ALGORITHMIC ENUMERATION OF IDEAL CLASSES FOR QUATERNION ORDERS

MARKUS KIRSCHMER AND JOHN VOIGHT

ABSTRACT. We provide algorithms to count and enumerate representatives of the (right) ideal classes of an Eichler order in a quaternion algebra defined over a number field. We analyze the run time of these algorithms and consider several related problems, including the computation of two-sided ideal classes, isomorphism classes of orders, connecting ideals for orders, and ideal principalization. We conclude by giving the complete list of definite Eichler orders with class number at most 2.

Since the very first calculations of Gauss for imaginary quadratic fields, the problem of computing the class group of a number field F has seen broad interest. Due to the evident close association between the class number and regulator (embodied in the Dirichlet class number formula), one often computes the class group and unit group in tandem as follows.

PROBLEM (ClassUnitGroup($\mathbb{Z}_F$)). Given the ring of integers $\mathbb{Z}_F$ of a number field F, compute the class group $\operatorname{Cl}\mathbb{Z}_F$ and unit group $\mathbb{Z}_F^*$.

This problem appears in general to be quite difficult. The best known (probabilistic) algorithm is due to Buchmann [7]: for a field F of degree n and absolute discriminant d_F, it runs in time $d_F^{1/2}(\log d_F)^{O(n)}$ without any hypothesis [32], and assuming the Generalized Riemann Hypothesis (GRH), it runs in *expected* time $\exp\big(O\big((\log d_F)^{1/2}(\log\log d_F)^{1/2}\big)\big)$, where the implied O-constant depends on n.

According to the Brauer-Siegel theorem, already the case of imaginary quadratic fields shows that the class group is often roughly as large as $d_F^{1/2}(\log d_F)^{O(1)}$. Similarly, for the case of real quadratic fields, a fundamental unit is conjectured to have height often as large as $d_F^{1/2}(\log d_F)^{O(1)}$, so even to write down the output in a naïve way requires exponential time (but see Remark 1.2). The problem of simply computing the class number $h(F) = \#\operatorname{Cl}\mathbb{Z}_F$, or for that matter determining whether or not a given ideal of $\mathbb{Z}_F$ is principal, appears in general to be no easier than solving Problem (ClassUnitGroup).

In this article, we consider a noncommutative generalization of the above problem. We refer to §1 for precise definitions and specification of the input and output.

PROBLEM (ClassNumber($\mathcal{O}$)). *Given an Eichler order $\mathcal{O}$ in a quaternion algebra over a number field F, compute the class number $h(\mathcal{O})$.*

PROBLEM (ClassSet($\mathcal{O}$)). *Given an Eichler order $\mathcal{O}$ in a quaternion algebra over a number field F, compute a set of representatives for the set of invertible right $\mathcal{O}$-ideal classes $\operatorname{Cl}\mathcal{O}$.*

The main results of this article are embodied in the following two theorems, which provide algorithms to solve these two problems depending on whether the order is definite or indefinite.

THEOREM A.

(a) *If $\mathcal{O}$ is indefinite, Problem (ClassNumber($\mathcal{O}$)) is deterministic polynomial-time reducible to Problem (ClassUnitGroup($\mathbb{Z}_F$)).*

(b) *If $\mathcal{O}$ is definite, then Problem (ClassNumber($\mathcal{O}$)) is reducible in probabilistic time*

$$O\big(d_F^{3/2}\log^4 d_F + \log^2 \mathrm{N}\,\mathfrak{d}\big)$$

to the factorization of the discriminant $\mathfrak{d}$ of $\mathcal{O}$ and $O(2^n)$ instances of Problem (ClassUnitGroup) with fields having discriminant of size $O(d_F^{5/2})$.

Here and throughout the paper, unless otherwise noted the implied O-constants are absolute.

COROLLARY. *There exists a probabilistic polynomial-time algorithm to solve Problem (ClassNumber) over a fixed field F for indefinite orders and definite orders with factored discriminant.*

THEOREM B. *There exists an algorithm to solve Problem (ClassSet) for orders over a fixed field F. This algorithm runs in probabilistic polynomial time in the size of the output for indefinite orders and for definite orders with factored discriminant.*

It is important to note in Theorem B that we do not claim to be able to solve Problem (ClassSet) in probabilistic polynomial time in the size of the *input*, since the output is of exponential size and so even to write ideal representatives (in the usual way) requires exponential time.

The algorithmic results embodied in Theorems A and B have many applications. Quaternion algebras are the noncommutative analogues of quadratic field extensions and so present an interesting and rewarding class to analyze. For example, the norm form on a quaternion order gives rise to quadratic modules of rank 3 and 4 over $\mathbb{Z}_F$ and computing ideal classes amounts to finding all isometry classes of forms in the same genus (see e.g. Alsina-Bayer [1, Chapter 3] for the case $F = \mathbb{Q}$). Ideal classes in quaternion orders are also intimately related to automorphic forms. In the simplest case where $F = \mathbb{Q}$, the ideal classes of a maximal order in a quaternion algebra of discriminant p are in bijection with the set of supersingular elliptic curves in characteristic p. This correspondence has been exploited by Pizer [39], Kohel [29], and others to explicitly compute spaces of modular forms over $\mathbb{Q}$. By extension, one can compute with Hilbert modular forms over a totally real field F of even degree using these methods via the Jacquet-Langlands correspondence [14], and the algorithms described below have already been used for this purpose [15]. Finally, this work allows explicit computations with Shimura curves, including the computation of CM points [47].

The outline of this article is as follows. In Section 1, we review background material from the theory of Eichler orders of quaternion algebras and their ideals. In Section 2, we introduce the algorithmic problems we will consider and discuss some of their interrelationships. In Section 3, we treat the problem of computing the set of two-sided ideal classes and connecting ideals for Eichler orders. In Section 4, we enumerate ideal classes in indefinite orders; we deduce Theorem A and its corollary in this case from Eichler's theorem of norms. In Section 5, we introduce the Eichler mass formula which gives rise to an algorithm to count ideal classes in a definite quaternion order, completing the proof of Theorem A. In Section 6, we discuss ideal principalization in definite orders, rigorously analyzing the lattice search employed to find a generator, if it exists. In Section 7, we show how to enumerate ideal classes in definite orders, and use the Ramanujan property of the $\mathfrak{p}$-neighbors graph

to prove Theorem B. Finally, in Section 8, we use our implementation of these algorithms in Magma [4] to compute the complete list of definite quaternion orders (over an arbitrary totally real field F) with class number at most 2 (Tables 8.2–8.3): counted up to a natural notion of equivalence, there are exactly 74 equivalence classes of definite Eichler orders with class number 1 and 172 with class number 2.

We conclude this introduction by indicating two other results of significance found in the paper. In Section 5, we give a rigorous complexity analysis for computing the value $\zeta_F(-1)$ of the Dedekind zeta function of a totally real field F. We then prove a complexity result (Proposition 5.8) which serves as a partial converse to Theorem B: the problem of factoring integers a with $O(\log \log a)$ prime factors is probabilistic polynomial time reducible to Problem (ClassNumber) over $\mathbb{Q}$. In particular, if one can compute the class number of a definite rational quaternion order efficiently, then one can factor RSA moduli $a = pq$ efficiently.

1. Quaternion algebras, orders, and ideals

In this section, we introduce quaternion algebras and orders, and describe some of their basic properties; for further reading, see Reiner [41], Vignéras [44], and Brezeziński [5]. Throughout, let F be a number field of degree $[F : \mathbb{Q}] = n$ and absolute discriminant d_F, and let $\mathbb{Z}_F$ be its ring of integers.

Number rings. We follow the usual algorithmic conventions for number fields and finitely generated abelian groups (see Cohen [11], Lenstra [32]). In particular, following Lenstra [32, 2.5], to *compute* a finitely generated abelian group G means to specify a finite sequence $d_i \in \mathbb{Z}_{\geq 0}$ and an isomorphism $\bigoplus_i \mathbb{Z}/d_i\mathbb{Z} \xrightarrow{\sim} G$, in turn specified by the images of the standard generators. Moreover, we represent a finitely generated torsion-free $\mathbb{Z}_F$-module I by a *pseudobasis* over $\mathbb{Z}_F$, writing $I = \bigoplus_i \mathfrak{a}_i \gamma_i$ with $\mathfrak{a}_i$ fractional ideals of $\mathbb{Z}_F$ and $\gamma_i \in I$. See Cohen [12, Chapter 1] for methods of computing with finitely generated modules over Dedekind domains using pseudobases.

As in the introduction, we have the following basic problem.

Problem 1.1 (ClassUnitGroup($\mathbb{Z}_F$))**.** *Given $\mathbb{Z}_F$, compute the class group* $\mathrm{Cl}\,\mathbb{Z}_F$ *and unit group* $\mathbb{Z}_F^*$.

Remark 1.2. The representation of the output of Problem (ClassUnitGroup) is not unique, and therefore different algorithms may produce correct output but conceivably of arbitrarily large size. Indeed, we do not require that the outputted generators of the unit group $\mathbb{Z}_F^*$ to be represented in the usual way as a $\mathbb{Z}$-linear combination of an integral basis for $\mathbb{Z}_F$, since in general these elements can be of exponential size (as in the case of real quadratic fields). Instead, we allow the units to be represented as a straight-line program involving elements of $\mathbb{Z}_F$ written in the usual way, for example as a (finite) product $\prod u^{c(u)}$ of elements $u \in F^*$

with $c(u) \in \mathbb{Z}$. In this way, one may be able to write down a set of generators of subexponential size.

Proposition 1.3. *There exists an algorithm to solve Problem* (ClassUnitGroup) *which runs in time* $d_F^{1/2}(\log d_F)^{O(n)}$; *assuming the generalized Riemann hypothesis* (GRH) *and a "smoothness condition", this algorithm runs in time*

$$\exp\big(O((\log d_F)^{1/2}(\log \log d_F)^{1/2})\big),$$

where the implied constant depends on n.

The algorithm underlying Proposition 1.3 is due to Buchmann [7] (see therein for the "smoothness condition", which is known to hold for quadratic fields). See Lenstra [32, Theorem 5.5], Cohen-Diaz y Diaz-Olivier [13], and Cohen [11, Algorithm 6.5.9] for further detail, and also Schoof [42] for a detailed analysis from the perspective of Arakelov geometry.

Remark 1.4. A deterministic variant of the algorithm in Proposition 1.3 runs in time $d_F^{3/4}(\log d_F)^{O(n)}$, due to the need to factor polynomials over finite fields. We allow probabilistic algorithms in what follows.

Further, there exists an algorithm which, given the internal calculations involved in the class group computation of Proposition 1.3, determines whether or not an ideal $\mathfrak{a} \subset \mathbb{Z}_F$ is principal and, if so, outputs a generator (see Cohen [11, Algorithm 6.5.10]). No estimates on the running time of this algorithm have been proven, but it is reasonable to expect that they are no worse than the time for the class group computation itself. (See also Remark 6.2 below for an alternative approach, which gives a principalization algorithm which runs in deterministic polynomial time over a fixed totally real field F.)

Quaternion algebras. A *quaternion algebra* B over F is a central simple algebra of dimension 4 over F, or equivalently an F-algebra with generators $\alpha, \beta \in B$ such that

$$(1.1) \qquad\qquad \alpha^2 = a, \quad \beta^2 = b, \quad \alpha\beta = -\beta\alpha$$

with $a, b \in F^*$. Such an algebra is denoted $B = \left(\dfrac{a, b}{F}\right)$ and is specified in bits by the elements $a, b \in F^*$, and an element $\gamma = x + y\alpha + z\beta + w\alpha\beta \in B$ is specified by the elements $x, y, z, w \in F$.

Let B be a quaternion algebra over F. Then B has a unique (anti-)involution $^- : B \to B$ called *conjugation* such that $\gamma + \overline{\gamma}, \gamma\overline{\gamma} \in F$ for all $\gamma \in B$. We define the *reduced trace* and *reduced norm* of γ to be $\operatorname{trd}(\gamma) = \gamma + \overline{\gamma}$ and $\operatorname{nrd}(\gamma) = \gamma\overline{\gamma}$, respectively. For $B = \left(\dfrac{a, b}{F}\right)$ as in (1.1) we have

$$(1.2) \quad \overline{\gamma} = x - (y\alpha + z\beta + w\alpha\beta), \quad \operatorname{trd}(\gamma) = 2x, \quad \operatorname{nrd}(\gamma) = x^2 - ay^2 - bz^2 + abw^2.$$

Let K be a field containing F. Then $B_K = B \otimes_F K$ is a quaternion algebra over K, and we say K *splits* B if $B_K \cong M_2(K)$. If $[K : F] = 2$, then K splits B if and only if there exists an F-embedding $K \hookrightarrow B$.

Now let v be a place of F, and let F_v denote the completion of F at v. We say B is *split* at v if F_v splits B, and otherwise we say that B is *ramified* at v. The set of ramified places of B is of even (finite) cardinality and uniquely characterizes B up to F-algebra isomorphism. We define the *discriminant* $\mathfrak{D} = \operatorname{disc}(B)$ of B to

be the ideal of $\mathbb{Z}_F$ given by the product of all finite ramified places of B. One can compute the discriminant of B in probabilistic polynomial time given an algorithm for integer factorization [51].

We say that B is *totally definite* if F is totally real and every real infinite place of F is ramified in B; otherwise, we say that B is *indefinite* or that B *satisfies the Eichler condition*.

Quaternion orders. A $\mathbb{Z}_F$-*lattice* $I \subset B$ is a finitely generated $\mathbb{Z}_F$-submodule of B with $IF = B$. An *order* $\mathcal{O} \subset B$ is a $\mathbb{Z}_F$-lattice which is also a subring of B (hence $1 \in \mathcal{O}$), and an order is *maximal* if it is not properly contained in another order. We represent a $\mathbb{Z}_F$-lattice by a pseudobasis, as above. The problem of computing a maximal order $\mathcal{O}$ is probabilistic polynomial-time equivalent to integer factorization [46].

We will use the general principle throughout that $\mathbb{Z}_F$-lattices are determined by their localizations. For every prime ideal $\mathfrak{p}$ of $\mathbb{Z}_F$, let $\mathbb{Z}_{F,\mathfrak{p}}$ denote the completion of $\mathbb{Z}_F$ at $\mathfrak{p}$. For a $\mathbb{Z}_F$-lattice I, we abbreviate $I_\mathfrak{p} = I \otimes_{\mathbb{Z}_F} \mathbb{Z}_{F,\mathfrak{p}}$. Then for two $\mathbb{Z}_F$-lattices $I, J \subset B$, we have $I = J$ if and only if $I_\mathfrak{p} = J_\mathfrak{p}$ for all primes $\mathfrak{p}$.

For $\gamma_1, \ldots, \gamma_4 \in B$, we let $\mathrm{disc}(\gamma_1, \ldots, \gamma_4) = \det(\mathrm{trd}(\gamma_i \gamma_j))_{i,j=1,\ldots,4}$. For an order $\mathcal{O} \subset B$, the ideal of $\mathbb{Z}_F$ generated by the set

$$\{\mathrm{disc}(\gamma_1, \ldots, \gamma_4) : \gamma_i \in \mathcal{O}\}$$

is a square, and we define the *(reduced) discriminant* $\mathfrak{d} = \mathrm{disc}(\mathcal{O})$ of $\mathcal{O}$ to be the square root of this ideal. If $\mathcal{O} = \bigoplus_i \mathfrak{a}_i \gamma_i$ then we compute the discriminant as

$$\mathfrak{d}^2 = (\mathfrak{a}_1 \cdots \mathfrak{a}_4)^2 \, \mathrm{disc}(\gamma_1, \ldots, \gamma_4).$$

An order $\mathcal{O}$ is maximal if and only if $\mathfrak{d} = \mathfrak{D}$.

An *Eichler order* is the intersection of two maximal orders, and it is this class of orders which we will study throughout. The *level* of an Eichler order $\mathcal{O}$ is the ideal $\mathfrak{N} \subset \mathbb{Z}_F$ satisfying $\mathfrak{d} = \mathfrak{D}\mathfrak{N}$; the level $\mathfrak{N}$ is coprime to the discriminant $\mathfrak{D}$ of B. Alternatively, given a maximal order $\mathcal{O} \subset B$, an ideal $\mathfrak{N}$ coprime to $\mathfrak{D}$ and an embedding $\iota_\mathfrak{N} : \mathcal{O} \hookrightarrow M_2(\mathbb{Z}_{F,\mathfrak{N}})$ where $\mathbb{Z}_{F,\mathfrak{N}}$ denotes the completion of $\mathbb{Z}_F$ at $\mathfrak{N}$, an Eichler order of level $\mathfrak{N}$ is given by

$$(1.3) \qquad \mathcal{O}_0(\mathfrak{N}) = \{\gamma \in \mathcal{O} : \iota_\mathfrak{N}(\gamma) \text{ is upper triangular modulo } \mathfrak{N}\},$$

and all Eichler orders arise in this way up to conjugation. In particular [41, Theorem 39.14], an order $\mathcal{O}$ is hereditary (all one-sided ideals of $\mathcal{O}$ are projective) if and only if $\mathcal{O}$ is an Eichler order with squarefree level.

We can compute an explicit pseudobasis for an Eichler order $\mathcal{O}_0(\mathfrak{N})$ from the description (1.3) as follows. First, we compute a maximal order $\mathcal{O} \subset B$ as above. Next, for each prime power $\mathfrak{p}^e \, \| \, \mathfrak{N}$, we compute an embedding $\iota_\mathfrak{p} : \mathcal{O} \hookrightarrow M_2(\mathbb{Z}_{F,\mathfrak{p}})$; this can be accomplished in probabilistic polynomial time [51]. From $\iota_\mathfrak{p}$, one easily computes $\mathcal{O}_0(\mathfrak{p}^e)$ using linear algebra. Then $\mathcal{O}_0(\mathfrak{N}) = \bigcap_{\mathfrak{p}^e \| N} \mathcal{O}_0(\mathfrak{p}^e)$, and this intersection can be computed as $\mathbb{Z}_F$-lattices.

Two orders $\mathcal{O}, \mathcal{O}'$ are *conjugate* (also *isomorphic* or *of the same type*) if there exists $\nu \in B^*$ such that $\mathcal{O}' = \nu^{-1}\mathcal{O}\nu$, and we write $\mathcal{O} \cong \mathcal{O}'$.

Proposition 1.5 ([44, Corollaire III.5.5])**.** *The number of isomorphism classes of Eichler orders $\mathcal{O} \subset B$ of level $\mathfrak{N}$ is finite.*

Quaternion ideals. We define the *reduced norm* $\mathrm{nrd}(I)$ of a $\mathbb{Z}_F$-lattice I to be the fractional ideal of $\mathbb{Z}_F$ generated by the set $\{\mathrm{nrd}(\gamma) : \gamma \in I\}$.

Let I, J be $\mathbb{Z}_F$-lattices in B. We define the product IJ to be the $\mathbb{Z}_F$-submodule of B generated by the set $\{\alpha\beta : \alpha \in I,\ \beta \in J\}$; we have $\mathrm{nrd}(IJ) \supset \mathrm{nrd}(I)\,\mathrm{nrd}(J)$. We define the *left colon*

$$(I : J)_L = \{\gamma \in B : \gamma J \subset I\}$$

and similarly the *right colon*

$$(I : J)_R = \{\gamma \in B : J\gamma \subset I\}.$$

The colons $(I : J)_L, (I : J)_R$ and the product IJ are $\mathbb{Z}_F$-lattices. If $I = J$, then $(I : I)_L = \mathcal{O}_L(I)$ (resp. $(I : I)_R = \mathcal{O}_R(I)$) also has the structure of a ring, called the *left* (resp. *right*) *order* of the $\mathbb{Z}_F$-lattice I. One can compute the left and right colon in deterministic polynomial time using the Hermite normal form for $\mathbb{Z}_F$-lattices (see Friedrichs [22, §2.3]).

Let $\mathcal{O} \subset B$ be an order. A *right fractional $\mathcal{O}$-ideal* is a $\mathbb{Z}_F$-lattice I such that $\mathcal{O}_R(I) = \mathcal{O}$. In a similar fashion, we may define left fractional ideals; however, conjugation

$$I \mapsto \overline{I} = \{\overline{\gamma} : \gamma \in I\}$$

gives a bijection between the sets of right and left fractional $\mathcal{O}$-ideals, so when dealing with one-sided fractional ideals it suffices to work with right fractional ideals. If I (resp. J) is a right fractional $\mathcal{O}$-ideal then $\mathcal{O}_R((I : J)_R) \subset \mathcal{O}$ (resp. $\mathcal{O}_L((I : J)_R) \subset \mathcal{O}$). Note that any $\mathbb{Z}_F$-lattice I is by definition a right fractional $\mathcal{O}_R(I)$-ideal (and left fractional $\mathcal{O}_L(I)$-ideal).

A $\mathbb{Z}_F$-lattice I is *integral* if $I \subset \mathcal{O}_R(I)$, or equivalently if I is a right ideal of $\mathcal{O}_R(I)$ in the usual sense; for any $\mathbb{Z}_F$-lattice I, there exists a nonzero $d \in \mathbb{Z}_F$ such that dI is integral.

A $\mathbb{Z}_F$-lattice I is a left fractional $\mathcal{O}_L(I)$-ideal and a right fractional $\mathcal{O}_R(I)$-ideal, and we say that I is a fractional $\mathcal{O}_L(I), \mathcal{O}_R(I)$-ideal; if $\mathcal{O}_L(I) = \mathcal{O}_R(I) = \mathcal{O}$ we say that I is a *two-sided $\mathcal{O}$-ideal*.

A right fractional $\mathcal{O}$-ideal is *left invertible* if there exists a left fractional $\mathcal{O}$-ideal I^{-1} such that $I^{-1}I = \mathcal{O}$. If I is left invertible, then necessarily

$$I^{-1} = (\mathcal{O} : I)_L = \overline{I}/\mathrm{nrd}(I).$$

Equivalently, I is left invertible if and only if I is *locally principal*, i.e., for each (finite) prime ideal $\mathfrak{p}$ of $\mathbb{Z}_F$, the ideal $I_\mathfrak{p}$ is a principal right $\mathcal{O}_\mathfrak{p}$-ideal. It follows that if I is an $\mathcal{O}', \mathcal{O}$-ideal then I is left invertible if and only if I is right invertible (analogously defined), and so we simply say I is *invertible*, and then $II^{-1} = \mathcal{O}'$ and $I^{-1} = (\mathcal{O}' : I)_R$. If I is an invertible right fractional $\mathcal{O}$-ideal and J is an invertible left fractional $\mathcal{O}$-ideal then $(IJ)^{-1} = J^{-1}I^{-1}$ and $\mathrm{nrd}(IJ) = \mathrm{nrd}(I)\,\mathrm{nrd}(J)$, and moreover

$$\mathcal{O}_L(IJ) = \mathcal{O}_L(I) \text{ and } \mathcal{O}_R(IJ) = \mathcal{O}_R(J).$$

We note that for an order $\mathcal{O}$, every right fractional $\mathcal{O}$-ideal I is invertible if and only if $\mathcal{O}$ is hereditary.

Let I, J be invertible right fractional ideals. Then $(I : J)_R$ is a fractional $\mathcal{O}_R(J), \mathcal{O}_R(I)$-ideal and similarly $(I : J)_L$ is a fractional $\mathcal{O}_L(I), \mathcal{O}_L(J)$-ideal, and so we will also call $(I : J)_L$ (resp. $(I : J)_R$) the *left* (resp. *right*) *colon fractional ideal*.

Let I, J be invertible right fractional $\mathcal{O}$-ideals. We say that I and J are in the same *right ideal class*, and write $I \sim J$, if there exists an $\alpha \in B^*$ such that $I = \alpha J$. We have $I \sim J$ if and only if I and J are isomorphic as right $\mathcal{O}$-modules, and so in this case we also say that I and J are *isomorphic*. It is clear that $\sim$ defines an equivalence relation on the set of right fractional ideals of $\mathcal{O}$; we write $[I]$ for the ideal class of I. Since B is noncommutative, the ideal class $[IJ]$ of two right fractional $\mathcal{O}$-ideals I, J is in general not determined by the ideal classes $[I]$ and $[J]$, so the set of right ideal classes may not form a group. We denote the set of invertible right $\mathcal{O}$-ideal classes by $\mathrm{Cl}\,\mathcal{O}$.

The set of invertible two-sided fractional $\mathcal{O}$-ideals forms a group under multiplication, and the quotient of this group by the (normal) subgroup of principal two-sided fractional $\mathcal{O}$-ideals is called the *two-sided ideal class group* of $\mathcal{O}$; two invertible two-sided fractional $\mathcal{O}$-ideals I, J are in the same *ideal class* if they are equal in the two-sided ideal class group of $\mathcal{O}$, or equivalently if IJ^{-1} is a principal two-sided fractional $\mathcal{O}$-ideal.

An order $\mathcal{O}$ is *connected* to an order $\mathcal{O}'$ if there exists an invertible fractional $\mathcal{O}, \mathcal{O}'$-ideal I, the *connecting ideal*. The relation of being connected is an equivalence relation, and two Eichler orders $\mathcal{O}, \mathcal{O}'$ are connected if and only if they have the same level $\mathfrak{N}$.

Proposition 1.6 ([44, Théorème III.5.4], [41, §26])**.** *The set $\mathrm{Cl}\,\mathcal{O}$ is finite and $\#\,\mathrm{Cl}\,\mathcal{O}$ is independent of the choice of Eichler order $\mathcal{O}$ of a given level.*

We let $h(\mathcal{O}) = \#\,\mathrm{Cl}\,\mathcal{O}$ denote the *class number* of the Eichler order $\mathcal{O}$.

2. Algorithmic problems

In the remainder of this article, we will be concerned with a constellation of interrelated algorithmic problems which we now introduce.

Problem 2.1 (ClassNumber($\mathcal{O}$))**.** *Given an Eichler order $\mathcal{O}$, compute the class number $h(\mathcal{O})$.*

Problem 2.2 (ClassSet($\mathcal{O}$))**.** *Given an Eichler order $\mathcal{O}$, compute a set of representatives for the set of invertible right $\mathcal{O}$-ideal classes $\mathrm{Cl}\,\mathcal{O}$.*

Obviously, a solution to Problem 2.2 (ClassSet) gives a solution to Problem 2.1 (ClassNumber), but as we will see, this reduction is not the most efficient approach.

Given a set of representatives for $\mathrm{Cl}\,\mathcal{O}$ and a right fractional ideal I of $\mathcal{O}$, we may also like to determine its class $[I] \in \mathrm{Cl}\,\mathcal{O}$ and so we are led to the following problems.

Problem 2.3 (IsIsomorphic(I, J))**.** *Given two invertible right fractional ideals I, J of an Eichler order $\mathcal{O}$, determine if $I \sim J$; and, if so, compute $\xi \in B^*$ such that $I = \xi J$.*

Problem 2.4 (IsPrincipal(I))**.** *Given an invertible right fractional ideal I of an Eichler order $\mathcal{O}$, determine if I is principal; and, if so, compute a generator ξ of I.*

In fact, these two problems are computationally equivalent.

Lemma 2.5. *Problem* (IsIsomorphic) *is equivalent to Problem* (IsPrincipal)*.*

Proof. Let I, J be invertible right fractional $\mathcal{O}$-ideals. Then $I = \xi J$ for $\xi \in B^*$ if and only if the left colon ideal $(I : J)_L$ is generated by ξ as a right fractional $\mathcal{O}_L(J)$-ideal. Therefore, $I \sim J$ if and only if $(I : J)_L$ is a principal fractional right $\mathcal{O}_L(J)$-ideal. $\square$

We also have the corresponding problem for two-sided ideals.

Problem 2.6 (TwoSidedClassSet($\mathcal{O}$))**.** *Given an Eichler order $\mathcal{O}$, compute a set of representatives for the two-sided invertible ideal classes of $\mathcal{O}$.*

Finally, we consider algorithmic problems for orders.

Problem 2.7 (IsConjugate($\mathcal{O}, \mathcal{O}'$))**.** *Given two Eichler orders $\mathcal{O}, \mathcal{O}'$ of B, determine if $\mathcal{O} \cong \mathcal{O}'$; and, if so, compute $\nu \in B^*$ such that $\nu \mathcal{O} \nu^{-1} = \mathcal{O}'$.*

Problem 2.8 (ConjClassSet($\mathcal{O}$))**.** *Given an Eichler order $\mathcal{O}$ of level $\mathfrak{N}$, compute a set of representatives for the conjugacy classes of Eichler orders of level $\mathfrak{N}$.*

Problem 2.9 (ConnectingIdeal($\mathcal{O}, \mathcal{O}'$))**.** *Given Eichler orders $\mathcal{O}, \mathcal{O}'$, compute a connecting ideal I with $\mathcal{O}_R(I) = \mathcal{O}$ and $\mathcal{O}_L(I) = \mathcal{O}'$.*

We conclude by relating Problem 2.2 (ClassSet) to Problem 2.8 (ConjClassSet).

Proposition 2.10. *Let $\mathcal{O}_i$ be representatives of the isomorphism classes of Eichler orders of level $\mathfrak{N}$. For each i, let I_i be a connecting fractional $\mathcal{O}_i, \mathcal{O}$-ideal and let $J_{i,j}$ be representatives of the two-sided invertible fractional $\mathcal{O}_i$-ideal classes.*
  Then the set $\{J_{i,j} I_i\}_{i,j}$ is a complete set of representatives of $\mathrm{Cl}\,\mathcal{O}$.

Proof. Let I be an invertible right fractional $\mathcal{O}$-ideal. Then $\mathcal{O}_L(I) \cong \mathcal{O}_i$ for a uniquely determined i, so $\mathcal{O}_L(I) = \nu^{-1}\mathcal{O}_i\nu$ for some $\nu \in B^*$. But then $I_i = \nu K I$ where $K = \nu^{-1} I_i I^{-1}$ is a two-sided invertible fractional $\mathcal{O}_L(I)$-ideal, and so $I \sim KI_i \sim J_{i,j} I_i$ for some j, again uniquely determined. $\square$

It follows from Proposition 2.10 that if one can solve Problem 2.8 (ConjClassSet) then one can solve Problem 2.2 (ClassSet), given algorithms to solve Problem 2.9 (ConnectingIdeal) and Problem 2.6 (TwoSidedClassSet). We will discuss this further in §§3–4.

Conversely, if one can solve Problem 2.2 (ClassSet) then one can solve Problem 2.8 (ConjClassSet) given an algorithm to solve Problem 2.7 (IsConjugate): indeed, by Proposition 2.10, one obtains a set of representatives for the conjugacy classes of orders by computing $\mathcal{O}_L(I)$ for $[I] \in \mathrm{Cl}\,\mathcal{O}$. The difficulty of solving Problem 2.7 (IsConjugate) is discussed in §4 and §6.

3. Two-sided ideal classes and connecting ideals

In this section, we discuss Problem 2.6 (TwoSidedClassSet) and Problem 2.9 (ConnectingIdeal).

Two-sided ideal classes. Let $\mathcal{O} \subset B$ be an Eichler order of discriminant $\mathfrak{d}$ and level $\mathfrak{N}$. The two-sided ideals of $\mathcal{O}$ admit a local description, as follows. Let $F_{\mathfrak{p}}$ denote the completion of F at $\mathfrak{p}$, let $\mathbb{Z}_{F,\mathfrak{p}}$ denote its ring of integers, and let π be a uniformizer for $\mathbb{Z}_{F,\mathfrak{p}}$.

First, suppose that $B_{\mathfrak{p}} = B \otimes_F F_{\mathfrak{p}}$ is a division ring. Then the discrete valuation v of $\mathbb{Z}_{F,\mathfrak{p}}$ extends to $B_{\mathfrak{p}}$, and $\mathcal{O}_{\mathfrak{p}}$ is the unique maximal order of $B_{\mathfrak{p}}$. The fractional right $\mathcal{O}_{\mathfrak{p}}$-ideals form a cyclic group generated by the principal ideal

$$\mathrm{rad}(\mathcal{O}_{\mathfrak{p}}) = \{\gamma \in \mathcal{O}_{\mathfrak{p}} : v(\gamma) > 0\};$$

in particular, they are all two-sided [41, Theorem 13.2] and invertible. We have $\mathrm{rad}(\mathcal{O}_{\mathfrak{p}}) = [\mathcal{O}_{\mathfrak{p}}, \mathcal{O}_{\mathfrak{p}}]$, where $[\mathcal{O}_{\mathfrak{p}}, \mathcal{O}_{\mathfrak{p}}]$ denotes the two-sided $\mathcal{O}_{\mathfrak{p}}$-ideal generated by the set $\{\gamma\delta - \delta\gamma : \gamma, \delta \in \mathcal{O}_{\mathfrak{p}}\}$ (see Reiner [41, Theorem 14.5]).

Next, suppose that $B_{\mathfrak{p}} \cong M_2(F_{\mathfrak{p}})$ and that

$$(3.1) \qquad \mathcal{O}_{\mathfrak{p}} \cong \begin{pmatrix} \mathbb{Z}_{F,\mathfrak{p}} & \mathbb{Z}_{F,\mathfrak{p}} \\ \mathfrak{p}^e \mathbb{Z}_{F,\mathfrak{p}} & \mathbb{Z}_{F,\mathfrak{p}} \end{pmatrix} \subset M_2(\mathbb{Z}_{F,\mathfrak{p}}),$$

so that $\mathfrak{p}^e \parallel \mathfrak{N}$. Then the principal (equivalently, invertible) two-sided fractional ideals of $\mathcal{O}_{\mathfrak{p}}$ form an abelian group generated by $\pi\mathcal{O}_{\mathfrak{p}}$ and

$$\begin{pmatrix} 0 & 1 \\ \pi^e & 0 \end{pmatrix} \mathcal{O}_{\mathfrak{p}} = [\mathcal{O}_{\mathfrak{p}}, \mathcal{O}_{\mathfrak{p}}]$$

(see the proof given by Eichler [18, Satz 5] for $e = 1$, which applies *mutatis mutandis* for all e). Since $[\mathcal{O}_{\mathfrak{p}}, \mathcal{O}_{\mathfrak{p}}]^2 = \pi^e \mathcal{O}_{\mathfrak{p}}$, this group is cyclic if and only if e is odd or $e = 0$.

In particular, it follows from the preceding discussion that $[\mathcal{O}, \mathcal{O}]$ is an invertible two-sided $\mathcal{O}$-ideal, and we have the following description of the group of two-sided ideals.

Lemma 3.1. *The set of invertible fractional two-sided $\mathcal{O}$-ideals forms an abelian group generated by the set*

$$\{\mathfrak{p}\mathcal{O} : \mathfrak{p} \subset \mathbb{Z}_F\} \cup \{[\mathcal{O}, \mathcal{O}] + \mathfrak{p}^e\mathcal{O} : \mathfrak{p}^e \parallel \mathfrak{d}\}.$$

Proof. The group of invertible two-sided fractional $\mathcal{O}$-ideals is abelian since it is so locally by the above.

Let I be an invertible two-sided fractional $\mathcal{O}$-ideal. Clearing denominators, we may assume I is integral. Let M be an invertible maximal two-sided $\mathcal{O}$-ideal containing I. Then by maximality, there exists a unique prime ideal $\mathfrak{p}$ of $\mathbb{Z}_F$ such that $M_{\mathfrak{q}} = \mathcal{O}_{\mathfrak{q}}$ for all $\mathfrak{q} \neq \mathfrak{p}$. Thus by the preceding discussion, $M = \mathfrak{p}\mathcal{O}$ or $M = [\mathcal{O}, \mathcal{O}] + \mathfrak{p}^e\mathcal{O}$ with $\mathfrak{p}^e \parallel \mathfrak{d}$. Now IM^{-1} is again integral and $\mathrm{nrd}(IM^{-1}) = \mathrm{nrd}(I)/\mathrm{nrd}(M) \mid \mathrm{nrd}(I)$, so the result follows by induction. $\square$

For an alternative proof of Lemma 3.1 when $\mathcal{O}$ is hereditary, see Vigneras [44, Théorème I.4.5].

Proposition 3.2. *The group of invertible, two-sided fractional ideal classes of $\mathcal{O}$ is a finite abelian group generated by the classes of*

$$\{\mathfrak{a}\mathcal{O} : [\mathfrak{a}] \in \mathrm{Cl}(\mathbb{Z}_F)\} \cup \{[\mathcal{O}, \mathcal{O}] + \mathfrak{p}^e\mathcal{O} : \mathfrak{p}^e \parallel \mathfrak{d}\}.$$

If B is indefinite, one can omit all generators $[\mathcal{O}, \mathcal{O}] + \mathfrak{p}^e\mathcal{O}$ for which e is even.

Proof. Since the principal two-sided fractional $\mathcal{O}$-ideals form a subgroup, the first statement follows from the preceding lemma. For the second statement, we skip ahead and apply Proposition 4.1: if e is even, the ideals $\mathfrak{p}^{e/2}\mathcal{O}$ and $[\mathcal{O}, \mathcal{O}] + \mathfrak{p}^e\mathcal{O}$ have the same reduced norm $\mathfrak{p}^e$, so they are in the same ideal class if B is indefinite. $\square$

Corollary 3.3. *Problem* (TwoSidedClassSet($\mathcal{O}$)) *for an Eichler order $\mathcal{O}$ with factored discriminant $\mathfrak{d}$ is polynomial-time reducible to Problem* (ClassUnitGroup)($\mathbb{Z}_F$) *and $O(h(\mathbb{Z}_F)^2 \operatorname{N} \mathfrak{d}^2)$ instances of Problem* (IsIsomorphic).

Proof. Since $([\mathcal{O}, \mathcal{O}] + \mathfrak{p}^e \mathcal{O})^2 = \mathfrak{p}^e \mathcal{O}$ (as this is true locally), there are at most $2^{\omega(\mathfrak{d})} h(\mathbb{Z}_F)$ two-sided ideal classes, where $\omega(\mathfrak{d})$ denotes the number of prime factors of $\mathfrak{d}$. We have trivially $2^{\omega(\mathfrak{d})} \le \operatorname{N} \mathfrak{d}$, and the result follows. $\square$

Eichler orders and connecting ideals. We now exhibit an algorithm to test if an order is an Eichler order.

Algorithm 3.4. *Let $\mathcal{O} \subset B$ be an order of discriminant $\mathfrak{d} = \mathfrak{D}\mathfrak{N}$ with $\mathfrak{N}$ prime to the discriminant $\mathfrak{D}$ of B, and let $\iota_{\mathfrak{N}} : \mathcal{O} \hookrightarrow M_2(F_{\mathfrak{N}})$. This algorithm determines if $\mathcal{O}$ is an Eichler order, and if so, returns an element $\nu \in B$ such that $\iota_{\mathfrak{N}}(\nu^{-1} \mathcal{O} \nu) = \mathcal{O}_0(\mathfrak{N})$ (as in (1.3)).*

  (1) Compute $\mu \in B$ such that $\iota_{\mathfrak{N}}(\mu^{-1} \mathcal{O} \mu) \subset M_2(\mathbb{Z}_{F_{\mathfrak{N}}})$. Let $\iota'_{\mathfrak{N}} = \mu \iota_{\mathfrak{N}} \mu^{-1}$.
  (2) Factor the ideal $\mathfrak{N}$, and for each prime power $\mathfrak{p}^e \parallel \mathfrak{N}$:
      a. From the restriction $\iota'_{\mathfrak{p}} : \mathcal{O} \hookrightarrow M_2(F_{\mathfrak{p}})$ of $\iota'_{\mathfrak{N}}$, use linear algebra over $\mathbb{Z}_{F,\mathfrak{p}}$ to test if there is a common eigenvector $(x_{\mathfrak{p}}, z_{\mathfrak{p}}) \in (\mathbb{Z}_F/\mathfrak{p}^e)^2$ for the elements of a $\mathbb{Z}_{F,\mathfrak{p}}$-module basis of $\mathcal{O}_{\mathfrak{p}}$. If not, return false.
      b. Compute $y_{\mathfrak{p}}, w_{\mathfrak{p}}$ such that $N_{\mathfrak{p}} = \begin{pmatrix} x_{\mathfrak{p}} & y_{\mathfrak{p}} \\ z_{\mathfrak{p}} & w_{\mathfrak{p}} \end{pmatrix} \in GL_2(\mathbb{Z}_F/\mathfrak{p}^e)$.
  (3) By the Chinese remainder theorem, compute $\nu \in B$ such that $\iota_{\mathfrak{p}}(\nu_{\mathfrak{p}}) \equiv N_{\mathfrak{p}}$ (mod $\mathfrak{p}^e$). Return true and $\mu \nu$.

Proof of correctness. We refer to work of the second author [51] for more on Step 1.

For the rest of the algorithm, we note that the property of being an Eichler order is local: in particular, we see that a local order $\mathcal{O}_{\mathfrak{p}} = \mathcal{O} \otimes_{\mathbb{Z}_F} \mathbb{Z}_{F,\mathfrak{p}}$ with $\operatorname{disc}(\mathcal{O}_{\mathfrak{p}}) = \mathfrak{p}^e$ is Eichler if and only if there exists such a common eigenvector modulo $\mathfrak{p}^e$ of all $\gamma \in \mathcal{O}_{\mathfrak{p}}$. Conjugation by the matrix $N_{\mathfrak{p}}$ as in Step 2b then shows that $(1, 0)$ is an eigenvector modulo all such $\mathfrak{p}^e$, as desired. $\square$

Now let $\mathcal{O}, \mathcal{O}'$ be two Eichler orders in B having the same level $\mathfrak{N}$. We consider Problem 2.9 (ConnectingIdeal) and compute an invertible $\mathcal{O}', \mathcal{O}$-ideal I.

For any prime $\mathfrak{p} \nmid \mathfrak{N}$, by maximality the $\mathbb{Z}_{F,\mathfrak{p}}$-lattice $(\mathcal{O}'\mathcal{O})_{\mathfrak{p}}$ is a $\mathcal{O}'_{\mathfrak{p}}, \mathcal{O}_{\mathfrak{p}}$-ideal. So suppose $\mathfrak{p} \mid \mathfrak{N}$. Since any two Eichler orders of the same level are locally conjugate, there exists $\nu_{\mathfrak{p}} \in B_{\mathfrak{p}}$ such that $\mathcal{O}'_{\mathfrak{p}} = \nu_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}} \nu_{\mathfrak{p}}^{-1}$. The map $I \mapsto \nu_{\mathfrak{p}} I$ gives an equivalence between the category of fractional two-sided $\mathcal{O}_{\mathfrak{p}}$-ideals and the category of fractional $\mathcal{O}'_{\mathfrak{p}}, \mathcal{O}_{\mathfrak{p}}$-ideals.

From this analysis, we arrive at the following algorithm.

Algorithm 3.5. *Let $\mathcal{O}, \mathcal{O}' \subset B$ be Eichler orders of level $\mathfrak{N}$. This algorithm computes an invertible fractional $\mathcal{O}', \mathcal{O}$-ideal.*

  (1) Let ν, ν' be the output of Algorithm 3.4 for the orders $\mathcal{O}, \mathcal{O}'$ and a common choice of splitting $\iota_{\mathfrak{N}}$.
  (2) Compute a nonzero $d \in \mathbb{Z}_F$ such that $\mu := d\nu^{-1}\nu' \in \mathcal{O}'$ as follows: write $\nu^{-1}\nu'$ in terms of a $\mathbb{Z}_F$-pseudobasis for $\mathcal{O}'$, and compute a nonzero d as the least common multiple of the denominators of the coefficients of $\nu^{-1}\nu'$.
  (3) Compute $\operatorname{nrd}(\mu)\mathbb{Z}_F = \mathfrak{n}\mathfrak{a}$ with $\mathfrak{a}$ prime to $\mathfrak{N}$, and return the $\mathbb{Z}_F$-lattice $I := \mu\mathcal{O} + \mathfrak{n}\mathcal{O}'\mathcal{O}$.

Proof of correctness. In Step 1, we obtain from Algorithm 3.4 that for all $\mathfrak{p} \mid \mathfrak{N}$ we have $\mathcal{O}_\mathfrak{p} = \nu_\mathfrak{p} \mathcal{O}_0(\mathfrak{N})_\mathfrak{p} \nu_\mathfrak{p}^{-1}$ and $\mathcal{O}_\mathfrak{p} = \nu_\mathfrak{p}' \mathcal{O}_0(\mathfrak{N})_\mathfrak{p} \nu_\mathfrak{p}'^{-1}$. It is clear that Step 2 gives the correct output, and hence $\mathcal{O}_\mathfrak{p}' = \mu_\mathfrak{p} \mathcal{O}_\mathfrak{p} \mu_\mathfrak{p}^{-1}$ for all such $\mathfrak{p}$.

To conclude, we need to show that $\mathcal{O}_L(I) = \mathcal{O}'$ and $\mathcal{O}_R(I) = \mathcal{O}$. It suffices to check this locally. For any prime $\mathfrak{p} \nmid \mathfrak{N}$, we have $\mu_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}' = \mathfrak{n}_\mathfrak{p} \mathcal{O}_\mathfrak{p}'$, so $I_\mathfrak{p} = (\mathcal{O}'\mathcal{O})_\mathfrak{p}$, which is a fractional $\mathcal{O}_\mathfrak{p}', \mathcal{O}_\mathfrak{p}$-ideal by the above. For $\mathfrak{p} \mid \mathfrak{N}$, we have

$$\mathfrak{n}_\mathfrak{p} \mathcal{O}_\mathfrak{p}' = \mathcal{O}_\mathfrak{p}' \mathfrak{n}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}' \overline{\mu}_\mathfrak{p} \mu_\mathfrak{p} \subset \mathcal{O}_\mathfrak{p}' \mu_\mathfrak{p} = \mu_\mathfrak{p} \mathcal{O}_\mathfrak{p}$$

since $\overline{\mu}_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}'$. Hence $I_\mathfrak{p} = \mu_\mathfrak{p} \mathcal{O}_\mathfrak{p}$ and the result follows by the equivalence above, since $\mathcal{O}_\mathfrak{p}$ is a two-sided $\mathcal{O}_\mathfrak{p}$-ideal so $I_\mathfrak{p}$ is a fractional $\mathcal{O}_\mathfrak{p}', \mathcal{O}_\mathfrak{p}$-ideal.   □

Corollary 3.6. *Problem* (IsConjugate) *for two Eichler orders with factored discriminant* $\mathfrak{d}$ *is probabilistic polynomial-time reducible to Problems* (TwoSidedClassSet) *and* (IsIsomorphic)*.*

Proof. By Proposition 2.10, if I is an invertible right $\mathcal{O}$-ideal, then $\mathcal{O}_L(I)$ is conjugate to $\mathcal{O}$ if and only if I is equivalent to an invertible two-sided $\mathcal{O}$-ideal J: in fact, if $J = \nu I$ then $\mathcal{O} = \nu \mathcal{O}' \nu^{-1}$. Thus, to check whether two given Eichler orders $\mathcal{O}, \mathcal{O}'$ (of the same level) are conjugate, it suffices to construct a connecting ideal I as in Algorithm 3.5—which can be done in probabilistic polynomial time— and one can accordingly check for an isomorphism given a solution to Problem (TwoSidedClassSet) and (IsIsomorphic).   □

4. Ideal classes in indefinite orders

In this section, we discuss the difficulty of solving Problems 2.1 (ClassNumber) and 2.2 (ClassSet) in the indefinite case.

Let B be an indefinite quaternion algebra and let $\mathcal{O} \subset B$ be an Eichler order. Let S_∞ denote the set of ramified (real) infinite places of B and let $\mathrm{Cl}_{S_\infty} \mathbb{Z}_F$ denote the ray class group of $\mathbb{Z}_F$ with modulus S_∞. The quotient group $\mathrm{Cl}_{S_\infty} \mathbb{Z}_F / \mathrm{Cl}\,\mathbb{Z}_F$ is an elementary 2-group isomorphic to $\mathbb{Z}_{F,S_\infty}^* / \mathbb{Z}_F^{*2}$ where

$$\mathbb{Z}_{F,S_\infty}^* = \{u \in \mathbb{Z}_F^* : v(u) > 0 \text{ for all } v \in S_\infty\}.$$

Proposition 4.1 (Eichler's theorem)**.** *If B is indefinite and $\mathcal{O} \subset B$ is an Eichler order, then the reduced norm map*

$$\mathrm{nrd} : \mathrm{Cl}\,\mathcal{O} \to \mathrm{Cl}_{S_\infty} \mathbb{Z}_F$$

is a bijection (of sets).

For a proof of this proposition, see Reiner [41, Corollary 34.21] or Vignéras [44, Théorème III.5.7]. We have the following immediate corollary, which proves Theorem A in the indefinite case; we restate it here for convenience.

Corollary 4.2. *If B is indefinite, then Problem* (ClassNumber$(\mathcal{O})$) *is reducible in deterministic polynomial time to Problem* (ClassUnitGroup$(\mathbb{Z}_F)$)*.*

In other words, there exists an algorithm to solve Problem (ClassNumber) which, given an algorithm to solve Problem (ClassUnitGroup), runs in deterministic polynomial time in its output size. (See Remark 1.2.)

Proof. We compute $h(\mathcal{O}) = \#(\mathbb{Z}_{F,S_\infty}^* / \mathbb{Z}_F^{*2}) h(\mathbb{Z}_F)$. Given the class group $\mathrm{Cl}\,\mathbb{Z}_F$, its order $h(\mathbb{Z}_F) = \#\,\mathrm{Cl}\,\mathbb{Z}_F$ can be computed in polynomial time. Similarly, given generators for the unit group $\mathbb{Z}_F^*$, one can compute in deterministic polynomial

time (in the size of their representation) their signs for each real place v, and using linear algebra over $\mathbb{F}_2$ determine the 2-rank of the group $\mathbb{Z}_{F,S_\infty}^*/\mathbb{Z}_F^{*2}$. $\qquad\square$

It follows immediately from Corollary 4.2 that for Eichler orders over a fixed number field F, Problem 2.1 (ClassNumber) can be solved in time $O(1)$, which proves the corollary to Theorem A.

Next, we discuss Theorem B in the indefinite case. First, we exhibit an auxiliary algorithm for computing ideals with given norm, which works for both definite and indefinite quaternion orders.

Algorithm 4.3. *Let $\mathcal{O}$ be an Eichler order and let $\mathfrak{a} \subset \mathbb{Z}_F$ be an ideal which is coprime to $\mathfrak{D}$. This algorithm returns an invertible right $\mathcal{O}$-ideal I such that $\mathrm{nrd}(I) = \mathfrak{a}$.*

(1) Factor $\mathfrak{a}$ into prime ideals.
(2) For each $\mathfrak{p}^e \parallel \mathfrak{a}$, find a zero of the quadratic form $\mathrm{nrd}(\alpha_\mathfrak{p}) \equiv 0 \pmod{\mathfrak{p}}$, and choose a random lift of $\alpha_\mathfrak{p}$ modulo $\mathfrak{p}^2$ so that $\mathrm{nrd}(\alpha_\mathfrak{p})$ is a uniformizer at $\mathfrak{p}$. Let $\beta_\mathfrak{p} = \alpha_\mathfrak{p}^e$.
(3) Use the Chinese remainder theorem to find $\beta \in \mathbb{Z}_F$ such that $\beta \equiv \beta_\mathfrak{p}$ $\pmod{\mathfrak{p}^e}$ for all $\mathfrak{p}^e \parallel \mathfrak{a}$. Return the right $\mathcal{O}$-ideal $\beta\mathcal{O} + \mathfrak{a}\mathcal{O}$.

From Eichler's theorem (Proposition 4.1), we then have the following straightforward algorithm.

Algorithm 4.4. *Let $\mathcal{O}$ be an indefinite Eichler order. This algorithm solves Problem 2.2 (ClassSet).*

(1) For each $\mathfrak{a}$ in a set of representatives for $\mathrm{Cl}_{S_\infty} \mathbb{Z}_F / 2\,\mathrm{Cl}_{S_\infty} \mathbb{Z}_F$, compute using Algorithm 4.3 an ideal $I_\mathfrak{a}$ of norm $\mathfrak{a}$.
(2) Return the set $\{\mathfrak{c}I_\mathfrak{a}\}_{\mathfrak{a},\mathfrak{c}}$, with $\mathfrak{c}^2$ in a set of representatives of $2\,\mathrm{Cl}_{S_\infty} \mathbb{Z}_F$.

Proposition 4.5. *Problem 2.2 (ClassSet) for indefinite orders over a fixed field F can be solved in probabilistic polynomial time.*

Proof. One can solve Problem (ClassUnitGroup) for the field F in constant time and one can further factor the generating ideals $\mathfrak{a}$ which are given as output. The statement follows by noting that Step 2 of Algorithm 4.3 can be performed in probabilistic polynomial time [51] by extracting square roots modulo $\mathfrak{p}$. $\qquad\square$

Proposition 4.5 thus proves the indefinite case of Theorem B.

Remark 4.6. In practice, in Algorithm 4.4 one may wish to find representatives of $\mathrm{Cl}\,\mathcal{O}$ with the smallest norm possible; one can then simply find small representatives $\mathfrak{a}$ for each ideal class of $\mathrm{Cl}_{S_\infty} \mathbb{Z}_F$ (using the LLL algorithm [33], part of the algorithms used in the algorithm described in Proposition 1.3) and then repeat Step 1 for each such ideal $\mathfrak{a}$.

To solve Problem 2.8 (ConjClassSet) for Eichler orders, we amend Algorithm 4.4 as follows.

Algorithm 4.7. *Let $\mathcal{O} \subset B$ be an indefinite Eichler order of discriminant $\mathfrak{d}$. This algorithm solves Problem 2.8 (ConjClassSet).*

(1) Let H be the subgroup of $\mathrm{Cl}_{S_\infty} \mathbb{Z}_F$ generated by $2\,\mathrm{Cl}\,\mathbb{Z}_F$ and $[\mathfrak{p}^e]$ for all $\mathfrak{p}^e \parallel \mathfrak{d}$ with e odd.

(2) For each $\mathfrak{a}$ in a set of representatives for $\mathrm{Cl}_{S_\infty} \mathbb{Z}_F / H$, let $\alpha \in \mathcal{O}$ be such that $\mathrm{nrd}(\alpha)$ is a uniformizer of $\mathfrak{a}$ and let $I_\mathfrak{a} := \alpha\mathcal{O} + \mathfrak{a}\mathcal{O}$.

(3) Return the set $\{\mathcal{O}_L(I_\mathfrak{a})\}_\mathfrak{a}$.

Proof of correctness. By Proposition 3.2, the image of the reduced norm of the set of two-sided ideal classes maps is exactly H. It then follows from Proposition 2.10 that one recovers all conjugacy classes of Eichler orders of level $\mathfrak{N}$ as $\mathcal{O}_L(I_\mathfrak{a})$ for the right $\mathcal{O}$-ideals $I_\mathfrak{a}$ with $\mathfrak{a}$ as in Step 2. $\square$

Finally, we are left with Problem 2.4 (IsPrincipal). Let I be a right fractional $\mathcal{O}$-ideal. Again, by Eichler's theorem (Proposition 4.1), we see that I is principal if and only if $\mathrm{nrd}(I) \subset \mathbb{Z}_F$ is trivial in $\mathrm{Cl}_{S_\infty} \mathbb{Z}_F$, and the latter can be tested as in §2. In other words, simply testing if a right $\mathcal{O}$-ideal is principal is no harder than testing if an ideal is principal in $\mathbb{Z}_F$.

To then actually exhibit a generator for a principal ideal, we rely upon the following standard lemma (see Pizer [39, Proposition 1.18]).

Lemma 4.8. *Let I be a right invertible fractional $\mathcal{O}$-ideal. Then $\gamma \in I$ generates I if and only if $\mathrm{nrd}(\gamma)\mathbb{Z}_F = \mathrm{nrd}(I)$.*

By Lemma 4.8, the right ideal I is principal if and only if there exists $\gamma \in I$ such $\mathrm{nrd}(\gamma) = \mathrm{nrd}(I) = c\mathbb{Z}_F$ (with $v(c) > 0$ for all $v \in S_\infty$). Unfortunately, since B is indefinite, the norm form $\mathrm{Tr}\,\mathrm{nrd} : B \to \mathbb{Q}$ is not positive definite, hence it does not induce the structure of a (definite) lattice on I (in the definite case it will, see §§6–7). One option is to use a form of indefinite lattice reduction (as in Ivanyos-Szántó [24]). We instead find a substitute quadratic form which will still allow us to find "small" elements. When F is totally real and B has a unique split real place, such a form has been found [50], and inspired by this result we make the following definitions.

Let $B = \left(\dfrac{a,b}{F}\right)$. For an infinite place v of F and $\gamma = x + y\alpha + z\beta + w\alpha\beta$, define

$$(4.1) \qquad Q_v(\gamma) = |v(x)|^2 + |v(a)||v(y)|^2 + |v(b)||v(z)|^2 + |v(ab)||v(w)|^2.$$

We then define the *absolute reduced norm* by

$$Q : B \to \mathbb{R}$$
$$\gamma \mapsto \sum_v Q_v(\gamma);$$

by construction, the form Q is positive definite and gives I the structure of a definite $\mathbb{Z}$-lattice of rank $4[F : \mathbb{Q}]$.

Remark 4.9. The form Q is clearly only one of many choices for such a positive definite form, and so one may reasonably try to understand what the cone of such forms corresponds to.

When F is totally real and B has a unique split real place, the choice of the positive definite quadratic form corresponds to the choice of a center p for a Dirichlet fundamental domain in the upper half-plane $\mathfrak{H}$ and at the split place measures the *inverse radius* of the corresponding isometric circle [50]. The same is true for a quaternion algebra of arbitrary signature as follows. If B has g split real places and s (split) complex places, then the group $\mathcal{O}_1^*$ of units of $\mathcal{O}$ of reduced norm 1 embeds in $SL_2(\mathbb{R})^g \times SL_2(\mathbb{C})^s$ and acts on $\mathfrak{H}^g \times (H^3)^s$ discretely, where $\mathfrak{H}$ (resp. H^3) denotes the upper half-plane (resp. hyperbolic 3-space) (see e.g. Beardon [3] and Elstrodt,

et al. [20]). In this case, the choice of a positive definite quadratic form corresponds again to the choice of a center p for a Dirichlet domain and at each place measures an inverse radius, either of an isometric circle or sphere. The above choice of form Q corresponds to a (normalized) choice of center $p = (i, \ldots, i, j, \ldots, j)$.

Because of the connection with the classical theory of positive definite quadratic forms on a real quadratic field, which can be understood more generally from the perspective of Arakelov theory [42], we view these observations as the beginning of a form of noncommutative Arakelov theory and leave it as a subject for further investigation.

We then have the following algorithm.

Algorithm 4.10. *Let $I \subset \mathcal{O}$ be a right fractional $\mathcal{O}$-ideal. This algorithm solves Problem* 2.4 (IsPrincipal).

(1) Compute $\mathrm{nrd}(I) \subset \mathbb{Z}_F$ and test if $\mathrm{nrd}(I)$ is principal; if not, then return false. Otherwise, let $\mathrm{nrd}(I) = c\mathbb{Z}_F$.

(2) Determine if there exists a unit $u \in \mathbb{Z}_F^*$ such that $v(uc) > 0$ for all ramified (real) places v; if not, then return false. Otherwise, let $c := uc$ and initialize $\alpha := 1$.

(3) If $c \in \mathbb{Z}_F^*$, return α. Otherwise, view I as a $\mathbb{Z}$-lattice equipped with the quadratic form Q. Reduce I using the LLL algorithm [33]. By enumerating short elements in I, find $\gamma \in I$ such that $\mathrm{nrd}(\gamma) = cd$ with $\mathrm{N}(d) < \mathrm{N}(c)$. Let $\alpha := \gamma\alpha/d$, let $I := d\gamma^{-1}I$, and let $c := d$, and return to Step 2.

Proof. In Step 2, we have $\mathrm{nrd}(d\gamma^{-1}I) = d^2/(cd)\,\mathrm{nrd}(I) = d\mathbb{Z}_F$, and so the algorithm terminates since in each step $\mathrm{N}\,\mathrm{nrd}(I) \in \mathbb{Z}_{>0}$ decreases. The algorithm gives correct output since $d\gamma^{-1}I = \alpha\mathcal{O}$ if and only if $I = (\gamma\alpha/d)\mathcal{O}$. □

In practice, Algorithm 4.10 runs quite efficiently and substantially improves upon a more naïve enumeration. However, we are unable to prove any rigorous time bounds for Algorithm 4.10. Already the first step of the algorithm requires the computation of the class group $\mathrm{Cl}\,\mathbb{Z}_F$; and even if we suppose that the class group has been precomputed, there do not appear to be rigorous time bounds for the principal ideal testing algorithm [11, Algorithm 6.5.10] (see §1). With that proviso, given the generator c as in Step 1, we can measure the value of the LLL-step as follows.

Lemma 4.11. *There exists $C(\mathcal{O}) \in \mathbb{R}_{>0}$, depending on $\mathcal{O}$, such that for every principal fractional ideal I of $\mathcal{O}$, the first basis element γ in the LLL-reduced basis of Algorithm* 4.10 *satisfies*

$$|\,\mathrm{N}(\mathrm{nrd}(\gamma))| \leq C(\mathcal{O})\,\mathrm{N}(\mathrm{nrd}(I)).$$

Proof. Suppose that $I = \xi\mathcal{O}$. The F-endomorphism of B given by left multiplication by ξ has determinant $\mathrm{nrd}(\xi)^2$, and it follows that the corresponding $\mathbb{Q}$-endomorphism of $L \otimes_{\mathbb{Z}} \mathbb{Q}$ has determinant $\mathrm{N}(\mathrm{nrd}(\xi))^2$. Hence

$$\det(I) = \det(\xi\mathcal{O}) = \mathrm{N}(\mathrm{nrd}(\xi))^4 \det(\mathcal{O}).$$

Now, for any $\gamma = x + y\alpha + z\beta + w\alpha\beta$, from (4.1) we have

$$|v(\mathrm{nrd}(\gamma))| \leq Q_v(\gamma) \leq Q(\gamma)$$

for all places v. Thus, the output of the LLL algorithm [33, Proposition 1.9] yields $\gamma \in I$ which satisfies

$$|v(\mathrm{nrd}(\gamma))| \leq Q(\gamma) \leq 2^{(4n-1)/4} \det(I)^{1/(4n)} = 2^{(4n-1)/4} \det(\mathcal{O})^{1/(4n)} \mathrm{N}(\mathrm{nrd}(I))^{1/n}.$$

We conclude that

$$|\mathrm{N}(\mathrm{nrd}(\gamma))| = \prod_v |v(\mathrm{nrd}(\gamma))| \leq 2^{(4n^2-n)/4} \det(\mathcal{O})^{1/4} \mathrm{N}(\mathrm{nrd}(I))$$

as claimed. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

From Lemma 4.8, we conclude that the algorithm produces elements which are close to being generators.

5. COMPUTING THE CLASS NUMBER FOR DEFINITE ORDERS

In this section, we discuss the difficulty of solving Problem 2.1 (ClassNumber) in the definite case. Throughout this section, let B denote a totally definite quaternion algebra of discriminant $\mathfrak{D}$. Here, the class number is governed by the Eichler mass formula.

Given an ideal $\mathfrak{N}$ (coprime to $\mathfrak{D}$), the *mass* is defined to be the function

$$(5.1) \qquad\qquad M(\mathfrak{D}, \mathfrak{N}) = 2^{1-n} |\zeta_F(-1)| h(\mathbb{Z}_F) \Phi(\mathfrak{D}) \Psi(\mathfrak{N})$$

where

$$(5.2) \qquad \Phi(\mathfrak{D}) = \prod_{\mathfrak{p} | \mathfrak{D}} (\mathrm{N}(\mathfrak{p}) - 1) \quad \text{and} \quad \Psi(\mathfrak{N}) = \mathrm{N}(\mathfrak{N}) \prod_{\mathfrak{p} | \mathfrak{N}} \left(1 + \frac{1}{\mathrm{N}(\mathfrak{p})} \right).$$

The mass of an Eichler order $\mathcal{O} \subset B$ of level $\mathfrak{N}$ is defined to be $M(\mathcal{O}) = M(\mathfrak{D}, \mathfrak{N})$.

The class number of an Eichler order differs from its mass by a correction factor coming from torsion, as follows. An *embedded elliptic subgroup* in B is an embedding $\mu_q \hookrightarrow \mathcal{O}^*/\mathbb{Z}_F^*$, where $q \in \mathbb{Z}_{\geq 2}$ and $\mathcal{O}$ is an Eichler order, such that the image is a maximal (cyclic) subgroup of $\mathcal{O}^*/\mathbb{Z}_F^*$; the *level* of the embedding is the level of $\mathcal{O}$. An *elliptic cycle* is a B^*-conjugacy class of embedded elliptic subgroups. Let $e_q(\mathfrak{D}, \mathfrak{N})$ denote the number of elliptic cycles of B^* of order q and level $\mathfrak{N}$.

Proposition 5.1 (Eichler mass formula [44, Corollaire V.2.5]). *Let $\mathcal{O} \subset B$ be an Eichler order of level $\mathfrak{N}$. Then*

$$h(\mathcal{O}) = M(\mathfrak{D}, \mathfrak{N}) + \sum_q e_q(\mathfrak{D}, \mathfrak{N}) \left(1 - \frac{1}{q} \right).$$

Remark 5.2. A variant of the Eichler mass formula [44, Corollaire V.2.3] which is also useful for algorithmic purposes (see Remark 7.5) reads

$$M(\mathfrak{D}, \mathfrak{N}) = \sum_{[I] \in \mathrm{Cl}\, \mathcal{O}} \frac{1}{[\mathcal{O}_L(I)^* : \mathbb{Z}_F^*]}.$$

We first characterize the embedding numbers $e_q(\mathfrak{D}, \mathfrak{N})$. Given an embedded elliptic subgroup $\mu_q \hookrightarrow \mathcal{O}^*/\mathbb{Z}_F^*$ of level $\mathfrak{N}$, the image of μ_q generates a quadratic subring $R \subset \mathcal{O}$; such an embedding $R \hookrightarrow \mathcal{O}$ with $RF \cap \mathcal{O} = R$ is said to be an *optimal embedding*. Conversely, to every optimal embedding $\iota : R \hookrightarrow \mathcal{O}$, where R is a quadratic $\mathbb{Z}_F$-order with $[R^* : \mathbb{Z}_F^*] = q$ and $\mathcal{O}$ is an Eichler order of level $\mathfrak{N}$, we have the embedded elliptic subgroup $R_{\mathrm{tors}}^*/\mathbb{Z}_F^* \cong \mu_q \hookrightarrow \mathcal{O}^*$. This yields a bijection

$$\{\text{Elliptic cycles of } B^* \text{ of order } q \text{ and level } \mathfrak{N}\}$$
$$\updownarrow$$
$$\left\{ \begin{array}{c} B^*\text{-conjugacy classes of optimal embeddings } \iota : R \hookrightarrow \mathcal{O} \\ \text{with } [R^* : \mathbb{Z}_F^*] = q \text{ and } \mathcal{O} \text{ an Eichler order of level } \mathfrak{N} \end{array} \right\}.$$

The quadratic $\mathbb{Z}_F$-orders R with $[R^* : \mathbb{Z}_F^*] = q$ come in two types. Either we have $R^*_{\text{tors}} \cong \mu_{2q}$ and we say R is *fully elliptic*, or $[R^* : \mathbb{Z}_F^* R^*_{\text{tors}}] = 2$ and we say R is *half elliptic*. We see that if R is half elliptic then in particular $R \subset \mathbb{Z}_F[\sqrt{-\epsilon}]$ for ϵ a totally positive unit of $\mathbb{Z}_F$.

The (global) embedding numbers $e_q(\mathfrak{D}, \mathfrak{N})$ can then be computed by comparison to the local embedding numbers

$$m(R_\mathfrak{p}, \mathcal{O}_\mathfrak{p}) = \#\{\mathcal{O}_\mathfrak{p}^*\text{-conjugacy classes of optimal embeddings } \iota : R_\mathfrak{p} \hookrightarrow \mathcal{O}_\mathfrak{p}\}$$

where $\mathcal{O}_\mathfrak{p}$ is a $\mathfrak{p}$-local Eichler order of level $\mathfrak{N}$.

Lemma 5.3 ([44, p. 143]). *We have*

$$e_q(\mathfrak{D}, \mathfrak{N}) = \frac{1}{2} \sum_{[R^*:\mathbb{Z}_F^*]=q} h(R) \prod_\mathfrak{p} m(R_\mathfrak{p}, \mathcal{O}_\mathfrak{p}).$$

There are formulas [49, §2] for the number of local embeddings $m(R_\mathfrak{p}, \mathcal{O}_\mathfrak{p})$, for example:

$$(5.3) \qquad m(R_\mathfrak{p}, \mathcal{O}_\mathfrak{p}) = \begin{cases} 1, & \text{if } \mathfrak{p} \nmid \mathfrak{D}\mathfrak{N}; \\ 1 - \left(\dfrac{K_q}{\mathfrak{p}} \right), & \text{if } \mathfrak{p} \mid \mathfrak{D} \text{ and } \mathfrak{p} \nmid \mathfrak{f}(R); \\ 1 + \left(\dfrac{K_q}{\mathfrak{p}} \right), & \text{if } \mathfrak{p} \parallel \mathfrak{N}; \end{cases}$$

here, we let $K_q = F(\zeta_{2q})$ and $\mathfrak{f}(R)$ denotes the conductor of R (in $\mathbb{Z}_{K_q}$). In particular, we have by Equation (5.3) that $m(R_\mathfrak{p}, \mathcal{O}_\mathfrak{p}) = 1$ for almost all $\mathfrak{p}$.

We now discuss the computability of the terms in the formula of Proposition 5.1. To compute the mass, we will use the following proposition.

Proposition 5.4. *The value* $\zeta_F(-1) \in \mathbb{Q}$ *can be computed using* $O\big(d_F^{3/2} \log^4 d_F\big)$ *bit operations.*

Proof. From the functional equation for the Dedekind zeta function, we have

$$(5.4) \qquad \zeta_F(-1) = \left(\frac{-1}{2\pi^2} \right)^n d_F^{3/2} \zeta_F(2).$$

From (5.1) and Proposition 5.1, we have $\zeta_F(-1) \in \mathbb{Q}$, in fact, $\zeta_F(-1)$ has denominator bounded by Q, the least common multiple of all $q \in \mathbb{Z}_{\geq 2}$ such that $[F(\zeta_{2q}) : F] = 2$.

We compute an approximation to $\zeta_F(-1)$ from the Euler product expansion for $\zeta_F(2)$, as follows (see also Buchmann-Williams [8, §2], or Dokchitser [17] for a more general approach). For $P \in \mathbb{Z}_{\geq 2}$, let

$$\zeta_{F, \leq P}(s) = \prod_{\text{N}\,\mathfrak{p} \leq P} \left(1 - \frac{1}{\text{N}\,\mathfrak{p}^s} \right)^{-1}$$

denote the truncated Euler product for $\zeta_F(s)$, where we take the product over all primes $\mathfrak{p}$ of $\mathbb{Z}_F$ for which $N\mathfrak{p} \leq P$. Note that for $s > 1$ real we have

$$\zeta_{F,\leq P}(s) \leq \zeta_F(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{N\mathfrak{p}^s}\right)^{-1} \leq \prod_p \left(1 - \frac{1}{p^s}\right)^{-n} = \zeta(s)^n.$$

Now we estimate

$$0 < \frac{\zeta_F(2)}{\zeta_{F,\leq P}(2)} - 1 = \prod_{N\mathfrak{p} > P} \left(1 - \frac{1}{N\mathfrak{p}^2}\right)^{-1} - 1$$

$$= \sum_{N\mathfrak{p} > P} \frac{1}{N\mathfrak{p}^2} + \sum_{N\mathfrak{p} \geq N\mathfrak{q} > P} \frac{1}{N(\mathfrak{p}\mathfrak{q})^2} + \cdots$$

$$\leq \sum_{p > P} \frac{n}{p^2} + \sum_{p,q > P} \frac{n^2}{(pq)^2} + \cdots \leq \sum_{x > P} \frac{n}{x^2} + \sum_{x > P^2} \frac{n^2}{x^2} + \cdots$$

$$\leq \frac{n}{P} + \frac{n^2}{P^2} + \cdots = \frac{1}{(P/n) - 1}.$$

It follows that $\zeta_F(2) - \zeta_{F,\leq P}(2) < \epsilon$ whenever $P > n(1 + \zeta_{F,\leq P}(2)/\epsilon)$ which is satisfied when

$$P > n\left(1 + \frac{\zeta(2)^n}{\epsilon}\right) = n\left(1 + \frac{(\pi^2/6)^n}{\epsilon}\right).$$

To obtain the value $\zeta_F(-1)$ within an interval of length smaller than $1/(2Q)$, from (5.4) it suffices to take

$$\epsilon = \frac{1}{2Q} \frac{(2\pi^2)^n}{d_F^{3/2}}.$$

To estimate Q, we note that if $[F(\zeta_{2q}) : F] = 2$ then in particular F contains the totally real subfield $\mathbb{Q}(\zeta_{2q})^+$ of $\mathbb{Q}(\zeta_{2q})$, hence $\phi(q)/2 \mid n$. Since the fields $\mathbb{Q}(\zeta_{2q})^+$ are linearly disjoint for q a power of a prime, we have $Q = O(n)$. (We note this bound is best possible in terms of n, since after all we may take $F = \mathbb{Q}(\zeta_{2q})^+$.) Putting these together, we need to evaluate the truncated Euler product with

$$P = O\left(n\left(\frac{\pi^2}{6}\right)^n \frac{1}{\epsilon}\right) = O\left(\frac{n^2}{12^n} d_F^{3/2}\right).$$

Evaluating $\zeta_{F,\leq P}(2)$ amounts to factoring a degree n polynomial over $\mathbb{F}_p$ for all primes $p \leq P$; each such factorization can be performed using a repeated squaring operation, requiring $O(n^3 \log p)$ operations in $\mathbb{F}_p$ (see e.g. the survey by von zur Gathen and Panario [23]) so time $O(n^3 \log^3 p)$, hence altogether time $O(n^3 P \log^2 P)$ by the prime number theorem, so the computation requires

$$O\left(\frac{n^5}{12^n} d_F^{3/2} \log^3 d_F\right) = O(d_F^{3/2} \log^3 d_F)$$

operations with real numbers of precision $O(1/\epsilon) = O(d_F^{3/2})$, requiring therefore $O(d_F^{3/2} \log^4 d_F)$ bit operations. $\qquad\square$

Remark 5.5. If F is an abelian field, then $\zeta_F(-1)$ can be computed much more efficiently in terms of Bernoulli numbers [52].

Putting these pieces together, we now prove the following theorem.

Theorem 5.6. *There exists a probabilistic algorithm which, given an Eichler order $\mathcal{O}$ in a definite quaternion algebra B with factored discriminant $\mathfrak{d}$, solves Problem* (ClassNumber) *in time*

$$O\big(d_F^{3/2}\log^4 d_F + \log^2 \mathrm{N}\,\mathfrak{d}\big)$$

and the time to solve $O(2^n)$ instances of Problem (ClassUnitGroup) *with fields of discriminant of size $O(d_F^{5/2})$.*

Proof. First, we compute the factored discriminant $\mathfrak{D}$ of B and level $\mathfrak{N}$ of $\mathcal{O}$ by computing Hilbert symbols [51]: given the factorization of the discriminant $\mathfrak{d}$ of $\mathcal{O}$, for each $\mathfrak{p} \mid \mathfrak{d}$ one can determine whether $\mathfrak{p} \mid \mathfrak{D}$ or $\mathfrak{p} \mid \mathfrak{N}$ in deterministic time $O(\log^2 \mathrm{N}\,\mathfrak{p})$.

We compute $h(\mathcal{O})$ from the Eichler mass formula (Proposition 5.1), with the mass $M(\mathfrak{D}, \mathfrak{N})$ given as in Equation (5.1). Given the factorization of $\mathfrak{D}$ and $\mathfrak{N}$, we can compute $\Phi(\mathfrak{D})$ and $\Psi(\mathfrak{N})$ in time $O(\log^2 \mathrm{N}(\mathfrak{D}\mathfrak{N}))$. One recovers $h(\mathbb{Z}_F)$ from the given algorithm to solve Problem (ClassUnitGroup). By Proposition 5.4, we can compute $|\zeta_F(-1)|$ in time $O(d_F^{3/2}\log^4 d_F)$.

We now estimate the time to compute the correction term $\sum_q e_q(\mathfrak{D}, \mathfrak{N})(1 - 1/q)$ in Lemma 5.3, up to further instances of Problem (ClassUnitGroup).

As in the proof of Proposition 5.4, if $e_q(\mathfrak{D}, \mathfrak{N}) \neq 0$ then $q = O(n)$. Thus, by factoring n (which can be done in negligible time using trial division) we obtain a finite set of $O(n)$ possible values of q. For each such q, we can factor the qth cyclotomic polynomial over F in deterministic time $(qn\log d_F)^{O(1)}$ (see Lenstra [31]) and determine if each of its irreducible factors has degree 2. (In practice, one might further restrict the set of possible q by verifying that $q \mid d_F$ if $q \geq 5$ and that for sufficiently many small prime ideals $\mathfrak{p}$ of $\mathbb{Z}_F$ coprime to qd_F that $q \mid (\mathrm{N}\mathfrak{p}^2 - 1)$, but this makes no difference in the analysis of the runtime.) Since $q = O(n)$ and $n = O(\log d_F)$ by the Odlyzko bounds [38], this becomes simply $(\log d_F)^{O(1)}$.

We pause to compute an estimate of discriminants. Let $q \in \mathbb{Z}_{\geq 2}$ be such that $K = F(\zeta_{2q})$ is quadratic over F. We estimate the discriminant $d_K = d_F^2\,\mathrm{N}_{F/\mathbb{Q}}\,\mathfrak{d}_{K/F}$. Let $\lambda_{2q} = \zeta_{2q} + 1/\zeta_{2q}$; then we have $\mathbb{Q}(\zeta_{2q})^+ = \mathbb{Q}(\lambda_{2q})$ and $\zeta_{2q}^2 - \lambda_{2q}\zeta_{2q} + 1 = 0$, so $\mathfrak{d}_{K/F} \mid (\lambda_{2q}^2 - 4)\mathbb{Z}_F$. Therefore

$$\mathrm{N}_{\mathbb{Q}(\zeta_{2q})^+/\mathbb{Q}}(\lambda_{2q}^2 - 4) = \mathrm{N}_{\mathbb{Q}(\zeta_{2q})^+/\mathbb{Q}}(\zeta_{2q} - 1/\zeta_{2q})^2 = \mathrm{N}_{\mathbb{Q}(\zeta_{2q})/\mathbb{Q}}(\zeta_q - 1)$$

$$= \begin{cases} p, & \text{if } q = p^r \text{ is an odd prime power;} \\ 4, & \text{if } q = 2^r; \\ 1, & \text{otherwise.} \end{cases}$$

So $d_K = d_F^2\,\mathrm{N}_{F/\mathbb{Q}}\,\mathfrak{d}_{K/F} \leq d_F^2\,\mathrm{N}_{F/\mathbb{Q}}(\lambda_{2q}^2 - 4) = d_F^2 p^{2n/\phi(2q)}$ if $q = p^r$ is an odd prime power, and similarly $d_K \leq d_F^2 4^{2n/\phi(2q)}$ if $q = 2^r$ and $d_K = d_F^2$ if q is not a power of a prime. For q a power of a prime p, by the conductor-discriminant formula [52, Theorem 3.11] we have $p^{\phi(2q)/2-1} \mid d_{\mathbb{Q}(\zeta_{2q})^+}$, so since $d_{\mathbb{Q}(\zeta_{2q})^+}^{2n/\phi(2q)} \mid d_F$ we have $p^n = O(d_F)$. Thus we have $p^{2n/\phi(2q)} = O(d_F^{2/\phi(2q)}) = O(d_F^{1/2})$ when $q = 5$ or $q \geq 7$, and hence $d_K = O(d_F^{5/2})$; but for $q \leq 4$ this also holds, since by the Odlyzko bounds there are only finitely many (totally real) number fields with $d_F \leq 16^n$. When $K = F(\sqrt{-\epsilon})$ for ϵ a totally positive unit of $\mathbb{Z}_F$, we have $d_K = O(d_F^2 4^n) = O(d_F^{5/2})$ as well. Thus in all cases, $d_K = O(d_F^{5/2})$.

To compute $e_q(\mathfrak{D}, \mathfrak{N})$, we need to compute $h(R)$ for all $R \subset K$ with $[R^* : \mathbb{Z}_F^*] = q$. First, suppose that R is fully elliptic. Then $\mathbb{Z}_F[\zeta_{2q}] \subset R \subset \mathbb{Z}_K$. We have the bound $\mathfrak{f}(R)^2 \mid (\lambda_{2q}^2 - 4) \mid p$ on the conductor of R as above, which implies there are at most $O(2^{n/\phi(2q)}) = O(d_F)$ such orders, corresponding to the possible products of ramified primes over p in the extension $F/\mathbb{Q}(\zeta_{2q})^+$. Each can be constructed by computing $\mathfrak{p}$-overorders for $\mathfrak{p}^2 \mid (\lambda_{2q}^2 - 4) \mid p$, requiring time $q^{O(1)}$. Now if $\mathfrak{f} = \mathfrak{f}(R)$, we have

$$h(R) = \frac{h(\mathbb{Z}_{K_q})}{[\mathbb{Z}_{K_q}^* : R^*]} \frac{\#(\mathbb{Z}_K/\mathfrak{f}\mathbb{Z}_K)^*}{\#(\mathbb{Z}_F/\mathfrak{f}\mathbb{Z}_F)^*}$$

and the time required to compute these terms is negligible except for $h(\mathbb{Z}_{K_q})$, for which we may call our hypothesized algorithm.

Next, suppose that R is half elliptic. In this case, we have $\mathbb{Z}_F[\sqrt{-\epsilon}] \subset R \subset \mathbb{Z}_K$. Here, we have the bound $\mathfrak{f}(R)^2 \mid 4$, hence there are at most $O(2^n) = O(d_F)$ such orders, and the arguments in the preceding paragraph apply.

In all, we have at most $O(2^n)$ imaginary quadratic fields K to consider, the worst case being when F has a fundamental system of units which are totally positive.

Finally, the calculation of the local embedding number $m(R_\mathfrak{p}, \mathcal{O}_\mathfrak{p})$ can be accomplished in time $O(\log^2(N\mathfrak{p}))$ for $\mathfrak{p}$ odd [49, Proposition 2.5] by computing a Legendre symbol (and in time $O(1)$ after that) and in time $n^{O(1)} = (\log d_F)^{O(1)}$ for $\mathfrak{p}$ even [49, Remark 2.6].

In all, aside from the time to compute class numbers, since there are $O(n)$ values of q, we can compute the correction term in time

$$O(\log^2 N(\mathfrak{D}\mathfrak{N})) + d_F(\log d_F)^{O(1)} + (\log d_F)^{O(1)}.$$

Combining this estimate with the time to compute the mass, the result follows. $\square$

Corollary 5.7. *For a fixed number field F, Problem 2.1 (ClassNumber) for definite orders $\mathcal{O}$ is probabilistic polynomial-time reducible to the factorization of the discriminant of $\mathcal{O}$.*

Proof. Only the quantities $\Phi(\mathfrak{D})$, $\Psi(\mathfrak{N})$, and $m(R_\mathfrak{p}, \mathcal{O}_\mathfrak{p})$ depend on $\mathcal{O}$—the others can be precomputed for fixed F. These quantities can be computed in probabilistic polynomial time knowing the factorization of $\mathfrak{D}$ and $\mathfrak{N}$. $\square$

Putting together Corollary 4.2, Theorem 5.6, and Corollary 5.7, we have proven the main Theorem A and its corollary.

We conclude this section by discussing the role of factoring the ideals $\mathfrak{D}, \mathfrak{N}$. It is well known that factoring ideals in the ring $\mathbb{Z}_F$ is probabilistic polynomial-time equivalent to factoring integers. But already for imaginary quadratic fields, it is also well known that an algorithm for (ClassUnitGroup) can be employed to factor integers (two such "class group" methods are attributed to Schnorr-Lenstra-Shanks-Pollard-Atkin-Rickert and Schnorr-Seysen-Lenstra-Lenstra-Pomerance). A noncommutative analogue of this result, already in the simplest case where $F = \mathbb{Q}$, is the following.

Proposition 5.8. *The problem of factoring integers a with $\omega(a) = O(\log \log a)$ prime factors is probabilistic polynomial-time reducible to Problem (ClassNumber) for definite quaternion algebras over $\mathbb{Q}$.*

Proof. For $F = \mathbb{Q}$, the class number is given simply by

$$h(\mathcal{O}) = \frac{1}{12}\phi(D)\psi(N) + \frac{e_2(D, N)}{2} + \frac{e_3(D, N)}{3}.$$

Let $a \in \mathbb{Z}_{>0}$ be an integer to be factored, which we may assume has $\gcd(a, 26) = 1$ and is not a prime power.

We consider quaternion algebras of the form $B = \left(\dfrac{-ac, -13b}{\mathbb{Q}} \right)$ where $b, c \in \mathbb{Z}_{>0}$ are chosen as follows. We choose $c \in \{1, 2\}$ so that $(-ac/13) = -1$: therefore the algebra B is ramified at 13 so $13 \mid D$, and it follows that $e_2(D, N) = e_3(D, N) = 0$ by (5.3), hence

$$h(\mathcal{O}) = \phi(D/13)\psi(N).$$

For simplicity, we assume $c = 1$; the same argument applies when $c = 2$.

We choose b to be a random squarefree factored positive integer modulo $4a$ (see e.g. Bach [2]) with $\gcd(b, 26) = 1$. If $\gcd(a, b) \neq 1$ and $a \neq 1, b$, we have factored a. Otherwise, with probability at least $(1/2)^{\omega(a)}$, we have $(-13b/p) = 1$ for all $p \mid a$, so then $p \nmid D$ for all $p \mid a$; since $\omega(a) = O(\log \log a)$ by assumption, after $O(\log a)$ attempts this condition will be satisfied with probability at least $1/2$.

Now compute an order $\mathcal{O} \subset B$ which is locally generated by the standard generators α, β for all primes $p \neq 2$ and which is maximal at 2. Then $\mathcal{O}$ is an order with discriminant $13ab\epsilon = DN$ where $\epsilon = 1$ or 2. We claim that $\mathcal{O}$ is Eichler. Since $\gcd(a, b) = 1$ and b is squarefree, and further a, b are odd, it suffices to show that $\mathcal{O}$ is Eichler at $p \mid a$. But for such $p^e \parallel a$, by assumption we have $(-13b/p) = 1$ so B is unramified at p, and there exists $t \in \mathbb{Z}_p^*$ such that $t^2 = -13b$. Then the embedding $\mathcal{O} \hookrightarrow \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ by

$$\alpha \mapsto \begin{pmatrix} 0 & 1 \\ ac & 0 \end{pmatrix}, \quad \beta \mapsto \begin{pmatrix} t & 0 \\ 0 & -t \end{pmatrix}$$

realizes $\mathcal{O}$ as an Eichler order of level p^e.

It follows that

$$h(\mathcal{O}) = \prod_{p \mid (D/13)} (p - 1) \prod_{p^e \parallel N} p^{e-1}(p + 1);$$

if a is not squarefree then $\gcd(h(\mathcal{O}), a)$ yields a prime factor of a, so we may assume that a is squarefree.

We now show how to recover a prime factor of a given the values $h(\mathcal{O})$. For each prime $p \mid b$, by computing $(-ac/p)$ we can determine if p is ramified in B or not, accordingly contributing a factor $p - 1$ or $p + 1$ to $h(\mathcal{O})$. Dividing $h(\mathcal{O})$ by these factors, we may compute the integer

$$g(b) = \prod_{p \mid D'} (p - 1) \prod_{p \mid N'} (p + 1)$$

and $\epsilon a = D'N'$. We compute one such value $g(b)$ and then many more values $g(b')$, and we claim that $\gcd(g(b) + g(b'), a)$ will find a factor of a. Indeed, with probability at least $\omega(a)(1/2)^{\omega(a)+1}$, we will have the following:

> There exists a prime $q \mid a$ for which $(-13b/q) = -(-13b'/q)$ and $(-13b/p) = (-13b'/p)$ for all $p \mid \epsilon a$ with $p \neq q$.

It follows then that $g(b) \equiv -g(b') \pmod q$ as claimed. Again, since by assumption $\omega(a) = O(\log \log a)$, after $O(\log a)$ attempts we will factor a with probability at least $1/2$. $\qquad\square$

6. Ideal principalization for definite orders

In this section, we discuss the totally definite case of Problem 2.4 (IsPrincipal), which by Lemma 2.5 is equivalent to Problem 2.3 (IsIsomorphic). We exhibit an algorithm (Algorithm 6.3) to solve this problem and analyze its running time (Proposition 6.9). This algorithm will be used in the next section to solve Problem 2.2 (ClassSet) for definite orders. Throughout this section, let B be a totally definite quaternion algebra over a totally real field F of discriminant $\mathfrak{D}$ and let $\mathcal{O} \subset B$ be an Eichler order of level $\mathfrak{N}$.

Our algorithm is similar to the indefinite case (Algorithm 4.10), where now we are in the easier situation that $\mathrm{Tr\,nrd} : B \to \mathbb{Q}$ is a positive definite quadratic form on the $\mathbb{Q}$-vector space B. We prove below that we can reduce the principalization problem to a shortest lattice vector problem (based initially on an idea due to Dembélé and Donnelly [15, §2.2].)

First of all, if I is a principal right fractional $\mathcal{O}$-ideal, then $\mathrm{nrd}\,I = c\mathbb{Z}_F$ is a principal ideal of $\mathbb{Z}_F$. To compute such a generator $c \in \mathbb{Z}_F$ over a general number field F, we refer to the discussion following Proposition 1.3. For F totally real as in this section, we first show that a principal ideal has a generator of polynomial size, with the constant depending on F. For a real place v of F, corresponding to an embedding $v : F \hookrightarrow \mathbb{R}$, we abbreviate $a_v = v(a)$ for $a \in F$.

Lemma 6.1. *For a principal fractional ideal $\mathfrak{a} \subset F$, there exists a generator a for $\mathfrak{a}$ with $|a_v| = O((\mathrm{N}\,\mathfrak{a})^{1/n})$ for all real places v of F, where the implied constant is effectively computable and depends on the field F.*

Proof. Consider the (Minkowksi unit) map

$$\sigma : F \to \mathbb{R}^n$$
$$u \mapsto (\log |u_v| - (1/n) \log \mathrm{N}(u))_v$$

where v runs over the real places of F. The image $\sigma(F)$ is contained in the hyperplane $H : \sum_v x_v = 0$, and the image of the units $\sigma(\mathbb{Z}_F^*)$ forms a lattice (of full rank $n-1$) in H. But since $\mathfrak{a}$ is principal, the image $\sigma(\mathfrak{a}) \subset H$ is simply a translate of this lattice. It follows that there is a generator a for $\mathfrak{a}$ with $\sigma(a)$ inside a fundamental parallelopiped for $\sigma(\mathbb{Z}_F^*)$. Therefore, if $u_1, \ldots, u_{n-1} \in \mathbb{Z}_F^*$ are a basis for $\mathbb{Z}_F^*/\{\pm 1\}$, then for each real place v we have

$$\left| \log |a_v| - \frac{1}{n} \log \mathrm{N}(a) \right| \leq \frac{1}{2} \sum_{i=1}^{n-1} |\log |u_{i,v}||.$$

Let $U_v = \prod_{i=1}^{n-1} e^{|\log |u_{i,v}||/2}$. Then

$$\frac{1}{U_v} \mathrm{N}(\mathfrak{a})^{1/n} \leq |a_v| \leq U_v \mathrm{N}(\mathfrak{a})^{1/n}$$

so if $U = \max U_v$ then

$$\frac{1}{U_F} \mathrm{N}(\mathfrak{a})^{1/n} \leq |a_v| \leq U \mathrm{N}(\mathfrak{a})^{1/n}$$

for all v, as claimed. $\qquad\square$

Remark 6.2. Although we will not make use of it, we remark that Lemma 6.1 gives a method for testing if an ideal $\mathfrak{a}$ is principal over $\mathbb{Z}_F$ and, if so, exhibiting a generator. We simply enumerate all elements $a \in \mathbb{Z}_F$ with $|a_v| \leq U \operatorname{N}(\mathfrak{a})^{1/n}$ for all v, where U is as in the above proof; we can accomplish this by embedding $\mathbb{Z}_F \hookrightarrow \mathbb{R}^n$ by $a \mapsto (a_v)_v$ as a lattice (by the Minkowski embedding) and enumerating all lattice elements of (square) norm bounded by $nU^2 \operatorname{N}(\mathfrak{a})^{2/n}$. By the analysis of Fincke and Pohst [21, (2.12), (3.1)] (or alternatively Elkies [19, Lemma 1]), we can enumerate all such elements in time $O(\operatorname{N}(\mathfrak{a}))$, where the implied constant depends only on F.

We now present the main algorithm in this section.

Algorithm 6.3. *Let $I \subset \mathcal{O}$ be a right fractional $\mathcal{O}$-ideal and let $c \in \mathbb{Z}_F$ such that* $\operatorname{nrd} I = c\mathbb{Z}_F$. *This algorithm solves Problem* 2.4 (IsPrincipal)*.*

    (1) Determine if there exists a unit $u \in \mathbb{Z}_F^*$ such that $c_v u_v > 0$ for all real places v; if not, then return false.
    (2) For each totally positive unit $z \in \mathbb{Z}_{F,+}^* / \mathbb{Z}_F^{*2}$:
        a. Let ξ be a shortest vector of the $\mathbb{Z}$-lattice I with respect to the rational quadratic form $\varphi_{(ucz)^{-1}}$.
        b. If $\varphi_{(ucz)^{-1}}(\xi) = [F : \mathbb{Q}]$ then return true and the element ξ.
    (3) Return false.

Remark 6.4. Note that if $F = \mathbb{Q}$ then in Step 2 we have $z = u = 1$. Hence the algorithm simply amounts to find a shortest vector in the $\mathbb{Z}$-lattice I (with respect to the reduced norm form).

Proof of correctness. If I is principal, then $\operatorname{nrd} I$ is generated by a totally positive element uc where $u \in \mathbb{Z}_F^*$. Then Lemma 4.8 implies that $\xi \in I$ generates I if and only if $\operatorname{nrd} \xi = ucz$ for some $z \in \mathbb{Z}_{F,+}^*$. To find such an element ξ, we only need to search for elements of norm ucz where z runs through some arbitrary transversal of $\mathbb{Z}_{F,+}^* / \mathbb{Z}_F^{*2}$.

Let $n = [F : \mathbb{Q}]$, $z \in \mathbb{Z}_{F,+}^*$, and $\xi \in I$. Then $\operatorname{nrd} \xi \in \operatorname{nrd} I = (ucz)\mathbb{Z}_F$, so $\alpha = (\operatorname{nrd} y)/(ucz) \in \mathbb{Z}_F$. The arithmetic-geometric mean inequality implies

$$n \leq n(\operatorname{N}\alpha)^{1/n} \leq \operatorname{Tr}\alpha = \varphi_{(ucz)^{-1}}(\xi).$$

Moreover, equality holds if and only if $1 = \operatorname{N}\alpha$ and α_v is independent of the real place v of F, so equality holds if and only if $\alpha = 1$. Hence $\operatorname{nrd}(\xi) = ucz$ if and only if $\xi \in I$ satisfies $\varphi_{(ucz)^{-1}}(y) = n$ and is a shortest vector. $\qquad\square$

To analyze the runtime of Algorithm 6.3, we first state and prove some preliminary results on enumeration of (short) vectors in lattices.

Lemma 6.5. *There exists an algorithm which, given a lattice L with basis vectors each of (square) norm at most $A \in \mathbb{R}_{>0}$, finds the shortest vectors in L in deterministic time $O(\log^3 A)$ for fixed dimension n.*

Proof. This lemma is a consequence of the celebrated LLL-algorithm of Lenstra, Lenstra, and Lovász [33]: see e.g. Kannan [26, Section 3]. $\qquad\square$

Remark 6.6. Using floating-point LLL, one could probably replace $\log^3 A$ with $\log^2 A$ in the lemma above, but this will have no impact on what follows so we neglect this possible improvement.

We pause to prove two results which will be used in the next section.

Lemma 6.7. *A uniformly random element of a lattice L with norm $\leq A$ can be computed in probabilistic probabilistic time (where the implied constant depends on the lattice L).*

Proof. Choose a random vector $v \in \mathbb{Z}^n$ with each component v_i chosen uniformly in the range $[-\sqrt{A}, \sqrt{A}]$. Using linear algebra over $\mathbb{Q}$, determine if $v \in L$; if so, output the vector, otherwise start again. This test can be performed by first computing once (for the lattice L) the change of basis from L to the standard basis and then multiplying the vector v by this matrix. The entries of the inverse will be of polynomial size for fixed dimension, and so each test can be performed in polynomial time. The probability of success in each trial depends on the density of the lattice, given by its determinant. $\square$

We apply this lemma to computing representatives of ideal classes, which we will use in the proof of Lemma 7.8.

Lemma 6.8. *There exists an algorithm which, given $x \in \mathbb{Z}_{>0}$ sufficiently large and an ideal class $[\mathfrak{a}] \in \mathrm{Cl}_{S_\infty}(\mathbb{Z}_F)$, computes a uniformly random ideal $\mathfrak{b} \subset \mathbb{Z}_F$ with $[\mathfrak{b}] = [\mathfrak{a}]$ and $\mathrm{N}\,\mathfrak{b} \leq x$, which runs in probabilistic polynomial time over a fixed totally real field F.*

Proof. Let $\mathfrak{b} \subset \mathbb{Z}_F$ be an ideal such that $N\mathfrak{b} \leq x$ and $[\mathfrak{b}] = [\mathfrak{a}]$. Then $\mathfrak{b}\mathfrak{a}^{-1}$ is principal. By Lemma 6.1, there exists a generator a for $\mathfrak{b}\mathfrak{a}^{-1}$ with

$$|a_v| \leq U \, \mathrm{N}(\mathfrak{b}\mathfrak{a}^{-1}) \leq Ux/\,\mathrm{N}\,\mathfrak{a} = T$$

for all real places v of F, where U is an effectively computable constant depending only on F. In particular, we have that

$$\{\mathfrak{b} : \mathrm{N}\,\mathfrak{b} \leq x, [\mathfrak{b}] = [\mathfrak{a}]\} \subset \{a\mathfrak{a}^{-1} : a \in \mathbb{Z}_F, |a_v| \leq T\}.$$

Now each fractional ideal of F is naturally a lattice under the Minkowski embedding $\sigma : F \to \mathbb{R}^n$ by $x \mapsto (x_v)_v$. Denote by $\mathrm{SV}(L)$ the set of shortest vectors in a lattice L. Then the map

$$\{a \in \mathbb{Z}_F : |a_v| \leq T \text{ for all } v \text{ and } a \in \mathrm{SV}(a\mathbb{Z}_F)\} \to \{\mathfrak{b} : \mathrm{N}\,\mathfrak{b} \leq x \text{ and } [\mathfrak{b}] = [\mathfrak{a}]\}$$

$$a \mapsto \mathfrak{b} = a\mathfrak{a}^{-1}$$

is a surjective map of finite sets. If we draw an element $a \in \mathbb{Z}_F$ on the left-hand side with probability $1/\#\,\mathrm{SV}(a\mathbb{Z}_F)$ and an ideal $\mathfrak{b}$ on the right-hand side uniformly, then this map preserves probabilities.

Therefore, we may compute a uniformly random ideal $\mathfrak{b}$ as follows. First, we compute a uniformly random element $a \in \mathfrak{a}^{-1}$ such that $\mathrm{N}(a) \leq x/\mathrm{N}\,\mathfrak{a}$ and let $\mathfrak{b} = a\mathfrak{a}$. We find such an element a by finding a uniformly random element $a \in \mathfrak{a}^{-1}$ of (square) norm $\leq nT^2$ in the Minkowski embedding, which can be done in probabilistic polynomial time by Lemma 6.7. If $\mathrm{N}\,a > T$, we return and compute another random a. Given a with $\mathrm{N}\,a \leq T$, we compute the shortest vectors in the lattice $a\mathbb{Z}_F$, which can be done in deterministic polynomial time by Lemma 6.5 (since a is of polynomial size, the lattice $a\mathbb{Z}_F$ has a basis which is of polynomial size with the constant depending on the size of a basis for $\mathbb{Z}_F$). If a is not a shortest vector, we return and compute another element a; if a is a shortest vector, then we keep a with probability $1/\#\,\mathrm{SV}(a\mathbb{Z}_F)$ and otherwise return. $\square$

We conclude this section by analyzing the runtime of the principalization algorithm.

Proposition 6.9. *Algorithm* 6.3 *runs in deterministic polynomial time in the size of the input over a fixed totally real field F.*

Proof. In Step 1, we must solve Problem (ClassUnitGroup) for the field F which can be done in constant time. In Step 2, we note that $\log C$ is of polynomial size in the input, with the constant depending only on F. In Step 3, there are at most 2^{n-1} totally positive units z. For each, in Step 3(a) the $\mathbb{Z}$-lattice aI has basis vectors with norm of polynomial size in the input pseudobasis for I, with the constant depending on F. In Step 3(b) we find the shortest vectors in this lattice, and by Lemma 6.5 this can be performed in deterministic polynomial time in fixed dimension.   □

Remark 6.10. We now present an alternative approach to Corollary 3.6 which solves Problem 2.7 (IsConjugate) for a definite algebra by constructing an isomorphism directly. Let

$$O(B) = \{\varphi \in \mathrm{End}_F(B) : \mathrm{nrd}(\varphi(x)) = \mathrm{nrd}(x) \text{ for all } x \in B\}$$

where $\mathrm{End}_F(B)$ denotes the endomorphisms of B as an F-vector space, and

$$SO(B) = \{\varphi \in O(B) : \det(\varphi) = 1\}.$$

It is well known (see e.g. Dieudonné [16, Appendix IV, Proposition 3]) that

$$SO(B) = \{\phi : x \mapsto \nu\delta x\delta^{-1} : \nu, \delta \in B^*, \ \mathrm{nrd}(\nu) = 1\}.$$

Since conjugation is an order-preserving anti-automorphism of determinant -1, we have the following result: Two orders $\mathcal{O}$ and $\mathcal{O}'$ of B are conjugate if and only if there exists $\varphi \in O(B)$ such that $\varphi(\mathcal{O}) = \mathcal{O}'$.

Therefore, such an isometry can be found using the approach described by Plesken and Souvignier [40].

Remark 6.11. For a definite quaternion order $\mathcal{O}$, we define its *theta series* simply to be the theta series of the corresponding lattice under the quadratic form $\mathrm{Tr}\,\mathrm{nrd}$, i.e.,

$$\theta(\mathcal{O}; q) = \sum_{\xi \in \mathcal{O}} q^{\mathrm{Tr}\,\mathrm{nrd}(\xi)} \in \mathbb{Z}[[q]].$$

Isomorphic quaternion orders have the same theta series, and so given a complete set of representatives $\{\mathcal{O}_i\}$ for the set of conjugacy classes of (definite) Eichler orders of a given level, one can identify the conjugacy class of a given order $\mathcal{O}$ by comparing the first few coefficients of their theta series. This approach is more efficient in practice to show that two orders are not conjugate than to test for conjugacy directly.

In this way, one can also show that two right ideals of an order $\mathcal{O}$ are not isomorphic, by showing that their left orders are not conjugate, and this idea can be used in practice to speed up the enumeration of ideal classes.

7. Computing the class set for definite orders

In this section, we discuss Problem 2.2 (ClassSet) in the totally definite case. The key algorithm is the S-neighbors algorithm (Algorithm 7.4), but see also Algorithm 7.10, and its running time is analyzed in Proposition 7.7. The main result (the definite case of Theorem B) appears as Theorem 7.9. As in the previous section, let B be a totally definite quaternion algebra of discriminant $\mathfrak{D}$ and let $\mathcal{O} \subset B$ be an Eichler order of level $\mathfrak{N}$.

One way to solve Problem (ClassSet) is to simply enumerate the right invertible fractional $\mathcal{O}$-ideals in some way, building a list of ideal classes by testing each ideal (an instance of Problem (IsIsomorphic)) to see if it is isomorphic to any ideal in the list, and stopping when one knows that the list is complete. Ultimately, our methods to solve Problem (ClassSet) will be a variant of just this simple idea. We use the mass formula (Proposition 5.1) and the accompanying solution to Problem (ClassNumber) and stop when equality holds. (See also Remark 7.5 below for the use of the alternate mass formula.)

Remark 7.1. In the commutative case, one bounds the norm of the ideals in a generating set for $\mathrm{Cl}\,\mathbb{Z}_F$ using a Minkowski-like bound (or the Bach bound, assuming the GRH). One can in a similar way use the geometry of numbers in the case of quaternion algebras: the first author [27] has proven that if $\mathcal{O}$ is maximal, every ideal class in $\mathrm{Cl}\,\mathcal{O}$ is represented by an ideal I with

$$\mathrm{nrd}(I) \leq M_n d_F^2 \sqrt{\mathrm{N}\,\mathfrak{D}}$$

where M_n is a constant growing exponentially with n. Although this bound is effective, just as in the commutative case, it would be all but useless in practice except in the simplest cases.

To enumerate ideals, we note that the group $\mathrm{Cl}\,\mathbb{Z}_F$ acts on the set of isomorphism classes of fractional right $\mathcal{O}$-ideals by multiplication (on the left or right). We say that an invertible right (integral) $\mathcal{O}$-ideal I is *primitive* if I is not contained in any nontrivial two-sided ideal of the form $J = \mathfrak{a}\mathcal{O}$ with $\mathfrak{a} \subset \mathbb{Z}_F$. We note that $I \subset J$ if and only if $IJ^{-1} \subset \mathcal{O}$ is integral, and if $I \subset J$ then $\mathrm{nrd}(J) \mid \mathrm{nrd}(I)$ so I is contained in only finitely many two-sided ideals J.

Therefore, to enumerate all right $\mathcal{O}$-ideals, we enumerate the products JI of primitive right $\mathcal{O}$-ideals I and two-sided ideals $J = \mathfrak{a}\mathcal{O}$. To enumerate primitive right ideals, we employ the following lemma. For a commutative ring R, we denote by

$$\mathbb{P}^1(R) = \{(x,y) : xR + yR = R\}/R^*$$

the points of the projective line over R, and denote by $(x : y)$ the class of (x, y) in $\mathbb{P}^1(R)$.

Lemma 7.2. *Let $\mathfrak{a}$ be an ideal of $\mathbb{Z}_F$ coprime to $\mathfrak{D}\mathfrak{N}$. Then the set of primitive right invertible $\mathcal{O}$-ideals of norm $\mathfrak{a}$ are in bijection with $\mathbb{P}^1(\mathbb{Z}_F/\mathfrak{a})$. Explicitly, given a splitting*

$$\phi_{\mathfrak{a}} : \mathcal{O} \hookrightarrow \mathcal{O} \otimes_{\mathbb{Z}_F} \mathbb{Z}_{F,\mathfrak{a}} \cong M_2(\mathbb{Z}_{F,\mathfrak{a}}) \to M_2(\mathbb{Z}_F/\mathfrak{a})$$

the bijection is given by

$$\mathbb{P}^1(\mathbb{Z}_F/\mathfrak{a}) \to \{I \subset \mathcal{O} : \mathrm{nrd}(I) = \mathfrak{a}\}$$

$$(x : y) \mapsto I_{(x:y)} = \phi_{\mathfrak{a}}^{-1} \begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} \mathcal{O} + \mathfrak{a}\mathcal{O}.$$

Proof. We may refer to Vignéras [44, Chap. II, Théorème 2.3(3)]); for convenience, we give a proof here.

It is clear that the ideal $I_{(x:y)}$ is a right $\mathcal{O}$-ideal of norm $\mathfrak{a}$; it is invertible since it is locally principal, and it is primitive since the only two-sided ideals with norm dividing $\mathfrak{a}$ are of the form $\mathfrak{p}\mathcal{O}$ with $\mathfrak{p} \mid \mathfrak{a}$, and $\begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} \notin \mathfrak{p}M_2(\mathbb{Z}_{F,\mathfrak{a}})$ for any such $\mathfrak{p}$.

To prove the lemma, it suffices to construct an inverse map. Let I be a right invertible $\mathcal{O}$-ideal of norm $\mathfrak{a}$. Then $\phi_{\mathfrak{a}}(I)$ is a right principal $M_2(\mathbb{Z}_F/\mathfrak{a})$-ideal, say, generated by $\xi \in M_2(\mathbb{Z}_F/\mathfrak{a})$. We have $\det(\xi) = 0$, so the kernel

$$V = \{v \in (\mathbb{Z}_F/\mathfrak{a})^2 : v\xi = 0\}$$

of ξ acting on the right is nonzero. We claim in fact that V is a free $\mathbb{Z}_F/\mathfrak{a}$-module of rank 1. Indeed, for each prime $\mathfrak{p} \mid \mathfrak{a}$, we have $V/\mathfrak{p}V$ one-dimensional since I is primitive and hence $\xi \not\equiv 0 \pmod{\mathfrak{p}}$; it follows from a Hensel lift that $V/\mathfrak{p}^e V$ is also one-dimensional, and the claim then follows by the Chinese remainder theorem. This argument also shows that a generator $v = (x, y)$ of V has $(x : y) \in \mathbb{P}^1(\mathbb{Z}_F/\mathfrak{a})$ (and this element is unique), since this is true modulo $\mathfrak{p}$ for all $\mathfrak{p} \mid \mathfrak{a}$. Thus the association $I \mapsto (-y : x)$ is well-defined, and it is easy to see that this furnishes the desired inverse. $\square$

One natural way to enumerate primitive ideals I would be to order them by $\mathrm{N}(\mathrm{nrd}(I))$, the absolute norm of their reduced norm. Alternatively, one may restrict the set of possible reduced norms as follows.

Proposition 7.3 (Strong approximation). *Let S be a nonempty set of (finite) prime ideals of $\mathbb{Z}_F$ coprime to $\mathfrak{D}$ which generate $\mathrm{Cl}_{S_\infty} \mathbb{Z}_F$. Then there exists a set of representatives I for $\mathrm{Cl}\,\mathcal{O}$ such that $\mathrm{nrd}(I)$ is supported in S.*

Proof. See Vignéras [44, Théorème III.4.3] and the accompanying discussion. $\square$

Let $\mathfrak{a}$ be a squarefree ideal of $\mathbb{Z}_F$, and let I, J be right invertible $\mathcal{O}$-ideals. Then J is said to be a $\mathfrak{a}$-*neighbor* of I if $I \supset J$ and $\mathrm{nrd}(J) = \mathfrak{a}\,\mathrm{nrd}(I)$, or equivalently if $[I : J] = \mathfrak{a}^2$, the index taken as $\mathbb{Z}_F$-lattices. Following Schulze-Pillot [43], Pizer [39], Kohel [29], and Mestre [37]), we enumerate primitive ideals by iteratively enumerate the $\mathfrak{p}$-neighbors as follows.

Algorithm 7.4 (*S*-neighbors). *Let $\mathcal{O}$ be an Eichler order of level $\mathfrak{N}$ in a quaternion algebra B of discriminant $\mathfrak{D}$, and let S be a nonempty finite set of prime ideals of $\mathbb{Z}_F$ coprime to $\mathfrak{D}\mathfrak{N}$ that generate $\mathrm{Cl}_{S_\infty} \mathbb{Z}_F$. This algorithm solves Problem* (ClassSet).

(1) Solve (ClassNumber) as in Theorem 5.6 and let $H = \#\,\mathrm{Cl}\,\mathcal{O}$.
(2) Compute $\mathrm{Cl}\,\mathbb{Z}_F$ and compute a set C of representatives of the set of ideals of $\mathbb{Z}_F$ supported at S modulo principal ideals.
(3) Initialize $\mathcal{I} := \emptyset$, $\mathcal{F} := \{\mathcal{O}\}$, and $\mathcal{F}_{\mathrm{new}} := \emptyset$.
(4) For each $I \in \mathcal{F}$, compute the primitive $\mathfrak{p}$-neighbors I' of I using Lemma 7.2 for $\mathfrak{p} \in S$. For each such I', determine if I' is isomorphic to any ideal in $\mathcal{I} \cup \mathcal{F}_{\mathrm{new}}$ by an algorithm to solve (IsIsomorphic); if not, add JI' to $\mathcal{F}_{\mathrm{new}}$ for all $J \in C$.
(5) Set $\mathcal{I} := \mathcal{I} \cup \mathcal{F}$, $\mathcal{F} := \mathcal{F}_{\mathrm{new}}$ and $\mathcal{F}_{\mathrm{new}} := \emptyset$. If $\#\mathcal{I} = H$, return $\mathcal{I}$, otherwise return to Step 4.

Proof of correctness. The algorithm enumerates all right invertible $\mathcal{O}$-ideals with norm supported at S by the discussion preceding Lemma 7.2 and so will find all ideal classes by Proposition 7.3. $\square$

Our algorithm was inspired by the implementation due to Kohel in the computer algebra system Magma [4] for definite quaternion algebras over $\mathbb{Q}$.

Remark 7.5. In Algorithm 7.4, one can alternatively use the mass formula as in Remark 5.2; here, one trades the difficulty of computing the class number directly with computing the unit index $[\mathcal{O}^* : \mathbb{Z}_F^*]$ for each order $\mathcal{O} = \mathcal{O}_L(I)$. To compute this unit index, we consult Vignéras [45, Theorem 6]. If all totally positive units of $\mathbb{Z}_F$ are squares, then the group $\mathcal{O}_L(I)^*/\mathbb{Z}_F^*$ is just the set of shortest vectors in $\mathcal{O}_L(I)$, i.e., the reduced norm 1 subgroup $\mathcal{O}_1^*$ modulo $\{\pm 1\}$, and this group can be computed by lattice enumeration. Otherwise, if the norm 1 subgroup is not cyclic, then $\mathcal{O}^*/\mathbb{Z}_F^*$ is at most an extension of $\mathcal{O}_1^*/\{\pm 1\}$ of index 2 and we can explicitly write down candidates for this extension. If the norm 1 subgroup is cyclic, then we must fall back on a lattice search in $\mathcal{O}$.

To analyze the running time of Algorithm 7.4 , we now examine the distribution of ideal classes among ideals following this enumerative strategy. Let S be a nonempty finite set of ideals of $\mathbb{Z}_F$ coprime to $\mathfrak{DN}$ (as in Algorithm 7.4). Let $G(S)$ be the graph with vertices $[I] \in \mathrm{Cl}(\mathcal{O})$ and edges as follows: for a vertex $[I]$, choose a representative ideal I, and for each primitive $\mathfrak{n}$-neighbor J with $\mathfrak{n} \in S$, draw an edge from $[I]$ to $[J]$. By Lemma 7.2 , $\Gamma(S)$ is k-regular (the out degree of each vertex is k), where $k = \sum_{\mathfrak{n} \in S} \Phi(\mathfrak{n})$ and

$$\Phi(\mathfrak{n}) = \prod_{\mathfrak{p}^e \| \mathfrak{n}} N\mathfrak{p}^{e-1}(N\mathfrak{p} + 1).$$

When $S = \{\mathfrak{n}\}$ consists of a single ideal, we abbreviate $G(S)$ by simply $G(\mathfrak{n})$.

Suppose now that the map $\mathrm{nrd} : S \to \mathrm{Cl}_{S_\infty}(\mathbb{Z}_F)$ is surjective (i.e., that norms of ideals in S cover all narrow ideal classes of $\mathbb{Z}_F$). Then the set of vertices of the quotient $G(S)$ is a set of representatives for $\mathrm{Cl}\,\mathcal{O}$ by Proposition 7.3 .

The graphs $G(\mathfrak{p})$ are known in many cases to be *Ramanujan graphs*, graphs whose eigenvalues other than $\pm k$ have absolute value at most $2\sqrt{k-1}$, and are therefore a type of *expander graphs*. In the simplest case where $F = \mathbb{Q}$ and $S = \{p\}$, they were first studied by Ihara, then studied in specific detail by Lubotzky, Phillips, and Sarnak [35] and Margulis [36]: the nontrivial spectrum of $G(p)$ can be identified with the spectrum of the Hecke operators acting on the space of cusp forms of weight 2 on $\Gamma_0(p)$, and the eigenvalue bound then follows from the Ramanujan-Petersson conjecture, a consequence of the Eichler-Shimura isomorphism and Deligne's proof of the Weil conjectures (though strictly speaking, one only needs the result in weight 2, so could be derived from earlier results of Eichler, Igusa, Weil, and Shimura). Charles, Goren, and Lauter [9] have shown that the same is true for graphs $G(\mathfrak{l})$ under the following set of hypotheses: F is a totally real field of narrow class number one, $B \cong B_p \otimes_{\mathbb{Q}} F$ where B_p is the quaternion algebra of discriminant p over $\mathbb{Q}$ and p is unramified in F, and $\mathfrak{l}$ is a prime ideal of $\mathbb{Z}_F$ coprime to p. We note that there are further constructions due to Jordan and Livné [25].

Let $T(S)$ be the adjacency matrix of $G(S)$. We begin by discussing the interpretation of $T(S)$ as representing the action of a Hecke operator on the space of Hilbert modular forms. We refer the reader to work of Dembélé and the second author [53] for a computational point of view on the statements below, and the references therein for further information.

The graph $G(\mathfrak{n})$, for an ideal $\mathfrak{n}$ coprime to $\mathfrak{DN}$, represents the action of a Hecke operator on a certain space of quaternionic modular forms of level $\mathfrak{N}$ for the quaternion algebra B. By the Jacquet-Langlands correspondence [55] (see also e.g. work of Hida [54]), this space as a Hecke module (finite-dimensional $\mathbb{C}$-vector space equipped

with the action of Hecke operators) is isomorphic to a subspace M_2 of the space of Hilbert modular forms of parallel weight 2 and level $\mathfrak{D}\mathfrak{N}$. Therefore, we may identify eigenvectors of $T(S)$ with Hilbert modular eigenforms.

Since the adjacency matrix $T(S)$ of the graph $G(S)$ is the sum of the adjacency matrices of the graphs $G(\mathfrak{n})$ for $\mathfrak{n} \in S$, the matrix $T(S)$ represents the action of the operator

$$T_S = \sum_{\mathfrak{n} \in S} T_{\mathfrak{n}}.$$

For $\mathfrak{n}$ coprime to $\mathfrak{D}\mathfrak{N}$, the operators $T_{\mathfrak{n}}$ are semisimple and pairwise commute, and so there is a set of common eigenforms for all $T_{\mathfrak{n}}$ which span M_2. The space $M_2 = S_2 \oplus E_2$ breaks up accordingly into a space of Eisenstein series E_2 and a space of cusp forms S_2.

We now apply eigenvalue bounds coming from geometry. We first discuss the Eisenstein series. The space of Eisenstein series E_2 corresponds, under Jacquet-Langlands, to the standard Eisenstein series and its twists by Hilbert class characters, and is spanned by those vectors which "factor through the reduced norm", i.e., vectors of the form $a_I[I]$ with $a_I = a_J$ whenever $[\mathrm{nrd}(I)] = [\mathrm{nrd}(J)] \in \mathrm{Cl}_{S_\infty}(\mathbb{Z}_F)$. The eigenvectors are then given concretely as follows: for every irreducible character χ of $\mathrm{Cl}_{S_\infty}(\mathbb{Z}_F)$, the vector $v_\chi = (\chi([\mathrm{nrd}(I)]))_{[I] \in \mathrm{Cl}(O)}$ is an eigenvector of $T(\mathfrak{p})$ with eigenvalue

$$\chi([\mathfrak{p}])\Phi(\mathfrak{p})$$

and thus an eigenvector of $T(S)$ with eigenvalue

$$\sum_{\mathfrak{n} \in S} \chi([\mathfrak{n}])\Phi(\mathfrak{n}).$$

Now we turn to eigenvalue bounds for the remaining space S_2 of cusp forms. (We obtain exactly those cusp forms of level $\mathfrak{D}\mathfrak{N}$ which are new at all primes dividing $\mathfrak{D}$, but this is not relevant for our bounds.) The general result we will need is due to Livné [34], as follows.

Theorem 7.6. *Let $\mathfrak{p}$ be a prime with $\mathfrak{p} \nmid d_F\mathfrak{D}\mathfrak{N}$. Then the eigenvalues of $T_\mathfrak{p}$ acting on the space of cusp forms S_2 are bounded by $2\sqrt{N\mathfrak{p}}$. In particular, the graph $G(\mathfrak{p})$ is Ramanujan if $\mathfrak{p} \nmid d_F\mathfrak{D}\mathfrak{N}$.*

Proof. See the proof of the Ramanujan-Petersson conjecture for Hilbert modular forms by Livné [34, Theorem 0.1] and the accompanying discussion. $\square$

Suppose from now on that $\mathfrak{n}$ is squarefree. Since $T_\mathfrak{n} = \prod_{\mathfrak{p}|\mathfrak{n}} T_\mathfrak{p}$, it follows that the eigenvalues of $T_\mathfrak{n}$ acting on S_2 are bounded by $\prod_{\mathfrak{p}|\mathfrak{n}} 2\sqrt{N\mathfrak{p}}$ and accordingly the eigenvalues of T_S on S_2 are bounded by

$$\sum_{\mathfrak{n} \in S} \prod_{\mathfrak{p}|\mathfrak{n}} 2\sqrt{N\mathfrak{p}}.$$

Finally, the space $M_2 = E_2 \oplus S_2$ is equipped with a natural inner product coming from the Jacquet-Langlands correspondence called the Petersson inner product, under which cuspidal eigenforms are mutually orthogonal and E_2 is the orthogonal complement of S_2. This inner product on the free $\mathbb{Z}$-module spanned by $[I] \in \mathrm{Cl}(\mathcal{O})$ is defined by

$$\langle [I], [J] \rangle = \delta_{[I],[J]} w_I / 2$$

where $w_I = \#\mathcal{O}_L(I)^\times / \mathbb{Z}_F^\times$ and $\delta_{[I],[J]} = 0$ or 1 according as $[I] \neq [J]$ or $[I] = [J]$.

More is true: in fact, the matrix $T(S)$ is normal with respect to this inner product. Since this is a key point in our proof and the source of our original mistake, we give a proof.

Claim. $T = T(S)$ *is normal with respect to the Petersson inner product.*

Proof. Let $I_1, \ldots, I_H$ be representatives of the right ideal classes of $\mathcal{O}$; for $i = 1, \ldots, H$ let $\mathcal{O}_i = \mathcal{O}_L(I_i)$, $\Gamma_i = \mathcal{O}_i^\times / \mathbb{Z}_F^\times$ and $w_i = \#\Gamma_i$. We have shown that T has a basis of eigenvectors; we show that these eigenvectors are orthogonal with respect to the Petersson inner product: this is true already for the ones corresponding to cusp forms, so it is enough to show that the vectors v_χ are orthogonal.

Since the eigenvalue of $T(\mathfrak{p})$ on v_χ is $\chi([\mathfrak{p}])\Phi(\mathfrak{p})$, by the Chebotarev density theorem we can choose primes $\mathfrak{p}$ so that the eigenvalues of v_χ are distinct for each χ. Since there is a common basis of eigenvectors for all $T(\mathfrak{p})$, we conclude that this common eigenbasis is unique (unordered). Therefore, if we show that $T(\mathfrak{p})$ is normal for each prime $\mathfrak{p}$, so the eigenbasis is orthogonal, then this is also an eigenbasis for $T(S)$, so $T(S)$ is normal.

So suppose that $S = \{\mathfrak{p}\}$. Let m be the order of $[\mathfrak{p}] \in \mathrm{Cl}_{S_\infty}(\mathbb{Z}_F)$. We will show that T^m is self-adjoint.

An inclusion $J = xI_i \subset I_j$ with $\mathrm{nrd}(J) = \mathrm{nrd}(I_j)\mathfrak{p}$ corresponds to an element $x \in I_j I_i^{-1}$ with $\mathrm{nrd}(xI_iI_j^{-1}) = \mathfrak{p}$ and x is uniquely determined by I_i and $J = xI_i$ up to multiplication on the right by an element of $\mathcal{O}_i^\times$. Therefore by definition, the coefficient $T(S)_{i,j}$ is equal to the cardinality of the set

$$\{x \in I_j I_i^{-1} : \mathrm{nrd}(xI_iI_j^{-1}) = \mathfrak{p}\}/\mathcal{O}_i^\times$$

which is

$$\frac{1}{w_i}\#\{x \in I_j I_i^{-1} : \mathrm{nrd}(xI_iI_j^{-1}) = \mathfrak{p}\}/\mathbb{Z}_F^\times.$$

We similarly see that the coefficient $w_i(T^m)_{i,j}$, interpreted as the (weighted) number of paths in $G(S)$ of length m, is equal to

$$w_i(T^m)_{i,j} = \#\Theta_{i,j}(\mathfrak{p}^m)$$
$$= \#\{x \in I_j I_i^{-1} : \mathrm{nrd}(xI_iI_j^{-1}) = \mathfrak{p}^m\}/\mathbb{Z}_F^\times.$$

If $(T^m)_{i,j} = 0$, then $(T^m)_{j,i} = 0$ as well by the argument below. So suppose that $\Theta_{i,j}(\mathfrak{p}^m)$ is nonempty. Then $[\mathrm{nrd}(I_iI_j^{-1})] = [\mathfrak{p}^m \mathrm{nrd}(x)^{-1}] = 1$, so there exists a totally positive $a_{ij} \in \mathbb{Z}_F$ such that $a_{ij}\mathbb{Z}_F = \mathrm{nrd}(I_iI_j^{-1})$. We define a map

$$\Theta_{i,j}(\mathfrak{p}^m) \to \Theta_{j,i}(\mathfrak{p}^m)$$
$$x \mapsto a_{ij}\overline{x}$$

where the bar $^-$ indicates conjugation in B. Indeed, if $x \in \Theta_{i,j}(\mathfrak{p}^m)$ then $x \in I_j I_i^{-1}$ so

$$\overline{x} \in \overline{I_i}^{-1}\overline{I_j} = I_iI_j^{-1}\mathrm{nrd}(I_jI_i^{-1})$$

so $a_{ij}\overline{x} \in I_iI_j^{-1}$; and

$$\mathrm{nrd}(a_{ij}\overline{x}I_jI_i^{-1}) = \mathrm{nrd}(x)a_{ij}^2\mathrm{nrd}(I_jI_i^{-1}) = \mathrm{nrd}(xI_iI_j^{-1}) = \mathfrak{p}^m.$$

Therefore, this map is a bijection, so $w_i(T^m)_{i,j} = w_j(T^m)_{j,i}$, and thus T^m is self-adjoint as claimed.

Now, in view of our comments above, the (uniquely defined) eigenbasis for T is an eigenbasis for T^m and so is pairwise orthogonal by the spectral theorem, thus T is normal. $\qquad\square$

Define the *distance* $d(v, w)$ between two vertices v, w in the graph $G(S)$ to be the length of the shortest path between them, and define the *diameter* of G to be $D(G) = \max_{v,w} d(v, w)$. To estimate the run time of the S-neighbors algorithm (7.4), we bound the diameter in a special case. Recall that for coprime ideals $\mathfrak{D}, \mathfrak{N}$, by Remark 5.2 we have the mass formula

$$M(\mathfrak{D}, \mathfrak{N}) = \sum_{[I] \in \mathrm{Cl}(\mathcal{O})} \frac{1}{w_I}.$$

Let $w_{\max} = \max_{[I] \in \mathrm{Cl}(\mathcal{O})} w_I$.

Proposition 7.7. *Let S be a finite set of primes $\mathfrak{p}$ of $\mathbb{Z}_F$ representing $\mathrm{Cl}_{S_\infty}(\mathbb{Z}_F)$ with $\mathfrak{p} \nmid d_F \mathfrak{D} \mathfrak{N}$. Let $\mathfrak{p}$ be the smallest prime in S. Let m be the smallest positive integer which is congruent to 1 modulo the exponent of $\mathrm{Cl}_{S_\infty}(\mathbb{Z}_F)$ which satisfies*

$$m > \frac{\log(M(\mathfrak{D}, \mathfrak{N}) w_{\max} / h^+(\mathbb{Z}_F))}{\log\big((N\mathfrak{p} + 1)/(2\sqrt{N\mathfrak{p}})\big)}.$$

Then $D(G(S)) \leq m$.

Proof. We follow the proof of Chung [10]. We want to find the minimum value of m such that $T(S)^m$ has all entries nonzero.

As in the proof of the claim, let $I_1, \ldots, I_H$ be representatives of the right ideal classes of $\mathcal{O}$; for $i = 1, \ldots, H$, let $w_i = \#(\mathcal{O}_L(I_i)/\mathbb{Z}_F^\times)$ and $\mathfrak{p}_i = \mathrm{nrd}(I_i)$, and let W be the diagonal matrix with entries $1/w_i$. Abbreviate $M = M(\mathfrak{D}, \mathfrak{N})$.

Let $1 \leq r, s \leq H$ be indices. We have $T(S) = \sum_{\mathfrak{p} \in S} T(\mathfrak{p})$ so

$$(T(S)^m)_{r,s} \geq \sum_{\mathfrak{p} \in S} (T(\mathfrak{p})^m)_{r,s}.$$

For indices r, s, let $\mathfrak{p}_{r,s}$ be such that $[\mathfrak{p}_{r,s}] = [\mathfrak{p}_s^{-1} \mathfrak{p}_r]$, possible since $\mathfrak{p}$ covers $\mathrm{Cl}_{S_\infty}(\mathbb{Z}_F)$. Then $(T(S)^m)_{r,s} \geq (T(\mathfrak{p})^m)_{r,s}$. So without loss of generality, we may assume $S = \{\mathfrak{p}_{r,s}\}$. To simplify, abbreviate $\mathfrak{p} = \mathfrak{p}_{r,s}$ and $T = T(S)$.

Let $\chi_1, \ldots, \chi_{h^+}$ be the irreducible characters of $\mathrm{Cl}_{S_\infty}(\mathbb{Z}_F)$, so $h^+ = h^+(\mathbb{Z}_F)$. For $i = 1, \ldots, h^+$, let

$$u_i = \frac{1}{\sqrt{M}} (\chi_i([\mathfrak{p}_j]))_{j=1,\ldots,H}$$

be the eigenvector corresponding to an Eisenstein series, with eigenvalue

$$\chi_i([\mathfrak{p}])(N\mathfrak{p} + 1).$$

Then the eigenvectors u_i are orthonormal with respect to the matrix W, i.e., $u_i W u_j^* = \delta_{ij}$ for $i, j = 1, \ldots, h^+$, where * denotes conjugate transpose.

Complete $u_1, \ldots, u_{h^+}$ to a basis $u_1, \ldots, u_H$ of (row) eigenvectors for T normalized so that $u_i W u_i^* = 1$ for all i. Then by the orthogonality relations of the Petersson inner product, we have $u_i W u_j^* = 0$ for all $i \neq j$. Let U be the matrix with rows u_i. Then $UWU^* = 1$, and since W is diagonal with positive diagonal entries, if $V = U\sqrt{W}$ (taking positive square roots), then $V^{-1} = V^*$ is unitary.

Now let D be the diagonal matrix whose diagonal entries are the eigenvalues $\lambda_1, \ldots, \lambda_H$ of $u_1, \ldots, u_H$. Let $T' = \sqrt{W}^{-1} T \sqrt{W}$. Then for any $m \geq 0$, since W is diagonal we have

$$(T')^m = \sqrt{W}^{-1} T^m \sqrt{W} = \sqrt{W}^{-1} U^{-1} D^m U \sqrt{W} = V^* D^m V.$$

Note that $(T')^m$ has nonnegative real entries, and since T^m has positive entries if and only if $(T')^m$ does, we may proceed using the argument in Chung's proof.

Let v_i be the rows of V. We have $T' = \sum_{i=1}^{H} \lambda_i v_i^* v_i$ and so for $r, s \in 1, \ldots, H$, the r, s-entry of $(T')^m$ is equal to

$$((T')^m)_{r,s} \geq \sum_{i=1}^{H} \lambda_i^m (v_i^* v_i)_{r,s} = \sum_{i=1}^{h^+} \lambda_i^m (v_i^* v_i)_{r,s} + \sum_{i=h+1}^{H} \lambda_i^m (v_i^* v_i)_{r,s}.$$

Then the first term is equal to

$$\sum_{i=1}^{h^+} \lambda_i^m (v_i^* v_i)_{r,s} = \frac{1}{M\sqrt{w_r w_s}} \sum_{i=1}^{h^+} \overline{\chi}_i([\mathfrak{p}_r]) \chi_i([\mathfrak{p}_s]) \left(\chi_i([\mathfrak{p}])(N\mathfrak{p}+1) \right)^m$$

$$= \frac{1}{M\sqrt{w_r w_s}} (N\mathfrak{p}+1)^m \sum_{i=1}^{h^+} \chi_i([\mathfrak{p}_s \mathfrak{p}^m]) \overline{\chi}_i([\mathfrak{p}_r]).$$

Now the theory of character sums says that for a finite abelian group G and $x, y \in G$, the sum over the set of all irreducible characters $\widehat{G}$

$$\sum_{\chi \in \widehat{G}} \chi(x) \overline{\chi}(y) = \begin{cases} \#G, & \text{if } x = y; \\ 0, & \text{if } x \neq y. \end{cases}$$

Therefore the inner first sum is h if $[\mathfrak{p}_s \mathfrak{p}^m] = [\mathfrak{p}_r]$ and 0 otherwise.

We now suppose $m \equiv 1 \pmod{\exp(\mathrm{Cl}_{S_\infty}(\mathbb{Z}_F))}$ where exp denotes the exponent of the group. Recall that we chose $\mathfrak{p}$ so that $[\mathfrak{p}] = [\mathfrak{p}_s^{-1} \mathfrak{p}_r]$. Therefore we have

$$\sum_{i=1}^{h^+} \lambda_i (v_i^* v_i)_{r,s} \geq \frac{h^+}{M\sqrt{w_r w_s}} (N\mathfrak{p}+1)^m.$$

Let $\lambda = 2\sqrt{N\mathfrak{p}}$. Then $|\lambda_i| \leq \lambda$ for $i = h+1, \ldots, H$. Continuing with the second sum, we reason as Chung that

$$\left| \sum_{i=h^++1}^{H} \lambda_i^m (v_i^* v_i)_{r,s} \right| \leq \lambda^m \left(1 - \sum_{i=1}^{h^+} |(v_i)_r|^2 \right)^{1/2} \left(1 - \sum_{i=1}^{h^+} |(v_i)_s|^2 \right)^{1/2}$$

$$= \lambda^m \left(1 - \frac{h^+}{M w_r} \right)^{1/2} \left(1 - \frac{h^+}{M w_s} \right)^{1/2} \leq \lambda^m.$$

Let $t = h^+/(M\sqrt{w_r w_s})$ and $k = N\mathfrak{p}+1$. Then putting these together, we have

$$((T')^m)_{r,s} \geq t k^m - \lambda^m.$$

Thus $((T')^m)_{r,s} > 0$ whenever

$$m > \frac{\log(t)}{\log(\lambda/k)} = \frac{\log(M\sqrt{w_r w_s}/h^+)}{\log(k/\lambda)}.$$

To obtain an estimate for all indices r, s, let $w_{\max} = \max_i w_i$, let $\mathfrak{p}_{\min} = \min_{\mathfrak{p} \in S} N\mathfrak{p}$ and $k_{\min} = N\mathfrak{p}_{\min} + 1$, and $\lambda_{\min} = 2\sqrt{N\mathfrak{p}_{\min}}$. Then for

$$m > \frac{\log(Mw_{\max}/h^+)}{\log k_{\min}/\lambda_{\min}}$$

with $m \equiv 1 \pmod{\exp(\mathrm{Cl}_{S_\infty}(\mathbb{Z}_F))}$ we have that every coefficient of $(T')^m$ is positive. This completes the proof of the proposition. $\square$

Before proving the definite case of Theorem B, we prove one further lemma.

Lemma 7.8. *There exists an algorithm which, given an ideal class $[\mathfrak{a}] \in \mathrm{Cl}_{S_\infty}(\mathbb{Z}_F)$ and a finite set T of primes of $\mathbb{Z}_F$, computes in probabilistic polynomial time a prime $\mathfrak{p} \notin T$ such that $[\mathfrak{p}] = [\mathfrak{a}]$ and $N\mathfrak{p} = O(\log^2 \prod_{\mathfrak{q} \in T} N\mathfrak{q})$ for a fixed totally real field F.*

Proof. We use a (weak) version of the effective Chebotarev density theorem due to Lagarias and Odlyzko, applied to the strict Hilbert class field of F. For an ideal class $[\mathfrak{a}] \in \mathrm{Cl}_{S_\infty}(\mathbb{Z}_F)$, define the counting function

$$\pi_{[\mathfrak{a}]}(x) = \#\{\mathfrak{p} \subset \mathbb{Z}_F \text{ prime} : [\mathfrak{p}] = [\mathfrak{a}] \text{ and } N\mathfrak{p} \leq x\}$$

for $x \in \mathbb{R}_{\geq 2}$. Then, by Lagarias and Odlyzko [30, Theorems 1.3–1.4], there exists an effectively computable constant $x_0 > 0$ which depends only on F such that for all $[\mathfrak{a}] \in \mathrm{Cl}_{S_\infty}(\mathbb{Z}_F)$ and all $x \geq x_0$, we have

$$(7.1) \qquad \left| \pi_{[\mathfrak{a}]}(x) - \frac{1}{h}\frac{x}{\log x} \right| \leq \frac{1}{2h}\frac{x}{\log x}$$

where $h = \#\mathrm{Cl}_{S_\infty}\mathbb{Z}_F$. (In fact, they prove a certainly stronger bound on the error and show that $\log x_0 = (d_F n)^{O(1)}$, but this weak version suffices for our purposes.)

We begin with two precomputation steps. We first compute the constant x_0, the strict class group $\mathrm{Cl}_{S_\infty} \mathbb{Z}_F$, and factor the discriminant d_F. Next, for each (rational) prime $p \leq \mathbb{Z}_F$ with $p \leq x$, we factor $p\mathbb{Z}_F$ and see if there exists a prime $\mathfrak{p} \mid p$ such that $[\mathfrak{p}] = [\mathfrak{a}]$ and $\mathfrak{p} \notin T$. If so, we return the ideal $\mathfrak{p}$. If not, then for all primes $\mathfrak{p}$ with $[\mathfrak{p}] = [\mathfrak{a}]$ we have $\mathfrak{p} \in T$.

Let $N(T) = \prod_{\mathfrak{q} \in T} N\mathfrak{q}$ and let $x = \max(x_0, \log^2 N(T), (4h)^4)$. Clearly $x = O(\log^2 N(T))$. Then

$$\#T \leq N(T) \leq \sqrt{x} \leq \frac{x}{4h\log x}.$$

By (7.1), we have

$$\frac{\pi_{[\mathfrak{a}]}(x) - \#T}{x} > \frac{1}{2h\log x} - \frac{1}{4h\log x} = \frac{1}{4h\log x}.$$

We have that $\#\{\mathfrak{b} \in [\mathfrak{a}] : N\mathfrak{b} \leq x\} \leq cx$ for some constant $c > 0$. Therefore, by employing the algorithm of Lemma 6.8, we can find in probabilistic polynomial time a prime ideal $\mathfrak{p}$ with $[\mathfrak{p}] = [\mathfrak{a}]$, $N\mathfrak{p} \leq x$, and $\mathfrak{p} \notin T$. $\square$

We now prove the definite case of Theorem B.

Theorem 7.9. *There exists an algorithm to solve Problem (ClassSet) for definite orders with factored discriminant over a fixed field F which runs in probabilistic polynomial time in the output size.*

Proof. We use Algorithm 7.4 . We must, for a given order $\mathcal{O}$ of discriminant $\mathfrak{d} = \mathfrak{D}\mathfrak{N}$, choose a set S of primes $\mathfrak{p}$ of $\mathbb{Z}_F$ which represents the elements of the narrow class group $\mathrm{Cl}_{S_\infty} \mathbb{Z}_F$ such that $\mathfrak{p} \nmid d_F \mathfrak{D}\mathfrak{N}$. We do this by first computing a set of representatives for $\mathrm{Cl}_{S_\infty} \mathbb{Z}_F$ (which runs in constant time for fixed F) and then using the algorithm of Lemma 7.8 with $T = \{\mathfrak{p} : \mathfrak{p} \mid d_F \mathfrak{D}\mathfrak{N}\}$, which runs in probabilistic polynomial time in the size of the input.

We now refer to Proposition 7.7 . We claim that we may arrange so that the diameter $D(G)$ of the S-neighbors graph $G = G(S)$ is $D(G) = 1$. The quantity

$$\frac{\log(M(\mathfrak{D}, \mathfrak{N}) w_{\max}/h^+(\mathbb{Z}_F))}{\log\big((N\mathfrak{p} + 1)/(2\sqrt{N\mathfrak{p}})\big)}.$$

has numerator of size $O(\log H)$, so by taking the smallest prime $\mathfrak{p} \in S$ to be sufficiently large and of polynomial size, we can assume this quantity is ≤ 1.

With the set S now computed, we employ Algorithm 7.4 . Step 1 can be performed in probabilistic polynomial time over a fixed totally real field F and we have already performed Step 2. We conclude from Theorem 7.7 that Step 3 requires a number of calls to Problem (IsPrincipal) which is polynomial in the size of the output $H = \# \mathrm{Cl}\,\mathcal{O}$, each with input of polynomial size. In solving Problems (IsIsomorphic) and consequently (IsPrincipal), we only need to check ideals with the same reduced norm, since S consists of primes representing each element in the narrow class group and $D(G) = 1$, if $[I] = [J]$ then $[\mathrm{nrd}(I)] = [\mathrm{nrd}(J)]$ so $\mathrm{nrd}(I) = \mathrm{nrd}(J)$. By Proposition 6.9 , each call to Algorithm 6.3 runs in deterministic polynomial time, and the proof is complete. $\square$

We conclude by proposing an alternative to Algorithm 7.4 which solves Problems 2.2 (ClassSet) and 2.8 (ConjClassSet) simultaneously by computing two-sided ideals and connecting ideals, as in Proposition 2.10. This algorithm appears to perform better than Algorithm 7.4 in practice, though we do not prove anything rigorous along these lines.

Algorithm 7.10. *Let $\mathcal{O}$ be an Eichler order of level $\mathfrak{N}$. This algorithm outputs a set $\mathcal{E} = \{\mathcal{O}_i\}$ of representatives of the conjugacy classes of Eichler orders of level $\mathfrak{N}$, a set $\mathcal{C} = \{C_i\}$ of integral invertible right $\mathcal{O}$-ideals such that $\mathcal{O}_L(C_i) = \mathcal{O}_i$, and a set $\mathcal{I}$ of representatives of $\mathrm{Cl}\,\mathcal{O}$.*

(1) Solve (ClassNumber) as in Theorem 5.6 and let $H = \# \mathrm{Cl}\,\mathcal{O}$.
(2) Initialize $\mathcal{E}, \mathcal{C} := \{\mathcal{O}\}$. Let $\mathcal{I}$ be a system of representatives for the two-sided $\mathcal{O}$-ideal classes as in Proposition 3.2.
(3) Choose $\mathcal{O}_i \in \mathcal{E}$ and $\mathfrak{p}$ an ideal of $\mathbb{Z}_F$ coprime to $\mathfrak{D}\mathfrak{N}$, and compute the set $\mathcal{J}$ of primitive right $\mathcal{O}_i$-ideals with norm $\mathfrak{p}$ as in Lemma 7.2.
(4) For all $I \in \mathcal{J}$ such that $\mathcal{O}_L(I)$ is not isomorphic to any order in $\mathcal{E}$, append $\mathcal{O}_L(I)$ to $\mathcal{E}$, and append $\{JIC_i\}_J$ to $\mathcal{I}$ where J ranges over a set of representatives for the two-sided $\mathcal{O}_L(I)$-ideal classes.
(5) If $\#\mathcal{I} = H$, return $\mathcal{E}, \mathcal{C}, \mathcal{I}$; otherwise, return to Step 3.

Proof of correctness. The completeness of $\mathcal{I}$ follows from Proposition 2.10 once we show that the algorithm eventually enumerates all conjugacy classes of orders. Indeed, let $\mathcal{O}'$ be an Eichler order of level $\mathfrak{N}$; then there exists an integral, invertible right $\mathcal{O}', \mathcal{O}$-ideal I. By Strong Approximation (Proposition 7.3), we may assume that $\mathrm{nrd}(I)$ is coprime to $\mathfrak{D}\mathfrak{N}$. As in the proof of Lemma 3.1, I factors into a

product $I = I_1 I_2 \cdots I_r$ where each I_j is an invertible integral ideal of prime reduced norm with $\mathcal{O}_R(I_j) = \mathcal{O}_L(I_{j+1})$. The result now follows. $\qquad\square$

Remark 7.11. In practice, the ability to choose prime ideals $\mathfrak{p}$ of small norm in Step 3 is essential to enumerate only a small number of ideals of norm $\mathfrak{p}$; for this reason, we find that it is usually faster to check different orders $\mathcal{O}_i$ than to compute with only one fixed order as in Algorithm 7.4. Nevertheless, the primes $\mathfrak{p}$ in Step 3 must be chosen in a way such that they generate the narrow class group of $\mathbb{Z}_F$.

Moreover, if some of the orders $\mathcal{O}_i$ have more than one isomorphism class of two-sided ideals, they contribute to $\mathcal{I}$ accordingly, which speeds up the enumeration. In this case, the alternative evaluation of the mass formula (Remark 7.5) also simplifies, since all right $\mathcal{O}$-ideals with conjugate left orders have the same mass. On the other hand, if each $\mathcal{O}_i$ has only the trivial two-sided ideal class, a condition which is not obviously anticipated, then Algorithm 7.10 may take somewhat longer than Algorithm 7.4.

8. Definite Eichler orders with class number at most two

In this section, we list all definite Eichler orders $\mathcal{O}$ with $h(\mathcal{O}) \leq 2$. From (5.1) and Proposition 5.1, for such an order we have

$$2 \geq h(\mathcal{O}) \geq M(\mathcal{O}) \geq 2^{1-n} |\zeta_F(-1)| \geq \frac{2}{(4\pi^2)^n} d_F^{3/2}$$

and hence

$$(8.1) \qquad \delta_F = d_F^{1/n} \leq (2\pi)^{4/3} \leq 11.594.$$

By the Odlyzko bounds, there are only finitely many such fields and they have been explicitly enumerated [48]: we have $1, 39, 47, 108, 37, 40, 4, 3$ fields of degrees $n = 1, 2, 3, 4, 5, 6, 7, 8$, respectively, and no field satisfying the bound (8.1) with $n \geq 9$, for a total of 279 fields.

For each such field, using the methods of §5 (Proposition 5.4) we compute the mass $M(\mathbb{Z}_F, \mathbb{Z}_F)$; then for an Eichler order of level $\mathfrak{N}$ in a quaternion algebra of discriminant $\mathfrak{D}$ over F, we have

$$M(\mathfrak{D}, \mathfrak{N}) = M(\mathbb{Z}_F, \mathbb{Z}_F) \Phi(\mathfrak{D}) \Psi(\mathfrak{N}) \leq 2$$

which gives a finite list of possible ideals $\mathfrak{D}, \mathfrak{N}$. For each such possibility, we compute the corresponding class number using the Eichler mass formula as in Theorem 5.6. To check the computation, we also enumerate the ideal classes explicitly as in §6 (using Algorithm 7.10 and the alternate mass formula, Remark 5.2) and see that in all cases they match.

We consider two Eichler orders, specified by the ideals $\mathfrak{D}, \mathfrak{N}$ of $\mathbb{Z}_F$ and $\mathfrak{D}', \mathfrak{N}'$ of $\mathbb{Z}_{F'}$, to be *equivalent* if there is an isomorphism $\sigma : F \xrightarrow{\sim} F'$ of fields such that $\sigma(\mathfrak{D}) = \mathfrak{D}'$ and $\sigma(\mathfrak{N}) = \mathfrak{N}'$. Two equivalent Eichler orders have the same class number by the mass formula.

Proposition 8.1. *There are exactly* 74 *equivalence classes of definite Eichler orders with class number* 1 *and* 172 *with class number* 2.

These classes are listed in Tables 8.2–8.3. Here we list the degree n, the discriminant d_F of F, and the norms D and N of the discriminant $\mathfrak{D}$ and level $\mathfrak{N}$. This way of recording orders is compact but ambiguous; nevertheless, in all cases the field F is determined by its discriminant, and in all but a handful of cases, for *any* choice

of squarefree $\mathfrak{D}$ and coprime $\mathfrak{N}$ an Eichler order of level $\mathfrak{N}$ in a quaternion algebra of discriminant $\mathfrak{D}$ has the given class number. For the handful of exceptions, we refer to the complete tables which are available online [28].

We note that the results in Table 8.2 for $F = \mathbb{Q}$ agree with those of Brzeziński [6] (when restricted to Eichler orders).

TABLE 8.2: Definite Eichler orders $\mathcal{O}$ with class number $h(\mathcal{O}) = 1$.

n	d_F	D	N	n	d_F	D	N	n	d_F	D	N	n	d_F	D	N
1	1	2	1	2	8	1	1	3	49	7	1	4	725	1	1
		2	3			1	2			8	1			1	11
		2	5			1	4			13	1			1	19
		2	9			1	7			29	1			1	29
		2	11			1	8			43	1		1957	1	1
		3	1			1	14		81	3	1			1	3
		3	2			1	16			3	8			1	9
		3	4			1	23			19	1		2777	1	1
		5	1			14	1			37	1			1	2
		5	2			18	1		148	2	1			1	4
		7	1			50	1			2	5	5	24217	5	1
		13	1		13	1	1			5	1				
2	5	1	1			1	3			5	2				
		1	4			1	9			13	1				
		1	5			12	1		169	5	1				
		1	9		17	1	1			13	1				
		1	11			1	2		316	2	1				
		1	16			1	4			2	2				
		1	19						321	3	1				
		1	20												
		1	25												
		1	29												
		1	44												
		1	59												
		20	1												
		44	1												

TABLE 8.3: Definite Eichler orders $\mathcal{O}$ with class number $h(\mathcal{O}) = 2$.

n	d_F	D	N	n	d_F	D	N	n	d_F	D	N	n	d_F	D	N
1	1	2	7	2	8	1	9	3	49	7	8	4	725	1	16
		2	15			1	17			7	13			1	25
		2	17			1	28			7	27			1	31
		2	23			1	31			8	7			1	41
		3	5			1	32			13	7			1	49
		3	7			1	47			13	13			1	79
		3	8			14	7			27	1			1	89
		3	11			34	1			41	1		1125	1	1
		5	3			62	1			71	1			1	5
		5	4			63	1			97	1			1	9
		7	2		12	1	1			113	1			1	29
		7	3			1	2			127	1			1	59
		11	1			1	3		81	3	17			80	1
		17	1			1	4			3	19		1600	1	1
		19	1			1	6			8	1		1957	1	7
		30	1			1	8			17	1			1	23
		42	1			1	11			19	3			21	1
		70	1			1	12			73	1		2000	20	1
		78	1			1	23		148	2	17		2048	1	1
2	5	1	31			6	1			2	23		2225	1	1
		1	36			6	11			5	4		2304	18	1
		1	41			26	1			17	1		2525	1	1
		1	45			39	1			25	1		2624	1	1
		1	49			50	1		169	5	5		2777	1	8
		1	55		13	1	4			8	1			1	11
		1	64			1	9		229	2	1		3981	1	1
		1	71			1	17			4	1			15	1
		1	79			1	23			7	1		4205	1	1
		1	80			9	1		257	3	1		4352	14	1
		1	81			12	3			5	1		4752	12	1
		1	89			39	1			7	1		6809	1	1
		1	95		17	1	4		316	2	1	5	14641	11	1
		1	99			1	8			2	4			23	1
		20	9			4	1		321	3	1		24217	17	1
		36	1			18	1			3	3		36497	3	1
		45	1			26	1			7	1		38569	7	1
		55	1		21	1	1		361	7	1			13	1
		95	1			1	3		404	2	1	6	300125	1	1
		99	1			1	5		469	4	1		371293	1	1
		124	1			12	1		568	2	1		434581	1	1
		155	1			20	1						485125	1	1
		164	1		24	6	1						592661	1	1
						15	1								
					28	6	1								
					29	1	1								
					33	6	1								
					37	1	1								
					41	1	1								

References

[1] M. Alsina and P. Bayer, *Quaternion orders, quadratic forms, and Shimura curves*, CRM monograph series, vol. 22, Amer. Math. Soc., Providence, 2004.

[2] E. Bach, *How to generate random integers with known factorization*, Proc. ACM Symposium on Theory of Computing, 1983, 184–188.

[3] A. F. Beardon, *The geometry of discrete groups*, Grad. Texts in Math., vol. 91, Springer, Berlin, 1983.

[4] W. Bosma. J. Cannon and C. Playoust, *The Magma algebra system. I. The user language.*, J. Symbolic Comput., **24** (3–4), 1997, 235–265.

[5] J. Brzeziński, *On orders in quaternion algebras*, Comm. Algebra **11** (1983), no. 5, 501–522.

[6] J. Brzeziński, *Definite quaternion orders of class number one*, J. Théorie Nombres Bordeaux **7** (1995), no. 1, 93–96.

[7] J. Buchmann, *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields*, Séminaire de Théorie des Nombres, Paris (1988–1989), Progr. Math., vol. 91, Birkhäuser, 1990, 27–41.

[8] J. Buchmann and H.C. Williams, *On the computation of the class number of an algebraic number field*, Math. Comp. **53** (1989), no. 188, 679–688.

[9] D. Charles, E. Goren and K. Lauter, *Families of Ramanujan graphs and quaternion algebras*, to appear.

[10] F. R.K. Chung, *Diameters and eigenvalues*, J. Amer. Math. Soc. **2** (1989), no. 2, 187–196.

[11] H. Cohen, *A course in computational algebraic number theory*, Grad. Texts in Math., vol. 138, Springer, Berlin, 1993.

[12] H. Cohen, *Advanced topics in computational algebraic number theory*, Grad. Texts in Math., vol. 193, Springer, Berlin, 2000.

[13] H. Cohen, F. Diaz y Diaz and M. Olivier, *Subexponential algorithms for class group and unit computations*, Computational algebra and number theory (London, 1993), J. Symbolic Comput. **24** (1997), no. 3-4, 433–441.

[14] L. Dembélé, *Quaternionic Manin symbols, Brandt matrices, and Hilbert modular forms*, Math. Comp. **76** (2007), no. 258, 1039–1057.

[15] L. Dembélé and S. Donnelly, *Computing Hilbert modular forms over fields with nontrivial class group*, in Algorithmic Number Theory, A. van der Poorten and A. Stein, eds., Lecture notes in computer science, vol. 5011, Springer, Berlin, 2008, 371–386.

[16] J. Dieudonné, *Linear algebra and geometry*, Hermann, Paris, 1969.

[17] T. Dokchitser, *Computing special values of motivic L-functions*, Experiment. Math. **13** (2004), no. 2, 137–149.

[18] M. Eichler, *Zur Zahlentheorie der Quaternionen-Algebren*, J. Reine Angew. Math. **195** (1955), 127–151.

[19] N. Elkies, *Rational points near curves and small nonzero $|x^3 - y^2|$ via lattice reduction*, Algorithmic Number Theory (Leiden, 2000), Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 2000, 33–63.

[20] J. Elstrodt, F. Grunewald and J. Mennicke, *Groups acting on hyperbolic space. Harmonic analysis and number theory*, Springer monographs in math., Springer, 1998.

[21] U. Fincke and M. Pohst, *Improved methods for calculating vectors of short length in a lattice, including a complexity analysis*, Math. Comp. **44** (1985), no. 170, 463–471.

[22] C. Friedrichs, *Berechnung von Maximalordnungen über Dedekindringen*, Dissertation, Fachbereich Mathematik, Technische Universität Berlin, 2000.

[23] J. von zur Gathen and D. Panario, *Factoring polynomials over finite fields: a survey*, J. Symb. Comput. **31** (2001), 3–17.

[24] G. Ivanyos and A. Szántó, *Lattice basis reduction for indefinite forms and an application*, Discrete Math. **153** (1996), no. 1, 177–188.

[25] B. W. Jordan and R. Livné, *The Ramanujan propery for regular cubical complexes*, Duke Math. J. **105** (2000), no. 1, 85–103.

[26] R. Kannan, *Minkowski's convex body theorem and integer programming*, Math. Oper. Res. **12** (1987), no. 3, 415–440.

[27] M. Kirschmer, *Konstruktive Idealtheorie in Quaternionenalgebren*, Diplomarbeit, Universität Ulm, 2005.

[28] M. KIRSCHMER AND J. VOIGHT, Definite quaternion orders of class number at most two, http://www.cems.uvm.edu/~voight/defeichler-tables/.

[29] D. R. KOHEL, *Hecke module structure of quaternions*, Class field theory—its centenary and prospect (Tokyo, 1998), Adv. Stud. Pure Math., vol. 30, Math. Soc. Japan, Tokyo, 2001, 177–195.

[30] J. C. LAGARIAS AND A. M. ODLYZKO, *Effective versions of the Chebotarev density theorem*, Algebraic number fields: *L*-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, 409–464.

[31] A. K. LENSTRA, *Factoring polynomials over algebraic number fields*, Computer algebra (London, 1983), Lecture Notes in Comput. Sci., vol. 162, Springer, Berlin, 1983, 245–254.

[32] H. W. LENSTRA, JR., *Algorithms in algebraic number theory*, Bull. Amer. Math. Soc. (N.S.) **26** (1992), no. 2, 211–244.

[33] A. K. LENSTRA, H. W. LENSTRA, JR. AND L. LOVÁSZ, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 513–534.

[34] R. LIVNÉ, *Communication networks and Hilbert modular forms*, Applications of algebraic geometry to coding theory, physics and computation (Eilat, 2001), NATO Sci. Ser. II Math. Phys. Chem., 36, Kluwer Acad. Publ., Dordrecht, 2001, 255–270.

[35] A. LUBOTZKY, R. PHILLIPS AND P. SARNAK, *Ramanujan graphs*, Combinatorica **8** (1988), 261–277.

[36] G. MARGULIS, *Explicit group theoretic constructions of combinatorial schemes and their application to the design of expanders and concentrators*, J. Prob. of Info. Trans. (1988) 39–46.

[37] J.-F. MESTRE, *La méthode des graphes. Exemples et applications*, Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata, 1986), Nagoya Univ., Nagoya, 1986, 217–242.

[38] A. M. ODLYZKO, *Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results*, Sém. Théor. Nombres Bordeaux (2) **2** (1990), no. 1, 119–141.

[39] A. PIZER, *An algorithm for computing modular forms on $\Gamma_0(N)$*, J. Algebra **64** (1980), no. 2, 340–390.

[40] W. PLESKEN AND B. SOUVIGNIER, *Computing isometries of lattices*, J. Symbolic Comput. **24** (1997), 327–334

[41] I. REINER, *Maximal orders*, Clarendon Press, Oxford, 2003.

[42] R. SCHOOF, *Computing Arakelov class groups*, Algorithmic number theory, MSRI Publications, vol. 44, Cambridge University Press, Cambridge, 2008, 447–495.

[43] R. SCHULZE-PILLOT, *An algorithm for computing genera of ternary and quaternary quadratic forms*, Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation, ISSAC '91, (Bonn, Germany, July 15–17, 1991), ed. S.M. Watt, ACM Press, New York, 1991, 134–143.

[44] M.-F. VIGNÉRAS, *Arithmétique des algèbres de quaternions*, Lecture notes in mathematics, vol. 800, Springer, Berlin, 1980.

[45] M.-F. VIGNÉRAS, *Simplification pour les ordres des corps de quaternions totalement définis*, J. Reine Angew. Math. **286** (1976).

[46] J. VOIGHT, *Quadratic forms and quaternion algebras: Algorithms and arithmetic*, Ph.D. thesis, University of California, Berkeley, 2005.

[47] J. VOIGHT, *Computing CM points on Shimura curves arising from cocompact arithmetic triangle groups*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, 406–420.

[48] J. VOIGHT, *Enumeration of totally real number fields of bounded root discriminant*, in Algorithmic Number Theory, A. van der Poorten and A. Stein, eds., Lecture notes in computer science, vol. 5011, Springer, Berlin, 2008, 268–281.

[49] J. VOIGHT, *Shimura curves of genus at most two*, Math. Comp. **78** (2009), 1155–1172.

[50] J. VOIGHT, *Fundamental domains for arithmetic Fuchsian groups*, J. Théorie de Nombres de Bordeaux **21** (2009), no. 2, 467-489.

[51] J. VOIGHT, *Algorithmic identification of quaternion algebras and the matrix ring*, in preparation.

[52] L. C. WASHINGTON, *Introduction to cyclotomic fields*, 2nd ed., Grad. Texts in Math., vol. 83, Springer, New York, 1997.

[53] Lassina Dembélé and John Voight, *Explicit methods for Hilbert modular forms*, arxiv.org/abs/1010.5727.

[54] Haruzo Hida, *On abelian varieties with complex multiplication as factors of the Jacobians of Shimura curves*, Amer. J. of Math. **103** (1981), no. 4, 727–776.

[55] Hervé Jacquet and Robert P. Langlands, *Automorphic forms on GL(2)*, Lectures Notes in Math., vol. 114, Springer-Verlag, Berlin, 1970.

LEHRSTUHL D FÜR MATHEMATIK, RWTH AACHEN UNIVERSITY, TEMPLERGRABEN 64, 52062 AACHEN, GERMANY

E-mail address: Markus.Kirschmer@math.rwth-aachen.de

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF VERMONT, 16 COLCHESTER AVE, BURLINGTON, VT 05401, USA

E-mail address: jvoight@gmail.com