Enumerating Totally Real Quartic Fields
Ashwath Rabindranath

1 Introduction

The problems of counting and enumeration of number fields of small degree up to bounded discriminant have been well-studied over the last fifty years. In 1971, Davenport and Heilbronn computed the density of discriminants of cubic fields using the parametrizations of [16] due to Delone-Faddeev and various techniques from the geometry of numbers, including important asymptotics for the class numbers of binary cubic forms from work of Davenport in 1951 [13], [12], [13], [14]. They showed that the number of cubic fields, having discriminant bounded in absolute value by $X$ is asymptotically linear. In 1997, Belabas used these parametrizations and various ideas derived from the geometry-of-numbers approach of Davenport-Heilbronn, to describe and implement an extremely fast algorithm to enumerate all cubic fields of discriminant bounded in absolute value by $10^{11}$ [1].

In Chapter 5 of his 2001 Ph.D thesis [2], revised and published as [4], Bhargava computed the density of discriminants of quartic fields using his own parametrizations from [3] and techniques from the geometry-of-numbers analogous to those used by Davenport-Heilbronn. However the corresponding problem of enumerating quartic fields has not really been approached from this perspective since the work of Buchmann and Ford from 1989 [8], and Buchmann, Ford, and Pohst from 1993 [9]. Indeed, the most recent approach to this problem is due to Cohen, Diaz y Diaz and Olivier using techniques from Kummer theory. In [10], they make complete tables of all quartic fields having discriminant bounded in absolute value by $10^7$.

The goal of this junior paper [1] is to outline an effectively linear algorithm to enumerate quartic fields up to bounded discriminant using the parametrizations of [3] and ideas derived from the techniques used in Chapter 5 of [2]. The main result achieved is a partial quartic analogue of the algorithm described in [1]:

Theorem. There exists an algorithm of complexity $O(X^{1+\varepsilon})$ to compute totally real quartic fields having Galois group (of the normal closure) either $S_4$ or $A_4$, and discriminant bounded in absolute value by $X$.

In Section 2, we describe Bhargava’s parametrizations of quartic rings. These parametrizations are given using certain integral orbits of the group $G_\mathbb{Z} := \text{GL}_2(\mathbb{Z}) \times \text{SL}_3(\mathbb{Z})$ acting on $\mathbb{R}^2 \otimes \text{Sym}^2(\mathbb{R}^3)$, the 12-dimensional space of pairs $(A, B)$ of ternary quadratic forms having real coefficients, denoted by $V_\mathbb{R}$. These parametrizations are key in the computations of [3] and are equally essential in our algorithm. In both cases, the shift in focus from fields to rings is crucial since it reduces the respective problems to searching for/counting lattice points within a region $R \subset \mathbb{R}^{12}$ that contains a fundamental region for the integral orbits mentioned above, from the significantly harder problems

---

1I pledge that this represents my own work in accordance with University regulations and the Honour Code – Ashwath Rabindranath
of searching for/counting rational points on homogeneous spaces. We also describe a reduction theory for the case of orders in totally real fields in Section 2. Key components of the reduction theory include the fundamental domain due to Grenier from [17], and explicitly written down [18] and the use of the quadratic covariant $\text{Tr}(x^2)|\text{Tr}(x)=0$ from [2].

In Section 3, we describe a region $\mathcal{R} \subset \mathbb{R}^{12}$ which contains pairs $(A, B)$ corresponding to all totally real quartic fields. However it turns out that $\mathcal{R}$ is both non-compact and has infinite volume. In order to impose the conditions of having Galois group $A_4$ or $S_4$, and having discriminant bounded in absolute value by $X$, we restrict to a bounded sub-region having finite volume. This is done by cutting off cusps of $\mathcal{R}$, using simultaneously the boundedness of the discriminant and the restrictions on the Galois group. In particular, we employ a notion of absolutely irreducibility used in [4], for pairs $(A, B)$ which is equivalent to the condition that the Galois group of the corresponding quartic field is $S_4$ or $A_4$. We then find bounds on the coefficients of $(A, B)$ in our bounded sub-region having finite volume, using the reduction theory developed in Section 2, with the view to search for absolutely irreducible points in the region $\mathcal{B}$ defined by these bounds. These bounds are controlled further by the so-called unconditional bounds for products of coefficients of $(A, B)$ derived from the action of the torus in $\text{GL}_2(\mathbb{R}) \times \text{SL}_3(\mathbb{R})$.

In Section 4, we outline the algorithm itself and explain the steps of checking whether a pair $(A, B)$ is absolutely irreducible and corresponds to a maximal order in a quartic field. The techniques used to do so include a theorem of Wood [24]. This section is rather incomplete and will be more substantial in future versions.

In Section 5, we prove that the algorithm described in Section 4 has complexity $O(X^{1+\epsilon})$. Finally in Section 6, we discuss further work to be done, both as part of this project and otherwise.

Acknowledgements

I would like to thank my advisor Manjul Bhargava for all his enthusiasm and guidance during the course of this project. My thanks are also due to Kevin Wilson for having suggested the project to me and for many discussions about it, Arul Shankar for various clarifications and discussions, Brenda Hiller for a conversation about the computational aspects of the project, and Ila Varma for her invaluable tips on writing. This junior paper represents a work in progress, as described in Sections 4 and 5, and I plan to keep working on this project after the official deadline has passed.

## 2 Parametrizations and Reduction Theory

### 2.1 Parametrizations of Quartic Rings

In this subsection, we describe the parametrizations of maximal orders in quartic fields due to Bhargava [3]. Let $G := \text{GL}_2 \times \text{SL}_3$ and let $G_k := \text{GL}_2(k) \times \text{SL}_3(k)$ where $k \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$. The integral orbits of the space of ternary quadratic forms under the natural action of $G_\mathbb{Z}$ are used in this parametrization. Let $V_\mathbb{R}$ be the 12-dimensional vector space of pairs $(A, B)$ of ternary quadratic forms over $\mathbb{R}$, where $A$ and $B$ are represented by $3 \times 3$ real symmetric matrices. Call $(A, B) \in V_\mathbb{R}$ integral if

$$2 \cdot (A, B) = \begin{pmatrix} 2a_{11} & a_{12} & a_{13} \\ a_{12} & 2a_{22} & a_{23} \\ a_{13} & a_{23} & 2a_{33} \end{pmatrix}, \begin{pmatrix} 2b_{11} & b_{12} & b_{13} \\ b_{12} & 2b_{22} & b_{23} \\ b_{13} & b_{23} & 2b_{33} \end{pmatrix},$$

where $a_{ij}$ and $b_{ij}$ are the entries of $A$ and $B$, respectively.
where \(a_{ij}\) and \(b_{ij}\) are integers. Let \(V_\mathbb{Z}\) denote the lattice of integral pairs in \(V_\mathbb{R}\). The group \(G_\mathbb{Z}\) acts naturally on \(V_\mathbb{R}\) as follows: If \(g = (g_2, g_3) \in G_\mathbb{Z}\) where \(g_2 = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \text{GL}_2(\mathbb{Z})\) and \(g_3 \in \text{SL}_3(\mathbb{Z})\), then \(g\) acts on \((A, B)\) as

\[
g \cdot (A, B) = \left( p(g_3 A g_3^t) + q(g_3 B g_3^t), r(g_3 A g_3^t) + s(g_3 B g_3^t) \right).
\]

It is clear that the above actions of \(\text{GL}_2(\mathbb{Z})\) and \(\text{SL}_3(\mathbb{Z})\) commute. This action turns out to have a unique polynomial invariant called the discriminant of \((A, B)\) given by \(\Delta_{A,B} := \text{Disc}(4 \cdot \text{Det}(Ax - By))\). Furthermore, the binary cubic form \(f_{A,B}(x, y) := 4 \cdot \text{Det}(Ax - By)\) is a covariant for the action of \(\text{GL}_2(\mathbb{Z})\) and is referred to as the cubic resolvent form.

The pair \((A, B) \in V_\mathbb{Z}\) is said to be absolutely irreducible if the cubic resolvent \(f_{A,B}\) is irreducible over \(\mathbb{Q}\), and if \(A\) and \(B\) have no common zeroes as conics in \(\mathbb{P}^2(\mathbb{Q})\). We then have the following theorem due to Bhargava that describes the parametrization of quartic rings:

**Theorem 2.1** (Bhargava, [3],[4]). There is a canonical discriminant-preserving bijection between the set of \(G_\mathbb{Z}\)-equivalence classes of elements \((A, B) \in V_\mathbb{Z}\) and the set of isomorphism classes of pairs \((Q, R)\) where \(Q\) is a quartic ring and \(R\) is a cubic resolvent ring. Moreover, if \((A, B)\) are absolutely irreducible, they correspond to pairs \((Q, R)\) where \(Q\) is an order in either an \(A_4\) or an \(S_4\)-quartic field.

The cubic resolvent ring of \(Q\) referred to above is a cubic ring \(R\) equipped with a certain quadratic resolvent mapping \(Q \rightarrow R\) whose definition can be found in [3]. It has been shown in [3] that every quartic ring has at least one cubic resolvent ring. Thus the above theorem tells us that by restricting to \((A, B)\) that are absolutely irreducible, we will be able to enumerate orders in quartic fields having Galois group (of the normal closure) isomorphic to either \(S_4\) or \(A_4\). If we further impose the condition that \(Q\) must be a maximal order, we will be essentially enumerating the quartic fields themselves. We do this checking that \(Q\) is maximal at every prime \(p \in \mathbb{Z}\), meaning that it is never contained in another order with index divisible by \(p\). This check terminates since we already know that \(Q\) is maximal at \(p \nmid \text{Disc}(Q)\). We discuss maximality in more detail in Section 4.

One additional restriction that we make is to the case of totally real orders, i.e. orders \(Q\) in quartic fields having 4 real embeddings, or equivalently, orders \(Q\) for which any corresponding pair of ternary quadratic forms has 4 common zeroes in \(\mathbb{P}^2(\mathbb{R})\). This is because the problem of reduction, which involves finding a suitable fundamental region containing representatives for all integral orbits, is easily solved in the totally real case but is harder otherwise. We discuss further prospects for these other cases in Section 5.

### 2.2 Reduction Theory

In this subsection, we describe a reduction theory for the case of totally real quartic fields. The action of \(G_\mathbb{C}\) on \(V_\mathbb{C}\) has a single Zariski open orbit over the complex numbers. Over \(\mathbb{R}\), this orbit breaks up into three non-degenerate real orbits \(V_\mathbb{R}^{(0)} \cup V_\mathbb{R}^{(1)} \cup V_\mathbb{R}^{(2)}\) where \(V_\mathbb{R}^{(i)}\) consists precisely of those elements \((A, B)\) having \(4 - 2i\) common zeroes in \(\mathbb{P}^2(\mathbb{R})\). We shall focus on \(V_\mathbb{R}^{(0)}\) whose absolutely irreducible elements correspond to orders in totally real \(S_4\) or \(A_4\)-quartic fields.

A pair \((A, B) \in V_\mathbb{R}^{(0)}\) is said to be \(\text{GL}_2(\mathbb{Z})\)-reduced if its cubic resolvent form \(f_{A,B}\) is \(\text{GL}_2(\mathbb{Z})\)-reduced [1]. More precisely, since we are interested in \(V_\mathbb{R}^{(0)}\), we say that \(f_{A,B}\) (having positive discriminant) is \(\text{GL}_2(\mathbb{Z})\)-reduced if its Hessian, a \(\text{GL}_2(\mathbb{Z})\)-covariant binary quadratic form having
negative discriminant, has one of its complex roots in the usual Gauss fundamental domain for the covariant action of the subgroup SL₂(Z) on ℱ, the upper half plane, denoted by ℱ₀(SL₂(Z)). We restrict to SL₂(Z) since the action of GL₂(Z) does not preserve ℱ – we can do this since the complex roots of the Hessian must be complex conjugates of each other, forcing one of them to lie in ℱ. Note that for covariance, the action of SL₂(Z) on ℱ must be a left action when the action on fₐₜₜₜ is a right action.

We describe ℱ₀(SL₂(Z)) using coordinates derived from the Iwasawa decomposition of SL₂(ℝ). The upper half plane ℱ is a symmetric space for the action of SL₂(ℝ) and can be viewed as SL₂(ℝ)/SO₂(ℝ). Taking the usual NAK decomposition for SL₂(ℝ), we have X ∈ ℱ corresponding to \[ \begin{pmatrix} 1 & u \\ u & 1 \end{pmatrix} \begin{pmatrix} t^{-1} \\ t \end{pmatrix}. \] Now if X ∈ ℱ₀(SL₂(Z)), we have from Gauss’s work that |u| ≤ \( \frac{1}{2} \) and \( t ≥ (1 - u^2)^{\frac{1}{2}} \) [21].

In order to describe the reduction theory for the action of SL₃(Z), we need to introduce a quadratic covariant denoted by Ωₐₜₜₜ[Z]. This covariant was written down by Bhargava in his Ph.D thesis [2], and is obtained by restricting the trace form \( Tr(x^2) \) on a quartic ring \( Qₐₜₜₜ \), associated to \( (A,B) \) by Theorem 2.1, to the subspace \( Tr(x) = 0 \). An explicit description of Ωₐₜₜₜ[Z] in terms of the coordinates of \( (A,B) \) can be found in the appendix to Chapter 5 of [2] and will be used in our computations. In the totally real case, Ωₐₜₜₜ[Z] is easily seen to be positive-definite which turns out to allow for a simple reduction theory.

We say that a pair \( (A,B) ∈ Vₗ₀(0) \) is SL₃(Z)-reduced if Ωₐₜₜₜ[Z] is SL₃(Z)-reduced, i.e. Ωₐₜₜₜ[Z] lies in a specific fundamental domain for the action of SL₃(Z) on the space \( Vₗ₀ \) of positive-definite ternary quadratic forms having real coefficients. This fundamental domain is specified by identifying \( Vₗ₀ \) with the symmetric space \( H' = SL₃(ℝ)/SO₃(ℝ) \). This identification is made by mapping positive-definite symmetric matrix \( ν' ∈ Vₗ₀ \) to \( X ∈ H' \) where \( ν' = XX^t \) is the Cholesky decomposition. The inverse identification takes \( X ∈ SL₃(ℝ)/SO₃(ℝ) \) to \( XX^t \) which is positive-definite using the NAK decomposition for SL₃(ℝ). We can now use the fundamental domain of Grenier for the action of SL₃(Z) on H’, introduced in [17] and described explicitly in [18], to reduce the quadratic covariant Ωₐₜₜₜ[Z]. Denote this fundamental domain by ℱ₀(SL₃(Z)) and let \( ℱ₀ : ℱ₀(Z) \times ℱ₀(Z) \to ℱ₀(Z) \).

ℱ₀₀(SL₃(Z)) is explicitly described in suitable Iwasawa coordinates for H’ by the inequalities given below. For \( Ω ∈ Vₗ₀(0) \), fix \( Ω' ∈ SL₃(C)/SO₃(C) \) corresponding to Ω under the identification described above (\( Ω = Ω'Ω'' \)), and write Ω’ in Iwasawa coordinates as follows:

\[
Ω' = \begin{pmatrix} 1 & u_1 & 1 \\ u_2 & 1 & u_3 \\ u_3 & u_2 & 1 \end{pmatrix} \begin{pmatrix} v \\ w \\ v' \end{pmatrix} = \begin{pmatrix} w \\ v \end{pmatrix}
\]

We describe Ω’ ∈ ℱ₀(SL₃(Z)) by the following inequalities [18][6]

1. \( v^3 ≤ v^3(1 - u_1 + u_2)^2 + w^2(1 - u_3)^2 + w^-2 \)
2. \( v^3 ≤ v^3(u_1 - u_2)^2 + w^2(u_3 - u_3)^2 + w^-2 \)

Bhargava denotes this covariant as \( Q \) which we have here reserved for quartic rings. Hence the change of notation to Ω.

The inequalities claimed to describe the fundamental domain, as stated in [18], do not in fact describe a fundamental domain – however, the error is computational and is easily fixed as in the inequalities given in our paper. In fact, the inequalities are unchanged except for \( v → v^3 \) and \( w → w^2 \).
3. \( v^3 \leq v^3 u_1^2 + u_2^2 \)
4. \( v^3 \leq v^3 u_1^2 + u_2^2 u_3^2 + w^{-2} \)
5. \( 1 \leq w^{-2} + u_3^2 \)
6. \( 0 \leq u_1, u_3 \leq \frac{1}{2} \)
7. \( 0 \leq |u_2| \leq \frac{1}{2} \)

Remark 2.2. We prefer to use this fundamental domain over the more standard fundamental domain obtained by Minkowski reduction since the unipotent coordinates \( u_i \) cut out an actual box in Grenier’s fundamental domain. In the case of Minkowski reduction, the bounds on \( u_3 \) are not constant making estimates harder to make.

Finally, a pair \((A, B) \in V^{(0)}_R\) is said to be \(G_Z\)-reduced if it is both \(GL_2(\mathbb{Z})\)-reduced and \(SL_3(\mathbb{Z})\)-reduced. This reduction theory allows us to test if two pairs \((A_1, B_1)\) and \((A_2, B_2)\) are \(G_Z\)-equivalent and also allows us to construct a fundamental region for the action of \(G_Z\) on \(V^{(0)}_R\).

3 Bounds on Coefficients

In this section, we describe bounds on the coefficients of \((A, B) \in V^{(0)}_R\) when \(|\Delta_{A,B}| \leq X\). These effectively define a “box” which contains all such pairs \((A, B)\) in which we perform our search. To construct this box, we first define a region \(\mathcal{R} \subset \mathbb{R}^{12}\) containing a fundamental region for the action of \(G_Z\) on \(V^{(0)}_R\) in which we search for pairs \((A, B)\). Fixing \(v_0 := (A_0, B_0) \in V^{(0)}_R\), we define \(\mathcal{R} := \mathcal{F} \cdot v_0\) where \(\mathcal{F} := N' \times \mathcal{F}_0 \times K(G_\mathbb{R}) \subset G_\mathbb{R}\). This allows us to test if two pairs \((A_1, B_1)\) and \((A_2, B_2)\) are \(G_Z\)-equivalent and also allows us to construct a fundamental region for the action of \(G_Z\) on \(V^{(0)}_R\).

We choose the pair of \(3 \times 3\) symmetric matrices

\[
(A_0, B_0) := \left( \begin{array}{c c}
1 & -2 \\
-2 & 1 \\
0 & \sqrt{3}
\end{array} \right)
\]

as \(v_0\) for our algorithm. This is because the Hessian of \(f_{A_0, B_0}\) is \(x^2 + y^2\) (upto a constant) while \(\Omega_{A_0, B_0}\) is \(x^2 + y^2 + z^2\) (upto a constant). Thus \(v_0\) is reduced and has its covariants to be invariant under the action of the orthogonal transformations in \(G_\mathbb{R}\). Moreover, if \(v := (A, B) \in \mathcal{F} \cdot v_0\), by covariance we have that \(f_{A, B} \in (\Lambda \times \mathcal{F}_0(SL_2(\mathbb{Z}))) \cdot f_{A_0, B_0}\) and \(\Omega_{A, B} \in \mathcal{F}_0(SL_3(\mathbb{Z})) \cdot \Omega_{A_0, B_0}\). This simplifies the process of estimating the coefficients of \((A, B) \in \mathcal{R}\).
3.1 Preliminary estimates

In this subsection, we make various preliminary estimates using the same notation as above. We first impose the condition of bounded discriminant on \( \mathcal{F} \). Since the only factor in \( \mathcal{F} = \Lambda' A' K \) that scales the discriminant of \( v \in V^{(0)}_R \) is \( \Lambda' \), bounding the discriminant by \( X \) translates to bounding \( \lambda \). If \( \Delta_{A_0,B_0} := \Delta_0 \), we have \( \Delta_{A_0,A_0^B} = \lambda^{12}\Delta_0 \). Thus we act by the subset

\[
\Lambda_X = \left\{ \left( \begin{array}{cc} \lambda & 0 \\ 0 & \lambda \end{array} \right), \left( \begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array} \right) \right\} : 0 < \lambda \leq \left( \frac{X}{\Delta_0} \right)^{\frac{1}{12}}.
\]

and denote \( \mathcal{F}_X = \Lambda_X N^A K \) and \( \mathcal{R}_X = \mathcal{F}_X \cdot v_0 \).

Since the actions of \( SL_2(\mathbb{Z}) \) and \( SL_3(\mathbb{Z}) \) commute, we act first by \( SL_3(\mathbb{Z}) \) and then by \( SL_2(\mathbb{Z}) \). We begin by bounding coefficients of \( SO_3(\mathbb{R}) \cdot (A_0, B_0) \). If \( \alpha \in SO_3(\mathbb{R}) \), since \( \alpha \alpha^t = I \), we have that

\[
\sum_{k=1}^3 \alpha_{ik}\alpha_{jk} = \delta_{ij}.
\]

It follows that for \( 1 \leq i, j, k \leq 3 \) and \( k \neq l \), we have

\[
|\alpha_{ik}\alpha_{jk} - \alpha_{il}\alpha_{jl}| \leq |\alpha_{ik}^2 + \alpha_{il}^2|^{1/2} |\alpha_{jk}^2 + \alpha_{jl}^2|^{1/2} \leq 1 \cdot 1 = 1.
\]

Thus if \( (C, D) = (\alpha A_0 \alpha^t, \alpha B_0 \alpha^t) \), we have that

\[
|c_{ij}| = |\alpha_{11}\alpha_{j1} - 2\alpha_{12}\alpha_{j2} + \alpha_{33}\alpha_{j3}| \leq |\alpha_{11}\alpha_{j1} - \alpha_{12}\alpha_{j2}| + |\alpha_{33}\alpha_{j3} - \alpha_{12}\alpha_{j2}| \leq 2.
\]

Similarly \( |d_{ij}| \leq \sqrt{3} \). We also note the bounds \( v \leq \frac{2}{\sqrt{3}} \) and \( t^{-1}, w \leq \frac{\sqrt{3}}{\sqrt{3}} \) from Section 2.

Finally, we include expressions for all \( a_{ij} \) and \( b_{ij} \) in terms of the coordinates derived from the Iwasawa decomposition and other \( a_{ij} \) and \( b_{ij} \). We omit the proofs since they are trivial but tedious. We use the same coordinates as in Section 2:

\[
\begin{align*}
a_{11} &= (v^2 \lambda/t) (c_{11} \cos \theta - d_{11} \sin \theta) \\
a_{12} &= u_1 a_{11} + (w\sqrt{v} \lambda/t) (c_{12} \cos \theta - d_{12} \sin \theta) \\
a_{13} &= u_3 a_{12} + (u_2 - u_1 u_3) a_{11} + (\lambda \sqrt{v})/((u/t)(c_{13} \cos \theta - d_{13} \sin \theta)) \\
a_{22} &= 2u_1 a_{12} - u_1^2 a_{11} + (w^2 \lambda)/(u/t)(c_{22} \cos \theta - d_{22} \sin \theta) \\
a_{23} &= 2u_3 a_{22} + u_1 a_{13} + (u_2 - 2u_1 u_3) a_{12} + (u_3^2 u_3 - u_1 u_2) a_{11} + \lambda/(u/t)(c_{23} \cos \theta - d_{23} \sin \theta) \\
a_{33} &= 2u_3 a_{23} - u_3^2 a_{22} + 2(u_2 - u_3 u_1) a_{13} + 2(u_1 u_3^2 - u_2 u_3) a_{12} - (u_1^2 u_3^2 - 2u_1 u_2 u_3 + u_2^2) a_{11} + (\lambda)/(w^2 v)(c_{33} \cos \theta - d_{33} \sin \theta) \\
b_{11} &= u a_{11} + v^2 \lambda t(c_{11} \sin \theta + d_{11} \cos \theta) \\
b_{12} &= u_1 b_{11} + \lambda w\sqrt{v}((u/t)(c_{12} \cos \theta - d_{12} \sin \theta) + t(c_{12} \sin \theta + d_{12} \cos \theta)) \\
b_{13} &= u_3 b_{12} + (u_2 - u_1 u_3) b_{11} + \lambda(\sqrt{v}/u)((u/t)(c_{13} \cos \theta - d_{13} \sin \theta) + t(c_{13} \sin \theta + d_{13} \cos \theta)) \\
b_{22} &= 2u_1 b_{12} - u_1^2 b_{11} + \lambda (w^2 v)/(u/t)(c_{22} \cos \theta - d_{22} \sin \theta) + t(c_{22} \sin \theta + d_{22} \cos \theta)) \\
b_{23} &= u_3 b_{22} + u_1 b_{13} + (u_2 - 2u_1 u_3) b_{12} + (u_3^2 u_3 - u_1 u_2) b_{11} + (\lambda)/(u/t)(c_{23} \cos \theta - d_{23} \sin \theta) + t(c_{23} \sin \theta + d_{23} \cos \theta)) \\
b_{33} &= 2u_3 b_{33} - u_3^2 b_{22} + 2(u_2 - u_3 u_1) b_{13} + 2(u_1 u_3^2 - u_2 u_3) b_{12} - (u_1^2 u_3^2 - 2u_1 u_2 u_3 + u_2^2) b_{11} + (\lambda)/(w^2 v)((u/t)(c_{33} \cos \theta - d_{33} \sin \theta) + t(c_{33} \sin \theta + d_{33} \cos \theta))
\end{align*}
\]
We note that the expressions given above are not independent of each other. In fact, the expression for a specific coefficient is dependent on previously defined coefficients precisely because our algorithm will comprise of 12-nested loops where each loop seeks to pick one of the twelve coefficients of a potential pair \((A, B)\) in terms of those already defined.

### 3.2 Cutting off the cusps

In this subsection, we explain how to reduce our problem to searching for lattice points in a compact region. Since we act on \(v_0\) by \(\mathcal{F}_X = \Lambda_X N' A' K'\) and \(N' A' K'\) is not compact, having 3 cuspidal regions going off to infinity, we have to cut off the cusps by imposing the conditions of absolute irreducibility on \((A, B) \in \mathcal{F} \cdot v_0\). Note that the cut-offs will depend on \(X\).

Fix the notation \(\chi_a = \frac{\sqrt{X}}{\sqrt{2}} \Delta_0^{-1/12}\) and \(\chi_b = \Delta_0^{-1/12}\) for convenience. Recall that absolute irreducibility implies that \(A\) and \(B\) do not have a common point in \(\mathbb{P}^2(\mathbb{Q})\) and the cubic resolvent \(f_{A,B}\) is irreducible over \(\mathbb{Q}\). By the covariance of \(f_{A,B}\), we have to check that \(f_{A_0,B_0}(x, y) = -8x^3 + 24xy^2\) has non-zero \(x^3\)-coefficient under the action of \(\mathcal{F}_X\) for otherwise it would be irreducible. Since the action of \(\text{SL}_3(\mathbb{R})\) fixes the cubic covariant, we only have to act by elements in \(\text{GL}_2(\mathbb{R})\). Picking Iwasawa coordinates, we find that the action of \(\Lambda_X \mathcal{F}_0(\text{SL}_2(\mathbb{Z})) \subset \text{GL}_2(\mathbb{R})\) on the \(x^3\)-coefficient takes

\[-8 \mapsto \frac{\lambda^3}{t^3} (-8 \cos^3 \theta + 24 \cos \theta \sin^2 \theta).\]

By imposing the conditions of absolute irreducibility and integrality, we have

\[t \leq \lambda \sqrt[3]{-8 \cos^3 \theta + 24 \cos \theta \sin^2 \theta} \leq 2 \left( \frac{X}{\Delta_0} \right)^{1/12} = 2 \chi_b X^{1/12}.\]

This cuts off the cusp when \(t \to \infty\) and \(\Delta_{A,B} \leq X\).

We need to cut off the two \(\text{SL}_3(\mathbb{R})\)-cusps as well. We do this using the condition that both \(a_{11}\) and \(b_{11}\) cannot be simultaneously zero as we would then have \([1:0:0] \in \mathbb{P}^2(\mathbb{Q}) \cap A \cap B\). We divide into two cases following [1]:

**Case 1:** \(|a_{11}| \geq 1\). Since \(|a_{11}| = \frac{w^2 \chi}{t} |c_{11} \cos \theta - d_{11} \sin \theta|\). If \(|a_{11}| \geq 1\), we have \(\frac{w^2 \chi}{t} \sqrt{t} \geq 1\) by Cauchy and the bounds for \(c_{ij}, d_{ij}\) from Section 2.1, which gives us the upper bound \(\chi_a^{1/2} X^{1/24}\) for \(\frac{1}{w}\). Further since \(v \leq \left( \frac{w^2}{1 - u^2} \right)^{1/3}\) we have that \(\frac{1}{w} \leq 8 \chi_a^{3/4} X^{1/16}\). This cuts off the cusp as \(v\) and \(w\) approach 0.

**Case 2:** If \(a_{11} = 0\) and \(b_{11} \neq 0\), we must have that

\[|b_{11}| = |v^2 \lambda (c_{11} \sin \theta + d_{11} \cos \theta)| \geq 1\]

implying that \(\frac{1}{v} \leq \chi_b \sqrt{2} \sqrt[3]{7} X^{1/12}\). Here we use the cut-off for \(t\) given above. We also have the estimate of \(\frac{1}{w} \leq \frac{2 \sqrt{2} \sqrt[3]{7} X^{3/2}}{\sqrt{3} \chi_b} X^{1/8}\) since \(\frac{1}{w^2} \leq \frac{4}{3 \sqrt{3}}\). This cuts off the cusp as \(v, w \to 0\). However, we divide here into two subcases for more precise estimates:
Case 2.1: \( a_{12} \neq 0 \). In this case we have that
\[
|a_{12}| = |u_1 a_{11} + w \frac{\lambda}{t} (c_{12} \cos \theta - d_{12} \sin \theta)| \geq 1
\]
which gives us that \( \frac{1}{w^{\sqrt{v}}} \leq \chi_a X^{\frac{1}{12}} \).

Case 2.2: \( a_{12} = 0 \). In this case, we must have by reducibility constraints that \( a_{22}, a_{13} \neq 0 \) and must therefore have absolute value atleast 1. Since
\[
|a_{13}| = \frac{\sqrt{v}}{w} \frac{\lambda}{t} |c_{13} \cos \theta - d_{13} \sin \theta| \geq 1
\]
implying that \( \frac{w}{\sqrt{v}} \leq \chi_a X^{\frac{1}{12}} \). Since
\[
|a_{22}| = \frac{w^2 \lambda}{v} \frac{\lambda}{t} |c_{22} \cos \theta - d_{22} \sin \theta| \geq 1
\]
we have that \( \frac{\sqrt{v}}{w} \leq \chi_a X^{\frac{1}{12}} \).

3.3 Asymptotics of coefficients

In this section we describe the asymptotics of coefficients of an absolutely irreducible pair \((A, B) \in \mathcal{R}_X\). We begin with the following lemma from [4]:

**Lemma 3.1** (Bhargava, [4]). Suppose \((A, B) \in \mathcal{F} \cdot v_0\) satisfies \(|\Delta_{A,B}| < X\). Let \(S\) be any multiset consisting of elements of the form \(a_{ij}\) or \(b_{ij}\). Let \(m\) denote the number of \(a\)'s which occur in \(S\), and let \(n = |S| - m\) denote the number of \(b\)'s; let \(i, j, k = 2|S| - i - j\) denote the number of indices in \(S\) equal to 1, 2 and 3 respectively. If \(m \geq n, 2i \geq j + k\) and \(i + j \geq 2k\), then
\[
\prod_{s \in S} |s| = O(X^{[S]/12}).
\]

Note: It is worth pointing out that while the result from above does in fact hold true in our situation, it depends on the choice of coordinates and it requires an effectively identical proof using the \(v, w\)-coordinates that we omit.

The asymptotics derived from Lemma 3.1 are unconditional, meaning that all terms in products of this form are bounded independent of the cut-offs for the cusps. In other words, the conditions of Lemma 3.1 are exactly those necessary to cancel out unbounded terms such as \(v^{-1}, w^{-1}\), and \(t\), in some of the coefficients with bounded terms such as \(v, w\) and \(t^{-1}\) in the others. The bound for \(\lambda\) is also independent of the cut-offs for the cusps. On the other hand, the asymptotics for the individual coefficients can and do depend on the cut-offs being used, for each of the three cases in the previous sub-section.

It is clear that \(a_{11}\) and \(a_{12}\) are \(O(X^{1/12})\) since the only term that scales them as \(X \to \infty\), is \(\lambda = O(X^{1/12})\). Now,
\[
a_{13} = u_2 a_{12} + u_1 a_{11} + \frac{\lambda \sqrt{v}}{w} \frac{\lambda}{t} (c_{13} \cos \theta - d_{13} \sin \theta)
\]
contains the term \(\sqrt{v}/w\) which is unbounded. To estimate this quantity, we have to use the cut-offs. If \(a_{11} \neq 0\), we find that \(a_{13} = O(X^{7/48})\) since \(w^{-1} = O(X^{1/16})\). If \(a_{11} = 0\) and \(a_{12} \neq 0\), we have
$a_{13} = O(X^{1/6})$ since $(w\sqrt{v})^{-1} = O(X^{1/12})$ whence $w^{-1} = O(X^{1/12})$ because $v \neq 0$. This estimate is seemingly imprecise, but the other option of using $|b_{11}| \geq 1$ yields $w^{-1} = O(X^{1/8})$ which isn’t as good. Finally, if $a_{11} = a_{12} = 0$, we have $a_{13} = O(X^{1/8})$ since $\sqrt{v}/w = O(X^{1/24})$. We can make similar arguments for all the other coefficients $a_{ij}$ and $b_{ij}$ which also yield asymptotics. However, doing so for $a_{33}, b_{13}, b_{22}, b_{23}$ and $b_{33}$ can gives us strictly worse asymptotics in some of the cases than certain unconditional bounds, obtained using Lemma 3.1. For instance, $b_{33}$ is asymptotically $O(X^{5/12})$, $O(X^{5/12})$, and $O(X^{1/2})$ when $a_{11} \neq 0$, $a_{11} = 0$ and $a_{12} \neq 0$, and $a_{11} = a_{12} = 0$ respectively. However because $a_{11}^2 b_{33} = O(X^{1/4})$, $a_{12}^2 b_{33} = O(X^{1/4})$, and $a_{13} a_{22} b_{11} b_{33} = O(X^{1/3})$ by Lemma 3.1, we get that $b_{33}$ is $O(X^{1/4})$, $O(X^{1/4})$, and $O(X^{1/3})$ in the three different cases. We note that in order for the third case to give us an actual asymptotic, we need $a_{13}, a_{22}, b_{11} \neq 0$. Similar asymptotics can be written down in some of the cases for $a_{33}, b_{13}, b_{22}, b_{23}$ and $b_{33}$ which are strictly stronger than those obtained using the cut-offs.

The following table contains individual asymptotics for all $a_{ij}$ and $b_{ij}$.

<table>
<thead>
<tr>
<th>Coefficient</th>
<th>Case 1</th>
<th>Case 2.1</th>
<th>Case 2.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a_{11}$</td>
<td>$O(X^{1/12})$</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$a_{12}$</td>
<td>$O(X^{1/12})$</td>
<td>$O(X^{1/12})$</td>
<td>0</td>
</tr>
<tr>
<td>$a_{13}$</td>
<td>$O(X^{1/48})$</td>
<td>$O(X^{1/6})$</td>
<td>$O(X^{1/8})$</td>
</tr>
<tr>
<td>$a_{22}$</td>
<td>$O(X^{1/8})$</td>
<td>$O(X^{1/6})$</td>
<td>$O(X^{1/8})$</td>
</tr>
<tr>
<td>$a_{23}$</td>
<td>$O(X^{1/8})$</td>
<td>$O(X^{1/6})$</td>
<td>$O(X^{1/8})$</td>
</tr>
<tr>
<td>$a_{33}$</td>
<td>$O(X^{1/4})$</td>
<td>$O(X^{1/4})$</td>
<td>$O(X^{1/8})$</td>
</tr>
<tr>
<td>$b_{11}$</td>
<td>$O(X^{1/6})$</td>
<td>$O(X^{1/6})$</td>
<td>$O(X^{1/6})$</td>
</tr>
<tr>
<td>$b_{12}$</td>
<td>$O(X^{1/6})$</td>
<td>$O(X^{1/6})$</td>
<td>$O(X^{1/8})$</td>
</tr>
<tr>
<td>$b_{13}$</td>
<td>$O(X^{1/6})$</td>
<td>$O(X^{1/6})$</td>
<td>$O(X^{1/8})$</td>
</tr>
<tr>
<td>$b_{22}$</td>
<td>$O(X^{1/6})$</td>
<td>$O(X^{1/6})$</td>
<td>$O(X^{1/4})$</td>
</tr>
<tr>
<td>$b_{23}$</td>
<td>$O(X^{1/6})$</td>
<td>$O(X^{1/4})$</td>
<td>$O(X^{1/3})$</td>
</tr>
<tr>
<td>$b_{33}$</td>
<td>$O(X^{1/4})$</td>
<td>$O(X^{1/4})$</td>
<td>$O(X^{1/5})$</td>
</tr>
</tbody>
</table>

There are two things to be noted about these asymptotics. Firstly, we make the obvious remark that they are not actual bounds but merely orders of growth. Thus using Lemma 3.1 to get asymptotics is insufficient - we are required to actually multiply terms together to find the necessary inequalities and constants. Secondly, it’s clear that the bounds obtained in this fashion are entirely insufficient to make the algorithm effectively linear. We need to impose further constraints on products of coefficients either by obtaining cancellation of diagonal terms as in Lemma 3.1 or by other means.

### 3.4 Estimating products of coefficients

In this subsection, we explain the various conditions that we use to constrain the growth of the coefficients. Each of the three cases involved in the cutting of the cusp is treated separately. A key problem faced in each is that of coefficients in a product becoming zero and trivializing bounds thus obtained. In order to deal with this, we have to choose the “right” inequalities from among the large number of possible unconditional bounds. We formulate this precisely as follows:
Problem. Consider the $n$-th nested loop for $1 \leq n \leq 12$ for a suitable as-yet-unspecified nesting of loops and let the corresponding coefficient be $\gamma[n-1]$. Write down all inequalities that control the size of $\gamma[n-1]$ and involve only the non-zero coefficients in the set of $n-1$ coefficients that have already been fixed.

It is clear that there are far too many inequalities for us to write them all down by hand. We therefore describe an algorithm that can be used to perform a precomputation for each of the three cases that produces all such inequalities, beginning with the case that $a_{11} \neq 0$.

We adopt the usual nesting of the loops in this case – coefficients of $A$ before coefficients of $B$, and the lexicographic ordering on the 6 distinct coefficients of $A$ and $B$ – to be able to use the positivity of $|a_{11}|$ in controlling the size of the other coefficients. Assume we are in the $n$-th loop, having already fixed $\{\gamma[0], \gamma[1], \ldots, \gamma[n-2]\}$ and trying to find a range of values for $\gamma[n-1]$. Define the sub-array of $\gamma$ denoted by $\xi$, which contains precisely the non-zero elements of $\gamma$ hitherto defined. Let $\xi[0] = a_{11}$ and let $\xi$ have $s \leq n-1$ elements defined. Assume $\gamma[n-1] \neq 0$, and $\xi[s] := \gamma[n-1]$. Now if $T \subset \{\xi[1], \ldots, \xi[s]\}$ such that $\xi[s] \in T$, there exists a minimal nonnegative integer $\ell_T$ such that $\left| a_{11}^{\ell_T} \prod_{\tau \in T} \tau \right|$ is bounded by satisfying Lemma 3.1; in particular, $\ell_T = 12 - |T|$ works. Observe from the expressions in Section 3.1 that $\xi[s]$ can be written as the sum of a linear expression in $\{\xi[0], \ldots, \xi[s-1]\}$ and a rational expression in $\lambda, v, w, t$, and functionals on $K(G_{\mathbb{R}})$ which were estimated in Section 3.1. Defining $F(T) := \prod_{\tau \in T} \tau$ we have

$$|\xi[s]a_{11}^{\ell_T} F(T)| \leq |F(T)| \sum_{\tau \in T \setminus \{\xi[s]\}} \alpha_\tau |F(T)||\tau| + |G(\lambda, v, w, t)||F(T)|,$$ for some $\alpha_\tau \in \mathbb{R}^+$

We can substitute the expressions for $\tau \in T \setminus \{\xi[s]\}$ in the product $|G(\lambda, v, w, t)F(T)|$ to obtain an unconditional bound from the resulting products of powers of $v, w,$ and $t$ that will be bounded. Thus we have an inequality that controls the size of $\xi[s]$ in terms of $T \subset \{\xi[0], \ldots, \xi[s-1]\}$.

Consider the case when $\gamma[n-1] = 0$. In general, there are no restrictions on individual coefficients being zero, but we also need that $\text{det}(A), \text{det}(B) \neq 0$. Thus $a_{12}, a_{22}$, and $a_{23}$ cannot all be simultaneously zero, since $\text{det}(A)$ would then be zero. The same applies for the following triples: $(a_{13}, a_{23}, a_{33})$, $(b_{11}, b_{12}, b_{13})$, $(b_{12}, b_{22}, b_{23})$, $(b_{12}, b_{22}, b_{23})$, $(b_{13}, b_{23}, b_{33})$, $(a_{22}, a_{23}, a_{33})$, $(b_{11}, b_{12}, b_{22})$, $(b_{22}, b_{23}, b_{33})$, and $(b_{33}, b_{13}, b_{11})$. Let $S_{\mathcal{B}}$ denote the set of all such 2 and 3-tuples that are never simultaneously zero. We impose these restrictions on $S_{\mathcal{B}}$ in the algorithm described in Section 4.

We give an example to illustrate the above method. Assume that $a_{12}$ is non-zero. Now using the expression for $a_{12}$, and $a_{13}$ in terms of the Iwasawa coordinates and some estimates from Section 3.1 we get,

$$|a_{12}a_{13}| \leq |(a_{11}a_{12}/2 + |a_{12}^2|)/2| + |a_{12}|(\sqrt{v}/tw)\lambda\sqrt{7}$$

$$\leq |(a_{11}a_{12}/2 + |a_{12}^2|)/2| + (v^2\lambda/(2t) + w\sqrt{v}\lambda/t)(\lambda\sqrt{v}/(wt))T^{7/2}$$

$$\leq |(a_{11}a_{12}/2 + |a_{12}^2|)/2| + (\lambda\sqrt{7}/t)^2(7v^5/2)(2w) + v^2$$

$$\leq |(a_{11}a_{12}/2 + |a_{12}^2|)/2| + (2\lambda^2/2)X^{1/4}.$$

The method described above is extremely general and applies to all unconditional bounds on products of coefficients of $A$ and $B$. 


If \( a_{11} = 0 \) and \( a_{12} \ne 0 \), we have also that \( b_{11} \ne 0 \). However, the approach taken in the first case will not always work here - in particular, the product \( a_{12}^2 \prod_{\tau \ne a_{11}, a_{12}} t \) is not bounded according to the conditions of Lemma 3.1. We use instead the following fact – for \((A, B)\) to be reduced, its quadratic covariant \( \Omega \) must also be reduced. We know that \( 0 \leq \omega_{12} \leq \omega_{11} \), since \( 0 \leq u_1 \leq \frac{1}{2} \) for reduced \( \Omega_{A, B} \). From the expression for \( \Omega_{A, B} \) in the appendix to Chapter 5 of [2], we can deduce an upper bound for \( |b_{33}| \) in terms of previously defined quantities. We nest the loops in the following order with non-zero elements at the outer-most nesting: \( a_{12}, b_{11}, a_{13}, \ldots, b_{33} \), and constrain the growth of coefficients using unconditional bounds of the form

\[
a_{12}^\ell_1 b_{11}^\ell_2 \prod_{\tau \in T} \tau \leq C_2 X^{(\ell_1 + \ell_2 + |T|)/12}
\]

for constant \( C_2 \) and minimal \( \ell_1 \) and \( \ell_2 \).

For \( a_{11} = a_{12} = 0 \), we mimic the previous case; here \( \{a_{13}, a_{22}, b_{11}\} \) are non-zero and can be used to constrain the growth of other coefficients. Observe from the expression for \( \Omega_{A, B} \), that in this case, \( \omega_{11} \) and \( \omega_{12} \) do not depend on \( b_{33} \). Furthermore, \( b_{13} \) appears in \( \omega_{11} \) in the term \( a_{13} a_{22} b_{11} b_{13} \) which is non-zero if \( b_{13} \) is non-zero. Thus we can extract an upper bound for \( |b_{13}| \) from the inequalities \( 0 \leq \omega_{12} \leq \omega_{11} \). Once \( b_{13} \) is fixed, we can extract an upper bound for \( |b_{33}| \) from \( |\omega_{13}| \leq \omega_{11} \) and \( \omega_{11} > 0 \) since \( |u_2| \leq \frac{1}{2} \) for reduced \( \Omega_{A, B} \). Thus we bound the coefficients \( b_{13} \) and \( b_{33} \) using the reduction theory for the quadratic covariant. We nest the loops as \( b_{11}, a_{13}, a_{22}, a_{23}, a_{33}, b_{12}, b_{22}, b_{23}, b_{13}, b_{33} \) and proceed as in the second case, replacing \( \{a_{12}, b_{11}\} \) with \( \{a_{13}, a_{22}, b_{11}\} \).

4 Outline of Algorithm

In this section we outline the steps of an algorithm to enumerate totally real quartic fields having Galois group \( A_4 \) or \( S_4 \) and discriminant bounded in absolute value by \( X \). This algorithm is a partial quartic analogue of [1], but is substantially more challenging since the dimension of the vector space under consideration is thrice as large. In particular, it is significantly harder to pick exactly the right set of inequalities by hand.[]

**Precomputation.** We perform a pre-computation to write down all bounds on the range of a specific coefficient. The method for doing this is discussed in Section 3.4.

**Step 1 (Searching for points in main loops).** We have three main loops through ranges for each of our coefficients \( a_{ij} \) and \( b_{ij} \) and as mentioned before, these are 12-nested loops. We loop through ranges for each coefficient which are defined using the precomputed inequalities. Since all our bounds are on the absolute values of the coefficients, we only search in positive ranges and assign signs only to the pairs \((A, B)\) that lie in our region. Let GAMMA be the array of previously defined coefficients stored with their corresponding indices and the character 'A' or 'B'. XI is the array of non-zero elements of GAMMA, Exp is a function that searches among the precomputed inequalities and finds all non-trivial bounds that can be deduced for the coefficient GAMMA[n][0].

---

[4] We emphasize that many aspects of this section are rather incomplete, notably the lack of an explicit algorithm to compute the splitting type of a pair of integral ternary quadratic forms and the lack of any implementation. This junior paper is a work in progress and future versions will be more complete.
and COND is a function that checks that no triple defined hitherto lies in $S_B$, defined in Section 3.4. The following is pseudo-code for a prototypical loop.

```python
Bound[n] = min(Exp(n, XI)))
for t in Range(Bound[n]):
    GAMMA[n][0] = t
    if t!=0:
        XI.append()= Gamma[n]
    else if(COND(n, GAMMA)==0:
        continue
    Bound[n+1] = ...
```

Proceed to **Step 2** for all points in our region.

**Step 2 (Checking if a pair is reduced).** We assign signs to the unsigned points; a positive sign for $a_{11}$, and all possible combinations of signs for other coefficients: this is because $(A, B)$ and $(-A, -B)$ correspond to the same quartic ring. Once we have a signed pair $(A, B)$, we have to check whether it is reduced. This is done by checking if $f_{A,B}$ is $\text{GL}_2(\mathbb{Z})$-reduced and if the quadratic covariant $\Omega_{A,B}$ is $\text{SL}_3(\mathbb{Z})$-reduced. We check that a root of the Hessian of $f_{A,B}$ lies in the Gauss fundamental domain described in Section 2.1 and also that $\Omega' \in \mathcal{H}'$ corresponding to $\Omega_{A,B}$ as defined in Section 2.1 lies in the fundamental domain of Grenier. Proceed to **Step 3** only for reduced pairs.

**Step 3 (Checking if a pair is absolutely irreducible).** To check that a reduced pair $(A, B)$ is absolutely irreducible, we must check that $f_{A,B}$ is $\mathbb{Q}$-irreducible and that $A, B$ have no points of intersection in $\mathbb{P}^2(\mathbb{Q})$. Since $f_{A,B}$ is a cubic, $\mathbb{Q}$-irreducibility implies the existence of a root in $\mathbb{P}^1(\mathbb{Q})$. Thus we can use the rational root theorem to make sure that $f_{A,B}$ is $\mathbb{Q}$-irreducible. The second condition is harder to make explicit. However we can use Theorem 4.1.1 in [24] due to Wood to switch from checking that $|A \cap B \cap \mathbb{P}^2(\mathbb{Q})| = 0$, to studying a binary quartic form associated to $(A, B)$. First, we check that the quadratic form $A$ is isotropic over $\mathbb{Q}$ by checking that it is isotropic over $\mathbb{Q}_p$, for $p \nmid \Delta_{A,B}$ [19], by the Hasse-Minkowski theorem [21]. If it isn’t, we’re done. Now that we know that $A$ has a $\mathbb{Q}$-point, we find one using the fast implementation of [11]. Call this point $P$. We use the existence of $P$ to find a transformation $\mu \in G_{\mathbb{Q}}$ such that

$$
\mu \cdot (A, B) = \begin{pmatrix}
0 & -\frac{1}{2} & 0 & 0 \\
-\frac{1}{2} & 0 & 0 & 1 \\
0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1
\end{pmatrix}
, 
\begin{pmatrix}
g_4 & 0 & \frac{g_4}{2} \\
g_0 & g_1 & \frac{g_2}{2} \\
\frac{g_2}{2} & \frac{g_2}{2} & g_2
\end{pmatrix}
$$

by taking $P$ to $[1 : 0 : 0]$, making $a_{11} = 0$, and then using a suitable combination of rational row and column operations (and) subtracting a multiple of $B$ from $A$, if the determinant of $A$ becomes zero at some stage. Theorem 4.1.1 in [24] now tells us that the rational étale algebra containing $Q_{A,B}$ is cut out by the binary quartic form

$$
g_{A,B}(x, y) := g_0x^4 + g_1x^3y + g_2x^2y^2 + g_3xy^3 + g_4y^4.
$$

Checking that $A \cap B \cap \mathbb{P}^2(\mathbb{Q}) = \emptyset$, is now equivalent to checking that $g_{A,B}$ has no linear factor, which is an application of the rational root theorem. Proceed to **Step 4** only for absolutely irreducible
Step 4 (Checking if a pair is maximal). As discussed in Section 2, to check that an absolutely irreducibly pair is maximal, we need to check that it is maximal at all primes. A quartic ring $Q$ is said to be maximal at prime $p$ if $Q \otimes \mathbb{Z}_p$ is not contained in any other quartic $\mathbb{Z}_p$-algebra. We note that if prime $p$ does not divide $\Delta_{A,B}$, the ring $Q_{A,B}$, which has the same discriminant as $(A, B)$, is unramified at $p$ and therefore maximal.

When considered over $\mathbb{F}_p$, $A$ and $B$ determine a pair of conics in $\mathbb{P}^2(\mathbb{F}_p)$. We recall the symbol $((A,B),p) := (f_1^{e_1}f_2^{e_2} \cdots)$ from [3], indexed by points of intersection of $A$ and $B$ in $\mathbb{P}^2(\mathbb{F}_p)$, where $f_i$ and $e_i$ are respectively the degree of the residue field and the multiplicity of point $i$. We find that there are 11 such symbols - $(1111)$, $(112)$, $(13)$, $(22)$, $(4)$, $(1^211)$, $(1^22)$, $(2^2)$, $(1^31)$, and $(1^4)$. However if $Q_{A,B}$ is ramified at $p$, we find that $e_i > 1$ and reduce to the list $(1^211), (1^22), (2^2), (1^31)$, and $(1^4)$. Now we have the following table of splitting types and corresponding greatest powers of $p$ dividing the discriminant of the quartic field containing $Q_{A,B}$, obtained from Table 2 in [6].

| Splitting Type | $p^\alpha || \Delta_{A,B}$ |
|----------------|-----------------------------|
| $1^211$        | $p$                         |
| $1^22$         | $p$                         |
| $1^21^2$       | $p^2$                       |
| $2^2$          | $p^2$                       |
| $1^21^2$       | $p^2$                       |
| $1^21$         | $p^4$                       |
| $1^4$          | $p^8$                       |

Now if we compute the splitting type of $(A,B)$, we just have to check that the greatest power of $p$ dividing $\Delta_{A,B}$ is the same as the corresponding power in the above table.

Once we check that $(A,B)$ is maximal at all primes, we know that $Q_{A,B}$ is the maximal order of the quartic field defined by $g_{A,B}(x,y)$. If necessary, we can determine the multiplication table of $Q_{A,B}$ from [3].

5 Complexity of Algorithm

In this section, we prove the following theorem:

**Theorem 5.1.** The algorithm has complexity $O(X^{1+\epsilon})$.

**Proof.** We prove the result separately in each of the three cases when $a_{11} \neq 0$, $a_{11} = 0$ but $a_{12} \neq 0$, and $a_{11} = a_{12} = 0$. Except in the second case which is more or less based on the third, the proof is drawn from the proofs of Lemmas 5.9 and 5.13 from [3]. If $a_{11} \neq 0$, we partition the set of pairs obtained at the end of our main loop into $2^{11}$ zero loci, one for each subset $T \in S := \{a_{12}, a_{13}, \ldots, b_{33}\}$. These loci are defined as the set of $(A, B)$ such that $a_{ij}$ or $b_{kl} = 0$ iff $a_{ij}$ or $b_{kl}$ are in $T$. For a specific $T$ and $(A, B)$ in its associated zero locus, it’s clear that

$$|a_{11}^{[T]} \prod_{t \in S \setminus T} t| < C_1 X$$
for some constant $C_1$ implying that the number of lattice points in the zero locus must be $O(X^{1+\epsilon})$. Summing up, we have the same for all pairs $(A, B)$ such that $a_{11} \neq 0$.

If $a_{11} = 0$ but $a_{12} \neq 0$, we have that $b_{11} \neq 0$. Assume that all variables except $b_{33}$ have been fixed. Now since we want the quadratic covariant to be reduced, we have $|\omega_{12}| \leq |\omega_{11}|$. We then deduce that

$$|\omega_{12}a_{12}a_{13}b_{13}b_{22}a_{23}b_{23}a_{33}b_{33}| \leq |\omega_{11}a_{12}a_{13}b_{13}b_{22}a_{23}b_{23}a_{33}b_{33}| = O(X)$$

by Lemma 3.1. Since the leading term of the smaller term of the above inequality as a polynomial in $b_{33}$ is $a_{12}^2b_{11}a_{13}b_{13}a_{22}b_{22}a_{23}b_{23}a_{33}b_{33}$, we get that the number of choices for $b_{33}$ when all other coefficients are fixed is

$$O(X/a_{12}^2b_{11}a_{13}b_{13}a_{22}b_{22}a_{23}b_{23}a_{33}b_{33}).$$

Summing over all other terms, we get $O(X^{1+\epsilon})$ choices for $(A, B)$.

If $a_{11} = a_{12} = 0$, we observe that $\omega_{12}$ does not depend on $b_{33}$. Using Lemma 3.1 and the fact that $\Omega$ is reduced,

$$|\omega_{12}a_{23}b_{23}| \leq \omega_{11}a_{23}b_{23} = O(X^{1/6}).$$

Since the leading term of $\omega_{12}a_{23}b_{23}$ as a polynomial in $b_{13}$ is $a_{13}a_{23}b_{12}b_{23}b_{13}$, we get that the number of choices for $b_{13}$ when all other coefficients except $b_{33}$ are fixed is

$$O(X^{1/2}/a_{13}a_{23}b_{12}b_{23}).$$

Similarly, from $|\omega_{13}| \leq |\omega_{11}|$ and Lemma 3.1, we get that the number of choices for $b_{33}$ when all other coefficients are fixed is

$$O(X^{1/2}/a_{13}a_{22}b_{11}a_{33}b_{22}).$$

Multiplying the two and summing over all other terms we get that the number of choices for $(A, B)$ in this case is $O(X^{1+\epsilon})$.

Since for each point picked, the additional computational complexity is constant, we get that the total complexity is $O(X^{1+\epsilon})$ as desired. \qed

### 6 Future Work

This junior paper is far from being a finished product and there is certainly much more work to be done. The next step is to implement the algorithm described in Section 4, keeping constants small to avoid a combinatorial explosion. One possible means of doing this is to reduce the number of inequalities used, especially since some of the bounds are never attained.

The subsequent task is less clear, but it falls vaguely under the goal of improving the complexity. While the algorithm described in this junior paper is effectively linear, one might hope to remove the logarithms to make it $O(X)$. In [2], Bhargava obtains a power saving by careful estimation of the sizes of the coefficients which if followed through carefully, appears to give a linear algorithm. However the error estimate in that case is $O(X^{191/192+\epsilon})$ which appears to be far too close to $O(X)$ to make any apparently significant difference for $X \sim 10^{10}$. One can hope that through further such estimates, this algorithm can be made linear with a sufficiently small error term. Work in this direction might also throw light on the existence and nature of a secondary term, analogous to the one conjectured by Roberts [20] and proved recently by Bhargava-Shankar-Tsimerman and
Taniguchi-Thorne \[7\] \[23\], especially since the work of Belabas in \[1\] was extremely crucial in the making of this conjecture.

A natural generalization of this work would be to find similar algorithms for fields that have complex embeddings. The key difficulty in doing so is the lack of a corresponding reduction theory for $\text{SL}_3(\mathbb{Z})$ since the reduction of indefinite forms is very difficult. One possible approach is to follow the reduction theory of \[22\] due to Stoll, which works for point clusters rather than forms; however, in this case the quadratic covariant is obtained by a process of minimization and is rather hard to make explicit. Furthermore, the covariant thus obtained is not necessarily integral.

At this stage, while the problem of counting for quintic extensions has been successfully addressed by Bhargava \[5\], the use of the averaging technique first introduced in \[4\] forces one to work harder to find a similar algorithm and it is not yet clear whether this is feasible.

References


