Ternary quadratic forms over number fields with small class number

Markus Kirschmer[1], David Lorch

Lehrstuhl B für Mathematik
RWTH Aachen University
52062 Aachen, Germany

Abstract

We enumerate all positive definite ternary quadratic forms over number fields with class number at most 2. This is done by constructing all definite quaternion orders of type number at most 2 over number fields. Finally, we list all definite quaternion orders of ideal class number 1 or 2.

Keywords: Quadratic form, genus, class number, quaternion order.
2010 MSC: Primary 11E41; Secondary 16H10.

1. Introduction

The question of finding all positive definite quadratic forms with small class number dates back to Gauß. The binary case (where at present, a complete unconditional classification is out of reach) is related to relative ideal class numbers of CM-fields. Over the rationals, one-class genera cannot exist in dimension ≥ 11 (cf. [36]). The rational one-class genera have been studied extensively by Watson, see [35, 37] and the references therein. He classified all such genera in three and more than five variables, and produced partial results in four and five variables. The authors have recently reinvestigated Watson's classification and filled in the details for the missing dimensions four and five (see [14]). An overview of the enumeration of genera with small class number is given in [30].

In the case of an arbitrary totally real number field, Pfeuffer [26] showed that one-class genera of positive definite quadratic forms cannot exist in more than 32 variables. The maximal integral forms with class number one have been enumerated recently by the first author in [13]. Though one expects very few examples of one-class genera of positive definite quadratic forms over totally real number fields in dimension ≥ 5, no complete classification is known.

Email addresses: markus.kirschmer@math.rwth-aachen.de (Markus Kirschmer), david.lorch@math.rwth-aachen.de (David Lorch)

[1]The author has been supported by DFG grant KI 1594/1-1

Pfeuffer's results give an upper bound on the local factors occurring in Siegel's mass formula, thus effectively bounding the discriminants of possible base fields for one-class genera. For non-maximal forms in dimension 3, these bounds are not quite sharp enough to yield the possible base fields using the currently available tables of totally real number fields.

The present article addresses this shortcoming by employing the correspondence of Brzezinski-Peters-Eichler-Brandt (see Section 3), which relates these genera to quaternion orders with type number at most 2 (we refer to Section 2 for definitions). Thus, we will enumerate all genera of positive definite ternary quadratic forms with class number at most 2 over any totally real number field. These Gorenstein orders can be enumerated directly using `Magma` [1]. This classification extends the work of Brzezinski [7] who computed the quaternion orders of type number one over the rationals.

It turns out that there are 4194 one-class genera of positive definite ternary quadratic forms over 30 different base fields. The largest base field has degree 5. Similarly, there are 18,538 two-class genera over 75 different base fields, the largest one of which has degree 6.

This article is organized as follows. In Section 2, we recall properties of quaternion algebras and orders. In Section 3, we discuss a correspondence between quaternion orders and lattices in definite quadratic spaces. The list of all definite hereditary quaternion orders of type number at most 2 will be computed in Section 4. In Section 5 we extend this list to all definite quaternion orders of type number at most 2. Finally, in the last section we enumerate all definite quaternion orders having ideal class number at most 2.

A complete list of these orders and genera can be obtained electronically from [15].

The authors want to thank J. Voight for pointing out an error in the definition of the Gorenstein closure, which is corrected in this version.

2. Preliminaries

In this section, we recall the definition of quaternion algebras and summarize some of their properties. Good references for this section are [31], [6], and [29].

Let K be a number field or a completion thereof. Further, let $\mathbb{Z}_K$ be the ring of integers of K.

Quadratic spaces

Let (V, Q) be a (regular) quadratic space of dimension m over K. There exists a K-basis $(v_1, \dots, v_m)$ of V and scalars $a_1, \dots, a_m \in K^*$ such that $Q(\sum_i x_i v_i) = \sum_i a_i x_i^2$ for all $x_1, \dots, x_m \in K$. If K is a totally real number field and each a_i is totally positive, then (V, Q) is said to be *positive definite*.

A $\mathbb{Z}_K$-lattice in V is a finitely generated $\mathbb{Z}_K$-submodule which contains a K-basis of V. Two lattices L, L' in V are said to be *isometric*, if there exists some K-linear map $\varphi \in \mathrm{End}_K(V)$ such that $\varphi(L) = L'$ and $Q(\varphi(x)) = Q(x)$ for all $x \in V$. Given a place v of K, we denote by K_v the completion of K at v. If

$\mathfrak{p}$ is a prime ideal of $\mathbb{Z}_K$, we write $L_\mathfrak{p}$ for the completion $L \otimes_{\mathbb{Z}_K} \mathbb{Z}_{K_\mathfrak{p}}$ of L at $\mathfrak{p}$. Finally, if K is a number field, then L and L' are said to be in the same *genus*, if $L_\mathfrak{p}$ and $L'_\mathfrak{p}$ are isometric at each prime ideal $\mathfrak{p}$ of $\mathbb{Z}_K$.

Quaternion algebras

A *quaternion algebra* over K is a central simple K-algebra of dimension 4. Given $a, b \in K^*$, let $\mathcal{Q} = \left(\frac{a,b}{K}\right)$ be the K-algebra with basis $(1, i, j, ij)$ satisfying the relations $i^2 = a, j^2 = b, ij = -ji$. Then $\mathcal{Q}$ is a quaternion algebra and every quaternion algebra is isomorphic to $\left(\frac{a,b}{K}\right)$ for some $a, b \in K^*$. The K-linear map

$$\bar{}: \mathcal{Q} \to \mathcal{Q},\ r + si + tj + uij \mapsto r - si - tj - uij$$

is the unique antiautomorphism of $\mathcal{Q}$ such that the *reduced norm* $\mathrm{nr}(x) := x\bar{x}$ and *reduced trace* $\mathrm{tr}(x) := x + \bar{x}$ are contained in K for all $x \in \mathcal{Q}$. The reduced norm is a quadratic form on $\mathcal{Q}$ and $(x, y) \mapsto \mathrm{tr}(x\bar{y})$ is the corresponding bilinear form. Let $\mathcal{Q}^0 = \{x \in \mathcal{Q} \mid \mathrm{tr}(x) = 0\}$ be the trace zero subspace of $\mathcal{Q}$. By restriction, $(\mathcal{Q}^0, \mathrm{nr})$ is a ternary quadratic space.

The algebra $\mathcal{Q}$ is said to be *ramified* at some place P of K if $\mathcal{Q}_P := \mathcal{Q} \otimes_K K_P$ is a skewfield. The *discriminant* $\mathcal{D}(\mathcal{Q})$ of $\mathcal{Q}$ is the product of all the prime ideals of $\mathbb{Z}_K$ at which $\mathcal{Q}$ ramifies. If K is a number field then $\mathcal{Q}$ is said to be *definite* if $\mathcal{Q}$ is ramified at all infinite places of K. This is equivalent to saying that $(\mathcal{Q}, \mathrm{nr})$ (or $(\mathcal{Q}^0, \mathrm{nr})$) is a totally positive definite quadratic space. Of course, definite quaternion algebras can only exist over totally real number fields.

Quaternionic lattices

Suppose that I is a $\mathbb{Z}_K$-lattice in $\mathcal{Q}$. Then the *dual* $I^\# := \{x \in \mathcal{Q} \mid \mathrm{tr}(xI) \subseteq \mathbb{Z}_K\}$ of I is also a $\mathbb{Z}_K$-lattice. The norm $\mathrm{nr}(I)$ of I is the fractional $\mathbb{Z}_K$-ideal generated by $\{\mathrm{nr}(x) \mid x \in I\}$.

Suppose J is another $\mathbb{Z}_K$-lattice in $\mathcal{Q}$. The product of I and J is the $\mathbb{Z}_K$-lattice generated by $\{xy \mid x \in I, y \in J\}$.

Orders

An *order* in $\mathcal{Q}$ is a subring of $\mathcal{Q}$ which is also a $\mathbb{Z}_K$-lattice. Given a $\mathbb{Z}_K$-lattice I, the sets $\mathcal{O}_l(I) = \{x \in \mathcal{Q} \mid xI \subseteq I\}$ and $\mathcal{O}_r(I) = \{x \in \mathcal{Q} \mid Ix \subseteq I\}$ are orders called the left and right orders of I respectively. Moreover, I is called *two-sided* if $\mathcal{O}_l(I) = \mathcal{O}_r(I)$.

Ideals

Let $\mathcal{O}$ be an order in $\mathcal{Q}$. A $\mathbb{Z}_K$-lattice I is called a *right $\mathcal{O}$-ideal* if for each prime ideal $\mathfrak{p}$ of $\mathbb{Z}_K$ there exists some $x \in \mathcal{Q}^*_\mathfrak{p}$ such that $I_\mathfrak{p} = x_\mathfrak{p}\mathcal{O}_\mathfrak{p}$. If this is the case, then clearly $\mathcal{O}_r(I) = \mathcal{O}$. If in addition I is two-sided, we call I a *two-sided $\mathcal{O}$-ideal*.

Ideal classes and genera

Two right $\mathcal{O}$-ideals I and J are isomorphic as right $\mathcal{O}$-modules if and only if $I = xJ$ for some unit $x \in \mathcal{Q}^*$. By the Jordan-Zassenhaus theorem (cf. [29, Theorem 26.4]), the set of all right $\mathcal{O}$-ideals is a disjoint union of finitely many isomorphism classes. The number of isomorphism classes of right $\mathcal{O}$-modules is called the *ideal class number* $h(\mathcal{O})$ of $\mathcal{O}$. Two-sided $\mathcal{O}$-ideals are said to be isomorphic if they are isomorphic as right $\mathcal{O}$-ideals. Let $H(\mathcal{O})$ denote the number of isomorphism classes of two-sided $\mathcal{O}$-ideals.

By the Skolem-Noether theorem, two orders $\mathcal{O}$ and $\mathcal{O}'$ are isomorphic (as $\mathbb{Z}_K$-algebras) if and only if they are conjugate in $\mathcal{Q}^*$. The *genus* $\mathrm{Gen}(\mathcal{O})$ of $\mathcal{O}$ is the set of all orders $\mathcal{O}'$ such that $\mathcal{O}_\mathfrak{p}$ and $\mathcal{O}'_\mathfrak{p}$ are conjugate for all prime ideals $\mathfrak{p}$ of $\mathbb{Z}_K$. The number of conjugacy classes in $\mathrm{Gen}(\mathcal{O})$ is called the *type number* $t(\mathcal{O})$. The type and ideal class numbers of $\mathcal{O}$ are related by the following result.

Lemma 2.1. *Let $\mathcal{O}$ and $\mathcal{O}'$ be orders in the same genus and let S be a set of representatives of the isomorphism classes of right $\mathcal{O}$-ideals. Then*

$$1 \leq H(\mathcal{O}) = \#\{I \in S \mid \mathcal{O}' \text{ is conjugate to } \mathcal{O}_l(I)\} \leq h(\mathcal{O})\,.$$

In particular, $1 \leq t(\mathcal{O}) \leq h(\mathcal{O})$.

Proof. See for example [8, Section VI.8.2] or [16, Proposition 2.10].

Types of orders

Let $\mathcal{O}$ be an order in $\mathcal{Q}$. The $\mathbb{Z}_K$-ideal generated by

$$\{\det(\mathrm{tr}(x_i\bar{x}_j))_{i,j} \mid x_1, \ldots, x_4 \in \mathcal{O}\}$$

is always a square. The square root of this ideal is the (reduced) *discriminant* $\mathcal{D}(\mathcal{O})$. If $\mathcal{O} \subseteq \Lambda$ are orders then $\mathcal{D}(\mathcal{O}) = \mathcal{D}(\Lambda) \cdot [\Lambda : \mathcal{O}]$ where $[\Lambda : \mathcal{O}]$ denotes the index ideal of Λ and $\mathcal{O}$. An order is called *maximal* if it is not properly contained in another order. This is equivalent to saying that $\mathcal{D}(\mathcal{O}) = \mathcal{D}(\mathcal{Q})$. In particular, the ideal $\mathcal{N}(\mathcal{O}) := \mathcal{D}(\mathcal{O})\mathcal{D}(\mathcal{Q})^{-1}$ is always integral.

Further, let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}_K$ and let $k := \mathbb{Z}_K/\mathfrak{p}$ be its residue class field. There exists some lattice $\mathfrak{p}\mathcal{O} \subseteq I \subset \mathcal{O}$ such that $I/\mathfrak{p}\mathcal{O}$ is the radical of the k-algebra $\mathcal{O}/\mathfrak{p}\mathcal{O}$. The lattice I is in fact two-sided and $\mathrm{Id}_\mathfrak{p}(\mathcal{O}) := \mathcal{O}_l(I) = \mathcal{O}_r(I)$ is called the *radical idealizer* of $\mathcal{O}$ at $\mathfrak{p}$. Suppose now in addition that $\mathfrak{p}$ divides $\mathcal{D}(\mathcal{O})$. Then the k-algebra $\mathcal{O}/I$ is isomorphic to k, $k \times k$, or to a quadratic extension of k, and the *Eichler invariant* $e_\mathfrak{p}(\mathcal{O})$ is defined to be 0, 1 or -1 accordingly.

The order $\mathcal{O}$ is called *hereditary* if every $\mathbb{Z}_K$-lattice I with $\mathcal{O} \subseteq \mathcal{O}_r(I)$ is a right $\mathcal{O}$-ideal. This is equivalent to saying that $\mathcal{D}(\mathcal{O})$ is square-free as seen from the classification [29, Theorem 39.14]. An *Eichler order* is the intersection of two (not necessarily distinct) maximal orders.

The order $\mathcal{O}$ is a *Gorenstein order* if $\mathcal{O}^\#$ is a right $\mathcal{O}$-ideal. Finally, if every order containing $\mathcal{O}$ is Gorenstein, then $\mathcal{O}$ is called a *Bass order*.

An order is maximal / hereditary / Eichler / Bass or Gorenstein if and only if each of its completions has the corresponding property. Further, these different families of orders satisfy the following inclusions:

$$\{maximal\} \subset \{hereditary\} \subset \{Eichler\} \subset \{Bass\} \subset \{Gorenstein\}\,.$$

If $\mathcal{O}$ is any order in $\mathcal{Q}$, then $G(\mathcal{O}) := \mathrm{nr}(\mathcal{O}^\#)^{-1}\mathcal{O}^\#\mathcal{O}^\#$ (i.e. the $\mathbb{Z}_K$-module generated by $\{\lambda xy \mid \lambda \in \mathrm{nr}(\mathcal{O}^\#)^{-1},\ x, y \in \mathcal{O}^\#\}$) is again an order. In fact, $G(\mathcal{O})$ is the unique Gorenstein order such that $\mathcal{O} = \langle 1, b(\mathcal{O})G(\mathcal{O})\rangle$ for some integral ideal $b(\mathcal{O}) \subseteq \mathbb{Z}_K$, (see [5, Proposition 3.2] and [6, Proposition 1.4]). The ideal $b(\mathcal{O})$ is called the *Brandt invariant* of $\mathcal{O}$. Moreover, $\mathcal{D}(\mathcal{O}) = b(\mathcal{O})^3\mathcal{D}(G(\mathcal{O}))$ and two orders are conjugate if and only if their Gorenstein closures are conjugate and they have the same Brandt invariant (or discriminant). In particular, $t(\mathcal{O}) = t(G(\mathcal{O}))$.

3. Ternary lattices and Gorenstein orders

In this section, we discuss a correspondence between ternary lattices and Gorenstein orders. The correspondence we are using is due to Brzezinski [4, 5] and Peters [25]. It is based on work of Eichler [10] and Brandt [2].

Let (V, Q) be a definite ternary quadratic space over some number field K.

Definition 3.1. Two lattices L, L' in V are said to be *equivalent* if there exists some totally positive element $c \in K^*$, some fractional ideal $\mathfrak{a}$ of K and some K-linear map $\varphi\colon V \to V$ such that $\varphi(L) = \mathfrak{a} \cdot L$ and $Q(\varphi(x)) = c \cdot Q(x)$ for all $x \in V$.

Clearly, two equivalent lattices have the same class number. Thus, if we want to classify all definite ternary quadratic lattices with class number h, it suffices to only look at the equivalence classes.

For example by [17, (6.20)], the even part of the Clifford algebra of (V, Q) is a definite quaternion algebra $\mathcal{Q}$ such that $(\mathcal{Q}^0, \mathrm{nr})$ is isometric to $(V, c \cdot Q)$ for some totally positive element $c \in K^*$. Since we are only interested in equivalence classes of lattices, we may now assume that $(V, Q) = (\mathcal{Q}^0, \mathrm{nr}) \subset (\mathcal{Q}, \mathrm{nr})$.

Further let L be a $\mathbb{Z}_K$-lattice in $\mathcal{Q}^0$. By slight abuse of notation, let $\mathrm{nr}(L)$ denote the fractional $\mathbb{Z}_K$-ideal generated by $\{\mathrm{nr}(x) \mid x \in L\}$. Then

$$\mathfrak{O}(L) := 1\mathbb{Z}_K + \sum_{x,y \in L} \mathrm{nr}(L)^{-1} \cdot xy$$

is a Gorenstein order in $\mathcal{Q}$ (see [25, Satz 7] and [5, Proposition 2.3]). Conversely, if $\mathcal{O}$ is an order in $\mathcal{Q}$ then

$$\mathfrak{L}(\mathcal{O}) := \mathcal{D}(\mathcal{O}) \cdot (\mathcal{O}^\# \cap \mathcal{Q}^0)$$

is a ternary lattice in $(\mathcal{Q}^0, \mathrm{nr})$.

Theorem 3.2. *Let $\mathcal{Q}$ be a quaternion algebra over some number field K and let L, L' be $\mathbb{Z}_K$-lattices in $(\mathcal{Q}^0, \mathrm{nr})$.*

(a) Each Gorenstein order $\mathcal{O}$ in $\mathcal{Q}$ satisfies $\mathcal{O} = \mathfrak{O}(\mathfrak{L}(\mathcal{O}))$.
(b) There exists a fractional $\mathbb{Z}_K$-ideal $\mathfrak{a}$ such that $\mathfrak{a}L = \mathfrak{L}(\mathfrak{O}(L))$.
(c) $\mathfrak{O}(L)$ and $\mathfrak{O}(L')$ are isomorphic if and only if L and L' are similar, i.e. L' is isometric to $\mathfrak{a}L$ for some fractional $\mathbb{Z}_K$-ideal $\mathfrak{a}$.

Proof. Part (a) follows immediately from [5, Proposition 3.2] and it implies $\mathfrak{O}(L) = \mathfrak{O}(\mathfrak{L}(\mathfrak{O}(L)))$. Hence L and $\mathfrak{L}(\mathfrak{O}(L))$ differ by some fractional ideal as [10, Satz 14.1] shows. Part (c) is proven in [4, Corollary 3.10].

As a consequence we get that $\mathfrak{O}$ and $\mathfrak{L}$ induce bijections between the equivalence classes of ternary lattices over K and the isomorphism classes of Gorenstein orders over K. Moreover, since the two constructions $\mathfrak{O}$ and $\mathfrak{L}$ are compatible with taking completions, we have the following result.

Corollary 3.3. *Let G be the genus of a ternary lattice L. Then the class number of G coincides with the type number of $\mathfrak{O}(L)$.*

By Corollary 3.3, the classification of all definite ternary lattices over $\mathbb{Z}_K$ with class number h is equivalent to the classification of all definite Gorenstein quaternion orders over $\mathbb{Z}_K$ having type number h.

Remark 3.4. There are several other correspondences between ternary quadratic lattices and quaternion orders which map lattices of class number h to orders of type number h. Most notably:

1. The correspondence of Pall [24] for $K = \mathbb{Q}$, which was extended by Nipp in [22] to arbitrary number fields K, is not onto in general.
2. The correspondence of Gross and Lucianovic [12] over PIDs, which was extended by Voight [34] to arbitrary rings.

The classification of all quaternion orders with type number h is equivalent to the classification of all Gorenstein quaternion orders with type number h. Hence we prefer bijections between ternary quadratic lattices (modulo some equivalence relation that preserves class numbers) and Gorenstein orders. The map of Pall and Nipp does not satisfy this condition. However, the correspondence of Gross-Lucianovic-Voight, which is functorial, could also be used instead of the maps $\mathfrak{O}$ and $\mathfrak{L}$ from Brzezinski-Peters-Eichler-Brandt.

4. Hereditary orders with type number one

Let $\mathcal{Q}$ be a definite quaternion algebra over some totally real number field K of degree n. If $\mathcal{O}$ is an order in $\mathcal{Q}$, we denote by $\mathrm{N}_{\mathcal{Q}^*}(\mathcal{O}) = \{x \in \mathcal{Q}^* \mid x\mathcal{O}x^{-1} = \mathcal{O}\}$ the *normalizer* of $\mathcal{O}$ in $\mathcal{Q}^*$. Conjugation with an element from $\mathrm{N}_{\mathcal{Q}^*}(\mathcal{O})$ induces an isometry on the positive definite $\mathbb{Z}$-lattice $(\mathcal{O}, \mathrm{Nr}_{K/\mathbb{Q}} \circ \mathrm{nr})$ where $\mathrm{Nr}_{K/\mathbb{Q}}$ denotes the usual norm of K. Moreover, two elements induce the same

isometry if and only if their quotient lies in K^*. Thus the index $[\mathrm{N}_{\mathcal{Q}^*}(\mathcal{O}) : K^*]$ is finite. The *unit group* $\mathcal{O}^* = \{x \in \mathcal{O} \mid \mathrm{nr}(x) \in \mathbb{Z}_K^*\}$ is a subgroup of $\mathrm{N}_{\mathcal{Q}^*}(\mathcal{O})$ and therefore the index $[\mathcal{O}^* : \mathbb{Z}_K^*]$ is finite since $\mathbb{Z}_K^* = K^* \cap \mathcal{O}^*$.

Definition 4.1. Let $\mathcal{O}$ be an order in $\mathcal{Q}$ and suppose that $I_1, \ldots, I_{h(\mathcal{O})}$ represent the isomorphism classes of right $\mathcal{O}$-ideals. By Lemma 2.1, we may assume that $\mathcal{O}_l(I_1), \ldots, \mathcal{O}_l(I_{t(\mathcal{O})})$ represent the conjugacy classes of all orders in the genus of $\mathcal{O}$. Then the *mass* of $\mathcal{O}$ is defined as

$$\mathrm{Mass}(\mathcal{O}) := \sum_{i=1}^{h(\mathcal{O})} \frac{1}{[\mathcal{O}_l(I_i)^* : \mathbb{Z}_K^*]} = \sum_{i=1}^{t(\mathcal{O})} \frac{H(\mathcal{O}_l(I_i))}{[\mathcal{O}_l(I_i)^* : \mathbb{Z}_K^*]} .$$

The mass can be computed from invariants of $\mathcal{O}$ and K as follows.

Theorem 4.2 (Eichler's mass formula). *Let $\mathcal{O}$ be an order in $\mathcal{Q}$. Then*

$$\mathrm{Mass}(\mathcal{O}) = 2^{1-n} \cdot |\zeta_K(-1)| \cdot h_K \cdot \mathrm{Nr}_{K/\mathbb{Q}}(\mathcal{D}(\mathcal{O})) \prod_{\mathfrak{p} \mid \mathcal{D}(\mathcal{O})} \frac{1 - \mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})^{-2}}{1 - e_{\mathfrak{p}}(\mathcal{O})\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})^{-1}}$$

where ζ_K and h_K denote the Dirichlet zeta function and the class number of K respectively.

Proof. See for example [19, Theorem 1].

If $\mathcal{O}$ is hereditary, the above mass formula simplifies to the version given by Eichler in [11, Section 4]:

$$\mathrm{Mass}(\mathcal{O}) = 2^{1-n} \cdot |\zeta_K(-1)| \cdot h_K \cdot \prod_{\mathfrak{p} \mid \mathcal{D}(\mathcal{Q})} (\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p}) - 1) \cdot \prod_{\mathfrak{p} \mid \mathcal{N}(\mathcal{O})} (\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p}) + 1) . \tag{4.1}$$

Given an ideal $\mathfrak{a}$ of $\mathbb{Z}_K$, let $\omega(\mathfrak{a})$ be the number of prime ideal divisors of $\mathfrak{a}$. The number of prime ideals of $\mathbb{Z}_K$ of norm 2 will be denoted by $\omega_2(K)$.

Suppose now $\mathcal{O}$ is hereditary. For each prime ideal $\mathfrak{p}$ that divides $\mathcal{D}(\mathcal{O})$, there exists a unique two-sided $\mathcal{O}$-ideal $P_{\mathfrak{p}}$ with $P_{\mathfrak{p}}^2 = \mathfrak{p}\mathcal{O}$. The two-sided $\mathcal{O}$-ideals form an abelian group $\mathfrak{J}(\mathcal{O})$ which is free on $\{P_{\mathfrak{p}} : \mathfrak{p} \mid \mathcal{D}(\mathcal{O})\} \cup \{\mathfrak{p}\mathcal{O} : \mathfrak{p} \nmid \mathcal{D}(\mathcal{O})\}$. Then $\mathrm{N}_{\mathcal{Q}^*}(\mathcal{O})/K^*$ acts on the quotient $\mathfrak{J}(\mathcal{O})/\{a\mathcal{O} \mid a \in K^*\}$ by left multiplication. The orbits are the isomorphism classes of two-sided $\mathcal{O}$-ideals and the stabilizer of any class is $\mathcal{O}^*K^*/K^* \cong \mathcal{O}^*/\mathbb{Z}_K^*$. Thus

$$H(\mathcal{O}) = \frac{2^{\omega(\mathcal{D}(\mathcal{O}))} \cdot h_K}{[\mathrm{N}_{\mathcal{Q}^*}(\mathcal{O}) : \mathcal{O}^*K^*]} = 2^{\omega(\mathcal{D}(\mathcal{O}))} \cdot h_K \cdot \frac{[\mathcal{O}^* : \mathbb{Z}_K^*]}{[\mathrm{N}_{\mathcal{Q}^*}(\mathcal{O}) : K^*]} . \tag{4.2}$$

See [11, Section 4] for details.

Theorem 4.3. *If $\mathcal{O}$ is a hereditary order in $\mathcal{Q}$, then*

$$d_K^{1/n} < ((t(\mathcal{O})/2)^{1/n} \cdot 4\pi^2 \cdot (3/2)^{\omega_2(K)/n})^{2/3} .$$

PROOF. Let $\{\mathcal{O}_1, \ldots, \mathcal{O}_{t(\mathcal{O})}\}$ be a set of representatives of the conjugacy classes in the genus of $\mathcal{O}$. From equations (4.1) and (4.2), we conclude that

$$\begin{aligned} t(\mathcal{O}) &\geq \sum_{i=1}^{t(\mathcal{O})} \frac{1}{[\mathrm{N}_{\mathcal{Q}^*}(\mathcal{O}_i) : K^*]} = \frac{1}{2^{\omega(\mathcal{D}(\mathcal{O}))} \cdot h_K} \cdot \sum_{i=1}^{t(\mathcal{O})} \frac{H(\mathcal{O}_i)}{[\mathrm{N}_{\mathcal{Q}^*}(\mathcal{O}_i) : K^*]} \\ &= \frac{\mathrm{Mass}(\mathcal{O})}{2^{\omega(\mathcal{D}(\mathcal{O}))} \cdot h_K} \\ &= 2^{1-n} \cdot |\zeta_K(-1)| \prod_{\mathfrak{p} | \mathcal{D}(\mathcal{Q})} \frac{\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p}) - 1}{2} \cdot \prod_{\mathfrak{p} | \mathcal{N}(\mathcal{O})} \frac{\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p}) + 1}{2} \qquad (4.3) \\ &\geq 2^{1-n} \cdot |\zeta_K(-1)| \cdot 2^{-\omega_2(K)} \,. \end{aligned}$$

The functional equation of the zeta function gives $|\zeta_K(-1)| = d_K^{3/2} \cdot \zeta_K(2)/(2\pi^2)^n$. Therefore,

$$\begin{aligned} t(\mathcal{O}) &\geq \frac{2 d_K^{3/2}}{(2\pi)^{2n}} \cdot \zeta_K(2) \cdot 2^{-\omega_2(K)} > \frac{2 d_K^{3/2}}{(2\pi)^{2n}} \cdot (4/3)^{\omega_2(K)} \cdot 2^{-\omega_2(K)} \\ &\geq \frac{2 d_K^{3/2}}{(2\pi)^{2n}} \cdot (2/3)^{-\omega_2(K)} \end{aligned}$$

as claimed.

We will make the last result effective for orders of type number at most 2.

Lemma 4.4. *If $\mathcal{O}$ is a hereditary order in $\mathcal{Q}$ with $t(\mathcal{O}) \leq 2$, then*

$$d_K^{1/n} < (4\pi^2 \cdot (3/2)^{\omega_2(K)/n})^{2/3} \,. \qquad (4.4)$$

There are 358 totally real number fields K that satisfy equation (4.4). The largest one has degree 8.

PROOF. Let K be a field that satisfies equation (4.4) and let n be its degree. Then $d_K^{1/n} < (6\pi^2)^{2/3} < 15.20$. With the bounds from [3] this implies that $n \leq 10$.
If $n = 10$, then [3] shows that $d_K^{1/n} < 15.20$ is only possible if $\omega_2(K) \leq 1$. But $d_K^{1/n} < (4\pi^2 \cdot (3/2)^{1/10})^{2/3} < 11.92$ is impossible by [32]. The case $n = 9$ is ruled out similarly.
Voight's tables [32] list all totally real number fields K with $d_K^{1/n} \leq 15.5$ and degree at most 8. The result follows from an explicit search.

Algorithm 4.5.
Input: Some totally real number field K of degree n and some bound $B \geq 1$.
Output: A list $\mathcal{L}$ of sets. For each genus of definite hereditary quaternion orders over K with type number at most B, precisely one set in the list $\mathcal{L}$ represents the conjugacy classes of orders in that genus.

1. *Initialize* $\mathcal{L} = \emptyset$.
2. *Compute the set* P *of all prime ideals* $\mathfrak{p}$ *of* $\mathbb{Z}_K$ *such that*

$$\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p}) \leq 2^{n+\omega_2(K)} \cdot |\zeta_K(-1)|^{-1} \cdot B + 1\,. \tag{4.5}$$

3. *For each pair* (D, N) *of disjoint subsets of* P *such that* $\#D + n$ *is even and*

$$B \geq 2^{1-n} \cdot |\zeta_K(-1)| \cdot \prod_{\mathfrak{p}\in D} \frac{\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p}) - 1}{2} \cdot \prod_{\mathfrak{p}\in N} \frac{\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p}) + 1}{2} \tag{4.6}$$

   do
   (a) *Construct the definite quaternion* K*-algebra* $\mathcal{Q}$ *with* $\mathcal{D}(\mathcal{Q}) = \prod_{\mathfrak{p}\in D} \mathfrak{p}$.
   (b) *Compute a hereditary order* $\mathcal{O}$ *in* $\mathcal{Q}$ *such that* $\mathcal{N}(\mathcal{O}) = \prod_{\mathfrak{p}\in N} \mathfrak{p}$.
   (c) *Compute a set* S *of representatives of the conjugacy classes of orders in the genus of* $\mathcal{O}$.
   (d) *If* $\#S \leq B$ *then include* S *in* $\mathcal{L}$.
4. *Return* $\mathcal{L}$.

Proof. Suppose $\mathcal{O}$ is a hereditary order in a definite quaternion algebra $\mathcal{Q}$ over K such that $t(\mathcal{O}) \leq B$. Let D and N denote the set of prime ideal divisors of $\mathcal{D}(\mathcal{Q})$ and $\mathcal{N}(\mathcal{O})$ respectively. The isomorphism type of $\mathcal{Q}$ is uniquely determined by D (see [31, Theorem III.3.1]) and $\mathcal{O}_\mathfrak{p}$ is defined by N up to conjugacy in $\mathcal{Q}_\mathfrak{p}^*$ for all prime ideals $\mathfrak{p}$ (see [31, Lemma II.2.4]). In particular (D, N) uniquely determines the genus of $\mathcal{O}$. Thus $\mathcal{L}$ does not contain two different sets representing the same genus. Further $n + \#D$ is even by [31, Theorem III.3.1] and $D \cap N = \emptyset$ since $\mathcal{D}(\mathcal{O})$ is square-free.
The pair (D, N) satisfies equation (4.6) as we have seen in equation (4.3). In particular, every prime ideal $\mathfrak{p} \in D \cup N \subseteq P$ satisfies equation (4.5). Thus, at some point, we will construct an order which is in the same genus as $\mathcal{O}$.

Remark 4.6. We give some hints how step (3) of Algorithm 4.5 can be done in practice.
The quaternion algebra $\mathcal{Q}$ in step (3a) can be computed as follows. Let $a \in \mathbb{Z}_K$ be totally positive such that it has valuation 1 at all prime ideals in the set D. Then one tries some totally positive $b \in \mathbb{Z}_K$ such that $b\mathbb{Z}_K + D = \mathbb{Z}_K$ until $\left(\frac{-a,-b}{K}\right)$ has the correct discriminant. For this last step, one has to compute several Hilbert symbols which can be done using [33, Sections 5 and 6]. Once one has found a suitable algebra $\mathcal{Q}$, one can compute a maximal order $\mathcal{M}$ in $\mathcal{Q}$ using Zassenhaus' Round 2 (see [38]) or Voight's specialized algorithm (see [33, Algorithm 7.10]). Let $\mathfrak{p}$ be a prime ideal in the set N. Then $\mathcal{M}/\mathfrak{p}\mathcal{M} \cong (\mathbb{Z}_K/\mathfrak{p})^{2\times 2}$. By trial and error, one quickly finds some element in the $\mathbb{Z}_K/\mathfrak{p}$-algebra $\mathcal{M}/\mathfrak{p}\mathcal{M}$ with reducible minimal polynomial. From such an element one immediately obtains an explicit isomorphism $\mathcal{M}/\mathfrak{p}\mathcal{M} \cong (\mathbb{Z}_K/\mathfrak{p})^{2\times 2}$ (see [33, Algorithms 4.2 and 4.3] for details).

Let $N' = \prod_{\mathfrak{p}\in N} \mathfrak{p}$. The Chinese Remainder Theorem yields an isomorphism $\varphi\colon \mathcal{M}/N'\mathcal{M} \to R^{2\times 2}$ where $R = \mathbb{Z}_K/N'$. Then $\mathcal{O} := N'\mathcal{M} + \varphi^{-1}\begin{pmatrix} R & R \\ 0 & R \end{pmatrix}$ is a (hereditary) order of discriminant $\prod_{\mathfrak{p}\in D\cup N} \mathfrak{p}$. Finally, for step (3c) one can apply an algorithm by Voight and the first author (see [16, Algorithm 7.10]).

5. Quaternion orders with small type number

Let $\mathcal{Q}$ be a definite quaternion algebra over some number field K. Further, let $\mathcal{O}$ be a Gorenstein order in $\mathcal{Q}$, and let $\mathfrak{p}$ denote some prime ideal of $\mathbb{Z}_K$.

The classification of all Gorenstein orders in $\mathcal{Q}$ having small type numbers is based on the following results.

Lemma 5.1.

1. *If $\mathcal{O}_\mathfrak{p}$ is a Bass order, then $C_\mathfrak{p}(\mathcal{O}) := \mathrm{Id}_\mathfrak{p}(\mathcal{O})$ is a Gorenstein order and $\langle 1, \mathfrak{p}C_\mathfrak{p}(\mathcal{O})\rangle \subsetneq \mathcal{O} \subseteq C_\mathfrak{p}(\mathcal{O})$. Moreover, $\mathcal{O} = C_\mathfrak{p}(\mathcal{O})$ if and only if $\mathcal{O}_\mathfrak{p}$ is hereditary.*
2. *If $\mathcal{O}_\mathfrak{p}$ is not a Bass order, let $C_\mathfrak{p}(\mathcal{O})$ be the Gorenstein closure of $\mathrm{Id}_\mathfrak{p}(\mathcal{O})$. Then $\langle 1, \mathfrak{p}^2C_\mathfrak{p}(\mathcal{O})\rangle \subsetneq \mathcal{O} \subsetneq \langle 1, \mathfrak{p}C_\mathfrak{p}(\mathcal{O})\rangle$.*

Proof. Let $\mathcal{O}$ be any order. Then $\langle 1, \mathfrak{p}\mathrm{Id}_\mathfrak{p}(\mathcal{O})\rangle \subseteq \mathcal{O} \subseteq \mathrm{Id}_\mathfrak{p}(\mathcal{O})$ (see for example [21, Remark 2.8]). A proof of the fact that $\mathcal{O}_\mathfrak{p}$ is hereditary if and only if $\mathcal{O} = \mathrm{Id}_\mathfrak{p}(\mathcal{O})$ is given in [29, Chapter 39]. Further, if $\mathcal{O}$ is a Bass order then $C_\mathfrak{p}(\mathcal{O})$ is Gorenstein by definition. This proves the first claim since $\langle 1, \mathfrak{p}\mathrm{Id}_\mathfrak{p}(\mathcal{O})\rangle$ is not Gorenstein by [6, Proposition 1.3]. Assume now that $\mathcal{O}_\mathfrak{p}$ is not a Bass order and set $\Lambda := \mathrm{Id}_\mathfrak{p}(\mathcal{O})$. By [6, Proposition 1.12], $\Lambda_\mathfrak{p}$ is the unique minimal overorder of $\mathcal{O}_\mathfrak{p}$. Moreover $\Lambda = \langle 1, \mathfrak{p}C_\mathfrak{p}(\mathcal{O})\rangle$ by [6, Proposition 4.2]. This proves the second claim.

Remark 5.2. For any $x \in \mathcal{Q}^*$ we have $C_\mathfrak{p}(x\mathcal{O}x^{-1}) = xC_\mathfrak{p}(\mathcal{O})x^{-1}$. In particular, $\mathrm{N}_{\mathcal{Q}^*}(\mathcal{O}) \subseteq \mathrm{N}_{\mathcal{Q}^*}(C_\mathfrak{p}(\mathcal{O}))$.

Definition 5.3. Given an additional Gorenstein order Λ in $\mathcal{Q}$, we denote by $\mathfrak{C}(\mathcal{O}, \Lambda, \mathfrak{p})$ the set $\{\mathcal{O}' \in \mathrm{Gen}(\mathcal{O}) \mid C_\mathfrak{p}(\mathcal{O}') = \Lambda\}$.

Lemma 5.4. *Let $(\Lambda_1, \ldots, \Lambda_t)$ represent the conjugacy classes of orders in the genus of $C_\mathfrak{p}(\mathcal{O})$. The normalizer $\mathrm{N}_{\mathcal{Q}^*}(\Lambda_i)$ acts on $\mathfrak{C}(\mathcal{O}, \Lambda_i, \mathfrak{p})$ by conjugation. Let $\{\mathcal{O}_{i,1}, \ldots, \mathcal{O}_{i,n_i}\}$ represent the orbits of this action. Then*

$$\{\mathcal{O}_{i,j} \mid 1 \le j \le n_i,\ 1 \le i \le t\}$$

is a complete set of representatives of the conjugacy classes in the genus of $\mathcal{O}$. In particular, $t(\mathcal{O}) \ge t(C_\mathfrak{p}(\mathcal{O})) \ge 1$.

Proof. The fact that $\mathrm{N}_{\mathcal{Q}^*}(\Lambda_i)$ acts on $\mathfrak{C}(\mathcal{O}, \Lambda_i, \mathfrak{p})$ follows immediately from Remark 5.2. Suppose first that $\mathcal{O}_{i,j} = x\mathcal{O}_{k,\ell}x^{-1}$ for some $x \in \mathcal{Q}^*$. Then

$$\Lambda_i = C_\mathfrak{p}(\mathcal{O}_{i,j}) = C_\mathfrak{p}(x\mathcal{O}_{k,\ell}x^{-1}) = xC_\mathfrak{p}(\mathcal{O}_{k,\ell})x^{-1} = x\Lambda_k x^{-1}\,.$$

The choice of $\Lambda_1, \ldots, \Lambda_t$ implies $i = k$. Hence $x \in \mathrm{N}_{\mathcal{Q}^*}(\Lambda_i)$ and thus $j = \ell$. Let $\mathcal{O}' \in \mathrm{Gen}(\mathcal{O})$. Then $C_\mathfrak{p}(\mathcal{O}') \in \mathrm{Gen}(C_\mathfrak{p}(\mathcal{O}))$. Thus $C_\mathfrak{p}(\mathcal{O}') = x\Lambda_i x^{-1}$ for some $1 \leq i \leq t$ and $x \in \mathcal{Q}^*$. After replacing $\mathcal{O}'$ by $x^{-1}\mathcal{O}'x$ we may assume that $C_\mathfrak{p}(\mathcal{O}') = \Lambda_i$. Then $\mathcal{O}'$ is conjugate to $\mathcal{O}_{i,j}$ for some $1 \leq j \leq n_i$.

Finally, we need a lower bound on $\#\mathfrak{C}(\mathcal{O}, \Lambda, \mathfrak{p})$.

Lemma 5.5. *Suppose $\mathcal{O}_\mathfrak{p}$ is not hereditary and $\mathfrak{p}$ does not divide $2\mathcal{D}(C_\mathfrak{p}(\mathcal{O}))$. Then*

$$\#\mathfrak{C}(\mathcal{O}, \Lambda, \mathfrak{p}) \geq \mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})(\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p}) - 1)/2$$

for all $\Lambda \in \mathrm{Gen}(C_\mathfrak{p}(\mathcal{O}))$.

Proof. Let $k = \mathbb{Z}_K/\mathfrak{p}$ and $q = \#k$. Since $\mathfrak{p}$ does not divide $\mathcal{D}(\Lambda)$, we have $\Lambda_\mathfrak{p}/\mathfrak{p}\Lambda_\mathfrak{p} \cong k^{2\times 2}$. Suppose first that $\mathcal{O}_\mathfrak{p}$ is a Bass order. Let $\varphi\colon \mathfrak{C}(\mathcal{O}, \Lambda, \mathfrak{p}) \to k^{2\times 2},\ \mathcal{O}' \mapsto \mathcal{O}'/\mathfrak{p}\Lambda$. Since $\mathcal{O}_\mathfrak{p}$ is not hereditary, we have $[\Lambda\colon \mathcal{O}] = \mathfrak{p}^2$ and thus $e_\mathfrak{p}(\mathcal{O}) \neq 0$. By [6, Proposition 5.4] it follows that

$$\mathfrak{C}(\mathcal{O}, \Lambda, \mathfrak{p}) = \{\mathcal{O}' \subset \Lambda \mid [\Lambda : \mathcal{O}'] = \mathfrak{p}^2 \text{ and } \mathcal{O}'_\mathfrak{p} \text{ is conjugate to } \mathcal{O}_\mathfrak{p}\}\,.$$

In particular, the image of φ is a full $\mathrm{GL}_2(k)$-orbit of some quadratic subalgebra of $k^{2\times 2}$. The stabilizer of any order in the image of φ has size $2(q-1)(q-e_\mathfrak{p}(\mathcal{O}))$, the factor 2 coming from the non-trivial automorphism. Thus

$$\#\mathfrak{C}(\mathcal{O}, \Lambda, \mathfrak{p}) \geq \frac{\#\mathrm{GL}_2(k)}{2(q^2-1)} = q(q-1)/2$$

as claimed.

Suppose now that $\mathcal{O}_\mathfrak{p}$ is not a Bass order. From [6, Proposition 5.4] it follows that $\langle 1, \mathfrak{p}^2(\mathcal{O}_\mathfrak{p})^\# \rangle$ is a local Bass order of discriminant $\mathfrak{p}^2$ and nonzero Eichler invariant. Hence

$$\mathfrak{C}(\mathcal{O}, \Lambda, \mathfrak{p}) \to \mathfrak{C}(\mathcal{O} + \mathfrak{p}^2\mathcal{O}^\#, \Lambda, \mathfrak{p}),\ \mathcal{O}' \mapsto \mathcal{O}' + \mathfrak{p}^2\mathcal{O}'^\#$$

is a conjugation preserving bijection. Thus $\mathfrak{C}(\mathcal{O}, \Lambda, \mathfrak{p}) \geq q(q-1)/2$ by the first part of the proof.

The non-hereditary Gorenstein orders having small type numbers can now be computed using the following algorithm.

Algorithm 5.6.
Input: Some totally real number field K and some bound $B \geq 1$.
Output: A list $\mathcal{L}$. For each genus of definite Gorenstein quaternion orders of type number at most B, precisely one set in the list $\mathcal{L}$ represents the conjugacy classes of orders in that genus.

1. *Initialize $\mathcal{L}$ to be the output of Algorithm 4.5 when applied to K and B.*

2. *For all* $S \in \mathcal{L}$ *and all prime ideals* $\mathfrak{p}$ *such that*

$$\mathfrak{p} \mid 2\mathcal{D}(\Lambda) \text{ for some } \Lambda \in S \text{ or } \sum_{\Lambda \in S} \left\lceil \frac{\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})(\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})-1)}{2\cdot[\mathrm{N}_{\mathcal{Q}^*}(\Lambda):K^*]} \right\rceil \leq B \qquad (5.1)$$

do:

   (a) *For each* $\Lambda \in S$*, compute a set* O_Λ *of orbit representatives of*

$$\{\mathcal{O} \subsetneq \Lambda \mid \mathcal{O} \text{ is an order with } C_{\mathfrak{p}}(\mathcal{O}) = \Lambda\}$$

   under the action of $\mathrm{N}_{\mathcal{Q}^*}(\Lambda)$.

   (b) *For each genus* G *which is represented by at most* B *orders in* $\bigcup_{\Lambda\in S} O_\Lambda$ *but not by any order in* $\mathcal{L}$*, include* $\bigcup_{\Lambda\in S}(O_\Lambda \cap G)$ *to* $\mathcal{L}$.

3. *Return* $\mathcal{L}$.

Proof. We first note that step (2b) ensures that no two sets in $\mathcal{L}$ represent the same genus. Suppose G is a genus of Gorenstein orders with type number at most B and let $\mathcal{O} \in G$. We show that $\mathcal{L}$ contains a set of representatives for the conjugacy classes of G by induction on the number of divisors of $\mathcal{D}(\mathcal{O})$. The case that $\mathcal{O}$ is hereditary is clear. So we may assume that $\mathcal{O}_{\mathfrak{p}}$ is not hereditary for some prime ideal $\mathfrak{p}$. Let $\Lambda := C_{\mathfrak{p}}(\mathcal{O})$. By induction, there exists some $S \in \mathcal{L}$ such that Λ is conjugate to some order in S. From Lemma 5.4 it follows that $t(\Lambda) \leq B$ and Lemma 5.5 shows that the pair $(\mathfrak{p}, S)$ satisfies condition (5.1). Again, by Lemma 5.4, the genus G is represented by $\bigcup_{\Lambda\in S}(O_\Lambda \cap G)$ where O_Λ is as in step (2a) of the algorithm.

We close this section by explaining how one can perform the non-trivial steps of Algorithm 5.6.

Remark 5.7. Let $\mathcal{O}$ be an order in $\mathcal{Q}$. Further, let $\mathrm{Aut}(\mathcal{O}, \mathrm{nr})$ denote the group of all isometries of the $\mathbb{Z}_K$-lattice $\mathcal{O}$ in the quadratic space $(\mathcal{Q}, \mathrm{nr})$. By [9, Appendix IV, Proposition 3], the map

$$\mathrm{N}_{\mathcal{Q}^*}(\mathcal{O})/K^* \to \{\varphi \in \mathrm{Aut}(\mathcal{O}, \mathrm{nr}) \mid \varphi(1) = \det(\varphi) = 1\},\ x \mapsto (y \mapsto xyx^{-1})$$

is an isomorphism of groups. Since $\mathrm{Aut}(\mathcal{O}, \mathrm{nr})$ can be computed using an algorithm of Plesken and Souvignier [28], this gives an effective way to compute $\mathrm{N}_{\mathcal{Q}^*}(\mathcal{O})/K^*$.

In step (2b) one has to test whether two orders $\mathcal{O}, \mathcal{O}'$ are in the same genus. By Section 3, this is equivalent to test whether the corresponding ternary lattices $\mathfrak{L}(\mathcal{O})$ and $\mathfrak{L}(\mathcal{O}')$ are in the same genus. The latter problem was solved by O'Meara, see [23, Theorems 92:2 and 93:28].

If one applies Algorithms 4.5 and 5.6 to the 358 possible base fields from Remark 4.4 with $B = 2$, one gets the following result.

Theorem I.

1. *There are* 4194 *genera of definite Gorenstein quaternion orders of type number one over* 30 *different base fields. The largest field has degree* 5.

2. *There are* 18,538 *genera of definite Gorenstein quaternion orders of type number two over* 75 *different base fields. The largest field has degree* 6.

A complete list of representatives is available electronically from [15].

Remark 5.8. Let $\mathcal{O}$ be a Gorenstein order in a definite quaternion algebra $\mathcal{Q}$ over some number field K. For any ideal $\mathfrak{a} \subsetneq \mathbb{Z}_K$, the order $\langle 1, \mathfrak{a}\mathcal{O}\rangle$ is the unique order with Gorenstein closure $\mathcal{O}$ and Brandt invariant $\mathfrak{a}$. Moreover, the orders $\langle 1, \mathfrak{a}\mathcal{O}\rangle$ and $\mathcal{O}$ have the same type numbers.

Thus Theorem I classifies all orders in definite quaternion algebras over number fields with type number at most 2.

We close this section by mentioning some interesting details of the above classification.

Remark 5.9. The classification in Theorem I shows that $\mathbb{Q}(\sqrt{15})$ is the only base field with nontrivial class group which admits definite ternary quadratic lattices with class number one.

Remark 5.10. Let $K = \mathbb{Q}(\sqrt{3})$ and $\mathcal{Q} = \left(\frac{-1,-1}{K}\right)$. Further let $\mathfrak{p}_2$ be the prime ideal of $\mathbb{Z}_K$ whose norm is 2. Then any maximal order in $\mathcal{Q}$ has type number 2, but any hereditary order in $\mathcal{Q}$ with discriminant $\mathfrak{p}_2$ has type number 1. Thus for classifying all orders with type number h, one really has to start with all hereditary orders of type number h, not just the maximal orders.

Remark 5.11. While the ideal class number of an order $\mathcal{O}$ is an upper bound to the type number of $\mathcal{O}$, these numbers can differ significantly as the following example shows.

Let $K = \mathbb{Q}[x]/(x^5 - 5x^3 + 4x - 1)$. Then $d_K = 38{,}569$ is a prime and K has class number one. In $\mathbb{Z}_K$ there exists a unique prime ideal $\mathfrak{p}_{13}$ of norm 13 and $2\mathbb{Z}_K$ is prime. Let $\mathcal{Q}$ be the definite quaternion algebra over K with discriminant $\mathfrak{p}_{13}$. Up to isomorphism, there exists a unique Gorenstein order $\mathcal{O}$ in $\mathcal{Q}$ with discriminant $2^4 \cdot \mathfrak{p}_{13}^2$ and $e_{\mathfrak{p}_{13}}(\mathcal{O}) = e_{2\mathbb{Z}_K}(\mathcal{O}) = 0$ and $t(\mathcal{O}) = 1$. See [15] for explicit generators of $\mathcal{O}$. From $\mathcal{O}^* = R^*$ and Eichler's mass formula (Theorem 4.2) it follows that the ideal class number of $\mathcal{O}$ is given by

$$2^{-4} \cdot \underbrace{|\zeta_K(-1)|}_{8/3} \cdot 13^2 \cdot 32^4 \cdot (1 - 13^{-2}) \cdot (1 - 32^{-2}) = 29{,}331{,}456\,.$$

Among all definite Gorenstein orders with type number one, this is by far the largest ideal class number, the second largest being 13,369,344.

6. Definite quaternion orders with small ideal class numbers

The classification of all definite quaternion orders with small type numbers also yields the classification of all definite quaternion orders with small ideal class numbers.

To make this statement explicit, we need some more results.

Lemma 6.1. *Let $\mathcal{O} \subseteq \Lambda$ be quaternion orders and let $\{I_1, \ldots, I_h\}$ represent the isomorphism classes of right Λ-ideals.*

1. *The sets $\mathcal{I}(I_i, \mathcal{O}) := \{I \subseteq I_i \mid I \text{ is a right } \mathcal{O}\text{-ideal with } I\Lambda = I_i\}$ are non-empty.*
2. *The group $O_l(I_i)^*$ acts on $\mathcal{I}(I_i, \mathcal{O})$ by left multiplication. Let $\{I_{i,1}, \ldots, I_{i,h_i}\}$ represent the orbits of this action. Then $\{I_{i,j} \mid 1 \leq i \leq h, 1 \leq j \leq h_i\}$ represents the isomorphism classes of right $\mathcal{O}$-ideals.*

In particular, $h(\mathcal{O}) \geq h(\Lambda)$.

Proof. For each prime ideal $\mathfrak{p}$ there exists some $x_\mathfrak{p} \in \mathcal{Q}_\mathfrak{p}$ such that $(I_i)_\mathfrak{p} = x_\mathfrak{p}\Lambda_\mathfrak{p}$ and we can choose $x_\mathfrak{p} = 1$ for all but finitely many places. In particular, there exists some right $\mathcal{O}$-ideal I such that $I_\mathfrak{p} = x_\mathfrak{p}\mathcal{O}_\mathfrak{p}$ locally everywhere. This proves the first assertion. We omit the proof of the second part as it is similar to the proof of Lemma 5.4.

Note that we will apply the above lemma repeatedly to orders satisfying $\mathfrak{p}\Lambda \subseteq \mathcal{O} \subseteq \Lambda$ for some prime ideal $\mathfrak{p}$. In this case, $\mathfrak{p}I_i \subseteq I \subseteq I_i$ for all $I \in \mathcal{I}(I_i, \mathcal{O})$. Thus $\mathcal{I}(I_i, \mathcal{O})$ can be computed easily.

Another method of computing ideal class representatives of quaternion orders is the following neighbor method which has been used by many authors such as Pizer [27], Mestre [20], Kohel [18] and also [16].

Algorithm 6.2. *Input: A definite quaternion order $\mathcal{O}$ over $\mathbb{Z}_K$.*
Output: A set S representing the isomorphism classes of right $\mathcal{O}$-ideals.

1. *Initialize $S = \{\mathcal{O}\}$.*
2. *While* $\mathrm{Mass}(\mathcal{O}) \neq \sum_{I \in S} [\mathcal{O}_l(I)^* : \mathbb{Z}_K^*]^{-1}$ *do:*
   (a) *Pick a random ideal $I \in S$ and some small prime ideal $\mathfrak{p}$ of $\mathbb{Z}_K$.*
   (b) *Compute a random right $\mathcal{O}_l(I)$-ideal $J \subset \mathcal{O}_l(I)$ with* $\mathrm{nr}(J) = \mathfrak{p}$.
   (c) *If JI is not isomorphic to some ideal in S, include JI to S.*
3. *Return S.*

Since we will only be interested in computing ideal class representatives for orders with $h(\mathcal{O}) \leq B$ and B will be very small, Algorithm 6.2 works very well as we can always stop whenever we have found more than B ideal classes.

Remark 6.3. Let $\mathcal{O}$ be an order in a definite quaternion algebra $\mathcal{Q}$ over K such that $h(\mathcal{O}) \leq B$.

1. Let M be a maximal order in $\mathcal{Q}$. Then $h(M) \leq B$.
2. The narrow class number of K is at most B.

Proof. The first statement follows from Lemma 6.1 and the fact that all maximal orders in $\mathcal{Q}$ are in the same genus. For the second statement, we may assume that $\mathcal{O}$ is maximal. The result then follows from a theorem of Swan, see for example [29, Theorem 35.14].

6.1. Gorenstein orders

Let $B \geq 1$ and let $\mathcal{O}$ be a definite Gorenstein quaternion order with $h(\mathcal{O}) \leq B$. Then $t(\mathcal{O}) \leq B$ by Lemma 2.1.

Hence we can simply run over all genera of Gorenstein orders having type number at most B (see Theorem I) and check whether some (and thus every) order in the genus has class number at most B using Algorithm 6.2 or Lemma 6.1.
Note that the conditions of Remark 6.3 can be used to rule out many genera immediately.

This way, one immediately obtains the following result:

Theorem II.

1. *There are* 144 *genera of definite quaternion Gorenstein orders with ideal class number one.*
2. *There are* 268 *genera of definite quaternion Gorenstein orders with ideal class number two and type number one.*
3. *There are* 182 *genera of definite quaternion Gorenstein orders with ideal class number two and type number two.*

A complete list is available electronically from [15].

We checked that our results agree with the list given in [16] when restricted to Eichler orders with type number one. We also found that the order of discriminant 9 in [7] does not have ideal class number one but two. Otherwise [7] agrees with our list when restricted to rational quaternion orders of type number one.

6.2. Non-Gorenstein orders

The classification of all non-Gorenstein with small ideal class number is based on Lemma 6.1.

Algorithm 6.4.
Input: A bound $B \geq 1$ and a definite Gorenstein quaternion order Λ with $h(\Lambda) \leq B$.
Output: A list of all orders with Gorenstein closure Λ and ideal class number at most B.

1. *Initialize $\mathcal{L} = \{\Lambda\}$.*
2. *For all $\mathcal{O} \in \mathcal{L}$ do*
   (a) *Let P be the set of prime ideals $\mathfrak{p}$ of $\mathbb{Z}_K$ such that*
   $$\mathfrak{p} \mid \mathcal{D}(\mathcal{O}) \text{ or } \mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})(\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})^2 - 1) \leq B/\mathrm{Mass}(\mathcal{O}) .$$
   (b) *For all $\mathfrak{p} \in P$ do*
      i. *Compute $h(\langle 1, \mathfrak{p}\mathcal{O}\rangle)$ using Lemma 6.1 or Algorithm 6.2.*
      ii. *If $h(\langle 1, \mathfrak{p}\mathcal{O}\rangle) \leq B$ then include $\langle 1, \mathfrak{p}\mathcal{O}\rangle$ in $\mathcal{L}$.*
3. *Return $\mathcal{L}$.*

PROOF. Let $\tilde{\mathcal{O}}$ be a non-Gorenstein order with $G(\tilde{\mathcal{O}}) = \Lambda$ and $h(\tilde{\mathcal{O}}) \leq B$. Let $\mathfrak{p}$ be a prime ideal divisor of $b(\tilde{\mathcal{O}})$ and set $\mathcal{O} = \langle 1, (b(\tilde{\mathcal{O}})/\mathfrak{p})\Lambda \rangle$. Then $h(\mathcal{O}) \leq B$ by Lemma 6.1 and $\mathcal{O}$ has Gorenstein closure Λ. Thus $\mathcal{O} \in \mathcal{L}$ by induction. Suppose now $\mathfrak{p}$ is coprime to $\mathcal{D}(\mathcal{O})$. Then $e_{\mathfrak{p}}(\tilde{\mathcal{O}}) = 0$ by [6, Propositions 2.1 and 3.1] and $\mathcal{D}(\tilde{\mathcal{O}}) = \mathcal{D}(\mathcal{O}) \cdot \mathfrak{p}^3$. Hence $\mathrm{Mass}(\mathcal{O}) \cdot \mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})(\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{p})^2 - 1) = \mathrm{Mass}(\tilde{\mathcal{O}}) \leq B$. Thus, the algorithm will test $\tilde{\mathcal{O}} = \langle 1, \mathfrak{p}\mathcal{O} \rangle$ in step (2c) at some point.

If one applies Algorithm 6.4 to all Gorenstein orders mentioned in Theorem II, one obtains the following result.

Theorem III.

1. *There are* 10 *conjugacy classes of non-Gorenstein quaternion orders with ideal class number one.*
2. *There are* 20 *conjugacy classes of non-Gorenstein quaternion orders* $\mathcal{O}$ *with ideal class number two such that* $G(\mathcal{O})$ *has ideal class number one.*
3. *There are* 5 *conjugacy classes of non-Gorenstein quaternion orders* $\mathcal{O}$ *with ideal class number two such that* $G(\mathcal{O})$ *has type number one and ideal class number two.*
4. *If* $\mathcal{O}$ *is a non-Gorenstein order with ideal class number two such that* $G(\mathcal{O})$ *has type number two, then* $G(\mathcal{O})$ *is a maximal order in* $\left(\frac{-1,-1}{\mathbb{Q}(\sqrt{3})}\right)$ *and the Brandt invariant of* $\mathcal{O}$ *is the prime ideal of norm* 2 *in* $\mathbb{Z}[\sqrt{3}]$.

A complete list is available electronically from [15].

References

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

[2] H. Brandt. Zur Zahlentheorie der Quaternionen. *Jber. Deutsch. Math. Verein.*, 53:23–57, 1943.

[3] S. Brueggeman and D. Doud. Local corrections of discriminant bounds and small degree extensions of quadratic base fields. *Int. J. Number Theory*, 4:349–361, 2008. See also `http://www.math.byu.edu/~doud/DiscBound.html`.

[4] J. Brzezinski. Arithmetical quadratic surfaces of genus 0, I. *Math. Scand.*, 46:183–208, 1980.

[5] J. Brzezinski. A characterization of Gorenstein orders in quaternion algebras. *Math. Scand.*, 50:19–24, 1982.

[6] J. Brzezinski. On orders in quaternion algebras. *Comm. Algebra*, 11:501–522, 1983.

[7] J. Brzezinski. Definite quaternion orders of class number one. *J. Théor. Nombres Bordeaux*, 7:93–96, 1995.

[8] M. Deuring. *Algebren*, volume 41 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer-Verlag, 1968.

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

[10] M. Eichler. *Quadratische Formen und orthogonale Gruppen*. Springer, 1952.

[11] M. Eichler. Zur Zahlentheorie der Quaternionen-Algebren. *J. Reine u. Angew. Math.*, 195:127–151, 1955. Berichtigung in: *J. Reine u. Angew. Math.* 197 (1957), S. 220.

[12] Benedict H. Gross and Mark W. Lucianovic. On cubic rings and quaternion rings. *J. Number Theory*, 129(6):1468–1478, 2009.

[13] M. Kirschmer. One-class genera of maximal integral quadratic forms. *Journal of Number Theory*, 136C:375–393, 2014.

[14] M. Kirschmer and D. Lorch. Single-class genera of positive integral lattices. *LMS J. Comput. Math.*, 16:172–186, 2013.

[15] M. Kirschmer and D. Lorch. The one-class genera of ternary quadratic forms. see `http://www.math.rwth-aachen.de/~kirschme/orders/`, 2014.

[16] M. Kirschmer and J. Voight. Algorithmic enumeration of ideal classes in quaternion orders. *SIAM J. Comput. (SICOMP)*, 39:1714–1747, 2010.

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

[18] D. R. Kohel. Hecke module structure of quaternions. In *Class field theory – its centenary and prospect (Tokyo, 1998)*, volume 30 of *Adv. Stud. Pure Math.*, pages 177–195. Math. Soc. Japan, 2001.

[19] O. Körner. Traces of Eichler-Brandt matrices and type numbers of quaternion orders. *Proc. Indian Acad. Sci.*, 97:189–199, 1987.

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

[21] G. Nebe. On the radical idealizer chain of symmetric orders. *J. Algebra*, 283:622–638, 2005.

[22] Gordon L. Nipp. Quaternion orders associated with ternary lattices. *Pacific J. Math.*, 53:525–537, 1974.

[23] O. T. O'Meara. *Introduction to Quadratic Forms*. Springer, 1973.

[24] Gordon Pall. On generalized quaternions. *Trans. Amer. Math. Soc.*, 59:280–332, 1946.

[25] M. Peters. Ternäre und quaternäre quadratische Formen und Quaternionenalgebren. *Acta Arith.*, 15:329–365, 1968/1969.

[26] Horst Pfeuffer. Einklassige Geschlechter totalpositiver quadratischer Formen in totalreellen algebraischen Zahlkörpern. *J. Number Theory*, 3:371–411, 1971.

[27] A. Pizer. An algorithm for computing modular forms on $\Gamma_o(N)$. *J. Algebra*, 64(2):340–390, 1980.

[28] W. Plesken and B. Souvignier. Computing isometries of lattices. *J. Symbolic Comput.*, 24:327–334, 1997.

[29] I. Reiner. *Maximal Orders*. Oxford Science Publications, 2003.

[30] R. Scharlau. Martin Kneser's work on quadratic forms and algebraic groups. In *Quadratic forms—algebra, arithmetic, and geometry*, volume 493 of *Contemp. Math.*, pages 339–357. Amer. Math. Soc., Providence, RI, 2009.

[31] M.-F. Vignéras. *Arithmétique des Algebrès de Quaternions*, volume 800 of *Lecture Notes in Mathematics*. Springer-Verlag, 1980.

[32] J. Voight. Enumeration of totally real number fields of bounded root discriminant. In Alfred van der Poorten and Andreas Stein, editors, *Algorithmic number theory (ANTS VIII, Banff, 2008)*, volume 5011 of *Lecture Notes in Comp. Sci.*, pages 268–281. Springer, 2008. See also `http://www.math.dartmouth.edu/~jvoight/nf-tables/index.html`.

[33] J. Voight. Identifying the matrix ring: Algorithms for quaternion algebras and quadratic forms. In K. Alladi, M. Bhargava, D. Savitt, and P. H. Tiep, editors, *Quadratic and Higher Degree Forms*, volume 31 of *Developments in Mathematics*, pages 255–298. Springer New York, 2013.

[34] John Voight. Characterizing quaternion rings over an arbitrary base. *J. Reine Angew. Math.*, 657:113–134, 2011.

[35] G. L. Watson. One-class genera of positive quadratic forms in six variables. unpublished.

[36] G. L. Watson. Transformations of a quadratic form which do not increase the class-number. *Proc. London Math. Soc. (3)*, 12:577–587, 1962.

[37] G. L. Watson. One-class genera of positive quadratic forms in seven variables. *Proc. London Math. Soc. (3)*, 48(1):175–192, 1984.

[38] H. Zassenhaus. On the second round of the maximal order program. In *Applications of number theory to numerical analysis (Proc. Sympos., Univ. Montréal, Montreal, Que., 1971)*, pages 389–431. Academic Press, New York, 1972.