2 - \pi^2 y^3 \\ &\xrightarrow{(0,0,1)} \pi(xz^2 - y^3) \end{aligned}$$

So this is an example where our algorithm takes the maximum possible of 4 iterations to give $v(F) \ge 1$.

4.3. **Minimisation of 4-coverings.** In this section we prove Theorems 3.5(i) and 3.6 in the case $n = 4$, assuming that $\mathrm{char}(k) \ne 2$. The proofs are constructive and give an algorithm for minimising quadric intersections. The modifications required when $\mathrm{char}(k) = 2$ are described in the next section.

We define a map

$$\begin{aligned} \mathfrak{d} : X_4(K) &\to X_2(K) \\ (Q_1, Q_2) &\mapsto F(x, z) = \det(Ax + Bz) \end{aligned} \tag{4.2}$$

where A and B are the matrices of second partial derivatives of Q_1 and Q_2. As noted in Definition 2.4 we have $\Delta(Q_1, Q_2) = 2^{-12}\Delta(F)$.

Lemma 4.6. *Let* $(Q_1, Q_2) \in X_4(K)$ *be a non-singular quadric intersection. Then* $F = \mathfrak{d}(Q_1, Q_2)$ *is non-singular, and there is a morphism of genus one curves* $\mathcal{C}_{(Q_1,Q_2)} \to \mathcal{C}_F$ *defined over* K.

Proof: A formula for this morphism is given by classical invariant theory, as we now recall from [AKM^{3}P], [MSS]. We write the binary quartic $F = \mathfrak{d}(Q_1, Q_2)$ as

$F(x,z) = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4$, and let T_1 and T_2 be the quadrics whose matrices of second partial derivatives M_1 and M_2 are determined by

$$\operatorname{adj}\big(\operatorname{adj}(A)x + \operatorname{adj}(B)z\big) = a^2Ax^3 + aM_1x^2z + eM_2xz^2 + e^2Bz^3 \,. \tag{4.3}$$

Then $J^2 \equiv F(T_1, -T_2) \mod (Q_1, Q_2)$ where $J = \frac{1}{4}\frac{\partial(Q_1,Q_2,T_1,T_2)}{\partial(x_1,x_2,x_3,x_4)}$. □

Lemma 4.7. *If $[M,N] \in \mathcal{G}_4(K)$ then there is a commutative diagram*

$$\begin{array}{ccc} X_4(K) & \xrightarrow{[M,N]} & X_4(K) \\ \Big\downarrow{\scriptstyle \mathfrak{d}} & & \Big\downarrow{\scriptstyle \mathfrak{d}} \\ X_2(K) & \xrightarrow{[\det N, M]} & X_2(K). \end{array}$$

In particular $\mathfrak{d}$ induces a well-defined map on K-equivalence classes.

PROOF: This is clear. □

Following the treatment in Womack's thesis [Wo], we deduce the Minimisation Theorem for $n=4$ from the Minimisation Theorem for $n=2$. The modifications required to prove Theorems 3.5(i) and 3.6 are given at the end of this section (see Proposition 4.12 below).

Proposition 4.8. *If $(Q_1,Q_2) \in X_4(K)$ is non-singular and K-soluble then it is K-equivalent to an integral model of level* 0.

PROOF: Since (Q_1,Q_2) is K-soluble, it follows by Lemma 4.6 that $\mathfrak{d}(Q_1,Q_2)$ is K-soluble. So by the minimisation theorem for $n=2$ we know that $\mathfrak{d}(Q_1,Q_2)$ is K-equivalent to an integral binary quartic $F(x,z)$ of level 0. It is clear by Lemma 4.7 that (Q_1,Q_2) is K-equivalent to a quadric intersection (Q_1',Q_2') with $\mathfrak{d}(Q_1',Q_2') = F$. The following lemma shows we may take (Q_1',Q_2') integral. This is then the required integral model of level 0. □

Notice that the next three lemmas are false when $\operatorname{char}(k) = 2$, as we could otherwise use the above proof to find integral models of level $-v(2)$.

Lemma 4.9. *Let $(Q_1,Q_2) \in X_4(K)$ be a K-soluble non-singular quadric intersection. If $\mathfrak{d}(Q_1,Q_2)$ is integral then (Q_1,Q_2) is K-equivalent to an integral quadric intersection (Q_1',Q_2') with $\mathfrak{d}(Q_1',Q_2') = \mathfrak{d}(Q_1,Q_2)$.*

PROOF: By a transformation $[\mu I_2, I_4]$ for suitable $\mu \in \mathcal{O}_K$ we obtain an integral quadric intersection (Q_1',Q_2') with $\mathfrak{d}(Q_1',Q_2') = \mu^4\mathfrak{d}(Q_1,Q_2)$. We now apply the following lemma, as many times as required, at each stage preserving the integrality of (Q_1',Q_2') while dividing $\mathfrak{d}(Q_1',Q_2')$ by a square in $\pi\mathcal{O}_K$. □

Recall that we write $v(F)$ for the minimum of the valuations of the coefficients of the binary quartic F. The following is Womack's "main reduction lemma".

Lemma 4.10. *Let $(Q_1, Q_2) \in X_4(\mathcal{O}_K)$ be a non-singular K-soluble integral quadric intersection. If $F = \mathfrak{d}(Q_1, Q_2)$ satisfies $v(F) \geq 2$ then (Q_1, Q_2) is K-equivalent to an integral quadric intersection of smaller level by means of a transformation $[\lambda I_2, N] \in \mathcal{G}_4(K)$ with $\lambda \in K^\times$ and $N \in \mathrm{GL}_4(K)$.*

The following geometric lemma prepares for the proof of Lemma 4.10. We say that two pairs of quadratic forms in m variables are k-equivalent if they are in the same orbit for the natural action of $\mathrm{GL}_2(k) \times \mathrm{GL}_m(k)$. (This extends our earlier definition in the case $m = 4$.) Over an algebraically closed field, the lemma may alternatively be deduced from the classification of pairs of quadrics using the Segre symbol, as given in [HP, Chapter XIII, §11].

Lemma 4.11. *Let Q_1 and Q_2 be quadratic forms in $m = 3$ or 4 variables over a field k with $\mathrm{char}(k) \neq 2$. Let A and B be the matrices of second partial derivatives of Q_1 and Q_2. Assume that*

- *$\{Q_1 = Q_2 = 0\} \subset \mathbb{P}^{m-1}$ is not a cone, i.e. $\ker(A) \cap \ker(B) = 0$, and*
- *The binary form $F(x, z) = \det(Ax + Bz)$ is identically zero.*

Then the k-equivalence class of (Q_1, Q_2) is uniquely determined:

(i) *If $m = 3$ then (Q_1, Q_2) is k-equivalent to (x_1x_2, x_2x_3)*
(ii) *If $m = 4$ then (Q_1, Q_2) is k-equivalent to $(x_1x_2, x_2x_3 - x_4^2)$.*

Proof: (i) We must show that the gcd of Q_1 and Q_2 is a linear form, and for this we may assume that k is algebraically closed. Since some quadric in the pencil has rank 2, we may assume that $Q_1 = x_1x_2$. Then the condition $\det(Ax + Bz) = 0$ works out as $b_{33} = b_{13}b_{23} = \det B = 0$. Swapping x_1 and x_2 if necessary, we may assume that $b_{13} = b_{33} = 0$. Then $b_{23} \neq 0$ (otherwise we would have a cone) and the condition $\det B = 0$ forces $b_{11} = 0$. Making a substitution for x_3 now puts (Q_1, Q_2) in the required form.
(ii) Suppose $\{Q_1 = Q_2 = 0\} \subset \mathbb{P}^3$ has a singular point defined over k. Moving this point to $(1 : 0 : 0 : 0)$, it is easy to reduce to the case

$$A = \left(\begin{array}{cc|cc} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & \multicolumn{2}{c}{\multirow{2}{*}{A'}} \\ 0 & 0 & & \end{array} \right), \qquad B = \left(\begin{array}{cc|cc} 0 & 0 & 0 & 0 \\ 0 & * & * & * \\ 0 & * & \multicolumn{2}{c}{\multirow{2}{*}{B'}} \\ 0 & * & & \end{array} \right).$$

The condition $\det(Ax + Bz) = 0$ now becomes $\det(A'x + B'z) = 0$. Hence we may assume that A' and B' are scalar multiples of $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Then $b_{23} \neq 0$ (otherwise we have a cone) and a substitution in x_3 brings us to the case

$$(Q_1, Q_2) = (x_1x_2 + \lambda x_4^2, x_2x_3 + \mu x_4^2)$$

for some $\lambda, \mu \in k$. Replacing one of these quadrics by a suitable linear combination, and then making a substitution in x_1 and x_3 to compensate, we may assume that $\lambda = 0$. Then $\mu \neq 0$ (otherwise we have a cone) and we rescale to get $\mu = -1$.

By Theorem 2.8(ii) there is a singular point defined over $\overline{k}$. So running the above proof over $\overline{k}$ shows that $\{Q_1 = Q_2 = 0\} \subset \mathbb{P}^3$ is the union of a conic and a line, meeting at a unique point. This point of intersection is a k-rational singular point. Our earlier proof now applies. □

PROOF OF LEMMA 4.10: We write $\overline{Q}_1$ and $\overline{Q}_2$ for the reductions of Q_1 and Q_2 mod π. In the proof we often arrive at one of the following three special situations.

Situation 1: The reduction $\mathcal{C}_{(\overline{Q}_1,\overline{Q}_2)}$ contains a plane defined over k.
By a $\mathrm{GL}_4(\mathcal{O}_K)$-transformation we may move the plane to $\{x_1 = 0\}$. We apply the transformation $[\pi^{-1}I_2, \mathrm{Diag}(\pi, 1, 1, 1)]$ to give an integral model of smaller level.

Situation 2: The reduction $\mathcal{C}_{(\overline{Q}_1,\overline{Q}_2)}$ is a cone over a point $\mathbf{x} \in \mathbb{P}^3(k)$ and moreover $Q_1(\mathbf{x}) \equiv Q_2(\mathbf{x}) \equiv 0 \pmod{\pi^2}$.
By a $\mathrm{GL}_4(\mathcal{O}_K)$-transformation we may move the point to $(1 : 0 : 0 : 0)$. We apply the transformation $[I_2, \mathrm{Diag}(\pi^{-1}, 1, 1, 1)]$ to give an integral model of smaller level.

Situation 3: The reduction $\mathcal{C}_{(\overline{Q}_1,\overline{Q}_2)}$ contains a line defined over k.
By a $\mathrm{GL}_4(\mathcal{O}_K)$-transformation we may move the line to $\{x_1 = x_2 = 0\}$. The "flip-flop" transformation $[\pi^{-1}I_2, \mathrm{Diag}(\pi, \pi, 1, 1)]$ gives an integral model of the same level.

Let A and B be the matrices of second partial derivatives of Q_1 and Q_2. Let $\overline{A}$ and $\overline{B}$ be their reductions mod π. We split into cases according to the value of the *common nullity*, defined as $s = \dim(\ker \overline{A} \cap \ker \overline{B})$.

If $s = 0$ then by Lemma 4.11(ii) we are in Situation 3. Applying the "flip-flop" transformation brings us to the case $s \geq 1$.

If $s = 1$ we may assume that $\overline{Q}_1$ and $\overline{Q}_2$ are quadratic forms in x_2, x_3, x_4 only. Let A' and B' be the 3 by 3 matrices of second partial derivatives. Then

$$F(x, z) \equiv (a_{11}x + b_{11}z) \det(A'x + B'z) \pmod{\pi^2}. \tag{4.4}$$

Since $v(F) \geq 2$ we have either $a_{11} \equiv b_{11} \equiv 0 \pmod{\pi^2}$ in which case we are in Situation 2, or $\det(A'x + B'z) = 0$ in which case Lemma 4.11(i) shows we are in Situation 1.

If $s \geq 2$ we may assume that $\overline{Q}_1$ and $\overline{Q}_2$ are binary quadratic forms in x_1 and x_2. If $\overline{Q}_1$ and $\overline{Q}_2$ simultaneously represent 0 over k, then we are in Situation 1. Otherwise we apply the "flip-flop" transformation $[\pi^{-1}I_2, \mathrm{Diag}(\pi, \pi, 1, 1)]$ to give an integral model (R_1, R_2) of the same level. Then $\overline{R}_1$ and $\overline{R}_2$ are binary quadratic forms in x_3 and x_4. If $\overline{R}_1$ and $\overline{R}_2$ simultaneously represent 0 over k then we are in Situation 1. Otherwise we obtain a contradiction to our hypothesis that (Q_1, Q_2) is K-soluble. Indeed if $(x_1 : x_2 : x_3 : x_4)$ were a K-point with $\min\{v(x_i) : 1 \leq i \leq 4\} = 0$ then from $Q_1(\mathbf{x}) \equiv Q_2(\mathbf{x}) \equiv 0 \pmod{\pi}$ we deduce $x_1 \equiv x_2 \equiv 0 \pmod{\pi}$ and from $Q_1(\mathbf{x}) \equiv Q_2(\mathbf{x}) \equiv 0 \pmod{\pi^2}$ we deduce $x_3 \equiv x_4 \equiv 0 \pmod{\pi}$. □

This completes the proof of Proposition 4.8. We now modify the proof so that we can deduce Theorems 3.5(i) and 3.6 in the case $n = 4$ from the corresponding results for $n = 2$. The situation considered at the end of the last paragraph motivates the definition of a critical model, see Definition 5.1(c) below.

Proposition 4.12. *If $(Q_1, Q_2) \in X_4(K)$ is non-singular then it is K-equivalent to either*

(i) *an integral model $\Phi \in X_4(\mathcal{O}_K)$ with $\mathfrak{d}(\Phi)$ minimal (and hence Φ minimal), or*

(ii) *a critical model, as specified in Definition 5.1(c) below.*

Proof: By Lemma 4.7 we may assume that $\mathfrak{d}(Q_1, Q_2)$ is a minimal binary quartic. We then follow the proof of Lemma 4.9, but without the hypothesis of K-solubility. This hypothesis was only used at the end of the proof of Lemma 4.10. We may assume that one of the pairs, say $\overline{Q}_1$ and $\overline{Q}_2$, simultaneously represents 0 over $\overline{k}$. (Otherwise we would have a critical model.) If they do not simultaneously represent 0 over k, then they must be linearly dependent. So it is clear we can reduce the level, but not necessarily using a transformation of the specified form. In the proof of Lemma 4.9 we repeatedly applied Lemma 4.10. For the final application it does not matter what transformation we use. In all earlier applications we have $v(F) \geq 3$. If A_1, B_1 and A_2, B_2 are the 2 by 2 matrices representing the pairs of binary quadratic forms $\overline{Q}_1, \overline{Q}_2$ and $\overline{R}_1, \overline{R}_2$ then

$$F(x, z) \equiv \pi^2 \det(A_1 x + B_1 z) \det(A_2 x + B_2 z) \pmod{\pi^3}.$$

The hypothesis $v(F) \geq 3$ therefore ensures that one of the pairs simultaneously represents 0 over k. We are then in Situation 1. $\square$

In Lemma 5.3 (see below) we show that critical models are minimal. Hence the proof of Proposition 4.12 gives an algorithm for minimising quadric intersections, even in the case they are not K-soluble. Proposition 4.12 also allows us to deduce the case $n = 4$ of Theorems 3.5(i) and 3.6 from the case $n = 2$. Here we use the easy facts that critical models are K^{sh}-insoluble, and remain critical after any unramified field extension.

4.4. **Minimisation in residue characteristic 2.** We describe how to modify our algorithms in the cases $n = 2, 4$ when $\mathrm{char}(k) = 2$. In the case $n = 2$ the issue is that we must work with generalised binary quartics instead of just binary quartics. Recall that a generalised binary quartic, or genus one model of degree 2, is an equation of the form

$$y^2 + P(x, z)y = Q(x, z)$$

where P and Q are homogeneous polynomials of degrees 2 and 4. We label the coefficients of P and Q as l, m, n and a, b, c, d, e. We observe that in characteristic 2 the binary quadratic form $\partial^2 Q/\partial x \partial z = bx^2 + dz^2$ is a covariant of the quartic Q.

Moreover this covariant vanishes if and only if Q is a square. (Recall that k is perfect, and so every element of k is a square.)

We say that two models are *y-equivalent* if they are related by a *y-substitution*, that is, a substitution of the form $x \leftarrow x$, $z \leftarrow z$, $y \leftarrow y + r_0x^2 + r_1xz + r_2z^2$. The *valuation* of $(P, Q) \in X_2(\mathcal{O}_K)$ is

$$v(P, Q) = \max\{\min(2v(P'), v(Q')) : (P', Q') \text{ is } y\text{-equivalent to } (P, Q)\}.$$

It is easy to check that $v(P, Q)$ only depends on the $\mathcal{O}_K$-equivalence class of (P, Q). If $v(P) = 0$, or $v(P) \geq 1$ and $Q(x, z)$ is not a square mod π, then $v(P, Q) = 0$. Otherwise we can make a y-substitution so that $v(Q) \geq 1$. Then either $v(Q) = 1$ in which case $v(P, Q) = 1$, or $v(Q) \geq 2$ in which case (P, Q) is non-minimal, and indeed dividing P and Q through by π and π^2 gives a K-equivalent integral model of smaller level. Theorem 4.2 has the following analogue.

Theorem 4.13. *Let $(P, Q) \in X_2(\mathcal{O}_K)$ be a non-singular generalised binary quartic. Suppose that $v(P, Q) = 0$ or 1, but (P, Q) has positive level.*

(i) *The reduction mod π of*

$$Q_1(x, z) = \begin{cases} P(x, z) & \text{if } v(P) = 0, \\ \partial^2 Q/\partial x \partial z & \text{if } v(P) \geq 1 \text{ and } v(P, Q) = 0, \\ \pi^{-1} Q(x, z) & \text{if } v(P) \geq 1 \text{ and } v(Q) = 1 \end{cases}$$

has a unique repeated root defined over k.

(ii) *The following procedure replaces (P, Q) by a K-equivalent integral model of the same level.*
- *If $v(P, Q) = 1$ then make a y-substitution so that $v(Q) \geq 1$.*
- *Move the repeated root of $Q_1(x, z)$ mod π to $(x : z) = (0 : 1)$.*
- *Make a y-substitution so that $\pi \mid e$. (This is possible since $\pi \mid n$ and every element of k is a square.)*
- *Replace $P(x, z)$ by $\pi^{-1} P(\pi x, z)$ and $Q(x, z)$ by $\pi^{-2} Q(\pi x, z)$.*

(iii) *If (P, Q) is non-minimal then the procedure in (ii) gives $v(P, Q) \geq 2$ after at most 2 iterations.*

Proof: We first show that if (i) holds for (P, Q) then it holds for any $\mathcal{O}_K$-equivalent model (P', Q'). We say that forms $f, g \in k[x, z]$ are k-equivalent if $f(x, z) = \lambda g(\alpha x + \beta z, \gamma x + \delta z)$ for some $\lambda, \alpha, \beta, \gamma, \delta \in k$ with $\lambda(\alpha\delta - \beta\gamma) \neq 0$. Each of the following claims is an easy consequence of the definition of $\mathcal{O}_K$-equivalence (as given in Section 2) and our assumption that $\mathrm{char}(k) = 2$.

- The reductions mod π of $P(x, z)$ and $P'(x, z)$ are k-equivalent; in particular, $v(P) = 0 \iff v(P') = 0$.
- If $v(P) \geq 1$ then the reductions mod π of $\partial^2 Q/\partial x \partial z$ and $\partial^2 Q'/\partial x \partial z$ are k-equivalent; note that $v(P, Q) = v(P', Q')$.

- If $v(P) \geq 1$ and $v(Q) = v(Q') = 1$ then the reductions mod π of $\pi^{-1}Q(x,z)$ and $\pi^{-1}Q'(x,z)$ are k-equivalent.

It is now clear that if (i) holds for (P,Q) then it holds for (P',Q').

Next we show that the procedure in (ii) gives a well defined map on $\mathcal{O}_K$-equivalence classes. This does not automatically follow from Lemma 4.1, since we also have to consider y-substitutions. Suppose we start with some model satisfying (i), and carry out the first three steps of the procedure in (ii) in two different ways. The result is a pair of $\mathcal{O}_K$-equivalent models (P,Q) and (P',Q') related by some $[1,r,M] \in \mathcal{G}_2(\mathcal{O}_K)$. Since the reduction of M mod π fixes the repeated root $(0:1)$ we have $\pi \mid m_{21}$. Labelling the coefficients of (P,Q) in the usual way, and likewise for (P',Q'), we have $\pi \mid n, e$ and $\pi \mid n', e'$. Therefore $\pi \mid r_2$. It is now routine to check that if (ii) holds for (P,Q), i.e. $\pi \mid n, d$ and $\pi^2 \mid e$, then (ii) holds for (P',Q'), i.e. $\pi \mid n', d'$ and $\pi^2 \mid e'$. Moreover the transformed models are related by $[1,(\pi r_0, r_1, \pi^{-1}r_2), \mathrm{Diag}(\pi,1) M \,\mathrm{Diag}(\pi^{-1},1)] \in \mathcal{G}_2(\mathcal{O}_K)$. Thus the procedure gives a well-defined map on $\mathcal{O}_K$-equivalence classes.

We are now free in the proof to replace (P,Q) by any $\mathcal{O}_K$-equivalent model. So if (P,Q) is non-minimal we may assume that $P(\pi^s x, z) \equiv 0 \pmod{\pi^{s+1}}$ and $Q(\pi^s x, z) \equiv 0 \pmod{\pi^{2s+2}}$ for some integer $s \geq 0$. We call the least such integer s the *slope*. As happened for binary quartics, the only possible slopes are $s = 0,1,2$. If $s = 0$ then $v(P,Q) \geq 2$ contrary to hypothesis. If $s = 1$ then the coefficients of (P,Q) have valuations satisfying

$$\geq 0 \quad \geq 1 \quad \geq 2 \qquad \geq 0 \quad \geq 1 \quad \geq 2 \quad \geq 3 \quad \geq 4.$$

If $v(P) = 0$ then $P(x,z)$ mod π has a double root at $(x:z) = (0:1)$. Otherwise, since every element of k is a square, we can make a y-substitution $y \leftarrow y + r_0 x^2$ so that $v(Q) \geq 1$. Then $\pi^{-1}Q(x,z)$ mod π has either a triple or quadruple root at $(x:z) = (0:1)$. If $s = 2$ then the coefficients of (P,Q) have valuations satisfying

$$\geq 0 \quad \geq 1 \quad \geq 3 \qquad \geq 0 \quad = 0 \quad \geq 2 \quad \geq 4 \quad \geq 6.$$

So in this case $v(P,Q) = 0$. If $v(P) = 0$ then $P(x,z)$ mod π has a double root at $(x:z) = (0:1)$. Otherwise $bx^2 + dz^2$ mod π has a double root at $(x:z) = (0:1)$. In each of the cases $s = 1,2$ it is now clear that the procedure in (ii) returns a K-equivalent integral model of smaller slope. Hence at most 2 iterations are required to give $v(P,Q) \geq 2$, establishing (iii).

It remains to give prove (i) and (ii) in the case (P,Q) has positive level (but could be minimal). If (P,Q) is K^{sh}-soluble then after an unramified extension $\mathcal{C}_{(P,Q)}(K) \neq \emptyset$. Then Theorem 3.4 shows that (P,Q) is non-minimal, and our earlier argument applies. Otherwise, we show in Proposition 5.6 below, that (P,Q) is $\mathcal{O}_K$-equivalent to a model whose coefficients have valuations satisfying

$$\geq 1 \quad \geq 1 \quad \geq 2 \qquad = 1 \quad \geq 2 \quad \geq 2 \quad \geq 3 \quad = 3.$$

Statements (i) and (ii) are then clear. $\square$

Next we modify the algorithm for minimising quadric intersections, as presented in Section 4.3. First we replace $\mathfrak{d}$ by the map

$$\begin{aligned} \mathfrak{d}' : X_4(K) &\to X_2(K) \\ (Q_1, Q_2) &\mapsto (P, Q) = (\mathrm{pf}(xQ_1 + zQ_2), \mathrm{rd}(xQ_1 + zQ_2)) \end{aligned} \tag{4.5}$$

where pf and rd were defined in the proof of Lemma 2.9. Then $\Delta(Q_1, Q_2) = \Delta(P, Q)$. We call (P, Q) the *doubling* of (Q_1, Q_2). (The reason for this name is that $\mathfrak{d}'$ acts as multiplication-by-2 on the Weil-Chatelet group.) The analogue of Lemma 4.6 (using $\mathfrak{d}'$ instead of $\mathfrak{d}$) is immediate if $\mathrm{char}(K) \neq 2$. Indeed the covering map $\mathcal{C}_{(Q_1,Q_2)} \to \mathcal{C}_{(P,Q)}$ is given by $(x_1 : x_2 : x_3 : x_4) \mapsto (T_1 : -T_2 : J')$ where $J' = \frac{1}{2}(J - lT_1^2 + mT_1T_2 - nT_2^2)$, and l, m, n are the coefficients of P. If $\mathrm{char}(K) = 2$ then the role of J' is taken by

$$\begin{aligned} J'' = \tfrac{1}{2}\big(J - lT_1^2 + mT_1T_2 - nT_2^2 + mn(lT_1 + mT_2)Q_1 + lm(nT_2 + mT_1)Q_2 \\ l^2n^3Q_1^2 + lmn(ln + m^2)Q_1Q_2 + l^3n^2Q_2^2\big) \,. \end{aligned}$$

It may be verified by direct calculation that T_1, T_2 and J'' have coefficients in $\mathbb{Z}[X_4]$. Moreover T_1 and T_2 cannot both vanish identically on $\mathcal{C}_{(Q_1,Q_2)}$. (We checked this for the models specified in Lemma 3.11, and then used the covariance of T_1 and T_2.) Hence in all characteristics there is a morphism $\mathcal{C}_{(Q_1,Q_2)} \to \mathcal{C}_{(P,Q)}$ given by $(x_1 : x_2 : x_3 : x_4) \mapsto (T_1 : -T_2 : J'')$

The diagram in Lemma 4.7 (using $\mathfrak{d}'$ instead of $\mathfrak{d}$) no longer commutes, but it does commute up to y-equivalence, and this is sufficient for our purposes.

Definition 4.14. Let $Q \in k[x_1, \ldots, x_m]$ be a quadratic form in m variables.

(i) The *kernel* $\ker(Q)$ of Q is the subspace of k^m defined by the vanishing of Q and all its partial derivatives. (Recall that k is perfect, so the restriction of Q to the subspace where all the partial derivatives vanish is the square of a linear form.) The *rank* of Q is $m - \dim\ker(Q)$.

(ii) The *discriminant* of Q is

$$\Delta_m(Q) = \begin{cases} \det(\frac{\partial^2 Q}{\partial x_i \partial x_j}) & \text{if } m \text{ is even} \\ \frac{1}{2}\det(\frac{\partial^2 Q}{\partial x_i \partial x_j}) & \text{if } m \text{ is odd.} \end{cases}$$

The discriminant Δ_m is a polynomial in the coefficients of Q with integer coefficients. Therefore Definition 4.14(ii) is valid in all characteristics. Recall that we defined pf and rd so that $\Delta_4(Q) = \mathrm{pf}(Q)^2 + 4\,\mathrm{rd}(Q)$.

Lemma 4.15. *Let Q_1 and Q_2 be quadratic forms in $m = 3$ or 4 variables over a field k with* $\mathrm{char}(k) = 2$*. Assume that*

- $\{Q_1 = Q_2 = 0\} \subset \mathbb{P}^{m-1}$ *is not a cone, i.e.* $\ker(Q_1) \cap \ker(Q_2) = 0$*, and*

- *if* $m = 3$ *then* $\Delta_3(xQ_1+zQ_2) = 0$*, whereas if* $m = 4$ *then* $\mathrm{pf}(xQ_1+zQ_2) = 0$ *and* $\mathrm{rd}(xQ_1 + zQ_2)$ *is a square.*

Then the k*-equivalence class of* (Q_1, Q_2) *is uniquely determined, and is as given in Lemma 4.11.*

PROOF: This is similar to the proof of Lemma 4.11. □

In Lemma 4.10 we made the hypothesis that $v(F) \geq 2$ where $F = \mathfrak{d}(Q_1, Q_2)$. This should now be replaced by the hypothesis that $\mathfrak{d}'(Q_1, Q_2)$ is y-equivalent to a model (P, Q) with $v(P) \geq 1$ and $v(Q) \geq 2$. Then

$$\begin{aligned} P(x,z) &= \mathrm{pf}(xQ_1 + zQ_2) + 2h(x,z) \\ Q(x,z) &= \mathrm{rd}(xQ_1 + zQ_2) - \mathrm{pf}(xQ_1 + zQ_2)h(x,z) - h(x,z)^2 \end{aligned} \tag{4.6}$$

for some $h \in K[x, z]$. Since (Q_1, Q_2) is integral it follows that $h \in \mathcal{O}_K[x, z]$. Then $\mathrm{pf}(x\overline{Q}_1 + z\overline{Q}_2) = 0$ and $\mathrm{rd}(x\overline{Q}_1 + z\overline{Q}_2)$ is a square. Moreover if $\mathrm{rd}(xQ_1 + zQ_2)$ vanishes mod π then it vanishes mod π^2.

The common nullity is $s = \dim(\ker \overline{Q}_1 \cap \ker \overline{Q}_2)$. In the case $s = 1$ we may assume that Q_1 and Q_2 reduce to quadratic forms in x_2, x_3, x_4 only. Call these Q'_1 and Q'_2. The analogue of (4.4) is

$$\mathrm{rd}(xQ_1 + zQ_2) \equiv (\alpha x + \beta z)\Delta_3(xQ'_1 + zQ'_2) \pmod{\pi^2}$$

where α and β are the coefficients of x_1^2 in Q_1 and Q_2. In all other respects, the proof of the Lemma 4.10 goes through as before. By repeated application of this lemma we obtain the following analogue of Lemma 4.9.

Lemma 4.16. *Let* $(Q_1, Q_2) \in X_4(K)$ *be a* K*-soluble non-singular quadric intersection. If* $\mathfrak{d}'(Q_1, Q_2)$ *is* y*-equivalent to an integral generalised binary quartic then* (Q_1, Q_2) *is* K*-equivalent to an integral quadric intersection* (Q'_1, Q'_2) *such that* $\mathfrak{d}'(Q'_1, Q'_2)$ *is* y*-equivalent to* $\mathfrak{d}'(Q_1, Q_2)$*.*

The Minimisation Theorem for $n = 4$ now follows from the Minimisation Theorem for $n = 2$ exactly as before.

The proof of Proposition 4.12 (with $\mathfrak{d}$ replaced by $\mathfrak{d}'$) is modified as follows. We follow the proof of Lemma 4.16 but without the hypothesis of K-solubility. This hypothesis is only used when $s \geq 2$. In this case

$$(\overline{Q}_1, \overline{Q}_2) = (\alpha_{11}x_1^2 + \alpha_{12}x_1x_2 + \alpha_{22}x_2^2, \beta_{11}x_1^2 + \beta_{12}x_1x_2 + \beta_{22}x_2^2)$$

and applying the transformation $[\pi^{-1}I_2, \mathrm{Diag}(\pi, \pi, 1, 1)]$ gives (R_1, R_2) with

$$(\overline{R}_1, \overline{R}_2) = (\gamma_{33}x_3^2 + \gamma_{34}x_3x_4 + \gamma_{44}x_4^2, \delta_{33}x_3^2 + \delta_{34}x_3x_4 + \delta_{44}x_4^2).$$

We must show that if $\overline{Q}_1$ and $\overline{Q}_2$ are linearly dependent and $\mathfrak{d}'(Q_1, Q_2)$ is y-equivalent to a model (P, Q) with $v(P) \geq 2$ and $v(Q) \geq 3$ then one of the pairs $\overline{Q}_1$, $\overline{Q}_2$ or $\overline{R}_1$, $\overline{R}_2$ simultaneously represents 0 over k. Since $s \geq 2$ we already know that $\mathrm{pf}(xQ_1 + zQ_2)$ vanishes mod π and $\mathrm{rd}(xQ_1 + zQ_2)$ vanishes mod π^2. It follows by (4.6) that $\mathrm{pf}(xQ_1 + zQ_2)$ vanishes mod π^2 and $\pi^{-2}\,\mathrm{rd}(xQ_1 + zQ_2)$ is a square mod π. Hence

$$\alpha_{12}\gamma_{34} = \beta_{12}\delta_{34} = \alpha_{12}\delta_{34} + \beta_{12}\gamma_{34} = 0$$

and

$$\begin{aligned} \alpha_{12}^2(\gamma_{33}\delta_{44} + \gamma_{44}\delta_{33}) + \gamma_{34}^2(\alpha_{11}\beta_{22} + \alpha_{22}\beta_{11}) = 0 \\ \beta_{12}^2(\gamma_{33}\delta_{44} + \gamma_{44}\delta_{33}) + \delta_{34}^2(\alpha_{11}\beta_{22} + \alpha_{22}\beta_{11}) = 0. \end{aligned}$$

Since $\overline{Q}_1$ and $\overline{Q}_2$ are linearly dependent we have $\alpha_{11}\beta_{22} + \alpha_{22}\beta_{11} = 0$. So either $\alpha_{12} = \beta_{12} = 0$, in which case $\overline{Q}_1$ and $\overline{Q}_2$ simultaneously represent 0 over k, or $\gamma_{34} = \delta_{34} = \gamma_{33}\delta_{44} + \gamma_{44}\delta_{33} = 0$ in which case $\overline{R}_1$ and $\overline{R}_2$ simultaneously represent 0 over k.

4.5. **Minimisation over global fields.** We have so far presented theorems and algorithms for minimising genus one models defined over local fields. We now discuss the global situation, and in particular prove Theorem 1.1. The following is a more precise version of that theorem. A genus one model defined over a number field K is called *integral* if its coefficients belong to the ring of integers $\mathcal{O}_K$.

Theorem 4.17. *Let $n = 2, 3$ or 4. Let K be a number field of class number one. Let $\Phi \in X_n(K)$ be a non-singular genus one model. If $\mathcal{C}_\Phi$ is locally soluble at all finite places of K then Φ is K-equivalent to an integral genus one model with the same discriminant as a global minimal model for the Jacobian E of $\mathcal{C}_\Phi$.*

Proof: To deduce this result directly from the statement of the Minimisation Theorem (Theorem 3.4) one is naturally led to use a version of strong approximation. See [Fi2] for details in the cases $n = 2, 3$. The case $n = 4$ is similar. Although these proofs are not difficult, it is a notable advantage of the algorithmic approach taken in this section that the passage from local to global becomes a triviality.

Indeed, suppose K is a number field with class number one. Let $\mathfrak{p} = \pi\mathcal{O}_K$ be a prime of K and put $k = \mathcal{O}_K/\mathfrak{p}$. Then for any pair of m-dimensional subspaces $U, V \subset k^n$ there exists $M \in \mathrm{SL}_n(\mathcal{O}_K)$ whose reduction mod $\mathfrak{p}$ takes U to V. (Indeed, the case $\dim U = \dim V = 1$ is Lemma 3.13, and the general case is similar.) We can therefore follow the algorithms for minimising at $\mathfrak{p}$, using π as the uniformiser, without changing the level (or integrality) at other primes.

After first scaling the given model to be integral at all primes, we apply this procedure to the finite number of primes at which the resulting model has positive level. This gives an integral model which has level zero at all primes of K. By definition of level, this model has the same discriminant as a global minimal model for E, up to a unit factor. Since this unit must be a 12th power, a final scaling by a suitable global unit gives the result. $\square$

Theorem 1.1 is an immediate corollary since, as recalled in the introduction, every n-covering which is locally soluble at all places of K, has a degree-n model.

To extend this theorem to a general number field K, we may replace integrality by S-integrality, where S is a (finite) set of primes generating the class group, so that the ring of S-integers is a principal ideal domain. The minimal model may then only be S-integral rather than integral. Just as with Weierstrass models for elliptic curves, there may be no global minimal model when the class number is greater than 1. In practice, we can alternatively find models which are simultaneously minimal at all primes in any given finite set, while being at least integral at all other primes.

Similar results may be deduced from our local results in the case where K is a function field, *i.e.*, a finite extension of $\mathbb{F}_q(t)$.

5. Minimisation of insoluble genus one models

We return to working over a discrete valuation field K as specified in Section 3.1. In this section we prove the Converse Theorem (Theorem 3.5(ii)). This shows that the Strong Minimisation Theorem (Theorem 3.5(i)) is best possible.

Definition 5.1.

(a) A generalised binary quartic $(P, Q) \in X_2(\mathcal{O}_K)$ is *critical* if the valuations of its coefficients l, m, n, a, b, c, d, e satisfy

$$\geq 1 \quad \geq 1 \quad \geq 2 \qquad = 1 \quad \geq 2 \quad \geq 2 \quad \geq 3 \quad = 3.$$

(b) A ternary cubic $F \in X_3(\mathcal{O}_K)$ is *critical* if the valuations of its coefficients satisfy the inequalities indicated in the following diagram.

$$\begin{array}{ccccccc} & & & z^3 & & & \\ & & xz^2 & & yz^2 & & \\ & x^2z & & xyz & & y^2z & \\ x^3 & & x^2y & & xy^2 & & y^3 \end{array} \qquad \begin{array}{ccccccc} & & & =2 & & & \\ & & \geq 2 & & \geq 2 & & \\ & \geq 1 & & \geq 1 & & \geq 2 & \\ =0 & & \geq 1 & & \geq 1 & & =1 \end{array}$$

(c) A quadric intersection $(Q_1, Q_2) \in X_4(\mathcal{O}_K)$ is *critical* if the reductions of Q_1 and Q_2 mod π are quadratic forms in x_1 and x_2 with no common root in $\mathbb{P}^1(\overline{k})$, and on putting

$$(R_1, R_2) = [\pi^{-1} I_2, \mathrm{Diag}(\pi, \pi, 1, 1)](Q_1, Q_2)$$

the reductions of R_1 and R_2 mod π are quadratic forms in x_3 and x_4 with no common root in $\mathbb{P}^1(\overline{k})$.

We show in the next three lemmas that critical models are insoluble, minimal and of positive level. We then show (for $n = 2, 3$) that every K^{sh}-insoluble model is K-equivalent to a critical model. There is a corresponding result for models of degree $n=4$.

Lemma 5.2. *Critical models are insoluble over K.*

Proof: We give details in the case $n=2$. Suppose $(x,y,z)\in K^3$ is a non-zero solution of $y^2+P(x,z)y=Q(x,z)$. Clearing denominators we may assume that $\min\{v(x),v(z)\}=0$. It follows that $y\in\mathcal{O}_K$. Then reducing the equation mod π^i for $i=1,2,3,4$ we successively deduce $\pi\,|\,y$, $\pi\,|\,x$, $\pi^2\,|\,y$ and $\pi\,|\,z$. In particular $\min\{v(x),v(z)\}>0$. This is the required contradiction. The cases $n=3,4$ are similar. □

Since the definition of a critical model is unchanged by an unramified field extension, it follows immediately that critical models are insoluble over K^{sh}.

Lemma 5.3. *Critical models are minimal.*

Proof: In the cases $n=2,3$ we give a very quick proof. Indeed, if Φ were non-minimal, then our algorithms in Sections 4.1, 4.2 and 4.4 would succeed in reducing the level. But on the contrary, when given a critical model, these algorithms endlessly cycle between two or three $\mathcal{O}_K$-equivalence classes. (Treating the case $n=4$ in the same way would give a circular argument, as the current lemma was cited at the end of Section 4.3.)

Alternatively we can imitate the proof of Lemma 5.2. We give details in the case $n=4$. We define

$$s(Q_1,Q_2)=\max\{-v(\det M):[M,I_4](Q_1,Q_2)\in X_4(\mathcal{O}_K)\}.$$

Suppose $[M,N]\in\mathcal{G}_4(K)$ is a transformation taking the critical model $\Phi=(Q_1,Q_2)$ to an integral model of smaller level. We may assume that N has entries in $\mathcal{O}_K$, not all in $\pi\mathcal{O}_K$. Let $\xi_j(x_1,\ldots,x_4)=\sum_{i=1}^4 n_{ij}x_i$. For $i=1,2$ we put

$$Q_i\circ N=Q_i(\xi_1,\ldots,\xi_4)\in\mathcal{O}_K[x_1,\ldots,x_4].$$

Our hypothesis is that $s(Q_1\circ N,Q_2\circ N)>v(\det N)$.

If $v(Q_1\circ N)=0$ then replacing Q_2 by $Q_2+\lambda Q_1$ for suitable $\lambda\in\mathcal{O}_K$ we may assume that $v(Q_2\circ N)>v(\det N)$. To understand this last condition, we put N in Smith normal form. Explicitly we write $N=U\,\mathrm{Diag}(\pi^a,\pi^b,\pi^c,1)V$ for some $U,V\in\mathrm{GL}_4(\mathcal{O}_K)$ and $a\geq b\geq c\geq 0$. Since $v(Q_2)=0$ we must have $2a>v(\det N)=a+b+c$ and therefore $a-b+c\geq 1$. It follows that $Q_2\circ U\equiv x_1(\sum_{i=1}^4\epsilon_i x_i)\pmod{\pi^2}$ for some $\epsilon_i\in\mathcal{O}_K$ with $\epsilon_2\equiv\epsilon_3\equiv\epsilon_4\equiv 0\pmod{\pi}$. In other words, $Q_2\equiv\mu\ell_1\ell_2\pmod{\pi^2}$ for some $\mu\in\mathcal{O}_K$ and linear forms $\ell_1,\ell_2\in\mathcal{O}_K[x_1,\ldots,x_4]$ with $\ell_1\equiv\ell_2\pmod{\pi}$. This contradicts the definition of a critical model (as it would follow that R_2 vanishes mod π). Hence $v(Q_1\circ N)\geq 1$. Similarly $v(Q_2\circ N)\geq 1$. Since $\overline{Q}_1$ and $\overline{Q}_2$ are binary quadratic forms with no common root we deduce $\xi_1\equiv\xi_2\equiv 0\pmod{\pi}$. Let $\xi_i'=\pi^{-1}\xi_i$ for $i=1,2$. We put

$$(R_1,R_2)=[\pi^{-1}I_2,\mathrm{Diag}(\pi,\pi,1,1)](Q_1,Q_2).$$

Let N' be the matrix with columns the coefficients of $\xi_3, \xi_4, \xi_1', \xi_2'$. Then (R_1, R_2) is a critical model and $s(R_1 \circ N', R_2 \circ N') > v(\det N')$. Repeating the same arguments we deduce $\xi_3 \equiv \xi_4 \equiv 0 \pmod{\pi}$. This contradicts our scaling of the matrix N. □

The next lemma describes the possible levels of a critical model. For this we need to work explicitly with the "a-invariants" defined in the proof of Lemma 2.9. Although $a_1, \ldots, a_6$ are not invariants (in the sense of Definition 2.7), they are isobaric in the sense that

$$\begin{aligned} n = 2: &\qquad a_i \circ [\mu, 0, \mathrm{Diag}(\xi_1, \xi_2)] = (\mu \xi_1 \xi_2)^i a_i \\ n = 3: &\qquad a_i \circ [\mu, \mathrm{Diag}(\xi_1, \xi_2, \xi_3)] = (\mu \xi_1 \xi_2 \xi_3)^i a_i \\ n = 4: &\qquad a_i \circ [\mathrm{Diag}(\mu_1, \mu_2), \mathrm{Diag}(\xi_1, \xi_2, \xi_3, \xi_4)] = (\mu_1 \mu_2 \xi_1 \xi_2 \xi_3 \xi_4)^i a_i \end{aligned}$$

for all i. (We use the notation for transformations of genus one models introduced in Section 2.) In the following we write $t^{(n)}$ as a short-hand for $\pi^{-n} t$.

Lemma 5.4. *The level of a critical model is at least* 1 *and equal to* 1 *if* $\mathrm{char}(k) \nmid n$.

Proof: Case $n = 2$. By (2.3) we have $\pi^i \mid a_i$ for all i. A convenient way to check this is to note that $\pi^{-3/2} P(\pi^{1/2} x, z)$ and $\pi^{-3} Q(\pi^{1/2} x, z)$ have coefficients in $\mathcal{O}_K[\pi^{1/2}]$, and then to use the isobaric property. It follows that (P, Q) has positive level. Now suppose that $\mathrm{char}(k) \neq 2$ and (P, Q) has level greater than 1. Completing the square we may assume that $l = m = n = 0$. Then $a_1 = a_3 = 0$ and $y^2 = x^3 + a_2^{(2)} x^2 + a_4^{(4)} x + a_6^{(6)}$ is an integral Weierstrass equation of positive level. According to Tate's algorithm the cubic polynomial

$$x^3 + a_2^{(2)} x^2 + a_4^{(4)} x + a_6^{(6)} \equiv (x + c^{(2)})(x^2 - 4a^{(1)} e^{(3)}) \pmod{\pi}$$

has a triple root defined over k. This contradicts the definition of a critical model. Case $n = 3$. By (2.4) we have $\pi^i \mid a_i$ for all i. A convenient way to check this is to note that $\pi^{-2} F(\pi^{2/3} x, \pi^{1/3} y, z)$ has coefficients in $\mathcal{O}_K[\pi^{1/3}]$, and then to use the isobaric property. It follows that F has positive level. Now suppose that $\mathrm{char}(k) \neq 3$ and F has level greater than 1. Then

$$y^2 + a_1^{(1)} xy + a_3^{(3)} y = x^3 + a_2^{(2)} x^2 + a_4^{(4)} x + a_6^{(6)}$$

is an integral Weierstrass equation of positive level. By (2.4) we find $a_2^{(2)} \equiv a_4^{(4)} \equiv 0 \pmod{\pi}$ and

$$\begin{aligned} a_1^{(1)} &\equiv m^{(1)} \pmod{\pi} \\ a_3^{(3)} &\equiv 9ab^{(1)} c^{(2)} \pmod{\pi} \\ a_6^{(6)} &\equiv -27(ab^{(1)} c^{(2)})^2 + ab^{(1)} c^{(2)} (m^{(1)})^3 \pmod{\pi}. \end{aligned}$$

So it suffices to show that if there is a Weierstrass equation over k of the form

$$y^2 + \alpha xy + 9\beta y = x^3 + (\alpha^3 - 27\beta)\beta$$

with $c_4 = \Delta = 0$, then $\beta = 0$. We compute $c_4 = \alpha(\alpha^3 - 216\beta)$ and $\Delta = -\beta(\alpha^3 + 27\beta)^3$. Since $216 + 27 = 3^5$ is non-zero in k, it follows that $\beta = 0$ as required.
Case $n = 4$. The quadric intersection $[\pi^{-1}I_2, \mathrm{Diag}(\pi^{1/2}, \pi^{1/2}, 1, 1)](Q_1, Q_2)$ has coefficients in $\mathcal{O}_K[\pi^{1/2}]$. It follows by the isobaric property of the a-invariants that $\pi^i \mid a_i$ for all i and hence that (Q_1, Q_2) has positive level. Now suppose that $\mathrm{char}(k) \neq 2$. Then $F = \mathfrak{d}(Q_1, Q_2)$ satisfies $F(x, z) \equiv \pi^2 f_1(x, z) f_2(x, z) \pmod{\pi^3}$ where $f_1, f_2 \in \mathcal{O}_K[x, z]$ are binary quadratic forms, neither having a repeated root mod π. (So their product cannot have a triple or quadruple root.) It follows by Theorem 4.2(i) that F and hence (Q_1, Q_2) has level 1. □

Example 5.5. The following examples of critical models, all of level 2, show that the hypothesis $\mathrm{char}(k) \nmid n$ cannot be removed from Lemma 5.4.

$$\begin{aligned} K &= \mathbb{Q}_2 & y^2 &= 2x^4 + 24x^2z^2 + 8z^4 \\ K &= \mathbb{Q}_3 & x^3 &+ 3y^3 + 9z^3 + 18xyz = 0 \\ K &= \mathbb{Q}_2 & x_1^2 &+ 2x_3^2 + 4x_2x_4 = x_2^2 + 2x_4^2 + 4x_1x_3 = 0 \end{aligned}$$

The following proposition completes the proof of Theorem 3.5(ii). The doubling map $\mathfrak{d}'$ was defined in Section 4.4. (If $\mathrm{char}(k) \neq 2$ then we can work with $\mathfrak{d}$ instead.)

Proposition 5.6. *Let $\Phi \in X_n(\mathcal{O}_K)$ be a K^{sh}-insoluble minimal genus one model.*

(i) *If $n = 2$ or 3 then Φ is $\mathcal{O}_K$-equivalent to a critical model.*
(ii) *If $n = 4$ then Φ is K-equivalent to either a critical model or an integral model (Q_1, Q_2) with $\mathfrak{d}'(Q_1, Q_2)$ critical.*

First we need three lemmas.

Lemma 5.7. *Let k be an algebraically closed field. Suppose that either*

(a) *$\Phi = (P, Q) \in X_2(k)$ and $P^2 + 4Q$ is not identically zero,*
(b) *$\Phi = (F) \in X_3(k)$ is non-zero and is not the cube of a linear form,*
(c) *$\Phi = (Q_1, Q_2) \in X_4(k)$ and every quadric in the pencil spanned by Q_1 and Q_2 has rank at least 2.*

Then $\mathcal{C}_\Phi$ has a smooth k-point (on some 1-dimensional component).

Proof: For $n = 2, 3$ this is clear. In the case $n = 4$ we are looking for a transverse point of intersection of Q_1 and Q_2, *i.e.* a point where the Jacobian matrix has rank 2. We prove the result more generally for intersections of two quadrics in m variables. This enables us to reduce to the case $\ker(Q_1) \cap \ker(Q_2) = 0$. Now let P be a singular point on the quadric intersection. (If there is no such point there is nothing to prove.) Then moving this point to $(1 : 0 : \ldots : 0)$ we may assume that $Q_1 = x_1x_2 + g_1(x_2, \ldots, x_m)$ and $Q_2 = g_2(x_2, \ldots, x_m)$ for some g_1 and g_2. Since

$\operatorname{rank}(Q_2) \geq 2$ we can pick a smooth point $(x_2 : \ldots : x_m)$ on $\{Q_2 = 0\} \subset \mathbb{P}^{m-2}$ with $x_2 \neq 0$. Then solving the equation $Q_1 = 0$ for x_1 gives the required transverse point of intersection on $\{Q_1 = Q_2 = 0\}$. □

Lemma 5.8. *Let $\Phi \in X_n(\mathcal{O}_K)$ be a K^{sh}-insoluble minimal genus one model.*

(a) *If $n = 2$ then $\Phi = (P, Q)$ with $v(P, Q) = 1$. Moreover if $v(Q) = 1$ then the reduction of $\pi^{-1}Q(x, z)$ mod π has either two double roots or a quadruple root (over $\overline{k}$).*

(b) *If $n = 3$ then Φ is a ternary cubic whose reduction mod π is (a constant times) the cube of a linear form.*

(c) *If $n = 4$ then there is a rank 1 quadric in the reduced pencil,* i.e. *if $\Phi = (Q_1, Q_2)$ then* $\operatorname{rank}(\lambda\overline{Q}_1 + \mu\overline{Q}_2) = 1$ *for some $(\lambda : \mu) \in \mathbb{P}^1(\overline{k})$.*

Proof: We recall that K^{sh} has residue field $\overline{k}$. The idea of the proof is that if Φ is not of the form listed, then we can use Lemma 5.7 to find a smooth $\overline{k}$-point on the reduction, and use the Henselian property to lift it to a K^{sh}-point, thereby obtaining a contradiction.

A little more needs to be said in the case $n = 2$. If $\operatorname{char}(k) \neq 2$ then completing the square gives $v(P) \geq 1$ and Lemma 5.7 shows that $v(Q) \geq 1$. If $\operatorname{char}(k) = 2$ then Lemma 5.7 shows that $v(P) \geq 1$. If $Q(x, z)$ mod π had a simple root over $\overline{k}$ then we could lift to a K^{sh}-point on $\mathcal{C}_{(P,Q)}$ with $y = 0$. It follows that $Q(x, z)$ is a square mod π. So by a y-substitution we may suppose $v(Q) \geq 1$. In all residue characteristics we now have $v(P) \geq 1$ and $v(Q) \geq 1$. We cannot have $v(Q) \geq 2$ since (P, Q) is minimal. If $\pi^{-1}Q(x, z)$ mod π had a simple root over $\overline{k}$ then we could lift to a K^{sh}-point on $\mathcal{C}_{(P,Q)}$ with $y = 0$. It follows that this polynomial has either two double roots or a quadruple root. □

Lemma 5.9. *Suppose $(P, Q), (P', Q') \in X_2(\mathcal{O}_K)$ are K-equivalent models of the same level related by a substitution $[\mu, r, M] \in \mathcal{G}_2(K)$ where $M \in \mathrm{GL}_2(K)$ has Smith normal form* $\operatorname{Diag}(1, \pi^s)$. *Then $v(\Delta(P, Q)) \geq 2s$.*

Proof: Let (P, Q) have coefficients l, m, n, a, b, c, d, e. Replacing our models by $\mathcal{O}_K$-equivalent ones we may assume $\mu = \pi^{-s}$ and $M = \operatorname{Diag}(\pi^s, 1)$. If we assume for simplicity that $r = 0$, then we have $\pi^s \mid n, d$ and $\pi^{2s} \mid e$. Since the discriminant $\Delta \in \mathbb{Z}[X_2]$ belongs to the ideal (n^2, nd, d^2, e) it follows that $v(\Delta(P, Q)) \geq 2s$.

For general r we can write the transformation $[\pi^{-s}, r, \operatorname{Diag}(\pi^s, 1)]$ either as

$$y \leftarrow \pi^s y + r_0 x^2 + r_1 xz + r_2 z^2 \quad \text{followed by} \quad x \leftarrow \pi^s x$$

or as

$$x \leftarrow \pi^s x \quad \text{followed by} \quad y \leftarrow \pi^s(y + \pi^s r_0 x^2 + r_1 xz + \pi^{-s} r_2 z^2).$$

Since Q' has coefficients in $\mathcal{O}_K$ we have $v(r_0^2+r_0l-a) \geq -2s$ and $v(r_2^2+r_2n-e) \geq 2s$. Hence $\pi^s r_0, r_2 \in \mathcal{O}_K$. So replacing our models by $\mathcal{O}_K$-equivalent ones we may assume that $r_0 = r_2 = 0$. Then the middle coefficient of Q' gives $v(r_1^2+r_1m-c) \geq 0$ and hence $r_1 \in \mathcal{O}_K$. Once more replacing (P, Q) by an $\mathcal{O}_K$-equivalent model we may assume that $r_0 = r_1 = r_2 = 0$. Our earlier proof now applies. □

Proof of Proposition 5.6: We split into the cases $n = 2, 3, 4$.

Case $n = 2$. Applying Lemma 5.8 to $\Phi = (P, Q)$ we may assume that $v(P) \geq 1$, $v(Q) = 1$, and $\pi^{-1}Q(x, z) \bmod \pi$ has either two double roots or a quadruple root.

We first rule out the possibility of two double roots. After an unramified field extension we may assume that these roots are defined over k. So without loss of generality $Q(x, z) \equiv \pi x^2 z^2 \pmod{\pi^2}$. We replace $P(x, z)$ by $\pi^{-1}P(\pi x, z)$ and $Q(x, z)$ by $\pi^{-2}Q(\pi x, z)$. By Lemma 5.8 we again have $v(P, Q) \geq 1$. We make a substitution $y \leftarrow y + r_2 z^2$ so that $v(P) \geq 1$ and $v(Q) \geq 1$. Now $\pi^{-1}Q(x, z) \bmod \pi$ has a double root at $(x : z) = (1 : 0)$. By Lemma 5.8 it has a second double root, say at $(\lambda : 1)$. We make the substitution $x \leftarrow x + \lambda z$. Then $Q(x, z) \equiv \pi x^2 z^2 \pmod{\pi^2}$. We can now repeat this process indefinitely. It follows by Lemma 5.9 that $\Delta(P, Q) = 0$. This is the required contradiction.

It remains to consider the case of a quadruple root, say $Q(x, z) \equiv \pi x^4 \pmod{\pi^2}$. Let $l_1, m_1, n_1, a_1, b_1, c_1, d_1, e_1$ be the coefficients of $P_1(x, z) = \pi^{-1}P(\pi x, z)$ and $Q_1(x, z) = \pi^{-2}Q(\pi x, z)$. By Lemma 5.8 we can make a substitution $y \leftarrow y+r_2 z^2$ so that $\pi \mid n_1, e_1$. Then $\pi^{-1}Q_1(x, z) \bmod \pi$ has at least a triple root at $(x : z) = (1 : 0)$. So by Lemma 5.8 we have $\pi^2 \mid d_1$ and $v(e_1) = 1$. The coefficients of (P, Q) now satisfy the definition of a critical model.

Case $n = 3$. By Lemma 5.8 our ternary cubic F must reduce mod π to the cube of a linear form. So without loss of generality, we have

$$F = \pi\, f_3(y, z) + \pi\, f_2(y, z)\, x + \pi\, f_1(y, z)\, x^2 + a\, x^3 .$$

with $\pi \nmid a$. Then $F_1(x, y, z) = \pi^{-1}F(\pi x, y, z)$ is a minimal ternary cubic and by Lemma 5.8 its reduction mod π is the cube of a linear form in y and z. After a suitable transformation of y and z, we may assume that $f_3(y, z) \equiv by^3 \pmod{\pi}$ with $\pi \nmid b$ (otherwise F would not be minimal). Now $F_2(x, y, z) = \pi^{-1}F_1(x, \pi y, z)$ is again a minimal ternary cubic, and its reduction mod π is $(c'x + cz)z^2$. Again this must be a non-zero cube. So $c' = 0$ and c is a unit. The coefficients of F now satisfy the definition of a critical model.

Case $n = 4$. We divide the proof into the following two lemmas.

Lemma 5.10. *Let $(Q_1, Q_2) \in X_4(\mathcal{O}_K)$ be a K^{sh}-insoluble minimal quadric intersection. Let $s = \dim(\ker(\overline{Q}_1) \cap \ker(\overline{Q}_2))$ be the common nullity of the reduced pencil.*

(i) *If $s \le 1$ then the reduced pencil contains a unique rank 1 quadric, and the following procedure replaces (Q_1, Q_2) by a K-equivalent minimal quadric intersection with $s \ge 1$.*
- *Make a $\mathrm{GL}_2(\mathcal{O}_K)\times\mathrm{GL}_4(\mathcal{O}_K)$-transformation so that $Q_2 \equiv x_1^2 \pmod{\pi}$.*
- *Apply the transformation $[\mathrm{Diag}(1,\pi^{-1}), \mathrm{Diag}(\pi,1,1,1)]$.*

(ii) *If $s \ge 2$ then (Q_1, Q_2) is $\mathcal{O}_K$-equivalent to a critical model.*

Proof: (i) By Lemma 5.8 there is a rank 1 quadric in the reduced pencil. It is unique (and therefore defined over k) as we would otherwise have $s \ge 2$. The remaining statements are clear.
(ii) We may assume that $\overline{Q}_1$ and $\overline{Q}_2$ are binary quadratic forms in x_1 and x_2. Since the model is minimal, these forms have no common root in $\mathbb{P}^1(\overline{k})$. We put

$$(R_1, R_2) = [\pi^{-1} I_2, \mathrm{Diag}(\pi, \pi, 1, 1)](Q_1, Q_2).$$

Then R_1 and R_2 reduce to binary quadratic forms in x_3 and x_4. Again, since the model is minimal, these forms have no common root in $\mathbb{P}^1(\overline{k})$. Hence (Q_1, Q_2) is critical. □

Lemma 5.11. *Let $\Phi \in X_4(\mathcal{O}_K)$ satisfy the hypotheses of Lemma 5.10 with $s = 1$. If the procedure in Lemma 5.10(i) may be iterated indefinitely, then Φ is $\mathcal{O}_K$-equivalent to a quadric intersection (Q_1, Q_2) where the valuations of the coefficients of Q_1 and Q_2 satisfy the inequalities indicated in the following diagram:*

$$\begin{array}{cccc} x_1^2 & x_1x_2 & x_1x_3 & x_1x_4 \\ & x_2^2 & x_2x_3 & x_2x_4 \\ & & x_3^2 & x_3x_4 \\ & & & x_4^2 \end{array} \qquad \begin{array}{cccc} \ge 0 & \ge 0 & = 0 & \ge 1 \\ & = 0 & \ge 1 & \ge 1 \\ & & \ge 1 & \ge 1 \\ & & & = 1 \end{array} \qquad \begin{array}{cccc} = 0 & \ge 1 & \ge 1 & \ge 1 \\ & \ge 1 & \ge 1 & = 1 \\ & & = 1 & \ge 2 \\ & & & \ge 2. \end{array}$$

Proof: We may assume that $\Phi = (Q_1, Q_2)$ has reduction

$$(\overline{Q}_1, \overline{Q}_2) = (x_1\ell(x_2, x_3) + f(x_2, x_3), cx_1^2) \tag{5.1}$$

for some $c \in k$ and $\ell, f \in k[x_2, x_3]$. Since (Q_1, Q_2) is minimal we have $cf \ne 0$. So the reduction is (set-theoretically) either a line or a pair of lines. We show in the case of a pair of lines that the procedure in Lemma 5.10(i) must give $s \ge 2$ after a finite number of iterations (bounded in terms of the valuation of the discriminant). The first iteration gives (R_1, R_2) with

$$(\overline{R}_1, \overline{R}_2) = (f(x_2, x_3), g(x_2, x_3, x_4))$$

for some $g \in k[x_2, x_3, x_4]$. Since f has rank 2 we may assume on replacing R_2 by $R_2 + \lambda R_1$ for suitable $\lambda \in \mathcal{O}_K$ that g has rank 1. If g has no coefficient of x_4^2 then $s \ge 2$. Otherwise a $\mathrm{GL}_4(\mathcal{O}_K)$-transformation puts $(\overline{R}_1, \overline{R}_2)$ in the form (5.1) with

$\ell = 0$ (and the same f as before). The process is then repeated. By considering the effect on the doubling it follows by Lemma 5.9 that only finitely many iterations are possible.

It remains to consider the case where the reduction is (set-theoretically) a line. We may assume that $\Phi = (Q_1, Q_2)$ and its transforms

$$(R_1, R_2) = [\mathrm{Diag}(1, \pi^{-1}), \mathrm{Diag}(\pi, 1, 1, 1)](Q_1, Q_2)$$
$$(S_1, S_2) = [\mathrm{Diag}(\pi^{-1}, 1), \mathrm{Diag}(1, \pi, 1, 1)](R_1, R_2)$$

under the first two iterations have reductions

$$(\overline{Q}_1, \overline{Q}_2) = (x_1(\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3) + x_2^2,\ x_1^2) \tag{5.2}$$

$$(\overline{R}_1, \overline{R}_2) = (x_2^2,\ x_2(\beta_2 x_2 + \beta_3 x_3 + \beta_4 x_4) + g(x_3, x_4)) \tag{5.3}$$

$$(\overline{S}_1, \overline{S}_2) = (\alpha_3 x_1 x_3 + \lambda x_3^3 + \mu x_3 x_4 + \nu x_4^2,\ g(x_3, x_4)) \tag{5.4}$$

for some $\alpha_i, \beta_i, \lambda, \mu, \nu \in k$ and $g \in k[x_3, x_4]$. By (5.2) we have $\alpha_3 \neq 0$ (otherwise $s \geq 2$). Since the reduction cannot be a pair of lines, we see first by (5.3) that g has rank 1, and then by (5.4) that $g = \gamma x_3^2$ for some $\gamma \neq 0$. Finally (5.3) and (5.4) show that $\beta_4 \neq 0$ and $\nu \neq 0$ (otherwise $s \geq 2$). The valuations of the coefficients of Q_1 and Q_2 now satisfy the inequalities indicated in the statement of the lemma. □

Proposition 5.6(ii) follows from the last two lemmas and the observation that if (Q_1, Q_2) satisfies the conclusions of Lemma 5.11 then its doubling is critical. □

6. Reduction

In this section, we assume that the ground field is $\mathbb{Q}$. The main reason for this is that a comparable theory of reduction over a general number field has not yet been sufficiently developed.

Let $\mathcal{C} \subset \mathbb{P}^{n-1}$ be a genus one normal curve defined over $\mathbb{Q}$ of degree n (or, if $n = 2$, let $\mathcal{C} \to \mathbb{P}^1$ be a double cover) with points everywhere locally, so that $\mathcal{C}$ represents an element of the n-Selmer group of its Jacobian elliptic curve E. If $n \in \{2, 3, 4\}$, we can, by the results and algorithms of the previous sections, assume that $\mathcal{C} = \mathcal{C}_\Phi$ where Φ is a genus one model which is both integral and minimal, so that its invariants c_4, c_6 and Δ coincide with those of a minimal model of E. This means that the invariants are as small as possible (in absolute value). However, it does not necessarily mean that the equations defining $\mathcal{C}$ will have small coefficients. To achieve this, we will employ *reduction*. Leaving aside the aesthetic value of equations with small coefficients, the main benefit of a reduced model is that further computations like searching for rational points on $\mathcal{C}$ or performing further descents on $\mathcal{C}$ are greatly facilitated.

The idea of reduction is to find a unimodular transformation (*i.e.*, an invertible integral linear change of coordinates on $\mathbb{P}^{n-1}$) that makes the equations defining $\mathcal{C}$

smaller. Unimodular transformations have the property of preserving the integrality and invariants of the model, so they will not destroy its minimality. In the language of Section 2, a unimodular transformation is just a $\mathbb{Z}$-equivalence.

If we were allowed to make a coordinate change from $\mathrm{SL}_n(\mathbb{C})$ instead, then we could always bring our model into one of the following standard forms, where in general $a, b \in \mathbb{C}$ (see for example [Hu]). When $n = 3$, we can achieve this normal form even by a transformation from $\mathrm{SL}_3(\mathbb{R})$, so in this case, we can take $a, b \in \mathbb{R}$. We will call these forms *Hesse forms*, generalising the classical terminology for $n = 3$. They are as follows.

$$\begin{array}{ll} n = 2: & y^2 = a(x_0^4 + x_1^4) + b\,x_0^2x_1^2 \\ n = 3: & a(x_0^3 + x_1^3 + x_2^3) + b\,x_0x_1x_2 = 0 \\ n = 4: & \begin{cases} a(x_0^2 + x_2^2) + b\,x_1x_3 = 0 \\ a(x_1^2 + x_3^2) + b\,x_0x_2 = 0 \end{cases} \end{array}$$

In these forms, the coefficients a and b are bounded in terms of the invariants, so we can expect them to be small. Therefore, we would like to come close to a model of this kind, but using a unimodular transformation.

We need some way of measuring how close two models are. On the standard Hesse models, the action of the n-torsion of the Jacobian, $E[n]$, is given by the "standard representation" where one generator multiplies each x_j by ζ_n^j and the other generator does a cyclic shift of the coordinates. (Here ζ_n denotes a primitive nth root of unity.) To this representation, we can associate an invariant inner product on $\mathbb{C}^n$, which is unique up to scaling. It is easy to check that this invariant inner product is just the standard one on $\mathbb{C}^n$. Now our approach is to associate an inner product to a given model $\mathcal{C}$, and consider the model to be close to a standard model when the associated inner product is close to the standard one, which means that it is reduced in an appropriate sense. This is explained in some detail in the following section.

6.1. **The reduction covariant.** Let $K = \mathbb{R}$ or $\mathbb{C}$. We write $\mathcal{Y}_n(K)$ for the set of all genus one normal curves of degree n defined over K, inside a fixed copy of $\mathbb{P}^{n-1}$. (If $n = 2$ we consider double covers of $\mathbb{P}^1$ instead.) The difference between $\mathcal{Y}_n(K)$ and $X_n(K)$ is that we now consider actual curves in $\mathbb{P}^{n-1}$ (or the set of ramification points of $\mathcal{C} \to \mathbb{P}^1$ when $n = 2$), instead of defining equations.

Let $\mathcal{H}_n^+(\mathbb{C})$ be the space of positive definite Hermitian $n \times n$ matrices, and $\mathcal{H}_n^+(\mathbb{R})$ the space of positive definite symmetric real $n \times n$ matrices. We can identify these spaces with the spaces of positive definite Hermitian and real quadratic forms in n variables, respectively. There are natural and compatible (left) actions of $\mathrm{SL}_n(K)$ on $\mathcal{Y}_n(K)$ and $\mathcal{H}_n^+(K)$ given by the canonical map $\mathrm{SL}_n(K) \to \mathrm{PGL}_n(K) = \mathrm{Aut}(\mathbb{P}_K^{n-1})$ on the one hand and by $g \cdot M = \bar{g}^{-t} M g^{-1}$ on the other hand (where γ^{-t} denotes the inverse transpose of the matrix γ). If we identify the matrix

$M \in \mathcal{H}_n^+(K)$ with the quadratic or Hermitian form $Q(x) = \bar{x}^t M x$, then the compatibility of the actions means that $(g \cdot Q)(gx) = Q(x)$.

Theorem 6.1. *For each $n \geq 2$ there is a unique $\mathrm{SL}_n(\mathbb{C})$-covariant map*

$$\varphi_{\mathbb{C}} : \mathcal{Y}_n(\mathbb{C}) \to \mathcal{H}_n^+(\mathbb{C})/\mathbb{R}_{>0}^\times .$$

This map is compatible with complex conjugation, and hence restricts to an $\mathrm{SL}_n(\mathbb{R})$-covariant map

$$\varphi_{\mathbb{R}} : \mathcal{Y}_n(\mathbb{R}) \to \mathcal{H}_n^+(\mathbb{R})/\mathbb{R}_{>0}^\times .$$

Proof: Let $\mathcal{C} \to \mathbb{P}^{n-1}$ be a genus one normal curve defined over $\mathbb{C}$, with Jacobian E. The action of $E[n]$ on $\mathcal{C}$ extends to $\mathbb{P}^{n-1}$ and hence defines a group homomorphism $\chi : E[n](\mathbb{C}) \to \mathrm{PGL}_n(\mathbb{C})$. Lifting to $\mathrm{SL}_n(\mathbb{C})$ we obtain a diagram

$$\begin{tikzcd}
0 \arrow[r] & \mu_n \arrow[r] \arrow[d, equal] & H_n \arrow[r] \arrow[d] & E[n](\mathbb{C}) \arrow[r] \arrow[d, "\chi"] & 0 \\
0 \arrow[r] & \mu_n \arrow[r] & \mathrm{SL}_n(\mathbb{C}) \arrow[r] & \mathrm{PGL}_n(\mathbb{C}) \arrow[r] & 0 .
\end{tikzcd}$$

The Heisenberg group H_n is a non-abelian group of order n^3. It comes with a natural n-dimensional representation, called the Schrödinger representation, which is known to be irreducible (since it is equivalent to the standard representation mentioned above). Now by the Weyl unitary trick, every irreducible complex representation of a finite group has a unique invariant inner product. (Recall that existence is proved by averaging over the group, and uniqueness (up to $\mathbb{R}_{>0}^\times$) using Schur's lemma.)

We define $\varphi_{\mathbb{C}}(\mathcal{C})$ to be the (matrix of the) Heisenberg invariant inner product, *i.e.*, $\varphi_{\mathbb{C}}(\mathcal{C})$ is uniquely determined up to positive real scalars by the property that

$$\bar{h}^{-t} \varphi_{\mathbb{C}}(\mathcal{C}) h^{-1} = \varphi_{\mathbb{C}}(\mathcal{C})$$

for all $h \in H_n$. If $g \in \mathrm{SL}_n(\mathbb{C})$, then the Heisenberg groups H_n and H_n' of $\mathcal{C}$ and $g \cdot \mathcal{C}$ are related by $H_n' = g H_n g^{-1}$. Then $g \cdot \varphi_{\mathbb{C}}(\mathcal{C}) = \bar{g}^{-t} \varphi_{\mathbb{C}}(\mathcal{C}) g^{-1}$ is an H_n'-invariant inner product, and so must be equal to $\varphi_{\mathbb{C}}(g \cdot \mathcal{C})$. Hence $\varphi_{\mathbb{C}}$ is $\mathrm{SL}_n(\mathbb{C})$-covariant. Moreover, since $H_n \subset \mathrm{SL}_n(\mathbb{C})$, this choice of covariant is forced on us. The compatibility with complex conjugation is seen in the same way. □

Remark 6.2. In general $\varphi_{\mathbb{R}}$ is not the only $\mathrm{SL}_n(\mathbb{R})$-covariant. However, it is if the points of $E[n]$ are defined over $\mathbb{R}$, as happens in the case $n = 2$ and $\Delta > 0$, cf. [SC2, Lemma 3.2].

In practical terms, we have the following corollary.

Corollary 6.3. *Let $M_T \in \mathrm{GL}_n(\mathbb{C})$ describe the action of $T \in E[n](\mathbb{C})$ on $\mathcal{C} \to \mathbb{P}^{n-1}$. Then the reduction covariant $\varphi_{\mathbb{C}}(\mathcal{C})$ is*

$$\sum_{T \in E[n](\mathbb{C})} \frac{1}{|\det M_T|^{2/n}} \overline{M}_T^{\,t} M_T.$$

Proof: To get an invariant inner product, we can take any inner product and average over its orbit under the action of H_n. Applying this to the standard inner product, we find that we can take, up to scaling,

$$\varphi_{\mathbb{C}}(\mathcal{C}) = \sum_{h \in H_n} \bar{h}^{-t} h^{-1} = \sum_{h \in H_n} \bar{h}^t h\,. \tag{6.1}$$

In the statement of the corollary, $M_T \in \mathrm{GL}_n(\mathbb{C})$ is any lift of the element $\tau_T \in \mathrm{PGL}_n(\mathbb{C})$ describing the action of T on $\mathbb{P}^{n-1}(\mathbb{C})$. The various pre-images of τ_T in H_n are given by $h = \alpha^{-1} M_T$ where $\alpha \in \mathbb{C}$ with $\alpha^n = \det M_T$. We then have

$$\bar{h}^t h = \bar{\alpha}^{-1} \alpha^{-1} \overline{M}_T^{\,t} M_T = \frac{1}{|\det M_T|^{2/n}} \overline{M}_T^{\,t} M_T.$$

Since this only depends on T, it is sufficient to take the sum in (6.1) just over $T \in E[n](\mathbb{C})$, instead of over $h \in H_n$. $\square$

We can now define what we mean by a reduced genus one normal curve.

Definition 6.4. A genus one normal curve $\mathcal{C} \to \mathbb{P}^{n-1}$ defined over $\mathbb{R}$ is *Minkowski* (respectively *LLL*) *reduced* if $\varphi_{\mathbb{R}}(\mathcal{C})$ is the Gram matrix of a Minkowski (respectively LLL) reduced lattice basis.

Note that a lattice basis is (Minkowski or LLL) reduced if it is close to the standard basis of the standard lattice in the sense that the basis vectors are (short and) nearly orthogonal. The notion of a Minkowski reduced model has nice theoretical properties (it is optimal and essentially unique), whereas for practical purposes, it is important to be able to compute a reduced lattice basis efficiently; this is possible when using LLL reduced models.

If we start with some given (minimal) model $\mathcal{C} \to \mathbb{P}^{n-1}$, then in order to reduce it, we first compute its reduction covariant $\varphi_{\mathbb{R}}(\mathcal{C})$. We apply the LLL algorithm [LLL] to this Gram matrix, resulting in a unimodular transformation U and an LLL reduced Gram matrix M, such that $M = U^t \varphi_{\mathbb{R}}(\mathcal{C}) U = U^{-1} \cdot \varphi_{\mathbb{R}}(\mathcal{C})$. We then apply the transformation U^{-1} to our model $\mathcal{C}$. Since $\varphi_{\mathbb{R}}(\mathcal{C})$ is a covariant, we will have that $\varphi_{\mathbb{R}}(U^{-1} \cdot \mathcal{C}) = M$ is LLL reduced. Therefore $U^{-1} \cdot \mathcal{C}$ is the (minimal and) reduced model we are looking for.

In the following sections we discuss how to compute $\varphi_{\mathbb{R}}$. There are two basic approaches. One is to find the hyperosculating points of $\mathcal{C}(\mathbb{C})$ numerically and to compute the covariant from them. If $n = 2$, we are looking for the ramification points of the covering $\mathcal{C} \to \mathbb{P}^1$; if $n = 3$, for the flex points of the plane cubic curve $\mathcal{C} \subset \mathbb{P}^2$. The other approach is to use the n-torsion points in $E(\mathbb{C})$ instead and compute their action on $\mathbb{P}^{n-1}$. Generally speaking, the first approach leads to simpler formulas, whereas the second approach tends to be numerically more stable.

6.2. **Reduction of 2-coverings.** We identify $\mathcal{H}_2^+(\mathbb{R})$ with the space of real positive definite binary quadratic forms, and $\mathcal{H}_2^+(\mathbb{R})/\mathbb{R}_{>0}^\times$ with the upper half plane. This identification maps a real positive definite binary quadratic form to its unique root in the upper half plane.

6.2.1. *Using the ramification points.* Let $F(x,z) \in \mathbb{R}[x,z]$ be homogeneous of degree 4. We assume that $f(X) = F(X,1)$ has degree 4 as well. (If the leading coefficient is zero, make a change of coordinates first.) Let $\theta_1, \dots, \theta_4 \in \mathbb{C}$ be the roots of f. It is shown in [SC2] that $\varphi_\mathbb{R}$ is given by

$$\varphi_\mathbb{R}(F)(x,z) = \sum_{i=1}^{4} \frac{1}{|f'(\theta_i)|}(x - \theta_i z)(x - \overline{\theta_i} z)\,.$$

This goes back to Julia's thesis [Ju], where three different formulas are given according to the number of real roots of f; see also [Cr2].

The formula is still valid for $\varphi_\mathbb{C}$, in the form

$$\varphi_\mathbb{C}(F)(x,z) = \sum_{i=1}^{4} \frac{1}{|f'(\theta_i)|}|x - \theta_i z|^2\,.$$

In practice one should first numerically compute the roots of the resolvent cubic (which is not changed by reduction) and then compute the roots of f from these.

6.2.2. *Using the* 2*-torsion of* E*.* The binary quartic

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

has invariants I and J (see Section 2) and resolvent cubic $r(X) = X^3 - 3IX + J$. For φ a root of r we set

$$\begin{aligned} \alpha_1(\varphi) &= 4a\varphi - 8ac + 3b^2 \\ \alpha_2(\varphi) &= b\varphi - 6ad + bc \\ \alpha_3(\varphi) &= (-2\varphi^2 + 2c\varphi - 9bd + 4c^2)/3 \end{aligned}$$

and

$$W = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad A_\varphi = \begin{pmatrix} \alpha_1(\varphi) & \alpha_2(\varphi) \\ \alpha_2(\varphi) & \alpha_3(\varphi) \end{pmatrix}.$$

Lemma 6.5. *If $\alpha_1(\varphi) \neq 0$, then the action of the corresponding point $T \in E[2]$ on $\mathbb{P}^1$ is given by*

$$M_T = WA_\varphi\,.$$

PROOF: Let $H(x,z)$ be the Hessian of F. The pencil spanned by F and H contains three degenerate quartics: for each root φ' of the resolvent cubic, we have

$$\alpha_1(\varphi')\big(4\varphi' F(x,z) - \tfrac{1}{3}H(x,z)\big) = \big(\alpha_1(\varphi')x^2 + 2\alpha_2(\varphi')xz + \alpha_3(\varphi')z^2\big)^2 .$$

Since the action of T leaves both F and H invariant, M_T must induce an involution on $\mathbb{P}^1$ that either fixes or swaps the roots of the quadratic on the right hand side; there is exactly one root φ' such that the roots of the corresponding quadratic are fixed. Therefore $\varphi' = \varphi$, and the lemma follows by checking that WA_φ does indeed fix the roots of the relevant quadratic. □

Lemma 6.6. *If $M_T \in \mathrm{GL}_2$ describes the action of $T \in E[2]$ on $\mathcal{C} \to \mathbb{P}^1$ then*

$$\sum_{T \in E[2]} \frac{1}{\det M_T} M_T^t M_T = 0. \tag{6.2}$$

PROOF: We can verify this generically using the formula of Lemma 6.5. □

Proposition 6.7. *Let $F \in \mathbb{R}[x,z]$ be a non-singular binary quartic, with resolvent cubic $r(X) = X^3 - 3IX + J$.*

(i) *If $\Delta(F) > 0$ then the reduction covariant is $\pm A_\varphi$ where φ is the unique root of r with $\det(A_\varphi) > 0$ and the sign is that of $\alpha_1(\varphi)$.*
(ii) *If $\Delta(F) < 0$ then the reduction covariant is*

$$\mathrm{Re}\left(\frac{1}{|\det A_\varphi|} \overline{A}_\varphi A_\varphi - \frac{1}{\det A_\varphi} A_\varphi^2 \right)$$

where φ is a complex root of r.

PROOF: If $\Delta(F) > 0$, then r has three real roots. Since $\det(A_\varphi) = -\alpha_1(\varphi) r'(\varphi)/3$, the analysis in [Cr2] shows that there is a unique root φ of r with $\det(A_\varphi) > 0$ (in particular, $\alpha_1(\varphi) \neq 0$). By Lemmas 6.5 and 6.6 the reduction covariant simplifies (up to a factor of 2) to

$$\sum_{T \in E[2],\, \det M_T > 0} \frac{1}{\det M_T} M_T^t M_T = I_2 + \frac{1}{\det A_\varphi} A_\varphi^2 = \frac{\mathrm{tr} A_\varphi}{\det A_\varphi} A_\varphi \,,$$

by the Cayley-Hamilton theorem. So $\pm A_\varphi$ is the positive definite symmetric matrix we are looking for, with the sign that makes the top left entry positive.

If $\Delta(F) < 0$, then r has a pair of complex conjugate roots, say φ and $\overline{\varphi}$. If $E[2] = \{0, S, T, \overline{T}\}$, then we can take $M_S = M_T \overline{M}_T$, so $\det(M_S) = |\det(M_T)|^2 > 0$. By Lemmas 6.5 and 6.6 again, the reduction covariant simplifies to

$$\mathrm{Re}\left(\frac{1}{|\det M_T|} \overline{M}_T^t M_T - \frac{1}{\det M_T} M_T^t M_T \right) = \mathrm{Re}\left(\frac{1}{|\det A_\varphi|} \overline{A}_\varphi A_\varphi - \frac{1}{\det A_\varphi} A_\varphi^2 \right).$$

Notice that we cannot have $\alpha_1(\varphi) = \alpha_1(\overline{\varphi}) = 0$, since then the resolvent cubic would have a repeated root, contradicting the fact that F is non-singular. □

6.2.3. *The cross terms.* So far, we have shown how to find a unimodular transformation of the coordinates on $\mathbb{P}^1$ that reduces the 2-covering. (If we start with a generalised binary quartic (P, Q) then we work with $F = P^2 + 4Q$.) There is still an ambiguity coming from the possibility of making a y-substitution in the general form of a 2-covering. The most reasonable convention seems to be to arrange that the cross term coefficients l, m, n are 0 or 1.

6.3. **Reduction of 3-coverings.**

6.3.1. *Using the flex points.* Let $F(x, y, z) \in \mathbb{R}[x, y, z]$ be a nonsingular ternary cubic. In order to find its reduction covariant (as a positive definite quadratic form $Q(x, y, z)$), we proceed as follows. Let $H(x, y, z)$ be the Hessian of F as defined in Section 2. Then the intersection of $F = 0$ and $H = 0$ consists of nine distinct points, the flex points of F. Three of them are real, the others come in three complex conjugate pairs.

There are twelve lines each containing three of the flex points, coming in four triples of lines that do not meet in a flex point. (These triples are the "syzygetic triangles" mentioned in Section 6.3.2 below.) One of these triples has all three lines real, call them L_{11}, L_{12}, L_{13}. Another one has one line real, call it L_{21}, and two complex conjugate lines, call them L_{22} and L_{23}. Then Q spans the one-dimensional intersection of the spaces spanned by L_{11}^2, L_{12}^2 and L_{13}^2, and by L_{21}^2 and $L_{22}L_{23}$, respectively.

In order to see why this recipe works, first observe that it clearly defines an $\mathrm{SL}_3(\mathbb{R})$-covariant map. We can always make an $\mathrm{SL}_3(\mathbb{R})$-transformation to bring F into the standard Hesse form

$$F(x, y, z) = a(x^3 + y^3 + z^3) + b\,xyz.$$

Then L_{11}, L_{22}, L_{33} are x, y, z, and L_{21}, L_{22}, L_{23} are $x + y + z$, $x + \zeta_3 y + \zeta_3^2 z$, $x + \zeta_3^2 y + \zeta_3 z$ (where ζ_3 is a primitive cube root of unity). One then looks at the intersection

$$\langle x^2, y^2, z^2\rangle \cap \langle (x + y + z)^2, x^2 + y^2 + z^2 - xy - yz - zx\rangle$$

and finds it is one-dimensional, spanned by $x^2 + y^2 + z^2$, which is the reduction covariant of any F in Hesse form.

The only way we know to implement this method in practice is by numerically solving for the flex points. If the given model is far from reduced, then usually several of the flex points are very close to one another, which makes the computation of the lines difficult. Another practical problem is that the two spaces of quadrics we compute are only approximate and therefore will usually not have nontrivial intersection.

6.3.2. *Using the 3-torsion on E.* This is the method described in [Fi1, §9.5]. Let $F(x,y,z)$ be a ternary cubic with invariants c_4 and c_6 and Hessian H as defined in Section 2. Let $T=(x_T,y_T)$ be a 3-torsion point on the Jacobian

$$E: \quad y^2 = x^3 - 27c_4x - 54c_6.$$

Then the cubic $\mathcal{T}(x,y,z) = 2x_TF - 3H$ is the product of 3 linear forms. (In [Hi, II.7] it is called a "syzygetic triangle".) Making a change of coordinates (if necessary) we may suppose $\mathcal{T}(1,0,0) \neq 0$. We label the coefficients

$$\mathcal{T}(x,y,z) = rx^3 + s_1x^2y + s_2xy^2 + s_3y^3 + t_1x^2z + t_2xz^2 + t_3z^3 + uxyz + vy^2z + wyz^2.$$

The proof of [Fi1, Theorem 7.1] describes how to compute a formula for M_T, where the entries are polynomials in $r, s_1, s_2, \ldots, w$ and y_T. Up to a scaling, this works out as $M_T = rA + 2y_TB$ where

$$\begin{aligned}
A_{11} &= -12rs_2w - 36rs_3t_2 + 12ruv + 4s_1^2w + 4s_1s_2t_2 - 8s_1t_1v - s_1u^2 + 12s_3t_1^2 \\
A_{12} &= -54rs_3w + 18rv^2 + 6s_1s_2w - 3s_1uv - 6s_2t_1v + 9s_3t_1u \\
A_{13} &= -81rs_3t_3 + 9rvw + 9s_1s_2t_3 - 3s_1t_2v - 3s_2t_1w + 9s_3t_1t_2 \\
A_{21} &= 36rs_2t_2 - 9ru^2 - 12s_1^2t_2 + 12s_1t_1u - 12s_2t_1^2 \\
A_{22} &= 24rs_2w + 18rs_3t_2 - 15ruv - 8s_1^2w - 2s_1s_2t_2 + 10s_1t_1v + 2s_1u^2 - 3s_2t_1u - 6s_3t_1^2 \\
A_{23} &= 54rs_2t_3 - 9ruw - 18s_1^2t_3 + 6s_1t_1w + 3s_1t_2u - 6s_2t_1t_2 \\
A_{31} &= 0 \\
A_{32} &= -18rs_2v + 27rs_3u + 6s_1^2v - 3s_1s_2u - 18s_1s_3t_1 + 6s_2^2t_1 \\
A_{33} &= -12rs_2w + 18rs_3t_2 + 3ruv + 4s_1^2w - 2s_1s_2t_2 - 2s_1t_1v - s_1u^2 + 3s_2t_1u - 6s_3t_1^2
\end{aligned}$$

and $B = rB_1 + (s_1^2t_2 - s_1t_1u + s_2t_1^2)E_{13}$ with

$$B_1 = \begin{pmatrix} s_1u - 2s_2t_1 & s_1v - 3s_3t_1 & s_1w - 4s_2t_2 - t_1v + u^2 \\ -3ru + 2s_1t_1 & -3rv + s_2t_1 & -3rw + s_1t_2 \\ 6rs_2 - 2s_1^2 & 9rs_3 - s_1s_2 & 3rv - s_1u + s_2t_1 \end{pmatrix}.$$

(Notes: E_{ij} is the 3 by 3 matrix with (i,j) entry 1 and all other entries 0. Our matrices A and B would be called $r^3(\det P)A$ and r^3B in the notation of [Fi1].) This formula comes with the caveat (see [Fi1, Remark 7.2]) that it may give zero. However, this will never happen for both T and $-T$, so we get round the problem by computing M_T as $(M_{-T})^{-1}$.

Once we have computed M_T for all $T \in E[3]$ the reduction covariant is computed using Corollary 6.3.

6.4. **Reduction of 4-coverings.** We could again try to find the reduction covariant starting from the 16 hyperosculating points on $\mathcal{C}$ and the quadruples of planes containing four of them, which are the analogue of the syzygetic triangles. However, this approach does not seem to be very promising.

Instead, we use the fact that below the given 4-covering $\mathcal{C}$, there is a 2-covering $\mathcal{C}_2$; let $\pi : \mathcal{C} \to \mathcal{C}_2$ be the covering map. If A and B are the symmetric matrices corresponding to the quadrics defining $\mathcal{C} \subset \mathbb{P}^3$, then $\mathcal{C}_2$ has equation $y^2 = F(x,z)$ where

$$F(x,z) := \det(Ax + Bz)\,.$$

Applying reduction to the quartic on the right hand side, we find a good basis of the pencil of quadrics. It remains to find the reduction covariant of $\mathcal{C}$.

Let $\theta_j \in \mathbb{C}$ $(j = 1,2,3,4)$ be the ramification points of $\mathcal{C}_2 \to \mathbb{P}^1$, *i.e.*, the roots of $f(X) = F(X,1)$. Let G_j $(j = 1,2,3,4)$ be a linear form (unique up to scaling) describing the preimage of θ_j on $\mathcal{C} \subset \mathbb{P}^3$. Then (fixing the polynomials giving the covering map $\pi : \mathcal{C} \to \mathcal{C}_2$) there are $\alpha_j \in \mathbb{C}^\times$ such that

$$(x - \theta_j\, z) \circ \pi = \alpha_j G_j^2\,.$$

Now the action of $T \in E[4]$ on $\mathcal{C}$ induces the action of $2T \in E[2]$ on $\mathcal{C}_2$. Therefore the action of $T \in E[2]$ on $\mathcal{C}$ will be trivial on $\mathcal{C}_2$, hence the corresponding matrix $M_T \in \mathrm{SL}_4$ will fix the G_j up to sign. In fact, it can be checked that the action of $E[2]$ on $\mathbb{P}^3$ lifts to a representation on $\mathbb{C}^4$, which is isomorphic to the regular representation, and the G_j span the four eigenspaces. So any Hermitian form that is invariant under H_4 must be invariant under $E[2]$ and thus be of the form

$$\sum_{j=1}^{4} \lambda_j |G_j|^2\,.$$

It remains to determine the coefficients λ_j.

Lemma 6.8. *Keep the notation introduced so far, and let $f(X) = F(X,1)$. Then the reduction covariant of $\mathcal{C}$ is the positive definite Hermitian form*

$$\varphi_{\mathbb{C}}(\mathcal{C}) = \sum_{j=1}^{4} \frac{|\alpha_j|}{|f'(\theta_j)|^{1/2}} |G_j|^2\,.$$

If $\mathcal{C}$ is defined over $\mathbb{R}$, then the restriction of this Hermitian form to $\mathbb{R}^4$ will be the positive definite quadratic form $\varphi_{\mathbb{R}}(\mathcal{C})$.

Proof: We first check that the given form is invariant under $\mathrm{SL}_2(\mathbb{C})$ acting on $\mathbb{P}^1$ (*i.e.*, does not depend on the choice of basis of the pencil of quadrics). We know (see Section 6.2.1 above) that $\sum_{j=1}^4 |f'(\theta_j)|^{-1}|x - \theta_j z|^2$ is an $\mathrm{SL}_2(\mathbb{C})$-covariant; the same computation (which deals with each summand separately) shows that $\sum_{j=1}^4 |f'(\theta_j)|^{-1/2}|x - \theta_j z|$ is a covariant as well. But $|x - \theta_j z| = |\alpha_j G_j^2|$, and the coordinates in G_j are not affected by the $\mathrm{SL}_2(\mathbb{C})$-action, so the expression given in the statement is invariant.

Now we check that the given form is covariant with respect to the action of $\mathrm{SL}_4(\mathbb{C})$. But this is clear since every $\alpha_j G_j^2$ is covariant.

Since we can move any $\mathcal{C}$ into standard form by the action of $\mathrm{SL}_2(\mathbb{C}) \times \mathrm{SL}_4(\mathbb{C})$, it now suffices to verify that our formula gives the correct result when $\mathcal{C}$ is in standard form

$$a(x_0^2 + x_2^2) + 2b\, x_1 x_3 = a(x_1^2 + x_3^2) + 2b\, x_0 x_2 = 0\,.$$

In this case, the 2-covering $\mathcal{C}_2$ is given by

$$y^2 = (a^4 + b^4)x^2 z^2 - a^2 b^2 (x^4 + z^4)$$

and the map π (see Lemma 4.6 for formulae), followed by the map $\mathcal{C}_2 \to \mathbb{P}^1$, is given by

$$(x : z) = \big(b^3(x_1^2 + x_3^2) + 2a^3\, x_0 x_2 : -b^3(x_0^2 + x_2^2) - 2a^3\, x_1 x_3\big)\,.$$

The roots θ_j of $f(X) = -a^2 b^2 X^4 + (a^4 + b^4)X^2 - a^2 b^2$ are a/b, $-a/b$, b/a, $-b/a$, and up to a common factor $b^4 - a^4$, we can take $\alpha_j = 1/b$, $1/b$, $1/a$, $-1/a$ and $G_j = x_1 - x_3$, $x_1 + x_3$, $x_0 - x_2$, $x_0 + x_2$. Also, $|f'(\theta_j)| = c|\theta_j|$ for some constant c. Since $|\alpha_j|/|\theta_j|^{1/2}$ has the same value $|ab|^{-1/2}$ for all j, our expression gives, up to a constant factor again,

$$|x_1 - x_3|^2 + |x_1 + x_3|^2 + |x_0 - x_2|^2 + |x_0 + x_2|^2 = 2\big(|x_0|^2 + |x_1|^2 + |x_2|^2 + |x_3|^2\big)\,,$$

which is the correct result for a 4-covering in standard form. □

In order to find the α_j and G_j, we can make use of a result from [Fi3], where it is observed that $\alpha_j G_j^2$ is the quadratic form corresponding to the matrix

$$e\theta_j^{-1} A + M_1 + \theta_j M_2 + a\theta_j^2 B\,;$$

here $F(x, z) = \det(Ax + Bz) = ax^4 + bx^3 z + cx^2 z^2 + dxz^3 + ez^4$ and M_1, M_2 are obtained from the relation (4.3) in the proof of Lemma 4.6.

7. Examples

In this section we illustrate minimisation and reduction for two explicit examples over $\mathbb{Q}$ (one a 3-covering and the other a 4-covering). We then give references to further examples.

7.1. **Minimisation and reduction of a 3-covering.** We consider the elliptic curve 105630d1 in [Cr3] with Weierstrass equation

$$E: \qquad y^2 + xy = x^3 + x^2 - 114848533x - 472424007827.$$

Computing the 3-Selmer group (see [ScSt]) we find $\mathrm{Sel}^{(3)}(\mathbb{Q}, E) \cong \mathbb{Z}/3\mathbb{Z}$. In [CFOSS] we show how to write down elements of the 3-Selmer group explicitly as 3-coverings of E. In this case our MAGMA programs find (before minimisation and reduction) that a generator is represented by the 3-covering $\mathcal{C} \subset \mathbb{P}^2$ with equation

$$\begin{aligned} F_1(x,y,z) = 27089x^3 + 2142y^3 + 291938z^3 + 10008x^2y - 127341x^2z \\ + 92937xy^2 + 104736y^2z + 21093xz^2 - 71172yz^2 - 2655xyz. \end{aligned}$$

(Random choices in the programs mean it need not return the same cubic every time. However, the answer will always be $\mathbb{Q}$-equivalent to F_1, and this can be checked using the algorithm in [Fi1].) The discriminant of this ternary cubic is $\Delta(F_1) = 3^{12} \cdot 503^{12} \cdot \Delta_E$ where $\Delta_E = 2^{39} \cdot 3 \cdot 5^9 \cdot 7^3 \cdot 503$ is the minimal discriminant of E. So F_1 has level 1 at the primes 3 and 503. Reducing mod 3 we find $F_1(x,y,z) = 2(x+z)^3 \pmod 3$. The level is decreased by the first iteration of our algorithm (see Theorem 4.3). Explicitly we put

$$F_2(x,y,z) = \frac{1}{3^2} F_1(3x-y,z,y).$$

Likewise we find $F_2(x,y,z) \equiv 284(x+329y+33z)^3 \pmod{503}$ and our algorithm puts

$$\begin{aligned} F_3(x,y,z) &= \frac{1}{503^2} F_2(503x - 33y + z, z, y - 10z) \\ &= 40877301x^3 - 11504y^3 + 12z^3 - 8035425x^2y - 64887x^2z \\ &\qquad + 526580xy^2 - 200y^2z + 5803xz^2 - 383yz^2 + 7307xyz. \end{aligned}$$

The 3-torsion of $y^2 = x^3 - 27c_4x - 54c_6$ over $\mathbb{C}$ is generated by

$$S = (667989.968057, 420236746.168), \quad T = (-264330.994609, 34120617.5970i).$$

The formulae in Section 6.3.2 show that S and T act on $\{F_3 = 0\}$ via

$$M_S = \begin{pmatrix} 285.46 & -19.022 & 3.4264 \\ 4352.6 & -290.04 & 52.341 \\ 509.05 & -33.785 & 4.5806 \end{pmatrix}$$

and

$$M_T = \begin{pmatrix} -50.656 + 47.060i & 3.2758 - 3.3464i & 0.11909 + 2.2683i \\ -786.55 + 717.15i & 50.871 - 51.000i & 1.8675 + 34.587i \\ -119.84 + 93.073i & 7.8268 - 6.5354i & -0.21547 + 3.9405i \end{pmatrix}.$$

We have scaled these matrices to have determinant 1. By Corollary 6.3 the reduction covariant has matrix

$$A = \begin{pmatrix} 176413988.185 & -11560848.1174 & 3471.84429193 \\ -11560848.1174 & 757736.524016 & -1499.92503970 \\ 3471.84429193 & -1499.92503970 & 13237.5156939 \end{pmatrix}.$$

Running the LLL algorithm on the lattice with Gram matrix A results in the unimodular transformation.

$$U = \begin{pmatrix} 0 & 0 & 1 \\ 4 & 61 & 6 \\ -3 & -46 & -4 \end{pmatrix}.$$

Accordingly we put $F_4(x,y,z) = F_3(4y-3z, 61y-46z, x+6y-4z)$ and find

$$\begin{aligned} F_4(x,y,z) = {} & 12x^3 + 12y^3 + 171z^3 + 65x^2y + 65x^2z \\ & - 94y^2z + 87xz^2 + 101yz^2 + 7xyz. \end{aligned}$$

This ternary cubic has solution

$$(x : y : z) = (345420 : -1638959 : -373029)$$

which by the formulae in [AKM³P] maps down to a point

$$x = \frac{-7487262077360842262305875791498106521 7}{109435039457696221^2}$$

$$y = \frac{510430470253203891760984943078477987229582280619164075 87}{109435039457696221^3}$$

on $E(\mathbb{Q})$ of canonical height $86.5313\ldots$. Since the torsion subgroup of $E(\mathbb{Q})$ is trivial, it follows that $\operatorname{rank} E(\mathbb{Q}) = 1$. It is equally convenient to find this generator using Heegner points.

Note that the MAGMA implementation of 3-descent does the minimisation and reduction automatically. To extract the intermediate model $F_1(x,y,z) = 0$, one should first specify that 3-descent prints out some of its working, using the command `SetVerbose("ThreeDescent",1);`

7.2. **Minimisation and reduction of a 4-covering.** In [Sk, §8.1], an example is given of a 4-covering $\mathcal{C}$ of the elliptic curve $E : y^2 = x^3 - 1221$ that represents an element of exact order 4 in the Shafarevich-Tate group of E. The symmetric matrices corresponding to the two quadrics defining $\mathcal{C} \subset \mathbb{P}^3$ are given as (to keep with our convention, we multiply by 2 so that entries are the second partial derivatives)

$$A = 2\begin{pmatrix} -1 & 11 & -66 & 396 \\ 11 & -66 & 396 & -2520 \\ -66 & 396 & -2520 & 16\,335 \\ 396 & -2520 & 16\,335 & -105\,786 \end{pmatrix} \quad \text{and} \quad B = 2\begin{pmatrix} -1 & -3 & 33 & -198 \\ -3 & 33 & -198 & 1188 \\ 33 & -198 & 1188 & -7560 \\ -198 & 1188 & -7560 & 49\,005 \end{pmatrix}.$$

We will use $x_1, \ldots, x_4$ as the coordinates on $\mathbb{P}^3$. We find that

$$\det(Ax + Bz) = 2^4 \cdot 3^8(-9x^4 + 13x^3z - 18x^2z^2 + 3z^4),$$

which makes it clear that the model is non-minimal at $p = 2$ and $p = 3$. We compute that the discriminant of our quadric intersection is $(2 \cdot 3^4)^{12}$ times the (minimal) discriminant $-2^4\,3^5\,11^2\,37^2$ of E, which shows that the level at 2 is 1 and the level at 3 is 4; the model is already minimal at all other primes.

We first minimise at $p = 3$. According to our algorithm (see Section 4.3), we have to look at the reductions of A and B mod 3, which are

$$\bar{A} = \begin{pmatrix} 1&1&0&0 \\ 1&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{pmatrix} \quad \text{and} \quad \bar{B} = \begin{pmatrix} 1&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{pmatrix}$$

The common nullity is $s = 2$, and the reduced quadratic forms already involve only the first two variables. They represent zero simultaneously over $\mathbb{F}_3$; the plane $x_1 = 0$ is contained in the reduction of the curve. So we apply the transformation $[\frac{1}{3}I_2, \mathrm{Diag}(3,1,1,1)]$, resulting in the new pair of matrices (which we will again denote A and B)

$$A = \begin{pmatrix} -6 & 22 & -132 & 792 \\ 22 & -44 & 264 & -1680 \\ -132 & 264 & -1680 & 10890 \\ 792 & -1680 & 10890 & -70524 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} -6 & -6 & 66 & -396 \\ -6 & 22 & -132 & 792 \\ 66 & -132 & 792 & -5040 \\ -396 & 792 & -5040 & 32670 \end{pmatrix}$$

The level at $p = 3$ of the new model is 3. Reducing mod 3, we have now

$$\bar{A} = \begin{pmatrix} 0&1&0&0 \\ 1&1&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{pmatrix} \quad \text{and} \quad \bar{B} = \begin{pmatrix} 0&0&0&0 \\ 0&1&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{pmatrix}$$

The common nullity is again $s = 2$, and there is a plane contained in the reduction. This time, the plane is $x_2 = 0$, so we swap x_1 and x_2 before we apply $[\frac{1}{3}I_2, \mathrm{Diag}(3,1,1,1)]$. The result is a model of level 2:

$$A = \begin{pmatrix} -132 & 22 & 264 & -1680 \\ 22 & -2 & -44 & 264 \\ 264 & -44 & -560 & 3630 \\ -1680 & 264 & 3630 & -23508 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 66 & -6 & -132 & 792 \\ -6 & -2 & 22 & -132 \\ -132 & 22 & 264 & -1680 \\ 792 & -132 & -1680 & 10890 \end{pmatrix}$$

Now we get a different situation mod 3:

$$\bar{A} = \begin{pmatrix} 0&1&0&0 \\ 1&1&1&0 \\ 0&1&1&0 \\ 0&0&0&0 \end{pmatrix} \quad \text{and} \quad \bar{B} = \begin{pmatrix} 0&0&0&0 \\ 0&1&1&0 \\ 0&1&0&0 \\ 0&0&0&0 \end{pmatrix}$$

The common nullity is $s = 1$. We swap x_1 and x_4 so that the reduced forms only involve the last three variables. Then we see that we are in 'Situation 2', so we apply the transformation $[I_2, \mathrm{Diag}(\frac{1}{3},1,1,1)]$. This results in a model of level 1, given by

$$A = \begin{pmatrix} -2612 & 88 & 1210 & -560 \\ 88 & -2 & -44 & 22 \\ 1210 & -44 & -560 & 264 \\ -560 & 22 & 264 & -132 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 1210 & -44 & -560 & 264 \\ -44 & -2 & 22 & -6 \\ -560 & 22 & 264 & -132 \\ 264 & -6 & -132 & 66 \end{pmatrix}$$

In the last minimisation step at $p = 3$, the reductions are now

$$\bar{A} = \begin{pmatrix} 1&1&1&1 \\ 1&1&1&1 \\ 1&1&1&0 \\ 1&1&0&0 \end{pmatrix} \quad \text{and} \quad \bar{B} = \begin{pmatrix} 1&1&1&0 \\ 1&1&1&0 \\ 1&1&0&0 \\ 0&0&0&0 \end{pmatrix}$$

The common nullity is again $s = 1$, and the common kernel is spanned by $(1,-1,0,0)$. We move it to $(1,0,0,0)$ and are in 'Situation 2' again. After applying

$[I_2, \mathrm{Diag}(\frac{1}{3}, 1, 1, 1)]$, we obtain a model that is now minimal at $p = 3$.

$$A = \begin{pmatrix} -310 & 30 & 418 & -194 \\ 30 & -2 & -44 & 22 \\ 418 & -44 & -560 & 264 \\ -194 & 22 & 264 & -132 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 144 & -14 & -194 & 90 \\ -14 & -2 & 22 & -6 \\ -194 & 22 & 264 & -132 \\ 90 & -6 & -132 & 66 \end{pmatrix}$$

We still have to minimise at $p = 2$, using the algorithm described in Section 4.4. We first find the 'double' of our model:

$$\begin{aligned} \mathfrak{d}'(A, B) = (P, Q) = \big(&2^2(6413x^2 - 5665xz + 1248z^2), \\ &2^2(41126578x^4 - 72659303x^3z \\ &\quad + 48099091x^2z^2 - 14139840xz^3 + 1557501z^4)\big) \end{aligned}$$

We see that we already have $v_2(P) \geq 1$ and $v_2(Q) \geq 2$. The common kernel of the reductions mod 2 of the two quadratic forms is spanned by $(1, 1, 0, 1)$ and $(0, 0, 1, 0)$, so the common nullity is $s = 2$. We change coordinates so that the common kernel is given by $x_1 = x_2 = 0$. Then the reductions of the quadrics are x_1^2 and x_2^2, so they do not simultaneously represent zero. We apply the 'flip-flop' transformation $[\frac{1}{2}I_2, \mathrm{Diag}(2, 2, 1, 1)]$, after which the reductions are x_3x_4 and x_4^2, so now there is the plane $x_4 = 0$ contained in the reduction of the curve. We swap x_1 and x_4 and then apply $[\frac{1}{2}I_2, \mathrm{Diag}(2, 1, 1, 1)]$ to obtain a pair of matrices representing a globally minimal model:

$$A = \begin{pmatrix} -728 & -424 & 319 & -474 \\ -424 & -252 & 187 & -280 \\ 319 & 187 & -140 & 209 \\ -474 & -280 & 209 & -310 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 348 & 198 & -152 & 220 \\ 198 & 114 & -86 & 130 \\ -152 & -86 & 66 & -97 \\ 220 & 130 & -97 & 144 \end{pmatrix}$$

We now apply reduction to this model as described in Section 6.4. We have

$$\det(Ax + Bz) = 4(-9x^4 + 13x^3z - 18x^2z^2 + 3z^4)\,.$$

Following [AKM^{3}P] and [Fi3], we compute the quadratic forms T_1, T_2 whose symmetric matrices M_1, M_2 are given by

$$\mathrm{adj}\big(\mathrm{adj}(A)x + \mathrm{adj}(B)z)\big) = 4^2 \cdot 81Ax^3 - 4 \cdot 9M_1x^2z + 4 \cdot 3M_2xz^2 + 4^2 \cdot 9Bz^3\,.$$

Then, writing Q_1 and Q_2 for the quadratic forms corresponding to A and B,

$$\alpha G^2 = 12\theta^{-1}Q_1 + T_1 + \theta T_2 - 36\theta^2 Q_2$$

for θ a root of $f(X) = \det(XA + B)$. We can for example take

$$G = (-18\theta^3 - 28\theta^2 + 6\theta + 2)x_1 + (18\theta^3 - 26\theta^2 + 2)x_2 + (18\theta^2 + \theta - 3)x_3 - 2x_4$$

and $\alpha = -1395\theta^3 + 1367\theta^2 - 2155\theta - 1001$. Also, $f'(\theta) = 12(-12\theta^3 + 13\theta^2 - 12\theta)$. The matrix corresponding to $\sqrt{12}\sum_\theta |\alpha||G|^2/|f'(\theta)|^{1/2}$ is (to five decimal digits precision)

$$\begin{pmatrix} 8857.72019 & 5117.00780 & -3885.97776 & 5665.67630 \\ 5117.00780 & 3080.24124 & -2279.16858 & 3348.18401 \\ -3885.97776 & -2279.16858 & 1716.07038 & -2498.36286 \\ 5665.67630 & 3348.18401 & -2498.36286 & 3706.96839 \end{pmatrix}.$$

We apply LLL to this Gram matrix and obtain the reducing transformation matrix

$$U = \begin{pmatrix} -5 & -2 & -6 & 0 \\ -6 & -3 & -7 & -1 \\ -15 & -7 & -17 & 0 \\ 3 & 1 & 4 & 1 \end{pmatrix},$$

which finally brings the two matrices defining $\mathcal{C}$ into the form

$$U^t A U = \left(\begin{smallmatrix} -2 & 0 & -1 & -2 \\ 0 & -2 & -1 & 0 \\ -1 & -1 & -2 & 2 \\ -2 & 0 & 2 & -2 \end{smallmatrix}\right) \quad \text{and} \quad U^t B U = \left(\begin{smallmatrix} 0 & 0 & -1 & 1 \\ 0 & 2 & -1 & -1 \\ -1 & -1 & 0 & -1 \\ 1 & -1 & -1 & -2 \end{smallmatrix}\right).$$

These correspond, after a sign change, to the quadratic forms

$$Q_1 = x_1^2 + x_1x_3 + 2x_1x_4 + x_2^2 + x_2x_3 + x_3^2 - 2x_3x_4 + x_4^2 \quad \text{and}$$
$$Q_2 = x_1x_3 - x_1x_4 - x_2^2 + x_2x_3 + x_2x_4 + x_3x_4 + x_4^2 .$$

7.3. **Further examples and applications.** One useful application of the methods described in this paper is to help find large generators in the Mordell-Weil group of an elliptic curve E. This has already be demonstrated in Section 7.1. Each rational point $P \in E(\mathbb{Q})$ lifts to one of the n-coverings of E. If we have a nice and small (*i.e.*, minimised and reduced) model $\mathcal{C}$ of this n-covering, then the logarithmic height with respect to $\mathcal{C} \to \mathbb{P}^{n-1}$ of the preimage Q of P in $\mathcal{C}(\mathbb{Q})$ will be smaller by a factor of about $\frac{1}{2n}$ than the logarithmic x-coordinate height of P — standard properties of heights imply that

$$h(Q) = \frac{1}{2n} h_x(P) + O(1)$$

where the implied constant depends on the equations defining $\mathcal{C} \to \mathbb{P}^{n-1}$. If the equations have small coefficients, this constant should be small as well. Therefore we can hope to find P much more easily by searching for Q on $\mathcal{C}$. In fact, this application was the motivation for the first tentative steps towards reduction of 4-coverings. The story begins with [GPZ], where the authors determined Mordell-Weil generators for all Mordell curves $y^2 = x^3 + D$, with D a nonzero integer of absolute value at most 10^4 (in order to determine all the integral points on these curves), with one exception, $D = 7823$. The analytic rank of this curve is 1, so we know that the Mordell-Weil rank must be also 1; however the Birch and Swinnerton-Dyer Conjecture predicts a generator of fairly large height. One of us

(Stoll) used minimisation and reduction of 4-coverings in a fairly *ad hoc* fashion to find a good model of the one relevant 4-covering of $E : y^2 = x^3 + 7823$, so that a point search on this 4-covering curve was successful, thus resolving this last open case. The result was reported in a posting [Sto] to the `NMBRTHRY` mailing list. We give a short summary of the steps and the result. By a standard 2-descent, one obtains a 2-covering curve

$$C : y^2 = -18x^4 + 116x^3 + 48x^2 - 12x + 30\,.$$

A second 2-descent on C following [MSS] produces a 4-covering of E, whose initial model was given by quadrics with coefficients of up 15 decimal digits. Using the methods described here, one finds a model $D \subset \mathbb{P}^3$ given by

$$\begin{aligned} 2x_1x_2 + x_1x_3 + x_1x_4 + x_2x_4 + x_3^2 - 2x_4^2 &= 0 \\ x_1^2 + x_1x_3 - x_1x_4 + 2x_2^2 - x_2x_3 + 2x_2x_4 - x_3^2 - x_3x_4 + x_4^2 &= 0 \end{aligned}$$

It is not very difficult to find the point $P = (116 : 207 : 474 : -332)$ on D. This point then gives rise to the point

$$Q = \left(\frac{53463613}{32109353}, \frac{23963346820191122}{32109353^2}\right)$$

on C, which in turn finally produces the Mordell-Weil generator on E, with coordinates

$$\begin{aligned} x &= \frac{2263582143321421502100209233517777}{119816734100955612^2} \\ y &= \frac{186398152584623305624837551485596770028144776655756}{119816734100955612^3} \end{aligned}$$

Note that in the version given in the mailing list posting, the model was not minimal at 2 (in fact, it had level 2 at 2).

4-descent including minimisation and reduction was also used to find some of the elliptic curves of high rank and prescribed torsion listed in [Du], for example the curve with $E(\mathbb{Q}) \cong \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}^4$.

Minimised and reduced models of 2-, 3-, and 4-coverings provide the starting point for the computation of 6- and 12-coverings as described in [Fi5]. These then allow us to find even larger generators (of logarithmic canonical height > 600). For example, this method was used to find the last missing generators for curves of prime conductor and rank at least 2 in the Stein-Watkins database [SW].

A table giving representatives of all elements of order 3 in the Shafarevich-Tate groups of all elliptic curves of conductor $< 130\,000$ can be found at [Fi6]. (It is only known that the table is complete if one assumes the conjecture of Birch and Swinnerton-Dyer.) The final form of these ternary cubics was obtained by applying the methods described in this paper to the original models produced by the algorithms described in [ScSt] and [CFOSS].

References

[AKM^{3}P] S.Y. An, S.Y. Kim, D.C. Marshall, S.H. Marshall, W.G. McCallum and A.R. Perlis, Jacobians of genus one curves, *J. Number Theory* **90** (2001), no. 2, 304–315.

[ARVT] M. Artin, F. Rodriguez-Villegas and J. Tate, On the Jacobians of plane cubics, *Adv. Math.* **198** (2005), no. 1, 366–382.

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

[BLR] S. Bosch, W. Lütkebohmert and M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), **21**, Springer-Verlag, Berlin, 1990.

[Co] I. Connell, *Elliptic Curve Handbook*, (unpublished on-line notes), McGill University, 1996.

[Cr1] J.E. Cremona, *Algorithms for modular elliptic curves*, Second edition, Cambridge University Press, Cambridge, 1997.

[Cr2] J.E. Cremona, Reduction of binary cubic and quartic forms, *LMS J. Comput. Math.* **2** (1999), 64–94 (electronic).

[Cr3] J.E. Cremona, Tables of Elliptic Curves,
`http://www.warwick.ac.uk/staff/J.E.Cremona/ftp/data/`

[CFOSS] J.E. Cremona, T.A. Fisher, C. O'Neil, D. Simon and M. Stoll, Explicit n-descent on elliptic curves, I Algebra, *J. reine angew. Math.* **615** (2008) 121-155; II Geometry, *J. reine angew. Math.* **632** (2009) 63-84; *III Algorithms*, in preparation.

[De] P. Deligne, Courbes elliptiques: formulaire d'après J. Tate, in *Modular functions of one variable, IV*, (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 53–73. Lecture Notes in Math., Vol. **476**, Springer, Berlin, 1975.

[DS] Z. Djabri and N. P. Smart, A comparison of direct and indirect methods for computing Selmer groups of an elliptic curve, in *Algorithmic number theory (ANTS-III),* J. Buhler (ed.), Lecture Notes in Comput. Sci. **1423**, Springer, Berlin, 1998, 502–513.

[Do] I. Dolgachev, Lectures on invariant theory, LMS Lecture Note Series, 296, CUP, Cambridge, 2003.

[Du] A. Dujella, High rank elliptic curves with prescribed torsion, online table at
`http://web.math.hr/~duje/tors/tors.html`

[Fi1] T.A. Fisher, Testing equivalence of ternary cubics, in *Algorithmic number theory (ANS-VII)*, F. Hess, S. Pauli, M. Pohst (eds.), Lecture Notes in Comput. Sci. **4076**, Springer, 2006, 333-345.

[Fi2] T.A. Fisher, A new approach to minimising binary quartics and ternary cubics, *Math. Res. Lett.* **14** (2007) Issue 4, 597–613.

[Fi3] T.A. Fisher, Some improvements to 4-descent on an elliptic curve, in *Algorithmic number theory (ANTS-VIII)*, A.J. van der Poorten, A. Stein (eds.), Lecture Notes in Comput. Sci. **5011**, Springer, 2008, 125–138.

[Fi4] T.A. Fisher, The invariants of a genus one curve, *Proc. Lond. Math. Soc.* (3) **97** (2008) 753-782.

[Fi5] T.A. Fisher, Finding rational points on elliptic curves using 6-descent and 12-descent, *Journal of Algebra* **320** (2008), no. 2, 853-884.

[Fi6] T.A. Fisher, Elements of order 3 in the Tate-Shafarevich group, online table at `http://www.dpmms.cam.ac.uk/~taf1000/g1data/order3.html`

[GPZ] J. Gebel, A. Pethő and H.G. Zimmer, On Mordell's equation, *Compositio Math.* **110** (1998), no. 3, 335–367.

[Hi] D. Hilbert, *Theory of algebraic invariants*, Cambridge University Press, Cambridge, 1993.

[HP] W.V.D. Hodge and D. Pedoe, *Methods of algebraic geometry*, Volume II, Reprint of the 1952 original, Cambridge University Press, Cambridge, 1994.

[Hu] K. Hulek, *Projective geometry of elliptic curves.* Astérisque No. **137** (1986), 143 pp.

[Ja] N. Jacobson, *Basic algebra I*, Second edition, W.H. Freeman and Company, New York, 1985.

[Ju] G. Julia, Étude sur les formes binaires non quadratiques à indeterminées réelles ou complexes, *Mem. Acad. Sci. l'Inst. France* **55** (1917) 1-293.

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

[Kr] A. Kraus, Quelques remarques à propos des invariants c_4, c_6 et Δ d'une courbe elliptique. *Acta Arith.* **54** (1989), no. 1, 75–80.

[La] M. Laska, An algorithm for finding a minimal Weierstrass equation for an elliptic curve, *Math. Comp.* **38** (1982), no. 157, 257–260.

[LLL] A.K. Lenstra, H.W. Lenstra and L. Lovász, Factoring polynomials with rational coefficients, *Math. Ann.* **261** (1982), no. 4, 515–534.

[Liu] Q. Liu, Modèles entiers des courbes hyperelliptiques sur un corps de valuation discrète, *Trans. Amer. Math. Soc.* **348** (1996), no. 11, 4577–4610.

[M] MAGMA is described in W. Bosma, J. Cannon and C. Playoust, The MAGMA algebra system I: The user language, *J. Symb. Comb.* **24**, (1997) 235–265. (See also the MAGMA home page at `http://magma.maths.usyd.edu.au/magma/`.)

[MSS] J. R. Merriman, S. Siksek and N. P. Smart, Explicit 4-descents on an elliptic curve, *Acta Arith.* **77** (1996), no. 4, 385–404.

[Mi] J. S. Milne, *Lectures on Etale Cohomology*, Version 2.10, available online from `http://www.jmilne.org/math/CourseNotes/math732.html`.

[Po] B. Poonen, An explicit algebraic family of genus-one curves violating the Hasse principle, *J. Théor. Nombres Bordeaux* **13** (2001), no. 1, 263–274.

[Sa] M. Sadek, *Models of genus one curves*, PhD thesis, University of Cambridge, in preparation.

[ScSt] E.F. Schaefer and M. Stoll, How to do a p-descent on an elliptic curve, *Trans. Amer. Math. Soc.* **356** no. 3 (2004), 1209–1231

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

[Sik] S. Siksek, *Descent on curves of genus one*, PhD thesis, University of Exeter, 1995. See `http://www.warwick.ac.uk/staff/S.Siksek/papers/phdnew.pdf`

[Sil1] J.H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, New York, 1986.

[Sil2] J.H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer-Verlag, New York, 1994.

[Sk] A. Skorobogatov, *Torsors and rational points*, Cambridge University Press, Cambridge, 2001.

[SW] W.A. Stein and M. Watkins, A database of elliptic curves—first report, *Algorithmic number theory* (Sydney 2002), 267–275, Lect. Notes Comp. Sci. **2369**, Springer, Berlin 2002.

[SC1] M. Stoll and J.E. Cremona, Minimal models for 2-coverings of elliptic curves, *LMS J. Comput. Math.* **5** (2002), 220–243.

[SC2] M. Stoll and J.E. Cremona, On the reduction theory of binary forms, *J. reine angew. Math.* **565**, 79–99 (2003).

[Sto] M. Stoll, posting to the NMBRTHRY mailing list, 10 January 2002. See `http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0201&L=NMBRTHRY&P=R500&I=-3`.

[Ta] J. Tate, Algorithm for determining the type of a singular fiber in an elliptic pencil, in *Modular functions of one variable IV*, B.J. Birch and W. Kuyk (eds.), Lecture Notes in Math. **476**, Springer, Berlin, 1975.

[We1] A. Weil, Remarques sur un mémoire d'Hermite, *Arch. Math.* (Basel) **5**, (1954) 197–202.

[We2] A. Weil, Euler and the Jacobians of elliptic curves, *Arithmetic and geometry, Vol. I*, 353–359, Progr. Math., **35**, Birkhäuser, Boston, MA, 1983.

[Wo] T.O. Womack, *Explicit descent on elliptic curves*, PhD thesis, University of Nottingham, 2003. See `http://www.warwick.ac.uk/staff/J.E.Cremona/theses/`

Mathematics Institute, University of Warwick, Coventry CV4 7AL, UK
E-mail address: `J.E.Cremona@warwick.ac.uk`

University of Cambridge, DPMMS, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, UK
E-mail address: `T.A.Fisher@dpmms.cam.ac.uk`

Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany
E-mail address: `Michael.Stoll@uni-bayreuth.de`