Algorithms for computing maximal lattices in bilinear (and quadratic) spaces over number fields

Jonathan Hanke

October 26, 2012

Abstract

In this paper we describe an algorithm that quickly computes a maximal $\mathfrak{a}$-valued lattice in an F-vector space equipped with a non-degenerate bilinear form, where $\mathfrak{a}$ is a fractional ideal in a number field F. We then apply this construction to give an algorithm to compute an $\mathfrak{a}$-maximal lattice in a quadratic space over any number field F where the prime $p = 2$ is unramified. We also develop the theory of $\mathfrak{p}$-neighbors for $\mathfrak{a}$-valued quadratic lattices at an arbitrary prime $\mathfrak{p}$ of $\mathcal{O}_F$ (including when $\mathfrak{p} \mid 2$) and prove its close connection to the residual geometry of certain quadrics mod $\mathfrak{p}$. Finally we give a well-known application of $\mathfrak{p}$-neighboring lattices and exact mass formulas to compute a complete set of representatives for the classes in a given genus of (totally definite) quadratic $\mathcal{O}_F$-lattices.

1 Introduction and Notation

In the study of the arithmetic of quadratic forms there has historically been a strong focus on explicit computations and specific examples. One of the first and most important instances of this was Gauss's computation of (proper integral) equivalence classes of primitive positive definite binary quadratic forms of fixed discriminant, and their arrangement into genera based on the values of certain "genus characters". These numerical investigations led to important conjectures about quadratic fields and quadratic forms of class number one that have only recently begun to be resolved. (See [41, 14] for an overview.)

Another well-known example is the explicit formula of Jacobi for the number $r_4(m)$ of representations of a positive integer m as a sum of four integer squares, given by

$$r_4(m) = 8 \sum_{\substack{0<d \mid m \\ 4 \nmid d}} d > 0,$$

and the many subsequent efforts of other authors to prove similar explicit representability and representation number formulas for other positive definite quadratic forms.

In recent times, the use of computers offers us the potential to perform previously unimaginable computations that can extend both the scope of our vision and our ability to prove concrete enumerative theorems too complex for a more traditional “by-hand” case-by-case enumeration. In the arithmetic theory of quadratic forms, this is still a promise largely waiting to be realized (e.g. see Remark 5.11).

One of the fundamental objects in this theory is the **maximal (integer-valued) quadratic lattice**, both because these have the fewest complications at “bad” primes (i.e. primes dividing the level of the associated local quadratic forms), and because there is exactly one genus of maximal quadratic lattices in any (non-degenerate) quadratic space. These are very much analogous to studying maximal orders in number fields, or more generally in central simple algebras over them, and many theorems become substantially simpler in that context (e.g. [35, 12, 3, 45, 37]).

While the importance of maximal lattices in the theory has been clear for a long time (e.g. [4, 5, 6]), proving explicit enumerative results even in this simplified context has been a rather daunting endeavor due to their complexity and many opportunities for errors. A pioneer in these investigations has been Shimura, whose many papers [39, 35, 36, 38] and recent book [37] focusing on the arithmetic of maximal lattices have set the stage for other authors' work [18, 12, 47, 20, 26]. Several other papers in a different style where maximal lattices play an important role are [1, 29, 30, 8, 46], and they are also mentioned in the introductory books [27, §82H and §104:9-10] and [13, §9.3].

Our hope is that this paper and the supporting open-source implementation [16, 15] over $\mathbb{Q}$ in the freely-available Sage computer algebra system [42] will make the arithmetic of maximal lattices more accessible to study and numerical experimentation. Among other things, this implementation includes functionality for computing with quadratic forms/spaces/lattices, as well as finding p-neighbors, genus representatives and maximal lattices when $F = \mathbb{Q}$. One application of these algorithms is the author's recent work [19] enumerating all maximal definite quadratic lattices over $\mathbb{Z}$ of class number one in $n \geq 3$ variables.

Outline: The main results of this paper are to:

1. Prove an algorithm for computing a maximal bilinear lattice in a given non-degenerate bilinear space over an arbitrary number field.

2. Prove an algorithm for computing a maximal quadratic lattice in a given non-degenerate quadratic space over a number field where $p = 2$ is unramified.

3. Explain a generalization of the theory of $\mathfrak{p}$-neighbors allowing $\mathfrak{a}$-valued quadratic lattices and its connection to residual geometry.

4. Prove an algorithm for enumerating the classes in a given genus of $\mathfrak{a}$-valued quadratic lattices over an arbitrary number field.

Acknowledgements: This is an outgrowth of some Sage code written for quadratic forms over $\mathbb{Z}$ together with Gabrielle Nebe shortly after the Sage Days 13 Conference on "Quadratic Forms and Lattices" held at the University of Georgia in March 2009. The author gratefully acknowledges her guidance and helpful comments, as well as the thoughtful comments and corrections of the anonymous referee, and several references provided by Wai Kiu Chan and Rainer Schulze-Pillot. The author also warmly acknowledges the hospitality of the Boston University Mathematics Department for allowing him to visit for two months in Spring 2012, where the final writing of this paper occurred. This work was partially supported by the author's NSF Grant DMS-0603976.

Notation:

Throughout this paper we denote by $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, and $\mathbb{F}_q$ respectively the positive integers, integers, rational numbers, real numbers, complex numbers, and finite field with q elements. If we take F to be a number field (i.e. a finite dimensional field extension of $\mathbb{Q}$), then we let $\mathcal{O}_F$ be the ring of integers in F, $\mathfrak{p}$ any non-zero prime ideal of $\mathcal{O}_F$, and take $\mathbb{F}_\mathfrak{p} := \mathcal{O}_F/\mathfrak{p}$ to be the (finite) residue field having $\mathrm{N}_{F/\mathbb{Q}}(\mathfrak{p})$ elements (where $\mathrm{N}_{F/\mathbb{Q}}(\mathfrak{p}) \in \mathbb{N}$ is the absolute norm of $\mathfrak{p}$). We also usually let $\mathfrak{a}$ and $\mathfrak{b}$ denote (non-zero) fractional ideals of F (i.e. invertible rank 1 $\mathcal{O}_F$-modules).

Given a number field F and a (non-zero) prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$, we let $F_\mathfrak{p}$ denote the $\mathfrak{p}$-adic completion of F and denote its (valuation) ring of integers by $\mathcal{O}_\mathfrak{p}$. By abuse of notation, we also denote the maximal ideal of $\mathcal{O}_\mathfrak{p}$ as $\mathfrak{p}$ and leave the reader to decide if the set $\mathfrak{p}$ is $\mathfrak{p}$-adically complete based on its usage.

If V is a finite dimensional vector space over a field K with ring of integers R, we say that a subset $L \subset V$ is a **lattice (in V)** if L is a finitely generated R-module whose K-span $L \otimes_R K = V$. Given a symmetric bilinear form $B : V \times V \to K$ we refer to the pair (V, B) as a **(symmetric) bilinear space** over K. Similarly, given a quadratic form $Q : V \to K$ we refer to the pair (V, Q) as a **quadratic space** over K. We also refer to an $\mathcal{O}_K$-lattice in a bilinear space or quadratic space over a number field K respectively as a **(global) bilinear** or **(global) quadratic lattice**.

Given a number field K and a (non-zero) prime $\mathfrak{p}$ of $\mathcal{O}_K$, we denote the associated **local bilinear** or **local quadratic spaces** at $\mathfrak{p}$ respectively as $(V_\mathfrak{p}, B_\mathfrak{p})$ or $(V_\mathfrak{p}, Q_\mathfrak{p})$, where $V_\mathfrak{p} := V \otimes_K K_\mathfrak{p}$ and where $B_\mathfrak{p}$ and $Q_\mathfrak{p}$ denote the unique continuous extensions of B and Q to $V_\mathfrak{p}$. (We could also view $B_\mathfrak{p}$ as the $K_\mathfrak{p}$-linear extension of B to $V_\mathfrak{p}$, and $Q_\mathfrak{p}$ as the $K_\mathfrak{p}$-quadratic extension of Q to $V_\mathfrak{p}$.) We also define the (possibly bilinear or quadratic) **local lattice** $L_\mathfrak{p} := L \otimes_{\mathcal{O}_K} \mathcal{O}_p \subset V_\mathfrak{p}$ associated to L at $\mathfrak{p}$.

Given a (local/global) bilinear space (V, B), we define the **associated quadratic space** (V, Q_B) by $Q_B(\vec{x}) := B(\vec{x}, \vec{x})$. Similarly, given a quadratic space (V, Q) we define the **associated (Hessian) bilinear space** (V, H) by $H(\vec{x}, \vec{y}) := H_Q(\vec{x}, \vec{y}) := Q(\vec{x} + \vec{y}) - Q(\vec{x}) - Q(\vec{y})$. Notice that these operations are *not inverses* of each other, and composing them has the effect of multiplying the (quadratic/bilinear) form by two. (While it is often a convention to associate the "Gram bilinear form" $\frac{1}{2}H$ to a quadratic form, this is not natural unless 2 is a unit, and not even possible over fields of characteristic 2.) We also adopt the convention that any notion for a bilinear space applied to a quadratic space (V, Q) is applied to its associated bilinear space (V, H), and conversely quadratic notions on a bilinear space (V, B) are applied to the associated quadratic space (V, Q).

Given a bilinear space (V, B), we say that $\vec{x}, \vec{y} \in V$ are **perpendicular** (or **orthogonal**) $\iff$ $B(\vec{x}, \vec{y}) = 0$, and for any subset $W \subseteq V$ we define $W^\perp := \{\vec{x} \in V \mid B(W, \vec{x}) = \{0\}\}$. We define the **radical** of V by $\mathrm{Rad}(V) := V^\perp$ and say that V is **non-degenerate** if $\mathrm{Rad}(V) = \{\vec{0}\}$. We call the 2-dimensional bilinear space (V, B) given by $B((x_1, x_2), (y_1, y_2)) := x_1y_2 + x_2y_1$ the **hyperbolic plane**, and refer to any direct sum of these as a **hyperbolic space**. We say that a subspace $W \subseteq (V, B)$ is **Lagrangian** if $W^\perp = W$, and that W is **weakly metabolic** if it admits a Lagrangian subspace.

We say that a vector $\vec{v} \neq \vec{0}$ in a quadratic space (V, Q) is **isotropic** if $Q(\vec{v}) = 0$. We say that a quadratic space is **isotropic** if it contains an isotropic vector, and that is **anisotropic** otherwise (i.e. $Q(\vec{x}) = 0 \implies \vec{x} = \vec{0}$). We also refer to a subspace $W \subseteq (V, Q)$ as **totally isotropic** if $Q(W) = \{0\}$.

Finally, given any vector space V we define $\mathbb{P}(V)$ as the set of lines in V passing through the origin $\vec{0}$, and for any subset $\mathbb{S} \subseteq V$ we define $\mathbb{P}(\mathbb{S}) \subseteq \mathbb{P}(V)$ as the set of lines in $\mathbb{P}(V)$ having non-empty intersection with $\mathbb{S}$. We also define a **maximal** object as being maximal with respect to the natural inclusion of such objects. For any $x \in \mathbb{R}$ we let $\lceil x \rceil$ denote the smallest integer $\geq x$ (i.e. the ceiling function). For any ring R we let $\mathrm{Char}(R)$ denote the characteristic of R, and for any subset $\mathbb{S}$ of an R-module we let $\mathrm{Span}_R(\mathbb{S})$ as the R-module generated by $\mathbb{S}$.

2 Duality for Bilinear Lattices

2.1 Dual lattices and Modular lattices

We begin by recalling some useful facts about bilinear forms and duality that we will use freely throughout the paper, as well as the all-important polarization identity.

Definition 2.1. *Given a lattice L in a bilinear space (V, B) over a number field F, and a non-zero fractional ideal $\mathfrak{a}$ of F, we define the* **$\mathfrak{a}$-dual lattice** *$L^{\#_\mathfrak{a}} \subset (V, B)$ of L as the $\mathcal{O}_F$-lattice*

$$L^{\#_\mathfrak{a}} := \{\vec{v} \in V \mid B(\vec{v}, L) \subseteq \mathfrak{a}\}.$$

When $\mathfrak{a} = \mathcal{O}_F$ this is simply referred to as the **dual lattice** *of L, denoted by $L^\#$. One of the main uses for the $\mathfrak{a}$-dual lattice is to help understand the $\mathfrak{a}$-valued superlattices of L.*

Lemma 2.2 ($\mathfrak{a}$-valued lattices and duals)**.** *If L is a lattice in a non-degenerate bilinear space (V, B) over a number field F and $\mathfrak{a}$ is a non-zero fractional ideal of F, then*

$$L \text{ is } \mathfrak{a}\text{-valued} \iff L \subseteq L^{\#_\mathfrak{a}}.$$

Proof. This follows since L is $\mathfrak{a}$-valued $\iff B(L,L) \subseteq \mathfrak{a} \iff L \subseteq L^{\#_\mathfrak{a}}$. □

Lemma 2.3 (Lattice scaling and Duality)**.** *Suppose that $\mathfrak{a}$ and $\mathfrak{b}$ are non-zero fractional ideals of F, and L is a lattice in a non-degenerate bilinear space over F. Then $L^{\#_\mathfrak{a}} = \mathfrak{a}L^\#$ and $(\mathfrak{b}L)^\# = L^{\#_{\mathfrak{b}^{-1}}}$.*

Proof. Since $B(\mathfrak{a}L^\#, L) \subseteq \mathfrak{a}B(L^\#, L) \subseteq \mathfrak{a}$ we know that $\mathfrak{a}L^\# \subseteq L^{\#_\mathfrak{a}}$, and conversely $B(L^{\#_\mathfrak{a}}, L) \subseteq \mathfrak{a} \implies B(\mathfrak{a}^{-1}L^{\#_\mathfrak{a}}, L) \subseteq \mathcal{O}_F \implies \mathfrak{a}^{-1}L^{\#_\mathfrak{a}} \subseteq L^\# \implies L^{\#_\mathfrak{a}} \subseteq \mathfrak{a}L^\#$, so we have the equality $L^{\#_\mathfrak{a}} = \mathfrak{a}L^\#$.

Similarly $B((\mathfrak{b}L)^\#, \mathfrak{b}L) \subseteq \mathcal{O}_F \implies B((\mathfrak{b}L)^\#, L) \subseteq \mathfrak{b}^{-1} \implies (\mathfrak{b}L)^\# \subseteq L^{\#_{\mathfrak{b}^{-1}}}$, and also $B(L^{\#_{\mathfrak{b}^{-1}}}, L) \subseteq \mathfrak{b}^{-1} \implies B(L^{\#_{\mathfrak{b}^{-1}}}, \mathfrak{b}L) \subseteq \mathcal{O}_F \implies L^{\#_{\mathfrak{b}^{-1}}} \subseteq (\mathfrak{b}L)^\#$, giving the desired equality $(\mathfrak{b}L)^\# = L^{\#_{\mathfrak{b}^{-1}}}$. □

Lemma 2.4 (Double duals)**.** *If L is a bilinear lattice in a non-degenerate bilinear space (V, B) and $\mathfrak{a}$ is a non-zero fractional ideal of F, then $(L^{\#_\mathfrak{a}})^{\#_\mathfrak{a}} = L$.*

Proof. The equality $(L^\#)^\# = L$ is given in [33, Lemma 1.5(ii), p203] and also [27, §82F, pp230-231]. From this and Lemma 2.3 we see that $(L^{\#_\mathfrak{a}})^{\#_\mathfrak{a}} = \mathfrak{a}(\mathfrak{a}L^{\#_\mathfrak{a}})^\# = \mathfrak{a} \cdot \mathfrak{a}^{-1}(L^\#)^\# = L$, proving the lemma. □

Definition 2.5. *We say that a bilinear lattice $L \subset (V, B)$ is* **$\mathfrak{a}$-modular** *for some fractional ideal $\mathfrak{a}$ if $L^\# = \frac{1}{\mathfrak{a}}L$. This is equivalent to saying that the $\mathfrak{a}$-dual lattice $L^{\#_\mathfrak{a}} = L$.*

Lemma 2.6 (Modular lattice value ideals)**.** *If $L \subset (V, B)$ is an $\mathfrak{a}$-modular bilinear lattice then its bilinear value ideal $B(L, L) = \mathfrak{a}$.*

Proof. This follows from [27, §82:14, pp232] since their definition of $\mathfrak{a}$-modular on page 231 includes that the scale ideal $\mathfrak{s}(L) := B(L, L) = \mathfrak{a}$. □

Lemma 2.7 (Scaling modular lattices)**.** *Suppose that $\mathfrak{a}$ and $\mathfrak{b}$ are non-zero fractional ideals of F. If $L \subset (V, B)$ is an $\mathfrak{a}$-modular bilinear lattice then the scaled lattice $\mathfrak{b}L \subset (V, B)$ is a $(\mathfrak{b}^2\mathfrak{a})$-modular lattice.*

Proof. By Definition 2.5 it is enough to show that $(\mathfrak{b}L)^{\#_{\mathfrak{b}^2\mathfrak{a}}} = \mathfrak{b}L$, but from Lemma 2.3 we know that $(\mathfrak{b}L)^{\#_{\mathfrak{b}^2\mathfrak{a}}} = \mathfrak{b}^2(\mathfrak{b}L)^{\#_\mathfrak{a}} = \mathfrak{b}^2L^{\#_{\mathfrak{a}\mathfrak{b}^{-1}}} = \mathfrak{b}L^{\#_\mathfrak{a}} = \mathfrak{b}L$ since L is $\mathfrak{a}$-modular. □

Remark 2.8 (Relation with O'Meara's notation)**.** *At the request of the referee, we include some comments about how our notation relates to the notions found in O'Meara's book [27]. Our notion of an $\mathfrak{a}$-modular lattice coincides with O'Meara's by [27, §82:14, p232], and our bilinear value ideal $B(L, L)$ is O'Meara's scale ideal $\mathfrak{s}(L)$ [27, §82E, p227]. However our notion of "scaling" differs from the notion in [27, §82J, p238] since given a bilinear lattice $L \subset (V, B)$ O'Meara denotes by L^α the lattice L in an ambient bilinear space $(V, \alpha B)$ whose values are scaled by $\alpha \in F^\times$, whereas our notion of scaling fixes the ambient bilinear space (V, B) and scales the lattice L within it.*

Lemma 2.9 (Polarization Identity). *Given a quadratic form $Q(\vec{x})$ in n variables over a ring R, we can associate to it the* **Hessian (symmetric) bilinear form** $H(\vec{x},\vec{y})$ *defined by the polarization identity*

$$Q(\vec{x}+\vec{y}) = Q(\vec{x}) + H(\vec{x},\vec{y}) + Q(\vec{y}),$$

which satisfies $H(\vec{x},\vec{x}) = 2Q(\vec{x})$ and also $H(\vec{x},\vec{y}) = (\vec{x})^t A\vec{y}$ where the matrix $A \in \mathrm{Sym}^n(R)$ is defined by $A := (a_{ij})$ with $a_{ij} := \frac{\partial^2 A}{\partial x_i \partial x_j}$.

Proof. This follows easily when 2 is invertible in R since we can write $Q(\vec{x}) = \vec{x}^t A\vec{x}$ for some $A \in \mathrm{Sym}_n(R)$, and can be verified in general by writing $Q(\vec{x}) = \sum_{i\leq j} c_{ij}x_ix_j$ with $c_{ij} \in R$ and evaluating $Q(\vec{x}+\vec{y}) - Q(\vec{x}) - Q(\vec{y})$. □

2.2 Discriminant modules

We now describe a finite module associated to an $\mathfrak{a}$-valued bilinear lattice L whose geometry will be very useful later for constructing maximal $\mathfrak{a}$-valued superlattices of L.

Definition 2.10 (Discriminant module). *Suppose that F is a number field, $\mathfrak{a}$ is a non-zero fractional ideal of F and $L \subset (V,B)$ is an $\mathfrak{a}$-valued bilinear $\mathcal{O}_F$-lattice. Then we define the* **$\mathfrak{a}$-discriminant module of** *L as the bilinear module $\mathcal{D}_\mathfrak{a} := \mathcal{D}_\mathfrak{a}(L) := L^{\#\mathfrak{a}}/L$ of L equipped with the $(F/\mathfrak{a})$-valued bilinear form $\widetilde{B}(\vec{x}+L,\vec{y}+L) := B(\vec{x},\vec{y}) + \mathfrak{a}$ induced from B on V.*

Lemma 2.11 (Non-degeneracy). *If L is a non-degenerate $\mathfrak{a}$-valued bilinear lattice, then its (bilinear) $\mathfrak{a}$-discriminant module $L^{\#\mathfrak{a}}/L$ is also non-degenerate.*

Proof. Suppose $\vec{v} \in L^{\#\mathfrak{a}}$ and $B(\vec{v}, L^{\#\mathfrak{a}}) \in \mathcal{O}_F$. Then $\vec{v} \in (L^{\#a})^{\#\mathfrak{a}} = L$ by Lemma 2.4, so $\vec{v} = \vec{0} \in \mathcal{D}_\mathfrak{a}(L)$. □

Lemma 2.12. *Suppose that L is an $\mathfrak{a}$-valued lattice in a non-degenerate bilinear space (V,B) over a number field F. Then there is a bijective inclusion-preserving correspondence*

$$\left\{\begin{matrix}\mathfrak{a}\text{-valued lattices } L' \\ \text{with } L \subsetneq L' \subseteq (V,B)\end{matrix}\right\} \quad \longleftrightarrow \quad \left\{\begin{matrix}\text{isotropic submodules} \\ L'/L \subseteq (L^{\#\mathfrak{a}}/L, \widetilde{B})\end{matrix}\right\}.$$

Proof. There is an inclusion-preserving bijection between lattices L' with $L \subsetneq L' \subseteq L^{\#\mathfrak{a}}$ and non-zero submodules L'/L of $L^{\#\mathfrak{a}}/L$, and the $\mathfrak{a}$-valued extra condition follows because L'/L is isotropic for $\widetilde{B} \iff B(L') \in \mathfrak{a}$. □

Lemma 2.13 (Sublattice discriminants). *If L is an $\mathfrak{a}$-valued lattice in a non-degenerate bilinear space over a number field and L' is a (finite index) sublattice of L, then*

$$|\mathcal{D}_\mathfrak{a}(L')| = [L : L']^2 \cdot |\mathcal{D}_\mathfrak{a}(L)|.$$

Proof. Since L is $\mathfrak{a}$-valued, we have the inclusions $L' \subseteq L \subseteq L^{\#\mathfrak{a}} \subseteq (L')^{\#\mathfrak{a}}$, and by the non-degeneracy of B we have that $[L' : L] = [(L')^{\#\mathfrak{a}} : L^{\#\mathfrak{a}}]$. Therefore

$$|\mathcal{D}_{\mathfrak{a}}(L')| = [(L')^{\#\mathfrak{a}} : L'] = [L' : L]^2 \cdot [L^{\#\mathfrak{a}} : L] = [L' : L]^2 \cdot |\mathcal{D}_{\mathfrak{a}}(L)|.$$

□

3 Maximal Bilinear Lattices

In this section we describe how to produce an $\mathfrak{a}$-maximal lattice in any given non-degenerate bilinear space (V, B) over a number field F. By Lemma 2.12 we can do this by finding a maximal isotropic submodule of its $\mathfrak{a}$-discriminant module $\mathcal{D}_{\mathfrak{a}}$.

3.1 Finding Saturated discriminant modules

We begin by performing a series of lattice operations to arrange that the $\mathfrak{a}$-discriminant module is a product of bilinear spaces over finite fields $\mathbb{F}_q$. This is a common first step in many algorithms to find maximal orders (e.g. [9, §6.1], [10, §2.4.1] [44, §7]). While our approach uses duality on global lattices, we can more clearly see the meaning of saturation in terms of local lattices, where it is just given by scaling certain summands of the local Jordan decomposition.

Definition 3.1. *Suppose F is a number field and $\mathfrak{a}$ is a non-zero fractional ideal of F. We say that an $\mathfrak{a}$-valued bilinear $\mathcal{O}_F$-lattice L is* **$\mathfrak{a}$-saturated** *if for every non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$ the* **local $\mathfrak{a}$-discriminant module** *$(\mathcal{D}_{\mathfrak{a}})_{\mathfrak{p}} := \mathcal{D}_{\mathfrak{a}}(L) \otimes_{\mathcal{O}_F} \mathcal{O}_{\mathfrak{p}}$ is annihilated by $\mathfrak{p}$.*

3.1.1 Local perspective on $\mathfrak{a}$-saturated lattices

For perspective we include the following algorithm to construct an $\mathfrak{a}$-saturated local lattice containing a given $\mathfrak{a}$-valued local lattice. The main idea is that scaling a bilinear lattice L by an ideal $\mathfrak{b}$ alters its values by the square of that ideal (i.e. $B(\mathfrak{b}L, \mathfrak{b}L) = \mathfrak{b}^2 B(L, L)$), so by a series of local scalings we can adjust L so that its modular components are at most one valuation larger than the valuation of the desired value ideal $\mathfrak{a}$.

Algorithm 3.2 (Finding a Local $\mathfrak{a}$-saturated lattice)**.** *Given an $\mathfrak{a}$-valued bilinear $\mathcal{O}_{\mathfrak{p}}$-lattice $L_{\mathfrak{p}}$ in a non-degenerate bilinear space (V, B) over $F_{\mathfrak{p}}$, we give an algorithm for finding an $\mathfrak{a}$-saturated superlattice of $L_{\mathfrak{p}}$.*

1. *Compute a Jordan decomposition $L_{\mathfrak{p}} = \oplus_{i \in \mathbb{Z} \geq 0} L_{i,\mathfrak{p}}$ where the $L_{i,\mathfrak{p}}$ are $\mathfrak{a}\mathfrak{p}^i$-modular (e.g. using [17, (2.2) and Lemma 2.1, pp354-5] or [27, §94, p279-280]).*

2. *Return $L'_{\mathfrak{p}} = \oplus_{i \in \mathbb{Z} \geq 0} \mathfrak{p}^{-\nu_i} L_{i,\mathfrak{p}}$ where $\nu_i := \lfloor \frac{i}{2} \rfloor$.*

Proof. We know that $i \geq 0$ for all non-zero $L_{i,\mathfrak{p}}$ since for these we have $B(L_{i,\mathfrak{p}}, L_{i,\mathfrak{p}}) = \mathfrak{a}\mathfrak{p}^i \subseteq \mathfrak{a}$ by Lemma 2.6. □

Remark 3.3 (Local-Global approach for $\mathfrak{a}$-saturated lattice)**.** *One could use Algorithm 3.2 to construct a global $\mathfrak{a}$-saturated bilinear lattice by first choosing some $\mathfrak{a}$-valued lattice L, computing the finite set of primes $\mathbb{S}$ where $L_\mathfrak{p}$ is not $\mathfrak{a}$-saturated, using Algorithm 3.2 to construct $\mathfrak{a}$-saturated local lattices $L'_\mathfrak{p} \supseteq L_\mathfrak{p}$ for all $\mathfrak{p} \in \mathbb{S}$, and then using an algorithm (e.g. Algorithm 3.4) to construct the unique $\mathcal{O}_F$-lattice L'' satisfying*

$$(L'')_\mathfrak{p} = \begin{cases} L'_\mathfrak{p} & \textit{if } \mathfrak{p} \in \mathbb{S}, \\ L_\mathfrak{p} & \textit{if } \mathfrak{p} \notin \mathbb{S}. \end{cases}$$

For the interested reader, we include a reference to an algorithm for performing the local-global construction with lattices, which is essentially an algorithm for Strong Approximation on GL_n over a number field.

Algorithm 3.4 (Local-Global Algorithm for lattices)**.** *Suppose that V is a finite-dimensional vector space over a number field F. Given (local) $\mathcal{O}_\mathfrak{p}$-lattices $L'_\mathfrak{p} \subseteq V_\mathfrak{p}$ for all non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}_F$ satisfying the compatibility condition that for all but finitely many $\mathfrak{p}$ we have that $L'_\mathfrak{p} = L''$ for some fixed $\mathcal{O}_F$-lattice $L' \subset V$, there is an algorithm for constructing a (global) $\mathcal{O}_F$-lattice $L \subseteq V$ so that its local lattices $L_\mathfrak{p} := L \otimes_{\mathcal{O}_F} \mathcal{O}_\mathfrak{p}$ satisfy $L_\mathfrak{p} = L'_\mathfrak{p}$ (as subsets of $V_\mathfrak{p}$) for all $\mathfrak{p}$.*

Proof. A constructive algorithm for this is given as the proof of [27, §84:14, pp218-219], which uses the algorithm in [27, §81:11, pp214-216] to normalize the presentation of two lattices in a common global vector space. □

3.1.2 Global algorithms for finding an $\mathfrak{a}$-saturated lattice

In this section we give a global algorithm using a scaled dual lattice construction to simultaneously reduce the divisibility of the annihilator ideal of the $\mathfrak{a}$-discriminant module $\mathcal{D}_\mathfrak{a}$ at all primes $\mathfrak{p}$. By repeating this process until the annihilator of $\mathcal{D}_\mathfrak{a}$ is a squarefree ideal, we obtain the desired $\mathfrak{a}$-saturated lattice.

Lemma 3.5. *If M is an $(\mathfrak{a}\mathfrak{p}^i)$-modular bilinear lattice in a non-degenerate bilinear space (V, B) over a number field F, then for any $\lambda \in \mathbb{Z}$ the scaled dual lattice $M' := \mathfrak{a}\mathfrak{p}^\lambda M^\#$ is $(\mathfrak{a}\mathfrak{p}^{2\lambda - i})$-modular, and M' is $\mathfrak{a}$-valued (as a bilinear lattice) iff $\lambda \geq \lceil \frac{i}{2} \rceil$.*

Proof. Since M is an $(\mathfrak{a}\mathfrak{p}^i)$-modular lattice we have that $M^\# = \frac{1}{\mathfrak{a}\mathfrak{p}^i} M$ and so $M' := \mathfrak{p}^{\lambda - i} M$. By Lemma 2.7, we have that M' is $(\mathfrak{p}^{2(\lambda - i)}\mathfrak{a}\mathfrak{p}^i) = (\mathfrak{a}\mathfrak{p}^{2\lambda - i})$-modular. This shows that the ideal $B(M', M') = B(\mathfrak{a}\mathfrak{p}^{2\lambda - i}(M')^\#, M') = \mathfrak{a}\mathfrak{p}^{2\lambda - i}$ is contained in $\mathfrak{a}$ iff $\lambda \geq \lceil \frac{i}{2} \rceil$. □

From Lemma 3.5 we see that the scaled dual lattice $(\mathfrak{p}^\alpha L_i^{\#\mathfrak{a}}, B)$ is proper $\mathfrak{a}$-valued superlattice of L_i when $i > \alpha \geq \lceil \frac{i}{2} \rceil$, so in particular we can use this idea on $\mathfrak{a}\mathfrak{p}^i$-modular lattices only when $i \geq \lceil \frac{i}{2} \rceil$, which only happens when $i \geq 2$. To make this idea useful for more general $\mathfrak{a}$-valued bilinear lattices, we make the following definition.

Definition 3.6 (Maximal scale index)**.** *Given a non-zero fractional ideal $\mathfrak{a}$ in a number field F, and a non-degenerate $\mathfrak{a} \cdot \mathcal{O}_\mathfrak{p}$-valued bilinear $\mathcal{O}_\mathfrak{p}$-lattice L, we define the* **maximal scale index** *$m_{\mathfrak{p},\mathfrak{a}}$ of L at $\mathfrak{p}$ (relative to $\mathfrak{a}$) to be the largest integer i so that the $\mathfrak{a}\mathfrak{p}^i$-modular component of L is non-zero (in any Jordan decomposition $L \cong \oplus_{i\in\mathbb{Z}} L_i$ over $\mathcal{O}_\mathfrak{p}$ where the L_i are $\mathfrak{p}^i$-modular). Since L is $\mathfrak{a}$-valued, we always have $m_{\mathfrak{p},\mathfrak{a}} \geq 0$.*

We now explain how to construct an $\mathfrak{a}$-saturated lattice from any $\mathfrak{a}$-valued lattice.

Theorem 3.7. *Suppose that L is an $\mathfrak{a}$-valued lattice in a non-degenerate bilinear space over a number field F, whose maximal scale index $m_{\mathfrak{p},\mathfrak{a}} \geq 2$ for some non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$. Then the bilinear lattice*

$$L' := L + \mathfrak{p}^\lambda L^{\#\mathfrak{a}} \qquad \textit{with} \qquad \lambda := \lceil \tfrac{m_{\mathfrak{p},\mathfrak{a}}}{2} \rceil$$

is a proper $\mathfrak{a}$-valued superlattice of L, for which the maximal scale index $m'_{\mathfrak{p},\mathfrak{a}} = \lambda < m_{\mathfrak{p},\mathfrak{a}}$. Therefore we can construct an $\mathfrak{a}$-valued superlattice L'' of L with maximal scale index $m''_{\mathfrak{p},\mathfrak{a}} \leq 1$ for all primes $\mathfrak{p}$.

Proof. Let $\alpha = \mathrm{ord}_\mathfrak{p}(\mathfrak{a})$ and let $L \cong \oplus_{i\in\mathbb{Z}} L_i$ be a Jordan decomposition of L over $\mathcal{O}_\mathfrak{p}$ where the L_i are $\mathfrak{a}\mathfrak{p}^i$-modular lattices. By assumption we know that $L_i = \{0\}$ unless $0 \leq i \leq m_{\mathfrak{p},\mathfrak{a}}$. Also since duality and scaling both preserve the Jordan decompositon we can compute the lattice L' in each Jordan summand. Suppose that M is a $(\mathfrak{p}^{\alpha+i})$-modular Jordan summand of L. Then by Lemma 3.5 the associated scaled dual lattice $\mathfrak{p}^\lambda M^{\#\mathfrak{a}} = \mathfrak{a}\mathfrak{p}^\lambda M^{\#}$ is $(\mathfrak{p}^{2\lambda+\alpha-i}) = (\mathfrak{p}^{\alpha+i+2(\lambda-i)})$-modular, so the sum $M' := M + \mathfrak{a}\mathfrak{p}^\lambda M^{\#}$ is $\mathfrak{p}^{\alpha+i+\min\{0,2(\lambda-i)\}}$-modular.

We now compute the maximal scale index $m'_{\mathfrak{p},\mathfrak{a}}$ for L' by varying over all possible Jordan summands M. When $i \leq \lambda$ we have $M' = M$ which is $\mathfrak{p}^{\alpha+i}$-modular with largest power $\alpha + \lambda$, but when $i > \lambda$ we have that M' is $\mathfrak{p}^{\alpha+2\lambda-i}$-modular with the largest power here being $\alpha + \lambda - 1$, giving $m'_{\mathfrak{p},\mathfrak{a}} = \lambda$. By repeatedly applying this procedure, we obtain a decreasing sequence of $m'_{\mathfrak{p},\mathfrak{a}}$ until $m'_{\mathfrak{p},\mathfrak{a}} \leq 1$ (since $\lceil \frac{x}{2} \rceil < x$ when $x \in \mathbb{Z} \geq 2$). □

Algorithm 3.8 (Construct an $\mathfrak{a}$-saturated lattice)**.** *Given a non-degenerate bilinear space (V, B) over a number field F and a non-zero fractional ideal $\mathfrak{a}$ of F, we give an algorithm for finding a saturated $\mathfrak{a}$-valued bilinear $\mathcal{O}_F$-lattice L in (V, B).*

1. *Choose an arbitrary $\mathcal{O}_F$-lattice $L \subset (V, B)$ by repeatedly choosing vectors $\vec{v}_k$ not in the F-span of the previous vectors $\{\vec{v}_1, \ldots, \vec{v}_{k-1}\}$ until their F-span is V. Then let $L := \mathrm{Span}_{\mathcal{O}_F}\{\vec{v}_1, \ldots, \vec{v}_n\}$, where $n = \dim_F(V)$.*

2. *Let $\mathfrak{b} := B(L, L)$. If $\mathfrak{b} \nsubseteq \mathfrak{a}$ then replace L by $\mathfrak{c}L$ where $\mathfrak{c}$ is any non-zero fractional ideal satisfying $\mathfrak{c}^2\mathfrak{b} \subseteq \mathfrak{a}$. (For convenience we often we take $\mathfrak{c}$ to be principal.)*

3. *If L is saturated then return L. Otherwise, let $\mathfrak{l}$ be the integral ideal $\mathfrak{l} := \prod_{\mathfrak{p}} \mathfrak{p}^{\lambda_{\mathfrak{p}}}$ where $\lambda_{\mathfrak{p}} := \lceil \frac{m_{\mathfrak{p},\mathfrak{a}}}{2} \rceil$ and let $L' := L + \mathfrak{l}L^{\#\mathfrak{a}}$.*

4. *Replace L by L' and repeat step 3.*

This algorithm terminates by Theorem 3.7, since there are only finitely many primes $\mathfrak{p}$ where $m_{\mathfrak{p},\mathfrak{a}} \neq 0$.

3.2 Finding a Maximal Isotropic subspace

To pass from an $\mathfrak{a}$-saturated bilinear lattice to an $\mathfrak{a}$-maximal lattice, we must be able to compute a maximal isotropic subspace of a bilinear space over a finite field. In this section we describe how to do this, with special attention to when the characteristic of the base field is two.

Remark 3.9 (Bilinear and semilinear quadratic forms in characteristic two)**.** *Given a non-degenerate bilinear space (V, B) over a field K of characteristic two, the polarization identity ensures that the associated quadratic form $Q_B(\vec{x}) := B(\vec{x}, \vec{x})$ is a homomorphism of additive groups (since $2B(\vec{x} + \vec{y}, \vec{x} + y) = 0$). In general Q_B is not a K-linear map since $Q_B(\alpha\vec{x}) = \alpha^2 Q_B(\vec{x}) \neq \alpha Q_B(\vec{x})$. However when K is a perfect field (e.g. K is a finite field) we know that squaring is a field automorphism σ of K (called the Frobenius automorphism), so the quadratic scaling property can be rewritten as $Q_B(\alpha\vec{x}) = \sigma(\alpha) \cdot Q_B(\vec{x})$, which says that the map Q_B is a "semilinear" map (see [28, §4.1, p28]). Therefore Q_B "behaves like" a K-linear map in that the image and pre-image of any K-subspace are again K-vectorspaces. We also have that $\dim_K(\mathrm{Im}(Q_B)(V)) + \dim_K(\mathrm{Ker}(Q_B)(V)) = \dim_K(V)$. This observation will be extremely useful for understanding the concept of isotropy in these bilinear spaces.*

We begin by recalling a well-known test (at least in odd characteristic) for the existence of a (non-zero) isotropic vector in a non-degenerate quadratic/bilinear space over a finite field.

Lemma 3.10 (Isotropy testing over $\mathbb{F}_q$)**.** *Given a non-degenerate bilinear space (V,B) over a finite field $\mathbb{F}_q$, we can use the following criteria to determine if (V, B) is isotropic (i.e. has a non-zero vector $\vec{v} \in V$ with $B(\vec{v}, \vec{v}) = 0$):*

1. *If $\dim(V) \geq 3$ then (V, B) is isotropic.*

2. *If $\dim(V) = 2$ then*

$$(V, B) \text{ is isotropic } \iff \det(B) = -1(\mathbb{F}_q^\times)^2.$$

When $\mathrm{Char}(\mathbb{F}_q) = 2$ then (V, B) is isotropic.

3. *If* $\dim(V) = 1$ *then* (V, B) *is not isotropic.*

Proof. First suppose that $\mathrm{Char}(\mathbb{F}_q) \neq 2$. Then when $n \geq 3$ this is [27, 62:1b, p158]. When $n = 2$ then by [27, §62:1, p157] there are exactly two non-degenerate quadratic forms over $\mathbb{F}_q$, the anisotropic norm form $N_{\mathbb{F}_q^2/\mathbb{F}_q}(\vec{x})$ and the (isotropic) hyperbolic plane.

Now suppose that $\mathrm{Char}(\mathbb{F}_q) = 2$. By Remark 3.9 we see that the kernel of the map $Q_B(\vec{x}) := B(\vec{x}, \vec{x})$ is an $\mathbb{F}_q$-subspace of dimension $\geq \dim(V) - 1$. Therefore when $\dim(V) \geq 2$ we have that $K \neq \{\vec{0}\}$ and so (V, B) is isotropic.

Finally, when $n = 1$ then $B(x, x) = \alpha x^2$ with $\alpha \neq 0$ iff (V, B) is isotropic. □

Once we determine that a bilinear space over $\mathbb{F}_q$ is isotropic, we need a way to find isotropic vectors in it. Over a finite field there are only finitely many lines, so an exhaustive search through all such lines is possible. We give a somewhat better algorithm that essentially checks if a random (rational) line intersects the projective quadric hypersurface $Q_B(\vec{x}) = 0$. Here the probability of success (for each attempt) is roughly 50% since by the quadratic formula the existence of an intersection is governed by whether the discriminant of the associated quadratic polynomial is a square in $\mathbb{F}_q$.

Algorithm 3.11 (Finding an isotropic vector over $\mathbb{F}_q$)**.** *Given an isotropic non-degenerate bilinear space* (V, B) *over* $\mathbb{F}_q$*, we give a randomized algorithm for finding some non-zero* $\vec{v} \in V$ *so that* $Q_B(\vec{v}) := B(\vec{v}, \vec{v}) = 0$.

1. *Randomly choose two linearly independent vectors* $\vec{a}, \vec{m} \in V$.

2. *Compute the intersection of the line* $L := \{\vec{a} + t\vec{m} \mid t \in \mathbb{F}_q\} \subseteq V$ *with* $Q_B(\vec{x}) = 0$ *by solving* $Q_B(\vec{a} + t\vec{m}) = 0$ *for* t *over* $\mathbb{F}_q$.

3. *If a solution* $t_0 \in \mathbb{F}_q$ *exists, then the vector* $\vec{v} := \vec{a} + t_0\vec{m}$ *is isotropic. Otherwise repeat from step 1.*

Proof. Since $\vec{a}$ and $\vec{m}$ are linearly independent, we know that the affine line L descends to a line in the projective space $\mathbb{P}(V)$, and that any vector $\vec{v} \in L$ is non-zero. □

We can now easily find a maximal isotropic subspace in any bilinear space over a finite field of characteristic $\neq 2$, since there any (non-zero) isotropic vector is contained within a hyperbolic plane.

Algorithm 3.12 (Isotropic vector ⇒ Hyperbolic plane)**.** *Given a non-degenerate bilinear space* (V, B) *and a (non-zero) isotropic vector* $\vec{v} \in V$*, we give an algorithm to find some* $\vec{w} \in V$ *so that the subspace of* V *spanned by the basis* $\mathcal{B} = \{\vec{v}, \vec{w}\}$ *is a hyperbolic plane.*

1. *Choose a basis* $\mathcal{B}$ *for* V *whose first basis vector is* $\vec{v}$.

2. *Find some* $\vec{w} \in \mathcal{B}$ *so that* $B(\vec{v}, \vec{w}) = 0$.

3. *Scale $\vec{w}$ so that $B(\vec{v}, \vec{w}) = 1$ (i.e. replace $\vec{w}$ by $\frac{\vec{w}}{B(\vec{v},\vec{w})}$).*

4. *Shear $\vec{w}$ by $\vec{v}$ to arrange that $B(\vec{w}, \vec{w}) = 0$ (i.e. replace $\vec{w}$ by $\vec{w} - B(\vec{v}, \vec{w}) \cdot \vec{v}$).*

Proof. Since $\vec{v} \neq \vec{0}$ we can extend $\{\vec{v}\}$ to a basis $\mathcal{B} = \{\vec{v}_1, \ldots, \vec{v}_n\}$ with $\vec{v}_1 = \vec{v}$ in Step 1. If $B(\vec{v}, \vec{v}_i) = 0$ for all $i \geq 2$ then by linearity we have $B(\vec{v}, V) = \{0\}$ and so $\vec{v} \in \mathrm{Rad}(V) = \{\vec{0}\}$, which cannot happen since $\vec{v} \neq \vec{0}$. Therefore some $B(\vec{v}, \vec{v}_i) = 0$ in Step 2. The remaining steps follow by linearity. □

Algorithm 3.13 (Maximal Totally Isotropic subspaces in odd characteristic)**.** *Suppose that (V, B) is a bilinear space over a finite field of characteristic $\neq 2$. Then we give an algorithm to find an orthogonal decomposition of V as $V = R \perp H \perp A$ where $R := \mathrm{Rad}(V)$, H is a hyperbolic space, and A is anisotropic.*

1. *Compute the radical subspace R of V, and find a complementary subspace V' of R in V. Then $(V', B\mid_{V'})$ is a non-degenerate bilinear space.*

2. *Use Lemma 3.10 and Algorithms 3.11 and 3.12 to repeatedly split off hyperbolic planes from V' until the remaining bilinear space is anisotropic (and take this as A).*

Further, by writing the hyperbolic space H as a (non-orthogonal) direct sum of two Lagrangian subspaces $H = L \oplus L'$ (which is done implicitly in Step 2), we have that the subspace $M := R + L$ is a maximal totally isotropic subspace of (V, B).

Proof. Certainly M is a totally isotropic subspace since for any $\vec{r} \in R$ and $\vec{l} \in L$ we have $B(\vec{r} + \vec{l}, \vec{r} + \vec{l}) = B(\vec{l}, \vec{l}) = 0$. To see maximality, suppose we have some totally isotropic subspace M' of V with $M' \supseteq M$ and write any $\vec{v}' \in M'$ as $\vec{v} = \vec{r} + \vec{l} + \vec{l}' + \vec{a}$ according to the decomposition above. Then we must have $\vec{l}' = \vec{0}$ since otherwise we can find some $\vec{l}_0 \in L$ so that $B(\vec{v}, \vec{l}_0) = B(\vec{l}, \vec{l}_0) \neq 0$. Similarly $B(\vec{v}, \vec{v}) = B(\vec{a}, \vec{a}) = 0 \implies \vec{a} = \vec{0}$ since A is anisotropic. This shows that $\vec{v} \in M$, so $M' \subseteq M$ and M is a maximal totally isotropic subspace of V. □

Over finite fields of characteristic two several new phenomena arise, including the failure of the Algorithm 3.12 due to the presence of "metabolic" bilinear spaces (e.g. $B(\vec{x}, \vec{y}) = x_1y_2 + x_2y_1 + x_2y_2$) that are isotropic but not hyperbolic. However to compensate for this complication, we gain the simplification that quadratic forms behave like linear forms in this setting (see Remark 3.9). With this in mind, we look for a maximal totally isotropic subspace of any bilinear space over a finite field of characteristic two.

Algorithm 3.14 (Maximal Totally Isotropic subspaces in characteristic two)**.** *Suppose that (V, B) is a bilinear space over a finite field K of characteristic two. Then we give an algorithm to find an orthogonal decomposition of V as $V = R \perp (I \oplus A)$ where $R := \mathrm{Rad}(V)$, I is a totally isotropic space, and A is anisotropic with $\dim(A) \leq 1$. For convenience we define $Q_B(\vec{x}) := B(\vec{x}, \vec{x})$.*

1. *Compute the radical subspace R of V, and find a complementary subspace V' of R in V. Then $(V', B\mid_{V'})$ is a non-degenerate bilinear space.*

2. *Choose a basis $\mathcal{B} = \{\vec{v}_1, \dots, \vec{v}_n\}$ for V', ordered so that $Q_B(\vec{v}_n) \neq 0$ if some $Q_B(\vec{v}_i) \neq 0$.*

3. *If $Q_B(\vec{v}_n) \neq 0$ then by shearing the $\vec{v}_i$ by $\vec{v}_n$ we can arrange that $Q_B(\vec{v}_i) = 0$ for all $1 \leq i < n$ (i.e. replace $\vec{v}_i$ by $\vec{v}_i - \sqrt{\frac{Q_B(\vec{v}_i)}{Q_B(\vec{v}_n)}}\vec{v}_n$).*

4. *If $Q_B(\vec{v}_n) = 0$ then set $I := Span_K(\{\vec{v}_1, \dots, \vec{v}_n\})$ and $A := \{\vec{0}\}$, otherwise set $I := Span_K(\{\vec{v}_1, \dots, \vec{v}_{n-1}\})$ and $A := Span_K(\{\vec{v}_n\})$.*

Given this decomposition, we have that the subspace $M := R + I$ is a maximal isotropic subspace of (V, B).

Proof. We know that M is a totally isotropic subspace since for any $\vec{r} \in R$ and $\vec{\iota} \in I$ we have $B(\vec{r} + \vec{\iota}, \vec{r} + \vec{\iota}) = B(\vec{\iota}, \vec{\iota}) = 0$. To see maximality, suppose we have some totally isotropic subspace M' of V with $M' \supseteq M$ and write any $\vec{v}' \in M'$ as $\vec{v} = \vec{r} + \vec{\iota} + \vec{a}$ according to the decomposition above. Then $0 = Q_B(\vec{r} + \vec{\iota} + \vec{a}) = Q_B(\vec{a})$ gives $\vec{a} = \vec{0}$ and so $\vec{v} \in M$. Therefore $M' \subseteq M$ and M is a maximal totally isotropic subspace of V. □

Remark 3.15. *It is interesting to note that the characteristic two Algorithm 3.14 is both stronger and weaker than its odd characteristic counterpart (Algorithm 3.13). It is stronger in that we more easily see the totally isotropic subspace and $\dim(A) \leq 1$ (instead of ≤ 2), but it is weaker in that we have concluded much less about the underlying bilinear space under the decomposition. This illustrates the general phenomenon that quadratic forms (i.e. questions about isotropy) and symmetric bilinear forms (i.e. questions about orthogonality) are distinct notions in characteristic two.*

3.3 Finding a Maximal bilinear lattice

Now that we can find a maximal isotropic subspace of $\mathfrak{a}$-discriminant module of a saturated $\mathfrak{a}$-valued bilinear lattice L, we are ready to compute a maximal $\mathfrak{a}$-valued bilinear superlattice of L.

Algorithm 3.16 (Construct a maximal $\mathfrak{a}$-valued bilinear lattice)**.** *Given a non-degenerate bilinear space (V, B) over a number field F and a non-zero fractional ideal $\mathfrak{a}$ of F, we give an algorithm for finding a maximal $\mathfrak{a}$-valued bilinear $\mathcal{O}_F$-lattice L in (V, B).*

1. *Use Algorithm 3.8 (or Algorithm 3.2 and Remark 3.3) to find an $\mathfrak{a}$-saturated lattice in (V, B). Let $\mathbb{S}$ denote the finite set of (non-zero) primes $\mathfrak{p}$ of $\mathcal{O}_F$ where the local discriminant module $(\mathcal{D}_{\mathfrak{a}}(L))_{\mathfrak{p}} \neq \{0\}$.*

2. *For each $\mathfrak{p} \in \mathbb{S}$, use Algorithm 3.13 or 3.14 to find a maximal isotropic subspace $I_\mathfrak{p}$ of the non-zero $\mathbb{F}_\mathfrak{p}$-vector space $(\mathcal{D}_\mathfrak{a}(L))_\mathfrak{p}$.*

3. *For each $\mathfrak{p} \in \mathbb{S}$, choose a lift of a basis $\mathcal{B}_\mathfrak{p}$ for $I_\mathfrak{p}$ to a set $\mathcal{B}'_\mathfrak{p} \subseteq L^{\#_\mathfrak{a}}$ of vectors so that for every $\mathfrak{q} \in \mathbb{S}$ their $\mathbb{F}_\mathfrak{q}$-span in $(\mathcal{D}_\mathfrak{a}(L))_\mathfrak{q}$ satisfies*

$$\mathit{Span}_{\mathbb{F}_\mathfrak{q}}(\mathcal{B}'_\mathfrak{p}) = \begin{cases} I_\mathfrak{p} & \text{if } \mathfrak{q} = \mathfrak{p}, \\ \{0\} & \text{if } \mathfrak{q} \neq \mathfrak{p}. \end{cases}$$

   This can be done with a constructive version of the Chinese Remainder Theorem.

4. *Then the lattice $L' := L + \mathit{Span}_{\mathcal{O}_F}(\cup_{\mathfrak{p}\in\mathbb{S}}\mathcal{B}'_\mathfrak{p})$ is a maximal $\mathfrak{a}$-valued bilinear $\mathcal{O}_F$-lattice containing L.*

Proof. Since $L^{\#_\mathfrak{a}} \supseteq L' \supseteq L$ and $L'/L \subseteq (\mathcal{D}_\mathfrak{a})_\mathfrak{p}$ is a maximal isotropic submodule, the correspondence in Lemma 2.12 ensures that L' is a maximal $\mathfrak{a}$-valued lattice in (V, B). □

We conclude with a very general lemma about the uniqueness of discriminant modules of maximal $\mathfrak{a}$-valued bilinear lattices which will be useful when thinking about maximal quadratic lattices. This proof was explained to the author by Prof. Gabrielle Nebe.

Lemma 3.17 (Uniqueness of Maximal Lattice Discriminant modules)**.** *Suppose that L_1 and L_2 are maximal $\mathfrak{a}$-valued lattices in a non-degenerate bilinear space (V, B) over a field F. Then the discriminant modules $\mathcal{D}_\mathfrak{a}(L_1) \cong \mathcal{D}_\mathfrak{a}(L_2)$ as $(F/\mathfrak{a})$-valued bilinear $\mathcal{O}_F$-modules.*

Proof. We first notice that the discriminant modules $\mathcal{D}_\mathfrak{a}(L_1) \cong \mathcal{D}_\mathfrak{a}(L_1 \cap L_2) \cong \mathcal{D}_\mathfrak{a}(L_2)$ in the Witt group of bilinear torsion $\mathcal{O}_F$-modules (i.e. up to weakly metabolic summands) since the submodules $N_i := L_i/(L_1 \cap L_2)$ of $\mathcal{D}_\mathfrak{a}(L_1 \cap L_2)$ are isotropic with $(N_i)^\perp = L_i^{\#_\mathfrak{a}}/(L_1 \cap L_2)$, so by [33, Lemma 1.4] we know that the orthogonal sums $\mathcal{D}_\mathfrak{a}(L_i) \perp -\mathcal{D}_\mathfrak{a}(L_1 \cap L_2)$ are weakly metabolic.

For convenience, let $\mathcal{D}_i := \mathcal{D}_\mathfrak{a}(L_i)$. Since the sum $\mathcal{D}_1 \perp -\mathcal{D}_2$ is weakly metabolic, we know that it has some submodule N with $N = N^\perp$ and further that $|\mathcal{D}_1| \cdot |\mathcal{D}_2| = |N| \cdot |N^\perp| = |N|^2$ by comparing cardinalities in the exact sequence of torsion $\mathcal{O}_F$-modules

$$0 \longrightarrow N^\perp \longrightarrow (\mathcal{D}_1 \perp -\mathcal{D}_2) \xrightarrow{B(\cdot,(x_1,-x_2))} N^* := \mathrm{Hom}_{\mathcal{O}_F}(N, F/\mathcal{O}_F) \longrightarrow 0.$$

We also know that the projections $\pi_i : N \to \mathcal{D}_i$ are injective since the kernel lies in $\mathcal{D}_{i'} \cap N = \{0\}$ where $i \neq i'$, so by the formula $|\mathcal{D}_1| \cdot |\mathcal{D}_2| = |N|^2$ we see that the π_i are also surjective. To see that $\pi_2 \circ \pi_1^{-1} : \mathcal{D}_1 \to -\mathcal{D}_2$ is an isomorphism of bilinear modules, suppose that it maps $x \mapsto y$ and $x' \mapsto y'$. Then since $x + y, x' + y' \in N$, we have that $0 = B(x + x', y + y') = B(x, x') + B(y, y')$, giving $B(x, x') = -B(y, y')$, which proves the lemma. □

4 Maximal Quadratic Lattices

One application of Algorithm 3.16 is to help with finding a maximal $\mathfrak{a}$-valued quadratic lattice (in a quadratic space) over a number field F where the prime $p = 2$ is unramified. To do this we require one additional notion for bilinear lattices.

Definition 4.1 (Even bilinear lattices)**.** *Given a lattice L in a bilinear space (V, H), we respectively define the* **full** *and* **partial $\mathfrak{a}$-even subsets** *of L as*

$$L_{\mathfrak{a}\text{-}even} := \{\vec{x} \in L \mid H(\vec{x}, \vec{x}) \in 2\mathfrak{a}\},$$

$$L_{\mathfrak{a}\text{-}even\ at\ \mathfrak{p}} := \{\vec{x} \in L \mid H(\vec{x}, \vec{x}) \in \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(2\mathfrak{a})}\}.$$

When L is $\mathfrak{a}$-valued these are actually **sublattices***. To see this, suppose $\vec{x}, \vec{y} \in L_{\mathfrak{a}\text{-}even(at\ \mathfrak{p})}$ and notice that*

$$H(\vec{x} + \vec{y}) = H(\vec{x}, \vec{x}) + H(\vec{y}, \vec{y}) + 2H(\vec{x}, \vec{y}) \subseteq 2\mathfrak{a}\ \textit{(or } \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(2\mathfrak{a})}\textit{)} \implies \vec{x} + \vec{y} \in L_{\mathfrak{a}\text{-}even(at\ \mathfrak{p})}.$$

We say that L is **$\mathfrak{a}$-even** *if $L = L_{\mathfrak{a}\text{-}even}$, and that L is* **$\mathfrak{a}$-even at $\mathfrak{p}$** *if $L = L_{\mathfrak{a}\text{-}even\ at\ \mathfrak{p}}$.*

Remark 4.2 ($\mathfrak{a}$-even $\implies$ $\mathfrak{a}$-valued)**.** *For a lattice L in a bilinear space (V, H) the property of being $\mathfrak{a}$-even is stronger than being $\mathfrak{a}$-valued. To see this, notice that if L is $\mathfrak{a}$-even then*

$$H(\vec{x}, \vec{y}) = \frac{H(\vec{x} + \vec{y}, \vec{x} + \vec{y}) - H(\vec{x}, \vec{x}) - H(\vec{y}, \vec{y})}{2} \in \frac{2\mathfrak{a}}{2} = \mathfrak{a}$$

for all $\vec{x}, \vec{y} \in L$, hence L is $\mathfrak{a}$-valued.

Remark 4.3 (Even observations)**.** *Notice that the full and partial $\mathfrak{a}$-even subsets/sublattices of an $\mathfrak{a}$-valued bilinear lattice L are related by the formula*

$$L_{\mathfrak{a}\text{-}even} = \cap_{\mathfrak{p}}(L_{\mathfrak{a}\text{-}even\ at\ \mathfrak{p}}),$$

and that L is $\mathfrak{a}$-even at all primes $\mathfrak{p} \nmid 2$.

For our purposes, the importance of $\mathfrak{a}$-even bilinear lattices comes from the following simple correspondence with $\mathfrak{a}$-valued quadratic lattices.

Lemma 4.4 (Even bilinear correspondence)**.** *Suppose that L is a lattice in a quadratic space (V, Q), $\mathfrak{a}$ is a non-zero fractional ideal of a ($\mathfrak{p}$-adic or number) field F, and (V, H) is the Hessian bilinear space associated to (V, Q). Then*

$$\begin{array}{c} L \subseteq (V, H) \textit{ is an} \\ \mathfrak{a}\textit{-even bilinear lattice} \end{array} \iff \begin{array}{c} L \subseteq (V, Q) \textit{ is an} \\ \mathfrak{a}\textit{-valued quadratic lattice.} \end{array}$$

Proof. This is just a restatement of the formula $H(\vec{x}, \vec{x}) = 2Q(\vec{x})$. □

Lemma 4.5 (The index of an even sublattice). *Suppose that L is an $\mathfrak{a}$-valued lattice in a non-degenerate bilinear space (V, H) over a number field F, for some fractional ideal $\mathfrak{a}$ of F. If L is not $\mathfrak{a}$-even at $\mathfrak{p}$ and $e_\mathfrak{p} := \mathrm{ord}_\mathfrak{p}(2) \leq 1$, then the quotient*

$$L/L_{\mathfrak{a}\text{-}even} \cong \mathbb{F}_\mathfrak{p}$$

as abelian groups.

Proof. Notice that $\mathfrak{p} \mid 2$ since otherwise $L_{\mathfrak{a}\text{-even}} = L$, which is not true by assumption. Consider the map $Q_H(\vec{x}) := H(\vec{x}, \vec{x})$ which descends to a well-defined injective map

$$Q_H : L/L_{\mathfrak{a}\text{-even}} \hookrightarrow \mathfrak{a}/2\mathfrak{a}.$$

From the definition of $L_{\mathfrak{a}\text{-even}}$ and the polarization identity we know that Q_H is an (additive) homomorphism of abelian groups, but usually not a linear map of $\mathcal{O}_F/\mathfrak{p}^{e_\mathfrak{p}}$-modules. Since $e_\mathfrak{p} \leq 1$ and $\mathfrak{p} \mid 2$ we know that $e_\mathfrak{p} = 1$ and so both the domain and range are $\mathbb{F}_\mathfrak{p}$-vector spaces. By Remark 3.9 we know that Q_H is a semilinear map, and so its image is a non-zero subspace of $\mathbb{F}_\mathfrak{p}$. This shows Q_H is surjective, hence bijective, proving the lemma. □

Algorithm 4.6 (Construct a maximal $\mathfrak{a}$-valued quadratic lattice). *Given a non-degenerate quadratic space (V, Q) over a number field F where $p = 2$ is unramified, and a non-zero fractional ideal $\mathfrak{a}$ of F, we give an algorithm for producing a maximal $\mathfrak{a}$-valued quadratic lattice L on (V, Q).*

1. *Use Algorithm 3.16 to find an $\mathfrak{a}$-maximal lattice L in the Hessian bilinear space (V, H) associated to (V, Q). Let $\mathbb{S}$ be the finite set of primes $\mathfrak{p}$ of $\mathcal{O}_F$ where L is not $\mathfrak{a}$-even at $\mathfrak{p}$. (Necessarily $\mathfrak{p} \in \mathbb{S} \implies \mathfrak{p} \mid 2$.)*

2. *For each $\mathfrak{p} \in \mathbb{S}$, we use Theorem 5.6 to check if some $\mathfrak{p}$-neighbor $L'$of L is $\mathfrak{a}$-even at $\mathfrak{p}$. If so, then replace L by L'. If not, then replace L by $L_{\mathfrak{a}\text{-}even\ at\ \mathfrak{p}}$.*

3. *This remaining L is a maximal $\mathfrak{a}$-even lattice in (V, H), so L is also a maximal $\mathfrak{a}$-valued quadratic lattice on (V, Q).*

Proof. Given L in step 1, we know by the correspondence in Lemma 4.4 that L is an $\mathfrak{a}$-maximal quadratic lattice at all primes $\mathfrak{p} \notin \mathbb{S}$. For each $\mathfrak{p} \in \mathbb{S}$ (so necessarily $\mathfrak{p} \mid 2$) we know that $L_{\mathfrak{a}\text{-even at }\mathfrak{p}}$ is $\mathfrak{a}$-even at $\mathfrak{p}$, but it may not be maximal among lattices in (V, H) with this property. If $L_{\mathfrak{a}\text{-even at }\mathfrak{p}}$ is maximal $\mathfrak{a}$-even at $\mathfrak{p}$, then by Lemma 4.4 we see that it is also a maximal $\mathfrak{a}$-valued *quadratic* lattice at $\mathfrak{p}$ and at all primes $\mathfrak{q} \notin \mathbb{S}$. If $L_{\mathfrak{a}\text{-even at }\mathfrak{p}}$ is not maximal $\mathfrak{a}$-even at $\mathfrak{p}$, then we have the inclusion $L_{\mathfrak{a}\text{-even at }\mathfrak{p}} \subsetneq L' \subseteq L'_{Max}$ where L' maximal $\mathfrak{a}$-even at $\mathfrak{p}$, L'_{Max} maximal $\mathfrak{a}$-valued at $\mathfrak{p}$, and $(L')_\mathfrak{q} = (L'_{Max})_\mathfrak{q} = L_\mathfrak{q}$ for all primes $\mathfrak{q} \neq \mathfrak{p}$.

By the Lemma 2.13, we have that

$$[L : L_{\mathfrak{a}\text{-even at }\mathfrak{p}}]^2 \cdot |\mathcal{D}(L)| = |\mathcal{D}(L_{\mathfrak{a}\text{-even at }\mathfrak{p}})| = [L'_{Max} : L_{\mathfrak{a}\text{-even at }\mathfrak{p}}]^2 \cdot |\mathcal{D}(L'_{Max})|,$$

but Lemma 3.17 shows that $|\mathcal{D}(L)| = |\mathcal{D}(L'_{Max})|$, so $[L : L_{\mathfrak{a}\text{-even at }\mathfrak{p}}] = [L'_{Max} : L_{\mathfrak{a}\text{-even at }\mathfrak{p}}]$. This together with Lemma 4.5 shows that $[L'_{Max} : L_{\mathfrak{a}\text{-even at }\mathfrak{p}}] = [L : L_{\mathfrak{a}\text{-even at }\mathfrak{p}}] = \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{p})$, so $[L' : L_{\mathfrak{a}\text{-even at }\mathfrak{p}}]$ divides $\mathrm{N}_{F/\mathbb{Q}}(\mathfrak{p})$.

Since $L'/L_{\mathfrak{a}\text{-even at }\mathfrak{p}}$ is a non-zero torsion $\mathcal{O}_\mathfrak{p}$-module its annihilator is $\mathfrak{p}^k$ for some k, we know that $[L' : L_{\mathfrak{a}\text{-even at }\mathfrak{p}}] = \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{p}^k)$, so $k = 1$ and $L' = L'_{Max}$. Finally, if $H(L, L') \subseteq \mathfrak{a}$ then the lattice $L + L'$ would be $\mathfrak{a}$-valued, violating the maximality of L. Therefore L' is a $\mathfrak{p}$-neighbor of L. □

Remark 4.7 (Maximal Quadratic lattices when $p = 2$ is ramified)**.** *If the prime $p = 2$ ramifies in F then the theory of integral quadratic forms/lattices is more complicated at any prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$ where $e_\mathfrak{p} := \mathrm{ord}_\mathfrak{p}(2) > 1$. (E.g. Lemma 4.5.) In the language of O'Meara's book [27, §82E, p227] this is because the containment of norm and (Gram) scale ideals*

$$2\mathfrak{s}(L_\mathfrak{p}) \subseteq \mathfrak{n}(L_\mathfrak{p}) \subseteq \mathfrak{s}(L_\mathfrak{p})$$

can both be strict containments when $e_\mathfrak{p} > 1$, so one cannot normalize the values of quadratic form (given by $\mathfrak{n}(L)$) by studying the values of the associated Hessian bilinear form (given by $2\mathfrak{s}(L)$) alone. In general there are many intermediate possibilities for the local norm ideals $\mathfrak{n}(L_\mathfrak{p})$ which must be analyzed to pass from a maximal bilinear lattice to a maximal quadratic lattice, which makes it difficult to generalize this algorithm to deal with ramified primes $\mathfrak{p} \mid 2$. In a future paper, we hope to give a different algorithm that produces $\mathfrak{a}$-maximal quadratic lattices over number fields where the prime $p = 2$ is allowed to ramify.

5 Neighbors and Genera

In this section we will explain theory of "Neighboring lattices", originally due to Kneser [24], and how it can be used to find representatives for a given genus of quadratic lattices. Special care will be given to describe $\mathfrak{p}$-neighbors for an arbitrary (possibly dyadic) prime ideal $\mathfrak{p}$ in the ring of integers of a number field, as this will be useful in the passage from a maximal bilinear lattice to a maximal quadratic lattice.

Definition 5.1 ($\mathfrak{p}$-neighbors)**.** *Suppose that L and L' are two $\mathfrak{a}$-valued quadratic lattices in a common quadratic space (V, Q) over a number field F, and that $\mathfrak{p}$ is a (non-zero) prime ideal of $\mathcal{O}_F$. Then we say that L and L' are* **$\mathfrak{p}$-neighboring $\mathfrak{a}$-lattices** *(or* **$\mathfrak{p}$-neighbors***) if $[L : L \cap L'] = [L' : L \cap L'] = \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{p})$ and the Hessian bilinear form $H(L, L') \nsubseteq \mathfrak{a}$.*

The $\mathfrak{p}$-neighboring lattices of a given lattice L can be described very explicitly in terms of the vectors of L whose values generate the ideal $\mathfrak{a}\mathfrak{p}$. These vectors also have a very nice description in terms of the residual quadric in the projective space of the $\mathbb{F}_\mathfrak{p}$-vector space $L/\mathfrak{p}L$, which we now define.

Definition 5.2 (Residual Quadrics)**.** *Suppose that L is an $\mathfrak{a}$-valued lattice in a n-dimensional quadratic space (V, Q) over a number field F, and that $\mathfrak{p}$ is a (non-zero) prime ideal of $\mathcal{O}_F$.*

Then we define the **residual $\mathfrak{a}$-quadric at $\mathfrak{p}$** *as the quadric hypersurface* $\mathcal{Q}_{\mathfrak{p};\mathfrak{a}} \subseteq \mathbb{P}(L/\mathfrak{p}L) \cong \mathbb{P}^{n-1}(\mathbb{F}_{\mathfrak{p}})$ *given by the homogeneous equation* $Q(\vec{x}) \in \mathfrak{a}\mathfrak{p}$. *I.e.,*

$$\mathcal{Q}_{\mathfrak{p};\mathfrak{a}} := \mathcal{Q}_{L,\mathfrak{p};\mathfrak{a}} := \mathbb{P}(\{\vec{x} \in L/\mathfrak{p}L \mid Q(\vec{x}) \in \mathfrak{a}\mathfrak{p} \text{ and } \vec{x} \neq \vec{0}\}).$$

Remark 5.3. *In terms of the latttice L, those $\vec{x} \in L$ reducing to $\mathcal{Q}_{\mathfrak{p};\mathfrak{a}}$ are exactly those $\vec{x} \notin \mathfrak{p}L$ for which $Q(\vec{x}) \in \mathfrak{a}\mathfrak{p}$.*

The singular points on $\mathcal{Q}_{\mathfrak{p};\mathfrak{a}}$, which can be understood from several different perspectives. Saying that $P \in \mathcal{Q}_{\mathfrak{p};\mathfrak{a}}$ is a **nonsingular point** by definition means that the gradient vector $(\vec{\nabla}Q)(P) := [\frac{\partial Q}{\partial x_1}(P) : \cdots : \frac{\partial Q}{\partial x_n}(P)] \neq \vec{0} \in (\mathfrak{a}/\mathfrak{p}\mathfrak{a})^n$, where $[x_1 : \cdots : x_n]$ are homogeneous coordinates for $\mathbb{P}^{n-1}(\mathbb{F}_{\mathfrak{p}})$. We can also rewrite the gradient condition in terms of the Hessian bilinear form.

Lemma 5.4 (Hessian singularity criterion)**.** *Suppose that $P \in \mathcal{Q}_{\mathfrak{p};\mathfrak{a}}$ corresponds to the non-zero line $\mathbb{F}_{\mathfrak{p}} \cdot \vec{v}_P \in L/\mathfrak{p}L$. Then P is a singular point of $\mathcal{Q}_{\mathfrak{p};\mathfrak{a}} \iff$ the $(\mathfrak{a}/\mathfrak{a}\mathfrak{p})$-valued linear form $H(\vec{v}_P, \cdot)$ on $L/\mathfrak{p}L$ is identically zero.*

Proof. This follows from noticing that $H(\vec{x}, \vec{y}) = (\vec{\nabla}Q)(\vec{x}) \cdot \vec{y}$, hence P is singular $\iff$ $H(\vec{v}_P, \vec{w}) \in \mathfrak{a}\mathfrak{p}$. □

Remark 5.5 (Singular points and duality)**.** *Another description of the singular points of $\mathcal{Q}_{\mathfrak{p};\mathfrak{a}}$ in terms of dual lattices can be given by noticing that for $\vec{x}, \vec{y} \in L$ we have that*

$$H(\vec{x}, \vec{y}) \in \mathfrak{a}\mathfrak{p} \text{ for all } \vec{y} \in L \iff \vec{x} \in (\mathfrak{p}L^{\#\mathfrak{a}} \cap L).$$

This shows that the singular points of $\mathcal{Q}_{\mathfrak{p};\mathfrak{a}}$ are exactly the points of $\mathcal{Q}_{\mathfrak{p};\mathfrak{a}}$ lying in the projective subspace $\mathbb{P}((\mathfrak{p}L^{\#\mathfrak{a}} \cap L)/\mathfrak{p}L) \subseteq \mathbb{P}(L/\mathfrak{p}L)$. For this reason, we call $\mathbb{P}((\mathfrak{p}L^{\#\mathfrak{a}} \cap L)/\mathfrak{p}L)$ the **(residual) $\mathfrak{a}$-singular subspace**.

It is interesting to notice that the singular subspace is closely related to the structure of the $\mathfrak{a}$-discriminant module $\mathcal{D}_{\mathfrak{a}}(L)$, and that for $\mathfrak{a}$-modular lattices (where $L^{\#\mathfrak{a}} = L$) there are no singular points on $\mathcal{Q}_{\mathfrak{p};\mathfrak{a}}$.

With these definitions we can now parametrize the $\mathfrak{p}$-neighbors of L in terms of the non-singular points of its residual quadric at $\mathfrak{p}$.

Theorem 5.6 ($\mathfrak{p}$-neighbors via residual geometry)**.** *The $\mathfrak{p}$-neighboring $\mathfrak{a}$-lattices of a given $\mathfrak{a}$-valued quadratic lattice L are in bijection with the non-singular points $\mathcal{Q}^{ns}_{\mathfrak{p};\mathfrak{a}}$ on its residual $\mathfrak{a}$-quadric at $\mathfrak{p}$. More explicitly, this bijection is given by the map*

$$\eta : P \in \mathcal{Q}^{ns}_{\mathfrak{p};\mathfrak{a}} \quad \mapsto \quad L' := L'' + \tfrac{1}{\mathfrak{p}} \cdot \vec{v}_P$$

where $L'' := \{\vec{x} \in L \mid H(\vec{v}_P, \vec{x}) \equiv 0 \pmod{\mathfrak{a}\mathfrak{p}}\}$ and $\vec{v}_P$ is any lift to L of a non-zero isotropic vector in $L/\mathfrak{p}^2L$ (i.e. $Q(\vec{v}_P) \in \mathfrak{p}^2\mathfrak{a}$ and $\vec{v}_P \notin \mathfrak{p}^2L$) that reduces to the given point $P \in \mathcal{Q}^{ns}_{\mathfrak{p};\mathfrak{a}}$ under the canonical reduction map $L \to \mathbb{P}(L/\mathfrak{p}L)$. Such a $\vec{v}_P \in L$ always exists since P is a non-singular point, and also $L'' = L \cap L'$.

Proof. 1) Non-singular shearing: To see that $P \in \mathcal{Q}^{\mathrm{ns}}_{\mathfrak{p};\mathfrak{a}}$ gives rise to some $\vec{v}_P$ as above, notice that Lemma 5.4 says that the gradient $(\vec{\nabla}Q)(\vec{v}_P) \in L/\mathfrak{p}L$ is non-zero in $\mathfrak{a}/\mathfrak{p}\mathfrak{a}$, so by chosing any lift $\vec{w} \in L$ of $(\vec{\nabla}Q)(\vec{v}_P)$ we can find some $\lambda \in \mathfrak{p}$ so that $Q(\vec{v}_P + \lambda\vec{w}) \in \mathfrak{a}\mathfrak{p}^2$.

2) $\mathfrak{p}$-neighbors: To see that $\eta(P)$ is a $\mathfrak{p}$-neighboring $\mathfrak{a}$-lattice of L, we notice that by Lemma 5.4 the non-singularity of P shows that the linear form $H(\vec{v}_P, \cdot)$ on L has non-trivial image in $\mathfrak{a}/\mathfrak{p}\mathfrak{a}$, hence $L/L'' \cong \mathbb{F}_\mathfrak{p}$ as abelian groups and $[L : L''] = \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{p})$. Since $\vec{v}_P \notin \mathfrak{p}L$, we know $\mathfrak{p}^{-1}\vec{v}_P \notin L$ and so similarly $L/L'' \cong \mathbb{F}_\mathfrak{p}$ and $[L' : L''] = \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{p})$. Finally we see that L and L' are $\mathfrak{p}$-neighbors since from 1) we have $H(\vec{v}_P, \vec{w}) \notin \mathfrak{p}\mathfrak{a}$ for some $\vec{w} \in L$, so therefore $H(\vec{w}, \mathfrak{p}^{-1}\vec{v}_P) \subseteq H(L, L') \nsubseteq \mathfrak{a}$.

3) Injectivity: To see that $\eta(P)$ is injective suppose that $\vec{v}_P$ and $\vec{v}_Q$ in L correspond to the points P and Q in $\mathcal{Q}^{\mathrm{ns}}_{\mathfrak{p};\mathfrak{a}}$, and that $\eta(P) = \eta(Q) = L'$. Then from 2) we know that $L + L' = \mathfrak{p}^{-1}\vec{v}_P + L = \mathfrak{p}^{-1}\vec{v}_Q + L$, so $\vec{v}_P$ and $\vec{v}_Q$ lie on the same residual line through the origin $\mathfrak{p}(L + L')/\mathfrak{p}L \subseteq L/\mathfrak{p}L$, so $P = Q$ on $\mathcal{Q}^{\mathrm{ns}}_{\mathfrak{p};\mathfrak{a}} \subseteq \mathbb{P}(L/\mathfrak{p}L)$.

4) Surjectivity: To see that $\eta(P)$ is surjective we first start with a $\mathfrak{p}$-neighbor L' of L and construct some point $P \in \mathcal{Q}^{\mathrm{ns}}_{\mathfrak{p};\mathfrak{a}}$ by the rule $P := \mathbb{P}(\mathfrak{p}(L + L')/\mathfrak{p}L) \subset \mathbb{P}(L/\mathfrak{p}L)$. Since $[L + L' : L] = [L' : L \cap L'] = \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{p})$ we know that $\dim_{\mathbb{F}_\mathfrak{p}}(L + L') = \dim_{\mathbb{F}_\mathfrak{p}}(L) + 1$ and so P is a point in $\mathbb{P}(L/\mathfrak{p}L)$. To see that $P \in \mathcal{Q}_{\mathfrak{p};\mathfrak{a}}$ we choose some non-zero $\vec{v}' \in L'/(L \cap L')$ giving $L + L' = L + \mathcal{O}_F\vec{v}'$ and set $\vec{v}_P := \pi_\mathfrak{p}\vec{v}'$ (giving $\mathbb{P}(\vec{v}_P) = P$). Knowing $\vec{v}' \in L'$ ensures that $Q(\vec{v}') \in \mathfrak{a}$, so $Q(\vec{v}_P) \in \mathfrak{a}\mathfrak{p}^2$ showing $P \in \mathcal{Q}_{\mathfrak{p};\mathfrak{a}}$. The non-singularity of P follows because

$$H(\mathfrak{p}(L + L'), L') = H(\mathfrak{p}L, L) + H(\mathfrak{p}L', L) \subseteq \mathfrak{p}\mathfrak{a} + \mathfrak{a} \subseteq \mathfrak{a}$$

(using here that $\mathfrak{p}L' \subseteq L \implies H(L, L') \subseteq \mathfrak{p}^{-1}\mathfrak{a}$), and if P were singular then it would force $H(L', L) \subseteq \mathfrak{a}$, which cannot occur so $P \in \mathcal{Q}^{\mathrm{ns}}_{\mathfrak{p};\mathfrak{a}}$.

To see that $\eta(P) = L'$, we first compute the sublattice

$$K := \{\vec{x} \in L + L' \mid H(\vec{v}', \vec{x}) \subseteq \mathfrak{a}\} \subset L + L'.$$

for $\vec{v}'$ as above, which is proper since $H(L, L') \nsubseteq \mathfrak{a}$. Since $\vec{v}' \in L'$ we see that $L' \subseteq K$, and $H(L', L') \subseteq \mathfrak{p}^{-1}\mathfrak{a}$ tells us that $(L + L')/K \cong \mathbb{F}_\mathfrak{p}$ as abelian groups, giving $[L + L' : K] = \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{p})$ and so $K = L'$. With this, we see that η first constructs the sublattice $L'' = L \cap K = L \cap L'$ and then takes $L' := \mathfrak{p}^{-1}\vec{v}_P + L''$, and this L' must be the $\mathfrak{p}$-neighbor L' that we started with since $\pi_\mathfrak{p}^{-1}\vec{v}_P = \vec{v}' \in L'$. This completes the proof the Theorem. □

Remark 5.7 ($\mathfrak{p}$-neighbor references)**.** *The idea of neighboring lattices was introduced in Kneser's paper [24], and is also discussed in his German book [25]. There are other discussions of $\mathfrak{p}$-neighboring lattices in English (e.g. [13, p202], [43, §3.1, pp31-35], [34, §1, pp1-3], [32, §2, pp738–743]), though these restrict either the base field (i.e. $F = \mathbb{Q}$) or the primes considered (i.e. $\mathfrak{p} \nmid |\mathcal{D}(L)|$) or both, and also assume that the quadratic lattices are $\mathcal{O}_F$-valued.*

The author has been unable to find a description of $\mathfrak{p}$-neighbors for $\mathfrak{a}$-maximal lattices discussed in the literature, so the notion of $\mathfrak{p}$-neighboring $\mathfrak{a}$-lattices here appears to be new *(though perhaps not very deep). We include it here to show that there is a natural notion of $\mathfrak{p}$-neighbors for lattices of any fixed value ideal $\mathfrak{a} := Q(L) \cdot \mathcal{O}_F$, and to provide context for results like [7, 8] that begin to describe connections between arithmetic and geometric models of lattices. This connection is an interesting direction for future research.*

For completeness, we conclude with an important application of the theory of $\mathfrak{p}$-neighboring lattices to enumerate all classes in a given genus of totally definite quadratic lattices over a totally real number field F. This result is essentially due to Benham and Hsia [2] where they actually give a way to compute all classes in the spinor genus of L, and here we describe a well-known modification of their idea using a mass formula to determine when the algorithm terminates.

The advantage of this modification is that we do not need to compute spinor norms in the idele group of F, but it comes at the rather high cost of needing an exact mass formula for the genus of quadratic lattices in question.

Algorithm 5.8 (Enumerating classes in a genus of quadratic lattices; [2])**.** *Given an $\mathfrak{a}$-valued quadratic lattice L in a non-degenerate totally definite quadratic space (V, Q) over a totally real number field F of rank ≥ 3, then we give an algorithm for finding representative lattices $L_i \subset V$ for every class in the genus of L.*

Proof. Begin with the set of lattices $\mathbb{S} = \{L\}$. Take the smallest (w.r.t. $|\mathrm{N}_{F/\mathbb{Q}}(\cdot)|$) prime $\mathfrak{p} \nmid |\mathcal{D}(L)|$ and compute the set $\mathbb{T}$ of (finitely many) non-isometric $\mathfrak{p}$-power neighbors of each $L \in \mathbb{S}$ and append $\mathbb{T}$ to $\mathbb{S}$. (Here we know we have computed $\mathbb{T}$ when taking $\mathfrak{p}$-neighbors of all classes of lattices of $\mathbb{T}$ produces no new classes.) If the partial mass

$$\mathrm{Mass}(\mathbb{S}) := \sum_{L' \in \mathbb{S}} \frac{1}{\#\mathrm{Aut}(L')}$$

satisfies $\mathrm{Mass}(\mathbb{S}) < \mathrm{Mass}(L)$, then repeat the procedure for the next smallest prime until $\mathrm{Mass}(\mathbb{S}) = \mathrm{Mass}(L)$. By [2, Proposition 1, (1.1), and Theorem 2] the $\mathfrak{p}$-power neighbors at the primes $\mathfrak{p}$ of bounded norm exhaust all classes in the genus of L. □

Remark 5.9 (Mass formula and halting conditions for indefinite lattices)**.** *Algorithm 5.8 also works for indefinite lattices L, though in this case the mass of a genus $\mathrm{Gen}(L)$ is given as a sum over all class representatives L_i of the covolumes $\mathrm{Vol}(\mathcal{Z}/\mathrm{Aut}_{\mathcal{O}_F}(L_i))$ of the integral automorphism group $\mathrm{Aut}_{\mathcal{O}_F}(L_i)$ with respect to some fixed measure on the symmetric space $\mathcal{Z}$ of the orthogonal group of Q (e.g. [18]). While these terms are computable in principle (by giving a presentation for $\mathrm{Aut}_{\mathcal{O}_F}(L_i)$ and computing an explicit integral), this is not nearly as pleasant as counting the finitely many automorphisms arising in the totally definite case.*

Remark 5.10 (Class numbers for indefinite lattices when $n \geq 3$)**.** *Conveniently, the computation of class numbers of indefinite lattices in $n \geq 3$ variables is much simpler* *that for definite lattices because of the strong approximation property of the spin group (e.g. [27, §104:4-5, pp315-319; §102:7-8, pp300-304]). From this property one can show that each spinor genus in such a genus contains exactly one class, so the class number is just the number of spinor genera in the genus and this number is known to be an easily (locally) computed power of two. Therefore Algorithm 5.8 and Remark 5.9 would only be interesting when $n = 2$, in which case these masses can be computed in terms of logarithms of fundamental units in quadratic extensions of F.*

Remark 5.11 (Literature)**.** *The idea of using an explicit mass formula to determine explicit genus representatives is well-known to experts, and has been used for some time to prove that certain genera have class number one (e.g. [40, §16.6, pp133-134], [35, §5.16, pp33-34]) or small class number, however almost all actual computational results have been limited to either the case $F = \mathbb{Q}$ or to unimodular lattices over real quadratic fields. When $[F : \mathbb{Q}] > 1$, the author is only aware of the papers [11, 22, 21, 23, 31].*

References

[1] Mikhail Belolipetsky. Counting maximal arithmetic subgroups. *Duke Math. J.*, 140(1):1–33, 2007. With an appendix by Jordan Ellenberg and Akshay Venkatesh.

[2] J. W. Benham and J. S. Hsia. Spinor equivalence of quadratic forms. *J. Number Theory*, 17(3):337–342, 1983.

[3] Siegfried Böcherer and Gabriele Nebe. On theta series attached to maximal lattices and their adjoints. *J. Ramanujan Math. Soc.*, 25(3):265–284, 2010.

[4] H. Brandt. Diskriminante einer quadratischen form. In Dr. Walter Saxner, editor, *Negotiations of the International Congress of Mathematicians Zurich 1932*, volume II, pages 10–11. Orell Füssli Verlag Zurich and Leipzig, 1932.

[5] H. Brandt. Zur Zahlentheorie der quadratischen Formen. *Jahresbericht der Deutschen Mathematiker-Vereinigung*, 47:149–159, 1937.

[6] H. Brandt. Über quadratische Kern- und Stammformen. In *Festschrift zum 60. Geburstag von Prof. Dr. Andreas Speiser*, pages 87–104. Füssli, Zürich, 1945.

[7] J. Brzezinski. Lattices and models of fields of genus 0. *Math. Scand.*, 32:22–30, 1973.

[8] J. Brzezinski. Remarks on relations between maximal lattices and relatively minimal models. *Math. Scand.*, 35:25–28, 1974.

[9] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[10] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[11] Patrick J. Costello and John S. Hsia. Even unimodular 12-dimensional quadratic forms over $\mathbf{Q}(\sqrt{5})$. *Adv. in Math.*, 64(3):241–278, 1987.

[12] Wee Teck Gan, Jonathan P. Hanke, and Jiu-Kang Yu. On an exact mass formula of Shimura. *Duke Math. J.*, 107(1):103–133, 2001.

[13] Larry J. Gerstein. *Basic quadratic forms*, volume 90 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2008.

[14] Dorian Goldfeld. The Gauss class number problem for imaginary quadratic fields. In *Heegner points and Rankin L-series*, volume 49 of *Math. Sci. Res. Inst. Publ.*, pages 25–36. Cambridge Univ. Press, Cambridge, 2004.

[15] Jonathan Hanke. Advanced Quadratic Forms library for the Sage computer algebra system. Ticket #11940 at `http://trac.sagemath.org/`. (≈ 11,000 lines).

[16] Jonathan Hanke. Quadratic Forms library for the Sage computer algebra system. Tickets #4470, 5418, and 5954 at `http://trac.sagemath.org/`. (≈ 22,000 lines).

[17] Jonathan Hanke. Local densities and explicit bounds for representability by a quadratic form. *Duke Math. J.*, 124(2):351–388, 2004.

[18] Jonathan Hanke. An exact mass formula for quadratic forms over number fields. *J. Reine Angew. Math.*, 584:1–27, 2005.

[19] Jonathan Hanke. Enumerating maximal definite quadratic forms of bounded class number over $\mathbb{Z}$ in $n \geq 3$ variables. `http://arxiv.org/abs/1110.1876`, 2011. (Submitted).

[20] Takahiro Hiraoka. On the class number of the genus of $\mathbb{Z}$-maximal lattices with respect to quadratic form of the sum of squares. *J. Math. Kyoto Univ.*, 46(2):291–302, 2006.

[21] J. S. Hsia. Even positive definite unimodular quadratic forms over real quadratic fields. *Rocky Mountain J. Math.*, 19(3):725–733, 1989. Quadratic forms and real algebraic geometry (Corvallis, OR, 1986).

[22] J. S. Hsia and D. C. Hung. Even unimodular 8-dimensional quadratic forms over $\mathbf{Q}(\sqrt{2})$. *Math. Ann.*, 283(3):367–374, 1989.

[23] David C. Hung. Even positive definite unimodular quadratic forms over $\mathbf{Q}(\sqrt{3})$. *Math. Comp.*, 57(195):351–368, 1991.

[24] Martin Kneser. Klassenzahlen definiter quadratischer Formen. *Arch. Math.*, 8:241–250, 1957.

[25] Martin Kneser. *Quadratische Formen*. Springer-Verlag, Berlin, 2002. Revised and edited in collaboration with Rudolf Scharlau.

[26] Manabu Murata. On the applications of Shimura's mass formula. In *Proceedings of the Symposium on Algebraic Number Theory and Related Topics*, RIMS Kôkyûroku Bessatsu, B4, pages 51–61. Res. Inst. Math. Sci. (RIMS), Kyoto, 2007.

[27] O. T. O'Meara. *Introduction to quadratic forms*. Springer-Verlag, New York, 1971. Second printing, corrected, Die Grundlehren der mathematischen Wissenschaften, Band 117.

[28] O. T. O'Meara. *Lectures on linear groups*. American Mathematical Society, Providence, R.I., 1974. Expository Lectures from the CBMS Regional Conference held at Arizona State University, Tempe, Ariz., March 26–30, 1973, Conference Board of the Mathematical Sciences Regional Conference Series in Mathematics, No. 22.

[29] Paul Ponomarev. Arithmetic of quaternary quadratic forms. *Acta Arith.*, 29(1):1–48, 1976.

[30] Paul Ponomarev. Ternary quadratic forms and Shimura's correspondence. *Nagoya Math. J.*, 81:123–151, 1981.

[31] Rudolf Scharlau. Unimodular lattices over real quadratic fields. *Math. Z.*, 216(3):437–452, 1994.

[32] Rudolf Scharlau and Boris Hemkemeier. Classification of integral lattices with large class number. *Math. Comp.*, 67(222):737–749, 1998.

[33] Winfried Scharlau. *Quadratic and Hermitian forms*, volume 270 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1985.

[34] Rainer Schulze-Pillot. An algorithm for computing genera of ternary and quaternary quadratic forms. In *ISSAC '91: Proceedings of the 1991 international symposium on Symbolic and algebraic computation*, pages 134–143, New York, NY, USA, 1991. ACM.

[35] Goro Shimura. An exact mass formula for orthogonal groups. *Duke Math. J.*, 97(1):1–66, 1999.

[36] Goro Shimura. The number of representations of an integer by a quadratic form. *Duke Math. J.*, 100(1):59–92, 1999.

[37] Goro Shimura. *Arithmetic and analytic theories of quadratic forms and Clifford groups*, volume 109 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2004.

[38] Goro Shimura. Integer-valued quadratic forms and quadratic Diophantine equations. *Doc. Math.*, 11:333–367 (electronic), 2006.

[39] Goro Shimura. Quadratic Diophantine equations, the class number, and the mass formula. *Bull. Amer. Math. Soc. (N.S.)*, 43(3):285–304 (electronic), 2006.

[40] Carl Ludwig Siegel. *Lectures on the analytical theory of quadratic forms*. Notes by Morgan Ward. Third revised edition. Buchhandlung Robert Peppmüller, Göttingen, 1963.

[41] H. M. Stark. The Gauss class-number problems. In *Analytic number theory*, volume 7 of *Clay Math. Proc.*, pages 247–256. Amer. Math. Soc., Providence, RI, 2007.

[42] W. A. Stein et al. *Sage Mathematics Software (Version 4.6.2)*. The Sage Development Team, 2011. `http://www.sagemath.org`.

[43] Gonzalo Tornaria. *The Brandt module of ternary quadratic lattices*. PhD thesis, University of Texas, Austin, 2005.

[44] John Voight. Identifying the matrix ring: Algorithms for quaternion algebras and quadratic forms. `http://arxiv.org/abs/1004.0994`, 2010.

[45] Lynne H. Walling. Explicit Siegel theory: an algebraic approach. *Duke Math. J.*, 89(1):37–74, 1997.

[46] Tonghai Yang. Local densities of 2-adic quadratic forms. *J. Number Theory*, 108(2):287–345, 2004.

[47] Takashi Yoshinaga. On the solutions of quadratic Diophantine equations. *Doc. Math.*, 15:347–385, 2010.