

COMPUTING HILBERT MODULAR FORMS AS ORTHOGONAL MODULAR FORMS

JEFFERY HEIN, GONZALO TORNARÍA, AND JOHN VOIGHT

ABSTRACT. We show how to efficiently compute Hilbert modular forms as orthogonal modular forms, generalizing and expanding upon the method of Birch.

CONTENTS

1. Introduction	2
2. Overview in the classical case	8
3. Algebraic modular forms	15
4. Hilbert modular forms as quaternionic modular forms	18
5. Ternary quadratic forms and the even Clifford algebra	26
6. The radical character	32
7. Newform theory for orthogonal modular forms	36
8. Orthogonal algorithms	37
9. Implementation and examples	42
Appendix A. A functorial inverse to the even Clifford map	43
References	55

1. INTRODUCTION

Motivation. Algorithms for the efficient computation of classical modular forms have applications in many areas in mathematics, and consequently their study and implementation remains a topic of enduring interest [BBB+21]. In 1991, Birch [Bir91] provided such an algorithm based on the Hecke action on classes of ternary quadratic forms. Of his method, Birch says [Bir91, p. 204, p. 191]:

[T]here is a great deal of interesting information to be calculated; since the program is very fast, it is possible for anyone who owns it to generate interesting numbers much faster than it is possible to read them. ...

[However,] this attempt ... has so far failed in two ways: first, it usually gives only half the information needed, and, second, when the level is not square-free it gives even less information. At least the program is very fast!

Birch's algorithm computes the *Anzahlmatrizen* of Eichler [Eic74, §17], which were studied in their relation to Brandt matrices by Ponomarev [Pon81] and Schulze-Pillot [SP86, §2, Lemma 1].

Birch's approach was first extended by Tornaría [Tor05] in his PhD thesis, where the notion of equivalence of quadratic lattices is refined to the notion of Θ -equivalence. In this way, the Hecke module is enlarged to obtain the missing information in the squarefree case, although there is no statement or proof of what eigenforms are constructed in general. In his PhD thesis, Hein [Hei16] generalized Birch's construction to work over a

totally real field and interpreted the modular forms obtained using the construction of the even Clifford algebra.

In this paper, we combine these approaches and exhibit an algorithm that simultaneously addresses both of Birch's issues, generalizes to Hilbert modular forms, and is still very fast: it gives as output all Hilbert modular forms of even weight and trivial character *except* in the case where the totally real base field has odd degree and the level is a square.

Results. Most of the effort in this paper is theoretical, but we begin with the motivating and recognizable algorithmic application. We consider the space of Hilbert cuspforms $S_k(\widehat{\Gamma}_0(\mathfrak{N}))$ with trivial central character, specified by:

- a *base field*, a totally real field F with ring of integers $R := \mathbb{Z}_F$;
- an even *weight*, a vector $k = (k_v)_{v|\infty} \in (2\mathbb{Z}_{\geq 1})^{[F:\mathbb{Q}]}$; and
- a *level*, a nonzero ideal $\mathfrak{N} \subseteq R$.

We abbreviate $|k| := \sum_v k_v$. For full definitions, see [section 4](#).

The space $S_k(\widehat{\Gamma}_0(\mathfrak{N}))$ comes equipped with an action by Hecke operators $T_{\mathfrak{n}}$ indexed by nonzero ideals $\mathfrak{n} \subseteq \mathbb{Z}_F$ with \mathfrak{n} coprime to \mathfrak{N} . The Hecke operators act semisimply and pairwise commute. The space $S_k(\widehat{\Gamma}_0(\mathfrak{N}))$ further comes equipped with degeneracy operators $S_k(\widehat{\Gamma}_0(\mathfrak{N}/\mathfrak{p})) \rightrightarrows S_k(\widehat{\Gamma}_0(\mathfrak{N}))$ for all primes $\mathfrak{p} \mid \mathfrak{N}$, commuting with the Hecke operators. Let $S_k^{\text{new}}(\widehat{\Gamma}_0(\mathfrak{N}))$ be the orthogonal complement of the images of these operators under the Petersson inner product, inheriting a Hecke action. The space $S_k^{\text{new}}(\widehat{\Gamma}_0(\mathfrak{N}))$ is furthermore equipped with Atkin–Lehner involutions $W_{\mathfrak{q}}$ for each prime power divisor $\mathfrak{q} = \mathfrak{p}^e \parallel \mathfrak{N}$, again commuting with the Hecke operators by the theory of newforms. For a *sign vector* $\varepsilon \in \prod_{\mathfrak{p}|\mathfrak{N}} \{\pm 1\}$, let

$$(1.1) \quad S_k^{\text{new}}(\widehat{\Gamma}_0(\mathfrak{N}))^\varepsilon := \{f \in S_k^{\text{new}}(\widehat{\Gamma}_0(\mathfrak{N})) : W_{\mathfrak{q}}f = \varepsilon_{\mathfrak{p}}f\}$$

be the subspace of forms with Atkin–Lehner eigenvalues matching the signs in ε . Then

$$(1.2) \quad S_k^{\text{new}}(\widehat{\Gamma}_0(\mathfrak{N})) = \bigoplus_{\varepsilon} S_k^{\text{new}}(\widehat{\Gamma}_0(\mathfrak{N}))^\varepsilon.$$

Our main algorithmic result is as follows.

Theorem 1.3. *There exists an explicit algorithm that, given as input*

*a base field F , an even weight k , and a factored level $\mathfrak{N} = \prod_{i=1}^r \mathfrak{p}_i^{e_i}$
such that $[F:\mathbb{Q}]$ is even or \mathfrak{N} is nonsquare,
and a sign vector ε ,*

computes as output the new space $S_k^{\text{new}}(\widehat{\Gamma}_0(\mathfrak{N}))^\varepsilon$ as a Hecke module.

If F and \mathfrak{N} are fixed, then this algorithm takes $\widetilde{O}(d^2 \text{Nm}(\mathfrak{p}))$ bit operations to compute the Hecke operator $T_{\mathfrak{p}}$, where $d := \dim_{\mathbb{C}} S_k^{\text{new}}(\widehat{\Gamma}_0(\mathfrak{N}))^\varepsilon$.

To compute $S_k^{\text{new}}(\widehat{\Gamma}_0(\mathfrak{N}))^\varepsilon$ as a Hecke module, we mean to return for each ideal \mathfrak{n} coprime to \mathfrak{N} a matrix $[T_{\mathfrak{n}}]$ representing the action of the Hecke operator $T_{\mathfrak{n}}$ (with respect to a consistent choice of basis for the space).

At least for $F = \mathbb{Q}$ [\[Mar18\]](#) (and likely also true more generally), the Atkin–Lehner operators cut up the space of newforms into subspaces of approximately the same size, giving the expectation $\dim_{\mathbb{C}} S_k^{\text{new}}(\widehat{\Gamma}_0(\mathfrak{N}))^\varepsilon \asymp 2^{-r} \text{Nm}(\mathfrak{N})^{|k-1|}$ as $\text{Nm}(\mathfrak{N}) \rightarrow \infty$ by the mass formula. After a precomputation (to set up the lattice), the running time becomes $\widetilde{O}(d \text{Nm}(\mathfrak{p}))$, so approximately linear in the dimension. To compute the systems of Hecke

eigenvalues on $S_k^{\text{new}}(\widehat{\Gamma}_0(\mathfrak{N}))^\varepsilon$, we could continue with techniques from linear algebra—our setup is especially well suited for this, as the matrices we produce are sparse.

The algorithm provided in Equation (1.3) uses orthogonal modular forms on a ternary quadratic space and passing through quaternionic modular forms. We succeed in computing the forms that Birch did not find by adding a character: for each sign vector ε , we define a *radical character* ν_ε in (6.3), and we consider orthogonal modular forms that transform according to this character.

To explain this in more detail, let V be a totally positive definite ternary quadratic space over F . Attached to V is its even Clifford algebra $B := \text{Clf}^0(V)$; let \mathfrak{D} be its discriminant, the product of the ramified primes. Let $\Lambda \subset V$ be an integral R -lattice such that $\Lambda^\#/\Lambda$ is cyclic. Then the even Clifford algebra $O := \text{Clf}^0(\Lambda) \subseteq B$ of Λ is a locally residually unramified quaternion R -order.

Our main result, underlying Equation (1.3) (proven as Equation (7.5)), is the following.

Theorem 1.4. *For each sign vector ε , there is a Hecke-equivariant bijection*

$$(1.5) \quad S_k(\text{SO}(\widehat{\Lambda}), \nu_\varepsilon) \xrightarrow{\sim} S_k(\widehat{O})^\varepsilon$$

between the space of cuspidal orthogonal modular forms for Λ with weight k and character ν_ε and the space of quaternionic cusp forms on O of weight k with Atkin–Lehner eigenvalues ε .

When O is a suitable quaternion order, the Eichler–Shimizu–Jacquet–Langlands correspondence (recalled in Equation (4.10)) then produces a final Hecke-equivariant bijection between the space of quaternionic forms and a space of Hilbert cusp forms. (Restricting orders in this way does not lose any newforms, and it keeps the newform theory quite simple.)

Discussion. The main result in Equation (1.4) could also be understood through analytic means via theta series or a Shimura correspondence for Hilbert modular forms. This method of proof is quite challenging, requiring half-integral weight forms and twists to ensure nonvanishing. By contrast, the proof using the even Clifford algebra is completely transparent—there is a natural bijection between the class set of Λ and the type set of its even Clifford order O , and so the corresponding spaces of functions taking values in a representation are canonically isomorphic, equivariant with respect to the Hecke operators. To highlight this simplicity, we present an overview of the proof in the case of $F = \mathbb{Q}$ in 2. A key innovation in this paper is the use of the radical character allowing us to recover all forms, not just those invariant by the Atkin–Lehner operators.

There are also other methods for computing with Hilbert modular forms, including quaternionic methods with either a definite or indefinite quaternion algebra: for an overview, see Dembélé–Voight [DV13]. However, there are two key advantages of the approach using ternary orthogonal modular forms, both implying that we may work in smaller-dimensional spaces and therefore save substantially in the cost of linear algebra operations.

- (1) We work directly in the space with trivial central character, even when F has nontrivial (narrow) class number.
- (2) We work directly in each Atkin–Lehner eigenspace.

Our matrices are also as sparse as in the definite quaternion algebra case, but with a simpler reduction theory—working with ternary quadratic forms instead of quaternion ideals (whose reduced norm forms are quaternary quadratic forms).

The implementation in Magma [BCP97] of a very general version of the algorithm to compute orthogonal modular forms has been reported on by Assaf–Fretwell–Ingalls–Logan–Secord–Voight [AFI+22], based on an initial implementation described by Greenberg–Voight [GV14]. For this paper, we provide a complexity analysis and also implemented an optimized version in C++ restricted to $F = \mathbb{Q}$ and squarefree level N , available online [Hei24]. As Birch notes, these algorithms perform very well in practice (see section 9)!

Organization. The paper is organized as follows. In section 2, to orient the reader we give a simplified overview and presentation of the method in the special case where $F = \mathbb{Q}$, recovering spaces of classical modular forms. In section 3, we provide a brief setup for algebraic modular forms. We then specialize first to the case of definite quaternionic modular forms, relating them to Hilbert modular forms in section 4. We then specialize to orthogonal modular forms and explain the functoriality of the even Clifford algebra relating ternary quadratic forms and quaternion orders in section 5: this provides a natural, Hecke-equivariant relationship between the two spaces. In section 6, we introduce the radical character. We then discuss orthogonal newform theory in section 7, present the algorithms in section 8, and finally report on a specialized implementation for $F = \mathbb{Q}$ in section 9. We conclude in section A with a categorical equivalence which gives an alternative and more general approach to the correspondence provided by the even Clifford functor.

Acknowledgements. The authors would like to thank Eran Assaf, Asher Auel, Bryan Birch, Dan Fretwell, Benedict Gross, Adam Logan, Ariel Pacetti, Gustavo Rama, and Rainier Schulze-Pillot for their helpful comments over many years. Voight was supported by grants from the Simons Foundation (550029 and SFI-MPS-Infrastructure-00008650).

2. OVERVIEW IN THE CLASSICAL CASE

In this section, we briefly describe our results over $F = \mathbb{Q}$, eventually restricting to the case of squarefree level N and weight $k = 2$, a case of special interest to Birch [Bir91]. The reader can skip this section entirely or take it as an overview of the proof of our main result.

Let $Q: V \rightarrow \mathbb{Q}$ be a positive definite ternary (i.e., $\dim_{\mathbb{Q}} V = 3$) quadratic space with associated bilinear form

$$(2.1) \quad T(x, y) := Q(x + y) - Q(x) - Q(y) \quad \text{for } x, y \in V.$$

Let $\Lambda \subset V$ be a lattice ($\Lambda \simeq \mathbb{Z}^3$ is the \mathbb{Z} -span of a \mathbb{Q} -basis for V) that is *integral*, i.e., $Q(\Lambda) \subseteq \mathbb{Z}$. Choosing a basis $\Lambda = \mathbb{Z}e_1 + \mathbb{Z}e_2 + \mathbb{Z}e_3 \simeq \mathbb{Z}^3$ gives a quadratic form

$$(2.2) \quad Q_{\Lambda}(xe_1 + ye_2 + ze_3) = ax^2 + by^2 + cz^2 + uyz + vxz + wxy \in \mathbb{Z}[x, y, z]$$

and vice versa. Define the *(half-)discriminant*

$$(2.3) \quad \begin{aligned} N := \text{disc}(\Lambda) = \text{disc}(Q_{\Lambda}) &:= \det(T(e_i, e_j))_{i,j} / 2 = \frac{1}{2} \det \begin{pmatrix} 2a & w & v \\ w & 2b & u \\ v & u & 2c \end{pmatrix} \\ &= 4abc + uvw - au^2 - bv^2 - cw^2 \in \mathbb{Z}_{>0} \end{aligned}$$

We define the orthogonal group

$$(2.4) \quad \text{O}(V) := \{g \in \text{GL}(V) : Q(gx) = Q(x) \text{ for all } x \in V\}$$

and define $O(\Lambda)$ similarly; we have $\# O(\Lambda) < \infty$. We say lattices $\Lambda, \Pi \subset V$ are *isometric*, written $\Lambda \simeq \Pi$, if there exists $g \in O(V)$ such that $g\Lambda = \Pi$. We make similar definitions over \mathbb{Q}_p . The *genus* of Λ is

$$(2.5) \quad \text{Gen}(\Lambda) := \{\Pi \subset V : \Lambda_p \simeq \Pi_p \text{ for all } p\}.$$

The *class set* $\text{Cl}(\Lambda)$ is the set of isometry classes in $\text{Gen}(\Lambda)$. We have $\# \text{Cl}(\Lambda) < \infty$ by the geometry of numbers.

Kneser's theory of p -neighbors [Kne57, Voi23] gives an effective method to compute the class set, and it also gives the Hecke action, as follows. Let $p \nmid \text{disc}(\Lambda)$ be prime. We say that a lattice $\Pi \subset V$ is a p -neighbor of Λ , and write $\Pi \sim_p \Lambda$, if Π is integral and

$$(2.6) \quad [\Lambda : \Lambda \cap \Pi] = [\Pi : \Lambda \cap \Pi] = p.$$

If $\Lambda \sim_p \Pi$, then $\Pi \in \text{Gen}(\Lambda)$. The set of p -neighbors is efficiently computable: $\Pi \sim_p \Lambda$ if and only if there exists $v \in \Lambda$, $v \notin p\Lambda$ such that $Q(v) \equiv 0 \pmod{p^2}$ and

$$\Pi = p^{-1}v + \{w \in \Lambda : T(v, w) \in p\mathbb{Z}\}.$$

The line spanned by v in $\Lambda/p\Lambda$ uniquely determines Π , accordingly there are exactly $p+1$ neighbors Π (see [Tor05, Theorem 3.5]).

The space of *orthogonal modular forms* for Λ and trivial weight is

$$(2.7) \quad M(O(\Lambda)) := \text{Map}(\text{Cl}(\Lambda), \mathbb{C}).$$

In the basis of characteristic functions for Λ , we have $M(O(\Lambda)) \simeq \mathbb{C}^{\# \text{Cl}(\Lambda)}$.

For $p \nmid \text{disc}(\Lambda)$, define the *Hecke operator*

$$(2.8) \quad \begin{aligned} T_p : M(O(\Lambda)) &\rightarrow M(O(\Lambda)) \\ T_p(f)([\Lambda']) &:= \sum_{\Pi' \sim_p \Lambda'} f([\Pi']). \end{aligned}$$

The operators T_p commute and are self-adjoint with respect to a natural inner product, so there is a basis of simultaneous eigenvectors, called *eigenforms*. The Hecke operators restrict to $S(O(\Lambda)) \subset M(O(\Lambda))$, the orthogonal complement of the constant functions.

To compute this action: there is an explicit reduction theory of integral ternary quadratic forms due to Eisenstein [Eis1853] and improved by Schiemann [Sch97, §2], generalizing Gauss reduction of integral quadratic forms, which allows us to uniquely identify (special) isometry classes.

Birch observed that there is an inclusion

$$(2.9) \quad S(O(\Lambda)) \hookrightarrow S_2(\Gamma_0(N))$$

adding that it was “provable” [Bir91, p. 203] and sketching an argument. Indeed, this inclusion is explained by the even Clifford algebra. We define the *even Clifford algebra* of Λ by

$$(2.10) \quad O := \text{Clf}^0(\Lambda) := \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k$$

with standard involution and multiplication laws

$$(2.11) \quad \begin{aligned} i^2 &= ui - bc & jk &= a\bar{i} = a(u - i) \\ j^2 &= vj - ac & ki &= b\bar{j} = b(v - j) \\ k^2 &= wk - ab & ij &= c\bar{k} = c(w - k). \end{aligned}$$

Completing the square, we have

$$(2.12) \quad O \subset O \otimes \mathbb{Q} := B \simeq \left(\frac{w^2 - 4ab, -aN}{\mathbb{Q}} \right)$$

(with other similar symmetric expressions) so O is an order in a definite quaternion algebra B . Let $D := \text{disc}(B)$ be the product of the primes p that ramify in B .

Theorem 2.13. *The association $\Lambda \mapsto O = \text{Clf}^0(\Lambda)$ is functorial and induces a (reduced) discriminant-preserving bijection*

$$(2.14) \quad \left\{ \begin{array}{l} \text{Lattices } \Lambda \subset V \\ \text{up to isometry} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{l} \text{Quaternion orders } O \subset B \\ \text{up to isomorphism} \end{array} \right\}.$$

Equation (2.13) has a long history [Voi21, Remark 22.5.13], with perhaps the earliest version going back to Hermite.

Just as we defined the genus of Λ , we similarly define the genus of O to be the set of orders in B which are locally isomorphic to O ; the set of (global) isomorphism classes in the genus is called the *type set* $\text{Typ } O$.

Corollary 2.15. *The even Clifford map induces a natural bijection*

$$(2.16) \quad \text{Cl } \Lambda \leftrightarrow \text{Typ } O.$$

Of course from this corollary we obtain an isomorphism

$$M(O(\Lambda)) = \text{Map}(\text{Cl } \Lambda, \mathbb{C}) \xrightarrow{\sim} \text{Map}(\text{Typ}(O), \mathbb{C}).$$

We now move from orders to ideals. Define the (*right*) *class set* of O to be the set of locally principal fractional right O -ideals (those locally isomorphic to O) up to left multiplication by B^\times . Then taking the left order gives a surjective map of (pointed) sets

$$(2.17) \quad \begin{aligned} \text{Cls } O &\rightarrow \text{Typ } O \\ [I] &\mapsto [O_L(I)] \end{aligned}$$

which induces an injective \mathbb{C} -linear map

$$(2.18) \quad \text{Map}(\text{Typ}(O), \mathbb{C}) \rightarrow M(O) := \text{Map}(\text{Cls } O, \mathbb{C}).$$

Suppose now for simplicity that N is *squarefree*. Then O is an Eichler order (in fact, a hereditary order). The fibers of (2.17) are naturally identified with two-sided ideals, measured by the group $\text{AL}(O) \simeq \prod_{p|N} C_2$ of Atkin–Lehner involutions. By naturality and restricting to the cuspidal subspace, we have a Hecke-equivariant isomorphism

$$(2.19) \quad S(O(\Lambda)) \xrightarrow{\sim} S(O)^+$$

where $S(O)^+$ are those forms invariant under $\text{AL}(O)$. Finally, the Jacquet–Langlands correspondence gives

$$(2.20) \quad S(O)^+ \hookrightarrow S_2^{D\text{-new}}(\Gamma_0(N))^\delta$$

where for $M \mid N$ we write ε_M for the sign vector which is -1 exactly at the primes $p \mid M$ and then $\delta := \varepsilon_D$ for the Hilbert symbol for B .

To get all forms, we add a representation. We equip V with an orientation (e.g., choose an ordered \mathbb{Q} -basis $V \simeq \mathbb{Q}^3$) and define $\text{SO}(V) := \text{O}(V) \cap \text{SL}(V)$. We note that $\text{O}(V) \simeq \{\pm 1\} \times \text{SO}(V)$. Therefore, we have a natural homomorphism obtained from the composition

$$(2.21) \quad \nu: \text{O}(V) \rightarrow \text{O}(V)/\{\pm 1\} \simeq \text{SO}(V) \simeq B^\times/\mathbb{Q}^\times \xrightarrow{\text{nrd}} \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$$

called the *spinor norm*. A delightful calculation (see Equation (8.3)) shows that if $\gamma \in \text{SO}(V)$ has $\text{tr}(\gamma) \neq -1$, then $\gamma(\nu) = \text{tr}(\gamma) + 1$.

For $r \mid N$, we define the *spinor character* for r by

$$(2.22) \quad \begin{aligned} \nu_r : \mathrm{O}(V) &\xrightarrow{\nu} \mathbb{Q}^\times / \mathbb{Q}^{\times 2} \rightarrow \{\pm 1\} \\ a &\mapsto \prod_{p \mid r} (-1)^{\mathrm{ord}_p(a)} \end{aligned}$$

The spinor characters “find” the remaining forms with all Atkin–Lehner signs. We let $M(\mathrm{SO}(\Lambda), \nu_r)$ be the space of functions from $\mathrm{Gen} \Lambda$ to \mathbb{C} that transform by ν_r : that is, $f(\gamma\Lambda') = \nu_r(\gamma)f(\Lambda')$ for all $\gamma \in \mathrm{SO}(V)$. We take again $S(\mathrm{SO}(\Lambda), \nu_r)$ the orthogonal complement of the constant functions: when $r \neq 1$, we have $S(\mathrm{SO}(\Lambda), \nu_r) = M(\mathrm{SO}(\Lambda), \nu_r)$.

Putting all of this together, we obtain Equation (1.4) in this special case: we have a Hecke-equivariant isomorphism

$$(2.23) \quad S(\mathrm{SO}(\Lambda), \nu_r) \simeq S_2^{D\text{-new}}(\Gamma_0(N))^{\delta_{\varepsilon_r}}.$$

To prove Equation (1.3), we compute the Hecke action on $S(\mathrm{SO}(\Lambda), \nu_r)$ using ternary forms and p -neighbors, giving the Hecke action on the space of classical modular forms. To compute T_p on $S(\mathrm{SO}(\Lambda), \nu_r)$ for $p \nmid N$, starting with Λ we iteratively compute p -neighbors and reduce to identify isomorphism classes: we repeat this $O(\#\mathrm{Cl} \Lambda) = O(d)$ times with $p+1$ neighbors, so the running time is $\tilde{O}(pd)$ where

$$(2.24) \quad d := \dim S(\mathrm{SO}(\Lambda), \nu_r)$$

is the dimension of the output space.

Remark 2.25. Birch says that his original motivation was to generalize the *method of graphs* due to Mestre–Oesterlé. This method was recently studied by Cowan [Cow22], so we briefly explain the connection here as this method provides an extension to nonsquare level with many parallel aspects. Let O be a maximal order in a quaternion algebra B with discriminant $\mathrm{disc}(B) = p$. Then there are at most two supersingular curves E up to isomorphism over $\mathbb{F}_p^{\mathrm{al}}$ such that $\mathrm{End}(E) \simeq O$; there are two such if and only if $j(E) \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ if and only if the unique two-sided ideal of O of reduced norm p is not principal. So if we identify E with its image $E^{(p)}$ under the Frobenius map when $j(E) \notin \mathbb{F}_p$, then we get a bijection of such classes with the type set $\mathrm{Typ} O$, which is in bijection with ternary quadratic forms of discriminant p (also known as the Deuring correspondence).

We conclude with a simple example.

Example 2.26. Let $\Lambda = \mathbb{Z}^3 = \mathbb{Z}e_1 + \mathbb{Z}e_2 + \mathbb{Z}e_3 \subset \mathbb{Q}^3$ have the quadratic form

$$Q_\Lambda(x, y, z) = x^2 + y^2 + 3z^2 + xz$$

and bilinear form given by

$$[T_\Lambda] = \begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & 6 \end{pmatrix}$$

so $\mathrm{disc}(Q_\Lambda) = 11$. We compute that among the 2-neighbors of Λ , one is isometric to Λ and the other two reduce to a new lattice Λ' with Gram matrix

$$\begin{pmatrix} 2 & -1 & 1 \\ -1 & 2 & -1 \\ 1 & -1 & 8 \end{pmatrix}.$$

Among the 2-neighbors of Λ' , all 3 are isometric to Λ . This yields

$$[T_2] = \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix}.$$

Similarly, we compute

$$[T_3] = \begin{pmatrix} 2 & 2 \\ 3 & 1 \end{pmatrix}, \quad [T_5] = \begin{pmatrix} 4 & 2 \\ 3 & 3 \end{pmatrix}, \quad \dots$$

The constant function $e = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in M(\mathrm{SO}(\Lambda))$ is an Eisenstein series with $T_p(e) = (p+1)e$.

Another eigenvector is $f = \begin{pmatrix} 2 \\ -3 \end{pmatrix}$ with $T_p(f) = a_p(f)$:

$$a_3 = -1, a_5 = 1, \dots$$

We match it with the familiar modular form [11.2.a.a](#):

$$\sum_{n=1}^{\infty} a_n q^n = \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{11n})^2 = q - 2q^2 - q^3 + \dots \in S_2(\Gamma_0(11)).$$

And indeed the Atkin–Lehner involution $z \mapsto \frac{-1}{11z}$ acts on $f(z) dz$ with eigenvalue $w_{11} = -a_{11} = -1$, as expected.

3. ALGEBRAIC MODULAR FORMS

We now begin the general case. In this section, we briefly review the theory of algebraic modular forms, as our quaternionic modular forms and orthogonal modular forms will be special cases of this theory. For further reference, see Gross [\[Gro99\]](#). Concrete versions of the general theory in this section will be provided in the two sections that follow.

Let F be a number field with ring of integers $R := \mathbb{Z}_F$. Let \mathbf{G} be a reductive algebraic group defined over F . Let $G_{\infty} := \prod_{v|\infty} \mathbf{G}(F_v)$. Then G_{∞} is a real Lie group with finitely many connected components. We consider a very special case: suppose that G_{∞} is compact modulo its center. This setup was investigated by Gross [\[Gro99\]](#), who showed that modular forms and automorphic representations can be fruitfully studied in the absence of analytic hypotheses; in particular, we are in an ideal setting to develop algorithms.

Let $\widehat{F} := \prod'_{\mathfrak{p}} F_{\mathfrak{p}}$ be the finite adeles of F . Let \widehat{K} be a compact open subgroup of $\widehat{G} := \mathbf{G}(\widehat{F})$, let $G := \mathbf{G}(F)$, and consider the double coset space

$$(3.1) \quad Y := G \backslash \widehat{G} / \widehat{K}.$$

The set Y is finite (being both discrete and compact), and so we can write a finite decomposition

$$(3.2) \quad \widehat{G} = \bigsqcup_i^{<\infty} G \widehat{\beta}_i \widehat{K}.$$

Each point $G \widehat{\beta}_i \widehat{K} \in Y$ has a (finite) stabilizer group

$$(3.3) \quad \Gamma_i := \widehat{\beta}_i \widehat{K} \widehat{\beta}_i^{-1} \cap G$$

whose conjugacy class in G is independent of the choice of representative $\widehat{\beta}_i$.

Let W be a finite-dimensional representation of G over \mathbb{C} with a left action $x \mapsto g \cdot x$ for $g \in G$ and $x \in W$. The space of *modular forms on \mathbf{G} of level \widehat{K} and weight W* is

$$(3.4) \quad M_W(\widehat{K}) := \{f: \widehat{G} \rightarrow W : f(g\widehat{\alpha}\widehat{u}) = g \cdot f(\widehat{\alpha}) \text{ for all } g \in G, \widehat{u} \in \widehat{K}\}$$

A form $f \in M_W(\widehat{K})$ is locally constant on \widehat{G} since it is invariant under the open compact \widehat{K} .

With respect to a decomposition (3.2), we see that as \mathbb{C} -vector spaces, we have an isomorphism

$$(3.5) \quad \begin{aligned} M_W(\widehat{K}) &\xrightarrow{\sim} \bigoplus_i H^0(\Gamma_i, W) \\ f &\mapsto (f(\widehat{\beta}_i))_i \end{aligned}$$

where $H^0(\Gamma_i, W)$ denotes Γ_i -invariants, since $g\widehat{\beta}_i\widehat{K} = \widehat{\beta}_i\widehat{K}$ if and only if $g \in \Gamma_i$.

We will also make use of two slight generalizations and modifications. First, we allow character. Suppose that $\widehat{K} \trianglelefteq \widehat{K}_0$ is a normal inclusion such that $C := \widehat{K}_0/\widehat{K}$ is *abelian*. Since \widehat{K}_0 normalizes \widehat{K} , the group C acts by right translation on \widehat{G}/\widehat{K} , inducing operators on $M_W(\widehat{K})$ which we call *diamond operators* by analogy with the classical case. Then we have an isotypic decomposition

$$(3.6) \quad M_W(\widehat{K}) \xrightarrow{\sim} \bigoplus_{\chi \in C^\vee} M_W(\widehat{K}_0, \chi)$$

according to characters $\chi: C \rightarrow \mathbb{C}^\times$, where we define

$$(3.7) \quad M_W(\widehat{K}_0, \chi) := \{f: \widehat{G} \rightarrow W : f(g\widehat{\alpha}\widehat{u}) = \chi(u)(g \cdot f(\widehat{\alpha})) \text{ for all } g \in G, \widehat{u} \in \widehat{K}_0\}.$$

Second, similarly the normalizer mod centralizer $A := N_{\widehat{G}}(\widehat{K})/(\widehat{K}C_{\widehat{G}}(\widehat{K}))$ acts by conjugation on \widehat{K} and hence on $M_W(\widehat{K})$. When A is abelian we have an isotypic decomposition

$$(3.8) \quad M_W(\widehat{K}) \xrightarrow{\sim} \bigoplus_{\chi \in A^\vee} M_W(\widehat{K})^\chi$$

where the subspace is defined by the condition that A acts via χ .

Remark 3.9. As further generalizations, we could equally well work with W a finite-dimensional representation over any field, and weaken the requirement that the groups $C = \widehat{K}_0/\widehat{K}$ and $A = N_{\widehat{G}}(\widehat{K})/(\widehat{K}Z_{\widehat{G}}(\widehat{K}))$ are abelian by instead taking the isotopic decomposition indexed instead by irreducible representations.

The space $M_W(\widehat{K})$ is equipped with the action of Hecke operators $T_{\widehat{\pi}}$ for $\widehat{\pi} \in \widehat{G}$, depending on the class $\widehat{K}\widehat{\pi}\widehat{K}$, as follows: write

$$(3.10) \quad \widehat{K}\widehat{\pi}\widehat{K} = \bigsqcup_j \widehat{\pi}_j\widehat{K}$$

as a finite disjoint union, and then for $f \in M_W(\widehat{K})$ define

$$(3.11) \quad (T_{\widehat{\pi}}f)(\widehat{\alpha}\widehat{K}) := \sum_j f(\widehat{\alpha}\widehat{\pi}_j\widehat{K}).$$

This is well-defined (independent of the choice of representative $\widehat{\pi}$ and representatives $\widehat{\pi}_j$) by the right \widehat{K} -invariance of f .

We call the subspace of $M_W(\widehat{K})$ of functions that factor through $\widehat{G}/[\widehat{G}, \widehat{G}]$ the space of *Eisenstein series*. There is a natural inner product on $M_W(\widehat{K})$ —the dot product weighted by $1/\#\Gamma_i$ —for which the Hecke operators are self-adjoint, and we let the *cuspidal subspace* be the orthogonal complement of the Eisenstein series under the inner product.

4. HILBERT MODULAR FORMS AS QUATERNIONIC MODULAR FORMS

In this section, we specialize the previous section to the case of groups from definite quaternion algebras.

Let B be a definite quaternion algebra over a totally real field F . We take \mathbf{G} to be the reductive group associated to $G = B^\times$, so that $G_\infty = B_\infty^\times \simeq \prod_{v|\infty} \mathbb{H}^\times$ where \mathbb{H} is the division ring of real Hamiltonians, and $\widehat{G} = \widehat{B}^\times$.

For level structure, we let $O \subseteq B$ be an R -order and take $\widehat{K} = \widehat{O}^\times$; let $\mathfrak{N} := \text{discrd}(O)$. Then the double coset space

$$(4.1) \quad Y = G \backslash \widehat{G} / \widehat{K} = B^\times \backslash \widehat{B}^\times / \widehat{O}^\times \leftrightarrow \text{Cls } O$$

is naturally identified with the (*right*) *class set* of O [Voi21, Lemma 27.6.8].

We restrict to weights $k = (k_v)_v \in \prod_{v|\infty} 2\mathbb{Z}_{>0}$, corresponding to the representation $W_k := \bigotimes_{v|\infty} \text{Sym}^{k_v-2}(\mathbb{C})(-k_v/2 - 1)$ with respect to a splitting $B^\times \hookrightarrow \text{GL}_2(\mathbb{C})$, but we also consider twists of these weights by characters. On the associated space of modular forms, there is an action by diamond operators corresponding to the class group [Voi21, 41.3.4] which picks out the central character; we let $M_k(\widehat{O}^\times)$ be the fixed space. The Eisenstein subspace consists of those functions that factor through the norm map $\text{nrd}: \widehat{B}^\times \rightarrow \widehat{F}^\times$; this space is trivial unless $k_v = 2$ for all $v \mid \infty$. We let $S_k(\widehat{O}^\times) \subseteq M_k(\widehat{O}^\times)$ be the orthogonal complement of the Eisenstein subspace.

We further define the group

$$(4.2) \quad \text{AL}(\widehat{O}) := N_{\widehat{B}^\times}(\widehat{O})/(\widehat{F}^\times \widehat{O}^\times) \simeq \prod_{\mathfrak{p}|\mathfrak{N}} \text{AL}(O_{\mathfrak{p}})$$

which we call the adelic *Atkin–Lehner group*. (Although there are complications in the global normalizer group [Voi21, §28.9], they do not arise adelically.) Then as in (3.8) when $\text{AL}(\widehat{O})$ is abelian—and more generally as in Equation (3.9)—we have

$$(4.3) \quad S_k(\widehat{O}^\times) \simeq \bigoplus_{\chi \in \text{AL}(\widehat{O})^\vee} S_k(\widehat{O}^\times)^\chi$$

checking that the Eisenstein subspace is preserved under the normalizer.

We now focus on a very general class of orders for which we have good control of the normalizers. See Voight [Voi21, §24.3] for background reading. Let $\mathfrak{N} \subseteq R$ be a nonzero ideal.

Definition 4.4. A quaternion algebra B over F is *suitable* for \mathfrak{N} provided that

- (i) B is ramified at all infinite places; and
- (ii) if B is ramified at \mathfrak{p} , then $v_{\mathfrak{p}}(\mathfrak{N})$ is odd.

Proposition 4.5. *There are quaternion algebras suitable for \mathfrak{N} except when $[F : \mathbb{Q}]$ is odd and \mathfrak{N} is a square.*

Proof. When $[F : \mathbb{Q}]$ is even, we can take B ramified at all the infinite places and split at all the finite places. When $[F : \mathbb{Q}]$ is odd and \mathfrak{N} is not a square, we can take B ramified at all infinite places and at one \mathfrak{p} , where $v_{\mathfrak{p}}(\mathfrak{N})$ is odd, and split at all other finite places. \square

Remark 4.6. We will not assume that the quaternion algebra is as given by the proof above. For reasons that will be clear later, it will be more convenient to have a quaternion algebra ramified at more primes.

An order O is *locally residually unramified* [Voi21, 24.3] if for all primes $\mathfrak{p} \mid \text{discrd}(O)$, the quotient $O_{\mathfrak{p}}/\text{rad}(O_{\mathfrak{p}})$ of the quotient of the completed order by the Jacobson radical is either $\mathbb{F}_{\mathfrak{p}} \times \mathbb{F}_{\mathfrak{p}}$ (*residually split* or *Eichler* at \mathfrak{p}) or $\mathbb{F}_{\mathfrak{p}^2}$ (*residually inert* at \mathfrak{p}), corresponding to the Eichler symbol values $1, -1$.

We will need to recall some facts in the residually inert case, studied by Pizer [Piz77, §2] (see also [Voi21, 24.3.7]). Let $O_{\mathfrak{p}}$ be residually inert. Lifting the extension $O_{\mathfrak{p}}/\text{rad } O_{\mathfrak{p}} \simeq \mathbb{F}_{\mathfrak{p}^2}$ we have a quadratic unramified extension $S_{\mathfrak{p}} \supseteq R_{\mathfrak{p}}$, the valuation ring in the quadratic unramified extension $K_{\mathfrak{p}} \supseteq F_{\mathfrak{p}}$. Diagonalizing, we find $O_{\mathfrak{p}} \simeq \begin{pmatrix} S_{\mathfrak{p}} & b \\ R_{\mathfrak{p}} & \end{pmatrix}$ for some $b \in R \setminus \{0\}$. Since $\text{Nm}_{S_{\mathfrak{p}}|R_{\mathfrak{p}}}(S_{\mathfrak{p}}^{\times}) = R_{\mathfrak{p}}^{\times}$, we may suppose that $b = \pi^e$ for some $e \geq 0$ with π a uniformizer for $R_{\mathfrak{p}}$, and then $\text{discrd } O_{\mathfrak{p}} = \mathfrak{p}^e$. We have e even when $B_{\mathfrak{p}} \simeq M_2(F_{\mathfrak{p}})$ and e odd when $B_{\mathfrak{p}}$ a division algebra [Voi21, 24.4.9]. Then [Voi21, Proof of Proposition 24.4.7] the order $O_{\mathfrak{p}} \otimes S_{\mathfrak{p}} \hookrightarrow M_2(S_{\mathfrak{p}})$ is residually split, and the regular representation identifies

$$(4.7) \quad O_{\mathfrak{p}} \hookrightarrow \left\{ \begin{pmatrix} u & v \\ b\bar{v} & \bar{u} \end{pmatrix} : u, v \in S_{\mathfrak{p}} \right\} \subseteq M_2(S_{\mathfrak{p}})$$

with $j \mapsto \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix}$.

Proposition 4.8. *If B is a suitable quaternion algebra for \mathfrak{N} , then there exists a residually unramified order $O \subseteq \mathfrak{N}$ with $\text{discrd}(O) = \mathfrak{N}$. Moreover, the genera of such orders are determined by the choice of residually inert or split for $\mathfrak{p}^e \parallel \mathfrak{N}$ with e even.*

We could make a unique choice in Equation (4.8) by taking $O_{\mathfrak{p}}$ residually split whenever $B_{\mathfrak{p}}$ is split.

Proof. As we have seen, all residually unramified orders in a local division quaternion algebra have odd exponent in their reduced discriminant, which is precisely guaranteed by the algebra being suitable; there is no condition at primes \mathfrak{p} split in B . See also Gross [Gro88, Proposition 3.4]. \square

Remark 4.9. Gross [Gro88] and Martin [Mar20] also consider residually ramified orders with bounded level, so our methods could be extended to that case too (e.g., the Lipschitz order in the Hurwitz order).

We are now ready to state the correspondence between Hilbert modular forms and quaternionic modular forms. Let B be a quaternion algebra suitable for \mathfrak{N} , let $\mathfrak{D} = \text{disc } B$, and let O be a residually unramified order with $\text{discrd}(O) = \mathfrak{N}$. Write $\mathfrak{N} = \mathfrak{N}_- \mathfrak{N}_+$ where \mathfrak{N}_- is divisible by exactly those primes where O is residually inert (i.e., Eichler invariant -1) and \mathfrak{N}_+ by primes where O is residually split (Eichler invariant $+1$). Whenever $\mathfrak{p} \mid \mathfrak{D}$, we must have $\mathfrak{p} \mid \mathfrak{N}_-$.

For Hilbert modular forms, we take adelic level structure $\widehat{\Gamma}_0(\mathfrak{N}) \leq \text{GL}_2(\widehat{R})$ writing the associated space of cuspidal Hilbert modular forms (with trivial central character) as $S_k(\widehat{\Gamma}_0(\mathfrak{N}))$. For $\mathfrak{M} \mid \mathfrak{N}$, let $S_k^{\mathfrak{M}\text{-new}}(\widehat{\Gamma}_0(\mathfrak{N})) \subseteq S_k(\widehat{\Gamma}_0(\mathfrak{N}))$ be the subspace consisting of forms which are \mathfrak{p} -new for all $\mathfrak{p} \mid \mathfrak{M}$ with respect to the natural degeneracy operators.

Theorem 4.10 (Eichler–Shimizu–Jacquet–Langlands correspondence). *Let O be a suitable quaternion order of level \mathfrak{N} . Then there is an isomorphism of Hecke-modules*

$$(4.11) \quad S_k(\widehat{O}) \simeq \bigoplus_{\mathfrak{M}} S_k^{\mathfrak{M}\text{-new}}(\widehat{\Gamma}_0(\mathfrak{M}\mathfrak{N}_+))$$

where the sum runs over all divisors $\mathfrak{M} \mid \mathfrak{N}_-$ such that $v_{\mathfrak{p}}(\mathfrak{M})$ and $v_{\mathfrak{p}}(\mathfrak{N})$ have the same parity for all $\mathfrak{p} \mid \mathfrak{N}_-$.

Proof. See Jacquet–Langlands [JL70, Chap. XVI], Gelbart–Jacquet [GJ79, §8], and Hida [Hid81, Proposition 2.12], and more recently Martin [Mar20, Theorem 1.1(ii)]. \square

For these nice lattices and orders, we have a simple description of the normalizer.

Proposition 4.12. *Suppose that O is residually unramified at \mathfrak{p} . Then the following statements hold.*

- (a) *The Atkin–Lehner group $\text{AL}(O_{\mathfrak{p}})$ has order 2, generated by $w_{\mathfrak{q}}$ where $\mathfrak{q} = \mathfrak{p}^e \parallel \mathfrak{N}$.*
- (b) *Under the correspondence with Hilbert modular forms (4.11), the involution $w_{\mathfrak{q}}$ on $S_k(\widehat{O}^{\times})$ corresponds to either the Atkin–Lehner involution on $S_k(\widehat{\Gamma}_0(\mathfrak{N}))$ or its negative, according as $\mathfrak{p} \mid \mathfrak{D}$ or not.*

Proof. We begin with (a). When $O_{\mathfrak{p}}$ is residually split (Eichler) the result is well-known [Voi21, Proposition 23.4.14]. The residually inert case can be derived from this, as follows. The inclusion (4.7) provides an inclusion $N_{B_{\mathfrak{p}}^{\times}}(O_{\mathfrak{p}}) \hookrightarrow N_{B_{K_{\mathfrak{p}}}^{\times}}(O_{S_{\mathfrak{p}}})$. We check that indeed $j \in N_{B_{\mathfrak{p}}^{\times}}(O_{\mathfrak{p}})$, and the rest is $O_{S_{\mathfrak{p}}}^{\times} \cap B_{\mathfrak{p}}^{\times} = O^{\times}$.

Part (b) follows from work of Jacquet–Langlands [JL70, Proposition 15.5], see also [GJ79, Theorem (8.1)] (Gelbart–Jacquet). The result may also be derived via theta series using work of Böcherer–Schulze-Pillot [BSP91, Lemma 8.2]. \square

As in the introduction, a *sign vector* (for \mathfrak{N}) is

$$(4.13) \quad \varepsilon = (\varepsilon_{\mathfrak{p}})_{\mathfrak{p}} \in \prod_{\mathfrak{p}^e \parallel \mathfrak{N}} \{\pm 1\}.$$

For a sign vector, we define

$$(4.14) \quad S_k(\widehat{O})^{\varepsilon} = \{f \in S_k(\widehat{O}) : w_{\mathfrak{q}}f = \varepsilon_{\mathfrak{p}}f\}$$

We conclude this section with newform theory, with attention to Atkin–Lehner eigenvalues. The algorithmic application will be to knowing precisely when we have carved away the old subspace.

Definition 4.15. Let α be the multiplicative function on divisors of \mathfrak{N} defined by

$$\alpha(\mathfrak{p}^e) = \begin{cases} 1 + e, & \text{if } \mathfrak{p} \mid \mathfrak{N}_+; \\ 1, & \text{if } \mathfrak{p} \mid \mathfrak{N}_- \text{ and } e \text{ is even; and} \\ 0, & \text{if } \mathfrak{p} \mid \mathfrak{N}_- \text{ and } e \text{ is odd.} \end{cases}$$

The function α records multiplicities in the newform decomposition as follows.

Theorem 4.16. *We have*

$$S_k(\widehat{O}^{\times}) \simeq \bigoplus_{\mathfrak{M} \mid \mathfrak{N}} S_k^{\text{new}}(\widehat{\Gamma}_0(\mathfrak{M}))^{\oplus \alpha(\mathfrak{N}/\mathfrak{M})}$$

Proof. First, we rewrite Equation (4.10) as

$$(4.17) \quad S_k(\widehat{O}^\times) \simeq \bigoplus_{\mathfrak{M}_- | \mathfrak{N}_-} S_k^{\mathfrak{M}_- \text{-new}}(\widehat{\Gamma}_0(\mathfrak{M}_- \mathfrak{N}_+))^{\oplus \alpha(\mathfrak{N}_- / \mathfrak{M}_-)}.$$

Second, we apply the usual Atkin–Lehner theory for Hilbert modular forms, see Roberts–Schmidt [RS07, p. 4] for a succinct summary. We obtain

$$(4.18) \quad S_k^{\mathfrak{M}_- \text{-new}}(\widehat{\Gamma}_0(\mathfrak{M}_- \mathfrak{N}_+)) \simeq \bigoplus_{\mathfrak{M}_+ | \mathfrak{N}_+} S_k^{\text{new}}(\widehat{\Gamma}_0(\mathfrak{M}_- \mathfrak{M}_+))^{\oplus \alpha(\mathfrak{N}_+ / \mathfrak{M}_+)}.$$

We conclude by substituting (4.18) into (4.17), using multiplicativity of α , and rewriting divisors as $\mathfrak{M} = \mathfrak{M}_- \mathfrak{M}_+ | \mathfrak{N}_- \mathfrak{N}_+ = \mathfrak{N}$. \square

Now we refine this theorem to take Atkin–Lehner signs into account. For $\mathfrak{p} | \mathfrak{N}_-$, there is no change in the Atkin–Lehner signs under degeneracy operators; for $\mathfrak{p} | \mathfrak{N}_+$, the possible Atkin–Lehner signs are as balanced as possible.

Definition 4.19. For a sign vector ε , let α^ε be the multiplicative function on divisors of \mathfrak{N} such that

$$\alpha^\varepsilon(\mathfrak{p}^e) = \begin{cases} \left\lceil \frac{1+\varepsilon}{2} \right\rceil, & \text{if } \mathfrak{p} | \mathfrak{N}_+ \text{ and } \varepsilon_{\mathfrak{p}} = +1; \\ \left\lfloor \frac{1+\varepsilon}{2} \right\rfloor, & \text{if } \mathfrak{p} | \mathfrak{N}_+ \text{ and } \varepsilon_{\mathfrak{p}} = -1; \\ 1, & \text{if } \mathfrak{p} | \mathfrak{N}_-, e \text{ is even, and } \varepsilon_{\mathfrak{p}} = +1; \text{ and} \\ 0, & \text{if } \mathfrak{p} | \mathfrak{N}_-, \text{ otherwise} \end{cases}$$

Considering cases, it is straightforward to show that $\sum_{\varepsilon} \alpha^\varepsilon = \alpha$.

Proposition 4.20. *Let ε be a sign vector. Then*

$$(4.21) \quad S_k^{\mathfrak{M}_- \text{-new}}(\widehat{\Gamma}_0(\mathfrak{M}_- \mathfrak{N}_+))^\varepsilon \simeq \bigoplus_{\mathfrak{M}_+ | \mathfrak{N}_+} \bigoplus_{\varepsilon'} (S_k^{\text{new}}(\widehat{\Gamma}_0(\mathfrak{M}_- \mathfrak{M}_+))^{\varepsilon'})^{\oplus \alpha^{\varepsilon \varepsilon'}(\mathfrak{N}_+ / \mathfrak{M}_+)}$$

the sum over all sign vectors ε' .

Proof. This is standard newform theory of Atkin–Lehner in the case of Hilbert modular forms: see e.g. Roberts–Schmidt [RS07, p. 4] for a concise statement. \square

Corollary 4.22. *Let δ be the sign vector with $\delta_{\mathfrak{p}} = -1$ if and only if $\mathfrak{p} | \mathfrak{D}$. Then we have*

$$(4.23) \quad S_k(\widehat{O}^\times)^\varepsilon \simeq \bigoplus_{\mathfrak{M} | \mathfrak{N}} \bigoplus_{\varepsilon'} (S_k^{\text{new}}(\widehat{\Gamma}_0(\mathfrak{M}))^{\delta \varepsilon \varepsilon'})^{\oplus \alpha^{\delta \varepsilon \varepsilon'}(\mathfrak{N} / \mathfrak{M})}.$$

Proof. Repeat the proof of Equation (4.16) but restrict to the Atkin–Lehner subspaces using Equation (4.20) and Equation (4.12)(b). \square

Remark 4.24. It is also enough in (4.21) and (4.23) to sum only over those sign vectors ε' such that $\varepsilon'_{\mathfrak{p}} = 1$ for all $\mathfrak{p} | \mathfrak{N}_-$.

5. TERNARY QUADRATIC FORMS AND THE EVEN CLIFFORD ALGEBRA

In this section, we review the even Clifford functor, relating ternary quadratic forms and quaternion orders. We then observe that this functor gives a Hecke-equivariant isomorphism between certain spaces of orthogonal modular forms and quaternionic modular forms. Importantly, we show that (because we are in odd rank) we can work equivalently with isometry classes or (twisted) similarity classes, the former being simpler for computation. We then restrict this result to a nice class of lattices—those with cyclic

discriminant—corresponding to a nice class of quaternion orders—those which are locally residually unramified, as in the previous section. For further background reading, see Voight [Voi21, Chapters 22–24].

Let R be a Dedekind domain with field of fractions $F := \text{Frac } R$. Let V be an F -vector space with $\dim_F V = 3$ and let $Q: V \rightarrow F$ be a nondegenerate quadratic form. Recall that the *similarity group* of V is the algebraic group $\text{GO}(V)$ consisting of linear maps that preserve the quadratic form V up to a scalar called the *similitude factor*, the *isometry group* $\text{O}(V)$ of V is the algebraic subgroup of similarities with similitude factor 1 [Voi21, §4.2], and the *special* (or *oriented*) *isometry group* $\text{SO}(V)$ of V is the subgroup fixing an orientation.

In fact, every similarity is in fact an oriented isometry composed with a scaling.

Lemma 5.1. *Multiplication gives an isomorphism*

$$(5.2) \quad \text{SO}(V) \times \text{GL}_{1,F} \rightarrow \text{GO}(V)$$

of algebraic groups over F .

Proof. Choose a basis $V \simeq F^3$ and let $[T]$ be the Gram matrix of the symmetric bilinear form T associated to Q in this basis and $A = [\phi]$. Certainly we have a homomorphism, it is injective because if $cA = 1$ then $c^3 \det A = c^3 = 1$ but also $A^t[T]A = [T]$ so $c^2 = 1$ so in fact $c = 1$.

To see the map is surjective, we define an inverse. If $A \in \text{GL}_3(F)$ has $A^t[T]A = u[T]$ with $u \in F^\times$, let $d := \det A$, then taking determinants and cancelling $\det[T] \in F^\times$ gives $d^2 = u^3$ so $u = (d/u)^2$ is a square; whence $(u/d)A \in \text{SO}(V)$ and so we can map $A \mapsto ((u/d)A, d/u)$.

This shows the isomorphism on F -points; repeating this over an arbitrary extension gives the result on the level of algebraic groups. \square

Remark 5.3. Equation (5.1) generalizes to nondegenerate quadratic forms of any odd dimension.

Let $\Lambda \subseteq V$ be an R -lattice. An *isometry* or *similarity* from Λ to an R -lattice Λ' is such a map ϕ on V such that $\phi(\Lambda) = \Lambda'$, and we define $\text{SO}(\Lambda) \leq \text{O}(\Lambda) \leq \text{GO}(\Lambda)$ for the corresponding stabilizers. Restricting (5.1) gives an isomorphism

$$(5.4) \quad \text{SO}(\Lambda) \times \text{GL}_{1,R} \xrightarrow{\sim} \text{GO}(\Lambda).$$

Attached to Λ will be four possible class sets corresponding to the notions above—but with one asterisk, they all end up being in natural bijection.

We first define the usual *genus* $\text{Gen}_\text{O}(\Lambda) = \text{Gen}(\Lambda)$ of Λ , consisting of all lattices $\Lambda' \subseteq V$ such that $\Lambda_{(\mathfrak{p})}$ is isometric to $\Lambda'_{(\mathfrak{p})}$ for all (nonzero) primes $\mathfrak{p} \subseteq R$, where the subscript denotes localization; then we define the *class set* $\text{Cl}_\text{O} \Lambda = \text{Cl } \Lambda$ to be the (global) isometry classes in $\text{Gen}(\Lambda)$.

Second, we could replace isometry with oriented isometry to get $\text{Cl}_{\text{SO}} \Lambda$, in fact the natural inclusion map $\text{Cl}_{\text{SO}} \Lambda \rightarrow \text{Cl}_\text{O} \Lambda$ is a bijection: we have $\text{O}(\Lambda) \simeq \{\pm 1\} \times \text{SO}(\Lambda)$, so two lattices are isometric if and only if they are oriented isometric, the same being true locally. (This holds more generally in odd rank.)

Third, we replace isometry with similarity, and get the *similarity genus* $\text{Gen}_{\text{GO}}(\Lambda)$ (lattices locally similar to Λ) and *similarity class set* $\text{Cl}_{\text{GO}} \Lambda$ (up to global similarity). On $\text{Cl}_{\text{GO}} \Lambda$, we have an action of $\text{Cl } R$ by $[\mathfrak{a}] \cdot [\Lambda] = [\mathfrak{a}\Lambda]$.

Definition 5.5. The *twist* of Λ by a fractional ideal \mathfrak{a} is the lattice $\mathfrak{a}\Lambda$. A *twisted similarity* between two R -lattices $\Lambda, \Lambda' \subseteq V$ is a similarity between a twist of Λ and Λ' .

Finally, we define analogously the *twisted similarity class set*, the quotient set $(\text{Cl}_{\text{GO}} \Lambda)^{\text{Cl} R}$.

Lemma 5.6. *There is a natural inclusion map $\text{Cl}_O \Lambda \hookrightarrow \text{Cl}_{\text{GO}} \Lambda$ which induces a bijection $\text{Cl}_O \Lambda \leftrightarrow (\text{Cl}_{\text{GO}} \Lambda)^{\text{Cl} R}$.*

Proof. The two maps are injective, since isometries are in particular similarities and twisted similarities. The second map is also surjective, as follows. Suppose Λ' is locally twisted similar to Λ ; we find a twist of Λ' which is locally isometric to Λ . Since the localizations are DVRs we conclude that Λ' is locally similar to Λ . Considering a local similarity over F , using (5.2) we see that there exists local isometries between $\Lambda_{(\mathfrak{p})}$ and $a_{(\mathfrak{p})}\Lambda'$ for each prime \mathfrak{p} . Since $\Lambda_{(\mathfrak{p})} = \Lambda'_{(\mathfrak{p})}$ for all but finitely many \mathfrak{p} , there is a unique fractional ideal $\mathfrak{a} \subseteq F$ such that $\mathfrak{a}_{(\mathfrak{p})} = a_{(\mathfrak{p})}R_{(\mathfrak{p})}$ for all \mathfrak{p} , and hence Λ is locally isometric to $\mathfrak{a}\Lambda'$, as desired. \square

We now turn to the main goal of this section: Clifford algebras. The even Clifford algebra [Voi21, §5.3] $B := \text{Clf}^0(Q)$ is a quaternion algebra over F (defined by a universal property [Voi21, Exercise 5.20]); and we recover $Q = \text{nrd}|_{B^0}$ up to similarity as the reduced norm on the trace zero subspace. The construction of the even algebra extends naturally to R -lattices in V .

Theorem 5.7. *The association $\Lambda \mapsto \text{Clf}^0(\Lambda)$ of the even Clifford algebra to a lattice defines a functor from the category of*

R -lattices $\Lambda \subseteq V$, under similarities

to the category of

Gorenstein quaternion R -orders $O \subseteq B$, under isomorphisms

Moreover, the association is functorial with respect to ring homomorphisms $R \rightarrow R'$.

Proof. See Voight [Voi21, Theorems 22.2.11 and 22.3.1]. Restricting R to a Dedekind domain implies that every order is projective over R , and we obtain only Gorenstein orders [Voi21, Theorem 24.2.10] because our quadratic forms are necessarily primitive: we take the codomain of the quadratic module to be the R -submodule generated by the values of the quadratic form. \square

Corollary 5.8. *The even Clifford map gives a bijection between the set of twisted similarity classes of R -lattices $\Lambda \subseteq V$ and the set of isomorphism classes of Gorenstein R -orders $O \subseteq B$. Moreover, it induces a natural bijections*

$$\text{Cl}_{\text{GO}}(\Lambda)^{\text{Cl} R} \leftrightarrow \text{Typ } O$$

to the type set of $O = \text{Clf}^0(\Lambda)$.

By Equation (5.6), we similarly get a natural bijection

$$(5.9) \quad \text{Cl}_{\text{SO}}(\Lambda) \leftrightarrow \text{Typ } O.$$

Proof. For the first statement, apply Voight [Voi21, Main Theorem 22.5.7] with the same modifications as in the proof of Equation (5.7); an explicit inverse is also given (arising from the reduced norm). The second statement is Voight [Voi21, Corollary 22.5.12]. \square

Remark 5.10. Although it is not needed in what follows, the bijections in Equation (5.8) also follow naturally from an equivalence of categories, something which holds over a more general base ring: this is developed in Voight [Voi11, Theorem B]. Algorithmically it is most convenient to work with (5.9) as isometries are easier to compute, so we explain this associated equivalence of categories in Equation (A.39).

We now apply this to orthogonal modular forms. Recall [Voi21, Proposition 4.5.10] that there is an exact sequence

$$(5.11) \quad 1 \rightarrow F^\times \rightarrow B^\times \rightarrow \mathrm{SO}(\mathrm{nrd}|_{B^0}) \rightarrow 1$$

giving an isomorphism $B^\times/F^\times \simeq \mathrm{SO}(Q)(F)$ (and $Q \simeq \mathrm{nrd}|_{B^0}$). This extends integrally: for a lattice $\Lambda \subseteq V$, computing stabilizers gives

$$(5.12) \quad \mathrm{SO}(\Lambda)(R) \simeq N_{B^\times}(O)/F^\times$$

with $O := \mathrm{Clf}^0(\Lambda)$.

Let $\rho: \mathrm{SO}(V) \rightarrow \mathrm{GL}(W)$ be a finite-dimensional representation. Via (5.11) we can lift to get a representation $\rho: B^\times \rightarrow \mathrm{GL}(W)$ whose restriction to F^\times is trivial, i.e., has trivial central character.

Recalling the Atkin–Lehner group $\mathrm{AL}(\widehat{O})$ in (4.2), we have the following result.

Theorem 5.13. *The even Clifford map induces a Hecke-equivariant bijection*

$$M_W(\mathrm{SO}(\widehat{\Lambda})) \xrightarrow{\sim} M_W(\widehat{O}^\times)^{\mathrm{AL}(\widehat{O})}$$

that restricts to a Hecke-equivariant bijection cuspidal subspaces

$$S_W(\mathrm{SO}(\widehat{\Lambda})) \xrightarrow{\sim} S_W(\widehat{O}^\times)^{\mathrm{AL}(\widehat{O})}.$$

Proof. From Equation (5.8), we have a bijection $\mathrm{Cl}\Lambda \leftrightarrow \mathrm{Typ} O$; from Equation (5.7) (restricting to oriented isometries), it is functorial with respect to the Hecke operators. The constant functions and inner product are preserved by this map, so the result restricts to their orthogonal complements, the cuspidal subspaces. \square

Equation (5.13) applies to a general ternary lattice with arbitrary weight, yielding a general (Gorenstein) quaternion order. Looking towards our application, where we restrict our classes of orders to those which are residually unramified, we characterize the corresponding lattices.

Lemma 5.14. *Let Λ be a ternary R -lattice. Then the following are equivalent.*

- (i) *The discriminant module Λ^\sharp/Λ is a cyclic R -module;*
- (ii) *For all (nonzero) primes $\mathfrak{p} \subseteq R$ we have*

$$(5.15) \quad \Lambda_{\mathfrak{p}} \simeq U_{\mathfrak{p}} \oplus R_{\mathfrak{p}}z$$

where $U_{\mathfrak{p}}$ is nonsingular (i.e., $\mathrm{disc}(U_{\mathfrak{p}}) \in R_{\mathfrak{p}}^\times/R_{\mathfrak{p}}^{\times 2}$); and

- (iii) *$\mathrm{Clf}^0(\Lambda)$ is residually unramified at all primes \mathfrak{p} .*

Proof. The equivalences of (i) and (ii) are almost immediate: for odd primes \mathfrak{p} , the condition in (ii) is equivalent to the rank of the reduction of Q modulo \mathfrak{p} (defined on $\Lambda/\mathfrak{p}\Lambda$) being at least 2, but when \mathfrak{p} is even we are asking further that the reduction is nonsingular. The equivalence (ii) \Leftrightarrow (iii) is given in Voight [Voi21, 24.3.9]. \square

6. THE RADICAL CHARACTER

We keep notations as in previous section: in particular, let $\Lambda \subset V$ be a definite ternary R -lattice of discriminant \mathfrak{N} , and let $O = \mathrm{Clf}^0(\Lambda)$ be its even Clifford algebra, an R -order in $B = \mathrm{Clf}^0(V)$.

Let $\mathfrak{p} \mid \mathfrak{N}$. We define the *radical* of $\Lambda_{\mathfrak{p}}$ as

$$(6.1) \quad \mathrm{rad}(\Lambda_{\mathfrak{p}}) := \{x \in \Lambda_{\mathfrak{p}} : T(x, y) \equiv 0 \pmod{2\mathfrak{N}} \text{ for all } y \in \Lambda_{\mathfrak{p}}\}.$$

The name is justified, as this recovers the usual radical of a quadratic space when the discriminant is 0.

We see that $\text{rad}_{\mathfrak{p}}(\Lambda)$ is a $R_{\mathfrak{p}}$ -lattice with $\text{rad}(\Lambda_{\mathfrak{p}}) \supseteq 2\mathfrak{N}\Lambda_{\mathfrak{p}}$.

Proposition 6.2. *If $\Lambda_{\mathfrak{p}}$ has cyclic discriminant, then $\text{rad}(\Lambda_{\mathfrak{p}})/(2\mathfrak{N}\Lambda_{\mathfrak{p}})$ is free of rank 1 over $R_{\mathfrak{p}}/2\mathfrak{N}R_{\mathfrak{p}}$.*

Proof. We apply Equation (5.14), (i) \Rightarrow (ii): it is generated by z , since $Q(z) \equiv 0 \pmod{\mathfrak{N}}$ and hence $T(z, z) = 2Q(z) \equiv 0 \pmod{2\mathfrak{N}}$; see also [DPRT24, Lemma 6.13]. \square

Since it is defined by the bilinear form, $\text{rad}(\Lambda_{\mathfrak{p}})$ is invariant under $O(\Lambda_{\mathfrak{p}})$, hence we obtain a character

$$(6.3) \quad \nu_{\mathfrak{p}}: \text{SO}(\widehat{\Lambda}) \rightarrow \text{SO}(\Lambda_{\mathfrak{p}}) \rightarrow O(\text{rad}_{\mathfrak{p}}(\Lambda)/2\mathfrak{N}\Lambda_{\mathfrak{p}}) \simeq (R_{\mathfrak{p}}/2\mathfrak{N}R_{\mathfrak{p}})^{\times}$$

which we call the *radical character* at \mathfrak{p} .

Lemma 6.4. *The image of the radical character $\nu_{\mathfrak{p}}$ is $\{\pm 1\}$, and it is uniquely defined by*

$$\sigma(z) \equiv \nu_{\mathfrak{p}}(\sigma)z \pmod{2\mathfrak{p}\Lambda}$$

for $\sigma \in \text{SO}(\Lambda_{\mathfrak{p}})$.

Proof. For the first statement, we have a (noncanonical) splitting $\Lambda_{\mathfrak{p}} \simeq U_{\mathfrak{p}} \oplus R_{\mathfrak{p}}z$ in Equation (5.14)(ii) with $z \in \text{rad}(\Lambda_{\mathfrak{p}})$. Let $\sigma \in \text{SO}(\Lambda_{\mathfrak{p}})$. Then from (6.3) we have $\sigma(z) = az + y$ with $a \in R_{\mathfrak{p}}^{\times}$ and $y \in 2\mathfrak{N}\Lambda_{\mathfrak{p}}$. Without loss of generality, we may suppose that $y \in 2\mathfrak{N}U_{\mathfrak{p}}$. Then $Q(z) = Q(\sigma z) = a^2Q(z) + Q(y) \equiv a^2Q(z) \pmod{4\mathfrak{N}^2}$ since $y \in 2\mathfrak{N}U_{\mathfrak{p}}$. Since $\text{ord}_{\mathfrak{p}}Q(z) = \text{ord}_{\mathfrak{p}}\mathfrak{N}$, we conclude that $a^2 \equiv 1 \pmod{4\mathfrak{N}}$, whence $a = \nu_{\mathfrak{p}}(\sigma) \equiv \pm 1 \pmod{2\mathfrak{N}}$. Composing a reflection in z with reflection in a vector in $U_{\mathfrak{p}}$ shows that the image is fully $\{\pm 1\}$, and this can already be seen modulo $2\mathfrak{p}$. \square

We extend the radical character multiplicatively, defining

$$(6.5) \quad \nu_{\mathfrak{M}} := \prod_{\mathfrak{p}|\mathfrak{M}} \nu_{\mathfrak{p}}: \text{SO}(\widehat{\Lambda}) \rightarrow \{\pm 1\}$$

for $\mathfrak{M} \mid \mathfrak{N}$ squarefree.

There is another character, the spinor norm character; we show these agree in odd exponent, as follows. Recall that the *spinor norm* is the map composition

$$(6.6) \quad \theta: \text{SO}(V) \simeq B^{\times}/F^{\times} \xrightarrow{\text{nr}} F^{\times}/F^{\times 2}.$$

We define the *spinor norm character* for $\mathfrak{M} \mid \mathfrak{N}$ by composing

$$(6.7) \quad \begin{aligned} \theta_{\mathfrak{M}}: \text{SO}(V) &\xrightarrow{\theta} F^{\times}/F^{\times 2} \rightarrow \{\pm 1\} \\ a &\mapsto \prod_{\mathfrak{p}|\mathfrak{M}} (-1)^{\text{ord}_{\mathfrak{p}}(a)}. \end{aligned}$$

We let $A := \langle \nu_{\mathfrak{M}} \rangle \simeq \prod_{\mathfrak{p}|\mathfrak{M}} C_2$ be the *radical character group*.

Proposition 6.8. *Suppose O is residually unramified. Then the following statements hold, under the isomorphism $\text{SO}(\widehat{\Lambda}) \xrightarrow{\sim} N_{\widehat{B}^{\times}}(\widehat{O})$ induced by the even Clifford map.*

(a) *The pairing*

$$(6.9) \quad \begin{aligned} A \times N_{\widehat{B}^{\times}}(\widehat{O}) &\rightarrow \{\pm 1\} \\ (\nu, \alpha) &\mapsto \nu(\alpha) \end{aligned}$$

is perfect.

(b) *If $\text{ord}_{\mathfrak{p}}\mathfrak{N}$ is odd, then $\nu_{\mathfrak{p}} = \theta_{\mathfrak{p}}$.*

Proof. First part (a). We computed $N_{B_p^\times}(O_p) = F_p^\times O_p^\times \langle w_p \rangle$ in Equation (4.12)(i). We now make that a bit more explicit. Writing

$$\Lambda_p = U_p \boxplus R_p z$$

we compute that

$$\mathrm{Clf}^0(\Lambda_p) = \mathrm{Clf}^0(U_p) \oplus U_p z.$$

Write $S_p := \mathrm{Clf}^0(U_p)$. Then S_p is unramified over R_p , either split or inert according as U_p is isotropic or anisotropic and according as $\mathfrak{p} \mid \mathfrak{N}_+$ or $\mathfrak{p} \mid \mathfrak{N}_-$. Abbreviate $J_p := U_p z$. Then $J_p = S_p j$ with $j^2 = b$ with $\mathrm{ord}_p(b) = \mathrm{ord}_p \mathfrak{N} = e$, and $j = w_p$.

Suppose first that $\alpha_p \in S_p^\times$. Then α_p commutes with z , since U_p is orthogonal to z . Similarly, suppose $\alpha_p = 1 + \beta_p \in 1 + J_p$. Then $\mathrm{Nm}(\alpha_p) = 1 - \beta_p^2$ with $\beta_p^2 \in \mathfrak{N}$, and $\beta_p z \in \mathfrak{N} \Lambda_p$. Hence

$$\begin{aligned} \alpha_p^{-1} z \alpha_p &= (1 + \beta_p)^{-1} (1 - \beta_p) z = \frac{(1 - \beta_p)^2}{1 - \beta_p^2} z \\ (6.10) \quad &\equiv \frac{1 + \beta_p^2}{1 - \beta_p^2} z - \frac{2\beta_p}{1 - \beta_p^2} z \equiv z \pmod{2\mathfrak{N} \Lambda_p} \end{aligned}$$

since $\beta_p^2 \equiv -\beta_p^2 \pmod{2\mathfrak{N}}$. This shows that ν_p is trivial on $O_p^\times = S^\times \cdot (1 + J_p)$. Thus it must be nontrivial on j , and indeed we quickly verify that $j^{-1} z j = j^{-1}(-j)z = -z$.

This shows that the radical character on the normalizer is simply the projection onto

$$(6.11) \quad N_{B_p^\times}(O_p)/F_p^\times \rightarrow N_{B_p^\times}(O_p)/(F_p^\times O_p^\times) \simeq \langle w_p \rangle \simeq \{\pm 1\}.$$

Part (a) follows directly.

For part (b), since $\mathrm{ord}_p \mathfrak{N} = \mathrm{ord}_p(b) = \mathrm{nrd}(j)$ is odd, the map in (6.11) is also exactly described by the spinor norm character θ_p in (6.7). (And this does not hold when $\mathrm{ord}_p \mathfrak{N}$ is even, in that case $\theta_p = 1$) \square

Corollary 6.12. *Let $\mathfrak{M} \mid \mathfrak{N}$ be squarefree, and let $\varepsilon_{\mathfrak{M}}$ be the sign vector with $(\varepsilon_{\mathfrak{M}})_p = -1$ if and only if $\mathfrak{p} \mid \mathfrak{M}$. Suppose that O is residually unramified. Then there is a Hecke-equivariant bijection*

$$(6.13) \quad M_k(\mathrm{SO}(\widehat{\Lambda}), \nu_{\mathfrak{M}}) \xrightarrow{\sim} M_k(\widehat{O}^\times)^{\varepsilon_{\mathfrak{M}}}$$

where the image is the space of forms where the Atkin–Lehner operators have signs agreeing with $\varepsilon_{\mathfrak{M}}$. The map (6.13) restricts to a similar bijection on cuspidal subspaces.

Proof. We apply Equation (5.13) and identify the fixed subspace for the characters using Equation (6.8). \square

7. NEWFORM THEORY FOR ORTHOGONAL MODULAR FORMS

In this section, we translate the degeneracy maps and newform theory provided in section 4 to the orthogonal side. This upgrades Equation (6.12) to a statement about newforms, and it explains the multiplicities of oldforms observed over $F = \mathbb{Q}$ by Birch [Bir91, pp. 202–203].

The degeneracy maps on the quaternion (and Hilbert) side are of the following form. Whenever we have $O \subseteq O'$, equivalently $\widehat{O} \subseteq \widehat{O}'$, we get a natural surjective map of

pointed sets

$$(7.1) \quad \begin{array}{c} B^\times \backslash \widehat{B}^\times / N_{\widehat{B}^\times}(\widehat{O}) = \text{Typ}(O) \\ \downarrow \\ B^\times \backslash \widehat{B}^\times / N_{\widehat{B}^\times}(\widehat{O}') = \text{Typ}(O'). \end{array}$$

Described in terms of type sets, given a order locally isomorphic to O , its adelization is $\widehat{\alpha}^{-1}\widehat{O}\widehat{\alpha}$; the map then makes the order $\widehat{\alpha}^{-1}\widehat{O}'\widehat{\alpha}$ which when intersected with B gives an order locally isomorphic to O' .

But we have already identified these double cosets (and type sets) using the even Clifford functor (5.9): corresponding to \widehat{O}' is an adelic lattice $\widehat{\Lambda}' \subseteq \widehat{V}$ and lattice $\Lambda' = \widehat{\Lambda}' \cap V \subseteq V$, giving again a map of pointed sets

$$(7.2) \quad \begin{array}{ccc} \text{Cl}(\Lambda) = \text{SO}(V) \backslash \text{SO}(\widehat{V}) / \text{SO}(\widehat{\Lambda}) & \longleftrightarrow & B^\times \backslash \widehat{B}^\times / N_{\widehat{B}^\times}(\widehat{O}) = \text{Typ}(O) \\ \downarrow & & \downarrow \\ \text{Cl}(\Lambda') = \text{SO}(V) \backslash \text{SO}(\widehat{V}) / \text{SO}(\widehat{\Lambda}') & \longleftrightarrow & B^\times \backslash \widehat{B}^\times / N_{\widehat{B}^\times}(\widehat{O}') = \text{Typ}(O') \end{array}$$

(We do not claim that $\widehat{\Lambda} \subseteq \widehat{\Lambda}'$, only that $\text{SO}(\widehat{\Lambda}) \leq \text{SO}(\widehat{\Lambda}')$.) On the level of class sets, the map is described in a similar way to the quaternionic case: for a lattice which is locally isometric to Λ its adelization is $\widehat{g}\widehat{\Lambda}$, we make the adelic lattice $\widehat{g}\widehat{\Lambda}'$ and then intersect with V to get a lattice locally isometric to Λ' .

Orthogonal and quaternionic modular forms are defined by equivariant maps on these sets. The degeneracy operators on quaternionic modular forms commute with

$$(7.3) \quad \alpha_{\Lambda'}: M_W(\text{SO}(\widehat{\Lambda}')) \hookrightarrow M_{W'}(\text{SO}(\widehat{\Lambda}))$$

via pullback. These maps give an old and new subspace as usual.

Definition 7.4. The *old subspace* $M_W^{\text{old}}(\text{SO}(\widehat{\Lambda})) \subseteq M_W(\text{SO}(\widehat{\Lambda}))$ is the span of the image of all degeneracy maps $\alpha_{\Lambda'}$ for lattices Λ' corresponding to superorders $O' \supseteq O$. The *new subspace* $M_W^{\text{new}}(\text{SO}(\widehat{\Lambda})) \subseteq M_W(\text{SO}(\widehat{\Lambda}))$ is the orthogonal complement of the old subspace with respect to the Petersson inner product.

Theorem 7.5. *If O is residually unramified, then there is a Hecke-equivariant bijection*

$$M_k^{\text{new}}(\text{SO}(\widehat{\Lambda}), \nu_{\mathfrak{M}}) \xrightarrow{\sim} M_k^{\text{new}}(\widehat{O})^{\varepsilon_{\mathfrak{M}}}$$

that restricts to the cuspidal subspaces.

Proof. We restrict Equation (6.12) to the new subspace on quaternionic modular forms; by definition, this corresponds to the new subspace on orthogonal modular forms. \square

8. ORTHOGONAL ALGORITHMS

A general reference for algorithms on orthogonal modular forms on lattices is Greenberg–Voight [GV14]. Further practical improvements are given by Assaf–Fretwell–Ingalls–Logan–Secord–Voight [AFI+22, §3].

We advance these algorithms with the following additions. First, we construct a ternary quadratic space with cyclic discriminant module given invariants, as follows.

Algorithm 8.1. *Given as input*

- a totally real field F ,

- a factored ideal $\mathfrak{N} = \prod_{i=1}^r \mathfrak{p}_i^{e_i}$ of $R = \mathbb{Z}_F$,
- a divisor $\mathfrak{N}_- \mid \mathfrak{N}$ such that if $\mathfrak{p}^e \parallel \mathfrak{N}_-$ then e is odd, and
- a squarefree divisor $\mathfrak{D} \mid \mathfrak{N}_-$ whose number of prime divisors has the same parity as $[F : \mathbb{Q}]$;

we return as output a residually unramified order O in a suitable quaternion algebra of discriminant \mathfrak{D} .

1. Compute a totally definite quaternion algebra B of discriminant \mathfrak{D} [GV14, Algorithm 4.1].
2. Compute a maximal order $O \subseteq B$ [Voi13, §7].
3. Compute an Eichler order $O_1 \subseteq O$ of level $\mathfrak{N}_+ := \mathfrak{N}/\mathfrak{N}_-$ by computing a \mathfrak{p} -matrix ring for all $\mathfrak{p} \mid \mathfrak{N}_+$ [Voi13, Corollary 7.13] and taking the preimage of the standard Eichler order.
4. Compute $O_2 \subseteq O_1$ residually inert for $\mathfrak{p} \mid \mathfrak{D}$, for each prime \mathfrak{p} :
 - a. Compute $J_{\mathfrak{p}} := \text{rad}(O_{\mathfrak{p}}) = [O_{\mathfrak{p}}, O_{\mathfrak{p}}]$.
 - b. Lift a basis of the quotient $O_{\mathfrak{p}}/J_{\mathfrak{p}}$ to $S_{\mathfrak{p}}$.
 - c. Take $O_{2,\mathfrak{p}} = S_{\mathfrak{p}} + J_{\mathfrak{p}}^{(e+1)/2}$ for $\mathfrak{p}^e \parallel \mathfrak{N}_-$ (with e odd).
5. Compute $O_3 \subseteq O_2$ residually inert for $\mathfrak{p} \mid \mathfrak{N}_-$ but $\mathfrak{p} \nmid \mathfrak{D}$:
 - a. Compute a \mathfrak{p} -matrix ring $O_{\mathfrak{p}} \simeq M_2(R_{\mathfrak{p}})$.
 - b. Compute $S_{\mathfrak{p}}$, the valuation ring in the quadratic unramified extension $K_{\mathfrak{p}} \supseteq F_{\mathfrak{p}}$.
 - c. By the regular representation, compute $S_{\mathfrak{p}} \hookrightarrow M_2(R_{\mathfrak{p}})$ and identify $S_{\mathfrak{p}}$ with its preimage in $O_{\mathfrak{p}}$. Compute $O'_{\mathfrak{p}} = S_{\mathfrak{p}} + \mathfrak{p}O_{\mathfrak{p}}$, let $J_{\mathfrak{p}} = \text{rad}(O'_{\mathfrak{p}})$, and take $O'_{3,\mathfrak{p}} = S_{\mathfrak{p}} + J_{\mathfrak{p}}^{e/2}$.
6. Return O_3 .

Theorem 8.2. Equation (8.1) returns correct output and runs in probabilistic polynomial time.

Proof. Steps 1–3 run in probabilistic polynomial time by the references given. (See in particular Voight [Voi13] for a discussion of exact global representations for \mathfrak{p} -adic computations.) In steps 4 and 5 we have only linear algebra steps other than finding an irreducible quadratic polynomial over $\mathbb{F}_{\mathfrak{p}}$, which can be found in probabilistic polynomial time. \square

To compute spaces of orthogonal modular forms with radical character, there is no trouble computing the radical character: part of the above suite of algorithms efficiently computes a \mathfrak{p} -splitting as in (5.15), and from there we just compute the action on the radical generator z (by matrix multiplication).

In the special case where the radical character is given spinor norm (when $\text{ord}_{\mathfrak{p}} \mathfrak{N}$ is odd, Equation (6.12)), we have the following extraordinary formula.

Lemma 8.3. Let V be a finite-dimensional nondegenerate quadratic space over a field k with $\text{char } k \neq 2$. Let $\sigma \in \text{SO}(V)$ have $\det(1 + \sigma) \neq 0$. Then the spinor norm of σ is

$$\theta(\sigma) = \det((1 + \sigma)/2) = 2^n \det(1 + \sigma) \in k^{\times}/k^{\times 2}.$$

If further $n = 3$, then $\theta(\sigma) = 1 + \text{tr}(\sigma)$.

Proof. See Zassenhaus [Zas62, Theorem, Corollary, p. 446], who actually shows one you can define the spinor norm this way (without the Clifford algebra). For completeness, we give a direct proof in the case $n = 3$.

The case $\sigma = \text{id}_V$ is immediate. By the Cartan–Dieudonné theorem, $\sigma = \tau_u \tau_v$ is a product of reflections where $u, v \in V$ are not colinear, where

$$\tau_u(x) = x - \frac{T(x, u)}{Q(u)}u$$

(and similarly for v). Let $w \in V$ be orthogonal to u and v , so that $\{u, v, w\}$ is a basis of V .

We compute σ in this basis:

$$\begin{aligned}\sigma(u) &= \tau_u \left(u - \frac{T(u, v)}{Q(v)}v \right) = -u - \frac{T(u, v)}{Q(v)} \left(v - \frac{T(v, u)}{Q(u)}u \right) \\ &= \left(\frac{T(u, v)^2}{Q(u)Q(v)} - 1 \right) u - \frac{T(u, v)}{Q(v)}v \\ \sigma(v) &= \tau_u(-v) = \frac{T(v, u)}{Q(u)}u - v \\ \sigma(w) &= w\end{aligned}$$

Hence

$$\det(1 + \sigma) = \frac{T(u, v)^2}{Q(u)Q(v)}$$

and

$$\text{tr}(\sigma) = \frac{T(u, v)^2}{Q(u)Q(v)} - 1,$$

and the claim follows since $\theta(\sigma) = Q(u)Q(v) \in k^\times/k^{\times 2}$. \square

For completeness, when $\text{tr}(\sigma) = -1$, we can still do something nice.

Corollary 8.4. *If $\sigma \in \text{SO}(V)$ with $\dim_k V = 3$ has $\text{tr}(\sigma) = -1$, then $\sigma^2 = \text{id}_V$ and $\ker(\sigma - 1) = kw$ for some nonzero $w \in V$ and $\theta(\sigma) = Q(w)$.*

Proof. If $\text{tr}(\sigma) = -1$ then $\sigma = \tau_u \cdot \tau_v$ with $T(u, v) = 0$, so taking the orthogonal complement we find an orthogonal basis $\beta = \{u, v, w\}$ for V such that $[\sigma]_\beta = \text{diag}(-1, -1, 1)$ is diagonal, and in particular $\sigma^2 = 1$ and $\ker(\sigma - 1) = kw$. Since the spinor norm of σ is by definition $\theta(\sigma) = Q(u)Q(v) \in k^\times/k^{\times 2}$ and the discriminant of Q is $\text{disc } Q = 4Q(u)Q(v)Q(w)$, the result holds. \square

To find a vector w with $\sigma(w) = w$ as in Equation (8.4), better than computing a kernel, we see that since σ is an involution, we can take $w := v + \sigma(v)$ for any $v \in V$ whenever $w \neq 0$. Since $\sigma \neq -1$, we need only try v in a basis for V .

We conclude with a runtime analysis, which we state in more generality.

Theorem 8.5. *There exists an explicit algorithm that, given as input a totally positive definite ternary quadratic space V over a totally real number field F with $n = [F : \mathbb{Q}]$, an R -lattice $\Lambda \subset V$, a nonzero prime ideal $\mathfrak{p} \subset R$, computes the Hecke operator $T_{\mathfrak{p}}$ using*

$$\tilde{\mathcal{O}}(\text{Nm}(\mathfrak{p})H_{3n}(\|\Lambda\|d^2))$$

bit operations, where $\|\Lambda\|$ denotes the number of bits required to encode Λ , $d = \#\text{Cl } \Lambda$, and H_{3n} is a polynomial that determines the number of bit operations to compute a Hermite normal form of a matrix in $M_{3n}(\mathbb{Z})$.

Proof. The algorithm is specified in [GV14, §6]; we focus on the ternary case. We first enumerate the points of the projective conic $Q_\Lambda(x, y, z) \equiv 0 \pmod{\mathfrak{p}}$ corresponding to isotropic lines, which can be done in time $\tilde{O}(Nm(\mathfrak{p}))$ by looping over values of $x \in \mathbb{F}_\mathfrak{p}$ and computing roots. In a fixed number of operations we can compute a hyperbolic complement, compute generators for the neighbor, and then we compute a Hermite normal form over \mathbb{Z} which by assumption has complexity $O(H_{3n}(\|\Lambda\|))$. Finally, we account for the isometry testing for the lattice projected to \mathbb{Z} which occurs at a complexity of $O((3n)^{O(3n)})$ by work of Haviv–Regev [HR14]: we treat V as a \mathbb{Q} -vector space with additional bilinear forms. \square

9. IMPLEMENTATION AND EXAMPLES

This algorithm has been implemented in Magma [BCP97] over a general totally real field (in arbitrary rank), as reported by Assaf–Fretwell–Ingalls–Logan–Secord–Voight [AFI+22].

We also implemented an optimized version restricted to $F = \mathbb{Q}$ and N squarefree, written in C++ and available online [Hei24]. On a standard desktop we can compute all rational newforms with squarefree conductor $N < 15\,000$ and their Hecke eigenvalues for all $p < 1000$ in just 25 minutes!

Example 9.1. For level $N = 1\,062\,347 = 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 = N_-$ so $N_+ = 1$ and hence we directly get the space of newforms, using Equation (8.1) we find the ternary form

$$Q(x, y, z) = x^2 + 187y^2 + 1467z^2 - 187xz$$

with $\# \text{Cl}(\Lambda) = 2016$.

Given Q , we can compute the Hecke matrices $[T_2], [T_3], [T_5], [T_7]$ for *all* radical (spinor) characters, giving all newforms, in 4 seconds on a standard desktop machine. Then 1 minute of linear algebra computing kernels with sparse matrices in Magma following methods in Cremona [Cre97, §2.7] gives that there are exactly 5 elliptic curves with conductor N .

The same computation with modular symbols Magma crashed after consuming all 24 GB of available memory!

The excellent performance in Equation (9.1) suggests that this method would be an effective method to get a “random” isogeny class of elliptic curves of moderately large conductor.

APPENDIX A. A FUNCTORIAL INVERSE TO THE EVEN CLIFFORD MAP

In section 5, we saw that the even Clifford functor associates to a nondegenerate ternary quadratic module a quaternion R -order, giving a bijection from twisted isometry classes of lattices to isomorphism classes of orders and inducing a bijection on class sets. In this appendix, we upgrade this to an equivalence of categories extending work of Voight [Voi11, Theorem B].

Throughout the appendix, let R be a (commutative) domain with $F := \text{Frac } R$. (The argument generalizes to an arbitrary base, but we keep this hypothesis in line with the paper and to simplify a few arguments.) The even Clifford functor associates to a nondegenerate ternary quadratic module a quaternion R -order. We show how to do the converse, furnishing a functorial inverse to the Clifford functor. The construction is due to Voight [Voi11, §2], following Bhargava [Bha04b] (who considered the case of commutative rings of rank 4) and a footnote of Gross–Lucianovic [GL09, Footnote 2].

Let $O \subset B$ be an R -order in a quaternion algebra B over F which is projective as an R -module.

Proposition A.1. *O/R is projective of rank 3 as an R -module, and there exists a unique quadratic map*

$$\psi = \psi_O : \Lambda^2(O/R) \rightarrow \Lambda^4 O$$

with the property that

$$(A.2) \quad \psi(x \wedge y) = 1 \wedge x \wedge y \wedge xy$$

for all $x, y \in O$.

Proof. See Voight [Voi11, Lemma 2.1]. □

The quadratic module $\psi_O : \Lambda^2(O/R) \rightarrow \Lambda^4 O$ in Equation (A.1) is called the *canonical exterior form* of O .

Proposition A.3. *The association $O \mapsto \psi_O$ yields a functor from the category of projective quaternion orders over R , under isomorphisms to the category of*

ternary quadratic modules, under similarity.

Proof. An isomorphism $\phi : O \rightarrow O'$ of quaternion R -orders induces a similarity

$$\begin{array}{ccc} \Lambda^2(O/R) & \xrightarrow{\psi} & \Lambda^4 O \\ \wr \downarrow \wedge^2 \phi & & \wr \downarrow \wedge^4 \phi \\ \Lambda^2(O'/R) & \xrightarrow{\psi'} & \Lambda^4 O' \end{array}$$

because for all $x, y \in O$ we have

$$\begin{aligned} (\wedge^4 \phi)(\psi(x \wedge y)) &= 1 \wedge \phi(x) \wedge \phi(y) \wedge \phi(xy) \\ (A.4) \quad &= 1 \wedge \phi(x) \wedge \phi(y) \wedge \phi(x)\phi(y) \\ &= \psi'(\phi(x) \wedge \phi(y)) = \psi'((\wedge^2 \phi)(x \wedge y)) \end{aligned}$$

as desired. □

Example A.5. Suppose that O is free with a good basis $1, i, j, k$ [Voi21, 22.4.7] and multiplication laws

$$(A.6) \quad \begin{aligned} i^2 &= ui - bc & jk &= a\bar{i} \\ j^2 &= vj - ac & ki &= b\bar{j} \\ k^2 &= wk - ab & ij &= c\bar{k}. \end{aligned}$$

We now compute the canonical exterior form [Voi11, Example 2.5]

$$\psi = \psi_O : \Lambda^2(O/R) \rightarrow \Lambda^4 O.$$

We choose bases, with

$$\Lambda^2(O/R) \xrightarrow{\sim} R(j \wedge k) \oplus R(k \wedge i) \oplus R(i \wedge j) = Re_1 \oplus Re_2 \oplus Re_3$$

and the generator $-1 \wedge i \wedge j \wedge k$ for $\Lambda^4 O$.

With these identifications, the canonical exterior form $\psi : R^3 \rightarrow R$ has

$$\psi(e_1) = \psi(j \wedge k) = 1 \wedge j \wedge k \wedge jk = 1 \wedge j \wedge k \wedge (-ai) = a(-1 \wedge i \wedge j \wedge k)$$

and

$$\begin{aligned}\psi(e_1 + e_2) - \psi(e_1) - \psi(e_2) &= \psi(k \wedge (i - j)) - \psi(j \wedge k) - \psi(k \wedge i) \\ &= -1 \wedge k \wedge j \wedge ki - 1 \wedge k \wedge i \wedge kj \\ &= -w(1 \wedge k \wedge i \wedge j) = w(-1 \wedge i \wedge j \wedge k).\end{aligned}$$

Continuing in this way, we see that

$$\psi(x(j \wedge k) + y(k \wedge i) + z(i \wedge j)) = Q(xe_1 + ye_2 + ze_3) = Q(x, y, z)$$

with

$$(A.7) \quad Q(x, y, z) = ax^2 + by^2 + cz^2 + uyz + vxz + wxy,$$

so that

$$(A.8) \quad \text{Clf}^0(\psi_O) \simeq O.$$

Therefore ψ furnishes an inverse to the map in Equation (5.7) when R is a PID. In particular, we have obtained the *same* quadratic form as constructed from the reduced norm [Voi21, Proposition 22.4.12], so

$$(A.9) \quad N \text{ nrd}(O^\sharp) \sim \psi_O.$$

Example A.10. Suppose that R is a Dedekind domain with field of fractions F . Then there is a good pseudobasis for O

$$(A.11) \quad O = R \oplus \mathfrak{a}i \oplus \mathfrak{b}j \oplus \mathfrak{c}k.$$

The canonical exterior form of O , by the same argument as in Equation (A.5) but keeping track of scalars, is given by

$$\psi_O: \mathfrak{b}ce_1 \oplus \mathfrak{a}ce_2 \oplus \mathfrak{a}be_3 \rightarrow \mathfrak{a}bc$$

under the identification

$$(A.12) \quad \begin{aligned} \bigwedge^4 O &\xrightarrow{\sim} \mathfrak{a}bc \\ 1 \wedge i \wedge j \wedge k &\mapsto -1; \end{aligned}$$

we again have

$$\psi_O(xe_1 + ye_2 + ze_3) = ax^2 + by^2 + cz^2 + uyz + vxz + wxy$$

as in (A.7), but now with x, y, z are restricted to their respective coefficient ideals.

The even Clifford algebra and the canonical exterior form carry with them one global property (Steinitz class) that must be taken into account before we obtain an equivalence of categories. Briefly, in addition to similarities one must also take into account twisted similarities, obtained not by a global map but by twisting by an invertible module.

Definition A.13. A quadratic module $d: P \rightarrow I$ with P, I projective of rank 1 is called a *twisting* quadratic module if the associated bilinear map $P \otimes P \rightarrow I$ is an R -module isomorphism.

Example A.14. The quadratic module $d: R \rightarrow R$ by $z \mapsto z^2$ is a (trivial) twisting.

If P is an invertible R -module, then the quadratic module

$$(A.15) \quad \begin{aligned} P &\rightarrow P^{\otimes 2} \\ z &\mapsto z \otimes z \end{aligned}$$

is twisting.

Definition A.16. Let $Q: M \rightarrow L$ be a quadratic module and let $d: P \rightarrow I$ be a twisting quadratic module. The *twist* of Q by d is the quadratic module

$$Q \otimes d: M \otimes P \rightarrow L \otimes I$$

$$x \otimes z \mapsto Q(x) \otimes d(z).$$

A *twisted similarity* between quadratic modules $Q: M \rightarrow L$ and $Q': M' \rightarrow L'$ is tuple (f, h, d) where $d: P \rightarrow I$ is a twisting quadratic module and (f, h) is a similarity between $Q \otimes d$ and Q' .

Example A.17. Let $Q: M \rightarrow L$ be a quadratic module and let $\mathfrak{a} \subseteq R$ be an invertible fractional ideal of R . Then $d: \mathfrak{a} \rightarrow \mathfrak{a}^2$ is twisting, and the twist of Q by \mathfrak{a} can be identified with

$$Q \otimes d: \mathfrak{a}M \rightarrow \mathfrak{a}^2L$$

$$zx \mapsto z^2Q(x).$$

If $\mathfrak{a} = aR$ is principal, then Q is similar to $Q \otimes d$ via the similarity (f, h) obtained by scaling by a . However, if \mathfrak{a} is not principal, then Q may not be similar to $Q \otimes d$.

Lemma A.18. *Let $Q: M \rightarrow L$ be a quadratic module and let $d: P \rightarrow I$ be twisting. Then there is a canonical isomorphism of R -algebras*

$$\mathrm{Clf}^0(Q) \xrightarrow{\sim} \mathrm{Clf}^0(Q \otimes d).$$

Proof. First, we have a canonical isomorphism

$$(A.19) \quad (M \otimes P) \otimes (M \otimes P) \otimes (L \otimes I)^\vee \xrightarrow{\sim} M \otimes M \otimes L^\vee$$

coming from rearranging, the canonical map $d: P \otimes P \rightarrow I$ followed by the evaluation map $I \otimes I^\vee \xrightarrow{\sim} R$. Now recall the definition of the even Clifford algebra $\mathrm{Clf}^0(Q)$ [Voi21, 22.2.1]:

$$\mathrm{Clf}^0(Q) = \mathrm{Ten}^0(M; L) / I^0(Q).$$

The canonical isomorphism (A.19) induces an isomorphism $\mathrm{Ten}^0(M \otimes P; L \otimes I)$ that maps $I^0(Q \otimes d) \xrightarrow{\sim} I^0(Q)$, and the result follows. \square

Theorem A.20. *Let R be a noetherian domain. Then the associations*

$$(A.21) \quad \left\{ \begin{array}{l} \text{Nondegenerate ternary} \\ \text{quadratic modules over } R \\ \text{up to twisted similarity} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{l} \text{Projective quaternion orders} \\ \text{over } R \text{ up to isomorphism} \end{array} \right\}$$

$$Q \mapsto \mathrm{Clf}^0(Q)$$

$$\psi_O \mapsto O$$

are mutually inverse, discriminant-preserving bijections that are also functorial with respect to R .

Before we begin the proof of the theorem, we need one preliminary lemma.

Lemma A.22. *Let M be a projective R -module of rank 3. Then there are canonical isomorphisms*

$$(A.23) \quad \bigwedge^3(\bigwedge^2 M) \xrightarrow{\sim} (\bigwedge^3 M)^{\otimes 2}$$

$$(A.24) \quad \bigwedge^2(\bigwedge^2 M) \xrightarrow{\sim} M \otimes \bigwedge^3 M.$$

Proof. The proof is a bit of fun with multilinear algebra [Voi11, Lemma 3.7]. To illustrate, we give the proof in the special case where M is completely decomposable $M = \mathfrak{a}e_1 \oplus \mathfrak{b}e_2 \oplus \mathfrak{c}e_3$ —so in particular the result holds when R is a Dedekind domain (and, more generally using the splitting principle). In this case, we have

$$\bigwedge^2 M \simeq \mathfrak{a}\mathfrak{b}(e_1 \wedge e_2) \oplus \mathfrak{a}\mathfrak{c}(e_1 \wedge e_3) \oplus \mathfrak{b}\mathfrak{c}(e_2 \wedge e_3)$$

and so

$$\bigwedge^3(\bigwedge^2 M) \simeq (\mathfrak{a}\mathfrak{b}\mathfrak{c})^2(e_1 \wedge e_2) \wedge (e_1 \wedge e_3) \wedge (e_2 \wedge e_3)$$

agreeing with

$$(\bigwedge^3 M)^{\otimes 2} \simeq (\mathfrak{a}\mathfrak{b}\mathfrak{c})^2(e_1 \wedge e_2 \wedge e_3)^{\otimes 2}$$

by rearranging the tensor in a canonical way. The second isomorphism follows similarly. \square

Proof of Equation (A.20). We have two functors, by Equation (5.7) and Equation (A.3), that are functorial with respect to the base ring R .

We now compose them. Let $Q: M \rightarrow L$ be a quadratic module with $O = \text{Clf}^0(Q)$, and consider its canonical exterior form $\psi: \bigwedge^2(O/R) \rightarrow \bigwedge^4 O$. As R -modules, we have canonically

$$(A.25) \quad O/R \simeq \bigwedge^2 M \otimes L^\vee.$$

By the isomorphism (A.24), we have as the domain of ψ the R -module

$$(A.26) \quad \begin{aligned} \bigwedge^2(O/R) &\simeq \bigwedge^2(\bigwedge^2 M \otimes L^\vee) \simeq \bigwedge^2(\bigwedge^2 M) \otimes (L^\vee)^{\otimes 2} \\ &\simeq M \otimes \bigwedge^3 M \otimes (L^\vee)^{\otimes 2} \end{aligned}$$

and as codomain we have by the canonical R -module isomorphism

$$\bigwedge^3(O/R) \xrightarrow{\sim} \bigwedge^4 O$$

and the isomorphism (A.23)

$$(A.27) \quad \begin{aligned} \bigwedge^4 O &\simeq \bigwedge^3(O/R) \simeq \bigwedge^3(\bigwedge^2 M \otimes L^\vee) \simeq \bigwedge^3(\bigwedge^2 M) \otimes (L^\vee)^{\otimes 3} \\ &\simeq (\bigwedge^3 M)^{\otimes 2} \otimes (L^\vee)^{\otimes 3}. \end{aligned}$$

Now we twist. Let

$$P := \bigwedge^3 M \otimes (L^\vee)^{\otimes 2}$$

and let $d: P^\vee \rightarrow (P^\vee)^{\otimes 2}$ be the natural twisting quadratic module. Then the twist $\psi \otimes d$ has domain and codomain canonically isomorphic to

$$(A.28) \quad \begin{aligned} \bigwedge^2(O/R) \otimes P^\vee &\simeq M \\ \bigwedge^4 O \otimes (P^\vee)^{\otimes 2} &\simeq L \end{aligned}$$

by (A.26)–(A.27) so we have a quadratic form $\psi_{\text{Clf}^0(Q)} \otimes d: M \rightarrow L$.

We show that the composition $Q \mapsto \text{Clf}^0(Q) = O \mapsto \psi_O$ is naturally isomorphic to the identity, via the twist d . But to do this (and show the induced maps are similarities), since the above construction is canonical, we can base change to F and check within the quadratic space $Q_F: V \rightarrow F$ where $V := M \otimes_R F$. Choosing a basis, we find that the composition is the identity by Equation (A.5).

We may then conclude that the map of sets in (A.21) is a well-defined bijection: functoriality shows that the map is well-defined and that both maps are injective, and the composition shows that it is surjective. \square

We now shift to isometries and upgrade the bijection to an equivalence of categories; this has Equation (2.15) as an immediate corollary.

Remark A.29. Over a field, we used orientations [Voi21, §4.5] to get an equivalence of categories: the crux of the problem being that the isometry $-1 : V \rightarrow V$ maps to the identity map on $\text{Clf}^0 V$ under the Clifford functor. However, -1 acts nontrivially on the odd Clifford module $\text{Clf}^1 V$, and the point of an orientation is to keep track of this action on piece of $\text{Clf}^1 V$ coming from the center. Restricting an orientation of V would also work here; but we add a different and more functorial structure on quaternion orders to allow for these extra morphisms.

Definition A.30. Let N be an invertible R -module. A *parity factorization* of N is a pair of invertible R -modules P, L and an isomorphism $p : N \xrightarrow{\sim} P^{\otimes 2} \otimes L$. If N has a parity factorization, we call it *paritized*.

An *isomorphism* (N, p) to (N', p') of paritized invertible R -modules is a pair of isomorphisms $N \simeq N', P \simeq P'$ such that the diagram

$$(A.31) \quad \begin{array}{ccc} N & \xrightarrow{p} & P^{\otimes 2} \otimes L \\ \downarrow \wr & & \downarrow \wr \\ N' & \xrightarrow{p'} & P'^{\otimes 2} \otimes L \end{array}$$

commutes.

We *do* want to fix the module L in order to work with isometries; this serves as an anchor for our construction.

Definition A.32. Let O be a quaternion R -order. Then O is *paritized* if O is equipped with a parity factorization of $\bigwedge^4 O$. An isomorphism of paritized quaternion orders is an isomorphism $\phi : O \simeq O'$ and an isomorphism of parity factorizations with the isomorphism $\bigwedge^4 O \simeq \bigwedge^4 O'$ given by $\wedge^4 \phi$.

Example A.33. Every invertible R -module N has the identity parity factorization, with $P = R$ and $L = N$; up to isomorphism, every other differs by a choice of isomorphism class of P . So parity factorizations can be thought of as factorizations according to parity inside $\text{Pic } R$.

Example A.34. The main example of a parity factorization comes from the even Clifford construction. Let $Q : M \rightarrow L$ be a nondegenerate ternary quadratic module. Let $O = \text{Clf}^0(Q)$, and let $P = \bigwedge^3 M \otimes (L^\vee)^{\otimes 2}$. Then by (A.27), we have a canonical parity factorization

$$(A.35) \quad p_Q : \bigwedge^4 O \simeq (\bigwedge^3 M)^{\otimes 2} \otimes (L^\vee)^{\otimes 3} \simeq P^{\otimes 2} \otimes L.$$

Lemma A.36. Let (O, p) be a paritized quaternion R -order. Then

$$\text{Aut}_R(O, p) \simeq \text{Aut}_R(O) \times \{\pm 1\}.$$

Proof. By definition, an automorphism of (O, p) is a pair of automorphisms (ϕ, h) with $\phi \in \text{Aut}_R(O)$ and $h \in \text{Aut}_R(P)$ such that the diagram

$$\begin{array}{ccc} \bigwedge^4 O & \xrightarrow{p} & P^{\otimes 2} \otimes L \\ \wedge^4 \phi \downarrow \wr & & \downarrow \wr \\ \bigwedge^4 O & \xrightarrow{p} & P^{\otimes 2} \otimes L \end{array}$$

commutes. The choice $\phi = \text{id}_O$ and $h = -1$ gives us an automorphism we denote by -1 . Since L is fixed, it plays no role in this part.

We claim that if $\phi \in \text{Aut}_R(O)$ is an R -algebra isomorphism, then there is a unique $h \in \text{Aut}_R(P)$ up to -1 such that $(\phi, h) \in \text{Aut}_R(O, p)$. We will prove this over each localization $R_{(\mathfrak{p})}$, including $R_{(0)} = F$: once we choose such an h over F , it follows that $\pm h \in \text{Aut}_{R_{(\mathfrak{p})}}(P_{(\mathfrak{p})})$ and hence by intersecting $h \in \text{Aut}_R(P)$. So we may suppose O is free with good basis and $P \simeq R$, and $\bigwedge^4 \phi$ acts by $\det \phi$; we want to show that $\det \phi = h^2$ is a square. This follows from [Voi21, 22.3.15]: we have $\phi = \text{adj}(\rho)$ where $\rho \in \text{GL}_3(R)$ is the action on the ternary quadratic module $M \simeq R^3$ associated to O , and $\det \phi = \det \text{adj}(\rho) = (\det \rho)^2$. \square

Example A.37. We recall the twist construction employed in (A.27) that we now define in the above terms. Let (O, p) be a paritized quaternion R -order, with the parity factorization

$$p: \bigwedge^4 O \xrightarrow{\sim} P^{\otimes 2} \otimes L.$$

Let $\psi_{O,p}: \bigwedge^2(O/R) \rightarrow \bigwedge^4 O$ be the canonical exterior form. We then define the quadratic module

$$(A.38) \quad \psi_{O,p} := p \circ \psi_O \otimes P^\vee: \bigwedge^2(O/R) \otimes P^\vee \rightarrow L$$

where p induces an isomorphism $\bigwedge^4 O \otimes (P^\vee)^{\otimes 2} \simeq L$.

We now have the following theorem.

Theorem A.39. *The associations*

$$\begin{aligned} Q &\mapsto (\text{Clf}^0(Q), p_Q) \\ \psi_{O,p} &\leftarrow (O, p) \end{aligned}$$

are functorial and provide a discriminant-preserving equivalence of categories between
nondegenerate ternary quadratic modules over R
under isometries

and

paritized projective quaternion R -orders under isomorphisms

that is functorial in R .

Proof. First, we show the associations are functorial. If $Q: M \rightarrow L$ and $Q': M' \rightarrow L$ are isometric (nondegenerate ternary) quadratic modules under $f: M \rightarrow M'$, then by functoriality of the even Clifford algebra, this induces an isomorphism $f: O \simeq O'$ and thereby an isomorphism

$$P = \bigwedge^3 M \otimes (L^\vee)^{\otimes 2} \simeq P' = \bigwedge^3 M' \otimes (L^\vee)^{\otimes 2}$$

and then of parity factorizations

$$(A.40) \quad \begin{array}{ccc} \bigwedge^4 O & \xrightarrow{p_Q} & P^{\otimes 2} \otimes L \\ \downarrow \wr & & \downarrow \wr \\ \bigwedge^4 O' & \xrightarrow{p_{Q'}} & P'^{\otimes 2} \otimes L \end{array}$$

Conversely, if (O, p) and (O', p') are isomorphic paritized quaternion R -orders under $\phi: O \rightarrow O'$ and $P \simeq P'$, then we get an isometry

$$(A.41) \quad \begin{array}{ccc} \bigwedge^2 O/R \otimes P^\vee & \xrightarrow{\psi_{O,p}} & L \\ \downarrow \wr & & \parallel \\ \bigwedge^2 O'/R \otimes (P')^\vee & \xrightarrow{\psi_{O',p'}} & L \end{array}$$

by Equation (A.3) (see (A.4)): the similitude factor is the identity by construction.

We now tackle the two compositions and show they are each naturally isomorphic to the identity. Let (O, p) be a paritized quaternion R -order. We first associate $(\psi_{O,p}, \text{id})$, and let $M = \bigwedge^2 O/R \otimes P^\vee$ be the domain of $\psi_{O,p}$. We then associate its even Clifford algebra. As R -modules, we have canonical isomorphisms

$$\begin{aligned}
\text{Clf}^0(\psi_{O,p}) &= R \oplus \bigwedge^2 M \otimes L^\vee = R \oplus \bigwedge^2(O/R \otimes P^\vee) \otimes L^\vee \\
&\simeq R \oplus \bigwedge^2(O/R) \otimes (P^{\otimes 2} \otimes L)^\vee \\
&\simeq R \oplus O/R \otimes \bigwedge^3(O/R) \otimes (P^{\otimes 2} \otimes L)^\vee \\
&\simeq R \oplus O/R
\end{aligned}
\tag{A.42}$$

where we have used (A.24) and in the last step we used the parity factorization p giving a natural isomorphism of the last piece to R . To check that the corresponding map is an R -algebra homomorphism, by functoriality we can do so over F , and we suppose that B is given by a good basis, and then the verification is as in (A.5). To finish, we show that the parity factorization is also canonically identified: we have

$$\begin{aligned}
\bigwedge^3 M \otimes (L^\vee)^{\otimes 2} &= \bigwedge^3(\bigwedge^2(O/R) \otimes P^\vee) \otimes (L^\vee)^{\otimes 2} \\
&\simeq \bigwedge^3(\bigwedge^3 O/R)^{\otimes 2} \otimes (P^\vee)^{\otimes 3} \otimes (L^\vee)^{\otimes 2} \simeq P
\end{aligned}$$

where now we use (A.23) and then again (twice) the parity factorization. Therefore we have a natural isomorphism of parity factorizations

$$\begin{array}{ccc}
\bigwedge^4 \text{Clf}^0(\psi_{O,p}) & \xrightarrow{p_{\psi_{O,p}}} & (\bigwedge^3 M \otimes L^\vee)^{\otimes 2} \otimes L \\
\downarrow \wr & & \downarrow \wr \\
\bigwedge^4 O & \xrightarrow{p} & P^{\otimes 2} \otimes L
\end{array}
\tag{A.43}$$

This completes the verification that the composition in this order is naturally isomorphic to the identity.

Now for the second composition. Let $Q: M \rightarrow L$ be a (nondegenerate ternary) quadratic module over R . We associate $O = \text{Clf}^0 Q$ and p_Q its parity factorization, and then ψ_{O,p_Q} . In (A.28), using (A.26)–(A.27), we showed that we had a natural isometry

$$\begin{array}{ccc}
\bigwedge^2 O/R \otimes P^\vee & \xrightarrow{\psi_{O,p_Q}} & L \\
f \downarrow \wr & & \parallel \\
M & \xrightarrow{Q} & L
\end{array}
\tag{A.44}$$

and this completes the proof. \square

REFERENCES

- [AFI+22] Eran Assaf, Dan Fretwell, Colin Ingalls, Adam Logan, Spencer Secord, and John Voight, *Definite orthogonal modular forms: computations, excursions, and discoveries*, Res. Number Theory **8**:70 (2022), 38 pages. [7](#), [37](#), [42](#)
- [BBB+21] Alex J. Best, Jonathan Bober, Andrew R. Booker, Edgar Costa, John Cremona, Maarten Derickx, David Lowry-Duda, Min Lee, David Roe, Andrew V. Sutherland, and John Voight, *Computing classical modular forms*, eds. Jennifer S. Balakrishnan, Noam Elkies, Brendan Hassett, Bjorn Poonen, Andrew V. Sutherland, and John Voight, Simons Symp., Springer, Cham, 2021, 131–213. [2](#)
- [Bha04b] Manjul Bhargava, *Higher composition laws. III. The parametrization of quartic rings*, Ann. of Math. (2) **159** (2004), no. 3, 1329–1360. [43](#)

- [Bir91] B.J. Birch, *Hecke actions on classes of ternary quadratic forms*, Computational number theory: proceedings of the colloquium on Computational Number Theory held at Kossuth Lajos University, Debrecen (Hungary, 1989), W. de Gruyter, Berlin, 1991, 191–212. [2](#), [8](#), [10](#), [36](#)
- [BSP91] Siegfried Böcherer and Rainer Schulze-Pillot, *Siegel modular forms and theta series attached to quaternion algebras*, Nagoya Math. J. **121** (1991), 35–96. [23](#)
- [BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), vol. 3–4, 235–265. [7](#), [42](#)
- [Cow22] Alex Cowan, *Computing newforms using supersingular isogeny graphs*, Res. Number Theory **8** (2022), no. 4, Paper No. 96, 23 pp. [14](#)
- [Cre97] J.E. Cremona, *Algorithms for modular elliptic curves*, 2nd. ed., Cambridge University Press, Cambridge, 1997. [43](#)
- [DPRT24] Neil Dummigan, Ariel Pacetti, Gustavo Rama, and Gonzalo Tornara, *Quinary forms and paramodular forms*, Math. Comp. **93** (2024), no. 348, 1805–1858. [32](#)
- [Eic74] Martin Eichler, *Quadratische Formen und orthogonale Gruppen*, second ed., Grundlehren Math. Wiss., vol. 63, Springer-Verlag, Berlin-New York, 1974. [2](#)
- [DV13] Lassina Dembele, *Explicit methods for Hilbert modular forms*, Elliptic curves, Hilbert modular forms and Galois deformations, Birkhauser, Basel, 2013, 135–198. [6](#)
- [Eis1853] G. Eisenstein, *Tabelle der reducirten positiven ternaren quadratischen Formen, nebst den Resultaten neuer Forschungen uber diese Formen, in besonderer Rucksicht auf ihre tabellarische Berechnung*, J. Reine Angew. Math. **41** (1851), 141–190. [10](#)
- [GJ79] Stephen Gelbart and Herve Jacquet, *Forms of $GL(2)$ from the analytic point of view*, Automorphic forms, representations and L-functions (Corvallis, OR, 1977), vol. 1, eds. A. Borel and W. Casselman, Proc. Sympos. Pure Math. **33**, Amer. Math. Soc., Providence, RI, 1979, 213–251. [22](#), [23](#)
- [GV14] Matthew Greenberg and John Voight, *Lattice methods for algebraic modular forms on classical groups*, Computations with modular forms, eds. Gebhard Boeckle and Gabor Wiese, Contrib. Math. Comput. Sci., vol. 6, Springer, Berlin, 2014, 147–179. [7](#), [37](#), [38](#), [41](#)
- [Gro88] Benedict H. Gross, *Local orders, root numbers, and modular curves*, Amer. J. Math. **110** (1988), no. 6, 1153–1182. [21](#)
- [Gro99] Benedict H. Gross, *Algebraic modular forms*, Isr. J. Math. **113** (1999), 61–93. [15](#), [16](#)
- [GL09] Benedict H. Gross and Mark W. Lucianovic, *On cubic rings and quaternion rings*, J. Number Theory **129** (2009), no. 6, 1468–1478. [43](#)
- [HR14] Ishay Haviv and Oded Regev, *On the lattice isomorphism problem*, Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms, ACM, New York, 2014, 391–404. [42](#)
- [Hei16] Jeffery Hein, *Orthogonal modular forms: an application to a conjecture of Birch, algorithms and computations*, PhD thesis, Dartmouth College, 2016. [3](#)
- [Hei24] Jeffery Hein, *ternary-birch*, <https://github.com/jefferyphein/ternary-birch>, accessed 26 June 2024. [7](#), [42](#)
- [Hid81] Haruzo Hida, *On abelian varieties with complex multiplication as factors of the Jacobians of Shimura curves*, Amer. J. of Math. **103** (1981), no. 4, 727–776. [22](#)
- [JL70] Herve Jacquet and Robert P. Langlands, *Automorphic forms on $GL(2)$* , Lect. Notes in Math., vol. 114, Springer-Verlag, Berlin, 1970. [22](#), [23](#)
- [Kne57] Martin Kneser, *Klassenzahlen definiter quadratischer Formen*, Arch. Math. **8** (1957), 241–250. [9](#)
- [Mar18] Kimball Martin, *Refined dimensions of cusp forms, and equidistribution and bias of signs*, J. Number Theory **188** (2018), 1–17. [4](#)
- [Mar20] Kimball Martin, *The basis problem revisited*, Trans. Amer. Math. Soc. **373** (2020), no. 7, 4523–4559. [21](#), [22](#)
- [Piz77] Arnold Pizer, *The action of the canonical involution on modular forms of weight 2 on $\Gamma_0(M)$* , Math. Ann. **226** (1977), no. 2, 99–116. [20](#)
- [Pon81] Paul Ponomarev, *Ternary quadratic forms and Shimura’s correspondence*, Nagoya Math. J. **81** (1981), 123–151. [2](#)
- [RS07] Brooks Roberts and Ralf Schmidt, *Local newforms for $GSp(4)$* , Lect. Notes in Math., vol. 1918, Springer, Berlin, 2007. [24](#), [25](#)
- [Sch97] Alexander Schiemann, *Ternary positive definite quadratic forms are determined by their theta series*, Math. Ann. **308** (1997), no. 3, 507–517. [10](#)

- [SP86] Rainer Schulze-Pillot, *Ternary quadratic forms and Brandt matrices*, Nagoya Math. J. **102** (1986), 117–126. [2](#)
- [Tor05] Gonzalo Tornaría, *The Brandt module of ternary quadratic lattices*, PhD thesis, University of Texas, Austin, 2005. [2](#), [10](#)
- [Voi11] John Voight, *Characterizing quaternion rings over an arbitrary base*, J. Reine Angew. Math. **657** (2011), 113–134. [30](#), [43](#), [44](#), [45](#), [48](#)
- [Voi13] John Voight, *Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms*, Quadratic and higher degree forms, eds. K. Alladi, M. Bhargava, D. Savitt, and P.H. Tiep, Developments in Math., vol. 31, Springer, New York, 2013, 255–298. [38](#), [39](#)
- [Voi21] John Voight, *Quaternion algebras*, Grad. Texts in Math., vol. 288, Springer, Cham, 2021. [11](#), [19](#), [20](#), [21](#), [23](#), [26](#), [29](#), [30](#), [32](#), [45](#), [46](#), [48](#), [50](#), [52](#)
- [Voi23] John Voight, *Kneser’s method of neighbors*, Arch. Math. (Basel) **121** (2023), 537–557. [9](#)
- [Zas62] Hans Zassenhaus, *On the spinor norm*, Arch. Math. **13** (1962), 434–451. [40](#)

UNIVERSIDAD DE LA REPÚBLICA, MONTEVIDEO, URUGUAY
Email address: `tornaria@cmat.edu.uy`

DEPARTMENT OF MATHEMATICS, DARTMOUTH COLLEGE, 6188 KEMENY HALL, HANOVER, NH 03755, USA
Email address: `jvoight@gmail.com`