Canad. J. Math. Vol. 77 (6), 2025 pp. 1938–1965
http://dx.doi.org/10.4153/S0008414X24000592

On elements of prescribed norm in maximal orders of a quaternion algebra

Eyal Z. Goren and Jonathan R. Love

Abstract. Let $\mathcal{O}$ be a maximal order in the quaternion algebra over $\mathbb{Q}$ ramified at p and ∞. We prove two theorems that allow us to recover the structure of $\mathcal{O}$ from limited information. The first says that for any infinite set S of integers coprime to p, $\mathcal{O}$ is spanned as a $\mathbb{Z}$-module by elements with norm in S. The second says that $\mathcal{O}$ is determined up to isomorphism by its theta function.

1 Introduction

Let p be a prime. Up to isomorphism, there is a unique quaternion algebra B_p over $\mathbb{Q}$ ramified at exactly p and ∞. The quaternion algebra B_p comes equipped with a canonical involution $x \mapsto \overline{x}$, a norm $x \mapsto N(x) \coloneqq x\overline{x}$, and a trace $x \mapsto \mathrm{Tr}(x) \coloneqq x + \overline{x}$. For background on quaternion algebras and their orders, the reader may consult [4, 21].

There will typically be many non-isomorphic maximal orders in B_p: the number of isomorphism classes of maximal orders in B_p (the *type number* of a maximal order) is between $\frac{p-1}{24}$ and $\frac{p+13}{12}$ inclusive [21, Exercise 30.6, Proposition 30.9.2]. This article presents two theorems, each of which allows one to recover information about a maximal order $\mathcal{O}$ in B_p, given only information about elements in $\mathcal{O}$ with prescribed norms.

Theorem 1.1 *Let $\mathcal{O}$ be a maximal order in B_p, and let S be an infinite set of positive integers coprime to p. There is a generating set for $\mathcal{O}$ as a $\mathbb{Z}$-module consisting of elements with norm in S.*

Remark 1.2 See Remark 2.11 for a discussion of the coprime to p condition. The theorem still holds if we take $\mathcal{O}$ to be an Eichler order in B_p with index coprime to 6, but is false for every other Eichler order in B_p (see Section 2.3.4).

To prove Theorem 1.1, we first establish a local–global principle for lattices having the property of being generated as a $\mathbb{Z}$-module by elements of norm in a given set S (Theorem 2.2). In Section 2.3, we check that under the conditions of Theorem 1.1, all the local conditions of Theorem 2.2 are satisfied.

As a special case, we can take $S = \{\ell^k : k \geq 0\}$ for any prime $\ell \neq p$, and conclude that maximal orders are generated by elements of norm equal to a power of ℓ. This

Received by the editors July 28, 2023; revised March 13, 2024; accepted July 2, 2024.
The first author was supported by an NSERC Discovery Grant, and the second author was supported by a CRM-ISM postdoctoral fellowship.
AMS subject classification: **11R52**, 11H55.
Keywords: Quaternion algebra, maximal order, theta function, quadratic form, norm.

has implications for the study of isogeny graphs of supersingular elliptic curves. If E is a supersingular elliptic curve over $\overline{\mathbb{F}_p}$, then $\mathrm{End}(E)$ is a maximal order in B_p, and endomorphisms of E with norm a power of ℓ can be generated by finding cycles from E in the ℓ-isogeny graph of supersingular curves over $\overline{\mathbb{F}_p}$ (see, for instance, [1, 9, 14]). Theorem 1.1 implies that such endomorphisms generate the entire endomorphism ring as an abelian group. This is used as a heuristic assumption in [9, Section 3.3]. This question is considered by [1], who determine when two cycles generate a full rank sublattice of $\mathrm{End}(E)$ (as an order), as well as a necessary condition for these cycles to generate $\mathrm{End}(E)$, but show by example that these necessary conditions are not sufficient.

The second result is that the isomorphism type of $\mathcal{O}$ is determined by the number of elements of each norm. Given a lattice Λ with integral quadratic form Q, we define the *theta function* of Λ,

$$\theta_\Lambda(q) \coloneqq \sum_{x\in\Lambda} q^{Q(x)},$$

so that the coefficient of q^n is the number of elements of norm n. This function encodes the spectrum of the Laplace operator of the Riemannian manifold $\Lambda \otimes \mathbb{R}/\Lambda$ (see [16] for more on this analytic interpretation). When $\mathcal{O}$ is a maximal order in B_p, $\theta_{\mathcal{O}}(q)$ is a modular form of weight 2 and level $\Gamma_0(p)$.

We say two lattices are *isospectral* if their theta functions are equal. Lattices of rank $n \le 3$ are uniquely determined up to isometry by their theta function [18], but in rank 4 and above, there exist pairs of non-isometric isospectral lattices. Even if we restrict to the set of lattices in the genus of a fixed maximal order of B_p, there may exist pairs of non-isometric integral lattices in B_p whose left and right orders are maximal and yet have the same theta function (see Section 3.1 for examples). However, we prove that this does not occur if we restrict to maximal orders in B_p.

Theorem 1.3 *If $\mathcal{O}, \mathcal{O}'$ are maximal orders in B_p with $\theta_{\mathcal{O}} = \theta_{\mathcal{O}'}$, then $\mathcal{O} \simeq \mathcal{O}'$.*

As an immediate consequence, a supersingular elliptic curve over $\overline{\mathbb{F}_p}$ can be identified uniquely up to Frobenius twist by the number of endomorphisms of each degree.

The proof of Theorem 1.3 is divided into two steps: the first may be of independent interest so we state it here as a separate theorem. Given an order $\mathcal{O}$ in B_p, we define its *Gross lattice*

$$\mathcal{O}^T \coloneqq \{2x - \mathrm{Tr}(x) : x \in \mathcal{O}\}.$$

This is a strict subset of the set of trace 0 elements in $\mathcal{O}$; see Section 3.3 for further details and discussion of the Gross lattice. For $i = 1, 2, 3$, the ith *successive minimum* of $\mathcal{O}^T$ is the minimum value D_i such that the span of all elements $\alpha \in \mathcal{O}^T$ with $N(\alpha) \le D_i$ has dimension at least i (Definition 3.3).

In [6], Chevyrev and Galbraith determine conditions under which the successive minima of the Gross lattice of $\mathcal{O}$ determine the isomorphism class of $\mathcal{O}$. The following result is a strengthening of [6, Theorem 1], and uses many of the same methods.

https://doi.org/10.4153/S0008414X24000592 Published online by Cambridge University Press

Theorem 1.4 *Let p be an odd prime. Suppose $\mathcal{O}_1$, $\mathcal{O}_2$ are orders of B_p, each of index r in some (not necessarily the same) maximal order. Suppose $\mathcal{O}_1^T$ and $\mathcal{O}_2^T$ have the same successive minima $D_1 \le D_2 \le D_3$, and that $D_1 \ge 8r^2$. Then $\mathcal{O}_1 \simeq \mathcal{O}_2$.*

In particular, for all primes p, a maximal order in B_p is determined up to isomorphism by the successive minima of its Gross lattice: this is vacuously true if $p = 2$ or $D_1 < 8$ because this information determines a unique maximal order in B_p (see Lemma 3.10), and it holds for $D_1 \ge 8$ by Theorem 1.4.

After setting up some preliminary results on the geometry of quaternion orders in Section 3, we prove Theorem 1.4 in Section 4.1. The remainder of Section 4 is used to show that the theta function of $\mathcal{O}$ determines the successive minima of $\mathcal{O}^T$, allowing us to conclude Theorem 1.3.

In future work, we will explore similar questions for quaternion algebras over totally real fields.

1.1 Lattice definitions and conventions

Let $R = \mathbb{Z}$ or $R = \mathbb{Z}_\ell$ for some prime ℓ, and K the fraction field of R. A *lattice* Λ is a free finite-rank R-module (so that $\Lambda \simeq R^n$ for some positive integer n) equipped with a nondegenerate quadratic form $Q\colon \Lambda \to K$. A quadratic form Q is *integral* if it takes values in R. For $\mathbf{x} \in \Lambda$, we will refer to the value $Q(\mathbf{x})$ as the *norm* of $\mathbf{x}$. Any quadratic form defines a bilinear form $x \cdot y \coloneqq \frac{1}{2}(Q(x+y) - Q(x) - Q(y))$; if Q is integral than the bilinear form is valued in $\frac{1}{2}R$. Given a basis $\mathbf{v}_1, \dots, \mathbf{v}_n$ for Λ, the *Gram matrix for* Λ (we will also say "the Gram matrix of Q") is the symmetric matrix $\mathbf{A}_\Lambda \in \frac{1}{2}M_n(R)$ defined by

$$\mathbf{A}_\Lambda \coloneqq (v_i \cdot v_j)_{1 \le i,j \le n}.$$

If we write $\mathbf{x} \in \Lambda$ as a vector in terms of the basis $\mathbf{v}_1, \dots, \mathbf{v}_n$, then the Gram matrix satisfies the relation

$$Q(\mathbf{x}) = \mathbf{x}^T \mathbf{A}_\Lambda \mathbf{x}.$$

If there is no room for confusion, the subscript of $\mathbf{A}_\Lambda$ may be dropped. The *determinant* of Λ, $\det \Lambda$, is defined to be the determinant of a Gram matrix for Λ. When $R = \mathbb{Z}$ and Q is positive definite, we have $\det \Lambda > 0$ and the value does not depend on the choice of basis.

Given $a_1, \dots, a_k \in \Lambda$, we use the notation $\langle a_1, \dots, a_k \rangle$ to denote the sublattice of Λ generated by $a_1, \dots, a_k$ as an R-module. We say that a subset $C \subseteq \Lambda$ is a *generating set* for Λ if C generates Λ as an R-module.

2 Generating sets for maximal orders

2.1 A local–global principle for being generated by elements of prescribed norms

Let $Q\colon \mathbb{Z}^n \to \mathbb{Z}$ be a quadratic form with Gram matrix $\mathbf{A} \in \frac{1}{2}M_n(\mathbb{Z})$. For a prime ℓ, set

$$\tau_\ell = \begin{cases} 1, & \ell > 2, \\ 3, & \ell = 2. \end{cases}$$

https://doi.org/10.4153/S0008414X24000592 Published online by Cambridge University Press

Aside from the last line, the following definition appears in Browning and Dietmann [3].

Definition 2.1 For $s \in \mathbb{Z}_{>0}$ and $\mathbf{A} \in M_n(\mathbb{Z})$, the pair (s, Q) satisfies the *strong local solubility condition* ("strong LSC") if for every prime ℓ, there exists $\mathbf{x} \in (\mathbb{Z}/\ell^{\tau_\ell}\mathbb{Z})^n$ with $Q(\mathbf{x}) \equiv s \pmod{\ell^{\tau_\ell}}$ and $\ell \nmid \mathbf{Ax}$.

If $\mathbf{A} \in \frac{1}{2}M_n(\mathbb{Z})\backslash M_n(\mathbb{Z})$, then we say (s, Q) satisfies strong LSC if $(2s, 2Q)$ does.

Note that the strong LSC condition does not depend on the basis for $\mathbb{Z}^n$ used to define the Gram matrix $\mathbf{A}$.

If for every prime ℓ, there exists $\mathbf{x} \in \mathbb{Z}_\ell^n$ with $Q(\mathbf{x}) = s$, we say (s, Q) satisfies the *weak local solubility condition* ("weak LSC"). Strong LSC implies weak LSC by Hensel-lifting, but the converse does not hold (Example 2.7).

The following theorem is a local–global principle for lattices with the property of being generated by elements with norm in S.

Theorem 2.2 *Let $n \geq 4$, Q a nondegenerate integral quadratic form on $\mathbb{Z}^n$, and $S \subseteq \mathbb{Z}_{>0}$. Suppose that for all $M \geq 0$ and all primes ℓ, there exists a generating set C_ℓ for $\mathbb{Z}_\ell^n$ such that for all $\mathbf{x} \in C_\ell$, the norm $s := Q(\mathbf{x})$ satisfies:*

(a) $s \in S$,
(b) $s \geq M$,
(c) (s, Q) *satisfies strong LSC.*

Then $\mathbb{Z}^n$ has a generating set consisting of elements with norm in S.

We prove this in Section 2.2. Before that we draw a corollary, and then discuss the necessity of the conditions in the theorem.

A quadratic form $Q\colon \mathbb{Z}^n \to \mathbb{Z}$ is *primitive* if $\gcd(\{Q(\mathbf{x}) : \mathbf{x} \in \mathbb{Z}^n\}) = 1$.

Corollary 2.3 *Let $n \geq 4$, Q a nondegenerate primitive integral quadratic form on $\mathbb{Z}^n$, and $S \subseteq \mathbb{Z}_{>0}$ an infinite set. Suppose that for all $s \in S$ and that for all primes ℓ, there exists a basis for $\mathbb{Z}_\ell^n$ consisting of elements of norm s. Then $\mathbb{Z}^n$ has a generating set consisting of elements with norm in S.*

Proof Since s can be arbitrarily large, we just need to check that (s, Q) satisfies strong LSC. We have a basis consisting of elements $\mathbf{x} \in \mathbb{Z}_\ell^n$ with $Q(\mathbf{x}) = s$, so it suffices to show that one such basis vector has $\ell \nmid \mathbf{Ax}$ (or $\ell \nmid (2\mathbf{A})\mathbf{x}$ when $\mathbf{A} \notin M_n(\mathbb{Z})$).

Let ℓ be an odd prime, and for the sake of contradiction, suppose $\ell \mid \mathbf{Ax}$ for all $\mathbf{x}$ in a basis for $\mathbb{Z}_\ell^n$. Then $\ell \mid \mathbf{Ax}$ for all $\mathbf{x} \in \mathbb{Z}_\ell^n$, so

$$\ell \mid \mathbf{x}^t\mathbf{Ax} = Q(\mathbf{x}),$$

contradicting the assumption that Q is primitive. Thus (s, Q) must satisfy strong LSC at ℓ.

Now suppose $\ell = 2$. If $\mathbf{A} \in M_n(\mathbb{Z})$, the same argument as above applies. Now suppose $\mathbf{A} \in \frac{1}{2}M_n(\mathbb{Z})\backslash M_n(\mathbb{Z})$, and for the sake of contradiction suppose $2 \mid (2\mathbf{A})\mathbf{x}$ for all $\mathbf{x}$ in a basis for $\mathbb{Z}_2^n$. Letting $\mathbf{B} \in \mathrm{GL}_n(\mathbb{Z}_2)$ denote the matrix with columns corresponding to this basis, we have $(2\mathbf{A})\mathbf{B} \in 2M_n(\mathbb{Z}_2)$. This implies $\mathbf{AB} \in M_n(\mathbb{Z}_2)$, so multiplying on the right by $\mathbf{B}^{-1} \in \mathrm{GL}_n(\mathbb{Z}_2)$, we have $\mathbf{A} \in M_n(\mathbb{Z}_2)$. This contradicts our initial assumption on $\mathbf{A}$, so $(2s, 2Q)$ – and therefore also (s, Q) – satisfies strong LSC at 2. ∎

https://doi.org/10.4153/S0008414X24000592 Published online by Cambridge University Press

We now discuss the technical conditions in the statement of Theorem 2.2, and demonstrate through example that they cannot be removed or substantially weakened.

Remark 2.4 The conditions $n \geq 4$, (b), and (c) of Theorem 2.2 will be familiar to experts in the study of representability of integers by quadratic forms. When $Q\colon \mathbb{Z}^n \to \mathbb{Z}$ is a quadratic form with $n \geq 4$, Browning and Dietmann find an explicit lower bound M such that whenever $k \geq M$ and (k, Q) satisfies strong LSC, k is representable by Q [3, Theorem 5]. In [3, Section 1.2], they discuss examples due to Watson [22, Section 7.7] demonstrating that a local–global principle can fail if $k < M$ or if (k, Q) does not satisfy strong LSC.

In each of the counterexamples below, on the other hand, every value in S is globally represented by Q. Even in this setting, we show that if we drop any of the conditions $n \geq 4$, (b), or (c), the existence of generating sets for $\mathbb{Z}_\ell^n$ with norms in S for all primes ℓ is not sufficient to conclude the existence of a generating set for $\mathbb{Z}^n$ with norms in S.

Example 2.5 If we remove the condition $n \geq 4$ from Theorem 2.2, a counterexample is given by the quadratic form

$$Q(x, y) = x^2 + 21y^2$$

on $\mathbb{Z}^2$ and $S = \{19^{2k} : k \geq 0\}$. The elements in $\mathbb{Z}^2$ with norm in S generate an index 4 sublattice of $\mathbb{Z}^2$: using the observation that $5^2 + 21 \cdot 4^2 = 19^2$, we can factor each side of the equation $x^2 + 21y^2 = 19^{2k}$ into prime ideals of $\mathbb{Z}[\sqrt{-21}]$ to show that we must have $4 \mid y$. But for any $k \geq 0$ and any prime ℓ, there is a basis for $\mathbb{Z}_\ell^2$ consisting of elements of norm 19^{2k}: we have:

$$\begin{array}{llllll} Q(19^k, 0) & \equiv & Q(19^k, 1) & \equiv & 19^{2k} \pmod{\ell} & \text{for } \ell = 3, 7, \\ Q(1, 0) & \equiv & Q(2, 1) & \equiv & 19^{2k} \pmod{8}, & \text{and} \\ Q(6, 1) & \equiv & Q(6, -1) & \equiv & 19^{2k} \pmod{19}, & \end{array}$$

and for remaining ℓ, we can use the fact that $x^2 + 21y^2 - 19^k t^2 = 0$ defines a smooth projective conic over $\mathbb{F}_\ell$ to find two independent points $(x, y) \in \mathbb{F}_\ell^2$ with $Q(x, y) \equiv 19^k \pmod{\ell}$. In each case these Hensel-lift to a basis for $\mathbb{Z}_\ell^2$ of elements with norm 19^k.

We do not currently know whether or not it is sufficient to assume $n \geq 3$ in Theorem 2.2.

Example 2.6 Condition (b) of Theorem 2.2 (that the local generators have norm at least M) can be thought of as a constraint coming from the infinite place of $\mathbb{Q}$. If we remove it, a counterexample is given by the quadratic form

$$Q(x, y, z, w) = x^2 + 9y^2 + 9z^2 + 9w^2$$

on $\mathbb{Z}^4$ with $S = \{37\}$. The only $x \in \mathbb{Z}$ satisfying $x^2 \equiv 37 \pmod{9}$ and $x^2 \leq 37$ is $x = \pm 1$, so the set of vectors of norm 37 generate an index 16 sublattice of $\mathbb{Z}^4$ with basis

$$(1, 2, 0, 0), (-1, 2, 0, 0), (1, 0, 2, 0), (1, 0, 0, 2).$$

https://doi.org/10.4153/S0008414X24000592 Published online by Cambridge University Press

However, for all primes ℓ, there is a basis for $\mathbb{Z}_\ell^4$ consisting of elements of norm 37: for odd ℓ we can use the above basis because 16 is a unit in $\mathbb{Z}_\ell^\times$, and for $\ell = 2$ we can let u be a square root of $\frac{11}{3}$ in $\mathbb{Z}_2^\times$ and use

$$(1,2,0,0),(2,u,0,0),(2,0,u,0),(2,0,0,u).$$

Example 2.7 If we weaken condition (c) to merely requiring that (s,Q) satisfies weak LSC, a counterexample is given by the quadratic form

$$Q(x,y,z,w) = 3x^2 + 5y^2 + 11\cdot 15^2 z^2 + 11\cdot 15^3 w^2$$

on $\mathbb{Z}^4$ and $S = \{3^k : k \geq 1 \text{ odd}\} \cup \{5^k : k \geq 1 \text{ odd}\}$. The elements $(3^{(k-1)/2},0,0,0)$ and $(0,5^{(k-1)/2},0,0)$ show that every element of S is globally represented (and hence everywhere locally represented). Further, for any odd $k \geq 1$ and $\ell \neq 5$, $\mathbb{Z}_\ell^4$ has a basis of elements of norm 5^k, using the observations that

$$\begin{aligned} Q(1,1,0,1) \equiv Q(0,1,1,1) \equiv Q(0,1,0,0) \equiv Q(0,0,0,1) &\equiv 5^k \pmod 8,\\ Q(0,1,0,0) \equiv Q(1,1,0,0) \equiv Q(0,1,1,0) \equiv Q(0,1,0,1) &\equiv 5^k \pmod 3,\\ Q(3r,0,0,0) \equiv Q(0,r,0,0) \equiv Q(0,r,1,0) \equiv Q(0,r,0,1) &\equiv 5^k \pmod{11} \end{aligned}$$

with $r = 5^{(k-1)/2}$. In a similar way, we can show that for any odd $k \geq 1$ and $\ell \neq 3$, $\mathbb{Z}_\ell^4$ has a basis of elements of norm 3^k.

However, for $k \geq 4$, the only elements of norm 5^k in $\mathbb{Z}_5^4$ are in $5\mathbb{Z}_5^4$:

$$\begin{aligned} 0 \equiv Q(x,y,z,w) &\equiv 3x^2 \pmod 5 && \Rightarrow 5 \mid x;\\ 0 \equiv Q(5x_1,y,z,w) &\equiv 5y^2 \pmod{25} && \Rightarrow 5 \mid y;\\ 0 \equiv Q(5x_1,5y_1,z,w) &\equiv 25(3x_1^2 + 4z^2) \pmod{125} && \Rightarrow 5 \mid x_1, z;\\ 0 \equiv Q(25x_2,5y_1,5z_1,w) &\equiv 125(y_1^2 + 2w^2) \pmod{625} && \Rightarrow 5 \mid y_1, w. \end{aligned}$$

Thus $(5^k,Q)$ does not satisfy strong LSC at 5. In a similar way, for $k \geq 4$, the only elements of norm 3^k in $\mathbb{Z}_3^4$ are in $3\mathbb{Z}_3^4$, so $(3^k,Q)$ does not satisfy strong LSC at 3. In particular, every element of $\mathbb{Z}^4$ with norm in S satisfies $15 \mid z,w$ (using the argument above for $k \geq 4$ and checking explicitly for small k), so such elements do not generate $\mathbb{Z}^4$.

2.2 Proof of Theorem 2.2

The proof is a direct application of a strong approximation theorem of Sardari. We quote a special case of this theorem here.

Given an integer s, a prime ℓ, an integer $t_\ell \geq 0$, and $\mathbf{a}_\ell \in \mathbb{Z}_\ell^n$, define the local density

$$\sigma_\ell(\mathbf{a}_\ell, t_\ell, s) \coloneqq \lim_{k\to\infty} \frac{n(\ell^k)}{\ell^{(n-1)k}},$$

where

$$n(\ell^k) \coloneqq \#\{\mathbf{x} \in (\mathbb{Z}/\ell^{k+t_\ell}\mathbb{Z})^n : Q(\mathbf{x}) \equiv s \pmod{\ell^{k+t_\ell}},\quad \mathbf{x} \equiv \mathbf{a}_\ell \pmod{\ell^{t_\ell}}\}.$$

Given a choice of t_ℓ and $\mathbf{a}_\ell$ for all ℓ with $t_\ell = 0$ for all but finitely many ℓ, set $\mathfrak{S}(s) \coloneqq \prod_\ell \sigma_\ell(\mathbf{a}_\ell, t_\ell, s)$ and $V = \prod_\ell \ell^{-t_\ell}$.

https://doi.org/10.4153/S0008414X24000592 Published online by Cambridge University Press

Theorem 2.8 [17, Theorem 1.6][1] *Let $n \geq 4$, $Q\colon \mathbb{Z}^n \to \mathbb{Z}$ a nondegenerate quadratic form, and $\varepsilon > 0$. For all primes ℓ and all integers s, the number of $\mathbf{x} \in \mathbb{Z}^n$ satisfying $Q(\mathbf{x}) = s$ and $\mathbf{x} \equiv \mathbf{a}_\ell \pmod{\ell^{t_\ell}}$ for all primes ℓ is*

$$\gg \mathfrak{S}(s) V^{n-1} s^{\frac{n-2}{2}} \left(1 + O\left(V^{-3(n-3)/2} s^{\varepsilon - \frac{n-3}{4}}\right)\right),$$

where the implied constants in $\gg$ and O depends only on ε and Q.

Lemma 2.9 *Let ℓ be a prime, s an integer, and $\mathbf{a}_\ell \in \mathbb{Z}_\ell^n$ satisfying $Q(\mathbf{a}_\ell) = s$. Let $t_\ell = 1$ and $t_{\ell'} = 0$ for $\ell' \neq \ell$. Suppose (s, Q) satisfies strong LSC. Then for all $\delta > 0$, we have $\mathfrak{S}(s) \gg |s|^{-\delta}$, where the implicit constant depends only on Q, ℓ, and δ (not on s).*

Proof Consider the modified singular series

$$\mathfrak{S}'(s, Q) := \prod_{\ell' \text{ prime}} \lim_{k \to \infty} \frac{\#\{\mathbf{x} \in (\mathbb{Z}/\ell'^k\mathbb{Z})^n : Q(\mathbf{x}) \equiv s \pmod{\ell'^k}\}}{\ell^{(n-1)k}}.$$

Note that for $\ell' \neq \ell$, the term at ℓ' is equal to the term at ℓ' of $\mathfrak{S}(s)$. The terms at ℓ are each bounded above and below by nonzero constants in s that depend on ℓ (the lower bound follows by an application of Hensel's lemma), so $\mathfrak{S}'(s)$ and $\mathfrak{S}(s)$ have the same rate of decay in s.

Browning and Dietmann prove [3, Proposition 2] that for any $\delta > 0$, if $\mathbf{A} \in M_n(\mathbb{Z})$ and (s, Q) satisfies strong LSC, then

$$\mathfrak{S}'(s, Q) \gg |s\Delta_Q|^{-\delta},$$

with Δ_Q the discriminant of Q, and the implicit constant depending only on δ.

If $\mathbf{A} \notin M_n(\mathbb{Z})$, then (s, Q) satisfying strong LSC implies

$$\mathfrak{S}'(2s, 2Q) \gg |2s\Delta_{2Q}|^{-\delta}.$$

Now $\mathfrak{S}'(2s, 2Q)$ and $\mathfrak{S}'(s, Q)$ are the same at every prime except 2, where they differ by at most a constant factor. So we reach the same conclusion for $\mathfrak{S}'(s, Q)$. ∎

Proof of Theorem 2.2 Fix any prime ℓ, and let M be large (we will specify how large later). Let C_ℓ be a generating set for $\mathbb{Z}_\ell^n$ satisfying conditions (a) through (c), let $\mathbf{a}_\ell \in C_\ell$, and let $s := Q(\mathbf{a}_\ell)$. Set $t_\ell = 1$ and $t_{\ell'} = 0$ for all primes $\ell' \neq \ell$. By Lemma 2.9, the corresponding singular series is asymptotically larger than $s^{-\frac{n-2}{2}}$. So by Theorem 2.8, if M is sufficiently large, there exists $\mathbf{y} \in \mathbb{Z}^n$ satisfying $Q(\mathbf{y}) = s$ and $\mathbf{y} \equiv \mathbf{a}_\ell \pmod{\ell}$. Here, "sufficiently large" may depend on ℓ, Q, and a choice of $0 < \varepsilon < \frac{n-3}{4}$, but these choices can all be made at the outset.

Thus, there is a set $\widehat{C_\ell} \subseteq \mathbb{Z}^n$ such that for each $\mathbf{a}_\ell \in C_\ell$, there is a corresponding $\mathbf{y} \in \widehat{C_\ell}$ with $Q(\mathbf{y}) = Q(\mathbf{a}_\ell) \in S$ and $\mathbf{y} \equiv \mathbf{a}_\ell \pmod{\ell}$. Since the inclusion $\mathbb{Z}^n \to \mathbb{Z}_\ell^n$ induces an isomorphism $\mathbb{Z}^n/\ell\mathbb{Z}^n \to \mathbb{Z}_\ell^n/\ell\mathbb{Z}_\ell^n$, and C_ℓ generates $\mathbb{Z}_\ell^n$, $\widehat{C_\ell}$ generates $\mathbb{Z}^n/\ell\mathbb{Z}^n$.

Since elements in $\mathbb{Z}^n$ with norm in S generate $\mathbb{Z}^n/\ell\mathbb{Z}^n$ for all primes ℓ, we can conclude that such elements generate $\mathbb{Z}^n$. ∎

[1] The full theorem has a stronger bound when $n \geq 5$, and includes terms accounting for Archimedean constraints.

https://doi.org/10.4153/S0008414X24000592 Published online by Cambridge University Press

Remark 2.10 If every element of S is coprime to $2p$, then a much shorter proof of Theorem 2.2 can be given using Theorem 1.2 of [17]. The authors were informed by Naser Sardari that a correction needs to be made to this result: as written it only requires N to be odd, but in fact N must also be relatively prime to the discriminant of Q.

2.3 Local generating sets for maximal orders

Let $\mathcal{O}$ be a maximal order in B_p, and let s be any positive integer relatively prime to p. We will show that for all primes ℓ, $\mathcal{O} \otimes \mathbb{Z}_\ell$ has a basis consisting of elements of norm s, so that Theorem 1.1 follows from Corollary 2.3.

2.3.1 $\ell \neq p$

In this case $\mathcal{O} \otimes \mathbb{Z}_\ell \simeq M_2(\mathbb{Z}_\ell)$, with the norm on $\mathcal{O}$ inducing the determinant on $M_2(\mathbb{Z}_\ell)$. The elements

$$\begin{pmatrix} s & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} s & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} s & 0 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & -1 \\ s & 0 \end{pmatrix}$$

each have norm s, and these evidently span $M_2(\mathbb{Z}_\ell)$.

2.3.2 $\ell = p \neq 2$

Let $K/\mathbb{Q}_p$ be the unique unramified quadratic extension, with Galois group generated by σ. Then

$$B_p \otimes \mathbb{Z}_p \simeq \left\{ \begin{pmatrix} u & pv \\ \sigma(v) & \sigma(u) \end{pmatrix} : u, v \in K \right\} \subseteq M_2(K)$$

[21, Corollary 13.3.14], and $\mathcal{O} \otimes \mathbb{Z}_p$ is the corresponding valuation ring [21, Proposition 13.3.4], obtained by restricting u and v to be in the valuation ring of K. The norm on $\mathcal{O} \otimes \mathbb{Z}_p$ is $u\sigma(u) - pv\sigma(v)$.

Remark 2.11 If u is not a multiple of p, then $u\sigma(u) - pv\sigma(v)$ is not a multiple of p. This shows that any basis of a maximal order $\mathcal{O} \subseteq B_p$ must contain at least two elements with norm relatively prime to p.

If $p \neq 2$, we have $K \simeq \mathbb{Q}_p(\sqrt{a})$ for some $a \in \mathbb{Q}_p$ such that a is not a square modulo p. Therefore $\mathcal{O} \otimes \mathbb{Z}_p \simeq \mathbb{Z}_p^4$ with quadratic form

$$(x, y, z, w) \mapsto Q(x, y, z, w) \coloneqq x^2 - ay^2 - pz^2 + apw^2.$$

Since $p \nmid s$, the equation $x^2 - ay^2 - st^2 = 0$ defines a smooth projective conic over $\mathbb{F}_p$. This curve has $p + 1 \geq 3$ $\mathbb{F}_p$-points, none of which has $t = 0$, and no three of which lie on a common line. Thus, there exist two linearly independent points $(c_1, d_1), (c_2, d_2) \in \mathbb{F}_p^2$ with $c_1^2 - ad_1^2 = c_2^2 - ad_2^2 = s$ in $\mathbb{F}_p$, so we have

$$Q(c_1, d_1, 0, 0) \equiv Q(c_1, d_1, 1, 0) \equiv Q(c_1, d_1, 0, 1) \equiv Q(c_2, d_2, 0, 0) \equiv s \pmod{p}.$$

By Hensel lifting, we obtain a basis for $\mathbb{Z}_p^4$ consisting of elements of norm s.

https://doi.org/10.4153/S0008414X24000592 Published online by Cambridge University Press

2.3.3 $\ell = p = 2$

As above, the norm on $\mathcal{O} \otimes \mathbb{Z}_p$ is $u\sigma(u) - pv\sigma(v)$, but this time, we have $K \simeq \mathbb{Q}_2(\zeta_3)$, where $\zeta_3 \in K$ satisfies $\zeta_3^2 + \zeta_3 + 1 = 0$. Therefore $\mathcal{O} \otimes \mathbb{Z}_2 \simeq \mathbb{Z}_2^4$ with quadratic form

$$(x, y, z, w) \mapsto Q(x, y, z, w) \coloneqq x^2 + xy + y^2 - 2z^2 - 2zw - 2w^2.$$

We have

$$\begin{aligned}
Q(1,0,0,0) \equiv Q(0,1,0,0) \equiv Q(1,1,1,0) \equiv Q(1,1,0,1) &\equiv 1 \pmod 2,\\
Q(1,1,0,0) \equiv Q(1,0,1,1) \equiv Q(0,1,1,2) \equiv Q(0,1,2,1) &\equiv 3 \pmod 8,\\
Q(1,1,1,1) \equiv Q(1,1,1,2) \equiv Q(1,1,2,1) \equiv Q(2,1,1,0) &\equiv 5 \pmod 8,\\
Q(1,0,1,0) \equiv Q(0,1,1,0) \equiv Q(1,0,0,1) \equiv Q(0,1,1,3) &\equiv 7 \pmod 8,
\end{aligned}$$

and for each row, the four vectors define a matrix with odd determinant. So regardless of the value of s, we can Hensel lift to obtain a basis for $\mathbb{Z}_2^4$ consisting of elements of norm s.

2.3.4 Eichler orders

An *Eichler order* is an intersection of two maximal orders. If $\mathcal{O}$ is an Eichler order in B_p, then $\mathcal{O} \otimes \mathbb{Z}_p$ is maximal, and for $\ell \neq p$, $\mathcal{O} \otimes \mathbb{Z}_\ell$ is conjugate to $\left(\begin{smallmatrix} \mathbb{Z}_\ell & \mathbb{Z}_\ell \\ \ell^{r_\ell}\mathbb{Z}_\ell & \mathbb{Z}_\ell \end{smallmatrix}\right)$ for some $r_\ell \geq 0$ [21, Section 23.4.19]. The exponent r_ℓ is nonzero only for finitely many primes ℓ, and the product $\prod_\ell \ell^{r_\ell}$ is the *index* of $\mathcal{O}$ (equal to the index of $\mathcal{O}$ in any maximal order containing it).

Let ℓ be a prime dividing the index of $\mathcal{O}$ (we necessarily have $\ell \neq p$). If $\ell \mid s$, then the elements

$$\begin{pmatrix} s & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} s & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} s & 0 \\ \ell^{r_\ell} & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & s \end{pmatrix}$$

each have norm s and form a basis for $\mathcal{O} \otimes \mathbb{Z}_\ell$. If $\ell \nmid 6s$, then the elements

$$\begin{pmatrix} s & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} s & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} s & 0 \\ \ell^{r_\ell} & 1 \end{pmatrix}, \quad \begin{pmatrix} 2s & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$$

each have norm s and contain $\left(\begin{smallmatrix} 3s & 0 \\ 0 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 3 \end{smallmatrix}\right)$ in their span, so they form a basis for $\mathcal{O} \otimes \mathbb{Z}_\ell$. So if the index of $\mathcal{O}$ is not divisible by 2 or 3, then for all primes ℓ, there is a basis for $\mathcal{O} \otimes \mathbb{Z}_\ell$ consisting of elements of norm s; by Corollary 2.3, we can conclude that $\mathcal{O}$ has a generating set with norms in S.

On the other hand, if the index of $\mathcal{O}$ is even, then $\mathcal{O}$ is not generated by elements of odd norm. This is because for $r \geq 1$, $\det\left(\begin{smallmatrix} x & y \\ 2^r z & w \end{smallmatrix}\right) \equiv 1 \pmod 2$ implies $x \equiv w \equiv 1 \pmod 2$, and the span of elements of this form lie in a proper sublattice of $\mathcal{O} \otimes \mathbb{Z}_2$. For a similar reason, if the index of $\mathcal{O}$ is a multiple of 3 and $i = 1$ or 2, then $\mathcal{O}$ is not generated by elements of norm congruent to $i \pmod 3$. So additional constraints on S are necessary if the index is not relatively prime to 6.

https://doi.org/10.4153/S0008414X24000592 Published online by Cambridge University Press

3 Theta function determines maximal order: background and setup

We now turn to the second topic of this article: determining maximal orders of B_p by their theta functions. In this section, we discuss some examples of isospectral lattices and then set up some results about the lattice structure of quaternion orders; the main results of Theorems 1.3 and 1.4 are proven in Section 4.

3.1 Isospectral lattices

Two integral lattices Λ, Λ' are *isospectral* if their theta functions are equal. Schiemann proved that there do not exist any pairs of non-isometric isospectral lattices of rank at most 3 [18], but there are many pairs of non-isometric but isospectral lattices of rank 4, including a four-parameter family due to Conway and Sloane [7].

Now, suppose we restrict to integral lattices in a quaternion algebra B_p whose left and right orders are maximal (every such lattice is locally similar to a maximal order of B_p, and every quadratic form locally similar to a maximal order can be obtained in this way up to oriented similarity [21, Section 19.6.7]). Equivalently, one can ask if a pair E, E' of supersingular elliptic curves over $\overline{\mathbb{F}_p}$ can be identified (up to Frobenius) by counting the number of isogenies of given degree from E to E'. Even in this constrained setting, it is common to find multiple lattices with the same theta function; the first instance of this occurring is for $p = 67$. At $p = 151$, we even find two non-isometric right ideals of the *same* maximal order that have equal theta functions. These observations were explored in depth by Shiota [19].

Example 3.1 We include a brief description of the isospectral right ideals in the case $p = 151$. Take $B_p = \mathbb{Q}\langle 1, i, j, k\rangle$ with $i^2 = -1$, $j^2 = -151$, and $k \coloneqq ij = -ji$. Consider the maximal order

$$O \coloneqq \left\langle \frac{1}{2} + \frac{1}{2}j + 4k, \frac{1}{32}i + \frac{3}{4}j + \frac{69}{32}k, j + 8k, 16k \right\rangle.$$

This order has right ideals

$$I_1 \coloneqq \langle -5 + i - j - 3k, 10 - 42i + 2j - 2k, -7 + 11i + 5j - k, 74 + 22i + 2j - 2k\rangle,$$
$$I_2 \coloneqq \langle -16 + 26i + 2k, 12 + 19i + 4j - k, 48 + 26i + 2k, -4 - 31i + 4j + 5k\rangle,$$

each of norm 512, and we can check that I_1 and I_2 have non-isomorphic left orders. For each of I_1 and I_2, we take the basis x_1, x_2, x_3, x_4 given above and compute the corresponding (normalized) Gram matrix $\frac{1}{1024}(\mathrm{Tr}(x_i\overline{x_j}))_{1\le i,j\le 4}$, yielding

$$\mathbf{A}_1 = \frac{1}{2}\begin{pmatrix} 6 & 2 & -1 & 1 \\ 2 & 12 & 5 & 4 \\ -1 & 5 & 16 & 6 \\ 1 & 4 & 6 & 28 \end{pmatrix}, \qquad \mathbf{A}_2 = \frac{1}{2}\begin{pmatrix} 6 & 0 & 2 & 3 \\ 0 & 12 & 3 & 4 \\ 2 & 3 & 14 & 2 \\ 3 & 4 & 2 & 28 \end{pmatrix}.$$

Both matrices have determinant $\frac{151^2}{16}$, as expected (by [21, Proposition 16.4.3] and Eq. (3.1)). The theta functions of both lattices begin with

$$1 + 2q^3 + 2q^6 + 2q^7 + 2q^8 + 4q^9 + 2q^{10} + 2q^{11} + 4q^{12} + 4q^{14} + 4q^{15} + \dots$$

https://doi.org/10.4153/S0008414X24000592 Published online by Cambridge University Press

and are weight 2 cusp forms for $\Gamma_0(151)$ [21, Section 40.4.5]. One can find a basis of $M_2(\Gamma_0(151))$ consisting of 13 elements, and check that under projection to the first 13 Fourier coefficients they remain independent. (The Sturm bound predicts that the first 25 coefficients are sufficient, but we can get by with fewer in this case.) Thus, if two elements of $M_2(\Gamma_0(151))$ agree on these coefficients, they must be equal. Hence, these lattices are isospectral. However, the lattices are not isometric because the vectors of norm 3 are orthogonal to the vectors of norm 6 in the second lattice but not in the first.

Remark 3.2 Even if two non-isometric lattices have equal theta functions, the lattices may be distinguished using an enriched theta function that carries more information about the structure of the lattice than just the number of elements of each norm. For $k \geq 1$, let $\mathbb{H}_k$ be the Siegel upper half-space, consisting of symmetric matrices $Z \in M_k(\mathbb{C})$ with positive-definite imaginary part. For an integral lattice Λ, one may define the *degree k theta function* of Λ by

$$\theta_\Lambda^{(k)}(Z) \coloneqq \sum_{(v_1,\ldots,v_k)\in\Lambda^k} \exp(2\pi i \operatorname{Tr}(T(v_1,\ldots,v_k)Z)),$$

where $Z \in \mathbb{H}_k$ and $T(v_1,\ldots,v_k) \in \frac{1}{2}M_k(\mathbb{Z})$ has $v_i \cdot v_j$ in the i,j component. We recover the classical theta function by taking $k = 1$ and setting $q = e^{2\pi i z}$ for z in the complex upper half-plane.

Kitaoka showed that for any collection of rank n lattices that are pairwise non-isometric, the corresponding degree $n-1$ theta functions are linearly independent [13]. Suppose we restrict our attention to the set of rank 4 integral lattices in a definite quaternion algebra over $\mathbb{Q}$ whose left and right orders are maximal. Böcherer and Schulze-Pillot classified all linear relations between the degree 2 theta functions of integral lattices of this form, and showed that two such lattices are isometric if and only if their degree 2 theta functions are equal [2, Corollary 9.2]). In this light, our Theorem 1.3 shows that for maximal orders, at least in B_p, already their degree 1 theta function distinguishes between them.

3.2 Lattice geometry of quaternion orders

As before, let B_p denote the quaternion algebra over $\mathbb{Q}$ ramified at p and ∞. There exists an isometry $B_p \otimes \mathbb{R} \simeq \mathbb{R}^4$, with the norm on B_p corresponding to the square of the standard Euclidean distance on $\mathbb{R}^4$, and $\frac{1}{2}\operatorname{Tr}(x\bar{y})$ giving the standard inner product $x \cdot y$.

Let Λ be a lattice in B_p of rank $1 \leq k \leq 4$; we say Λ is an *integral lattice* if for all $x \in \Lambda$, we have $N(x), \operatorname{Tr}(x) \in \mathbb{Z}$. Given a basis $\{v_1,\ldots,v_k\}$ of an integral lattice Λ, we can define a *Gram matrix*

$$\mathbf{A}_\Lambda \coloneqq (v_i \cdot v_j)_{1\leq i,j\leq k} = \left(\tfrac{1}{2}\operatorname{Tr}(v_i\overline{v_j})\right)_{1\leq i,j\leq k},$$

and *determinant* $\det\Lambda \coloneqq \det \mathbf{A}_\Lambda$ as in Section 1.1. The quaternion norm N on B_p defines an integral quadratic form on Λ, and $\mathbf{A}_\Lambda \in \frac{1}{2}M_k(\mathbb{Z})$.

Now suppose Λ is an order in B_p, so it is contained in a maximal order $\mathcal{O}$ with finite index. We define the *discriminant* of Λ to be $\operatorname{disc}\Lambda \coloneqq \det(2\mathbf{A}_\Lambda)$. Note that the

https://doi.org/10.4153/S0008414X24000592 Published online by Cambridge University Press

discriminant of Λ is a positive integer, while the determinant may not be an integer. In particular, if $\mathcal{O}$ is a maximal order containing Λ then

$$\operatorname{disc}\Lambda = 16\det\Lambda = [\mathcal{O}:\Lambda]^2 p^2 \tag{3.1}$$

[21, Lemma 15.2.15, Theorem 15.5.5]. If Λ has basis $v_1,\dots,v_4$, then we have

$$\operatorname{disc}\Lambda = \det(\operatorname{Tr}(v_i\bar{v_j}))_{1\le i,j\le 4} = \left|\det(\operatorname{Tr}(v_i v_j))_{1\le i,j\le 4}\right| \tag{3.2}$$

[21, Exercise 15.13], where we call $(\operatorname{Tr}(v_i v_j))_{1\le i,j\le 4}$ the *trace matrix* of the basis $\{v_1,\dots,v_4\}$.

Definition 3.3 Let Λ be a lattice of rank k with a positive definite quadratic form Q. For $1 \le i \le k$, the ith *successive minimum* of Λ is the minimum value D_i such that the rank of the $\mathbb{Z}$-module generated by $\{v \in \Lambda : Q(v) \le D_i\}$ is greater than or equal to i. An ordered list $v_1,\dots,v_k \in \Lambda$ *attains the successive minima of* Λ if it is linearly independent and $Q(v_i) = D_i$ for each $i = 1,\dots,k$.

Remark 3.4 This is a nonstandard definition, following the notation of [6]; if (Λ, Q) is embedded isometrically in a Euclidean space $\mathbb{R}^n$, then the successive minima under Definition 3.3 are the squares of the corresponding successive minima under the standard definition. There always exists a list of elements attaining the successive minima, for instance, by [5, Section VIII.1.2, Lemma 1].

Lemma 3.5 *Let Λ be a lattice of rank $k \le 3$. If a list of k vectors attains the successive minima of Λ, then these vectors form a basis for Λ. The same holds true for $k = 4$ if we additionally assume that Λ is an order in B_p for p odd.*

Note that a counterexample for $p = 2$ is given by the Hurwitz quaternions, $\mathcal{Z} := \langle 1, i, j, \frac{1}{2}(1+i+j+k)\rangle$ where $i^2 = j^2 = -1$ and $ij = k$. The elements $1, i, j, k$ attain the successive minima, but $\frac{1}{2}(1+i+j+k)$ is not contained in their span.

Proof Among all lattices of rank at most 4, the rank 4 cubic centered lattice $\mathbf{D}_4$ (which is isometric to $\mathcal{Z}$ after rescaling) is the only lattice up to similarity for which an arbitrary list of vectors attaining the successive minima is not always a basis [15, Corollary 6.2.3]. If Λ is an order in B_p for p odd then the first successive minimum is equal to 1, so if Λ were a cubic centered lattice then its Gram matrix would have determinant $\frac{1}{4}$. This contradicts the fact that the determinant of an order in B_p must be an integer multiple of $\frac{p^2}{16}$ by Eq. (3.1). ∎

3.3 The Gross lattice

We define an additive map $\tau\colon B_p \to B_p$ by

$$\tau(x) = 2x - \operatorname{Tr}(x).$$

If we restrict τ to an order $\mathcal{O} \subseteq B_p$, then the kernel of this map is $\mathbb{Z}$, and the image is the *Gross lattice* of $\mathcal{O}$,

$$\mathcal{O}^T := \tau(\mathcal{O}) = \{2x - \operatorname{Tr}(x) : x \in \mathcal{O}\}$$

(cf. [11, Section 12]). The Gross lattice is a strict subset of $\mathcal{O}^0$, the subset of $\mathcal{O}$ consisting of trace zero elements; more precisely, we have $\mathcal{O}^T = \mathcal{O}^0 \cap (\mathbb{Z} + 2\mathcal{O})$. Some relations

https://doi.org/10.4153/S0008414X24000592 Published online by Cambridge University Press

between sublattices of $\mathcal{O}$ are given below: inclusion arrows below are labeled by the index of one sublattice in the other, and $\oplus$ denotes orthogonal direct sum.

$$\begin{array}{ccccccc} \mathbb{Z}+2\mathcal{O}=\mathbb{Z}\oplus\mathcal{O}^T & \xhookrightarrow{4} & \mathbb{Z}\oplus\mathcal{O}^0 & \xhookrightarrow{2} & \mathcal{O} & & \text{(rank 4)} \\ & & \downarrow\tau & & \downarrow\tau & & \\ & & 2\mathcal{O}^0 & \xhookrightarrow{2} & \mathcal{O}^T & \xhookrightarrow{4} & \mathcal{O}^0 \quad \text{(rank 3)} \end{array} \tag{3.3}$$

The index of $\mathbb{Z}\oplus\mathcal{O}^0$ in $\mathcal{O}$ can be computed by noting that $\mathbb{Z}\oplus\mathcal{O}^0$ consists of all elements of $\mathcal{O}$ with even trace, and that $\mathcal{O}$ must contain an element of odd trace (since $\det\mathcal{O}=\frac{p^2}{16}$ implies the Gram matrix of $\mathcal{O}$ cannot be an integer matrix).

Remark 3.6 Given a lattice $\Lambda\subseteq B_p$, define the *dual lattice* $\Lambda^\sharp$ by

$$\Lambda^\sharp := \{y\in\mathbb{Q}\Lambda : \mathrm{Tr}(x\bar{y})\in\mathbb{Z} \text{ for all } x\in\Lambda\}.$$

While this will not be used in the rest of the article, we note that $\mathcal{O}^T$ can be related to $(\mathcal{O}^\sharp)^0$, the trace zero part of the dual lattice of $\mathcal{O}$. (This lattice arises in the correspondence between quaternion orders and ternary quadratic forms via the Clifford algebra construction; see [21, Chapter 22].) Specifically, we have the equality

$$(\tfrac{1}{2}\mathcal{O}^T)^\sharp=(\mathcal{O}^\sharp)^0,$$

because when $\mathrm{Tr}(y)=0$ and $x\in\mathcal{O}$ we have $\mathrm{Tr}(\tau(x)\bar{y})=2\,\mathrm{Tr}(x\bar{y})$. Since $\frac{1}{2}\mathcal{O}^T$ is the orthogonal projection of $\mathcal{O}$ onto B_p^0, we can summarize this by saying that the dual of the projection equals the restriction of the dual.

The primary motivation for studying the Gross lattice is that elements of $\mathcal{O}^T$ correspond to embeddings of imaginary quadratic orders in $\mathcal{O}$. Observe that for any $x\in B_p$, we have the equality

$$N(\tau(x))=4N(x)-\mathrm{Tr}(x)^2. \tag{3.4}$$

So for any $\beta\in\mathcal{O}^T\backslash\{0\}$, $-N(\beta)$ is equal to the discriminant of the quadratic order generated by a preimage of β under τ.

Given an imaginary quadratic order R of discriminant $-D$ for $D>0$, an *orientation* of R is a choice of $x\in R$ satisfying $x^2+D=0$ (which we will usually denote $\sqrt{-D}$). Given two oriented orders (R,x) and (R,x'), an *oriented isomorphism* is an isomorphism $R\to R'$ sending $x\mapsto x'$. Note that for every imaginary quadratic discriminant $-D$, there are exactly two oriented quadratic orders R up to oriented isomorphism, sent to each other by the nontrivial Galois action on R.

Given an imaginary quadratic order R and an embedding $\phi: R\hookrightarrow\mathcal{O}$, we say the embedding is *optimal* if $\mathbb{Q}\phi(R)\cap\mathcal{O}=\phi(R)$. Given a nonzero element v of a lattice L, we say v is *primitive* if there does not exist $w\in L$ and $n\geq 2$ with $v=nw$. The following proposition is implicit in [11, Proposition 12.9]; we include the proof for completeness.

Proposition 3.7 *There is a one-to-one correspondence between nonzero elements $\beta\in\mathcal{O}^T$ and embeddings $R\hookrightarrow\mathcal{O}$ of oriented imaginary quadratic orders R up to oriented isomorphism. Under this correspondence, we have* $\mathrm{disc}\,R=-N(\beta)$, *and the embedding $R\hookrightarrow\mathcal{O}$ is optimal if and only if the corresponding β is primitive.*

https://doi.org/10.4153/S0008414X24000592 Published online by Cambridge University Press

Proof The imaginary quadratic order $R = \mathbb{Z}[\frac{1}{2}(D + \sqrt{-D})]$ has discriminant $-D$ and orientation determined by the element $\sqrt{-D}$. To an embedding $\phi: R \to \mathcal{O}$, we associate the element

$$\beta := \phi(\sqrt{-D}) = 2\phi\left(\frac{D + \sqrt{-D}}{2}\right) - \mathrm{Tr}\left(\phi\left(\frac{D + \sqrt{-D}}{2}\right)\right) \in \mathcal{O}^T.$$

Conversely, given an element $\beta = 2x - \mathrm{Tr}(x)$ of $\mathcal{O}^T$, set $D = N(\beta)$ and associate to β the embedding of $\mathbb{Z}[\frac{1}{2}(D + \sqrt{-D})]$ into $\mathcal{O}$ determined by

$$\frac{D + \sqrt{-D}}{2} \mapsto x + \frac{D - \mathrm{Tr}(x)}{2}.$$

We have $x + \frac{D - \mathrm{Tr}(x)}{2} \in \mathcal{O}$ because $D \equiv \mathrm{Tr}(x) \pmod 2$ by Eq. (3.4). Further, both sides have trace D, and applying Eq. (3.4) to the fact that $\tau\left(x + \frac{D - \mathrm{Tr}(x)}{2}\right) = \beta$ we find that both sides have norm $\frac{1}{4}(D^2 + D)$. Hence, this map is well-defined. It is straightforward to verify that these two associations are inverses and that the remaining claims are satisfied. ∎

Note that if two embeddings $R \to \mathcal{O}$ are related by Galois conjugation on R, then the corresponding elements of $\mathcal{O}^T$ are negatives of each other.

For any $\beta \in \mathcal{O}^T$, there exists a unique $\alpha \in \mathcal{O}$ satisfying $\tau(\alpha) = \beta$ and $\mathrm{Tr}(\alpha) \in \{0, 1\}$ (explicitly, we can let $\delta \in \{0, 1\}$ satisfy $\delta \equiv N(\beta) \pmod 2$ and set $\alpha = \frac{1}{2}(\delta + \beta)$). By Eq. (3.4), this element α attains the minimal norm among all elements of $\mathcal{O}$ mapping under τ to β.

Lemma 3.8 *Let $\beta_1, \beta_2, \beta_3 \in \mathcal{O}^T$ be linearly independent, and let $\alpha_1, \alpha_2, \alpha_3 \in \mathcal{O}$ satisfy $\tau(\alpha_i) = \beta_i$ and $\mathrm{Tr}(\alpha_i) \in \{0, 1\}$ for each i. The following are equivalent:*

(a) *The successive minima for $\mathcal{O}^T$ are attained by $\beta_1, \beta_2, \beta_3$.*
(b) *The successive minima for $\mathcal{O}$ are attained by $1, \alpha_1, \alpha_2, \alpha_3$, and if $\mathrm{Tr}(\alpha_i) = 0$ for some $i = 1, 2, 3$, then for all $\gamma \in \mathcal{O}$ with $N(\gamma) = N(\alpha_i)$ that are linearly independent from $1, \alpha_1, \ldots, \alpha_{i-1}$, we have $\mathrm{Tr}(\gamma) = 0$.*

Proof Observe that $1, \alpha_1, \alpha_2, \alpha_3$ are linearly independent, because applying τ to a linear dependence would induce a dependence among $\beta_1, \beta_2, \beta_3$. Now assume (a). For $i = 1, 2, 3$, let S_i denote the set of $\gamma \in \mathcal{O}$ satisfying $N(\gamma) < N(\alpha_i)$. For any $\gamma \in S_i$, we have

$$N(\tau(\gamma)) = 4N(\gamma) - \mathrm{Tr}(\gamma)^2 \le 4(N(\alpha_i) - 1) < 4N(\alpha_i) - \mathrm{Tr}(\alpha_i)^2 = N(\beta_i),$$

and since $N(\beta_i)$ is the ith successive minimum for $\mathcal{O}^T$, the span of $\tau(\gamma)$ for all $\gamma \in S_i$ has dimension at most $i - 1$. Thus the span of S_i has dimension at most i, proving by induction on i that $1, \alpha_1, \alpha_2, \alpha_3$ attain the successive minima for $\mathcal{O}$. Now for the sake of contradiction suppose that $\mathrm{Tr}(\alpha_i) = 0$, and there exists $\gamma \in \mathcal{O}$ linearly independent from $1, \alpha_1, \ldots, \alpha_{i-1}$ with $N(\gamma) = N(\alpha_i)$ and $\mathrm{Tr}(\gamma) \neq 0$. Then $\beta_1, \ldots, \beta_{i-1}, \tau(\gamma)$ are i independent elements of $\mathcal{O}^T$, but

$$N(\tau(\gamma)) = 4N(\gamma) - \mathrm{Tr}(\gamma)^2 < 4N(\alpha_i) = N(\beta_i),$$

https://doi.org/10.4153/S0008414X24000592 Published online by Cambridge University Press

contradicting the assumption that β_i attains the ith successive minimum for $\mathcal{O}^T$. Thus (a) implies (b).

Now assume (b). For $i = 1, 2, 3$, let S_i denote the set of $x \in \mathcal{O}^T$ satisfying $N(x) < N(\beta_i)$. For any $x \in S_i$, there exists $\gamma \in \mathcal{O}$ with $\tau(\gamma) = x$ and $\mathrm{Tr}(\gamma) \in \{0, 1\}$. If $N(x) < N(\beta_i) - 1$, then in fact $N(x) \leq N(\beta_i) - 3$ because the norm of every element of $\mathcal{O}^T$ is either 0 or 3 mod 4 by Eq. (3.4), and so

$$N(\gamma) = \frac{1}{4}(N(\tau(\gamma)) + \mathrm{Tr}(\gamma)^2) \leq \frac{1}{4}(N(\beta_i) - 2) < N(\alpha_i).$$

Since $N(\alpha_i)$ is the $(i+1)$st successive minimum for $\mathcal{O}$, this implies $1, \alpha_1, \ldots, \alpha_{i-1}, \gamma$ must be linearly dependent. On the other hand, suppose $N(x) = N(\beta_i) - 1$. Then $N(\gamma) = N(\alpha_i)$, $\mathrm{Tr}(\gamma) = 1$, and $\mathrm{Tr}(\alpha_i) = 0$, so once again $1, \alpha_1, \ldots, \alpha_{i-1}, \gamma$ are linearly dependent. Either way we can conclude that $x = \tau(\gamma)$ is in the $\mathbb{Q}$-span of $\beta_1, \ldots, \beta_{i-1}$. This shows that the span of S_i has dimension less than i, so $N(\beta_i)$ is indeed the ith successive minimum for $\mathcal{O}^T$. ∎

Remark 3.9 It is possible for $1, \alpha_1, \alpha_2, \alpha_3$ to attain the successive minima of $\mathcal{O}$, but $\tau(\alpha_1), \tau(\alpha_2), \tau(\alpha_3)$ not attain the successive minima of $\mathcal{O}^T$. A simple example is given by the Hurwitz quaternions $\mathcal{Z} = \langle 1, i, j, \frac{1}{2}(1 + i + j + k)\rangle$ with $i^2 = j^2 = -1$ and $ij = k$. The successive minima of $\mathcal{Z}$ are all 1, and the successive minima of $\mathcal{Z}^T$ are all 3. The elements $1, i, j, k$ attain the successive minima of $\mathcal{O}$, but $N(\tau(i)) = N(\tau(j)) = N(\tau(k)) = 4$, and so $\tau(i), \tau(j), \tau(k)$ do not realize the successive minima of $\mathcal{Z}^T$. And indeed, condition (b) of Lemma 3.8 does not hold; for any of $i = 1, 2, 3$, we can take $\gamma = \frac{1}{2}(1 + i + j + k)$.

Lemma 3.10 *Let $D_1 < 15$. Up to isomorphism, there is at most one maximal order $\mathcal{O} \subseteq B_p$ such that the first successive minimum of $\mathcal{O}^T$ is equal to D_1.*

Proof If D_1 is not 0 or 3 mod 4, then there is no maximal order with first successive minimum D_1 by Proposition 3.7. For all remaining D_1, the quadratic order of discriminant $-D_1$ has class number 1; in this case, there is a unique maximal order (up to isomorphism) in which this quadratic order embeds [21, Corollary 30.4.23], and therefore a unique $\mathcal{O}$ (up to isomorphism) such that $\mathcal{O}^T$ has an element of norm D_1. ∎

Remark 3.11 If $-D$ is a fundamental discriminant, an explicit maximal order admitting an optimal embedding of the ring of integers of discriminant $-D$ can be written down explicitly using [8, Eq. (5)] (see also [8, Theorem 1]).

3.4 Constraints on short Gross lattice vectors

A key idea we will apply is that there are very strict constraints on arrangements of short elements in the Gross lattice. This idea can be made precise using a construction due to Kaneko [12], which we present as Proposition 3.12 with minor modifications for our convenience. Kaneko used this construction to prove a bound on the discriminants of quadratic orders embedding into a quaternion order, a special case of which is given by Corollary 3.14. In addition to this bound (a constraint on the norms of independent elements in $\mathcal{O}^T$), we also establish a constraint on the angle between two

https://doi.org/10.4153/S0008414X24000592 Published online by Cambridge University Press

elements of $\mathcal{O}^T$, Corollary 3.15.[2] Together, these constraints will be sufficient to show that a quaternion order is uniquely determined up to isomorphism by the numbers of short vectors in $\mathcal{O}^T$.

Proposition 3.12 *Let $\mathcal{O}$ be an order in B_p, and let $\beta_1, \beta_2 \in \mathcal{O}^T$ be linearly independent. Then*

$$N(\beta_1)N(\beta_2) - \frac{1}{4}\operatorname{Tr}(\beta_1\bar{\beta}_2)^2$$

is a positive integer multiple of $4p$.

The number $N(\beta_1)N(\beta_2) - \frac{1}{4}\operatorname{Tr}(\beta_1\bar{\beta}_2)^2$ is the determinant of the Gram matrix of the lattice $\langle \beta_1, \beta_2 \rangle$, so this can be interpreted as saying that every parallelogram in $\mathcal{O}^T$ has area $2\sqrt{kp}$ for some positive integer k. A version of this is proven by Kaneko in [12, Section 3]; see also Equation (3.2) of [6]. A similar idea also appears in [10].

Proof The value is positive because it is the determinant of the Gram matrix of the lattice $\langle \beta_1, \beta_2 \rangle$, so it suffices to show divisibility by $4p$. For $i = 1, 2$, set $D_i = N(\beta_i)$, and let $\alpha_i \in \mathcal{O}$ be a minimal norm preimage of β_i under τ; that is, take $\delta_i \in \{0, 1\}$ with $\delta_i \equiv D_i \pmod 2$ and set $\alpha_i = \frac{1}{2}(\beta_i + \delta_i)$. Define an order

$$\Lambda = \langle 1, \alpha_1, \alpha_2, \alpha_1\alpha_2 \rangle \subseteq \mathcal{O}.$$

Letting $s = \operatorname{Tr}(\alpha_1\alpha_2)$, one can compute the trace matrix of Λ (Eq. (3.2)),

$$\mathbf{T} = \begin{pmatrix} 2 & \delta_1 & \delta_2 & s \\ \delta_1 & \delta_1^2 - 2N(\alpha_1) & s & -\delta_2 N(\alpha_1) + \delta_1 s \\ \delta_2 & s & \delta_2^2 - 2N(\alpha_2) & -\delta_1 N(\alpha_2) + \delta_2 s \\ s & -\delta_2 N(\alpha_1) + \delta_1 s & -\delta_1 N(\alpha_2) + \delta_2 s & s^2 - 2N(\alpha_1)N(\alpha_2) \end{pmatrix}.$$

Since $N(\alpha_i) = \frac{1}{4}(\delta_i + D_i)$, we compute

$$\operatorname{disc}\Lambda = |\det \mathbf{T}| = \frac{(D_1D_2 - (2s - \delta_1\delta_2)^2)^2}{16}.$$

Noting that

$$\operatorname{Tr}(\beta_1\beta_2) = \operatorname{Tr}((2\alpha_1 - \delta_1)(2\alpha_2 - \delta_2)) = 4\operatorname{Tr}(\alpha_1\alpha_2) - 2\delta_1\delta_2, \tag{3.5}$$

we can replace $2s - \delta_1\delta_2$ with $\frac{1}{2}\operatorname{Tr}(\beta_1\beta_2) = -\frac{1}{2}\operatorname{Tr}(\beta_1\bar{\beta}_2)$. Since Λ is an order in B_p, we can use Eq. (3.1) to conclude that $\frac{1}{4}(D_1D_2 - \frac{1}{4}\operatorname{Tr}(\beta_1\bar{\beta}_2)^2)$ is an integer multiple of p. ∎

Some immediate consequences of this calculation are as follows.

Corollary 3.13 *Let $\mathcal{O}$ be an order in B_p of discriminant $\Delta \in \mathbb{Z}$. Let D_1, D_2, D_3 be the successive minima of $\mathcal{O}^T$. Then*

[2] This is the only part of the argument that relies the fact that our quaternion algebra B_p is ramified at a single prime; if we consider orders in definite quaternion algebras ramified at multiple primes, the corresponding constraint becomes much less strict.

https://doi.org/10.4153/S0008414X24000592 Published online by Cambridge University Press

$$D_1 \le 2\Delta^{1/3},$$
$$\frac{4p}{D_1} \le D_2 \le \left(\frac{8\Delta}{D_1}\right)^{1/2}.$$

Proof Since $\det \mathcal{O} = \frac{\Delta}{16}$, Eq. (3.3) implies that

$$\det \mathcal{O}^T = \det(\mathbb{Z} \oplus \mathcal{O}^T) = 8^2 \det \mathcal{O} = 4\Delta.$$

(Recall that $\det \Lambda$ refers to the determinant of the Gram matrix of Λ, so $\Lambda' \subseteq \Lambda$ implies $\det \Lambda' = [\Lambda : \Lambda']^2 \det \Lambda$.) We also have $D_1 D_2 D_3 \le 2 \det \mathcal{O}^T$ (a bound specific to rank 3 lattices) by [20, Lecture XI(25)]. The desired upper bounds follow from $D_1^3 \le D_1 D_2 D_3$ and $D_1 D_2^2 \le D_1 D_2 D_3$. The lower bound $D_1 D_2 \ge 4p$ follows from Proposition 3.12. ∎

Corollary 3.14 *If a quadratic order R has two embeddings in $\mathcal{O}$ with distinct images, then* $\operatorname{disc} R > p$.

Proof This is a special case of [12, Theorem 2']. Let $D \coloneqq \operatorname{disc} R$, and $\beta_1, \beta_2 \in \mathcal{O}^T$ be the elements corresponding to the two embeddings of R under Proposition 3.7. Then from Proposition 3.12, we obtain

$$p \mid \left(\frac{D+t}{2}\right)\left(\frac{D-t}{2}\right),$$

where $t = \frac{1}{2}\operatorname{Tr}(\beta_1 \bar{\beta}_2) \in \mathbb{Z}$ by Eq. (3.5). Each factor is an integer: $D + t$ and $D - t$ have the same parity, and since their product is a multiple of 4, both must be even. Thus p divides one of the factors, so $p \le \frac{1}{2}(D + t)$. Since $D^2 - t^2 > 0$, we have $t < D$, so $p < D$. ∎

Recall that $(v_1, v_2) \mapsto \frac{1}{2}\operatorname{Tr}(v_1 \overline{v_2})$ defines an inner product on B_p. The following result says that if two elements of $\mathcal{O}^T$ are sufficiently small, then their norms uniquely determine the angle between them (up to negating either element). This is one of the most important conceptual ingredients of the proofs of Theorems 1.3 and 1.4: while the theta function records lengths of elements but loses all information about angles between them, this result allows us to recover information about angles from information about lengths.

Corollary 3.15 *Let β_1, β_2 be independent elements of $\mathcal{O}^T$. Suppose $N(\beta_1) \le p$, and that β_2 has minimal norm in $\beta_2 + \mathbb{Z}\beta_1$. Then $|\frac{1}{2}\operatorname{Tr}(\beta_1 \bar{\beta}_2)|$ equals the smallest positive square root of $N(\beta_1)N(\beta_2)$ modulo p.*

Proof By Proposition 3.12, we have $\frac{1}{4}\operatorname{Tr}(\beta_1 \bar{\beta}_2)^2 \equiv N(\beta_1)N(\beta_2) \pmod{4p}$, so that $|\frac{1}{2}\operatorname{Tr}(\beta_1 \bar{\beta}_2)|$, an integer by Eq. (3.5), is a square root of $N(\beta_1)N(\beta_2)$ modulo p. Expanding $N(\beta_2 \pm \beta_1) - N(\beta_2) \ge 0$, we obtain $\mp \operatorname{Tr}(\beta_1 \bar{\beta}_2) \le N(\beta_1)$; since this is true for both choices of sign, we have

$$0 \le |\tfrac{1}{2}\operatorname{Tr}(\beta_1 \bar{\beta}_2)| \le \frac{N(\beta_1)}{2} \le \frac{p}{2}.$$

There is a unique square root of $D_1 D_2$ modulo p in this interval. ∎

https://doi.org/10.4153/S0008414X24000592 Published online by Cambridge University Press

4 Theta function determines maximal order

In this section, we prove Theorems 1.3 and 1.4. We begin in Section 4.1 with a proof of Theorem 1.4, the statement that the successive minima of $\mathcal{O}^T$ determine the isomorphism type of $\mathcal{O}$. So to prove Theorem 1.3, all that remains to show is that the theta function of $\mathcal{O}$ determines the successive minima D_1, D_2, D_3 of $\mathcal{O}^T$. In Section 4.2, we introduce a decomposition of the theta function of $\mathcal{O}$. Using this decomposition and the results of Section 3.4, we show that the theta function of $\mathcal{O}$ determines D_1 and D_2, and in Section 4.4, we show that the theta function of $\mathcal{O}$ determines D_3.

4.1 Successive minima of Gross lattice determines the order

Let p be an odd prime, and let $\mathcal{O}$ be an order in B_p of discriminant r^2p^2. Let $\beta_1, \beta_2, \beta_3 \in \mathcal{O}^T$ attain the successive minima $D_1 \le D_2 \le D_3$ of $\mathcal{O}^T$, and assume $D_1 \ge 8r^2$. We will begin by showing that $\mathcal{O}^T$ is determined up to isometry by D_1, D_2, D_3.

For each pair $1 \le i < j \le 3$, let $0 \le T_{ij} \le \frac{p}{2}$ be the unique integer satisfying $T_{ij}^2 \equiv D_iD_j \pmod p$. Using Corollary 3.13, we have

$$N(\beta_1) \le N(\beta_2) \le \sqrt{\frac{8r^2p^2}{D_1}} \le p,$$

so by Corollary 3.15, we have $|\frac{1}{2}\operatorname{Tr}(\beta_i\bar{\beta}_j)| = T_{ij}$ for each pair i, j.

Since $\beta_1, \beta_2, \beta_3$ attain successive minima for the rank 3 lattice $\mathcal{O}^T$, they form a basis by Lemma 3.5. Let $\mathbf{A} = (\frac{1}{2}\operatorname{Tr}(\beta_i\bar{\beta}_j))_{i,j}$ be the corresponding Gram matrix. By replacing β_i with $-\beta_i = \bar{\beta}_i$ if necessary for some values of i, we can ensure that any two of the equations

$$\frac{1}{2}\operatorname{Tr}(\beta_1\bar{\beta}_2) = T_{12}, \qquad \frac{1}{2}\operatorname{Tr}(\beta_1\bar{\beta}_3) = T_{13}, \qquad \frac{1}{2}\operatorname{Tr}(\beta_2\bar{\beta}_3) = T_{23}$$

hold. So if in addition, we have $T_{ij} = 0$ for some pair i, j, then we can choose $\beta_1, \beta_2, \beta_3$ so that $\frac{1}{2}\operatorname{Tr}(\beta_i\bar{\beta}_j) = T_{ij}$ for all i, j. Thus, $\mathcal{O}^T$ is determined up to isometry.

On the other hand, suppose all T_{ij} are nonzero. Then without loss of generality, we have either $\mathbf{A} = \mathbf{A}_+$ or $\mathbf{A} = \mathbf{A}_-$, where

$$\mathbf{A}_\pm \coloneqq \begin{pmatrix} N(\beta_1) & T_{12} & \pm T_{13} \\ T_{12} & N(\beta_2) & T_{23} \\ \pm T_{13} & T_{23} & N(\beta_3) \end{pmatrix}.$$

Now the orthogonal direct sum $\mathbb{Z} \oplus \mathcal{O}^T$ is a sublattice of $\mathcal{O}$, and so $16\det\mathbf{A}$ must be a multiple of p^2. But we have

$$16\det(\mathbf{A}_+) - 16\det(\mathbf{A}_-) = 4T_{12}T_{23}T_{13}.$$

Since the integers T_{ij} satisfy $0 < T_{ij} \le \frac{p}{2}$, this difference is not a multiple of p, and therefore only one of $16\det(\mathbf{A}_+)$ and $16\det(\mathbf{A}_-)$ can be a multiple of p. This determines $\mathbf{A}$ uniquely, and so again, $\mathcal{O}^T$ is determined up to isometry. If we replace $\beta_1, \beta_2, \beta_3$ with $-\beta_1, -\beta_2, -\beta_3$, then we preserve $\mathcal{O}^T$ (and $\mathbf{A}$) but obtain a basis with opposite orientation. Thus $\mathcal{O}^T$ is determined up to orientation-preserving isometry.

https://doi.org/10.4153/S0008414X24000592 Published online by Cambridge University Press

Now, let $\mathcal{O}_1, \mathcal{O}_2$ be two orders in B_p, each of index r in some (perhaps different) maximal order. Suppose that $\mathcal{O}_1^T$ and $\mathcal{O}_2^T$ have the same successive minima. We established above that there exists an orientation-preserving isometry $\varphi : \mathcal{O}_1^T \to \mathcal{O}_2^T$, which extends by linearity to an orientation-preserving isometry $\varphi : B_p^0 \to B_p^0$ on the trace 0 subspace of B_p. Every such isometry can be written as a conjugation map $\varphi(x) = \gamma^{-1}x\gamma$ for some $\gamma \in B_p^\times$ [21, Proposition 4.5.10]. Finally, by a result of Chevyrev and Galbraith [6, Lemma 4], the conjugation map $\varphi : \mathcal{O}_1^T \to \mathcal{O}_2^T$ extends to an isomorphism $\mathcal{O}_1 \to \mathcal{O}_2$. This proves Theorem 1.4.

4.2 Decomposing the theta series along fibers of τ

Let $\tau: B_p \to B_p^0$ denote the map $\tau(x) = 2x - \mathrm{Tr}(x)$. Given any integral lattice $L \subseteq B_p$ that contains $\mathbb{Z}$, the fibers of τ partition L into cosets of $\mathbb{Z}$, allowing us to decompose the theta function of L into a sum over these cosets.

Define power series $\theta_0, \theta_1 \in \mathbb{Z}[[q]]$ by

$$\theta_0(q) = \sum_{n\in\mathbb{Z}} q^{n^2} = 1 + 2q + 2q^4 + 2q^9 + \dots,$$
$$\theta_1(q) = \sum_{n\in\mathbb{Z}} q^{n^2+n} = 2 + 2q^2 + 2q^6 + 2q^{12} + \dots.$$

Lemma 4.1 *Given an integral lattice $L \supseteq \mathbb{Z}$, we have*

$$\theta_L(q) = \left(\sum_{\substack{\beta\in\tau(L)\\ N(\beta)\equiv 0 \bmod 4}} q^{N(\beta)/4}\right)\theta_0(q) + \left(\sum_{\substack{\beta\in\tau(L)\\ N(\beta)\equiv 3 \bmod 4}} q^{(1+N(\beta))/4}\right)\theta_1(q).$$

In the case $L = \mathbb{Z}$, we have $\tau(L) = \{0\}$, and this reduces to the trivial observation $\theta_{\mathbb{Z}}(q) = \theta_0(q)$.

Proof We can write

$$\theta_L(q) = \sum_{x\in L} q^{N(x)} = \sum_{\beta\in\tau(L)} \sum_{x\in\tau^{-1}(\beta)} q^{N(x)}.$$

For all $\beta \in \tau(L)$, $N(\beta)$ is either 0 or 3 mod 4 by Eq. (3.4). We will determine the sum of $q^{N(x)}$ over x in $\tau^{-1}(\beta)$ in each of these two cases.

If $N(\beta) \equiv 0 \pmod 4$, then every $x \in \tau^{-1}(\beta)$ has even trace (cf. Proposition 3.7), so $\tau^{-1}(\beta) = \{\frac{1}{2}\beta + n : n \in \mathbb{Z}\}$. Since β is orthogonal to 1, we have

$$\sum_{x\in\tau^{-1}(\beta)} q^{N(x)} = \sum_{n\in\mathbb{Z}} q^{N(\beta/2)+n^2} = q^{N(\beta)/4}\theta_0(q).$$

If $N(\beta) \equiv 3 \pmod 4$, then every $x \in \tau^{-1}(\beta)$ has odd trace, so that $\tau^{-1}(\beta) = \{\frac{1}{2}\beta + n + \frac{1}{2} : n \in \mathbb{Z}\}$. Then

$$\sum_{x\in\tau^{-1}(\beta)} q^{N(x)} = \sum_{n\in\mathbb{Z}} q^{N(\beta/2)+(n+\frac{1}{2})^2} = q^{(N(\beta)+1)/4}\theta_1(q). \qquad \blacksquare$$

https://doi.org/10.4153/S0008414X24000592 Published online by Cambridge University Press

Remark 4.2 By identifying each of the terms in Lemma 4.1 as the even or odd parts of appropriate theta functions, we can rewrite the equality more elegantly as

$$\begin{aligned}\theta_L(q^4) = {} & \tfrac{1}{4}\big(\theta_{\tau(L)}(q)+\theta_{\tau(L)}(-q)\big)\big(\theta_{\mathbb{Z}}(q)+\theta_{\mathbb{Z}}(-q)\big)\\ & + \tfrac{1}{4}\big(\theta_{\tau(L)}(q)-\theta_{\tau(L)}(-q)\big)\big(\theta_{\mathbb{Z}}(q)-\theta_{\mathbb{Z}}(-q)\big)\\ = {} & \tfrac{1}{2}\big(\theta_{\tau(L)}(q)\theta_{\mathbb{Z}}(q)+\theta_{\tau(L)}(-q)\theta_{\mathbb{Z}}(-q)\big).\end{aligned}$$

This can also be obtained by recognizing $2L$ as the set of elements of even norm in $\mathbb{Z}\oplus\tau(L)$ (as in Eq. (3.3)). However, the form given in the lemma statement will be more convenient, as it displays more clearly the contributions to $\theta_L(q)$ from individual elements of $\tau(L)$.

One consequence of this lemma is that the theta series of an integral lattice containing $\mathbb{Z}$ can be determined from the theta series of its image under τ. The difficulty is recovering information about $\tau(L)$ from the theta series of L: the power series $f(q), g(q) \in \mathbb{Z}[\![q]\!]$ such that $\theta_L(q) = f(q)\theta_0(q) + g(q)\theta_1(q)$ are far from being unique.

Example 4.3 Let B_3 be the quaternion algebra over $\mathbb{Q}$ ramified at 3, defined by $i^2 = -1$ and $j^2 = k^2 = -3$ (with $k = ij$). Consider the two integral lattices

$$L_1 := \left\langle 1, i, \frac{1+j}{2}, k \right\rangle, \qquad L_2 := \left\langle 1, i, \frac{i+j}{2}, k \right\rangle.$$

These lattices are isometric (via swapping 1 with i) and therefore have the same theta function. However, their images under τ,

$$\tau(L_1) = \langle 2i, j, 2k \rangle, \qquad \tau(L_2) = \langle 2i, i+j, 2k \rangle,$$

are not isometric; they have different successive minima (3, 4, 12 and 4, 4, 12, respectively) and different theta functions. This demonstrates that the decomposition of a theta series as in Lemma 4.1 is not unique, and that we can not in general determine the lattice structure of $\tau(L)$ from the lattice structure of L alone.

From now on, we suppose $\mathcal{O}$ is a maximal order. Our goal in the remainder of the article is to use the geometry of $\mathcal{O}$ to obtain constraints on the terms appearing in Lemma 4.1, and so deduce the successive minima of $\mathcal{O}^T$. The strategy is to start with $L = \mathbb{Z}$ and inductively build up a lattice $\mathbb{Z} \subseteq L \subseteq \mathcal{O}$ with known structure, one dimension at a time. If $c_n q^n$ is the smallest nonzero term of $\theta_{\mathcal{O}}(q) - \theta_L(q)$, we can conclude that there are c_n elements of norm n in $\mathcal{O}\backslash L$, and no shorter elements. We then use general properties of quaternion orders to show that the traces of these elements can be determined; this allows us to determine the minimal polynomial of an element $\alpha \in \mathcal{O}$ of norm n whose image under τ attains the next successive minimum of $\mathcal{O}^T$. Finally, we can use Corollary 3.15 to determine the full lattice structure of $L + \langle\alpha\rangle$.

4.3 Determining D_1 and D_2

As above, let $\mathcal{O} \subseteq B_p$ be a maximal order, and let D_1, D_2, D_3 denote the successive minima of $\mathcal{O}^T$. If $p = 2, 3, 5, 7$, then there is a unique maximal order in B_p (for instance,

https://doi.org/10.4153/S0008414X24000592 Published online by Cambridge University Press

by [21, Exercise 30.6]), so the isomorphism type of $\mathcal{O}$ (and in particular, the successive minima of $\mathcal{O}^T$) are uniquely determined. Thus from now on, we can assume $p \geq 11$.

Lemma 4.4 *Let $c_n q^n$ denote the first nonzero term of $\theta_{\mathcal{O}}(q) - \theta_{\mathbb{Z}}(q)$. Then one of the following occurs:*

- *$c_n = 2$, in which case $D_1 = 4n$ and $D_2, D_3 \geq 4n + 3$.*
- *$c_n = 4$, in which case $D_1 = 4n - 1$ and $D_2, D_3 \geq 4n + 3$.*
- *$c_n = 6$, in which case $D_1 = 4n - 1$, $D_2 = 4n$, and $D_3 \geq 4n + 3$.*

Proof By Lemma 4.1, the term $c_n q^n$ has contributions from $\beta \in \mathcal{O}^T \backslash \{0\}$ with norm $4n$ or $4n - 1$. Since n is minimal these elements are primitive, so by Proposition 3.7 they correspond to optimal embeddings of quadratic orders of discriminant $4n$ and $4n - 1$, respectively. We have $4n - 1 \leq D_1 \leq 2p^{2/3}$ by Corollary 3.13, which implies $4n \leq p$ since $p \geq 11$. So by Corollary 3.14, there cannot exist $\alpha, \alpha' \in \mathcal{O}$ both of norm n but generating distinct isomorphic subfields of $\mathcal{O}$. Hence, there are only three options: only $\mathbb{Z}[\sqrt{-n}]$ optimally embeds in $\mathcal{O}$, only $\mathbb{Z}[\frac{1+\sqrt{1-4n}}{2}]$ optimally embeds, or both optimally embed. These three cases can each be identified by counting the number of norm n elements in each quadratic order. ∎

If $D_1 < 15$, then the isomorphism type of $\mathcal{O}$ is uniquely determined by Lemma 3.10; in particular, the remaining successive minima D_2 and D_3 of $\mathcal{O}^T$ are also determined. So from now on, we assume $D_1 \geq 15$. Using Lemma 4.4, we use $\theta_{\mathcal{O}}$ to deduce the existence of an element $\alpha_1 \in \mathcal{O}$ with norm n and trace either 0 or 1, depending on the parity of D_1; hence we can determine the structure of $\mathbb{Z}[\alpha_1]$.

Lemma 4.5 *Suppose $D_1 \geq 15$, and let $c_n q^n$ denote the first nonzero term of $\theta_{\mathcal{O}}(q) - \theta_{\mathbb{Z}[\alpha_1]}(q)$. Then one of the following occurs:*

- *$c_n = 2$, in which case $D_2 = 4n$ and $D_3 \geq 4n + 3$.*
- *$c_n = 4$, in which case $D_2 = 4n - 1$ and $D_3 \geq 4n + 3$.*
- *$c_n = 6$, in which case $D_2 = 4n - 1$ and $D_3 = 4n$.*

Proof The term $c_n q^n$ has contributions from $\beta \in \mathcal{O}^T \backslash \tau(\mathbb{Z}[\alpha_1])$ with norm $4n$ or $4n - 1$. We can use the same argument as in Lemma 4.4, except that here, we use the bound $4n - 1 \leq D_2 \leq p\sqrt{8/D_1}$ from Corollary 3.13; since $D_1 \geq 15$ and $p \geq 11$ we can conclude $4n \leq p$ as before. ∎

Using our information about D_1 and D_2, we can determine the structure of a particular rank 3 sublattice of $\mathcal{O}$. (The exact form of the Gram matrix is not important to the proof; we only require the fact that it can be determined knowing only D_1, D_2, and p.)

Lemma 4.6 *Let $\delta_i \in \{0, 1\}$ satisfy $\delta_i \equiv D_i \pmod 2$ for $i = 1, 2$, and let T be the unique integer satisfying $0 \leq T \leq \frac{p-1}{2}$ and $T^2 \equiv D_1 D_2 \pmod p$. There exist $\alpha_1, \alpha_2 \in \mathcal{O}$ such that $\tau(\alpha_1), \tau(\alpha_2)$ attain the first two successive minima for $\mathcal{O}^T$, and the Gram matrix for $L \coloneqq \langle 1, \alpha_1, \alpha_2 \rangle$ is*

$$\begin{pmatrix} 1 & \frac{1}{2}\delta_1 & \frac{1}{2}\delta_2 \\ \frac{1}{2}\delta_1 & \frac{1}{4}(D_1 + \delta_1) & \frac{1}{4}(T + \delta_1\delta_2) \\ \frac{1}{2}\delta_2 & \frac{1}{4}(T + \delta_1\delta_2) & \frac{1}{4}(D_2 + \delta_2) \end{pmatrix}.$$

https://doi.org/10.4153/S0008414X24000592 Published online by Cambridge University Press

Proof Let α_1, α_2 be such that

$$N(\tau(\alpha_i)) = 4N(\alpha_i) - \mathrm{Tr}(\alpha_i)^2 = D_i$$

for $i = 1, 2$. Adding an integer to α_i if necessary, we may assume $\mathrm{Tr}(\alpha_i) = \delta_i$, so $N(\alpha_i) = \frac{1}{4}(D_i + \delta_i)$. Replacing α_2 with $\bar{\alpha_2}$ if necessary, we can further assume that $\mathrm{Tr}(\tau(\alpha_1)\overline{\tau(\alpha_2)}) \geq 0$. We have $D_1 \leq 2p^{2/3} \leq p$, so by Corollary 3.15, we have

$$T = \frac{1}{2}\mathrm{Tr}(\tau(\alpha_1)\overline{\tau(\alpha_2)}) = 2\,\mathrm{Tr}(\alpha_1\bar{\alpha_2}) - \delta_1\delta_2.$$

We can then solve for $\mathrm{Tr}(\alpha_1\bar{\alpha_2}) = \frac{1}{2}(T + \delta_1\delta_2)$, and this determines the Gram matrix for the basis $1, \alpha_1, \alpha_2$. ∎

4.4 Determining D_3 from D_1 and D_2

As above, we assume $D_1 \geq 15$ (since Lemma 3.10 applies when $D_1 < 15$). We can identify the fourth successive minimum of $\mathcal{O}$ as the index of the smallest nonzero term of $\theta_{\mathcal{O}} - \theta_L$, where $L = \langle 1, \alpha_1, \alpha_2 \rangle$ as in Lemma 4.6. Recall that in Lemma 4.4 (resp. Lemma 4.5), we showed that if $c_n q^n$ is the first nonzero term of $\theta_{\mathcal{O}} - \theta_{\mathbb{Z}}$ (resp. $\theta_{\mathcal{O}} - \theta_{\mathbb{Z}[\alpha_1]}$), then there are at most two elements with norm n in $\mathcal{O}\backslash\mathbb{Z}$ (resp. in $\mathcal{O}\backslash\mathbb{Z}[\alpha]$) up to negation and conjugation. Using this constraint, we could determine the traces of these elements, and hence the first (resp. second) successive minimum of $\mathcal{O}^T$.

Unfortunately, n can be much larger than in previous cases, so Corollary 3.14 may no longer be useful; it is possible for there to exist two elements of $\mathcal{O}$ of the same norm n generating distinct but isomorphic subfields. Thus the first nonzero coefficient may not be sufficient to determine D_3. However, we will show that the first two coefficients of $\theta_{\mathcal{O}} - \theta_L$ are sufficient.

We begin with two plane geometry lemmas.

Lemma 4.7 *Let $\Lambda \subseteq \mathbb{R}^2$ be a rank 2 lattice with positive-definite quadratic form Q, and $v \in \mathbb{R}^2$. Let c denote the minimum of $Q(v - w)$ for $w \in \Lambda$, and λ the minimum of $Q(w)$ for $w \in \Lambda\backslash\{0\}$. Then, there exists a set of four points $P \subseteq \Lambda$, forming the vertices of a translated fundamental parallelogram of Λ, such that for all $w \in \Lambda\backslash P$, we have $Q(v - w) \geq c + \lambda$.*

We call a set P satisfying the conclusion of Lemma 4.7 a *separating set* for v, since we can use it to ensure that no other element of Λ is too close to v. Note that elements $w \in P$ may themselves satisfy $Q(v - w) \geq c + \lambda$, and a separating set for v in Λ is not necessarily unique.

Proof Let $\cdot$ denote the bilinear form associated with Q. By standard lattice basis reduction arguments, there exists a basis u_1', u_2' for Λ such that the triangle with vertices $0, u_1', u_2'$ is right or acute, in the sense that $u_1' \cdot u_2'$, $(-u_2') \cdot (u_1' - u_2')$, and $(-u_1') \cdot (u_2' - u_1')$ are all nonnegative. The plane is tiled by congruent copies of this triangle with vertices lying in Λ; let Δ be one such triangle containing v (allowing v to lie on the boundary of Δ). Let r_1, r_2, r_3 be the vertices of Δ, and s the orthocenter of Δ (that is, s satisfies $(r_i - s) \cdot (r_j - r_k) = 0$ for all permutations i, j, k of $1, 2, 3$). Then Δ can be written as the union of three triangles Δ_{12}, Δ_{23}, and Δ_{13}, where Δ_{ij} is defined

https://doi.org/10.4153/S0008414X24000592 Published online by Cambridge University Press

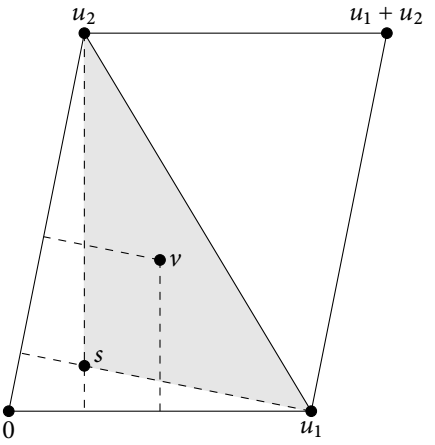

Figure 1: If v lies in the highlighted gray triangle, then $P = \{0, u_1, u_2, u_1 + u_2\}$ satisfies the conclusion of Lemma 4.7.

as the triangle with vertices r_i, r_j, s. Without loss of generality, suppose $v \in \Delta_{12}$. After translation by $-r_3$, and setting $u_1 \coloneqq r_1 - r_3$ and $u_2 \coloneqq r_2 - r_3$, we can assume that Δ has vertices $0, u_1, u_2$ and that v lies in the triangle with vertices s, u_1, u_2, as in Figure 1. By computing the orthogonal projections of u_2, v, u_1 onto the span of u_1 (and similarly onto the span of u_2), we obtain the relations

$$0 \le u_2 \cdot u_1 \le v \cdot u_1 \le u_1 \cdot u_1,$$
$$0 \le u_1 \cdot u_2 \le v \cdot u_2 \le u_2 \cdot u_2.$$

To simplify notation set

$$t \coloneqq u_1 \cdot u_2, \qquad s_1 \coloneqq v \cdot u_1, \qquad s_2 \coloneqq v \cdot u_2,$$

so we have $0 \le t \le s_i \le Q(u_i)$ for each $i = 1, 2$.

Now for any lattice element $w \in \Lambda$, we exhibit $w_0 \in P \coloneqq \{0, u_1, u_2, u_1 + u_2\}$ such that $(v - w_0) \cdot (w - w_0) \le 0$. Set $w = as_1 + bs_2$ for some $a, b \in \mathbb{Z}$.

- If $a, b \le 0$, then $v \cdot w = as_1 + bs_2 \le 0$.
- If $a \ge 1$ and $b \le 0$, then $(v - u_1) \cdot (w - u_1) = (a-1)(s_1 - Q(u_1)) + b(s_2 - t) \le 0$.
- If $a \le 0$ and $b \ge 1$, then $(v - u_2) \cdot (w - u_2) = a(s_1 - t) + (b-1)(s_2 - Q(u_2)) \le 0$.
- If $a, b \ge 1$, then

$$(v - u_1 - u_2) \cdot (w - u_1 - u_2) = (a-1)(s_1 - Q(u_1) - t) + (b-1)(s_2 - Q(u_2) - t) \le 0.$$

We therefore have

$$Q(v - w) \ge Q(v - w_0) + Q(w - w_0).$$

We have $Q(v - w_0) \ge c$, and $Q(w - w_0) \ge \lambda$ unless $w = w_0$. ∎

https://doi.org/10.4153/S0008414X24000592 Published online by Cambridge University Press

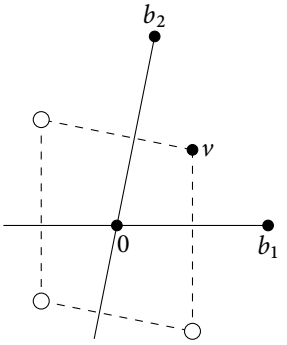

Figure 2: The white circles indicate the points $w \in \mathbb{R}^2$ with $w \neq v$ and $|w \cdot b_j| = |v \cdot b_j|$ for $j = 1, 2$. If b_1 and b_2 are not orthogonal, then the only such point with the same norm as v is $-v$.

Lemma 4.8 *Let $b_1, b_2 \in \mathbb{R}^2$ be linearly independent vectors, and let $v_1, v_2 \in \mathbb{R}^2$ be distinct vectors. Let $(x, y) \mapsto x \cdot y$ denote the bilinear form associated with a positive-definite quadratic form on $\mathbb{R}^2$. If $b_1 \cdot b_2 \neq 0$, $v_1 \cdot v_1 = v_2 \cdot v_2$, and $|v_1 \cdot b_j| = |v_2 \cdot b_j|$ for $j = 1, 2$, then $v_1 = -v_2$.*

See Figure 2 for an intuitive explanation of this result.

Proof Since b_1, b_2 form a basis for $\mathbb{R}^2$, it suffices to show that $v_1 \cdot b_j = -v_2 \cdot b_j$ for each $j = 1, 2$. For the sake of contradiction, suppose $v_1 \cdot b_1 = v_2 \cdot b_1 \neq 0$. Since v_1 and v_2 are distinct, we must then have $v_1 \cdot b_2 \neq v_2 \cdot b_2$, so $v_1 \cdot b_2 = -v_2 \cdot b_2$. Set $b_2^* = b_2 - \frac{b_2 \cdot b_1}{b_1 \cdot b_1} b_1$, so that for $i = 1, 2$, we can write

$$v_i = \frac{v_i \cdot b_1}{b_1 \cdot b_1} b_1 + \frac{v_i \cdot b_2^*}{b_2^* \cdot b_2^*} b_2^*$$

with b_1, b_2^* orthogonal. Since $v_1 \cdot v_1 = v_2 \cdot v_2$ but $v_1 \neq v_2$, we can conclude that $v_1 \cdot b_2^* = -v_2 \cdot b_2^*$, or expanding,

$$v_1 \cdot b_2 - \frac{b_2 \cdot b_1}{b_1 \cdot b_1}(v_1 \cdot b_1) = -v_2 \cdot b_2 + \frac{b_2 \cdot b_1}{b_1 \cdot b_1}(v_2 \cdot b_1).$$

Since $v_1 \cdot b_2 = -v_2 \cdot b_2$ and $v_1 \cdot b_1 = v_2 \cdot b_1 \neq 0$, we conclude $b_2 \cdot b_1 = 0$, a contradiction. Hence $v_1 \cdot b_1 = -v_2 \cdot b_1$, and similarly $v_1 \cdot b_2 = -v_2 \cdot b_2$, so that $v_1 = -v_2$. ∎

We now return to the quaternion setting; we continue to assume $D_1 \geq 15$ and $p \geq 11$ (though all we will use from now on is $D_1 > 5$ and p odd). Note that from $L = \langle 1, \alpha_1, \alpha_2 \rangle$, we obtain a rank 2 lattice

$$\tau(L) = \langle \beta_1, \beta_2 \rangle;$$

under the isomorphism between $B_p \otimes \mathbb{R}$ and $\mathbb{R}^4$, we obtain a lattice in $\mathbb{R}^2$ to which we can apply Lemmas 4.7 and 4.8.

Lemma 4.9 *There exists a set $S \subseteq \mathcal{O}^T \backslash \tau(L)$ of four elements with the following properties:*

https://doi.org/10.4153/S0008414X24000592 Published online by Cambridge University Press

(a) *For all* $\gamma \in \mathcal{O}^T \backslash (\tau(L) \cup S \cup -S)$, *we have* $N(\gamma) \geq D_3 + D_1$.
(b) *At most two elements of* S *have even norm.*
(c) *If* S *contains two elements* γ_1, γ_2 *with* $N(\gamma_1) = N(\gamma_2) < D_3 + D_1$, *then the remaining two elements* $\gamma_3, \gamma_4 \in S$ *satisfy* $N(\gamma_3) = N(\gamma_4)$.

Proof Let $\beta_1, \beta_2, \beta_3 \in \mathcal{O}^T$ attain the successive minima D_1, D_2, D_3. By Lemma 3.5, these elements form a basis of $\mathcal{O}^T$, so the quotient $\mathcal{O}^T/\tau(L)$ is an infinite cyclic group generated by β_3. Let v be the orthogonal projection of β_3 onto $\mathbb{R}\tau(L)$, so $u \coloneqq \beta_3 - v$ is orthogonal to $\mathbb{R}\tau(L)$. Note that if we had $N(v - w) < N(v)$ for some $w \in \tau(L)$, this would imply

$$N(\beta_3 - w) = N(v - w) + N(u) < N(v) + N(u) = N(\beta_3),$$

contradicting the fact that β_3 attains the third successive minimum. Hence $N(v) \leq N(v - w)$ for all $w \in \tau(L)$. In particular, $N(v)$ is bounded by the square of the covering radius of $\tau(L)$; since the covering radius is bounded by $\frac{\sqrt{2}}{2}\sqrt{D_2}$ we have $N(v) \leq \frac{1}{2}D_2$.

Now any $\gamma \in \mathcal{O}^T \backslash \tau(L)$ can be written in the form

$$\gamma = a\beta_3 - w = au + (av - w)$$

for some $a \in \mathbb{Z}\backslash\{0\}$ and $w \in \tau(L)$. If $|a| \geq 2$, then using $N(v) \leq \frac{1}{2}D_2 \leq \frac{1}{2}D_3$, we have

$$N(\gamma) = |a|^2 N(u) + N(av - w) \geq 4N(u) = 4(N(\beta_3) - N(v)) \geq 2D_3 \geq D_3 + D_1.$$

On the other hand, suppose $a = 1$, so that $\gamma = u + (v - w)$. Then by Lemma 4.7, there exists $P \subseteq \tau(L)$ forming the vertices of a translated fundamental parallelogram for $\tau(L)$ such that for all $w \in \tau(L)\backslash P$, we have

$$N(\gamma) = N(u) + N(v - w) \geq N(u) + N(v) + D_1 = D_3 + D_1.$$

In other words, we have $N(\gamma) \geq D_3 + D_1$ provided $\gamma \notin \beta_3 - P$. Finally, if $a = -1$ (so $\gamma = -u + (-v - w)$), the same argument shows that $N(\gamma) \geq D_3 + D_1$ unless $\gamma \in -\beta_3 + P$. So taking $S \coloneqq \beta_3 - P$ as in Figure 3, (a) follows.

Now for the sake of contradiction, suppose $N(\gamma_i)$ is even for three elements $\gamma_1, \gamma_2, \gamma_3 \in S$. The points $w_i = \beta_3 - \gamma_i$ lie on P, so their pairwise differences $\gamma_i - \gamma_j = w_j - w_i$ (for $i, j \in \{1, 2, 3\}$) contain a basis for $\tau(L)$. This implies that $\langle \gamma_1, \gamma_2, \gamma_3 \rangle = \mathcal{O}^T$. But since $\mathrm{Tr}(uv)$ is even for all $u, v \in \mathcal{O}^T$ (Eq. (3.5)), the set of points in $\mathcal{O}^T$ with even norm is closed under addition. Hence, every element of $\mathcal{O}^T$ must have even norm. This is a contradiction, because $\mathcal{O}$ contains an element of odd trace (see Eq. (3.4) and the discussion after Eq. (3.3)). Thus (b) must hold.

Finally, suppose $N(\gamma_1) = N(\gamma_2) < D_3 + D_1$ for some distinct $\gamma_1, \gamma_2 \in S$. For each $i, j \in \{1, 2\}$, we have

$$D_3 \leq N(\gamma_i \pm \beta_j) = N(\gamma_i) + N(\beta_j) \pm \mathrm{Tr}(\gamma_i \bar{\beta}_j) < (D_3 + D_1) + D_2 \pm \mathrm{Tr}(\gamma_i \bar{\beta}_j),$$

and, since $D_1, D_2 < p$ by Corollary 3.13 (recall we are assuming $D_1 \geq 15$), we have $|\mathrm{Tr}(\gamma_i \bar{\beta}_j)| < 2p$. We also have $|\frac{1}{2}\mathrm{Tr}(\gamma_i \bar{\beta}_j)|^2 \equiv N(\gamma_i)N(\beta_j) \pmod{4p}$ by Proposition 3.12. So $|\frac{1}{2}\mathrm{Tr}(\gamma_i \bar{\beta}_j)|$ equals the square root modulo $2p$ of $N(\gamma_i)N(\beta_j)$ in the interval $[0, p)$, which is unique because $(\mathbb{Z}/2p\mathbb{Z})^\times$ is cyclic.

https://doi.org/10.4153/S0008414X24000592 Published online by Cambridge University Press

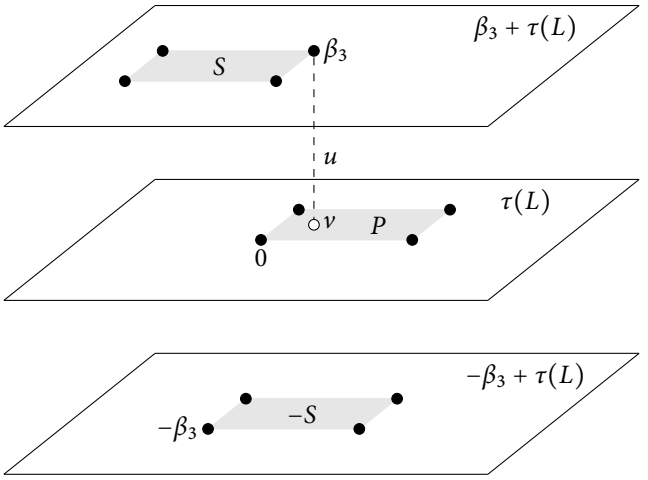

Figure 3: Setup for the proof of Lemma 4.9. Black dots correspond to elements of $\mathcal{O}^T$. The sets P, S, and $-S$ are the vertices of the parallelograms with the corresponding labels.

For $i = 1, 2$, let v_i be the projection of γ_i onto $\mathbb{R}\tau(L)$, so that $\gamma_i = u + v_i$ with u orthogonal to v_i; note that $v_1 \neq v_2$. Since $N(\gamma_1) = N(\gamma_2)$, we have $N(v_1) = N(v_2)$, and for $j = 1, 2$, we have

$$|\operatorname{Tr}(v_1\bar{\beta}_j)| = |\operatorname{Tr}(\gamma_1\bar{\beta}_j)| = |\operatorname{Tr}(\gamma_2\bar{\beta}_j)| = |\operatorname{Tr}(v_2\bar{\beta}_j)|.$$

Further, we have $0 < N(\beta_1), N(\beta_2) < p$ by Corollary 3.13, and so $\operatorname{Tr}(\beta_2\bar{\beta}_1) \neq 0$ by Proposition 3.12. So by Lemma 4.8, we can conclude $v_1 = -v_2$. Now if $\gamma_3, \gamma_4 \in S$ are the remaining two elements with $\gamma_3 = u + v_3$ and $\gamma_4 = u + v_4$, then we must have $v_3 = -v_4$ because the four elements of S form the vertices of a parallelogram. Hence $N(\gamma_3) = N(\gamma_4)$, proving (c). ∎

Lemma 4.10 *Suppose $D_1 \geq 15$, and let*

$$(\theta_{\mathcal{O}} - \theta_L)(q) = c_n q^n + c_{n+1} q^{n+1} + \dots$$

for some $n \geq 0$. If $c_n = 2$, or if $c_n = 4$ and $c_{n+1} \geq 8$, then $D_3 = 4n$; otherwise $D_3 = 4n - 1$.

Proof As in Lemma 4.4, the existence of an element of norm n in $\mathcal{O}\backslash L$ (and no smaller norm) guarantees that D_3 is equal to either $4n - 1$ or $4n$. Let $S \subseteq \mathcal{O}^T\backslash\tau(L)$ be as in Lemma 4.9. Since $N(\gamma) \geq D_3 + 15 > 4n + 4$ for all $\gamma \in \mathcal{O}^T\backslash(\tau(L) \cup S \cup -S)$, the series $\theta_{\mathcal{O}}(q) - \theta_L(q)$ is congruent to

(4.1)
$$\left(\sum_{\substack{\beta\in S \\ N(\beta)\equiv 0 \bmod 4}} 2q^{N(\beta)/4}\right)\theta_0(q) + \left(\sum_{\substack{\beta\in S \\ N(\beta)\equiv 3 \bmod 4}} 2q^{(1+N(\beta))/4}\right)\theta_1(q) \pmod{q^{n+2}}.$$

https://doi.org/10.4153/S0008414X24000592 Published online by Cambridge University Press

We divide into cases based on the number of elements of norm $4n-1$ and $4n$ in S. First, we consider the cases that S has no elements of norm $4n-1$, so that $D_3 = 4n$. Then S contains either one or two elements of norm $4n$: S cannot contain more than two elements of norm $4n$ by Lemma 4.9(b). Recall that $\theta_0(q) \equiv 1 + 2q \pmod{q^2}$ and $\theta_1(q) \equiv 2 \pmod{q^2}$.

- If S contains one element of norm $4n$, this element contributes $2q^n\theta_0(q)$ to Eq. (4.1) and every other element of S contributes a multiple of q^{n+1}, so $c_n = 2$.
- If S contains two elements of norm $4n$, these elements contribute $4q^n\theta_0(q)$ to Eq. (4.1) and every other element of S contributes a multiple of q^{n+1}, so $c_n = 4$ and $c_{n+1} \geq 8$.

Now consider the cases that S has at least one element of norm $4n-1$, so that $D_3 = 4n-1$.

- If S contains at least two elements of norm $4n-1$, these contribute $4q^n\theta_1(q)$ to Eq. (4.1), so $c_n \geq 8$.
- If S contains at least one element of norm $4n-1$ and at least one element of norm $4n$, these contribute $2q^n\theta_0(q) + 2q^n\theta_1(q)$ to Eq. (4.1), so $c_n \geq 6$.
- Suppose S contains exactly one element of norm $4n-1$, and no elements of norm $4n$. The element of norm $4n-1$ contributes $2q^n\theta_1(q)$ to Eq. (4.1), so $c_n = 4$. Now by Lemma 4.9(c), S contains at most one element of norm $4n+3$ and at most one element of norm $4n+4$. Thus the largest possible value of c_{n+1} is attained by

$$2q^n\theta_1(q) + 2q^{n+1}\theta_0(q) + 2q^{n+1}\theta_1(q),$$

  which has $c_{n+1} = 6$. In any case, we will have $c_n = 4$ and $c_{n+1} \leq 6$.

Combining these results, we see that if $D_3 = 4n$, then either we have $c_n = 2$ or we have $c_n = 4$ and $c_{n+1} \geq 8$. When $D_3 = 4n-1$, then either we have $c_n \geq 6$ or we have $c_n = 4$ and $c_{n+1} \leq 6$. ∎

In conclusion, the theta function of $\mathcal{O}$ uniquely determines the successive minima D_1, D_2, D_3 of $\mathcal{O}^T$. By Theorem 1.4, these values uniquely determine the isomorphism type of $\mathcal{O}$, establishing Theorem 1.3.

Acknowledgments We thank Eran Assaf, Naser Sardari, and John Voight for useful discussion. We also thank Jens Funke for interesting comments and bringing the paper [2] to our attention.

References

[1] E. Bank, C. Camacho-Navarro, K. Eisenträger, T. Morrison, and J. Park, *Cycles in the supersingular ℓ-isogeny graph and corresponding endomorphisms*. In: J. Balakrishnan, A. Folsom, M. Lalín, and M. Manes (eds.), Research directions in number theory—Women in numbers IV. Vol. 19. Association for Women in Mathematics Series, Springer, Cham, 2019, pp. 41–66. https://doi.org/10.1007/978-3-030-19478-9_2

[2] S. Böcherer and R. Schulze-Pillot, *Siegel modular forms and theta series attached to quaternion algebras*. Nagoya Math. J. **121**(1991), 35–96. https://doi.org/10.1017/S0027763000003391

[3] T. D. Browning and R. Dietmann, *On the representation of integers by quadratic forms*. Proc. Lond. Math. Soc. (3) **96**(2008), 389–416. https://doi.org/10.1112/plms/pdm032

[4] J. Brzeziński, *On orders in quaternion algebras*. Comm. Algebra **11**(1983), no. 5, 501–522. https://doi.org/10.1080/00927878308822861

[5] J. W. S. Cassels, *An introduction to the geometry of numbers*, Classics in Mathematics, corrected reprint of the 1971 edition, Springer, Berlin, 1997.
[6] I. Chevyrev and S. D. Galbraith, *Constructing supersingular elliptic curves with a given endomorphism ring*. LMS J. Comput. Math. **17**(2014), 71–91. https://doi.org/10.1112/S1461157014000254
[7] J. H. Conway and N. J. A. Sloane, *Four-dimensional lattices with the same theta series*. Internat. Math. Res. Notices **4**(1992), 93–96. https://doi.org/10.1155/S1073792892000102
[8] D. Dorman, *Global orders in definite quaternion algebras as endomorphism rings for reduced CM elliptic curves*. In: J.-M. De Koninck and C. Levesque (eds.), Théorie des nombres (Quebec, PQ, 1987), de Gruyter, Berlin, 1989, pp. 108–116.
[9] K. Eisenträger, S. Hallgren, K. Lauter, T. Morrison, and C. Petit, *Supersingular isogeny graphs and endomorphism rings: Reductions and solutions*. In: J. B. Nielsen and V. Rijmen (eds.), Advances in cryptology—EUROCRYPT 2018. Part III. Vol. 10822, Lecture Notes in Computer Science, Springer, Cham, 2018, pp. 329–368. https://doi.org/10.1007/978-3-319-78372-7_11
[10] E. Z. Goren and K. E. Lauter, *Class invariants for quartic CM fields*. Ann. Inst. Fourier (Grenoble) **57**(2007), no. 2, 457–480.
[11] B. H. Gross, *Heights and the special values of L-series*. In: H. Kisilevsky and J. Labute (eds.), Number theory (Montreal, QC, 1985), Vol. 7, CMS Conference Proceedings, American Mathematical Society, Providence, RI, 1987, pp. 115–187.
[12] M. Kaneko, *Supersingular j-invariants as singular moduli* mod p. Osaka J. Math. **26**(1989), no. 4, 849–855.
[13] Y. Kitaoka, *Representations of quadratic forms and their application to Selberg's zeta functions*. Nagoya Math. J. **63**(1976), 153–162.
[14] D. R. Kohel, *Endomorphism rings of elliptic curves over finite fields*. Ph.D. thesis, University of California, Berkeley, 1996.
[15] J. Martinet, *Perfect lattices in Euclidean spaces*, Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 327, Springer, Berlin, 2003. https://doi.org/10.1007/978-3-662-05167-2
[16] E. Nilsson, J. Rowlett, and F. Rydell, *The isospectral problem for flat tori from three perspectives*. Bull. Amer. Math. Soc. (N.S.) **60**(2023), 39–83. https://doi.org/10.1090/bull/1770
[17] N. T. Sardari, *Optimal strong approximation for quadratic forms*. Duke Math. J. **168**(2019), no. 10, 1887–1927. https://doi.org/10.1215/00127094-2019-0007
[18] A. Schiemann, *Ternary positive definite quadratic forms are determined by their theta series*. Math. Ann. **308**(1997), no. 3, 507–517. https://doi.org/10.1007/s002080050086
[19] K. Shiota, *On theta series and the splitting of* $S2(\Gamma 0(q))$. J. Math. Kyoto Univ. **31**(1991), 909–930. https://doi.org/10.1215/kjm/1250519669
[20] C. L. Siegel, *Lectures on the geometry of numbers*, Notes by B. Friedman, Rewritten by Komaravolu Chandrasekharan with the assistance of Rudolf Suter, With a preface by Chandrasekharan, Springer, Berlin, 1989. https://doi.org/10.1007/978-3-662-08287-4
[21] J. Voight, *Quaternion algebras*, Graduate Texts in Mathematics, 288, Springer, Cham, 2021. https://doi.org/10.1007/978-3-030-56694-4
[22] G. L. Watson, *Integral quadratic forms*, Cambridge Tracts in Mathematics and Mathematical Physics, 51, Cambridge University Press, New York, 1960.

Department of Mathematics and Statistics, McGill University, Montréal, QC, Canada
e-mail: eyal.goren@mcgill.ca jon.love@mcgill.ca