MINIMISATION AND REDUCTION OF 5-COVERINGS OF ELLIPTIC CURVES

TOM FISHER

Abstract. We consider models for genus one curves of degree 5, which arise in explicit 5-descent on elliptic curves. We prove a theorem on the existence of minimal models with the same invariants as the minimal model of the Jacobian elliptic curve and give an algorithm for computing such models. Finally we describe how to reduce genus one models of degree 5 defined over $\mathbb{Q}$.

Introduction

Let E be an elliptic curve defined over a number field K. An *n-covering* of E is a morphism $\pi : C \to E$ where C is a smooth curve of genus one, and $\pi = [n] \circ \psi$ for some isomorphism $\psi : C \to E$ defined over $\overline{K}$. An n-descent on E computes the everywhere locally soluble n-coverings of E. For such n-coverings we have $\psi^*(n.0_E) \sim D$ for some K-rational divisor D on C. The complete linear system $|D|$ defines a morphism $C \to \mathbb{P}^{n-1}$. Thus in the cases $n = 2, 3, 4$ we may represent C by a binary quartic, ternary cubic, or pair of quadrics in 4 variables. In the case $n = 5$ we obtain curves $C \subset \mathbb{P}^4$ of degree 5 that are defined by the 4×4 Pfaffians of a 5×5 alternating matrix of linear forms.

The question naturally arises as to how we can choose co-ordinates on $\mathbb{P}^{n-1}$ so that the equations for C have small coefficients. In the cases $n = 2, 3, 4$ this was answered in [CFS], using the combination of two techniques called *minimisation* and *reduction*. In this paper we extend to the case $n = 5$. We establish results on minimisation over an arbitrary local field (immediately implying results over any number field of class number 1), whereas those for reduction are specific to the case $K = \mathbb{Q}$. Implementations of our algorithms in the case $K = \mathbb{Q}$ are available in MAGMA [BCP].

1. Genus one models

A *genus one model* (of degree 5) is a 5×5 alternating matrix of linear forms in variables $x_1, \ldots, x_5$. We write $X_5(R)$ for the space of all genus one models with coefficients in a ring R. Models Φ and Φ' are *R-equivalent* if $\Phi' = [A, B]\Phi$ for some $A, B \in \mathrm{GL}_5(R)$. Here the action of A is via $\Phi \mapsto A\Phi A^T$, and the action of B is

Date: 21st December 2011.

via $(\Phi_{ij}(x_1,\ldots,x_5)) \mapsto (\Phi_{ij}(x'_1,\ldots,x'_5))$ where $x'_j = \sum_{i=1}^5 B_{ij}x_i$. The *determinant* of the transformation $g = [A, B]$ is $\det g = (\det A)^2 \det B$.

We write $\mathrm{Pf}(\Phi)$ for the row vector $(p_1,\ldots,p_5)$ where p_i is $(-1)^{i-1}$ times the Pfaffian of the 4×4 submatrix obtained by deleting the ith row and column of Φ. This choice of signs is made so that $\mathrm{Pf}(\Phi)\Phi = 0$. For $A \in \mathrm{GL}_5(R)$ we note that $\mathrm{Pf}(A\Phi A^T) = \mathrm{Pf}(\Phi)\,\mathrm{adj}\,A$.

A genus one model $\Phi \in X_5(K)$ over a field K is *non-singular* if the subscheme $\mathcal{C}_\Phi = \{\mathrm{rank}\,\Phi \le 2\} \subset \mathbb{P}^4$ defined by the 4×4 Pfaffians of Φ is a smooth curve of genus one. We write $K[X_5]$ for the polynomial ring in the 50 coefficients of a genus one model. A polynomial $F \in K[X_5]$ is an *invariant* of *weight* k if $F\circ g = (\det g)^k F$ for all $g = [A, B]$ with $A, B \in \mathrm{GL}_5(\overline{K})$. Taking A and B to be scalar matrices shows that an invariant of weight k is a homogeneous polynomial of degree $5k$.

Theorem 1.1. *Let $c_4, c_6, \Delta \in \mathbb{Z}[X_5]$ be the invariants of weights $4, 6, 12$, satisfying $c_4^3 - c_6^2 = 1728\Delta$, and scaled as specified in* [F1].

(i) *A model $\Phi \in X_5(K)$ is non-singular if and only if $\Delta(\Phi) \neq 0$.*

(ii) *There exist $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}[X_5]$ and $b_2, b_4, b_6 \in \mathbb{Z}[X_5]$ satisfying*

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \qquad b_4 = a_1a_3 + 2a_4, \qquad b_6 = a_3^2 + 4a_6, \\ c_4 &= b_2^2 - 24b_4, \qquad c_6 = -b_2^3 + 36b_2b_4 - 216b_6. \end{aligned} \tag{1}$$

(iii) *If $\Phi \in X_5(K)$ is non-singular then $\mathcal{C}_\Phi$ has Jacobian elliptic curve*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_i = a_i(\Phi)$.

For the proof of Theorem 1.1(ii) we use the following lemma.

Lemma 1.2. *Let $c_4, c_6, \Delta \in R = \mathbb{Z}[x_1,\ldots,x_N]$ be primitive polynomials satisfying $c_4^3 - c_6^2 = 1728\Delta$. If there exists $a_1 \in R$ satisfying $a_1^2c_4 + c_6 \equiv 0 \pmod 4$ then there exist $a_2, a_3, a_4, a_6, b_2, b_4, b_6 \in R$ satisfying (1).*

Proof: By unique factorisation in $\mathbb{F}_3[x_1,\ldots,x_N]$ and the Chinese Remainder Theorem there exists $b_2 \in R$ with $c_4 \equiv b_2^2 \pmod 3$, $c_6 \equiv -b_2^3 \pmod 3$ and $b_2 \equiv a_1^2 \pmod 4$. Then $b_2c_4 + c_6 \equiv 0 \pmod{12}$ and $c_4^3 \equiv c_6^2 \equiv b_2^2c_4^2 \pmod{24}$. Since c_4 is primitive it follows that $c_4 \equiv b_2^2 \pmod{24}$. Next putting $x = b_2$ in an identity of Kraus [K],

$$(x^2 - c_4)^3 = (x^3 - 3xc_4 - 2c_6)(x^3 + 2c_6) + 3(xc_4 + c_6)^2 + c_6^2 - c_4^3,$$

we deduce $b_2^3 - 3b_2c_4 - 2c_6 \equiv 0 \pmod{432}$. We put $b_4 = (b_2^2 - c_4)/24$ and $b_6 = (b_2^3 - 3b_2c_4 - 2c_6)/432$. Then $0 \equiv c_4^3 - c_6^2 \equiv 16b_2^2(b_2b_6 - b_4^2) \pmod{64}$ and so $b_2b_6 \equiv b_4^2 \pmod 4$. By unique factorisation in $\mathbb{F}_2[x_1,\ldots,x_N]$ there exists $a_3 \in R$ with $b_4 \equiv a_1a_3 \pmod 2$. Then $b_4^2 \equiv a_1^2a_3^2 \pmod 4$ and $b_6 \equiv a_3^2 \pmod 4$. We put $a_2 = (b_2 - a_1^2)/4$, $a_4 = (b_4 - a_1a_3)/2$ and $a_6 = (b_6 - a_3^2)/4$. □

PROOF OF THEOREM 1.1: (i) This is [F1, Theorem 4.4(ii)].
(ii) By Lemma 1.2 it suffices to construct $a_1 \in \mathbb{Z}[X_5]$ with $a_1^2c_4 + c_6 \equiv 0 \pmod 4$. In [F1, Section 10] we constructed an invariant $a_1 \in \mathbb{F}_2[X_5]$ of weight 1 and showed that together with Δ it generates the ring of invariants in characteristic 2. In particular $c_4 \equiv a_1^4 \pmod 2$ and $c_6 \equiv a_1^6 \pmod 2$. So if we lift a_1 to $\mathbb{Z}[X_5]$ then $a_1^2c_4 + c_6 = 2f$ for some $f \in \mathbb{Z}[X_5]$. Since a_1 is an invariant mod 2, a_1^2 is an invariant mod 4, and f is an invariant mod 2. Therefore $f \equiv \lambda a_1^6 \pmod 2$ for some $\lambda \in \{0, 1\}$. Hence $a_1^2c_4 \pm c_6 \equiv 0 \pmod 4$. Specialising to one of the Weierstrass models in [F1, Section 6] shows that the sign is +.
(iii) It is shown in [F1, Theorem 4.4(iii)] that if K is a perfect field with characteristic not 2 or 3 then $\mathcal{C}_\Phi$ has Jacobian $y^2 = x^3 - 27c_4(\Phi)x - 54c_6(\Phi)$. The proof is now identical to that of [CFS, Theorem 2.10]. This generalises a result of Artin, Rodriguez-Villegas and Tate [ARVT] in the case $n = 3$. □

2. MINIMISATION THEOREMS

Let K be a discrete valuation field, with ring of integers $\mathcal{O}_K$, and normalised valuation $v : K^\times \to \mathbb{Z}$. We assume throughout that the residue field k is perfect. A genus one model $\Phi \in X_5(K)$ is *integral* if it has coefficient in $\mathcal{O}_K$. If Φ is non-singular and integral then, by Theorem 1.1 and the standard formulae for transforming Weierstrass equations, we have $v(\Delta(\Phi)) = v(\Delta_E) + 12\ell(\Phi)$ where Δ_E is the minimal discriminant of $E = \mathrm{Jac}(\mathcal{C}_\Phi)$ and $\ell(\Phi)$ is a non-negative integer we call the *level*. We say that Φ is *minimal* if $v(\Delta(\Phi))$, or equivalently the level, is minimal among all integral models K-equivalent to Φ. Notice that if $\Phi' = g\Phi$ for some $g = [A, B]$ with $A, B \in \mathrm{GL}_5(K)$ then $\ell(\Phi') = \ell(\Phi) + v(\det g)$.

Theorem 2.1. *Let $\Phi \in X_5(K)$ be non-singular.*

(i) *(Weak minimisation theorem) If $\mathcal{C}_\Phi(K) \neq \emptyset$ then Φ is K-equivalent to an integral model of level 0.*
(ii) *(Strong minimisation theorem) If $\mathcal{C}_\Phi(L) \neq \emptyset$ where L is an unramified extension of K then Φ is K-equivalent to an integral model of level 0.*

In this section we prove the weak minimisation theorem. In Section 3 we describe an explicit algorithm for minimising. Inspection of this algorithm shows that the minimal level is unchanged by an unramified extension. Theorem 2.1(ii) then follows from Theorem 2.1(i). In Section 7 we prove a converse to the strong minimisation theorem, thereby showing this result is best possible.

We refer to [CFS, Section 2] for notation and results analogous to those in Section 1 for genus one models of degree 4, i.e. quadric intersections. Let E be an elliptic curve over K, and D a K-rational divisor on E of degree $n = 4$ or 5. The complete linear system $|D|$ defines an embedding $E \subset \mathbb{P}^{n-1}$. The image is defined by a genus one model $\Phi \in X_n(K)$, and this model is uniquely determined,

up to K-equivalence, by the pair $(E, [D])$. Moreover every non-singular model $\Phi \in X_n(K)$ with $\mathcal{C}_\Phi(K) \neq \emptyset$ arises in this way. Therefore Theorem 2.1(i) is an immediate consequence of the following.

Theorem 2.2. *Let E/K be an elliptic curve, with integral Weierstrass equation*

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

and let $D \in \mathrm{Div}_K(E)$ be a divisor on E of degree $n = 4$ or 5. Then $(E, [D])$ can be represented by an integral genus one model with the same discriminant as (2).

The case $n = 4$ is proved in [CFS, Theorem 3.8]. To deduce the case $n = 5$ from the case $n = 4$ we use the following lemma.

Lemma 2.3. *Let $D \in \mathrm{Div}_K(E)$ be a divisor of degree 4 and let $P \in E(K)$. Let $\ell_i, \alpha_i, \beta_i$ for $i = 1, 2, 3$ be linear forms in $x_1, \ldots, x_4$ over K. The following statements are equivalent.*

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

$$\begin{aligned} \ell_1\alpha_1 + \ell_2\alpha_2 + \ell_3\alpha_3 &= 0 \\ \ell_1\beta_1 + \ell_2\beta_2 + \ell_3\beta_3 &= 0 \end{aligned} \tag{3}$$

and P is the point defined by $\ell_1 = \ell_2 = \ell_3 = 0$.

(ii) *The pair $(E, [D + P])$ is represented by the genus one model of degree 5*

$$\begin{pmatrix} 0 & \gamma & \alpha_1 & \alpha_2 & \alpha_3 \\ & 0 & \beta_1 & \beta_2 & \beta_3 \\ & & 0 & \ell_3 & -\ell_2 \\ & - & & 0 & \ell_1 \\ & & & & 0 \end{pmatrix} \tag{4}$$

where $\gamma = x_5$ and P is the point $(x_1 : \ldots : x_5) = (0 : \ldots : 0 : 1)$.

Proof: An isomorphism $\psi : C_4 \to C_5$, between the curves C_4 and C_5 defined by (3) and (4), is given by

$$\psi : (x_1 : x_2 : x_3 : x_4) \mapsto (x_1\ell_i : x_2\ell_i : x_3\ell_i : x_4\ell_i : \alpha_j\beta_k - \alpha_k\beta_j)$$

(where i, j, k are any cyclic permutation of $1, 2, 3$) with inverse

$$\psi^{-1} : (x_1 : x_2 : x_3 : x_4 : x_5) \mapsto (x_1 : x_2 : x_3 : x_4).$$

This isomorphism identifies the points $\{\ell_1 = \ell_2 = \ell_3 = 0\} \in C_4(K)$ and $(0 : \ldots : 0 : 1) \in C_5(K)$. To prove the equivalence of (i) and (ii) we note that if $C_4 \subset \mathbb{P}^3$ meets some plane in the divisor $D = P_1 + P_2 + P_3 + P_4$ then the points $\psi(P_i)$ and $(0 : \ldots : 0 : 1)$ are a hyperplane section for $C_5 \subset \mathbb{P}^4$. □

Lemma 2.4. *The genus one models (3) and (4) have the same invariants.*

PROOF: Let Φ be the matrix (4) and write $P = \mathrm{Pf}(\Phi) = (p_1, \ldots, p_5)$. According to [F1, Section 5.4] there are invariant differentials ω_4 on $C_4 = \{p_1 = p_2 = 0\} \subset \mathbb{P}^3$ and ω_5 on $C_5 = \{\mathrm{rank}\,\Phi \leq 2\} \subset \mathbb{P}^4$ given by

$$\omega_n = \frac{x_1^2 d(x_2/x_1)}{\Omega_n(x_1, \ldots, x_n)}$$

where

$$\Omega_4 = \frac{\partial p_1}{\partial x_3}\frac{\partial p_2}{\partial x_4} - \frac{\partial p_1}{\partial x_4}\frac{\partial p_2}{\partial x_3} \qquad \text{and} \qquad \Omega_5 = \frac{\partial P}{\partial x_3}\,\frac{\partial \Phi}{\partial x_5}\,\frac{\partial P^T}{\partial x_4}.$$

In the expression for Ω_5 we have written the partial derivative of a matrix as a short-hand for the matrix of partial derivatives. Since the only entries of Φ to involve x_5 are in the top left 2×2 submatrix, it is clear that $\Omega_4 = \pm\Omega_5$. Hence the isomorphism $\psi : C_4 \to C_5$ identifies the invariant differentials ω_4 and ω_5 (up to sign). It follows by [F1, Proposition 5.23] that (3) and (4) have the same invariants c_4, c_6 and Δ. □

PROOF OF THEOREM 2.2: Let $D \in \mathrm{Div}_K(E)$ be a divisor of degree 4, and let $P \in E(K)$. We show that if the theorem holds for D then it holds for $D + P$. Suppose $(E, [D])$ is represented by an integral quadric intersection with discriminant Δ. Since $\mathcal{O}_K$ is a principal ideal domain, $\mathrm{SL}_4(\mathcal{O}_K)$ acts transitively on $\mathbb{P}^3(K)$. So we may assume P is the point $(x_1 : x_2 : x_3 : x_4) = (0 : 0 : 0 : 1)$. Our model is now of the form (3) with $\ell_i = x_i$ for $i = 1, 2, 3$. We may choose the linear forms α_i and β_i to have coefficients in $\mathcal{O}_K$. Then the genus one model (4) is an integral model of discriminant Δ representing the pair $(E, [D + P])$. □

3. Minimisation algorithms

For $\Phi \in X_5(\mathcal{O}_K)$ we write $\phi \in X_5(k)$ for its reduction mod π. The *singular locus* $\mathrm{Sing}\,\mathcal{C}_\phi$ is the set of points $P \in \mathcal{C}_\phi$ with tangent space of dimension greater than 1. (We make this definition regardless of whether $\mathcal{C}_\phi$ is a curve. In particular all points on components of dimension at least 2 are singular.) For example, if ϕ takes the form (4) with $\gamma = x_5$ and $\ell_i, \alpha_i, \beta_i$ linear forms in $x_1, \ldots, x_4$, then $P = (0 : \ldots : 0 : 1)$ is singular if and only if ℓ_1, ℓ_2, ℓ_3 are linearly dependent. An integral genus one model $\Phi \in X_5(\mathcal{O}_K)$ is *saturated* if its 4×4 Pfaffians $p_1, \ldots, p_5$ are linearly independent mod π. We write I_m for the $m \times m$ identity matrix.

Our algorithm for minimising genus one models of degree 5 generalises the algorithm for models of degree 3 in [CFS, Section 4B].

Theorem 3.1. *Let $\Phi \in X_5(\mathcal{O}_K)$ be saturated and of positive level.*

(i) *The singular locus* $\mathrm{Sing}\,\mathcal{C}_\phi$ *does not span* $\mathbb{P}^4$.

(ii) *Let $B \in \mathrm{GL}_5(\mathcal{O}_K)$ represent a change of co-ordinates on $\mathbb{P}^4$ mapping the linear span of the singular locus in (i) to $\{x_{m+1} = \ldots = x_5 = 0\}$. Then there exist $A \in \mathrm{GL}_5(K)$ and $\mu \in K^\times$ such that $[A, \mu\,\mathrm{Diag}(I_m, \pi I_{5-m})B]\Phi$ is an integral model of the same or smaller level.*

(iii) *If Φ is non-minimal then repeating the procedure in (ii) either gives a non-saturated model or decreases the level after finitely many iterations.*

As it stands Theorem 3.1 does not give an algorithm for minimising since we must show how to find A and μ in (ii), and show how to decrease the level of a non-saturated model. We do this in Theorem 3.2 below. Theorem 3.1 is proved in Sections 4 and 5. In Section 6 we bound the number of iterations required in (iii).

Theorem 3.2. *Let $\Phi \in X_5(\mathcal{O}_K)$ be non-singular. Let ℓ_0 be the minimum of the levels of all integral models that are K-equivalent to Φ via a transformation of the form $[A, \mu I_5]$ where $A \in \mathrm{GL}_5(K)$ and $\mu \in K^\times$.*

(i) *We may compute an integral model of the form $[A, \mu I_5]\Phi$ with level ℓ_0 as follows:*

Step 1: *Write $\mathrm{Pf}(\Phi) = (p_1, \ldots, p_5)$. Compute $A = (a_{ij}) \in \mathrm{GL}_5(K)$ and quadrics $q_1, \ldots, q_5 \in \mathcal{O}_K[x_1, \ldots, x_5]$ such that $p_j = \sum_{i=1}^5 a_{ij} q_i$ and $q_1, \ldots, q_5$ are linearly independent mod π. Then replace Φ by $[A, \mu I_5]\Phi$ where $\mu \in K^\times$ is chosen so that Φ has coefficients in $\mathcal{O}_K$ not all in $\pi\mathcal{O}_K$.*

Step 2: *Replace Φ by $[A, I_5]\Phi$ where $A \in \mathrm{GL}_5(\mathcal{O}_K)$ is chosen so that the first two rows of Φ are divisible by π^e, with $e \geq 0$ as large as possible. Then divide the first row and column by π^e.*

(ii) *If the model computed in Step 1 is non-saturated, then we may compute an integral model of level smaller than ℓ_0 by modifying Step 2 so that we divide the first two rows and columns by π^e, and then make a transformation of the form $[I_5, B]$ to preserve integrality.*

Proof: With the notation of Step 1 we have

$$\mathrm{Pf}(A\Phi A^T) = \mathrm{Pf}(\Phi)\,\mathrm{adj}\,A = (q_1, \ldots, q_5)A\,\mathrm{adj}\,A = (\det A)(q_1, \ldots, q_5).$$

So after Step 1 we have $\mathrm{Pf}(\Phi) = (\lambda q_1, \ldots, \lambda q_5)$ where $\lambda := \mu^2 \det A \in \mathcal{O}_K$. We split into the cases $v(\lambda) = 0$ and $v(\lambda) \geq 1$. First we need two lemmas.

Lemma 3.3. *Let $\Phi, \Phi' \in X_5(\mathcal{O}_K)$ be non-singular models with $\Phi' = [A, \mu I_5]\Phi$ for some $A \in \mathrm{GL}_5(K)$ and $\mu \in K^\times$.*

(i) *If Φ is saturated then $\ell(\Phi') \geq \ell(\Phi)$ with equality if and only if Φ and Φ' are $\mathcal{O}_K$-equivalent.*

(ii) *If Φ and Φ' are of the form output by Step 1 then they are $\mathcal{O}_K$-equivalent.*

PROOF: We have $\mathrm{Pf}(\Phi') = \mathrm{Pf}(\Phi)M$ where $M := \mu^2 \operatorname{adj} A$.
(i) Since Φ is saturated, M has entries in $\mathcal{O}_K$. Hence $\ell(\Phi') - \ell(\Phi) = \frac{1}{2}v(\det M) \geq 0$ with equality if and only if $M \in \mathrm{GL}_5(\mathcal{O}_K)$. If $M \in \mathrm{GL}_5(\mathcal{O}_K)$ then replacing $[A, \mu I_5]$ by $[\lambda A, \lambda^{-2}\mu I_5]$ for suitable $\lambda \in K^\times$ we may assume $A \in \mathrm{GL}_5(\mathcal{O}_K)$. Since Φ and Φ' have the same level they must therefore be $\mathcal{O}_K$-equivalent.
(ii) Since $\mathrm{Pf}(\Phi)$ and $\mathrm{Pf}(\Phi')$ are scalar multiples of bases for the same $\mathcal{O}_K$-module, some scalar multiple of M belongs to $\mathrm{GL}_5(\mathcal{O}_K)$. Replacing $[A, \mu I_5]$ by $[\lambda A, \lambda^{-2}\mu I_5]$ for suitable $\lambda \in K^\times$ we may assume $A \in \mathrm{GL}_5(\mathcal{O}_K)$. Since Φ and Φ' are primitive they must therefore be $\mathcal{O}_K$-equivalent. □

Lemma 3.4. *Let $\phi \in X_5(k)$ be a genus one model all of whose 4×4 Pfaffians are identically zero. Then ϕ is k-equivalent to either*

$$\begin{pmatrix} 0 & \ell_2 & \ell_3 & \ell_4 & \ell_5 \\ & 0 & 0 & 0 & 0 \\ & & 0 & 0 & 0 \\ & - & & 0 & 0 \\ & & & & 0 \end{pmatrix} \quad \textit{or} \quad \begin{pmatrix} 0 & x_1 & x_2 & 0 & 0 \\ & 0 & x_3 & 0 & 0 \\ & & 0 & 0 & 0 \\ & - & & 0 & 0 \\ & & & & 0 \end{pmatrix}$$

where $\ell_2, \ldots, \ell_5$ are linear forms.

PROOF: This is clear. □

We now complete the proof of Theorem 3.2. If $v(\lambda) = 0$ then Φ is saturated and we are done by Lemma 3.3(i). So suppose $e := v(\lambda) \geq 1$. In Step 1 the matrix A has entries in $\mathcal{O}_K$. So $v(\mu) \leq 0$ and the level is increased by

$$2v(\det A) + 5v(\mu) \leq 2v(\mu^2 \det A) = 2e.$$

Lemma 3.3(ii) shows that when we apply Step 1 to both Φ and the model implicit in the definition of ℓ_0 then we obtain models that are $\mathcal{O}_K$-equivalent. So it will suffice to show that Step 2 reduces the level by $2e$, whereas the modified version in (ii) reduces the level by more than $2e$.

Since $\mathrm{Pf}(\Phi) = (\lambda q_1, \ldots, \lambda q_5)$ we have $(q_1, \ldots, q_5)\Phi = 0$. The reduction of Φ takes one of the forms specified in Lemma 3.4. In the first case we have $q_1\ell_j \equiv 0 \pmod{\pi}$ for $j = 2, \ldots, 5$. This contradicts the choices of $q_1, \ldots, q_5$ and μ in Step 1. So we must be in the second case. Replacing Φ by an $\mathcal{O}_K$-equivalent model we may assume it takes the form (4) with $\ell_i = x_i$ for $i = 1, 2, 3$ and $\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3, \gamma$ linear forms that vanish mod π. By row and column operations we may assume $\alpha_2 \in \langle x_2, \ldots, x_5 \rangle$ and $\alpha_3 \in \langle x_3, \ldots, x_5 \rangle$. Then since $\pi^e \,|\, (x_1\alpha_1 + x_2\alpha_2 + x_3\alpha_3)$ we have $\pi^e \,|\, \alpha_1, \alpha_2, \alpha_3$. Likewise we may assume $\pi^e \,|\, \beta_1, \beta_2, \beta_3$. The remaining Pfaffians show that $\pi^e \mid \gamma$. Steps 2 and its modified version in (ii) now reduce the level by $2e$ and $3e$ respectively. □

Corollary 3.5. *For the proof of Theorem 3.1 we are free to replace Φ by an $\mathcal{O}_K$-equivalent model, and to replace K by an unramified field extension.*

PROOF: Let $\Phi_1, \Phi_2 \in X_5(\mathcal{O}_K)$ be $\mathcal{O}_K$-equivalent models and $\Phi_1', \Phi_2' \in X_5(\mathcal{O}_K)$ the models returned by Theorem 3.1(ii). Lemma 3.3(i) and [CFS, Lemma 4.1] together show that if Φ_1' is saturated and $\ell(\Phi_1') = \ell(\Phi_2')$ then Φ_1' and Φ_2' are $\mathcal{O}_K$-equivalent. Therefore the number of iterations required in Theorem 3.1(iii) depends only on the $\mathcal{O}_K$-equivalence class of Φ.

For the final statement we note that the performance of the algorithms in Theorems 3.1 and 3.2 is unchanged by an unramified field extension. □

Replacing K by its strict Henselisation, we may assume in the next three sections that K is Henselian and its residue field k is algebraically closed.

4. The singular locus

In this section and the next we prove Theorem 3.1.

Lemma 4.1. *Let $\phi \in X_5(k)$ be a genus one model. Suppose $\Gamma \subset \mathcal{C}_\phi$ is either a line or a (non-singular) conic. Then either $\Gamma \subset \operatorname{Sing} \mathcal{C}_\phi$ or*

$$\#(\Gamma \cap \operatorname{Sing} \mathcal{C}_\phi) = \begin{cases} 1 & \text{if } c_4(\phi) = c_6(\phi) = 0, \\ 2 & \text{otherwise.} \end{cases}$$

PROOF: (i) If $\mathcal{C}_\phi$ contains the line $\Gamma = \{x_3 = x_4 = x_5 = 0\}$, but not every point on Γ is singular, then (unless $\mathcal{C}_\phi$ is a cone – which is an easy special case with $c_4(\phi) = c_6(\phi) = 0$) we may suppose ϕ is

$$\begin{pmatrix} 0 & x_1 & x_2 & * & * \\ & 0 & * & \alpha & \beta \\ & & 0 & \gamma & \delta \\ & - & & 0 & x_5 \\ & & & & 0 \end{pmatrix}$$

where $\alpha, \beta, \gamma, \delta$ and the entries $*$ are linear forms in x_3, x_4, x_5. By row and column operations (and substitutions for x_1 and x_2) we may suppose $\alpha, \beta, \gamma, \delta$ do not involve x_5. We write $\alpha = \alpha_3 x_3 + \alpha_4 x_4, \ldots, \delta = \delta_3 x_3 + \delta_4 x_4$ and put

$$q(s,t) = \det\left(\begin{pmatrix} \gamma_3 & \gamma_4 \\ \delta_3 & \delta_4 \end{pmatrix} s - \begin{pmatrix} \alpha_3 & \alpha_4 \\ \beta_3 & \beta_4 \end{pmatrix} t \right).$$

By the Jacobian criterion we have

$$\Gamma \cap \operatorname{Sing} \mathcal{C}_\phi = \{(s : t : 0 : 0 : 0) \mid q(s,t) = 0\}.$$

A calculation using Lemma 2.4 shows that $c_4(\phi) = \Delta(q)^2$ and $c_6(\phi) = -\Delta(q)^3$ where $\Delta(q)$ is the discriminant of the binary quadratic form q.

(ii) Suppose $\mathcal{C}_\phi$ contains the conic $\Gamma = \{f(x_1, x_2, x_3) = x_4 = x_5 = 0\}$, but not every point on Γ is singular. Let $\mathrm{Pf}(\phi) = (p_1, \ldots, p_5)$. Replacing ϕ by an equivalent model we may suppose $p_i(x_1, x_2, x_3, 0, 0) = 0$ for $i = 1, 2, 3, 4$ and $p_5(x_1, x_2, x_3, 0, 0) = f$. Since $\mathrm{Pf}(\phi)\phi = 0$, and Γ is not contained in any component of $\mathcal{C}_\phi$ of higher dimension, we may further suppose the last column of ϕ has entries $x_4, x_5, 0, 0, 0$. The monomials appearing in the invariants c_4 and c_6 are limited by the fact they are invariant under all pairs of diagonal matrices. These restrictions show that $c_4(\phi)$ and $c_6(\phi)$ are unchanged if we set $x_4 = x_5 = 0$ in all entries of ϕ outside the last row and column. Writing $f = \sum_{i \le j} a_{ij} x_i x_j$ and $\phi_{34} = \sum b_i x_i$ we put

$$\delta = \begin{vmatrix} 2a_{11} & a_{12} & a_{13} & b_1 \\ a_{12} & 2a_{22} & a_{23} & b_2 \\ a_{13} & a_{23} & 2a_{33} & b_3 \\ b_1 & b_2 & b_3 & 0 \end{vmatrix}.$$

A calculation using Lemma 2.4 shows that $c_4(\phi) = \delta^2$ and $c_6(\phi) = -\delta^3$. By a change of co-ordinates we may suppose $f = x_1 x_3 - x_2^2$. Then δ is the discriminant of the binary quadratic form $q(s, t) = \phi_{34}(s^2, st, t^2, 0, 0)$ and by the Jacobian criterion

$$\Gamma \cap \operatorname{Sing} \mathcal{C}_\phi = \{(s^2 : st : t^2 : 0 : 0) \mid q(s, t) = 0\}. \qquad \square$$

Lemma 4.2. *Let $\phi \in X_5(k)$ be a genus one model. Suppose the 4×4 Pfaffians $p_1, \ldots, p_5$ are linearly independent and $c_4(\phi) = c_6(\phi) = 0$. Then either $\operatorname{Sing} \mathcal{C}_\phi$ is a linear subspace of $\mathbb{P}^4$ or ϕ is equivalent to a model of the form*

$$\begin{pmatrix} 0 & \xi & \alpha & \beta & \eta \\ & 0 & \gamma & \delta & x_5 \\ & & 0 & x_5 & 0 \\ & - & & 0 & 0 \\ & & & & 0 \end{pmatrix} \tag{5}$$

where $\xi, \eta, \alpha, \beta, \gamma, \delta$ are linear forms in $x_1, \ldots, x_5$.

Proof: If $P_1, P_2 \in \operatorname{Sing} \mathcal{C}_\phi$ are distinct and the line ℓ between them is contained in $\mathcal{C}_\phi$ then by Lemma 4.1 we have $\ell \subset \operatorname{Sing} \mathcal{C}_\phi$. So either $\operatorname{Sing} \mathcal{C}_\phi$ is a linear subspace of $\mathbb{P}^4$ or there exist $P_1, P_2 \in \operatorname{Sing} \mathcal{C}_\phi$ joined by a line not contained in $\mathcal{C}_\phi$. We move these points to $(1 : 0 : \ldots : 0)$ and $(0 : 1 : \ldots : 0)$. Writing $\phi = \sum x_i M_i$, the matrices M_1 and M_2 have rank 2 but their sum has rank 4. Therefore ϕ is equivalent to a model with $\phi_{12} = x_1$, $\phi_{34} = x_2$ and all other ϕ_{ij} (for $i < j$)

linear forms in x_3, x_4, x_5. Since P_1 and P_2 are singular, ϕ_{35} and ϕ_{45} are linearly dependent, and ϕ_{15} and ϕ_{25} are linearly dependent. So the space of linear forms spanned by the entries of the last column has dimension at most 2. In fact it has dimension exactly 2, since $p_1, \ldots, p_5$ are linearly independent.

Replacing ϕ by an equivalent model we may assume it has last column with entries $x_4, x_5, 0, 0, 0$. The transformation used here does not move P_1 and P_2 but may change the matrices M_1 and M_2. Let $\Gamma = \{x_4 = x_5 = p_5 = 0\} \subset \mathcal{C}_\phi$. Then P_1 and P_2 are contained in Γ but the line between them is not. It follows that Γ is either a non-singular conic or a pair of concurrent lines. In either case Lemma 4.1 shows that $\Gamma \subset \operatorname{Sing} \mathcal{C}_\phi$. By the Jacobian criterion it follows that $\phi_{34} \in \langle x_4, x_5 \rangle$. However ϕ_{34} is non-zero since $p_1, \ldots, p_5$ are linearly independent. Therefore ϕ is equivalent to a model of the form (5). □

Lemma 4.3. *Let $\Phi \in X_5(\mathcal{O}_K)$ be a saturated non-singular model with reduction ϕ of the form (5). Suppose $\operatorname{Sing} \mathcal{C}_\phi$ has linear span $\{x_{m+1} = \ldots = x_5 = 0\}$.*

(i) *There exist $A \in \mathrm{GL}_5(K)$ and $\mu \in K^\times$ such that $[A, \mu \operatorname{Diag}(I_m, \pi I_{5-m})]\Phi$ is an integral model of the same or smaller level.*

(ii) *Suppose that either $\delta = 0$ and $\Phi_{45} \equiv 0 \pmod{\pi^2}$, or $\Phi_{35} \equiv \Phi_{45} \equiv 0 \pmod{\pi^2}$. Then there is a transformation as in (i) that decreases the level.*

Proof: Computing the 4×4 Pfaffians of (5) we find

$$\mathcal{C}_\phi = \{\eta = x_5 = \alpha\delta - \beta\gamma = 0\} \cup \{\gamma = \delta = x_5 = 0\}. \tag{6}$$

First suppose γ, δ, x_5 are linearly dependent. By an $\mathcal{O}_K$-equivalence we may assume $\delta = 0$. Then $\{\gamma = x_5 = 0\} \subset \operatorname{Sing} \mathcal{C}_\phi \subset \{x_5 = 0\}$. Therefore $m = 3$ or 4. The required transformations are as follows.

	$m = 3$	$m = 4$
(i)	$A = \operatorname{Diag}(\pi, 1, 1, 1, 1), \quad \mu = \pi^{-1}$	$A = \operatorname{Diag}(\pi, \pi, 1, 1, 1), \quad \mu = \pi^{-1}$
(ii)	$A = \operatorname{Diag}(\pi, 1, 1, 1, 1), \quad \mu = \pi^{-1}$	$A = \operatorname{Diag}(\pi, 1, 1, \pi^{-1}, \pi^{-1}), \quad \mu = 1$

Now suppose γ, δ, x_5 are linearly independent. Since Φ is saturated η, x_5 are linearly independent. A calculation shows that $\operatorname{Sing} \mathcal{C}_\phi$ is the first of the two components in (6). Therefore $m = 2$ or 3. If $m = 2$ then we may assume $\beta, \gamma, \delta, \eta$ are linear combinations of x_3, x_4, x_5. The required transformations are as follows

	$m = 2$	$m = 3$
(i)	$A = \operatorname{Diag}(\pi, 1, 1, 1, 1), \quad \mu = \pi^{-1}$	$A = \operatorname{Diag}(1, 1, 1, 1, \pi^{-1}), \quad \mu = 1$
(ii)	$A = \operatorname{Diag}(1, 1, 1, \pi^{-1}, \pi^{-1}), \quad \mu = 1$	$A = \operatorname{Diag}(\pi, \pi, 1, 1, \pi^{-1}), \quad \mu = \pi^{-1}$

□

We now prove the first two parts of Theorem 3.1. Let $\Phi \in X_5(\mathcal{O}_K)$ be saturated and of positive level. Lemma 4.2 shows that either $\operatorname{Sing} \mathcal{C}_\phi$ is a linear subspace

or $\mathcal{C}_\phi$ is contained in a hyperplane. Since $\mathcal{C}_\phi$ is defined by 5 linearly independent quadrics it cannot be all of $\mathbb{P}^4$. This proves Theorem 3.1(i).

The proof of Theorem 3.1(ii) in the case ϕ takes the form (5) was already given in Lemma 4.3(i). So by Lemma 4.2 we may assume $\operatorname{Sing}\mathcal{C}_\phi = \{x_{m+1} = \ldots = x_5 = 0\}$. We apply Lemma 3.4 to the reduction mod π of $[I_5, \operatorname{Diag}(I_m, \pi I_{5-m})]\Phi$. In the second case of that lemma we have $m \geq 3$. We take $A = \operatorname{Diag}(1,1,1,1,\pi^{-1})$ and $\mu = 1$. Otherwise we are in the first case. If $m \geq 2$ then we take $A = \operatorname{Diag}(\pi,1,1,1,1)$ and $\mu = \pi^{-1}$. It remains to treat the case $m = 1$, in other words the case $\operatorname{Sing}\mathcal{C}_\phi$ is a point.

By [F1, Lemma 5.8] every component of $\mathcal{C}_\phi$ has dimension at least 1. So if $\operatorname{Sing}\mathcal{C}_\phi$ is just a point then there are also smooth points on $\mathcal{C}_\phi$. Since K is Henselian it follows that $\mathcal{C}_\Phi(K) \neq \emptyset$ and so, by Theorem 2.1(i), Φ is non-minimal. With this extra hypothesis we show in the next section that the singular point on $\mathcal{C}_\phi$ is non-regular (as a point on the $\mathcal{O}_K$-scheme $\mathcal{C}_\Phi$).

We may suppose $\phi_{12} = x_1$ and all other ϕ_{ij} (for $i < j$) are linear forms in $x_2, \ldots, x_5$. Since $P = (1 : 0 : \ldots : 0)$ is singular, $\phi_{34}, \phi_{35}, \phi_{45}$ are linearly dependent. So replacing Φ by an $\mathcal{O}_K$-equivalent model we may assume $\phi_{45} = 0$. In the presence of the stronger condition that P is non-regular we may further arrange that the coefficient of x_1 in Φ_{45} is divisible by π^2. Taking $A = \operatorname{Diag}(1,1,1,\pi^{-1},\pi^{-1})$ and $\mu = 1$ now preserves the level.

5. Weights and slopes

In this section we complete the proof of Theorem 3.1.

Definition 5.1. (i) The set of *weights* is

$$\mathcal{W} = \left\{ (r,s) \in \mathbb{Z}^5 \times \mathbb{Z}^5 \;\middle|\; \begin{array}{c} r_1 \leq r_2 \leq \ldots \leq r_5, \quad s_1 \leq s_2 \leq \ldots \leq s_5, \\ 2\sum_{i=1}^5 r_i = 1 + \sum_{i=1}^5 s_i \end{array} \right\}.$$

(ii) A *weight for* $\Phi \in X_5(\mathcal{O}_K)$ is $(r,s) \in \mathcal{W}$ such that the model

$$[\operatorname{Diag}(\pi^{-r_1}, \ldots, \pi^{-r_5}), \operatorname{Diag}(\pi^{s_1}, \ldots, \pi^{s_5})]\Phi \tag{7}$$

has coefficients in $\mathcal{O}_K$.
(iii) Let $w = (r,s)$ and $w' = (r',s')$ be weights. Then w *dominates* w' if

$$\max(r_i + r_j - s_k, 0) \geq \max(r'_i + r'_j - s'_k, 0)$$

for all $1 \leq i < j \leq 5$ and $1 \leq k \leq 5$.

Let $\mathbf{1} = (1,1,\ldots,1)$. Then $\lambda \in \mathbb{Z}$ acts on $\mathcal{W}$ as $(r,s) \mapsto (r + \lambda\mathbf{1}, s + 2\lambda\mathbf{1})$. Since weights in the same $\mathbb{Z}$-orbit determine the same transformation (7) we may regard such weights as equivalent.

Lemma 5.2. *Let $\Phi \in X_5(\mathcal{O}_K)$ be an integral genus one model.*
(i) If Φ is non-minimal then it is $\mathcal{O}_K$-equivalent to a model with a weight.
(ii) If Φ has weight w and w dominates w' then Φ has weight w'.

PROOF: (i) By hypothesis there exist $A, B \in \mathrm{GL}_5(K)$ with $[A, B]\Phi$ integral and $2v(\det A) + v(\det B) = -1$. We put A and B in Smith normal form.
(ii) Let $\Phi = (\Phi_{ij})$ with $\Phi_{ij} = \sum_k a_{ijk}x_k$. Then Φ has weight (r, s) if and only if $v(a_{ijk}) \geq \max(r_i + r_j - s_k, 0)$ for all $1 \leq i < j \leq 5$ and $1 \leq k \leq 5$. □

Lemma 5.3. *Let $\Phi \in X_5(\mathcal{O}_K)$ have weight $(r, s) \in \mathcal{W}$ with either $r_1 + r_4 > s_1$ or $r_2 + r_3 > s_1$. Then $P = (1 : 0 : \ldots : 0) \in \mathcal{C}_\phi$ is a singular point. Moreover if $s_1 < s_3$ then P is non-regular (as a point on the $\mathcal{O}_K$-scheme $\mathcal{C}_\Phi$).*

PROOF: We write $\phi = \sum x_i M_i$. If $r_1 + r_4 > s_1$ then the only non-zero entries of M_1 are in the top left 3×3 submatrix. If $r_2 + r_3 > s_1$ then the only non-zero entries of M_1 are in the first row and column. In both cases $\operatorname{rank} M_1 \leq 2$ and so $P \in \mathcal{C}_\phi$. If $M_1 = 0$ then P is singular (and non-regular). So we may assume $M_1 \neq 0$. We are free to multiply rows of Φ by units in $\mathcal{O}_K$ and to subtract $\mathcal{O}_K$-multiples of later rows from earlier rows (it being understood that we also make the corresponding column operations). In particular these operations do not upset our hypothesis that Φ has weight (r, s). Let E_{ij} be the 5×5 matrix with a 1 in the (i, j)-place and zeros elsewhere. By row and column operations we reduce to the case $M_1 = E_{ij} - E_{ji}$ where $(i, j) \in \{(1, 2), (1, 3), (1, 4), (1, 5), (2, 3)\}$. Let $a < b < c$ be chosen such that $\{i, j, a, b, c\} = \{1, \ldots, 5\}$. Since $r_i + r_j \leq s_1 \leq s_2$ it follows by the definition of $\mathcal{W}$ that

$$s_3 + s_4 + s_5 < (r_a + r_b) + (r_a + r_c) + (r_b + r_c).$$

Therefore at least one of the following three inequalities holds:

$$\begin{aligned} s_3 < r_a + r_b \quad &\Longrightarrow \quad \phi_{ab}, \phi_{ac}, \phi_{bc} \in \langle x_4, x_5 \rangle, \\ s_4 < r_a + r_c \quad &\Longrightarrow \quad \phi_{ac}, \phi_{bc} \in \langle x_5 \rangle, \\ s_5 < r_b + r_c \quad &\Longrightarrow \quad \phi_{bc} = 0. \end{aligned}$$

Since the tangent space at P is $\{\phi_{ab} = \phi_{ac} = \phi_{bc} = 0\}$ it follows that $P \in \mathcal{C}_\phi$ is a singular point.

If $s_1 < s_3$ then the same argument shows there is some $\mathcal{O}_K$-linear combination of $\Phi_{ab}, \Phi_{ac}, \Phi_{bc}$ (with not all coefficients in $\pi\mathcal{O}_K$) that not only vanishes mod π, but whose coefficient of x_1 vanishes mod π^2. Hence P is non-regular. □

Lemma 5.4. *Let $(r,s) \in \mathcal{W}$ be a weight with $r_1 + r_4 \leq s_1$ and $r_2 + r_3 \leq s_1$. Then (r,s) dominates one of the weights $w_1, \ldots, w_7$ in the following table.*

	r_1	r_2	r_3	r_4	r_5	s_1	s_2	s_3	s_4	s_5
w_1	0	0	0	0	1	0	0	0	0	1
w_2	0	0	1	1	1	1	1	1	1	1
w_3	0	0	1	1	2	1	1	1	2	2
w_4	0	1	1	2	2	2	2	2	2	3
w_5	0	1	1	2	3	2	2	2	3	4
w_6	0	1	1	2	3	2	2	3	3	3
w_7	0	1	2	3	4	3	3	4	4	5

PROOF: We checked the lemma by writing a computer program using the simplex algorithm. See the proof of Lemma 6.1 for details. □

Definition 5.5. The *slope* of $\Phi \in X_5(\mathcal{O}_K)$ is the least possible value of $v(\det B)$ for $B \in \mathrm{GL}_5(K)$ a matrix with entries in $\mathcal{O}_K$ for which there exist $A \in \mathrm{GL}_5(K)$ and $\mu \in K^\times$ such that $[A, \mu B]\Phi$ is an integral model of smaller level.

We now complete the proof of Theorem 3.1. Since $\Phi \in X_5(\mathcal{O}_K)$ is non-minimal it has a slope σ, say. Lemma 3.3(i) shows that if $\sigma = 0$ then Φ is non-saturated. So we may assume $\sigma > 0$. By Lemma 5.2 (and Corollary 3.5) we may replace Φ by an $\mathcal{O}_K$-equivalent model with a weight, say (r,s). Moreover we may assume the weight realises the slope, i.e. $\sigma = \sum_{i=1}^{5}(s_i - s_1)$.

Suppose that either $r_1 + r_4 > s_1$ or $r_2 + r_3 > s_1$. Since $\sigma > 0$ there exists $1 \leq m \leq 4$ such that $s_1 = \ldots = s_m < s_{m+1}$. Lemma 5.3 shows (by first making unimodular transformations involving only $x_1, \ldots, x_m$) that

$$\{x_{m+1} = \ldots = x_5 = 0\} \subset \mathrm{Sing}\, \mathcal{C}_\phi \ . \tag{8}$$

Moreover if $m = 1$ then the point we have constructed is non-regular. (This is needed to complete the proof of Theorem 3.1(ii) at the end Section 4.)

Regardless of whether we have equality in (8) it follows that if the level is preserved then the slope is decreased. So after finitely many iterations Φ is either non-saturated or has weight (r,s) with $r_1 + r_4 \leq s_1$ and $r_2 + r_3 \leq s_1$. In this last case Lemmas 5.2 and 5.4 show that Φ has weight w for some $w \in \{w_1, \ldots, w_7\}$. If $w \in \{w_1, w_2, w_6\}$ then Φ is non-saturated. If $w \in \{w_5, w_7\}$ then Φ is $\mathcal{O}_K$-equivalent to a model with weight w_3. (This is achieved by a unimodular transformation involving only the second and third rows and columns, respectively a unimodular transformation involving only x_3 and x_4.) Finally if $w \in \{w_3, w_4\}$ then Φ is $\mathcal{O}_K$-equivalent to a model of the form considered in Lemma 4.3(ii)

6. The number of iterations

We have shown that if we start with a non-minimal model then iterating the procedure in Theorem 3.1(ii) eventually gives a non-saturated model or decreases the level. In this section we show that the maximum number of iterations required is 5. (In our MAGMA implementation we count the use of Theorem 3.2 to decrease the level of a non-saturated model as a further iteration. With this convention the maximum number of iterations is 6.)

Lemma 6.1. *Let $(r,s) \in \mathcal{W}$ be a weight. Then (r,s) dominates one of the weights $w_1, \ldots, w_{29}$ in the following table. (The weights in Lemma 5.4 appear with new numberings. We have marked these weights in bold.)*

	r_1	r_2	r_3	r_4	r_5	s_1	s_2	s_3	s_4	s_5	λ_ν		r_1	r_2	r_3	r_4	r_5	s_1	s_2	s_3	s_4	s_5	λ_ν
w_1	0	0	0	0	0	−1	0	0	0	0	1	w_{16}	0	1	1	2	2	1	2	2	3	3	7
$\mathbf{w_2}$	0	0	0	0	1	0	0	0	0	1	1	w_{17}	0	1	1	2	2	1	2	2	2	4	6
$\mathbf{w_3}$	0	0	1	1	1	1	1	1	1	1	1	w_{18}	0	1	1	2	2	1	1	2	3	4	7
w_4	0	1	1	1	1	1	1	1	2	2	1	$\mathbf{w_{19}}$	0	1	1	2	3	2	2	3	3	3	6
w_5	0	0	0	1	1	0	0	1	1	1	3	$\mathbf{w_{20}}$	0	1	1	2	3	2	2	2	3	4	7
w_6	0	0	0	1	1	0	0	0	1	2	3	w_{21}	0	1	1	2	3	1	2	3	3	4	13
w_7	0	0	1	1	1	0	0	1	2	2	3	w_{22}	0	1	1	2	3	1	2	2	3	5	12
w_8	0	0	1	1	1	0	1	1	1	2	3	w_{23}	0	1	2	2	3	2	3	3	3	4	9
$\mathbf{w_9}$	0	1	1	2	2	2	2	2	2	3	3	w_{24}	0	1	2	2	3	2	2	3	4	4	9
$\mathbf{w_{10}}$	0	0	1	1	2	1	1	1	2	2	4	w_{25}	0	1	2	2	3	1	3	3	4	4	10
w_{11}	0	0	1	1	2	0	0	2	2	3	5	w_{26}	0	1	2	2	3	1	2	3	4	5	15
w_{12}	0	0	1	1	2	0	1	2	2	2	8	$\mathbf{w_{27}}$	0	1	2	3	4	3	3	4	4	5	12
w_{13}	0	0	1	1	2	0	1	1	2	3	8	w_{28}	0	1	2	3	4	2	3	4	5	5	20
w_{14}	0	1	1	1	2	1	2	2	2	2	4	w_{29}	0	1	2	3	4	1	3	4	5	6	22
w_{15}	0	1	1	1	2	1	1	2	2	3	4												

Proof: We define a *standard inequality* to be an inequality of the form $r_i + r_j \leq s_k + m$ where $1 \leq i < j \leq 5$, $1 \leq k \leq 5$ and m is a non-negative integer. The condition that $(r,s) \in \mathcal{W}$ does not dominate w_ν is equivalent to a list of λ_ν standard inequalities, at least one of which must hold, where λ_ν is as given in the table. For example, $(r,s) \not\geq w_1$ if and only if $r_1 + r_2 \leq s_1$, whereas $(r,s) \not\geq w_5$ if and only if $r_1 + r_4 \leq s_2$ or $r_4 + r_5 \leq s_2 + 1$ or $r_4 + r_5 \leq s_5$. (We have used the conditions $r_1 \leq \ldots \leq r_5$ and $s_1 \leq \ldots \leq s_5$ to remove redundant inequalities.)

We wrote a program using the simplex algorithm to maximise $\sum(2r_i - s_i)$ for $(r, s) \in \mathbb{R}^{10}$ subject to $0 \le r_1 \le \ldots \le r_5$, $0 \le s_1 \le \ldots \le s_5$, and a list of standard inequalities. Our program starts with the basic feasible solution $(r, s) = (0, 0)$. If there is a finite maximum, and it is less than 1, then (by definition of $\mathcal{W}$) there are no weights satisfying these inequalities. If the maximum is 1 then we add the constraint $\sum(2r_i - s_i) = 1$. We then use the simplex algorithm to maximise each of the functions $r_i + r_j - s_k$ in turn. In the case of a finite maximum α we obtain an additional standard inequality $r_i + r_j \le s_k + \max(\lfloor \alpha \rfloor, 0)$. Then running our original program on the enlarged set of standard inequalities we may still be able to show that $\sum(2r_i - s_i) < 1$.

After processing the inequalities coming from $w_1, \ldots, w_\nu$ for $\nu = 1, \ldots, 29$ the number of cases remaining were as follows:

$$1,\ 1,\ 1,\ 1,\ 3,\ 5,\ 8,\ 13,\ 16,\ 30,\ 31,\ 49,\ 58,\ 47,\ 60,$$
$$64,\ 58,\ 53,\ 45,\ 36,\ 39,\ 34,\ 25,\ 15,\ 14,\ 10,\ 3,\ 1,\ 0.$$

The final zero indicates that no cases remain, and this proves the lemma. The proof of Lemma 5.4 is similar but easier. □

If $\Phi \in X_5(\mathcal{O}_K)$ is non-minimal then by Lemmas 5.2 and 6.1 it has slope at most 14. This already shows that the algorithm in Theorem 3.1(iii) takes at most 14 iterations. The next lemma improves this bound to 7 iterations.

Lemma 6.2. *If the procedure in Theorem 3.1(ii) returns a saturated model with the same level then the slope goes down by at least* 2*.*

Proof: We revisit the proof of Theorem 3.1(iii) at the end of Section 5. If the slope goes down by only one then $\operatorname{Sing} \mathcal{C}_\phi$ spans a hyperplane. If $\operatorname{Sing} \mathcal{C}_\phi$ is a hyperplane then the proof of Theorem 3.1(ii) at the end of Section 4 shows that the level is decreased. Otherwise by Lemma 4.2 we may assume ϕ takes the form (5). We then follow the proof of Lemma 4.3(i) with $m = 4$. After applying the transformation suggested there, the second row of ϕ has at most one non-zero entry. This implies that Φ is non-saturated. □

The next lemma will be used to show that only 5 iterations are required.

Lemma 6.3. *Let $\Phi \in X_5(\mathcal{O}_K)$ be non-minimal and of slope greater than* 10*. Then replacing Φ by an $\mathcal{O}_K$-equivalent model we may assume it has weight w_{29} and the coefficient of x_k in Φ_{ij} is a unit for*

$$(i, j, k) \in \{(1, 2, 1), (1, 4, 2), (1, 5, 3), (2, 3, 2), (2, 4, 3), (2, 5, 4), (3, 4, 4), (3, 5, 5)\}.$$

Proof: By Lemma 5.2 we know that Φ is $\mathcal{O}_K$-equivalent to a model with one of the 29 weights listed in Lemma 6.1. For all but one of these weights (r, s) we have $\sum_{i=1}^{5}(s_i - s_1) \le 10$. The remaining case is w_{29}. If one of the coefficients listed is not a unit then Φ has weight w_ν for some $\nu \in \{1, 5, 13, 26, 16, 21, 8, 12\}$. □

We write $[j,\ldots,5]$ for a linear combination of $x_j,\ldots,x_5$, and underline in cases where we know the coefficient is non-zero. Lemma 6.3 shows that $\Phi \in X_5(\mathcal{O}_K)$ has reduction $\phi \in X_5(k)$ of the form

$$\begin{pmatrix} 0 & [\underline{1},2,3,4,5] & [2,3,4,5] & [\underline{2},3,4,5] & [\underline{3},4,5] \\ & 0 & [\underline{2},3,4,5] & [\underline{3},4,5] & [\underline{4},5] \\ & & 0 & [\underline{4},5] & [\underline{5}] \\ & & & 0 & 0 \\ & & & & 0 \end{pmatrix}.$$

Let $\mathrm{Pf}(\phi) = (p_1,\ldots,p_5)$. By considering the partial derivatives of p_1, p_2, p_4 with respect to x_1, x_2, x_3 we see that if $P = (x_1 : \ldots : x_5) \in \operatorname{Sing} \mathcal{C}_\phi$ then $x_5 = 0$. Then since $P \in \mathcal{C}_\phi$ we have $x_4 = x_3 = x_2 = 0$. So $(1 : 0 : \ldots : 0)$ is the unique singular point.

Our algorithm applies the transformation

$$[\mathrm{Diag}(1,1,1,\pi^{-1},\pi^{-1}), \mathrm{Diag}(1,\pi,\pi,\pi,\pi)].$$

The result is a model Φ with weight $w_{26} = (0,1,2,2,3;1,2,3,4,5)$ whose reduction ϕ takes the form

$$\begin{pmatrix} 0 & [\underline{1}] & 0 & [\underline{2},3,4,5] & [\underline{3},4,5] \\ & 0 & 0 & [\underline{3},4,5] & [\underline{4},5] \\ & & 0 & [\underline{4},5] & [\underline{5}] \\ & & & 0 & [5] \\ & & & & 0 \end{pmatrix}.$$

A calculation similar to that above shows that $\operatorname{Sing} \mathcal{C}_\phi = \{x_3 = x_4 = x_5 = 0\}$.

Our algorithm applies the transformation

$$[\mathrm{Diag}(\pi,1,1,1,1), \mathrm{Diag}(\pi^{-1},\pi^{-1},1,1,1)]$$

The result is a model Φ with weight $w_{13} = (0,0,1,1,2;0,1,1,2,3)$ whose reduction ϕ takes the form

$$\begin{pmatrix} 0 & [\underline{1}] & 0 & [\underline{2}] & 0 \\ & 0 & [\underline{2}] & [2,\underline{3},4,5] & [\underline{4},5] \\ & & 0 & [\underline{4},5] & [\underline{5}] \\ & & & 0 & [5] \\ & & & & 0 \end{pmatrix}.$$

A calculation similar to that above shows that $\operatorname{Sing} \mathcal{C}_\phi = \{x_2 = x_4 = x_5 = 0\}$.

The next transformation $[\mathrm{Diag}(1,\pi,1,1,1), \mathrm{Diag}(\pi^{-1},1,\pi^{-1},1,1)]$ gives a model with weight $w_{15} = (0,1,1,1,2;1,1,2,2,3)$. So after 3 iterations the slope is at most 4. It follows by Lemma 6.2 that at most 5 iterations are required.

Example 6.4. The simplest example of a genus one model satisfying the conditions of Lemma 6.3 is

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

We find that $\mathcal{C}_\Phi$ is a rational curve with a cusp, parametrised by

$$(s : t) \mapsto (-s^5 : s^3t^2 : s^2t^3 : st^4 : t^5).$$

In this case our algorithm takes the maximum of exactly 5 iterations to give a non-saturated model. (The first 3 iterations are already described above.) Although the model in this example is singular, there are π-adically close non-singular models that are treated in the same way by our algorithm.

7. Insoluble models

In this section we prove a result converse to the strong minimisation theorem. This is analogous to the results for models of degrees $n = 2, 3, 4$ proved in [CFS, Section 5]. As in Section 2 we work over a discrete valuation field K. We write K^{sh} for the strict Henselisation of K. (If K is a p-adic field then this is the maximal unramified extension.)

Theorem 7.1. *If $\Phi \in X_5(K)$ is non-singular and $\mathcal{C}_\Phi(K^{\mathrm{sh}}) = \emptyset$ then the minimal level is at least 1, and is equal to 1 if $\mathrm{char}(k) \neq 5$.*

As in Section 6 we write $[j, \dots, 5]$ for a linear combination of $x_j, \dots, x_5$, and underline in cases where we require the coefficient is non-zero.

Definition 7.2. A genus one model $\Phi \in X_5(\mathcal{O}_K)$ is *critical* if it has reduction mod π of the form

$$\begin{pmatrix} 0 & [\underline{1}, 2, 3, 4, 5] & [\underline{2}, 3, 4, 5] & [\underline{3}, 4, 5] & [\underline{4}, 5] \\ & 0 & [\underline{3}, 4, 5] & [\underline{4}, 5] & [\underline{5}] \\ & & 0 & [\underline{5}] & 0 \\ & & & 0 & 0 \\ & & & & 0 \end{pmatrix}$$

and $\pi^{-1}\Phi_{35}$, $\pi^{-1}\Phi_{45}$ have reductions mod π of the form $[\underline{1}, 2, 3, 4, 5]$, $[\underline{2}, 3, 4, 5]$.

We show in the next three lemmas that critical models are insoluble, minimal and of positive level. We then show that every insoluble model $\Phi \in X_5(K)$ is K-equivalent to a critical model.

Lemma 7.3. *Critical models are insoluble over K.*

PROOF: Suppose $(x_1, \ldots, x_5) \in K^5$ is a non-zero solution with $\min\{v(x_i)\} = 0$. By considering the 4×4 Pfaffians we successively deduce $\pi \,|\, x_5$, $\pi \,|\, x_4$, $\ldots$, $\pi \,|\, x_1$. In particular $\min\{v(x_i)\} > 0$. This is the required contradiction. □

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 7.4. *Critical models are minimal.*

PROOF: It is easy to see that critical models are saturated. Moreover every point on $\mathcal{C}_\phi = \{x_3 = x_4 = x_5 = 0\}$ is singular. Our algorithm (see Theorem 3.1) makes the transformation $[\mathrm{Diag}(\pi, 1, 1, 1, 1), \pi^{-1}\,\mathrm{Diag}(1, 1, \pi, \pi, \pi)]$. This gives an integral model of the same level, that is $\mathcal{O}_K$-equivalent (by a pair of cyclic permutation matrices) to a critical model.

If Φ were non-minimal then our algorithm would succeed in reducing the level. But on the contrary, when given a critical model, our algorithm endlessly cycles between five $\mathcal{O}_K$-equivalence classes. □

The next lemma describes the possible levels of a critical model. To treat the cases $\mathrm{char}(k) = 2, 3$ we need to work with the a-invariants defined in Section 1. Although these are not $\mathrm{SL}_5 \times \mathrm{SL}_5$-invariant, if we make our choices of a_1, b_2, a_3 so as not to introduce any new monomials when we lift to characteristic 0, then they will be invariant under all pairs of diagonal matrices. It follows by the proof of Lemma 1.2 that $a_1, \ldots, a_6$ are isobaric, i.e.

$$a_i \circ [\mathrm{Diag}(\lambda_1, \ldots, \lambda_5), \mathrm{Diag}(\mu_1, \ldots, \mu_5)] = (\prod \lambda_\nu)^{2i} (\prod \mu_\nu)^i a_i.$$

Lemma 7.5. *The level of a critical model is at least* 1 *and equal to* 1 *if* $\mathrm{char}(k) \neq 5$.

PROOF: Applying $[\mathrm{Diag}(1, \pi^{-1/5}, \pi^{-2/5}, \pi^{-3/5}, \pi^{-4/5}), \mathrm{Diag}(\pi^{1/5}, \pi^{2/5}, \pi^{3/5}, \pi^{4/5}, \pi)]$ to a critical model Φ gives a model with coefficients in $\mathcal{O}_K[\pi^{1/5}]$. It follows by the isobaric property that $\pi^i \,|\, a_i(\Phi)$ for all i. Hence Φ has positive level.

The model with coefficients in $\mathcal{O}_K[\pi^{1/5}]$ has reduction

$$\begin{pmatrix} 0 & \lambda_1 x_1 & \mu_2 x_2 & -\mu_3 x_3 & -\lambda_4 x_4 \\ & 0 & \lambda_3 x_3 & \mu_4 x_4 & -\mu_5 x_5 \\ & & 0 & \lambda_5 x_5 & \mu_1 x_1 \\ & & & 0 & \lambda_2 x_2 \\ & & & & 0 \end{pmatrix}$$

for some $\lambda_1, \ldots, \lambda_5, \mu_1 \ldots, \mu_5 \in k^\times$. The invariants of this model are

$$c_4(\lambda,\mu) = \lambda^4 + 228\lambda^3\mu + 494\lambda^2\mu^2 - 228\lambda\mu^3 + \mu^4,$$
$$c_6(\lambda,\mu) = -\lambda^6 + 522\lambda^5\mu + 10005\lambda^4\mu^2 + 10005\lambda^2\mu^4 - 522\lambda\mu^5 - \mu^6,$$

and $\Delta(\lambda,\mu) = \lambda\mu(\lambda^2 - 11\lambda\mu - \mu^2)^5$, where $\lambda = \prod \lambda_i$ and $\mu = \prod \mu_i$. Computing a resultant shows that if $\mathrm{char}(k) \neq 5$ then $c_4(\lambda,\mu)$ and $\Delta(\lambda,\mu)$ have no common roots. Therefore the critical model Φ we started with satisfies either $v(c_4(\Phi)) = 4$ or $v(\Delta(\Phi)) = 12$. It follows that Φ has level at most 1. □

Remark 7.6. The following example of a critical model of level 2 over $K = \mathbb{Q}_5$ shows that the hypothesis $\mathrm{char}(k) \neq 5$ cannot be removed from Lemma 7.5.

$$\begin{pmatrix} 0 & x_1 & x_2 & -x_3 & -x_4 \\ & 0 & x_3 & x_4 & -x_5 \\ & & 0 & x_5 & 35x_1 \\ & - & & 0 & 5x_2 \\ & & & & 0 \end{pmatrix}$$

We recall that the minimal level is unchanged by an unramified field extension. Replacing K by K^{sh} we may assume for the rest of this section that K is Henselian and its residue field k is algebraically closed. To complete the proof of Theorem 7.1 we show

Theorem 7.7. *If $\Phi \in X_5(\mathcal{O}_K)$ is minimal and $\mathcal{C}_\Phi(K) = \emptyset$ then Φ is $\mathcal{O}_K$-equivalent to a critical model.*

We start the proof of Theorem 7.7 with the following lemma.

Lemma 7.8. *If $\Phi \in X_5(\mathcal{O}_K)$ is minimal then its reduction $\phi \in X_5(k)$ has the following properties.*

(i) *The 4×4 Pfaffians of ϕ are linearly independent.*
(ii) *The subscheme $\mathcal{C}_\phi \subset \mathbb{P}^4$ does not contain a plane.*
(iii) *The entries of ϕ span the space of linear forms on $\mathbb{P}^4$.*

Proof: (i) This follows by Theorem 3.2 and Lemma 3.3(i).
(ii) Suppose $\mathcal{C}_\phi$ contains the plane $\{x_4 = x_5 = 0\}$. By Lemma 3.4 we may assume the reduction mod π of $[I_5, \mathrm{Diag}(1,1,1,\pi,\pi)]\Phi$ takes one of the two forms given in the lemma. We decrease the level by applying either $[\mathrm{Diag}(\pi,1,1,1,1), \pi^{-1}I_5]$ or $[\mathrm{Diag}(1,1,1,\pi^{-1},\pi^{-1}), B]$ where B is chosen to preserve integrality.
(iii) This is clear, as we could otherwise decrease the level by dividing one of the co-ordinates by π. □

Lemma 7.9. *Let $\phi \in X_5(k)$ be a genus one model satisfying the conclusions of Lemma 7.8. Suppose that every point on $\mathcal{C}_\phi$ is singular. Then ϕ is k-equivalent to*

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

Our proof of Lemma 7.9 uses the following classification of degenerations of the twisted cubic. (Only the last sentence of the statement is needed.)

Lemma 7.10. *Let ψ be a 3×2 matrix of linear forms in $R = k[x_1, \ldots, x_4]$. Suppose the 2×2 minors of ψ are linearly independent and no linear combination of them has rank 1. Then ψ is $\mathrm{GL}_2 \times \mathrm{GL}_3 \times \mathrm{GL}_4$-equivalent to one of the following:*

$$\begin{pmatrix} x_1 & x_2 \\ x_2 & x_3 \\ x_3 & x_4 \end{pmatrix}, \quad \begin{pmatrix} x_1 & x_2 \\ x_2 & x_3 \\ x_4 & 0 \end{pmatrix}, \quad \begin{pmatrix} x_1 & x_2 \\ 0 & x_3 \\ x_4 & 0 \end{pmatrix}, \quad \begin{pmatrix} x_1 & 0 \\ x_2 & x_2 \\ 0 & x_3 \end{pmatrix}. \tag{9}$$

In particular the locus of smooth points on $\Gamma = \{\operatorname{rank} \psi \leq 1\} \subset \mathbb{P}^3$ spans $\mathbb{P}^3$.

Proof: We may realise Γ as the intersection of the image of the Segre embedding $\mathbb{P}^1 \times \mathbb{P}^2 \to \mathbb{P}^5$ with a linear subspace $\mathbb{P}^3$. So every component of Γ has dimension at least 1. If every component has dimension 1 then by the Buchsbaum-Eisenbud acyclicity criterion there is a minimal free resolution

$$0 \longrightarrow R(-3)^2 \xrightarrow{\psi} R(-2)^3 \xrightarrow{M} R \tag{10}$$

where M is the vector of 2×2 minors of ψ. If in addition $\dim T_P \Gamma = 1$ for every $P \in \Gamma$ then by an argument using Serre's criterion (see [E, Section 18.3]) the ideal in R generated by the 2×2 minors of ψ is a prime ideal. By (10) the Hilbert polynomial is

$$h(t) = \binom{t+3}{3} - 3\binom{t+1}{3} + 2\binom{t}{3} = 3t + 1.$$

Therefore Γ is a twisted cubic and ψ is equivalent to the first of the matrices in (9).

In all other cases there exists $P \in \Gamma$ with $\dim T_P \Gamma > 1$. First suppose $\operatorname{rank} \psi(P) = 1$. Moving P to $(1 : 0 : 0 : 0)$ we may suppose

$$\psi = \begin{pmatrix} x_1 & \alpha \\ \delta & \beta \\ \gamma & 0 \end{pmatrix}$$

where $\alpha, \beta, \gamma, \delta$ are linear forms in x_2, x_3, x_4. Our hypotheses on the 2×2 minors ensure that α, β, γ are linearly independent; say they are x_2, x_3, x_4. By row and column operations (and a substitution for x_1) we may assume δ is a multiple of x_2. This gives the second and third cases in (9).

Now suppose $\operatorname{rank} \psi(P) = 0$. Let $Q \in \Gamma$ be any other point. If $\operatorname{rank} \psi(Q) = 0$ then the 2×2 minors are binary quadratic forms, and so some linear combination has rank 1. Therefore $\operatorname{rank} \psi(Q) = 1$. If $\dim T_Q \Gamma > 1$ then our earlier analysis applies (and in fact gives a contradiction). Otherwise we may assume

$$\psi = \begin{pmatrix} x_1 & 0 \\ \alpha & x_2 \\ \beta & x_3 \end{pmatrix}$$

where α, β are linear forms in x_2, x_3. (The zero in the top right has been cleared by row operations.) Since $\alpha x_3 - \beta x_2$ is a rank 2 quadratic form in x_2, x_3 we can make a change co-ordinates so that $\Gamma = \{x_1 x_2 = x_1 x_3 = x_2 x_3 = 0\}$. Then ψ is equivalent to the last of the matrices in (9).

For the final statement, we note that the 4 cases correspond geometrically to (i) a twisted cubic, (ii) a conic and a line, (iii) three non-concurrent lines, and (iv) three concurrent lines. In each case Γ spans $\mathbb{P}^3$ and the only singular points are the points where the components meet. □

Proof of Lemma 7.9: Let $P \in \mathcal{C}_\phi$ be a singular point. Moving P to $(1:0:0:0:0)$ we may assume ϕ takes the form

$$\begin{pmatrix} 0 & x_1 & \ell_2 & \alpha_1 & \beta_1 \\ & 0 & \ell_3 & \alpha_2 & \beta_2 \\ & & 0 & \alpha_3 & \beta_3 \\ & - & & 0 & 0 \\ & & & & 0 \end{pmatrix}$$

where $\ell_i, \alpha_i, \beta_i$ are linear forms in $x_2, \ldots, x_5$. Let ψ be the top right 3×2 submatrix and let $\Gamma \subset \mathbb{P}^3$ be the curve defined by its 2×2 minors. Since the 2×2 minors of ψ are a subset of the 4×4 Pfaffians of ϕ, they are linearly independent. In particular α_3 and β_3 cannot both vanish identically. Without loss of generality α_3 is non-zero.

Suppose no linear combination of the 2×2 minors of ψ has rank 1. Then by Lemma 7.10 there is a smooth point $Q = (x_2 : x_3 : x_4 : x_5)$ on Γ with $\alpha_3(Q) \neq 0$. Solving for x_1 gives a smooth point $(x_1 : x_2 : \ldots : x_5)$ on $\mathcal{C}_\phi$. This is a contradiction. Therefore some linear combination of the 2×2 minors of ψ has rank 1. It is then easy to see that ϕ is k-equivalent to a model of the form (5).

By properties (i) and (ii), η, x_5 are linearly independent and γ, δ, x_5 are linearly independent. However if $\eta, \gamma, \delta, x_5$ were linearly independent then taking them to be $x_2, \ldots, x_5$ would give that $(0:1:0:0:0)$ is a smooth point on $\mathcal{C}_\phi$. By row and column operations we may therefore suppose $\eta = \delta$ $(= x_4$ say).

By property (ii), β, x_4, x_5 are linearly independent and γ, x_4, x_5 are linearly independent. By row and column operations (and substitutions for the x_i) we may suppose $\beta = x_3$ and $\gamma = x_2$ or x_3. If $\gamma = x_2$ then by further row and column operations (and substitutions for the x_i) we may suppose α is a multiple of x_1. The lemma now follows using property (iii). □

Proof of Theorem 7.7: Since K is Henselian any smooth point on $\mathcal{C}_\phi$ lifts to a K-point on $\mathcal{C}_\Phi$. So we may assume ϕ takes one of the three forms in Lemma 7.9. In the first two cases ϕ defines a pair of concurrent lines with multiplicities 2 and 3. (These cases may be distinguished by the dimension of the tangent space at the point of intersection). In the third case it defines a line with multiplicity 5.

We apply the transformation $[\mathrm{Diag}(1,1,1,1,\pi^{-1}), \mathrm{Diag}(1,1,1,\pi,\pi)]$. This gives an integral model of the same level. So the reduction must again be k-equivalent to one of the three models in Lemma 7.9. We tidy up by an $\mathcal{O}_K$-equivalence that cyclically permutes the rows and columns, and makes substitutions for x_4 and x_5. The reduction $\phi \in X_5(k)$ now takes the form

$$\begin{pmatrix} 0 & x_4 & x_5 & \alpha & \beta \\ & 0 & 0 & x_1 & x_3 \\ & & 0 & x_2 & 0 \\ & - & & 0 & 0 \\ & & & & 0 \end{pmatrix} \text{ or } \begin{pmatrix} 0 & x_4 & x_5 & \alpha & \beta \\ & 0 & x_1 & 0 & x_3 \\ & & 0 & x_2 & 0 \\ & - & & 0 & 0 \\ & & & & 0 \end{pmatrix} \text{ or } \begin{pmatrix} 0 & x_4 & x_5 & \alpha & \beta \\ & 0 & x_1 & x_2 & x_3 \\ & & 0 & x_3 & 0 \\ & - & & 0 & 0 \\ & & & & 0 \end{pmatrix}$$

where α and β are linear forms in x_1, x_2, x_3.

In the first case $(0:0:0:1:0)$ is a point with tangent space of dimension 3 and $\mathcal{C}_\phi$ contains points not on the line $\{x_1 = x_2 = x_3 = 0\}$. So the transformation has moved us to the second case.

In second case we obtain a contradiction as follows. If $\alpha = x_1 + \lambda x_2 + \mu x_3$ then adding μ times the fifth row/column to the third row/column, and making substitutions for x_1 and x_5 we may assume $\mu = 0$. Then $(0:0:1:0:0)$ is a smooth point on $\mathcal{C}_\phi$. Likewise if $\beta = x_1 + \lambda x_2 + \mu x_3$ then subtracting λ times the fourth row/column from the second row/column and making substitutions for x_1 and x_4 we may assume $\lambda = 0$. Then $(0:1:0:0:0)$ is a smooth point on $\mathcal{C}_\phi$. We are forced to the conclusion that neither α nor β involves x_1. But then $\mathcal{C}_\phi$ contains the plane $\{x_2 = x_3 = 0\}$ and by Lemma 7.8 this contradicts that Φ is minimal.

In the third case we show that if the transformation above brings us back to the third case, then the original model is critical. If $\beta = x_1 + \lambda x_2 + \mu x_3$ then adding λ times the fourth row/column to the third row/column, and making substitutions

for x_1 and x_5 we may assume $\lambda = 0$. Then $\mathcal{C}_\phi$ contains the lines $\{x_1 = x_2 = x_3 = 0\}$ and $\{x_1 = x_3 = x_5 = 0\}$. So if the transformation returns us to third case then β cannot involve x_1. Since $\mathcal{C}_\phi$ does not contain a plane, and the 4×4 Pfaffians of ϕ are linearly independent, α must involve x_1 and β must involve x_2. It follows by Definition 7.2 that the original model is $\mathcal{O}_K$-equivalent to a critical model. □

8. Reduction

Let $C \subset \mathbb{P}^4$ be a genus one normal curve of degree 5 defined over $\mathbb{Q}$. We may represent it by a non-singular genus one model $\Phi \in X_5(\mathbb{Z})$. Running the algorithm in Section 3 locally at p, for all primes p dividing the discriminant $\Delta(\Phi)$, we obtain a $\mathbb{Q}$-equivalent model (still with coefficients in $\mathbb{Z}$) whose discriminant is minimal in absolute value. If C is everywhere locally soluble then this discriminant is the minimal discriminant of $E = \mathrm{Jac}(C)$. It remains to make a $\mathrm{GL}_5(\mathbb{Z})$ change of co-ordinates on $\mathbb{P}^4$ so that (after running the LLL algorithm on the space of 5 quadrics defining the curve) the coefficients (and not just the invariants) are small. The general method, described in [CFS, Section 6], is to run the LLL algorithm on the Gram matrix for the (unique) Heisenberg invariant inner product. In this section we outline how to compute this inner product in the case $n = 5$.

We recall that the Heisenberg group is the subgroup of $\mathrm{SL}_5(\mathbb{C})$ consisting of matrices M_T that describe the action of $T \in E[5]$ on $C \subset \mathbb{P}^4$ by translation. For $T \neq 0_E$ we call the 5 points in $\mathbb{P}^4$ fixed by M_T a *syzygetic* 5*-tuple*. It may be shown (for example by adapting the proof of [F2, Proposition 4.1] or using that $H^1(\mathbb{R}, E[5])$ is trivial) that Φ is $\mathrm{SL}_5(\mathbb{R}) \times \mathrm{SL}_5(\mathbb{R})$-equivalent to a model in Hesse form:

$$\begin{pmatrix} 0 & ax_0 & bx_1 & -bx_2 & -ax_3 \\ & 0 & ax_2 & bx_3 & -bx_4 \\ & & 0 & ax_4 & bx_0 \\ & - & & 0 & ax_1 \\ & & & & 0 \end{pmatrix}. \tag{11}$$

The invariants of this model are

$$\begin{aligned} c_4 &= a^{20} + 228a^{15}b^5 + 494a^{10}b^{10} - 228a^5b^{15} + b^{20}, \\ c_6 &= -a^{30} + 522a^{25}b^5 + 10005a^{20}b^{10} + 10005a^{10}b^{20} - 522a^5b^{25} - b^{30}, \end{aligned}$$

and $\Delta = D^5$ where $D = ab(a^{10} - 11a^5b^5 - b^{10})$. For a model in Hesse form the Heisenberg group is generated by $\mathrm{Diag}(1, \zeta, \ldots, \zeta^4)$, where ζ is a primitive 5th root of unity, and a cyclic permutation matrix. Since these matrices are unitary, the Heisenberg invariant inner product is the standard inner product on $\mathbb{R}^5$.

The Hessian, introduced in [F2], is an $\mathrm{SL}_5 \times \mathrm{SL}_5$-equivariant polynomial map $H : X_5 \to X_5$ with the property that the Hessian of (11) is of the same form with a and b replaced by $-\partial D/\partial b$ and $\partial D/\partial a$.

Theorem 8.1. *Let $\Phi \in X_5(\mathbb{C})$ be a non-singular genus one model with invariants c_4 and c_6. Let A be the 3×5 matrix of quadrics such that $\lambda\Phi + \mu H(\Phi)$ has 4×4 Pfaffians*

$$\{\lambda^2 A_{1i} + \lambda\mu A_{2i} + \mu^2 A_{3i} : i = 1, \ldots, 5\}$$

Then $\mathcal{X} = \{\operatorname{rank} A \leq 1\} \subset \mathbb{P}^4$ consists of 30 points and the syzygetic 5-tuples for $\mathcal{C}_\Phi$ are the fibres of the map $\alpha : \mathcal{X} \to \mathbb{P}^2$ given by the first (or indeed any) column of A. The image of α is the set of 6 points $(x : y : z) \in \mathbb{P}^2$ satisfying

$$\operatorname{rank} \begin{pmatrix} 0 & 5x & y & 6c_4x + z \\ x & y & 6c_4x - z & 8c_6x \\ y & -z & 8c_6x & 9c_4^2x \end{pmatrix} \leq 2. \tag{12}$$

Proof: It suffices to prove this for Φ in Hesse form. Then $\mathcal{X}$ is defined by

$$\operatorname{rank} \begin{pmatrix} x_0^2 & x_1^2 & x_2^2 & x_3^2 & x_4^2 \\ x_1x_4 & x_0x_2 & x_1x_3 & x_2x_4 & x_0x_3 \\ x_2x_3 & x_3x_4 & x_0x_4 & x_0x_1 & x_1x_2 \end{pmatrix} \leq 1 \tag{13}$$

and by [BHM, Proposition 1] is a set of 30 points. Evaluating the columns of (13) at these points we obtain $(1 : 0 : 0)$ and $(1 : \zeta^i : \zeta^{-i})$ for $i = 0, \ldots, 4$. These are the points $(\xi : \eta : \nu) \in \mathbb{P}^2$ satisfying

$$\operatorname{rank} \begin{pmatrix} \xi & \eta & \nu & 0 \\ \nu & \xi & 0 & -\eta \\ 0 & 0 & \eta & \nu \end{pmatrix} \leq 2. \tag{14}$$

The remaining statements follow by direct calculation. In particular our description (12) of the image of α is checked by making the substitution

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} ab & b^2 & -a^2 \\ -a\frac{\partial D}{\partial a} + b\frac{\partial D}{\partial b} & -2b\frac{\partial D}{\partial a} & -2a\frac{\partial D}{\partial b} \\ -\frac{\partial D}{\partial b}\frac{\partial D}{\partial a} & (\frac{\partial D}{\partial a})^2 & -(\frac{\partial D}{\partial b})^2 \end{pmatrix} \begin{pmatrix} \xi \\ \eta \\ \nu \end{pmatrix}.$$

We note that this change of co-ordinates, and the matrix relating the 3×3 minors of (12) and (14), each have determinant a constant times a power of D. □

After computing the Hessian exactly (using the algorithm in [F2, Section 11]) we use Theorem 8.1 to compute the syzygetic 5-tuples numerically. We then compute a Gram matrix for the Heisenberg invariant inner product as follows.

Proposition 8.2. *Let $C \subset \mathbb{P}^4$ a genus one normal curve defined over $\mathbb{R}$.*

(i) *Exactly two of the syzygetic 5-tuples for C are defined over $\mathbb{R}$, say*

$$Y = \{y_i y_j = 0 : i < j\} \subset \mathbb{P}^4,$$
$$Z = \{z_i z_j = 0 : i < j\} \subset \mathbb{P}^4,$$

where $y_0, \ldots, y_4$ and $z_0, \ldots, z_4$ are linear forms in $\mathbb{C}[x_0, \ldots, x_4]$.

(ii) *One of the 5-tuples in (i) has 5 real points and the other has 1 real point. We may therefore arrange that $y_0, \ldots, y_4$ and z_0 have real coefficients and that the pairs z_1, z_4 and z_2, z_3 are complex conjugates.*

(iii) *The Heisenberg invariant quadratic form spans the 1-dimensional real vector space*

$$\langle y_0^2, \ldots, y_4^2 \rangle \cap \langle z_0^2, z_1 z_4, z_2 z_3 \rangle.$$

PROOF: For C in Hesse form we may take $y_i = x_i$ and $z_i = \sum_{j=0}^4 \zeta^{ij} x_j$. In this case the Heisenberg invariant quadratic form is $x_0^2 + \ldots + x_4^2$. □

9. Examples

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

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

His example (see also [F1, Section 9]) is defined by the 4×4 Pfaffians of

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

This model has discriminant $2^{132}\Delta_E$ where Δ_E is the minimal discriminant of E. In other words, the model is minimal at all primes except $p = 2$, where the level is 11. Minimisation and reduction suggest the change of co-ordinates

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

so that Wuthrich's example simplifies to

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

Our MAGMA function `DoubleGenusOneModel`, described in [F3], computes a genus one model Φ' that represents twice the class of Φ in the 5-Selmer group. This model has entries

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

The discriminant of Φ' is Δ_E^{49}. In particular this model is non-minimal at all bad primes of E. Minimisation and reduction suggest the change of co-ordinates

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

so that Φ' simplifies to

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

References

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

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

[BHM] W. Barth, K. Hulek and R. Moore, Shioda's modular surface $S(5)$ and the Horrocks-Mumford bundle, *Vector bundles on algebraic varieties* (Bombay, 1984), 35–106, Tata Inst. Fund. Res. Stud. Math., **11**, Tata Inst. Fund. Res., Bombay, 1987.

[CFS] J.E. Cremona, T.A. Fisher and M. Stoll, Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves, *Algebra & Number Theory* **4** (2010), no. 6, 763-820.

[E] D. Eisenbud, *Commutative algebra, with a view toward algebraic geometry*, Graduate Texts in Mathematics **150**, Springer-Verlag, New York, 1995.

[F1] T.A. Fisher, The invariants of a genus one curve, *Proc. Lond. Math. Soc.* (3) **97** (2008) 753-782.

[F2] T.A. Fisher, The Hessian of a genus one curve, to appear in *Proc. Lond. Math. Soc.*

[F3] T.A. Fisher, *Invariant theory for the elliptic normal quintic, I. Twists of X(5)*, preprint, `arXiv:1110.3520v1`

[K] 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.

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

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

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