On the Spinor Genus and the Distinguishing Lattice Isomorphism Problem

Cong Ling[1], Jingbo Liu[2], and Andrew Mendelsohn[1]

[1] Department of EEE, Imperial College London, United Kingdom.
c.ling@imperial.ac.uk, andrew.mendelsohn18@imperial.ac.uk
[2] Department of Computational, Engineering, and Mathematical Sciences, Texas A&M University-San Antonio, USA.
jliu@tamusa.edu

Abstract. This paper addresses the spinor genus, a previously unrecognized classification of quadratic forms in the context of cryptography, related to the lattice isomorphism problem (LIP). The spinor genus lies between the genus and equivalence class, thus refining the concept of genus. We present algorithms to determine whether two quadratic forms belong to the same spinor genus. If they do not, it provides a negative answer to the distinguishing variant of LIP. However, these algorithms have very high complexity, and we show that the proportion of genera splitting into multiple spinor genera is vanishing (assuming rank $n \geq 3$). For the special case of anisotropic integral binary forms ($n = 2$) over number fields with class number 1, we offer an efficient quantum algorithm to test if two forms lie in the same spinor genus. Our algorithm does not apply to the HAWK protocol, which uses integral binary Hermitian forms over number fields with class number greater than 1.

Keywords: quadratic forms · lattice isomorphism problem · spinor genus · class group.

1 Introduction

Lattices have been studied for almost 30 years by the cryptographic community, since works by Ajtai [1, 2] gave worst-case to average-case reductions for lattice problems and an encryption scheme whose hardness was based on such worst-case lattice problems, as well as the introduction of NTRU [21]. Since then other foundational problems for lattice-based cryptography have been introduced, notably Learning with Errors [28]. A recent addition to these is the Lattice Isomorphism problem.

Informally, the Lattice Isomorphism problem (LIP) is, given two lattices, to decide if they are isomorphic or not. This can be rephrased in the language of quadratic forms: the LIP is, given two quadratic forms, to decide whether they lie in the same equivalence class or not, and if so to find such an isomorphism. This problem was studied by Haviv and Regev [20], who gave an $n^{O(n)}$ algorithm to solve the problem. This problem was given cryptographic applications by van

Woerden and Ducas [15], who gave worst-case to average-case reductions for certain forms of the problem, and constructed a KEM and signature scheme relying on the hardness of LIP. This was followed by the signature scheme HAWK [14], which relied on the security of LIP restricted to module lattices. The growing application and use of LIP-based schemes thus makes cryptanalysis of interest to the cryptological community. We also note [5], which studied a closely related problem to the LIP, named the lattice distortion problem.

The first step in a cryptanalytic direction was made in [7], which analysed the distribution of quadratic forms corresponding to random q-ary lattices in genera. Each quadratic form has an associated equivalence class, and each equivalence class lies in a genus. The disjoint union of equivalence classes 'fills out' the genera (i.e. each genus is a disjoint union of equivalence classes, and each class lies in one genus). Thus, *if* two forms were to lie in distinct genera, and this could be efficiently verified, a method for providing a negative answer to the LIP would be provided. The conclusion of that study was, informally, that 'most' random q-ary lattices lie inside one of few 'large' genera, and thus two forms can be sampled at random from a 'large' genus with the property that rejection sampling only negligibly biases the final distribution of forms.

Further work was done investigating the viability of using lattice hulls to solve LIP instances in [13], and the possibility of using characteristic vectors and lattice automorphisms to solve LIP was studied in [23].

In this work we continue the above line of investigation, studying notions of equivalence for positive definite integral quadratic forms. The contribution of this paper begins with a largely expository account of the *spinor genus*, a collection of equivalence classes with respect to an equivalence relation defined by the kernel of a certain homomorphism known as the *spinor norm*. A spinor genus is a disjoint union of equivalence classes, much like the genus, but a genus may contain multiple spinor genera. Thus, given two quadratic forms, one might compute their spinor genera, and if they lie in different spinor genera, the forms are not equivalent, providing a negative answer to distinguish LIP for those two forms. We observe that the spinor genus was omitted from the 'arithmetic fingerprint' of [15], and we here fill this lacuna.

1.1 Overview of Methodology

At a high level, spinor genera provide a finer classification of quadratic forms over $\mathbb{Z}$ than genera. It is well known that for quadratic forms over $\mathbb{Q}$, the equivalence of two forms can be determined by checking their equivalence over the p-adic fields $\mathbb{Q}_p$ for all primes p (including $p = \infty$). According to the famous local-global principle, two forms are equivalent over $\mathbb{Q}$ if and only if they are equivalent over $\mathbb{Q}_p$ for all p. While it may seem tempting to extend this method to classify quadratic forms over $\mathbb{Z}$, the theory encounters limitations. If two forms are equivalent over the p-adic integers $\mathbb{Z}_p$ for all p (including $p = \infty$), they are not necessarily equivalent over $\mathbb{Z}$; rather, they only belong to the same genus. In a sense, the genus highlights the constraints of local methods.

The spinor genus is a new classification intermediate between the genus and

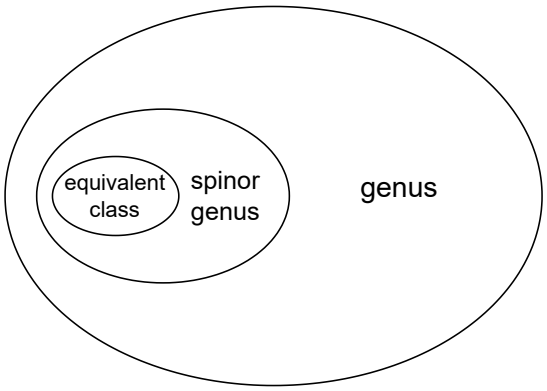

Fig. 1: Relation between the genus and spinor genus of quadratic forms.

the integrally equivalent class. It combines local and global methods. To study the spinor genus, we need the theory of Clifford algebra to define the spin group and spinor norm. A Clifford algebra is an algebra generated by a vector space V equipped with a quadratic form, which is a powerful mathematical machinery to study quadratic forms. The spin group $\mathrm{Spin}(n)$ gives a double cover of the special orthogonal group of a vector space. A prototype spin group, Spin(3), consisting of unit quaternions, is widely used in computer graphics to rotate objects in 3 dimensions. The spin group is closely related to the spinor kernel, which consists of autometries of a vector space determined by certain elements with spinor norm 1 in the Clifford algebra [8]. Therefore, the spinor kernel is well suited to the study of LIP.

The relation between the genus and spinor genus is illustrated in Fig. 1. Using the language of lattices, we give in Table 1 a more precise comparison of the definitions of the equivalent class, spinor genus and genus. Since both orthogonal group $O(V)$ and spinor kernel $\Theta(V_p)$ are subgroups of orthogonal group $O(V_p)$, it is easy to see the inclusions in Fig. 1. For extensive treatments of quadratic forms, see the classic references [8, 27].

Classification	Definition	Transform	Remark
Class	$\Gamma = \gamma\Lambda$	$\gamma \in O(V)$	O orthogonal group
Spinor genus	$\Gamma_p = \gamma\delta_p\Lambda_p, \forall p$	$\gamma \in O(V), \delta_p \in \Theta(V_p)$	Θ spinor kernel
Genus	$\Gamma_p = \beta_p\Lambda_p, \forall p$	$\beta_p \in O(V_p)$	p prime

Table 1: Comparison of various classifications of lattices. Γ, Λ are lattices, V is a vector space, and subscript $_p$ denotes localization. See Sections 2, 3 for details.

1.2 Main Results

It is well known that the while genera of quadratic forms exist in any dimension $n \geq 3$ which contain multiple spinor genera, such genera are in some sense rare. To each quadratic form is associated a *Jordan p-symbol*, which classifies the genus of the form. We show that the proportion of Jordan p-symbols which correspond to genera which split into multiple spinor genera is a vanishing fraction of all possible Jordan p-symbols. We summarise this as

Theorem 1. *(Informal) For the set of quadratic forms of prime power determinant and rank such that the genus could split into multiple spinor genera, only a negligible proportion of such forms do in fact lie in such genera.*

A similar result holds for composite determinant. We then proceed to study algorithms to compute the number of spinor genera in a genus, and whether two forms lie in the same spinor genus. We consider such algorithms first over the rational integers, and then over rings of integers in number fields. The latter case is extracted from the work of [4]. We include discussion of the complexity of this algorithm. Summarising the results of Section 5, we find:

Theorem 2. *Let F be a number field with ring of integers $\mathcal{O}_F$ is a PID. Assume V is an n-dimensional vector space over F with a non-degenerate quadratic form ϕ and associated symmetric bilinear form b, and $n \geq 3$. Suppose L and $\tilde{L}$ are quadratic lattices on V and they are in the same genus. Then there is an effective algorithm to decide if $\tilde{L} \in \mathrm{spn}^+(L)$, the proper spinor genus of L.*

We also discuss the barriers to this algorithm being efficient. Currently, the complexity of these algorithms to compute the spinor genus appears to be super-exponential, and we welcome further research to reduce their complexity.

Finally, we study the special case of integral binary quadratic forms over the ring of integers of a number field. This is of particular cryptographic interest, since HAWK relies on the hardness of these instances. In this case, when the ring of integers of the number field is a principal ideal domain (PID), it turns out that the spinor genus can be computed via a particularly simple algorithm: deciding if two forms lie in the same spinor genus is equivalent to deciding quartic residuosity in a certain class group, which can be done efficiently using (quantum) algorithms by Hallgren. We note that in the case of forms over $\mathbb{Z}$, a similar result was proved in [19]; we rely on the subsequent work of [16, 17].

To state our result, let F be a number field with ring of integers $\mathcal{O}_F$. If (V, ϕ) is a quadratic space over F and we need not reference ϕ, we may simply write V for the space; in the binary case, when (V, ϕ) is anisotropic, we may view V as a quadratic field extension of F with ring of integers $\mathcal{O}_V$. Let the proper spinor genus of a quadratic form g be written $\mathrm{spn}^+(g)$. Let L_g be the lattice corresponding to the quadratic form g. Finally, denote the left order of a lattice L by $\mathcal{O}_l(L) := \{x \in V : xL \subset L\} \subset V$. We prove:

Theorem 3. *Let F be a number field with ring of integers $\mathcal{O}_F$ is a PID. Let f and g be two anisotropic binary quadratic forms, integral over $\mathcal{O}_F$, in the same*

genus. Let V be the dimension 2 quadratic space containing L_f and L_g. Then if $L_f \cdot L_g^{-1}$ generates an ideal coprime to the conductor of $\mathcal{O}_l(L_g)$ in $\mathcal{O}_V$, there is a quantum polynomial time algorithm to decide if $f \in \mathrm{spn}^+(g)$.

We note that this does not affect HAWK, since HAWK uses integral binary Hermitian forms over cyclotomic fields of conductor $n \in \{512, 1024\}$. The cyclotomic field of largest conductor such that it has ring of integers a PID has $n = 90$. However, our work complements that of [26], since they show that module-LIP over the ring of integers of totally real fields has an efficient solution, and we note that the class number of maximal totally real subfields of cyclotomic fields of power-of-two conductor is believed to be 1 for all powers of two, and that this is confirmed up to $n = 256$, and assuming GRH, for $n = 512$ [25]. Our result does not just hold for these (maximal totally real sub-) fields, however, since it applies to all integral binary quadratic forms over number fields with ring of integers a PID.

1.3 Paper Organisation

After providing some background, we then define the notion of spinor genera in Section 3. We begin with quadratic forms over $\mathbb{Z}$: in Section 3.3, a step is taken towards understanding 'how often' genera split into distinct spinor genera, while in Section 4, an algorithm is presented to compute the spinor genus of a positive definite integral quadratic form, adapted from Conway and Sloane [12, Chapter 15]. After this, we move to quadratic forms over number fields: in Section 5 Conway and Sloane's algorithm is extended to lattices over number fields; in Section 6 we specialise to binary quadratic forms over maximal orders of number fields, and give a quantum polynomial time algorithm to decide if two forms lie in the same spinor genus. We conclude the paper in Section 7, applying our results to LIP and commenting on their applicability to existing schemes.

2 Preliminaries

2.1 Notation

We write $[n]$ for the set of integers $\{1, ..., n\}$. For any field F, we denote by $F^\times$ its group of units. For two orthogonal subspaces V_1, V_2 we use $V_1 \perp V_2$ to denote their direct sum. The dual space of V will be denoted $\widehat{V}$.

2.2 Lattices

A lattice is a discrete additive subgroup of $\mathbb{R}^n$. A lattice L can be generated by a number of linearly independent vectors $\mathbf{b}_1, ..., \mathbf{b}_m$ that form a basis $B = [\mathbf{b}_1, ..., \mathbf{b}_m]$, and if $m = n$ then L is full-rank. A lattice L with basis B may be written $L = L(B)$.

One may consider lattices, more abstractly, as discrete additive subgroups of a vector space V over a field F. The case of the previous paragraph is then that

of $F = \mathbb{R}$. We state an important theorem for lattices, known as the *Invariant Factors Theorem*:

Theorem 4. *[27, §81D] Let L_1 and L_2 be lattices on a vector space V/F. Then there is a basis $x_1, ..., x_n$ for V such that*

$$L_1 = \mathfrak{a}_1 x_1 + ... + \mathfrak{a}_n x_n \text{ and } L_2 = \mathfrak{a}_1\mathfrak{t}_1 x_1 + ... + \mathfrak{a}_n\mathfrak{t}_n x_n$$

where the $\mathfrak{a}_i$ and $\mathfrak{t}_i$ are fractional ideals satisfying $\mathfrak{t}_1 \supset \mathfrak{t}_2 \supset ... \supset \mathfrak{t}_n$. Moreover, the $\mathfrak{t}_i$ satisfying the above are unique.

2.3 Quadratic Forms

Let F be a number field with characteristic not equal to 2, and $\mathcal{O}_F$ be the ring of integers of F. A quadratic form is a homogeneous polynomial of degree two, written $f(\mathbf{x}) = \sum_{i,j=1}^{m} a_{ij}x_i x_j$, with coefficients a_{ij} lying in F. Such a form can be associated to an $m \times m$ symmetric matrix $A_f = (a_{ij})_{i,j}$. The determinant of f is the determinant of A_f.

We say that two quadratic forms f, g are *equivalent* over $\mathcal{O}_F$ if and only if there exists $U \in GL_m(\mathcal{O}_F)$ such that $A_g = U^T A_f U$. This is an equivalence relation, and the classes obtained from the quotient by this relation are called *classes* of quadratic forms.

Definition 1. A quadratic form f is called *isotropic* if there exists $x \in V \setminus \{0\}$ such that $f(x) = 0$. If no such x exists, we call f *anisotropic*.

When F is a totally real number field (i.e., all embeddings of F into $\mathbb{C}$ are real), we will be most concerned with certain families of quadratic forms:

Definition 2. We call f *positive definite* if $f(x)$ is totally positive (i.e., all conjugates of $f(x)$ are positive) for any $x \in V\setminus\{0\}$, and f *negative definite* if $f(x)$ is totally negative (i.e., all conjugates of $f(x)$ are negative) for any $x \in V \setminus \{0\}$. Otherwise, we call f *indefinite*.

All forms over totally real number fields below will be assumed positive definite. Note if a form is positive definite, it is anisotropic. One may then obtain the Cholesky decomposition of A_f, $A_f = B_f^T B_f$, so one can always write the symmetric matrix of a quadratic form in such a manner. We denote the lattice with basis B satisfying $A_f = B^T B$ by $L_f = L(B)$.

Given a lattice L with basis B, one can form the symmetric matrix $B^T B$. This can then be considered as the matrix corresponding to a quadratic form f. Thus one can move between the 'world' of lattices and the 'world' of quadratic forms. In this vein, we call the pair of a vector space V over F and a quadratic form mapping from V to F, say ϕ, a *quadratic space*. We call V *regular* if $\det \phi \neq 0$.

To any quadratic form ϕ on V is also associated a symmetric bilinear form $b : V \times V \to F$, which can be constructed via the *polarisation identity*

$$b(v, w) = \frac{1}{2}(\phi(v + w) - \phi(v) - \phi(w))$$

2.4 Orthogonal Groups

Let (V, ϕ) be a quadratic space. We may then consider the isomorphisms $\sigma : V \to V$ such that $\phi(\sigma x) = \phi(x)$, that is the set of automorphisms preserving the quadratic form. This collection forms a group known as the *orthogonal group* $O(V)$ of V. These are linear transformations, so we can define the determinant of σ to be the determinant of the corresponding linear transformation of V, fixing some basis of V/F. An element of the orthogonal group has either determinant equal to 1 or -1; it thus contains a subgroup known as the *proper orthogonal group*; we have

$$O(V) = \{\sigma : V \to V : \phi(\sigma x) = \phi(x) \forall x\} \text{ and } O^+(V) = \{\sigma \in O(V) : \det \sigma = 1\}$$

These notions have analogues for lattices within a quadratic space: for any lattice $L \subset V$ we set

$$O(L) = \{\sigma \in O(V) : \sigma L = L\} \text{ and } O^+(L) = \{\sigma \in O^+(V) : \sigma L = L\}$$

Important subsets of $O(V)$ are the involutions and symmetries. An element $\sigma \in O(V)$ is called an *involution* if $\sigma^2 = \mathrm{Id}$. There is a family of involutions known as symmetries, which we will use below: we say an involution τ is a *symmetry*[3] if there is some fixed anisotropic vector $y \in V$ such that

$$\tau(x) = \tau_y(x) := x - \frac{b(x, y)}{\phi(y)} y$$

for all $x \in V$.

We can use the orthogonal group to give a definition of equivalence of lattices: we say Γ is equivalent to Λ if and only if there exists some $\gamma \in O(V)$ such that $\Gamma = \gamma\Lambda$.

2.5 p-adic Integers

We give a brief introduction to p-adic arithmetic; for a fuller introduction aimed at cryptographers, see for example [10].

Let p be a prime and $\frac{a}{b} \in \mathbb{Q}^\times$. We may then write $\frac{a}{b} = p^i \cdot \frac{a'}{b'}$ uniquely with both a', b' coprime with p and $i \in \mathbb{Z}$. We may then define the p-adic norm on $\mathbb{Q}$ as $|\frac{a}{b}|_p := p^{-i}$. One may verify that this satisfies the properties of a norm, and satisfies the ultrametric inequality.

Taking the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$ for some fixed prime p yields the p-adic rationals $\mathbb{Q}_p$. This contains a subring $\mathbb{Z}_p$, the p-adic integers, defined

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$$

One may view $\mathbb{Z}_p$ as the completion of $\mathbb{Z}$ with respect to the p-adic norm.

It will also be useful to consider another subring of $\mathbb{Q}_p$, the localisation of $\mathbb{Z}$ at a prime p:

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{Z} \setminus p\mathbb{Z} \right\}$$

[3] Sometimes known as a 'reflection'.

This is in fact both a subring of $\mathbb{Z}_p$ and a subring of $\mathbb{Q}$.

We now record some useful properties of $\mathbb{Z}_p$ and $\mathbb{Z}_{(p)}$. We begin with units. We have

$$\mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p : |x|_p = 1\} \text{ and } \mathbb{Z}_{(p)}^\times = \left\{ \frac{a}{b} \in \mathbb{Z}_{(p)} : \gcd(a,p) = 1 \right\}$$

Both rings each has only one prime ideal, which is therefore maximal:

$$\mathrm{Spec}(\mathbb{Z}_p) = p\mathbb{Z}_p \text{ and } \mathrm{Spec}(\mathbb{Z}_{(p)}) = p\mathbb{Z}_{(p)}$$

The units therefore are

$$\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus p\mathbb{Z}_p \text{ and } \mathbb{Z}_{(p)}^\times = \mathbb{Z}_{(p)} \setminus p\mathbb{Z}_{(p)}$$

We may define an equivalence relation on $\mathbb{Q}_p^\times$ as follows: we say $a \sim b$ if and only if $\frac{a}{b} \in \left(\mathbb{Q}_p^\times\right)^2$. The quotient of $\mathbb{Q}_p^\times$ by this relation yields a number of p-adic *square classes*. We list the possible classes here, for future reference, categorised by the value of p (following the notation of [12]; for more detail see [8]):

1. $p = \infty$ (i.e. the case of $\mathbb{R}$): we have representatives u and $-u$, where u is any strictly positive number.
2. $p = 2$: we have 8 classes, with representatives $u_1, u_3, u_5, u_7, 2u_1, 2u_3, 2u_5, 2u_7$, where $u_i \in \mathbb{Z}_2^\times$ satisfies $u_i \equiv i \bmod 8$.
3. $p > 2$: we have 4 classes, with representatives u_+, u_-, pu_+, pu_-, where u_+ (u_- respectively)$\in \mathbb{Z}_p^\times$ is a quadratic residue (nonresidue respectively).

***p*-adic Diagonalisation** Given any quadratic form f, it is possible to diagonalise the matrix A_f over the p-adic integers, and in fact diagonalise A_f over the subring $\mathbb{Z}_{(p)} \subset \mathbb{Z}_p$ (except that this is a block-diagonalisation if $p = 2$). The algorithm to perform this diagonalisation is given in [12], and runs as follows: find the entry of A_f least divisible by p. If this entry is on the diagonal, begin diagonalising as usual (subtracting multiples of rows and columns from one another). If this entry is off the diagonal in the (i,j)th position, add the jth row to the ith row and the jth column to the ith column, and proceed as before. If $p = 2$, it is possible to obtain a block of the form

$$2^k \begin{pmatrix} a & b \\ b & c \end{pmatrix}$$

for some k, where a, c are even and b is odd, instead of a wholly diagonal matrix.

One then obtains a corresponding decomposition of f over $\mathbb{Z}_p$. If $p > 2$, this has the form

$$f = f_0 \oplus pf_1 \oplus \ldots \oplus p^k f_k \oplus \ldots$$

where the f_i are p-adically integral represented by diagonal $n_{p^i} \times n_{p^i}$ matrices with $\gcd(\det f_i, p) = 1$, and if $p = 2$ the f_i may possibly be represented by the 2×2 matrices given above. The f_i are called the *Jordan constituents* of f.

Genera We say f and g lie in the same *genus* if and only if they are locally equivalent for all primes p, and over the reals; that is to say, we have

$$A_g \sim_{\mathbb{Z}_p} A_f \quad \forall\ p$$

and $A_g \sim_{\mathbb{R}} A_f$, which is the case if and only if there exist $U_p \in GL_m(\mathbb{Z}_p)$ such that $A_g = U_p^T A_f U_p$ for all p, and $U \in GL_m(\mathbb{R})$ such that $A_g = U^T A_f U$. There are finitely many genera with the given determinant and dimension, and each genus is a finite disjoint union of equivalence classes.

Equivalently, in terms of lattices we say that Γ and Λ which are on the same space V lie in the same genus if there exist $\beta_p \in O(V_p)$ such that $\Gamma_p = \beta_p \Lambda_p$ for all primes p.

$\mathfrak{p}$-adic Norms and Number Fields The above can all be extended to algebraic number fields. We assume some familiarity with the splitting and ramification of primes in rings of integers of number fields; for background, see for example [24]. We begin with a definition: say two norms $|\cdot|_1, |\cdot|_2$ are equivalent if there exists some $\varrho \in \mathbb{R}^+$ such that $|\cdot|_1^\varrho = |\cdot|_2$.

Let F be a number field with ring of integers $\mathcal{O}_F$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$. Then we say there is a *norm* of F corresponding to each prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$, each embedding σ of F into $\mathbb{R}$, and each pair of embeddings into $\mathbb{C}$. The latter two kinds of norms are called *real* and *complex* respectively.

We first consider the norms associated to prime ideals. For any $\alpha \in F^\times$, let $(\alpha) = \mathfrak{p}^i \prod_j \mathfrak{p}_j^{e_j}$ be the factorisation of (α) into products of prime ideals. We then define $|\alpha|_\mathfrak{p} = N_{F/\mathbb{Q}}(\mathfrak{p})^{-i}$. By a *prime spot* $\mathfrak{p}$ we mean the equivalence class of norms containing $|\cdot|_\mathfrak{p}$. We may then consider the completion $F_\mathfrak{p}$ of F under $|\cdot|_\mathfrak{p}$.

For a real embedding σ, we define a norm $|\cdot|_\sigma = |\sigma(\cdot)|$, the absolute value of the embedding into $\mathbb{R}$. We call the equivalence class of norms containing $|\cdot|_\sigma$ a real spot. We can define the complex spots in a similar manner.

2.6 Jordan p-Symbols

From a p-adic diagonalisation of f as above, one can read off a number of invariants of f, which classify the genus of f. In fact, with $\left(\frac{a}{p}\right)$ denoting the Legendre symbol, one can say

Theorem 5. *[12, Chapter 15, Theorem 9] For $p \neq 2$, f is equivalent to g over $\mathbb{Z}_p$ if and only if the precise powers of p, the dimensions n_{p^i}, and the signs $\epsilon_{p^i} = \left(\frac{\det f_i}{p}\right)$ occuring in their Jordan decompositions are identical.*

These invariants are encoded in the Jordan p-symbol (called the 'p-adic symbol' in [12]), which is a formal product of factors q^{ϵ_q, n_q}.

A similar but more complicated result holds for $p = 2$, which we omit for brevity.

3 Spinor Genera and Proportion of Splitting Genera

In this section we define the spinor genus of a quadratic form. In order to make the definition precise, we proceed via Clifford algebra.

3.1 Clifford Algebra

Let (V, ϕ) be a regular quadratic space of dimension n over a field K. There is a unique algebra $C(V)$ over K of dimension 2^n satisfying

1. $C(V)$ is spanned by 1 and formal products $x_1...x_r$, $x_i \in V$,
2. $xx = \phi(x)$ for $x \in V$.

If V has normal basis $e_1, ..., e_n$, then in $C(V)$ we have $e_i e_j = -e_j e_i$ and $e_i e_i = \phi(e_i) \in K$. This $C(V)$ is the Clifford algebra associated to V.

For $J \subset [n]$ with $j_1 < ... < j_r$, define $e(J) := e_{j_1} e_{j_2} ... e_{j_r}$ and set $e(I)e(J) = \ell(I, J)e(K)$ where $K = \{i : i \in I \text{ or } i \in J,\ i \notin I \cap J\}$, and

$$\ell(I, J) = \left(\prod_{i \in I, j \in J, i > j} -1 \right) \cdot \left(\prod_{i \in I \cap J} \phi(e_i) \right).$$

Sending $x \mapsto -x \in V$ extends to give an automorphism of $C(V)$. Set

$$C_0(V) = \{u \in C(V) : u \text{ is fixed by the above automorphism}\}.$$

The *involution* on $C(V)$ is defined by extending linearly the map

$$e(J) = e_{j_1} e_{j_2} ... e_{j_r} \mapsto e_{j_r} e_{j_{r-1}} ... e_{j_1} =: e(J)'$$

This involution[4] satisfies

1. $(u')' = u$ for all $u \in C(V)$
2. $u' = u$ if $u \in V$
3. $(uv)' = v'u'$ for any $u, v \in C(V)$.

For $u \in C(V)$, if u is (multiplicatively) invertible define $T_u : x \mapsto uxu^{-1}$. Then

Lemma 1. *[8, Chapter 10, Lemma 3.1] If $u \in C(V)$ is invertible and $T_u(x) = uxu^{-1} \in V$ for all $x \in V$, then $T_u \in O(V)$.*

Inspired by this, define the group

$$M_0(V) = \{u \in C_0(V) : u^{-1} \text{ exists},\ T_u : V \to V\}$$

Then

Lemma 2. *[8, Chapter 10, Theorem 3.1] $O^+(V) \cong M_0(V)/K^\times$.*

[4] The involution (sometimes called the 'transpose') is not to be confused with the automorphism used to define $C_0(V)$.

Moreover, if $u \in M_0(V)$, then $u = a_1 ... a_r$ for an even r, $a_j \in V$, and $uu' \in K^\times$. Define the spin group

$$\mathrm{Spin}(V) = \{u \in M_0(V) : uu' = 1\}$$

and

$$\Theta(V) = \{T_u : uu' = 1\}.$$

The latter is called the *spinor kernel*, a name which will be clarified in the following section. We now relate $\mathrm{Spin}(V)$ and $\Theta(V)$:

Theorem 6. *[8, Chapter 10, Theorem 3.3] There is an homomorphism*

$$\mathrm{Spin}(V) \twoheadrightarrow \Theta(V),\ u \mapsto T_u$$

with kernel $\{\pm 1\}$.

Spinor Norm We reach the application of the theory developed in the previous sections. Let $\sigma \in O^+(V)$. Then we can write σ as a map T_u for some $u \in M_0(V)$, and then map $u \mapsto uu' \bmod (K^\times)^2$. The composition of these maps is called the *spinor norm*:

Theorem 7. *[8, Chapter 10, Corollary 3] The map* $\theta : \sigma \mapsto uu' \bmod (K^\times)^2$ *is a multiplicative homomorphism.*

Proof. It is plain that the identity maps to the identity. Consider $\sigma, \tau \in O^+(V)$. We show $\theta(\sigma\tau) = \theta(\sigma)\theta(\tau)$.

First note that by Lemma 2, $\sigma\tau$ corresponds to some product $uv \in M_0(V)/K^\times$. Then $\theta(\sigma\tau) = (uv)(uv)' = uvv'u' = uu'vv'$ since $vv' \in K^\times$. Moreover, we have $\theta(\sigma)\theta(\tau) = uu'vv'$. □

3.2 Defining the Spinor Genus

The spinor norm can be used to define an equivalence relation on the space of quadratic forms, via lattices.

Definition 3. Let Γ, Λ be lattices on the quadratic space (V, ϕ). Say $S(\Gamma, \Lambda)$ holds if there exist $\gamma \in O^+(V)$ and $\delta_p \in \Theta(V_p)$ such that

$$\Gamma_p = \gamma\delta_p\Lambda_p, \text{ for all } p.$$

We call the equivalence classes under this relation the (proper) *spinor genera*. Note that if $f \sim g$, then setting the δ_p to be the identity for all p implies that $S(L_f, L_g)$ holds. So equivalent lattices lie in the same spinor genus. Moreover, if $S(L_f, L_g)$ holds, then since $\Theta(V_p) \subset O(V_p)$, we have $g \in \mathrm{gen}(f)$. The following demonstrates that the spinor genus truly is an 'intermediate' relation to the class and the genus:

Theorem 8. *[8, Chapter 11, Lemma 1.4]* $S(\Gamma, \Lambda)$ *is an equivalence relation.*

Proof. Symmetry and reflexivity are straightforward; here we demonstrate transitivity. Suppose Γ, Λ, Δ are three lattices satisfying $S(\Gamma, \Lambda)$ and $S(\Lambda, \Delta)$. Then there are $\gamma_1, \gamma_2 \in O^+(V)$ and $\beta_{1p}, \beta_{2p} \in \Theta(V_p)$ such that $\Gamma_p = \gamma_1\beta_{1p}\Lambda_p$ and $\Lambda_p = \gamma_2\beta_{2p}\Delta_p$ for each prime p. Combining these, one has

$$\Gamma_p = \gamma_1\beta_{1p}\gamma_2\beta_{2p}\Delta_p = (\gamma_1\gamma_2)(\gamma_2^{-1}\beta_{1p}\gamma_2\beta_{2p})\Delta_p$$

for each prime p. It is easy to check $\gamma_1\gamma_2 \in O^+(V)$ and $\gamma_2^{-1}\beta_{1p}\gamma_2\beta_{2p} \in \Theta(V_p)$. Hence $S(\Gamma, \Lambda)$ holds. □

We record some standard facts on the set of spinor genera [8, Chapter 11]:

Proposition 1. *1. The number of spinor genera in any genus is a power of 2.*
2. For all $n \geq 3$ there exist lattices whose genus contains multiple spinor genera.
3. Let (V, ϕ) be a quadratic space of dimension $n \geq 3$, $\Lambda \subset V$ a lattice, and ϕ takes integral values on Λ. If $\mathrm{gen}(\Lambda)$ contains multiple spinor genera, either there exists $p > 2$: $p^{\frac{n(n-1)}{2}} \mid \det(\Lambda)$, or $2^{n(n-3)/2+\lfloor(n+1)/2\rfloor} \mid \det(\Lambda)$.

3.3 Proportion of Genera Splitting into Multiple Spinor Genera

In this section we obtain an upper bound on the number of Jordan p-symbols corresponding to forms which lie in a genus which splits into multiple spinor genera. In the rest of this subsection we will call such genera, forms in a given genera, and their corresponding p-symbols, 'splitting', for convenience. The point of this result is to show that a negligible number of such p-symbols in the prime-power case correspond to forms in such genera, when $n \geq 3$.

Odd Prime-power Determinant We begin by considering forms of rank $n \geq 3$ and determinant $p^{n(n-1)/2}$ for some prime $p > 2$, as this is the minimal prime-power determinant for which the genus of a form specified by rank and determinant can split into more than one spinor genus (cf. Proposition 1). Observe that a necessary condition for such splitting is that the Jordan decomposition of the form has no component with dimension larger than one, i.e. the prime powers occurring in the p-adic diagonalisation of the form are all distinct (this may be seen from Section 4, (i)). That is, up to multiplication by p-adic quadratic residues or non-residues on the diagonal elements and reordering, f has corresponding matrix A p-adically diagonalising to

$$A_{D,p} = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & p & 0 & \dots & 0 \\ 0 & 0 & p^2 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & p^{n-1} \end{pmatrix},$$

which has determinant $p^{n(n-1)/2}$. If a form has determinant a higher power of p, the proportion of forms will be upper bounded by the below result also. We

do not address the power-of-two case, for simplicity.

We will proceed by (straightforwardly) finding the number of splitting Jordan p-symbols, and we then lower bound the total number of p-symbols for forms with the above-specified parameters ($\text{rank}\, f = n$, $\det f = p^{n(n-1)/2}$). In the latter instance, f has corresponding matrix A p-adically diagonalising to

$$A_{D,p} = \begin{pmatrix} p^{i_1} & 0 & ... & 0 \\ 0 & p^{i_2} & ... & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & ... & p^{i_n} \end{pmatrix}, \tag{1}$$

up to multiplication by quadratic residues (or non-residues), with determinant $p^{n(n-1)/2}$, so $\sum_j i_j = n(n-1)/2$. In the more general case of determinant p^m for some $m > n(n-1)/2$, one has $\sum_j i_j = m$.

Step 1: splitting symbols To find the number of splitting Jordan p-symbols, observe from the algorithm reproduced above that we must have distinct prime powers on the diagonal of $A_{D,p}$. Thus the Jordan p-symbol of a splitting form must be $1^{\epsilon_1,1}p^{\epsilon_p,1}p^{2^{\epsilon_{p^2}},1}...p^{n-1^{\epsilon_{p^{n-1}}},1}$. Moreover, in the case of prime-power determinant, all the ϵ_i agree: the diagonals must all be distinct powers of p, either multiplied by quadratic residues modulo p, or all multiplied by quadratic non-residues modulo p. So there are at most two splitting p-symbols for such fixed parameters.

Step 2: bounding the number of p-symbols We lower bound the number of p-symbols for the family of forms mentioned above. The number we are seeking to approximate is the following:

$$A_{n,m} := \left| \left\{ 1^{\epsilon_1,n_1}p^{\epsilon_p,n_p}...p^{n-1^{\epsilon_{p^{n-1}},n_{p^{n-1}}}} \,:\, \sum_{i=0}^{n-1} n_{p^i} = n \text{ and } \sum_{i=0}^{n-1} i n_{p^i} = m \right\} \right|,$$

initially in the specific instance $m = n(n-1)/2$. By observing (1), it is sufficient to count the number of n-tuples $(i_1, ..., i_n)$ satisfying $\sum_j i_j = m$, each multiplied by 2^{k-1}, where k is number of distinct terms in the n-tuple; this multiplicative factor, since each entry of the diagonal of (1) may be multiplied by a quadratic residue or non-residue.

We use some elementary partition theory to conduct this counting exercise; for more background on partitions, see for example [3].

Definition 4. Let l be an integer. A decomposition $l = \lambda_1 + ... + \lambda_k$ into positive integers λ_i is called a partition of l. The λ_i are called the parts of the partition, and k is called the length of the partition. The number of partitions of an integer l is denoted by $p(l)$.

Now let

$$p_{i,j}(l) := |\{\text{partitions of } l \text{ of length } i \text{ with } j \text{ distinct parts}\}|.$$

Write $r := n(n-1)/2$. One can then express $A_{n,r}$ as a weighted sum of $p_{i,j}(r)$:

$$A_{n,r} = \sum_{(i,j)\,:\,i\geq j\geq 1}^{n} p_{i,j}(r)\cdot 2^j,$$

because of the quadratic residues or non-residues on each diagonal term of (1).

Pick (i,j) such that $i+j$ is maximal in $[2,2n]$ with respect to the property that $p_{i,j}(r)\neq 0$. Then $A_{n,r} > p_{i,j}(r)\cdot 2^j$. So we now proceed to find (i,j) maximal with respect to $i+j$ such that $p_{i,j}(r)\neq 0$.

Recall $r = n(n-1)/2$. Then

$$p_{i,j}(r) = |\{\text{partitions of } n(n-1)/2 \text{ of length } i \text{ with } j \text{ distinct parts}\}|$$

is $p_{i,j}(\cdot)$ applied to the $(n-1)$th triangle number, which has a maximal partition of length $n-1$ into distinct parts of length $n-1$ by definition. So $(i,j) = (n-1,n-1)$ is a pair satisfying $i+j$ is maximal and $p_{i,j}(r)$ is non-zero. Then

$$\begin{aligned} A_{n,r} &= \sum_{i\geq j\geq 1}^{n} p_{i,j}(n(n-1)/2)\cdot 2^j \\ &> p_{n-1,n-1}(n(n-1)/2)\cdot 2^{n-1} = 2^{n-1}. \end{aligned}$$

Now suppose $\det f \geq p^m$ for odd prime p and integer $m \geq r$. The number of splitting p-symbols in this case is upper bounded by

$$2\left(p_{n,n}(m) + p_{n-1,n-1}(m)\right) \leq 4p_{n-1,n-1}(m)$$

To bound the total number of symbols, observe that $p_{n-1,n-1}(m) \geq 1$ for $m \geq r$. From the above reasoning it follows that a lower bound on $A_{n,m}$ is

$$\begin{aligned} A_{n,m} &= \sum_{i\geq j\geq 1}^{n} p_{i,j}(m)\cdot 2^j \\ &\geq p_{n-1,n-1}(m)\cdot 2^{n-1} \geq 2^{n-1} \end{aligned}$$

Step 3: proportion of splitting forms for odd prime-power determinants Since there are at most 2 splitting Jordan p-symbols, for a form of determinant p^r and rank n, the fraction of symbols corresponding to forms whose genus splits into multiple spinor genera is less than $2/2^{n-1} = \frac{1}{2^{n-2}}$, which is a negligible function in n. We have thus arrived at

Theorem 9. *Let $p > 2$ be a prime. The proportion of splitting p-symbols corresponding to positive definite quadratic forms of rank $n \geq 3$ and determinant $p^{n(n-1)/2}$ among all possible p-symbols is strictly less than $2^{-(n-2)}$.*

When $m > r$, an upper bound for the proportion of splitting p-symbols is

$$\frac{4p_{n-1,n-1}(m)}{\sum_{i\geq j\geq 1} p_{i,j}(m)\cdot 2^j}$$

The proportion can then be bounded by considering $i = j = n - 1$:

$$\frac{4p_{n-1,n-1}(m)}{\sum_{i\geq j\geq 1}^{n} p_{i,j}(m)\cdot 2^j} \leq \frac{4}{2^{n-1}} = \frac{1}{2^{n-3}},$$

which is a negligible function in n.

For the case of odd composite determinants, we note the following. As above, we have a set $\mathcal{S}$, comprised of prime divisors of $2d$ and ∞. Suppose $|\mathcal{S}| = t$. We then have to compute the Jordan p-symbols at each element of this set. By Proposition 1, there must be at least one prime divisor of the determinant which divides the determinant many times, and any element of $\mathcal{S}$ may be this divisor. We can thus upper bound the proportion of splitting symbols by $\frac{t}{2^{n-3}}$, which is negligible when t is polynomially large.

We leave the $p = 2$ case to the interested reader, for brevity; the details of this case can be found in [12].

4 An Algorithm to Compute Spinor Genera

Inspired by Conway and Sloane [12, Chapter 15], in this section we provide a (quantum) polynomial time algorithm to calculate the number of spinor genera in the given genus with rank n is at least 3. Let f and g be two positive definite quadratic forms with determinant d in the same genus. In view of [30, Theorem 50], there is a rational matrix M such that $A_f = M^t A_g M$ with $|\det M| = 1$ and denominators of its entries are relatively prime to $2d$. Let L_f and L_g be the corresponding lattices that reflect this property. Then $[L_f : L_f \cap L_g] = [L_g : L_f \cap L_g] = r$ for some integer r which is relatively prime with $2d$.

Let $\mathcal{S}$ be the finite set of prime divisors of $2d$. We denote a spinor operator by a sequence $(\ldots, r_p, \ldots)_{p\in\mathcal{S}}$, where r_p is a p-adic unit square class. For each $p \in \mathcal{S}$, choose a proper isometry $\sigma_p \in O^+(V_p)$ with $\theta(\sigma_p) = r_p$. Let L_h be the lattice in the genus of L_f with $(L_h)_p = \sigma_p(L_f)_p$ for each $p \in \mathcal{S}$ and $(L_h)_p = (L_f)_p$ for each $p \notin \mathcal{S}$. Then the spinor operator $(\ldots, r_p, \ldots)_{p\in\mathcal{S}}$ sends $\mathrm{spn}^+(f)$ to $\mathrm{spn}^+(h)$ where h is a quadratic form defined on L_h. More information about the action of a spinor operator can be found in [8, Chapter 11]. In this notation the group operation is componentwise multiplication, and the rational or p-adic integers can be regarded as spinor operators in the following way. For a rational integer r that is relatively prime to $2d$, the corresponding spinor operator is $\Delta(r) = (r, \ldots, r)$; for a p-adic integer $A_p = p^k a$ there corresponds the spinor operator $\Delta_p(A_p) = (p^k, \ldots, p^k, a, p^k, \ldots, p^k)$ whose q-coordinate for $q \neq p$ is the q-adic unit square class of p^k and whose p-coordinate is the p-adic unit square class of a.

By [8, Theorem 4.1 in Chapter 11], $\Delta(r) * \mathrm{spn}^+(f) = \mathrm{spn}^+(g)$ where $r = [L_f : L_f \cap L_g]$. Moreover when the rank is at least 3, $\Delta(r) * \mathrm{spn}^+(f)$ is defined for every positive integer r prime to $2d$. Thus there is a surjective map from the set of spinor operators $\Delta(r)$ with r positive integers prime to $2d$ to the set of spinor genera in $\mathrm{gen}(f)$, and we can determine the number of the spinor genera

by determining the kernel of this map, i.e., those $\Delta(r)$ which fix each spinor genus.

By Theorem 16 and Theorem 17 in [12, Chapter 15], the spinor operator kernel consists of the spinor operators $\Delta(r)$ for which the positive integer r is an automorphous number (the spinor norm of a proper integral isometry in $O^+(L_f)$) and relatively prime to $2d$. The spinor operator kernel can be calculated locally and is generated by the spinor operators $\Delta_p(A_p)$ for each $p \in \mathcal{S}$ where A_p is a p-adically automorphous number (the spinor norm of a proper p-adic integral isometry in $O^+((L_f)_p)$).

As the spinor operator kernel is completely determined by the p-adically automorphous numbers, it is necessary to introduce an algorithm for identifying the p-adically automorphous numbers associated with the given quadratic form f. Recall that f is diagonalizable at $p \geq 3$, and f is a direct sum of quadratic forms that are of the shapes $2^k(x)$ or $2^k \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ at $p = 2$, where a, c are even and x, b are odd. Now we want to create a set consisting of numbers in the following two parts:

(I) when $p \geq 3$, all the diagonal entries; when $p = 2$, the diagonal entries $2^k x$.
(II) only when $p = 2$, the numbers $2^{k+1}u_1, 2^{k+1}u_3, 2^{k+1}u_5, 2^{k+1}u_7$ for every 2-dimensional component $2^k \begin{pmatrix} a & b \\ b & c \end{pmatrix}$.

Then the group of p-adically automorphous numbers is generated by the p-adic square classes of the products of all pairs of numbers from the above list, and supplemented by:

(i) all p-adic units if either $p \geq 3$ and $\dim f_k \geq 2$ for any k, or $p = 2$ and $2^k f_k \oplus 2^{k+1} f_{k+1} \oplus 2^{k+2} f_{k+2} \oplus 2^{k+3} f_{k+3}$ has dimension ≥ 3 for any k.
(ii) the square classes $2u_1, 2u_3, u_5, u_3, u_7$ whenever $p = 2$ and part (I) of the list contains two entries whose product has the form $u_1, u_5, (1 \text{ or } 4 \text{ or } 16)u_{\text{odd}}$, $(2 \text{ or } 8)u_{1 \text{ or } 5}, (2 \text{ or } 8)u_{3 \text{ or } 7}$ respectively.

Remark:

1. If there is a prime p such that, for each p-adic unit u, the spinor operator $\Delta_p(1, \ldots, 1, u, 1, \ldots, 1)$ is in the spinor operator kernel, then the prime p can be removed from the set $\mathcal{S}$, as it conveys no information modulo the spinor operator kernel. We call such a prime *p tractable*.
2. For any spinor operator $(r_1, \ldots, r_s)$, by the Strong Approximation Theorem [27, 21:2], there is a positive integer r such that $\Delta(r) = (r_1, \ldots, r_s)$.

Theorem 10. *There is a (quantum) polynomial time algorithm to determine the number of spinor genera in the genus of the given quadratic form f.*

Proof. Let d be the determinant of the given quadratic form f. There are at most $\log_2(2d)$ different prime divisors of $2d$. We can compute in time poly(n, $\log_2 d$) the diagonalisation of f_p using the method introduced in Section 2.5 and its p-adically automorphous numbers for all primes p dividing $2d$.

Algorithm 1: An algorithm to determine the number of spinor genera in gen(f)

Input: Quadratic form f
Output: Answer
1: Compute the p-adic diagonalisation of f for each $p \mid 2d$
2: Compute p-adically automorphous numbers for each $p \mid 2d$
3: $\mathcal{S} := \{p \mid 2d : p \text{ is intractable}\}$
4: Compute a basis $\mathcal{G}$ of the spinor operators kernel with respect to $\mathcal{S}$.
5: **if** $2 \in \mathcal{S}$ **then**
6: Output'$2^{|\mathcal{S}|+1-|\mathcal{G}|}$,
7: **else**
8: output '$2^{|\mathcal{S}|-|\mathcal{G}|}$,
9: **end if**

When $p \geq 3$, p is tractable if the non-square unit u_- is in $\theta(O^+((L_f)_p)$ or both pu_+ and pu_- are contained in $\theta(O^+((L_f)_p)$. Therefore, if p is intractable, then p contributes at most one non-trivial spinor operator $\Delta_p(pu_+)$ or $\Delta_p(pu_-)$ to the generators of the spinor operator kernel. The prime 2 is tractable if one of the following is true:

1. two of three non-square units u_3, u_5, u_7 are in $\theta(O^+((L_f)_2)$;
2. three of four prime elements $2u_1, 2u_3, 2u_5, 2u_7$ are contained in $\theta(O^+((L_f)_2)$;
3. one non-square unit u and two prime elements whose product is in the different square class from u in $\theta(O^+((L_f)_2)$.

Therefore if 2 is intractable, then 2 contributes at most three non-trivial spinor operators to the generators of the spinor operator kernel. Let $\mathcal{S} = \{p \mid 2d : p \text{ is intractable}\}$. Then there are $2^{|\mathcal{S}|}$ different spinor operators with respect to $\mathcal{S}$ when $2 \notin \mathcal{S}$ and $2^{|\mathcal{S}|+1}$ different spinor operators with respect to $\mathcal{S}$ when $2 \in \mathcal{S}$. Once we can determine the size of the spinor operator kernel with respect to $\mathcal{S}$, the number of the spinor genera in gen(f) will be determined.

Let $\mathcal{G} = \{\Delta_1, \ldots, \Delta_t\}$ ($t \leq \log_2(8d)$) be the set of different non-trivial spinor operators obtained from the p-adically automorphous numbers for all $p \in \mathcal{S}$. It generates the spinor operator kernel with respect to $\mathcal{S}$. We can further obtain a basis by applying Gaussian elimination to the matrix G with $\log \Delta_1, \ldots, \log \Delta_t$ as its rows. We denote $\log u_1 = 0$ for $p = 2$ and $\log u_+ = 0$ for $p \geq 3$. Suppose $\log \Delta'_1, \ldots, \log \Delta'_{t'}$ are all nonzero rows in the "Echelon form" of G, then the set $\tilde{\mathcal{G}} = \{\Delta'_1, \ldots, \Delta'_{t'}\}$ is a basis of the spinor operator kernel with respect to $\mathcal{S}$ and can be obtained in time poly($\log_2 d$). □

Algorithm 1 shows the pseudocode of the procedure given above. The spinor operator kernel can also help us to identify if two quadratic forms f and g are in the same spinor genus or not: f and g are in the same spinor genus if and only if $\Delta(r)$ where $r = [L_f : L_f \cap L_g]$ is a product of some generators $\Delta_p(A_p)$ where $A_p \in \theta(O^+(L_f)_p)$. This is shown in Algorithm 2, where all the steps can be completed in (quantum) polynomial time except for Steps 1. For Step 1, [12]

Algorithm 2: An algorithm to distinguish the spinor genera

Input: Quadratic forms f and g in the same genus
Output: Answer

1: Compute a rational matrix M with denominators of its entries relatively prime to $2d$ by solving the system of quadratic equations $A_f = M^t A_g M$
2: Compute a matrix B_g such that $B_g^t B_g = A_g$ using Cholesky decomposition
3: $L_g \leftarrow$ lattice generated by B_g
4: $B_f := B_g M$ and $L_f \leftarrow$ lattice generated by B_f
5: Compute $r = [L_f : L_f \cap L_g]$ using Hermite Normal Form
6: Compute the p-adic diagonalisation of f_p for each $p \mid 2d$
7: Compute p-adically automorphous numbers and the corresponding spinor operators for each $p \mid 2d$
8: **if** $\Delta(r)$ is a product of some spinor operators obtained in the above step **then**
9: output 'same spinor genus'
10: **else**
11: output 'different spinor genera'
12: **end if**

suggested an exhaustive search through all rational matrices until a rational equivalence with denominator r relatively prime to $2d$ is found. This would cost complexity at least $e^{O(n^2)}$, which may be reduced significantly using a better method. For Step 8, we can determine whether $\Delta(r)$ is in the spinor operator kernel by applying Gaussian elimination in time poly$(\log_2 d)$ since the number of generators of spinor operator kernel is bounded by $t \leq \log_2(8d)$, as explained above.

5 Spinor Genus Algorithm for Quadratic Forms over Number Fields

In this section, we will investigate the complexity of an algorithm, that was introduced by Benham and Hsia [4], to determine if two quadratic forms over number fields which are in the same genus are in the same spinor genus or not. For the convenience, we discuss it in the lattice setting. This algorithm was implemented in MAGMA (see [11]) but without discussion of its complexity. Let F be an algebraic number field with $\mathcal{O}$ its ring of integers. Assume V is an n-dimensional vector space over F with a non-degenerate quadratic form ϕ and its associated symmetric bilinear form b satisfying $b(v,w) = \frac{1}{2}(\phi(v+w) - \phi(v) - \phi(w))$, and L is a quadratic lattice on V. We assume $n \geq 3$ in the sequel.

Let Ω be the set consisting of all spots on F. For a prime spot $\mathfrak{p} \in \Omega$, define $dL_\mathfrak{p}$, the discriminant of $L_\mathfrak{p} = \mathcal{O}_\mathfrak{p} v_1 + \cdots + \mathcal{O}_\mathfrak{p} v_n$ with respect to the basis $\{v_1, \ldots, v_n\}$, as the determinant of the Gram matrix $A_{L_\mathfrak{p}} = (b(v_i, v_j))_{n\times n}$ when n is even and as half of the determinant when n is odd. We say L is good at $\mathfrak{p}$ (or simply $L_\mathfrak{p}$ is good) if $\phi(L_\mathfrak{p}) \subseteq \mathcal{O}_\mathfrak{p}$ and $dL_\mathfrak{p} \in 2^{-n}\mathfrak{u}_\mathfrak{p}$ where $\mathfrak{u}_\mathfrak{p}$ is the group of units of $F_\mathfrak{p}$. Recall that we say $L_\mathfrak{p}$ is $\mathcal{O}_\mathfrak{p}$-maximal if $\phi(L_\mathfrak{p}) \subseteq \mathcal{O}_\mathfrak{p}$ and if for

every lattice $N_\mathfrak{p}$ with $L_\mathfrak{p} \subseteq N_\mathfrak{p}$ and $\phi(N_\mathfrak{p}) \subseteq \mathcal{O}_\mathfrak{p}$ we have $L_\mathfrak{p} = N_\mathfrak{p}$. The following lemma shows that $L_\mathfrak{p}$ is $\mathcal{O}_\mathfrak{p}$-maximal if $L_\mathfrak{p}$ is good.

Lemma 3. *When L is good at $\mathfrak{p}$, $L_\mathfrak{p}$ is $\mathcal{O}_\mathfrak{p}$-maximal.*

Proof. Let $A_{L_\mathfrak{p}} = (a_{ij})_{n\times n}$ be the Gram matrix of $L_\mathfrak{p}$. Define the scale ideal $\mathfrak{s}L_\mathfrak{p}$ to be the fractional ideal generated by the entries a_{ij} with $1 \le i, j \le n$, and the volume $\mathfrak{v}L_\mathfrak{p}$ to be the fractional ideal generated by $\det A_{L_\mathfrak{p}}$. Remember that the discriminant $dL_\mathfrak{p}$ is $\det A_{L_\mathfrak{p}}$ when n is even and is $\frac{1}{2}\det A_{L_\mathfrak{p}}$ when n is odd. When L is good at $\mathfrak{p}$, $\phi(L_\mathfrak{p}) \subseteq \mathcal{O}_\mathfrak{p}$ and $dL_\mathfrak{p} = 2^{-n}u$ with u a $\mathfrak{p}$-unit. Therefore $\mathfrak{v}L_\mathfrak{p} = 2^{-n}\mathcal{O}_\mathfrak{p}$ when n is even and $\mathfrak{v}L_\mathfrak{p} = 2^{-n+1}\mathcal{O}_\mathfrak{p}$ when n is odd.

When $\mathfrak{p}$ is non-dyadic ($|2|_\mathfrak{p} = 1$), 2 is a $\mathfrak{p}$-unit. We have $L_\mathfrak{p}$ is unimodular since $\mathfrak{s}L_\mathfrak{p} \subseteq \mathcal{O}_\mathfrak{p}$ and $\mathfrak{v}L_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$ (see [27, 82G]). By [27, 82:19], $L_\mathfrak{p}$ is $\mathcal{O}_\mathfrak{p}$-maximal.

Now let $\mathfrak{p}$ be dyadic ($0 < |2|_\mathfrak{p} < 1$). Suppose that there is a lattice $N_\mathfrak{p}$ on $V_\mathfrak{p}$ such that $L_\mathfrak{p} \subseteq N_\mathfrak{p}$ and $\phi(N_\mathfrak{p}) \subseteq \mathcal{O}_\mathfrak{p}$. We want to show that $L_\mathfrak{p} = N_\mathfrak{p}$ by comparing their volumes. When n is even, since $\phi(N_\mathfrak{p}) \subseteq \mathcal{O}_\mathfrak{p}$, we have $\mathfrak{s}N_\mathfrak{p} \subseteq \frac{1}{2}\mathcal{O}_\mathfrak{p}$ and $\mathfrak{v}N_\mathfrak{p} \subseteq (\mathfrak{s}N_\mathfrak{p})^n \subseteq 2^{-n}\mathcal{O}_\mathfrak{p} = \mathfrak{v}L_\mathfrak{p}$. When n is odd, $N_\mathfrak{p} = \langle\alpha\rangle \perp N'_\mathfrak{p}$ with $\alpha \in \mathcal{O}_\mathfrak{p}$. Then $\mathfrak{v}N_\mathfrak{p} = \alpha\mathfrak{v}N'_\mathfrak{p} \subseteq (\mathfrak{s}N'_\mathfrak{p})^{n-1} \subseteq 2^{-n+1}\mathcal{O}_\mathfrak{p} = \mathfrak{v}L_\mathfrak{p}$. Therefore, by [27, 82:11], $N_\mathfrak{p} = L_\mathfrak{p}$ and $L_\mathfrak{p}$ is $\mathcal{O}_\mathfrak{p}$-maximal. □

Suppose $\tilde{L}$ is a lattice on V that is also good at $\mathfrak{p}$, so $L_\mathfrak{p}$ and $\tilde{L}_\mathfrak{p}$ are $\mathcal{O}_\mathfrak{p}$-maximal lattices. By [27, 91:2], there is a local basis $\{e_1, f_1, \ldots, e_t, f_t, z_{2t+1}, \ldots, z_n\}$ for $L_\mathfrak{p}$ satisfying $\phi(e_i) = \phi(f_i) = 0$, $b(e_i, f_j) = \frac{1}{2}\delta_{ij}$, $b(e_i, e_j) = b(f_i, f_j) = 0$ for $i \neq j$, $b(e_i, z_k) = b(f_i, z_k) = 0$, the subspace spanned by $\{z_{2t+1}, \ldots, z_n\}$ is anisotropic, and

$$\tilde{L}_\mathfrak{p} = \mathfrak{p}^{a_1}e_1 + \mathfrak{p}^{-a_1}f_1 + \cdots + \mathfrak{p}^{a_t}e_t + \mathfrak{p}^{-a_t}f_t + \mathcal{O}_\mathfrak{p}z_{2t+1} + \cdots + \mathcal{O}_\mathfrak{p}z_n,$$

where $a_1, \ldots, a_t$ are nonnegative exponents. It follows that

$$[L_\mathfrak{p} : L_\mathfrak{p} \cap \tilde{L}_\mathfrak{p}] = [\tilde{L}_\mathfrak{p} : L_\mathfrak{p} \cap \tilde{L}_\mathfrak{p}] = |\mathcal{O}/\mathfrak{p}|^{a_1+\cdots+a_t}.$$

We define $R(L : \mathfrak{p})$ to be the global graph containing lattices $\tilde{L} \in \mathrm{gen}(L)$ such that $\tilde{L}_\mathfrak{q} = L_\mathfrak{q}$ at all prime spots $\mathfrak{q} \neq \mathfrak{p}$ as vertices. The distance $\mathrm{dist}(L, \tilde{L}, \mathfrak{p})$ between $\tilde{L}$ and L is $r = a_1 + \cdots + a_t$. In particular, two vertices $\tilde{L}$ and L are connected by an edge when $r = 1$ and they are called neighbors. It is known that the vertices of $R(L : \mathfrak{p})$ belong to at most two spinor genera, and two vertices belong to the same spinor genus when r is even. Therefore, all the vertices are in the same spinor genus $\mathrm{spn}^+(L)$ if and only if the neighbor of L is in $\mathrm{spn}^+(L)$.

Let $J_V = \{\Sigma \in \prod_{\mathfrak{q}\in\Omega} O^+(V_\mathfrak{q}) : ||\Sigma_\mathfrak{q}||_\mathfrak{q} = 1 \text{ for almost all } \mathfrak{q} \in \Omega\}$ be the group of split rotations and $J_V^L = \{\Sigma \in J_V : \Sigma L = L\}$ be the set of stabilizers of L. Let $\pi_\mathfrak{p}$ be a fixed prime element of the local field $F_\mathfrak{p}$. Define $\Sigma(\mathfrak{p}) \in J_V$ by setting $\Sigma(\mathfrak{p})_\mathfrak{q}$ to be the identity map for all primes $\mathfrak{q} \neq \mathfrak{p}$ and $\Sigma(\mathfrak{p})_\mathfrak{p} = \tau_{e_1-f_1} \cdot \tau_{e_1-\pi_\mathfrak{p}f_1}$, where τ_w denotes the symmetry with respect to the anisotropic line $F_\mathfrak{p}w$. It is easy to check that the action of $\Sigma(\mathfrak{p})$ does not depend on the choice of $\pi_\mathfrak{p}$. Let $J_F = \{\mathfrak{i} \in \prod_{\mathfrak{q}\in\Omega} F_\mathfrak{q}^\times : |\mathfrak{i}_\mathfrak{q}|_\mathfrak{q} = 1 \text{ for almost all } \mathfrak{q} \in \Omega\}$. Define $j(\mathfrak{p}) \in J_F$ to have 1 at all primes $\mathfrak{q} \neq \mathfrak{p}$ and $\pi_\mathfrak{p}$ at prime $\mathfrak{p}$. Since $L_\mathfrak{p}$ is maximal,

$\theta(O^+(L_\mathfrak{p}))$ contains all the units in $F_\mathfrak{p}$ [27, 91:8] so that $j(\mathfrak{p})$ is well-defined modulo $\theta(J_V^L)$. Moreover, $\theta(\Sigma(\mathfrak{p})) \equiv j(\mathfrak{p}) \bmod \theta(J_V^L)$.

Suppose $L' = \Sigma(\mathfrak{p})L$ is a neighbor of L; then the graph $R(L:\mathfrak{p})$ contains only one spinor genus if and only if $L' \in \mathrm{spn}^+(L)$ if and only if $j(\mathfrak{p}) \in P_D J_F^L$ ([27, 102:7]), where P_D is the subgroup of principal idèles generated by the elements in $D = \theta(O^+(V))$ which equals the set of elements in $F^\times$ that are positive at all real spots $\mathfrak{q}$ at which $V_\mathfrak{q}$ is anisotropic ([27, 101:8]), and $J_F^L = \{\mathfrak{i} \in J_F : \mathfrak{i}_\mathfrak{q} \in \theta(O^+(L_\mathfrak{q}))$ for all prime spots $\mathfrak{q}\}$.

Given a lattice $\tilde{L}$ in the genus of L, based on the above observations, Benham and Hsia designed an algorithm to identify a prime spot $\mathfrak{p}$ such that $L' = \Sigma(\mathfrak{p})L \in \mathrm{spn}^+(\tilde{L})$ is a neighbor of L in the graph $R(L:\mathfrak{p})$. One can determine whether $\tilde{L}$ is in $\mathrm{spn}^+(L)$ by checking if $j(\mathfrak{p}) \in P_D J_F^L$.

Step 1: Compute X and T where X is the set of all real spots on F and T is a finite set of prime spots satisfying

1. $\mathfrak{q} \in T$ for all dyadic prime spots $\mathfrak{q}$;
2. $L_\mathfrak{q}$ is unimodular at all prime spots $\mathfrak{q} \notin T$;
3. $L_\mathfrak{q} = \tilde{L}_\mathfrak{q}$ for all prime spots $\mathfrak{q} \notin T$.

Step 2: For each $\mathfrak{q} \in T$, compute an isometry $\Sigma_\mathfrak{q} \in \mathrm{O}^+(V_\mathfrak{q})$ such that $\tilde{L}_\mathfrak{q} = \Sigma_\mathfrak{q} L_\mathfrak{q}$.

Step 3: For each $\mathfrak{q} \in T$, compute an element $x_\mathfrak{q} \in \mathcal{O}_\mathfrak{q} \cap \theta(\Sigma_\mathfrak{q}) \cdot F_\mathfrak{q}^{\times 2}$ and set $a_\mathfrak{q} = \mathrm{ord}_\mathfrak{q}(x_\mathfrak{q}) + \mathrm{ord}_\mathfrak{q}(4) + 1$.

Step 4: Compute an algebraic integer $c \in \mathcal{O}$ such that c is positive with respect to all $\mathfrak{q} \in X$ and c is congruent to $x_\mathfrak{q} \bmod \mathfrak{q}^{a_\mathfrak{q}}$ for each $\mathfrak{q} \in T$.

Step 5: Write the ideal $(c) = \prod_{\mathfrak{q}\in T} \mathfrak{q}^{k_\mathfrak{q}} \cdot \mathfrak{a}$ where $\mathfrak{a}$ is relatively prime to each $\mathfrak{q}$ in T and define a modulus $\mathfrak{m} = \prod_{\mathfrak{q}\in T} \mathfrak{q}^{a_\mathfrak{q}} \cdot \prod_{\mathfrak{q}\in X} \mathfrak{q}$. Given a fractional ideal $\mathfrak{u} = \mathfrak{b}\mathfrak{c}^{-1}$ where $\mathfrak{b}$ and $\mathfrak{c}$ are integral ideals, $\mathfrak{u}$ is said to be relatively prime to $\mathfrak{q}$ if both $\mathfrak{b}$ and $\mathfrak{c}$ are relatively prime to $\mathfrak{q}$. Let $I_F^\mathfrak{m} := \{$fractional ideals of F that are relatively prime to each $\mathfrak{q} \in T\}$, $F_{\mathfrak{m},1} := \{a \in F^\times : a \equiv 1 \bmod \mathfrak{m}\}$ where $a \equiv 1 \bmod \mathfrak{m}$ means $\mathrm{ord}_\mathfrak{q}(a-1) \geq a_\mathfrak{q}$ for each $\mathfrak{q} \in T$ and $a > 0$ at each $\mathfrak{q} \in X$, and $S_\mathfrak{m} = \{a\mathcal{O} : a \in F_{\mathfrak{m},1}\}$. By a density theorem from class field theory, each ray class in the ray class group $I_F^\mathfrak{m}/S_\mathfrak{m}$ contains infinitely many primes. Compute a prime ideal $\mathfrak{p}$ in the ray class $\mathfrak{a} \cdot S_\mathfrak{m}$. This $\mathfrak{p}$ is the prime spot we are looking for.

Step 6: Determine if $j(\mathfrak{p}) \in P_D J_F^L$.

In the remaining of this section, we would like to restrict our attention to the number fields with class number 1, and study the complexity of this algorithm. Every quadratic lattice is free with a basis $\{v_1, \ldots, v_n\}$ such that $L = \mathcal{O}v_1 + \cdots + \mathcal{O}v_n$, and $dL = \det(b(v_i, v_j))$ is called the discriminant of L with respect to the basis $\{v_1, \ldots, v_n\}$. Moreover, if L is given in the form $\mathfrak{a}_1 w_1 + \cdots + \mathfrak{a}_n w_n$ where $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ are fractional ideals, then $\mathfrak{a}_1^2 \ldots \mathfrak{a}_n^2 \det(b(w_i, w_j)) = dL\mathcal{O}$. We use the same symbol $\mathfrak{q}$ to denote the prime ideal in both $\mathcal{O}$ and $\mathcal{O}_\mathfrak{q}$, and use $\pi_\mathfrak{q}$ to denote their common generator.

Lemma 4. *Suppose $L_\mathfrak{q}$ and $\tilde{L}_\mathfrak{q}$ are maximal lattices, then there is an isometry $\sigma_\mathfrak{q}$ in $O^+(V_\mathfrak{q})$ sending $L_\mathfrak{q}$ to $\tilde{L}_\mathfrak{q}$ and $\theta(\sigma_\mathfrak{q}) = \pi_\mathfrak{q}^{\frac{1}{2}\mathrm{ord}_\mathfrak{q}(d(L\cap\tilde{L})/dL)\mathcal{O}}$.*

Proof. Since $L_\mathfrak{q}$ and $\tilde{L}_\mathfrak{q}$ are maximal lattices, by [27, 91:2] there is a local basis $\{e_1, f_1, \ldots, e_t,\ f_t, z_{2t+1}, \ldots, z_n\}$ for $L_\mathfrak{q}$ satisfying $\phi(e_i) = \phi(f_i) = 0$, $b(e_i, f_j) = \frac{1}{2}\delta_{ij}$, $b(e_i, e_j) = b(f_i, f_j) = 0$ for $i \neq j$, $b(e_i, z_k) = b(f_i, z_k) = 0$, the subspace spanned by $\{z_{2t+1}, \ldots, z_n\}$ is anisotropic, and $\tilde{L}_\mathfrak{q} = \mathfrak{q}^{a_1}e_1 + \mathfrak{q}^{-a_1}f_1 + \cdots + \mathfrak{q}^{a_t}e_t + \mathfrak{q}^{-a_t}f_t + \mathcal{O}_\mathfrak{q}z_{2t+1} + \cdots + \mathcal{O}_\mathfrak{q}z_n$. Define the isometry

$$\sigma_\mathfrak{q} = \tau_{e_1-f_1}\tau_{e_1-\pi_\mathfrak{q}^{a_1}f_1}\cdots\tau_{e_t-f_t}\tau_{e_t-\pi_\mathfrak{q}^{a_t}f_t},$$

then $\sigma_\mathfrak{q}(L_\mathfrak{q}) = \tilde{L}_\mathfrak{q}$ and $\theta(\sigma_\mathfrak{q}) = \pi_\mathfrak{q}^{a_1+\cdots+a_t}$. Note that

$$L_\mathfrak{q} \cap \tilde{L}_\mathfrak{q} = \mathfrak{q}^{a_1}e_1 + \mathcal{O}_\mathfrak{q}f_1 + \cdots + \mathfrak{q}^{a_t}e_t + \mathcal{O}_\mathfrak{q}f_t + \mathcal{O}_\mathfrak{q}z_{2t+1} + \cdots + \mathcal{O}_\mathfrak{q}z_n,$$

and $\mathfrak{q}^{2(a_1+\cdots+a_n)} = (d(L_\mathfrak{q} \cap \tilde{L}_\mathfrak{q})/dL_\mathfrak{q})\mathcal{O}_\mathfrak{q}$. Therefore

$$\theta(\sigma_\mathfrak{q}) = \pi_\mathfrak{q}^{\frac{1}{2}\mathrm{ord}_\mathfrak{q}(d(L_\mathfrak{q}\cap\tilde{L}_\mathfrak{q})/dL_\mathfrak{q})\mathcal{O}_\mathfrak{q}} = \pi_\mathfrak{q}^{\frac{1}{2}\mathrm{ord}_\mathfrak{q}(d(L\cap\tilde{L})/dL)\mathcal{O}}.$$

□

Lemma 5. *Suppose $\tilde{L}$ is in the genus of L. Then $L_\mathfrak{q} = \tilde{L}_\mathfrak{q}$ if and only if $\mathrm{ord}_\mathfrak{q}(d(L \cap \tilde{L})/dL)\mathcal{O} = 0$.*

Proof. Since both L and $\tilde{L}$ are lattices on V, their intersection $L \cap \tilde{L}$ is also a lattice on V. Now, by the Invariant Factors Theorem (Theorem 4), there is a basis $\{v_1, \ldots, v_n\}$ of V such that

$$L = \mathcal{O}v_1 + \cdots + \mathcal{O}v_n \qquad\qquad L \cap \tilde{L} = \mathfrak{a}_1v_1 + \cdots + \mathfrak{a}_nv_n$$

with $\mathfrak{a}_1 \supseteq \cdots \supseteq \mathfrak{a}_n$ integral ideals. Therefore, $L_\mathfrak{q} = \tilde{L}_\mathfrak{q}$ if and only if $L_\mathfrak{q} = L_\mathfrak{q} \cap \tilde{L}_\mathfrak{q}$ if and only if $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ are $\mathcal{O}_\mathfrak{q}$ at $\mathfrak{q}$, i.e., $\mathrm{ord}_\mathfrak{q}(d(L \cap \tilde{L})/dL)\mathcal{O} = 0$. □

Lemma 6. *The finite set T of prime spots in Step 1 can be computed in (quantum) polynomial time.*

Proof. The set T in Step 1 consists of the prime ideals that appear in the factorization of $2dL\mathcal{O}$ or in the factorization of $d((L\cap\tilde{L})/dL)\mathcal{O}$. The basis of $L\cap\tilde{L}$ can be found using Hermite Normal Form in polynomial time, and the factorization of fractional ideals can be obtained in (quantum) polynomial time according to [18, Lemma 4.1]. □

Lemma 7. *The algebraic integer c in Step 4 can be computed in (quantum) polynomial time.*

Proof. Since $\mathcal{O}$ is dense in the set $\mathcal{O}_\mathfrak{q}$, we can choose $x_\mathfrak{q}$ to be an element in $\mathcal{O}$. An algebraic integer c such that $c \equiv x_\mathfrak{q} \mod \mathfrak{q}^{a_\mathfrak{q}}$ can be obtained in (quantum) polynomial time according to [18, Lemma 3.1, Lemma 3.5]. Also, let $q_1, \ldots, q_t$ be the rational prime numbers lying below the prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_t$ in T. We can add a multiple of the product $q_1^{a_{\mathfrak{q}_1}} \ldots q_t^{a_{\mathfrak{q}_t}}$ to c to satisfy the positive conditions at each real spot in X. □

For Steps 2, 3 and 5, there are effective but possibly not efficient methods to compute the solutions. Let B_L and $B_{\tilde{L}}$ be the generating matrix of L and $\tilde{L}$ respectively. Search for a matrix $M \in M_{n\times n}(F)$ with $\det M$ is a unit and whose entries are in $\mathcal{O}_{\mathfrak{q}}$ for each prime spot $\mathfrak{q}$ dividing $2dL\mathcal{O}$ such that $B_L^t B_L = M^t(B_{\tilde{L}}^t B_{\tilde{L}})M$. The existence of such a matrix M can be found in [27, Example 102:4], and we can replace L by the lattice generated by $B_{\tilde{L}}M$ which is in the proper class of L.

Then in Steps 2 and 3, for all primes spots $\mathfrak{q}$ dividing $2dL\mathcal{O}$, since $L_{\mathfrak{q}} = \tilde{L}_{\mathfrak{q}}$, we can choose $\Sigma_{\mathfrak{q}}$ to be the identity map and $\theta(\Sigma_{\mathfrak{q}}) = 1$. For the remaining prime spots $\mathfrak{q} \in T$, both $L_{\mathfrak{q}}$ and $\tilde{L}_{\mathfrak{q}}$ are maximal and $\Sigma_{\mathfrak{q}}$ and its spinor norm can be found in Lemma 4.

For Step 5, one can find a prime ideal $\mathfrak{p}$ in the ray class of $\mathfrak{a}$ by searching through all (finitely many) prime ideals with norm bounded by the constant given in [31] that can be effectively calculated.

6 Spinor Genera of Binary Forms over Number Fields

Many results given above, which appear to frustrate algebraic approaches to solving LIP via computing spinor genera, have the condition $n \geq 3$. However, HAWK uses rank 2 forms, integral over a cyclotomic field. In this section we ask: how does the spinor norm behave in this setting? In Section 7.1 we explain in more detail the connection between our results and the HAWK signature scheme.

Our result relies on the work of Earnest and Estes, who prove in [16] (via [17]) that in the binary setting, two lattices in the same genus lie in the same spinor genus if and only if they are fourth powers (quartic residues) in the class group of some order in the field, when the ring of integers is a PID. Thus if one can compute quartic residues in class groups of non-maximal orders, one could correctly decide the answer to the distinguish LIP problem, when the forms lie in different spinor genera.

There are quantum algorithms to compute the class group of a suborder of any number field efficiently, under GRH [6]. Moreover, deciding quadratic residuosity in the class group can be performed efficiently, given the data from those quantum algorithms; and the same is true for quartic residuosity. The quantum algorithm we will need is:

Theorem 11. *[6, Theorem 1.2] (Class group Computation) Under the Generalized Riemann Hypothesis, there is a quantum algorithm for computing the class group of an order $\mathcal{O}$ in a number field K which runs in polynomial time in the parameters $n = \deg(K)$ and $\log(|\Delta|)$, where Δ is the discriminant of $\mathcal{O}$.*

We note that the above algorithm 'computes the class group' by computing a generating set of prime ideals together with the relations between them.

We now explain in more detail the result of Earnest and Estes. In the following, we consider regular binary quadratic spaces (V, ϕ) over a number field F

and anisotropic binary quadratic forms over the ring of integers $\mathcal{O}_F$. These correspond to lattices of rank 2 over that ring of integers, contained in V. We may fix a basis such that this vector space is in fact isomorphic to a field extension of degree 2, when (V, ϕ) is anisotropic. We then have $V \cong F(\sqrt{-d})$ for some d, and we write $\mathcal{O}_V$ for the ring of integers of $F(\sqrt{-d})$. There is then an involution * on V fixing F such that $\phi(x) = xx^*$ for any $x \in V$. For more details see [17].

The following two results combine to imply that two lattices $L_1, L_2 \subset V$ in the same genus are in the same proper spinor genus if and only if $L_1 L_2^{-1}$ is a quartic residue in the class group of the left order of L_2 in V. Recall that the left order is defined as $\mathcal{O}_l(L_2) := \{x \in V : xL_2 \subset L_2\} \subset V$, and any lattice is a left ideal in its left order.

Proposition 2. *[17, Proposition 2.3] A necessary and sufficient condition that L_1 be in $\mathrm{cls}^+(L_2)$ (resp. $\mathrm{spn}^+(L_2)$ or $\mathrm{gen}(L_2)$) is that $L_1 L_2^{-1}$ be in $\mathrm{cls}^+(\mathcal{O}_l(L_2))$ (resp. $\mathrm{spn}^+(\mathcal{O}_l(L_2))$ or $\mathrm{gen}(\mathcal{O}_l(L_2))$).*

For any (possibly non-maximal) $\mathcal{O}_F$-order $\mathcal{O} \subset V$, denote the group of invertible fractional ideals of $\mathcal{O}$ by $\mathcal{I}(\mathcal{O})$, and the subgroup of principal invertible fractional ideals by $\mathcal{P}(\mathcal{O})$. Set

$$\mathcal{H}(\mathcal{O}) = \mathrm{gen}(\mathcal{O}) / \mathrm{spn}^+(\mathcal{O}),$$

and

$$\mathcal{C}(\mathcal{O}) = \mathcal{I}(\mathcal{O}) / \mathcal{P}(\mathcal{O}).$$

Then

Corollary 1. *[16, §4] Suppose F is a number field and $\mathcal{O}_F$ is a PID. Let $\mathcal{O}$ be a degree 2 order over $\mathcal{O}_F$. Then we have $\mathcal{H}(\mathcal{O}) \cong \mathcal{C}(\mathcal{O})^2 / \mathcal{C}(\mathcal{O})^4$.*

A consequence of this is that we find $\mathrm{spn}^+(\mathcal{O}) / \mathrm{cls}^+(\mathcal{O}) \cong \mathcal{C}(\mathcal{O})^4$. Thus we can prove

Theorem 12. *Let F be a number field and suppose $\mathcal{O}_F$ is a PID. Let f and g be two anisotropic binary quadratic forms, integral over $\mathcal{O}_F$, lying in the same genus. Let V $(= F \cdot L_f = F \cdot L_g)$ be the rank 2 quadratic space containing L_f and L_g. Then if $L_f \cdot L_g^{-1}$ generates an ideal coprime to the conductor of $\mathcal{O}_l(L_g)$ in $\mathcal{O}_V$, there is a quantum polynomial time algorithm to decide if $f \in \mathrm{spn}^+(g)$.*

Proof. Let the corresponding lattices to f, g be denoted by L_f, L_g. Since f, g are anisotropic, V is anisotropic and hence isomorphic to a quadratic field extension of F; identify V with this extension. Begin by computing a basis of the left order of L_g in V, $\mathcal{O}_l(L_g)$. Next, use Theorem 11 to compute the class group structure, obtaining a generating set of prime ideals in the class group of $\mathcal{O}_l(L_g)$ in quantum polynomial time, together with their defining relations. This system of relations forms a lattice Λ, and we obtain an isomorphism $\mathcal{C}(\mathcal{O}_l(L_g)) \to \mathbb{Z}^n / \Lambda$ by writing an element of $\mathcal{C}(\mathcal{O}_l(L_g))$ as a product of powers of prime ideals from our generating set, and mapping to the vector of exponents (modulo the lattice of relations). That is, for $I \in \mathcal{C}(\mathcal{O}_l(L_g))$, we write $I = \prod_{i=1}^n \mathfrak{p}_i^{e_i}$ and then send

$I \mapsto (e_1, ..., e_n) + \Lambda$.

Since $\mathbb{Z}^n/\Lambda$ is an abelian group, we can then consider $\mathcal{C}(\mathcal{O}_l(L_g)) \cong \oplus_i \mathbb{Z}/d_i\mathbb{Z}$, and the image of $L_f \cdot L_g^{-1}$ in $\oplus_i \mathbb{Z}/d_i\mathbb{Z}$ for some integers d_i, where the factors d_i are obtained by the algorithm of Theorem 11. Moreover, the algorithm outputs a list of vectors $\overline{g}_i$ of order d_i which form a basis of $\mathbb{Z}^n/\Lambda \cong \oplus_i \mathbb{Z}/d_i\mathbb{Z}$ [9, §6.5.4].

If $\mathcal{O}_l(L_g)$ is a maximal order or more generally if $L_f \cdot L_g^{-1}$ generates an ideal coprime to the conductor of $\mathcal{O}_l(L_g)$ in $\mathcal{O}_V$, this can be done by factorising $L_f \cdot L_g^{-1}$ into a product of prime ideals contained in our generating set, and then reducing modulo the relations between the prime ideals in the class group obtained by the algorithm of Theorem 11. We then map $L_f \cdot L_g^{-1} \mapsto (f_1, ..., f_n) + \Lambda$ for some exponents f_i.

Testing such an element for quartic residuosity can then be done efficiently as follows: we may take the basis $\overline{g}_1, ..., \overline{g}_n$ and express $(f_1, ..., f_n) = \sum_i \lambda_i \overline{g}_i$ for some coefficients $\lambda_i \in \mathbb{Z}/d_i\mathbb{Z}$, $i = 1, ..., n$; thus $f_j = \sum_i \lambda_i \overline{g}_{i_j}$. We then express the above as a matrix-vector equation: $(f_1, ..., f_n)^T = G \cdot \lambda$ where G is the matrix with ith column $\overline{g}_i^T$ and λ is a vector with ith entry λ_i. We then compute $G^{-1} \cdot (f_1, ..., f_n)^T = \lambda$; if $\lambda_i = 4\gamma_i \bmod d_i$ for some $\gamma_i \in \mathbb{Z}/d_i\mathbb{Z}$ and for all $i = 1, ..., n$, we conclude that $L_f \cdot L_g^{-1}$ is a quartic residue in the class group.

Finally, if $L_f \cdot L_g^{-1}$ is a quartic residue in $\mathcal{C}(\mathcal{O}_l(L_g))$, then $f \in \mathrm{spn}^+(g)$ by Corollary 1; otherwise, $f \notin \mathrm{spn}^+(g)$. □

Algorithm 3: Quantum Algorithm for Spinor Genus of Binary Forms

Input: Quadratic forms f and g in the same genus
Output: Answer
1: Compute basis of $\mathcal{O}_l(L_g)$
2: $(\{\mathfrak{p}_1, ..., \mathfrak{p}_n\}, \Lambda, \{d_1, ..., d_n\}, \{\overline{g}_1, ..., \overline{g}_n\}) \leftarrow$ Algorithm of Theorem 11
3: $L_f \cdot L_g^{-1} = \prod \mathfrak{p}_i^{f_i}$
4: $(f_1', ..., f_n') := (f_1, ..., f_n) \bmod \Lambda$
5: Compute $G^{-1} \cdot (f_1', ..., f_n')^T$
6: **if** $G^{-1} \cdot (f_1', ..., f_n')^T = \mathbf{0} \bmod 4$ **then**
7: Output 'Yes'
8: **else**
9: Output 'No'
10: **end if**

We make the following remark:

Corollary 2. *Let F be a number field and suppose $\mathcal{O}_F$ is a PID. Let f and g be two anisotropic binary quadratic forms, integral over $\mathcal{O}_F$, in the same genus. Let V be the rank 2 quadratic space containing L_f and L_g. Suppose $L_f \cdot L_g^{-1}$ generate an ideal coprime to the conductor of $\mathcal{O}_l(L_g)$ in $\mathcal{O}_V$, and* $\gcd(|\mathcal{C}(\mathcal{O}_l(L_g))|, 2) = 1$. *Then $f \in \mathrm{spn}^+(g)$.*

Proof. When $|\mathcal{C}(\mathcal{O}_l(L_g))|$ is odd, then none of the d_i obtained in the course of the algorithm implicit in the proof of Theorem 6 are even. Then in the penultimate

paragraph of the proof, when one computes $G^{-1} \cdot (f_1, ..., f_n)^T = \lambda$, and checks if $\lambda_i = 4\gamma_i \bmod d_i$ for some $\gamma_i \in \mathbb{Z}/d_i\mathbb{Z}$ and for all $i = 1, ..., n$, we must find that there always exist such $\gamma_i \bmod d_i$, since $\gcd(4, d_i) = 1$. Thus in this setting the two forms f, g always lie in the same spinor genus. □

We note that there are many examples of number fields with odd class numbers which may be considered relevant to LIP in cryptography: for instance, the power-of-two cyclotomic fields $\mathbb{Q}(\zeta_{64})$, $\mathbb{Q}(\zeta_{128})$, and $\mathbb{Q}(\zeta_{256})$ all have odd class number, being 17, 359057, and 10449592865393414737 respectively (see [22],[25],[29]). However, many cyclotomic fields have even class number, such as $\mathbb{Q}(\zeta_{130})$, which has class number 64. We conclude from this that if one is choosing parameters for LIP-based schemes over number fields, one must choose the number field carefully to avoid distinguishing attacks as detailed in the section below.

We also derive two corollaries regarding cyclotomic fields:

Corollary 3. *Let $F = \mathbb{Q}(\zeta_n)$ be a cyclotomic field and*

$$n \in \{1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84\}$$

Let f and g be two anisotropic binary quadratic forms, integral over $\mathcal{O}_F$, in the same genus. Let V be the rank 2 quadratic space containing L_f and L_g. Then if $L_f \cdot L_g^{-1}$ generates an ideal coprime to the conductor of $\mathcal{O}_l(L_g)$ in $\mathcal{O}_V$, there is a quantum polynomial time algorithm to decide if $f \in \mathrm{spn}^+(g)$.

Proof. [29, Theorem 11.1] states that the cyclotomic fields with n as in the corollary statement are all the cyclotomic fields with class number equal to one. We may then apply the theorem for binary integral anisotropic quadratic forms over such rings of integers. □

Corollary 4. *Let F be the maximal totally real subfield of $\mathbb{Q}(\zeta_n)$ and $n \in S := \{4, 8, 16, 32, 64, 128, 256\}$ (and assuming GRH, $n \in S \cup \{512\}$). Then there is a quantum polynomial time algorithm to decide if $f \in \mathrm{spn}^+(g)$.*

Proof. [25, Theorem 2.1] states that the cyclotomic fields with n as in the corollary statement are all the cyclotomic fields for which we know unconditionally (and conditionally for $n = 512$) that the maximal real subfield has class number equal to one. We may then apply the theorem for binary integral anisotropic quadratic forms over such rings of integers. □

7 Application to Distinguish LIP

We now apply the theory of the previous sections to the lattice isomorphism problem. We begin by defining these problems. Denote the real orthogonal group in n dimensions by $O_n(\mathbb{R})$.

Definition 5. (search LIP, lattices) Given two isometric lattices $L_1, L_2 \subset \mathbb{R}^n$, find an orthogonal transformation $O \in O_n(\mathbb{R})$ such that $L_2 = O \cdot L_1$.

We redefine this in terms of quadratic forms:

Definition 6. (search LIP, quadratic forms) Given two positive definite integral quadratic forms Q_1, Q_2 in the same equivalence class, find a unimodular $U \in GL_n(\mathbb{Z})$ such that $Q_2 = U^t Q_1 U$.

There is a distinguishing variant of this problem:

Definition 7. (distinguish LIP, quadratic forms) Given two positive definite integral quadratic forms Q_0, Q_1, the distinguish LIP problem Δ-LIP is, given any quadratic form $Q' \in [Q_b]$ for $b \in \{0, 1\}$ a uniform random bit, to find b.

And a decision variant:

Definition 8. Given positive definite integral quadratic form Q, the decision LIP problem dLIP^Q is, given any Q', to decide if $Q' \in [Q]$ or not.

As discussed in [15], for Δ-LIP to be hard Q_0 and Q_1 must be equivalent over $\mathbb{Q}, \mathbb{R}, \mathbb{Q}_p$, and $\mathbb{Z}_p$ for all p, as well as the forms to agree on any other computable invariant. However, that paper did not discuss the spinor genus of the forms; we fill in that gap in this section.

We outline the immediate consequence of Section 6 for LIP over number fields. Suppose in the Δ-LIP experiment, Q_0 and Q_1 are integral binary quadratic forms over the ring of integers of a number field which is a PID, lying in the same genus (and that the implicit quadratic space is anisotropic). Then suppose we are given Q' which lies in either $[Q_0]$ or $[Q_1]$. We run the algorithm implicit in the proof of Theorem 12 on the pairs (Q', Q_0), (Q', Q_1). If the spinor genus has not been accounted for and the forms Q_0, Q_1 lie in different spinor genera within the same genus, we may answer Δ-LIP correctly in polynomial time by ruling out the form lying in the wrong spinor genus, since Q' lies in the same spinor genus as Q_b.

Similarly, in the dLIP^Q experiment, if Q' and Q lie in the same genus but in distinct spinor genera, in the event that the forms not only lie in distinct equivalence classes but also distinct spinor genera, we may detect this and correctly answer 'No'.

7.1 Implications for the Schemes of [15] and [14]

In [15], the authors gave a KEM and a signature scheme, both having their hardness founded on distinguish LIP. These schemes were designed for integral forms of rank n ($\gg 5$) and we conclude from the analysis of Section 3.3 that, if a 'random' quadratic form of determinant p^m has its Jordan p-symbol uniformly distributed among possible Jordan p-symbols, then with only negligible probability do two such forms lie in a genus which splits into multiple spinor genera.

However, our work does have consequences for structured cases of these LIP instances. Moving from forms over the rational integers of rank $n = 2m$ to binary quadratic forms over the ring of integers of a number field of degree m yields forms of the same overall rank, yet would introduce structure into the

LIP instances which makes them vulnerable to our Theorem 12. We thus caution against the use of such structured LIP instances in cryptography.

In HAWK [14], the authors gave a signature scheme, which was later submitted to the first round of NIST's additional post-quantum standardisation process for digital signatures. This scheme was designed for rank two forms over the ring of integers of cyclotomic fields of power-of-two conductor. These correspond to rank two modules over such rings. At first sight, it might seem that our result affects the security of HAWK. However, firstly, these rings of integers are not PIDs, so our theorem does not apply; secondly, our result applies to distinguish LIP, whereas the security of HAWK is based on a search problem; and thirdly, HAWK is based on Hermitian forms, which we do not consider. To explain this last point, we give a brief overview of HAWK which illuminates the differences to the notions studied in this work, following the notation of [26].

Let K be an algebraic number field of degree n. Then there are n embeddings $\sigma_i : K \hookrightarrow \mathbb{C}$. We define the canonical embedding of K as

$$\sigma_K : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2}$$

defined by

$$x \mapsto (\sigma_1(x), ..., \sigma_n(x))$$

Here $\operatorname{im} \sigma_K \subset H := \{(x_1, ..., x_n) \in \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2} : x_{r_1+r_2+j} = \overline{x_{r_1+j}}, 1 \leq j \leq r_2\}$. This map is extended to vectors over K componentwise. For every module $\mathcal{M} \subset K^\ell$ of finite rank over a Dedekind domain $R \subset K$, there exist ideals I_k of R and linearly independent vectors b_k of K^ℓ such that $\mathcal{M} = \sum_{k=1}^{m} I_k \cdot b_k$. Then $[(I_k)_k, (b_k)_k]$ is a *pseudo-basis* of $\mathcal{M}$. Write $K_\mathbb{R} = K \otimes \mathbb{R}$. Then a *module lattice* in $\sigma_K(K_\mathbb{R})^\ell$ for some $\ell > 0$ is given by the embedding of $\mathcal{M}$ under σ_K.

Let $U_n(K_\mathbb{R})$ denote the $n \times n$ unitary matrices with entries in $K_\mathbb{R}$, that is, matrices $A \in M_n(K_\mathbb{R})$ such that $A^{-1} = \overline{A}^T$, where $\bar{\cdot}$ is complex conjugation. We then say that two module lattices $\mathcal{M}_1, \mathcal{M}_2 \subset \sigma_K(K_\mathbb{R})^\ell$ are isomorphic if there exists $U \in U_\ell(K_\mathbb{R})$ such that $\mathcal{M}_2 = U\mathcal{M}_1$. The module LIP problem is, given two such module lattices, to find such a U.

There is a corresponding notion of quadratic forms; these are Hermitian forms, defined as follows. A matrix A in $M_n(K_\mathbb{R})$ is a Hermitian form if $\overline{A}^T = A$. Such a form is positive definite when $\phi_A(x) = \overline{x}^T Ax > 0$ for all $x \in K_\mathbb{R}^n$ with entries which do not embed to 0.

We call K totally real if the image of every embedding lies properly in $\mathbb{R}$. Then $U_m(K_\mathbb{R})$ is the set of matrices A such that $A^{-1} = A^T$, since complex conjugation acts trivially. Then isomorphism of module lattices corresponds to our above definitions of equivalence of lattices, and our results may apply to such problems. However, this is the very setting in which [26] solved the binary module LIP problem.

In the case when K is not totally real, we use a different notion of equivalence of lattices to HAWK (since we do not define equivalence by the *conjugate* transpose above). Thus our results do not affect HAWK. However, we leave it as an open problem to see if the spinor genus can be efficiently computed for integral binary Hermitian forms over number fields.

Acknowledgements

This work was supported in part by the Engineering and Physical Sciences Research Council (EPSRC) [grant numbers EP/X037010/1 and EP/Y037243/1]. The authors would like to thank Dr. Fuchun Lin for helpful discussions. The second author was also partially supported by the Texas A&M University-San Antonio 2024 Research Council Grant, and extends her thanks to the Department of Electrical and Electronic Engineering at Imperial College London for their hospitality and financial support during her summer visits.

References

[1] M. Ajtai. "Generating Hard Instances of Lattice Problems". In: *Electron. Colloquium Comput. Complex.* TR96 (1996). DOI: 10.1145/237814.237838.

[2] M. Ajtai and C. Dwork. "A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence". In: *STOC 97*. Association for Computing Machinery, 1997, 284–293. DOI: 10.1145/258533.258604.

[3] G.E. Andrews and K. Eriksson. *Integer Partitions*. Cambridge University Press, 2004. ISBN: 9780521600903.

[4] J.W. Benham and J.S. Hsia. "Spinor equivalence of quadratic forms". In: *Journal of Number Theory* 17.3 (1983), pp. 337–342. DOI: https://doi.org/10.1016/0022-314X(83)90051-3.

[5] H. Bennett, D. Dadush, and N. Stephens-Davidowitz. "On the Lattice Distortion Problem". In: *ESA 2016*. Ed. by P. Sankowski and C. Zaroliagis. Vol. 57. LIPIcs. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2016. DOI: 10.4230/LIPIcs.ESA.2016.9.

[6] J.-F. Biasse and F. Song. "Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields". In: SODA '16. Society for Industrial and Applied Mathematics, 2016, 893–902.

[7] P. Bruin, L. Ducas, and S. Gibbons. "Genus distribution of random q-ary lattices". In: *NuTMiC 2021*. Vol. 126. Banach Center Publications, Jan. 2023, pp. 137–159. DOI: 10.4064/bc126-9.

[8] J.W.S. Cassels. *Rational Quadratic Forms*. Dover Books on Mathematics. Dover Publications, 2008. ISBN: 9780486466705.

[9] H. Cohen. *A Course in Computational Algebraic Number Theory*. Graduate Texts in Mathematics. Springer Berlin Heidelberg, 2013. ISBN: 9783662029459.

[10] H. Cohen, G. Frey, R. M. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren. "Handbook of Elliptic and Hyperelliptic Curve Cryptography". In: ed. by K. Rosen. Discrete Mathematics and its Applciations. Chapman and Hall/CRC, 2005.

[11] School of Mathematics Computational Algebra Group and University of Sydney Statistics. *Genera and Spinor Genera. MAGMA documentation*. Accessed 24/05/2024. URL: https://magma.maths.usyd.edu.au/magma/handbook/text/339.

[12] J. Conway and N. Sloane. *Sphere Packings, Lattices and Groups*. Vol. 290. Jan. 1988. ISBN: 978-1-4757-2018-1. DOI: 10.1007/978-1-4757-2016-7.

[13] L. Ducas and S. Gibbons. "Hull Attacks on the Lattice Isomorphism Problem". In: *PKC 2023*. Ed. by A. Boldyreva and V. Kolesnikov. Vol. 13940. LNCS. Springer Nature Switzerland, 2023, pp. 177–204. DOI: 10.1007/978-3-031-31368-4_7.

[14] L. Ducas, E. W. Postlethwaite, L. N. Pulles, and W. van Woerden. "Hawk: Module LIP Makes Lattice Signatures Fast, Compact And Simple". In: *ASIACRYPT 2022*. Vol. 13794. LNCS. Springer-Verlag, 2023, 65–94. DOI: 10.1007/978-3-031-22972-5_3.

[15] L. Ducas and W. van Woerden. "On the Lattice Isomorphism Problem, Quadratic Forms, Remarkable Lattices, and Cryptography". In: *EUROCRYPT 2022*. Ed. by O. Dunkelman and S. Dziembowski. Vol. 13277. LNCS. Springer International Publishing, pp. 643–673. DOI: 10.1007/978-3-031-07082-2_23.

[16] A. G. Earnest and D. R. Estes. "An algebraic approach to the growth of class numbers of binary quadratic lattices". In: *Mathematika* 28.2 (1981), pp. 160–168. DOI: https://doi.org/10.1112/S0025579300010214.

[17] A. G. Earnest and D. R. Estes. "Class Groups in the Genus and Spinor Genus of Binary Quadratic Lattices". In: *Proceedings of the London Mathematical Society* s3-40.1 (1980), pp. 40–52. DOI: https://doi.org/10.1112/plms/s3-40.1.40.

[18] K. Eisenträger and S. Hallgren. "Algorithms for ray class groups and Hilbert class fields". In: *Proceedings of the Twenty-First Annual ACM-SIAM Symposium on Discrete Algorithms* (2010), 471–483.

[19] D. R. Estes and G. Pall. "Spinor genera of binary quadratic forms". In: *Journal of Number Theory* 5.6 (1973), pp. 421–432. DOI: 10.1016/0022-314X(73)90012-7.

[20] I. Haviv and O. Regev. "On the Lattice Isomorphism Problem". In: *SODA 2014*, pp. 391–404. DOI: 10.1137/1.9781611973402.29.

[21] J. Hoffstein, J. Pipher, and J. Silverman. "NTRU: A Ring-Based Public Key Cryptosystem". In: *ANTS 1998*. Vol. 1423. LNCS. Springer, 1998, 267–288.

[22] OEIS Foundation Inc. *Relative class number h^- of cyclotomic field $\mathbb{Q}(\zeta_n)$. Entry A061653 in The On-Line Encyclopedia of Integer Sequences*. Accessed 21/05/2024. URL: https://oeis.org/A061653.

[23] K. Jiang, A. Wang, H. Luo, G. Liu, Y. Yu, and X. Wang. "Exploiting the Symmetry of $\mathbb{Z}^n$: Randomization and the Automorphism Problem". In: *ASIACRYPT 2023*. Ed. by J. Guo and R. Steinfeld. Vol. 14441. LNCS. Springer Nature Singapore, 2023, pp. 167–200. DOI: 10.1007/978-981-99-8730-6_6.

[24] D. Marcus. *Number Fields*. Universitext. Springer-Verlag, 1977. ISBN: 9783319902326.

[25] J. Miller. "Class numbers of totally real fields and applications to the Weber class number problem". In: *Acta Arithmetica* 164 (May 2014). DOI: 10.4064/aa164-4-4.

[26] G. Mureau, A. Pellet-Mary, G. Pliatsok, and A. Wallet. "Cryptanalysis of Rank-2 Module-LIP in Totally Real Number Fields". In: *EUROCRYPT 2024*. Ed. by M. Joye and G. Leander. Vol. 14657. LNCS. Springer Nature Switzerland, 2024, pp. 226–255.

[27] O.T. O'Meara. *Introduction to Quadratic Forms*. Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 2013. ISBN: 9783662419229.

[28] O. Regev. "On lattices, learning with errors, random linear codes, and cryptography". In: *J. of the ACM* 56 (6 2009). DOI: 10.1145/1568318.

[29] L. C. Washington. *Introduction to Cyclotomic Fields*. Graduate Texts in Mathematics. Springer New York, 2012. ISBN: 9781461219347.

[30] G.L. Watson. *Integral Quadratic Forms*. Cambridge University Press, 1960. ISBN: 9780521091817.

[31] A. R. Weiss. "The least prime ideal". In: *J. Reine Angew. Math.* 338 (1983), 56–94.