LIFTING PROBLEM FOR UNIVERSAL QUADRATIC FORMS

VÍTEZSLAV KALA AND PAVLO YATSYNA

Abstract. We study totally real number fields that admit a universal quadratic form whose coefficients are rational integers. We show that \( \mathbb{Q}(\sqrt{5}) \) is the only such real quadratic field, and that among fields of degrees 3, 4, 5, and 7 which have principal codifferent ideal, the only one is \( \mathbb{Q}(\zeta_7 + \zeta_7^{-1}) \), over which the form \( x^2 + y^2 + z^2 + w^2 + xy + xz + xw \) is universal. Moreover, we prove an upper bound for Pythagoras numbers of orders in number fields that depends only on the degree of the number field.

1. Introduction

The question which integers can be represented by a given quadratic form has long played a central role in number theory, involving works of mathematicians such as Diophantus, Brahmagupta, Fermat, Euler, and Gauss. Of particular interest have been universal quadratic forms, i.e., positive definite forms that represent all natural numbers. The first example of the sum of four squares \( x^2 + y^2 + z^2 + w^2 \) was followed by many others, including classification of quaternary diagonal universal forms by Ramanujan and Dickson, and culminating in the 15- and 290- theorems of Conway-Schneeberger and Bhargava-Hanke [Bh, BH].

A natural generalization has been the study of universal quadratic forms over number fields \( K \) and their rings of algebraic integers \( \mathcal{O}_K \). When the field has a complex embedding, every quadratic form over \( K \) is indefinite, and so it is comparatively easy to understand which algebraic integers it represents. For example, Siegel [Si3] and Estes-Hsia [EH] considered complex fields with universal sums of 5 and 3 squares (respectively) and characterized them. Hence of particular interest are totally real number fields where one expects to have a rich and hard theory of representations by totally positive definite quadratic forms.

In 1941 Maaß [Ma] used theta series to show that the sum of three squares is universal over the ring of integers of \( \mathbb{Q}(\sqrt{5}) \). Siegel [Si3] then in 1945 proved that the sum of any number of squares is universal only over the number fields \( K = \mathbb{Q}, \mathbb{Q}(\sqrt{5}) \). However, universal forms exist over every totally real number field [HKK], and there have been numerous recent results concerning them, see, e.g., [CKR, Ek, Ki1, Ki2, Cl, Sa, De1, BK1, BK2, Ka1, Ya, KS, CL+] and the references therein.

Almost all of these results involve quadratic forms which do not have rational integers as all of their coefficients. This is not an accident, as indeed Siegel’s result immediately implies that a diagonal positive definite quadratic form with \( \mathbb{Z} \)-coefficients can be universal only over \( K = \mathbb{Q}, \mathbb{Q}(\sqrt{5}) \). This suggests the following natural generalization: when is it possible for a positive definite quadratic form with \( \mathbb{Z} \)-coefficients to be universal over the ring of integers \( \mathcal{O}_K \) of a number field \( K \)? Or more generally, one can consider two (totally real) number fields \( K \subseteq L \) and ask whether there is a quadratic form with \( \mathcal{O}_K \) coefficients that is universal over \( \mathcal{O}_L \). This is sometimes known as the lifting problem for universal quadratic forms over number fields; the main goal of the present article is to consider it for \( \mathbb{Z} \)-forms, i.e., positive definite quadratic form with \( \mathbb{Z} \)-coefficients.

We completely solve this problem for real quadratic fields by proving

Theorem 1. There does not exist a \( \mathbb{Z} \)-form that is universal over a real quadratic number field \( K \), unless \( K = \mathbb{Q}(\sqrt{5}) \).

Over \( \mathbb{Q}(\sqrt{5}) \), there are indeed quite a few universal \( \mathbb{Z} \)-forms, such as \( x^2 + y^2 + z^2 \) [Ma], \( x^2 + y^2 + 2z^2 \) [CKR], \( x^2 + xy + y^2 + z^2 + zw + w^2 \) [De1], \( x^2 + y^2 + z^2 + w^2 + xy + xz + xw \) [De2]. Lee [Le] classified...
all quaternary classical universal forms (recall that a form is classical if all its off-diagonal coefficients are divisible by 2), but his list does not give any other examples that are $\mathbb{Z}$-forms. We are not aware of any classification universal $\mathbb{Z}$-forms over $\mathbb{Q}(\sqrt{5})$ (or any other number field); this is another very interesting open problem.

We then turn our attention to number fields of higher degree, where the situation is much more convoluted.

In the spirit of the study of the minimal number of variables required by a universal form, we first show in Corollary 6 that there are no classical universal $\mathbb{Z}$-forms of rank strictly less than 6 over any totally real number field (of arbitrary degree), except for $\mathbb{Q}$, $\mathbb{Q}(\sqrt{5})$.

We finally focus on the existence of universal $\mathbb{Z}$-forms over certain number fields of small degree.

**Theorem 2.** There does not exist a totally real number field $K$ of degree 1, 2, 3, 4, 5 or 7 which has principal codifferent ideal and a universal $\mathbb{Z}$-form defined over it, unless $K = \mathbb{Q}, \mathbb{Q}(\sqrt{5})$ or $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$.

The $\mathbb{Z}$-form $x^2 + y^2 + z^2 + w^2 + xy + xz + xw$ is universal over $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$.

We prove this result as Theorems 14 and 16. Note that the codifferent is principal for example when $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha$ or when $K$ has class number one.

The limiting assumptions in the theorem come from the tools that we use. First of all, the composition of a $\mathbb{Z}$-form with (twisted) trace form decomposes as a tensor product, and so we study tensor products of positive definite $\mathbb{Z}$-lattices and their minimal vectors. In particular, lattices of $E$-type (which were first introduced by Kitaoka [Kt2]) play a prominent role in Section 4. We use them to show that if certain “additively indecomposable” algebraic integers are represented by a $\mathbb{Z}$-form, then they have to be squares. This in turn for example implies that if a number field possesses a universal $\mathbb{Z}$-form, then it has units of all signatures. Not every lattice is of $E$-type, but in the small degrees considered in Theorem 2 this poses no restrictions.

Our second main tool is Siegel’s formula for the value of Dedekind zeta function at $s = -1$ [Si1, Za], which expresses this value in terms of elements of the codifferent of small trace. In particular, we are interested in elements of trace 1, and these are the only ones that appear in the formula for degrees 2, 3, 4, 5 or 7. When the codifferent is principal, the resulting bound on their number gives (together with the results of Section 4) an estimate on the number of minimal vectors of the trace form. However, this estimate can hold only for very few number fields, which in turn implies the theorem. It is tempting to try to apply Siegel’s formula also for higher degrees by (for example) using elements of trace 2 to deduce the existence of elements of trace 1. Unfortunately, the resulting bounds seem to be too weak to be of much use.

In several of the proofs we use computer calculations to deal with specific number fields and quadratic forms. All of these computations were done in Magma [BCP] and are straightforward.

Note that Theorem 1 is a special case of Theorem 2. However, in the quadratic case we have more explicit control of elements of small trace, and so the proof of Theorem 1 is more elementary and does not require the use of Dedekind zeta function.

The question whether there exists a universal $\mathbb{Z}$-form over a number field not covered by Theorem 2 remains open and may be very hard. Our results provide some clues towards conjecturing that there are perhaps no number fields with $\mathbb{Z}$-forms except for $\mathbb{Q}, \mathbb{Q}(\sqrt{5})$, and $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$, but the evidence is of course quite weak. Even more broadly, the following general lifting problem question remains completely open.

**Question.** Is there a totally real number field $K$ such that there are infinitely many totally real number fields $L \supset K$ that admit a universal quadratic form with $\mathcal{O}_K$-coefficients?

The auxiliary results that we obtain are also useful for the study of Pythagoras numbers of orders $\mathcal{O}$ in totally real fields. While we know that typically not all totally positive integers are sums of squares, we can ask what is the smallest integer $m$ such that if an element is the sum of squares, then it is the sum of at most $m$ squares. This integer $m$ is called the Pythagoras number of the order $\mathcal{O}$ and is known to be always finite, but can be arbitrarily large [Sch]. In the aforementioned article, Scharlau asked whether Pythagoras numbers of orders are bounded by the degree of the corresponding number field. We answer this question affirmatively as Corollary 5.

Let us note that while we state most of our results only for the maximal order $\mathcal{O}_K$ (as it is, arguably, the most interesting case), many of them can probably be quite straightforwardly extended to general
orders, at least the material in Sections 2–4. However, the references that we use typically also deal only with the full ring of integers \( \mathcal{O}_K \), and so this extension would require reproofing all these referenced results in the more general setting.

### Acknowledgments

We thank Tomáš Hejda for our interesting conversations and for his help with computations related to this research.

### 2. Preliminaries

Throughout the article, \( K \) will denote a totally real number field of degree \( d \) over \( \mathbb{Q} \) with the ring of integers \( \mathcal{O}_K \). In Section 3 we will also work with an order \( \mathcal{O} \subset \mathcal{O}_K \), for which we also fix an integral basis \( \omega_1, \ldots, \omega_d \) and denote its group of units by \( \mathcal{O}^\times \).

Let \( \sigma_1 = \text{id}, \sigma_2, \ldots, \sigma_d : K \to \mathbb{R} \) be the (distinct) real embeddings of \( K \). The norm of \( \alpha \in K \) is then \( N(\alpha) = \sigma_1(\alpha) \cdot \sigma_2(\alpha) \cdot \cdots \cdot \sigma_d(\alpha) \), and its trace is \( \text{Tr}(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_d(\alpha) \).

We write \( \alpha \succ \beta \) to mean that \( \sigma_i(\alpha) > \sigma_i(\beta) \) for all \( 1 \leq i \leq d \); moreover, \( \alpha \succeq \beta \) denotes \( \alpha \succ \beta \) or \( \alpha = \beta \).

An algebraic integer \( \alpha \in \mathcal{O}_K \) is totally positive if \( \alpha > 0 \); the semiring of totally positive integers that lie in the order \( \mathcal{O} \) will be denoted \( \mathcal{O}^+ \); moreover, we let \( \mathcal{O}^{x,+} = \mathcal{O}^x \cap \mathcal{O}^+ \). By the signature of \( \alpha \in K \) we mean the \( d \)-tuple of signs of \( \sigma_i(\alpha) \).

We say that \( \alpha \in \mathcal{O}^+ \) is indecomposable if it cannot be decomposed as the sum of two totally positive elements of \( \mathcal{O} \), or equivalently if there is no \( \beta \in \mathcal{O}^+ \) such that \( \alpha \succ \beta \). Indecomposable integers and their norms are quite well studied, especially over real quadratic fields [DS, JK, Ka2].

When an element has sufficiently small norm, then it has to be indecomposable. In particular, every totally positive unit is indecomposable.

**Lemma 3.** a) For all \( \alpha_1, \alpha_2 \in \mathcal{O}^+ \) we have

\[
N(\alpha_1 + \alpha_2)^{1/d} \geq N(\alpha_1)^{1/d} + N(\alpha_2)^{1/d}.
\]

b) If \( \beta \in \mathcal{O}^+ \) has norm \( N(\beta) < 2^d \), then \( \beta \) is indecomposable.

**Proof.** Both parts are easy to show and quite well-known: a) follows by a simple use of Hölder’s inequality, see, e.g., [OM2, 3.1].

b) Assume that \( \beta \) is decomposable as \( \alpha_1 + \alpha_2 \). Then \( 2 > N(\beta)^{1/d} = N(\alpha_1 + \alpha_2)^{1/d} \geq N(\alpha_1)^{1/d} + N(\alpha_2)^{1/d} \geq 1 + 1 \), which is not possible. \( \square \)

We denote by \( \mathcal{O}^V = \{ \beta \in K : \text{Tr}(\beta \mathcal{O}) \subseteq \mathbb{Z} \} \) the codifferent of \( \mathcal{O} \); \( \mathcal{O}^{V,+} \) is the semiring of all totally positive elements of \( \mathcal{O}^V \). Recall that if \( \mathcal{O}_K = \mathbb{Z}[\alpha] \) for some \( \alpha \) with minimal polynomial \( f(x) \in \mathbb{Z}[x] \), then the codifferent is the principal fractional ideal \( \mathcal{O}_K^V = \mathcal{O}_K / f(\alpha) \mathcal{O}_K [\text{Nar, Proposition 4.17}]. \)

We shall often work with positive definite quadratic forms \( Q \in \mathbb{Z}[x_1, \ldots, x_r] \), i.e., \( Q(x) = \sum_{ij \geq j} a_{ij} x_i x_j \) with \( a_{ij} \in \mathbb{Z} \), and refer to such quadratic forms as \( \mathbb{Z} \)-forms from now on; \( r \) is the rank of \( Q \). If \( a_{ij} \in \mathbb{Z} \) for all \( i \neq j \), then we say that \( Q \) is classical \( \mathbb{Z} \)-form (and non-classical, otherwise). For a given quadratic form \( Q \) we can define the bilinear form \( B_Q \in \mathbb{Z}[x_1, \ldots, x_r] \) such that \( Q(x) = B_Q(x, x) \). Furthermore, we can associate to \( Q \) a \( \mathbb{Z} \)-lattice \( (\mathbb{Z}^r, Q) \), and so we will interchangeably talk of \( Q \) as a \( \mathbb{Z} \)-form and as a \( \mathbb{Z} \)-lattice. Unless specified otherwise, throughout the paper \( Q \) will denote a \( \mathbb{Z} \)-form of rank \( r \).

We will sometimes also need to work with quadratic forms over \( \mathcal{O} \), i.e., \( Q(x) = \sum_{ij \geq j} a_{ij} x_i x_j \) with \( a_{ij} \in \mathcal{O} \). Such a form is totally positive definite if \( Q(a) > 0 \) for all \( a \in \mathcal{O}^r, a \neq 0 \).

A \( \mathbb{Z} \)-form \( Q \) represents an element \( \alpha \in \mathcal{O}^+ \) over the order \( \mathcal{O} \) if \( Q(v) = \alpha \) for some \( v \in \mathcal{O}^r \). We say that \( Q \) is universal over \( \mathcal{O} \) if it represents every element \( \alpha \in \mathcal{O}^+ \) over \( \mathcal{O} \). When dealing with the maximal order \( \mathcal{O}_K \), we often just say that \( Q \) is universal (or universal over \( K \) to specify the number field).

Let \( Q_1(x_1, \ldots, x_r), Q_2(y_1, \ldots, y_s) \) be two quadratic forms. Their orthogonal sum is defined as the \((r + s)\)-ary form \( Q_1 \perp Q_2 \). Similarly when \( Q \) is a quadratic form of rank \( r \) and \( m \in \mathbb{N} \), then \( Q^{1,m} = Q \perp Q \perp \cdots \perp Q \) \((m\)-times\) is a quadratic form of rank \( rm \).

Let \( Q \) be a \( \mathbb{Z} \)-form. If it cannot decomposed as the orthogonal sum \( Q = Q_1 \perp Q_2 \) of \( \mathbb{Z} \)-forms \( Q_1, Q_2 \), we say that \( Q \) is an indecomposable form, otherwise that it is decomposable. Each \( \mathbb{Z} \)-form \( Q \)
can be uniquely decomposed as the orthogonal sum of indecomposable \(\mathbb{Z}\)-forms, its indecomposable constituents; we also have analogous notions for totally positive quadratic forms over \(\mathcal{O}\).

3. Pythagoras number

Let us start with a preliminary consideration of the rank of a \(\mathbb{Z}\)-form that represents a given totally positive element \(\alpha\) of an order \(\mathcal{O} \subset K\).

**Proposition 4.** If \(\alpha \in \mathcal{O}^+\) is represented by some \(\mathbb{Z}\)-form over \(\mathcal{O}\), then there exists a \(\mathbb{Z}\)-form \(Q\) of rank at most \(d\) that represents \(\alpha\) over \(\mathcal{O}\). Moreover, there exists a \(d\)-ary positive semidefinite quadratic form \(Q_0\) with \(\mathbb{Z}\)-coefficients that represents \(\alpha\) over \(\mathcal{O}\).

**Proof.** Let \(\omega_1, \ldots, \omega_d\) be an integral basis of the order \(\mathcal{O}\) and let \(Q'\) be a \(\mathbb{Z}\)-form of rank \(r\) that represents \(\alpha\), i.e., \(Q'(v) = \alpha\) for some \(v \in \mathcal{O}^r\). We can write

\[
v = \sum_{i=1}^d v_i \omega_i,
\]

where \(v_i \in \mathbb{Z}\). In particular, we have that

\[
Q'(v) = Q' \left( \sum_{i=1}^d v_i \omega_i \right) = \sum_{i=1}^d \omega_i^2 Q'(v_i) + 2 \sum_{i>j} \omega_i \omega_j B_{Q'}(v_i, v_j).
\]

Consider the \(\mathbb{Z}\)-form \(Q_0\) corresponding to the matrix \((B_{Q'}(v_i, v_j))\). This quadratic form is positive semidefinite, as \(Q'\) is a positive definite quadratic form. The form \(Q_0\) is \(d\)-ary and letting \(w = (\omega_1, \ldots, \omega_d) \in \mathbb{O}^d\), it follows that \(Q_0(w) = \alpha\). Finally, it is easy to prove (e.g., see the discussion at the beginning of [Mo2]) that there is a \(\mathbb{Z}\)-form \(Q\) of rank \(\leq d\) that represents \(Q_0\) (i.e., \(Q_0\) is obtained from \(Q\) after a linear substitution). Thus \(Q\) also represents \(\alpha\) over \(\mathcal{O}\). \(\square\)

This proposition in particular gives an algorithm for deciding whether a given element \(\alpha \in \mathcal{O}\) is represented by some \(\mathbb{Z}\)-form. Namely, it allows us to restrict our attention only to \(\mathbb{Z}\)-forms \(Q\) of rank at most \(d\), and for forms of given rank there is a positive integer \(k = k(d)\) (depending only on \(d\)) such that \(kQ\) is the sum of squares of \(\mathbb{Z}\)-forms [CS, Theorem 1]. Thus we need only to check whether \(k\alpha\) is the sum of squares (e.g., using Lemma 3) and then whether these squares are of the correct shape corresponding to the decomposition of \(kQ\).

Let \(R\) be a ring, and let \(\sum R^2\) denote the set of elements that are sums of squares in \(R\) and \(\sum_{m} R^2\) denote the set of elements that are sums of \(m\) squares in \(R\). Then

\[
P(R) = \inf\{m : \sum_{m} R^2 = \sum R^2\}
\]

is the Pythagoras number of \(R\) (if no such \(m\) exists, then \(P(R) = \infty\)). It is known that if \(K\) is a totally real number field, then \(P(K) \leq 4\) [Si2, Ho]. Furthermore, \(P(\mathcal{O})\) is finite when \(\mathcal{O}\) is an order in \(K\), but it can grow arbitrary large [Sch]. In the aforementioned work, Scharlau asked whether the Pythagoras number of orders is bounded in terms of the field degree. Let us now show that this is indeed so.

**Corollary 5.** Let \(\mathcal{O}\) be an order in a totally real number field of degree \(d\). Then \(P(\mathcal{O}) \leq f(d)\), where \(f\) is some function which depends only on \(d\). If \(d = 2, 3, 4\), or 5, then \(P(\mathcal{O}) \leq d + 3\).

**Proof.** Assume that \(\alpha \in \sum \mathcal{O}^2\), i.e., \(\alpha\) is represented by the \(\mathbb{Z}\)-form \(x_1^2 + \cdots + x_r^2\) over \(\mathcal{O}\) for some \(r\). From Proposition 4 it follows that \(\alpha\) is represented by some \(d\)-ary semidefinite form \(Q_0\). Moreover, from its construction in the proof of Proposition 4, it is clear that this form \(Q_0\) is represented by the original form \(x_1^2 + \cdots + x_r^2\), i.e., that it is the sum of squares of linear forms.

Thus by [Ic, Proposition 3], there exists a function \(f(d)\) such that \(Q_0\) is the sum of \(f(d)\) squares of linear forms. Since \(Q_0\) represents \(\alpha\) over \(\mathcal{O}\), we see that \(\alpha\) is the sum of \(f(d)\) squares of elements of \(\mathcal{O}\). In other words, \(P(\mathcal{O}) \leq f(d)\). For \(d = 2, \ldots, 5\), the bounds are classical and are due to Ko and Mordell [Ko, Mo1]. \(\square\)

The bound for real quadratic number fields is sharp [Pe].

Let us now consider \(\mathbb{Z}\)-forms again. If we restrict to classical ones, we get the following result:
Corollary 6. Let $K \neq \mathbb{Q}(\sqrt{5})$ be a totally real number field of degree $d > 1$ and $\mathcal{O}_K$ the ring of integers in $K$. Then there does not exist a classical $\mathbb{Z}$-form of rank 3, 4 or 5 that is universal over $\mathcal{O}_K$.

Proof. For contradiction assume that $Q$ is a classical $\mathbb{Z}$-form of rank strictly less than 6 that is universal over $\mathcal{O}_K$. By [GS, Theorem 1], $Q$ is the sum of squares of linear forms with $\mathbb{Z}$-coefficients. Since $Q$ is universal over $\mathcal{O}_K$, it follows that $\mathcal{O}_K^+ = \sum \mathcal{O}_K^2$. But this is impossible if $K \neq \mathbb{Q}(\sqrt{5})$ [Si3, Theorem 1].

The previous corollary answers a (very) special case of Kitaoka’s conjecture [Km] that there exist only finitely many totally real number fields which admit a universal ternary quadratic form. Note that the use of [Si3, Theorem 1] was the only place in the proof of Corollary 6 where we used the assumption that $\mathcal{O}_K$ is the maximal order. This probably can be avoided by generalizing Siegel’s theorem to general orders (most likely using essentially the same proof).

4. Forms of $E$-type

Given two (positive definite) $\mathbb{Z}$-lattices $(L_1, Q_1)$ and $(L_2, Q_2)$, we define their tensor product over $\mathbb{Z}$ as $(L_1 \otimes L_2, Q_1 \otimes Q_2)$, so that

$$(Q_1 \otimes Q_2)(v \otimes w) = Q_1(v)Q_2(w),$$

for all $v \in L_1$ and $w \in L_2$. Given bases $\{v_1, \ldots, v_r\}$ of $L_1$ and $\{w_1, \ldots, w_r\}$ of $L_2$, then $\{v_i \otimes w_j\}$ is the canonical basis of the tensor product $L_1 \otimes L_2$. If we denote by $(B_{L_1}(v_i, v_j))$ the matrix corresponding to $L_k$, $k = 1, 2$, then the matrix associated to the lattice $L_1 \otimes L_2$ is $(B_{L_1}(v_i, v_j)) \otimes (B_{L_2}(w_i, w_j))$, i.e., the Kronecker product of matrices (see [Kt1, Chapter 7] for more details on tensor products of lattices).

In general $(L_1 \otimes L_2, Q_1 \otimes Q_2)$ is not a $\mathbb{Z}$-lattice, as the quadratic form $Q_1 \otimes Q_2$ need not be integer valued: for example, the tensor product of the lattice corresponding to the non-classical quadratic form $x^2 + xy + y^2$ with itself will have quadratic form

$$X^2 + Y^2 + Z^2 + W^2 + XY + XZ + YZ + YW + \frac{1}{2}(XW + YZ).$$

However, this happens if and only if we are tensoring two non-classical forms; as long as one of the forms is classical, the tensor product will be a $\mathbb{Z}$-lattice. This will always be the case in our paper.

For a $\mathbb{Z}$-lattice $(L, Q)$, let $\min(L) = \min_{v \neq 0 \in L} Q(v)$ be the minimum of $L$ and

$$\mathcal{M}(L) = \{v \in L : Q(v) = \min(L)\}$$

be the set of minimal vectors of $L$. For two $\mathbb{Z}$-lattices $(L_1, Q_1)$ and $(L_2, Q_2)$ (one of which is classical) we clearly have

$$\min(L_1 \otimes L_2) \leq \min(L_1) \min(L_2).$$

There are examples of this inequality being strict (see [MH, page 47]), but there are important classes of lattices for which one has equality:

Definition 7. We say that a $\mathbb{Z}$-lattice $L$ is of $E$-type if $\mathcal{M}(L \otimes M) \subseteq \{v \otimes w : v \in \mathcal{M}(L), w \in \mathcal{M}(M)\}$ for every classical $\mathbb{Z}$-lattice $M$.

Note that although lattices of $E$-type are usually defined only for classical $\mathbb{Z}$-lattices in the literature (e.g., [Kt1]), we are extending the definition also to non-classical lattices. Nevertheless, all the results concerning lattices of $E$-type, such as Kitaoka’s Theorem 8 below, still hold since a non-classical lattice $L$ is of $E$-type if and only if the classical lattice $2L$ is of $E$-type.

Given two $\mathbb{Z}$-lattices $L_1$ and $L_2$, then of course not all elements of $L_1 \otimes L_2$ are split, i.e., of the form $v_1 \otimes v_2$, $v_i \in L_i$. However, if either of $L_i$ is of $E$-type, then all the minimal vectors of $L_1 \otimes L_2$ are split [Kt1, Lemma 7.1.1].

Although certainly not every lattice is of $E$-type, this is true in several important cases, as the following theorem of Kitaoka shows.

Theorem 8. [Kt1, Theorems 7.1.1, 7.1.2, 7.1.3] Let $Q$ be a $\mathbb{Z}$-form of rank $r$. Then $Q$ is of $E$-type if at least one of the following conditions holds:

- $r \leq 43$,
• \( \min(Q) \leq 6 \),
• \( Q(x_1, \ldots, x_r) = \Tr_{K/Q}(\sum x_i \omega_i)^2 \), where \( K \) is an abelian number field of degree \( r \) with integral basis \( \omega_1, \ldots, \omega_r \).

We will only use the first criterion in this paper; it is an open question what is the smallest rank of a \( Z \)-form not of \( E \)-type.

From now on, we will work only with the maximal order \( O_K \) in a totally real number field \( K \) of degree \( d \), although as we discussed in the Introduction, probably many of our results generalize to the case of general orders.

For \( \delta \in O_K^{\vee,+} \), we can consider the “twisted trace form”, i.e., the unary quadratic form \( T_\delta(x) = \Tr(\delta x^2) \) for \( x \in O_K \). Fixing an integral basis \( \omega_1, \ldots, \omega_d \) for \( O_K \), we identify \( O_K \) with \( \mathbb{Z}^d \). Then we can denote by \( t_\delta \) the \( \mathbb{Z} \)-form of rank \( d \) such that

\[
t_\delta(x_1, \ldots, x_d) = \Tr(\sum x_i \omega_i)^2),
\]

i.e., \( (O_K, t_\delta) = (\mathbb{Z}^d, t_\delta) \) under the identification of \( O_K \) with \( \mathbb{Z}^d \). Since \( \delta \) lies in the codifferent, the form \( T_\delta \) is \( \mathbb{Z} \)-valued, and since \( \delta \) is totally positive, the form \( T_\delta \) is totally positive definite, and so \( t_\delta \) is positive definite. Moreover, we see that the matrix of the form \( t_\delta \) is \( (\Tr(\delta \omega_i \omega_j))_{ij} \), hence all its entries are (rational) integers. In other words, we have verified that \( t_\delta \) is a classical \( \mathbb{Z} \)-form, and so it makes sense to consider the tensor product \( t_\delta \otimes Q \) with any \( \mathbb{Z} \)-form \( Q \). Finally, although \( t_\delta \) of course depends on the choice of the integral basis, we will not need to worry about this, as the basis will be considered fixed throughout the paper. We now have the following classical result on tensor products.

**Lemma 9.** For a \( \mathbb{Z} \)-form \( Q \) of rank \( r \) and \( \delta \in O_K^{\vee,+} \), we have that

\[
(O_K, \Tr(\delta Q)) = (O_K \otimes \mathbb{Z}^r, T_\delta \otimes Q) = (\mathbb{Z}^d \otimes \mathbb{Z}^r, t_\delta \otimes Q).
\]

**Proof.** Given that \( O_K^\vee \), \( O_K \otimes \mathbb{Z}^r \), and \( \mathbb{Z}^d \otimes \mathbb{Z}^r \) are isomorphic as \( \mathbb{Z} \)-modules and that \( T_\delta \) and \( t_\delta \) are clearly equivalent, it suffices to show that \( \Tr(\delta Q) \) is equivalent to \( T_\delta \otimes Q \). It suffices to show that the corresponding bilinear forms are equal on all split vectors; let us give the easy calculation only for the quadratic forms so as not to introduce additional notations.

Let \( \beta \in O_K \), \( w \in \mathbb{Z}^r \), and \( Q(w) = \sum_{i \geq j} a_{ij} w_i w_j \). Then

\[
(T_\delta \otimes Q)(\beta \otimes w) = T_\delta(\beta)Q(w) = \Tr(\delta Q)(\beta \otimes w) = \Tr(\delta Q(\beta w)).
\]

The most important case for us will be when \( t_\delta \) is of \( E \)-type, which we will assume from now; let us summarize all our assumptions for the rest of the paper:

• \( K \) is a totally real number field of degree \( d \) over \( Q \),
• \( O_K \) is the ring of integers in \( K \),
• the quadratic form \( t_\delta \) is of \( E \)-type for every \( \delta \in O_K^\vee \); this is true if \( d \leq 43 \) by Theorem 8,
• \( Q(x) \) is a \( \mathbb{Z} \)-form of rank \( r \), i.e., a positive definite quadratic form with \( \mathbb{Z} \)-coefficients.

Let us now prove a series of auxiliary results that restrict possible number fields \( K \) over which there may exist a universal \( \mathbb{Z} \)-form.

**Proposition 10.** Assume that an indecomposable element \( \alpha \in O_K^\vee \) is represented by \( Q \) over \( O_K \) and satisfies \( \Tr(\delta \alpha) = \min(t_\delta \otimes Q) \) for some \( \delta \in O_K^\vee \). Then \( \alpha \) is a square in \( O_K \) and \( \min(Q) = 1 \).

**Proof.** From the assumption that \( \Tr(\delta \alpha) = \min(t_\delta \otimes Q) \), we conclude that the element \( v \) of \( O_K^\vee \) representing \( \alpha \in O_K \) is a minimal vector of the form \( t_\delta \otimes Q \) (which we identify with \( \Tr(\delta Q) \) by Lemma 9). Since \( t_\delta \) is of \( E \)-type, the minimal vector \( v \in O_K^\vee = O_K \otimes \mathbb{Z}^r \) is split, that is, \( v = \beta \otimes w \), where \( \beta \in O_K \) and \( w \in \mathbb{Z}^r \). We then have

\[
\alpha = Q(v) = \beta^2 Q(w).
\]

Given that \( \alpha \) is indecomposable and \( Q(w) \in \mathbb{Z} \), we conclude that \( Q(w) = 1 \) and that \( \alpha \) is a square. \( \square \)
Corollary 11. If $Q$ is universal over $\mathcal{O}_K$, then every totally positive unit is a square in $\mathcal{O}_K$. Hence there is a unit of every signature in $\mathcal{O}_K$.

Proof. Since totally positive units are indecomposable (Lemma 3), by Proposition 10 it suffices to show that for a given totally positive unit $\varepsilon$ there exists $\delta \in \mathcal{O}_K^{\vee^*}$ such that $\text{Tr}(\delta \varepsilon) = \min(t_\delta \otimes Q)$. Let $w \in \mathcal{O}_K'$ be such that $Q(w) = \varepsilon$. Clearly $\varepsilon^{-1} \in \mathcal{O}_K^{\vee^*}$ and the minimum of $t_{\varepsilon^{-1}}$ is the same as the minimum of $\text{Tr}$, that is $d$. Our assumption that $t_{\varepsilon^{-1}}$ is of $E$-type then implies

$$\min(t_{\varepsilon^{-1}} \otimes Q) = \min(t_{\varepsilon^{-1}}) \min(Q) = d \min(Q) \geq d.$$ 

On the other hand,

$$\text{Tr}(\varepsilon^{-1}Q(w)) = \text{Tr}(1) = 1,$$

and so $\varepsilon$ satisfies the assumptions of Proposition 10 for $\delta = \varepsilon^{-1}$, hence it is a square. Finally, recall the well-known fact [Nar, p. 111, Corollary 3] that every totally positive unit is a square in $\mathcal{O}_K$ if and only if there is a unit of every signature in $\mathcal{O}_K$. \hfill \Box

Lemma 12. Assume that $Q$ is universal over $\mathcal{O}_K$ and let $\alpha \in \mathcal{O}_K^+$. If there exists $\delta \in \mathcal{O}_K^{\vee^*}$ such that $\text{Tr}(\delta \alpha) \leq \text{Tr}(\delta \beta)$ for all $\beta \in \mathcal{O}_K^+$, then $\alpha$ is a unit in $\mathcal{O}_K$.

Of course, when $Q$ is universal, the condition $\text{Tr}(\delta \alpha) \leq \text{Tr}(\delta \beta)$ in the lemma is equivalent to our earlier assumption that $\text{Tr}(\delta \alpha) = \min(t_\delta \otimes Q)$.

Proof. Suppose that $\alpha$ satisfies the assumption, but is not a unit. We can also assume without loss of generality that $\alpha$ is such an element with the smallest possible norm. Moreover, the element $\alpha$ is clearly indecomposable.

Let $v \in \mathcal{O}_K'$ be such that $Q(v) = \alpha$. Since $Q$ is universal, every element $\beta \in \mathcal{O}_K^+$ is represented by $Q$, and so $v \in \mathcal{M}(t_\delta \otimes Q)$. Proposition 10 then implies that $\alpha$ is a square, say $\alpha = \gamma^2$, $\gamma \in \mathcal{O}_K$. Let $\varepsilon \in \mathcal{O}_K^+$ be such that $\varepsilon \gamma > 0$; such a unit exists by Corollary 11. Then $Q$ represents $\varepsilon \gamma$, say, $Q(v') = \varepsilon \gamma$. Denote by $\delta' = \delta \gamma \varepsilon^{-1} \in \mathcal{O}_K^{\vee^*}$. Then

$$\min(t_{\delta'} \otimes Q) \geq \min(t_\delta \otimes Q).$$

But we also have

$$t_{\delta'} \otimes Q(v') = \text{Tr}(\delta' \varepsilon \gamma) = \text{Tr}(\delta \alpha) = \min(t_\delta \otimes Q).$$

Therefore the element $\varepsilon \gamma \in \mathcal{O}_K^+$ has the property that $\text{Tr}(\delta' \varepsilon \gamma) \leq \text{Tr}(\delta' \beta)$ for all $\beta \in \mathcal{O}_K^+$, but has smaller norm than $\alpha$, a contradiction. \hfill \Box

Clearly, if for $\alpha \in \mathcal{O}_K^+$ there exists $\delta \in \mathcal{O}_K^{\vee^*}$ such that $\text{Tr}(\delta \alpha) = \min(t_\delta)$, then $\alpha$ is indecomposable. Unfortunately, the converse implication does not hold, one counterexample being the indecomposable $\zeta_3^2 + \zeta_7^2 - 2 \in K = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$.

Let us now turn our attention to the (non-)existence of universal $\mathbb{Z}$-forms using the results established above. For specific fields, one can often use the following proposition to deal with classical forms, although in general there of course need not exist any non-unit with norm smaller than $2^d$.

Proposition 13. If there exists $\alpha \in \mathcal{O}_K$ such that $1 < |N(\alpha)| < 2^d$, then there does not exist a classical $\mathbb{Z}$-form that is universal over $\mathcal{O}_K$.

Proof. Let $\alpha \in \mathcal{O}_K$ be such that $1 < |N(\alpha)| < 2^d$. If $Q$ is universal over $\mathcal{O}_K$, then by Corollary 11 there are units of all signatures in $\mathcal{O}_K$. Thus, after multiplying by a suitable unit, we can assume that $\alpha > 0$, and furthermore take $\alpha$ to be such element of the smallest possible norm. By Lemma 3, $\alpha$ is indecomposable.

Let $Q'$ be the indecomposable constituent of $Q$ that represents $\alpha$ over $\mathcal{O}_K$. By corollary to Theorem 4 in [Kl13], it follows that $Q'$ is a $\mathbb{Z}$-form (to use this theorem, we need the assumption that $Q$, and thus also $Q'$, is classical).

Let $m \in \mathbb{N}$ be such that $m \text{Tr}(\frac{\alpha}{\delta}) \in \mathbb{Z}$ for all $\beta \in \mathcal{O}_K$. We denote $\delta = \frac{\beta}{\alpha}$, we then have that $\delta \in \mathcal{O}_K^{\vee^*}$. There are now two possible cases:

Either $\text{Tr}(\delta \alpha) = \min(t_\delta \otimes Q')$, in which case by Lemma 12 it follows that $\alpha$ is a unit, a contradiction.

Otherwise there exists $\beta \in \mathcal{O}_K^+$ such that $Q'(w) = \beta$ and $w \in \mathcal{M}(t_\delta \otimes Q')$ so that $\text{Tr}(\delta \alpha) > \text{Tr}(\delta \beta)$. Therefore

$$dm = \text{Tr}(\delta \alpha) > \text{Tr}(\delta \beta) = m \text{Tr}(\frac{\beta}{\alpha}),$$
and so $d > \text{Tr}\left(\frac{\beta}{\alpha}\right)$.

The inequality between arithmetic and geometric means then gives

$$1 > \frac{1}{d} \text{Tr}\left(\frac{\beta}{\alpha}\right) \geq N\left(\frac{\beta}{\alpha}\right)^{1/d},$$

and so $\varrho d > N(\alpha) > N(\beta)$. Thus $\beta$ is indecomposable by Lemma 3.

By Proposition 10 we have that $\min(Q') = 1$, and given that $Q'$ is an indecomposable classical $\mathbb{Z}$-form, this implies that $Q'$ is just a form of one variable, $Q'(x) = x^2$. This form represents $\alpha$, which therefore is a square $\alpha = \gamma^2$, and therefore there exists a non-unit element $\gamma$ with a smaller norm than $\alpha$, contradicting the assumption of minimality of norm of $\alpha$.

$\blacksquare$

**Theorem 1.** There does not exist a $\mathbb{Z}$-form that is universal over a real quadratic number field $K$, unless $K = \mathbb{Q}(\sqrt{5})$.

**Proof.** Let $K = \mathbb{Q}(\sqrt{D})$, where $D \geq 2$ is squarefree integer. Let $O_K = \mathbb{Z}[\omega]$ be the ring of integers in $K$, where $\omega = \sqrt{D}$ or $\frac{1 + \sqrt{D}}{2}$, depending on whether $D \equiv 2, 3 \pmod{4}$ or not. Let $f$ be the minimal polynomial of $\omega$, and $\omega'$ the conjugate of $\omega$. From Corollary 11 it follows that if there exists a universal $\mathbb{Z}$-form over $O_K$, then $O_K$ has units of all signatures. We know that $\mathcal{O}_K^\varphi = \frac{1}{\det(\alpha)}O_K$, and so there exists $\delta > 0$ in $K$ such that $\mathcal{O}_K^\varphi = \delta O_K$. The form $t_\delta$ has rank 2, and so from Theorem 8 it follows that $t_\delta$ is of $E$-type.

Therefore by Lemma 12 we have that all the elements $\alpha \in \mathcal{O}_K^\varphi$ such that $\text{Tr}(\delta \alpha) = 1$ are units. Up to multiplication by a unit, these elements can be written as $\omega + b$, where $b \in (\omega', \omega) \cap \mathbb{Z}$ [Ya, Example 1], and so they form an arithmetic progression of units in $O_K$. The number of such elements is $2|\sqrt{D}| + 1 \left(2 \left\lfloor \frac{1 + \sqrt{D}}{2} \right\rfloor\right)$, resp., and so it clearly grows with $D$.

On other hand, it is known ([New, Theorem 1] and comments there) that there does not exist a non-trivial arithmetic progression with more than 4 consecutive units in real quadratic number fields. Thus, to prove the theorem, it suffices to check the finitely many number fields with $H((\omega', \omega) \cap \mathbb{Z}) \leq 4$. Moreover, when $D \equiv 3 \pmod{4}$, then $N(\omega) = N(\sqrt{D}) = D$, and so $\omega$ is never a unit. For $D \equiv 1 \pmod{4}$, we have the possibilities $D = 5, 13, 17, 21$, and only for $D = 5$ we have that $N(\alpha)$ is a unit. $\blacksquare$

5. **Dedekind zeta function**

Let $K$ be a totally real number field of degree $d$ and let $\Delta_K$ denote the discriminant of $K$. Results of the previous section suggest that elements of the codifferent which have small trace play a key role in the study of universal $\mathbb{Z}$-forms; we shall use Siegel’s formula [Si1] to estimate the number of these elements in terms of Dedekind zeta function $\zeta_K(s)$. We start by reviewing its basic properties following [Za, §1] as reference for all the facts that we mention.

Dedekind zeta function $\zeta_K(s)$ of $K$ for $s \in \mathbb{C}$ is the meromorphic function that for $\text{Re}(s) > 1$ satisfies

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{F(n)}{n^s},$$

where $F(n)$ is the number of ideals in $O_K$ of norm $n$ (and the norm of an ideal $I$ is $N(I) = \#O_K/I$). We can bound $|\zeta_K(s)| \leq \zeta(s)^d$ for $s \in \mathbb{R}$ (where $\zeta(s) = \zeta_\mathbb{Q}(s)$ is Riemann zeta function).

We will be interested in the values at the points $s = 2$ and $s = -1$; clearly $\zeta_K(2) > \zeta(2) > 1$. From the functional equation we see that

$$\zeta_K(-1) = (-1)^d |\Delta_K|^{3/2} \left(\frac{1}{2\pi^2}\right)^d \zeta_K(2).$$

Assume from now on that the degree $d = 2, 3, 4, 5, 7$, and let $b_d = \frac{1}{240}, \frac{-1}{504}, \frac{1}{480}, \frac{-1}{264}, \frac{-1}{24}$, respectively. Then we have

$$\zeta_K(-1) = 2^d b_d \sum_{\alpha \in \mathcal{O}_K^\varphi \atop \text{Tr}(\alpha) = 1} \sigma((\alpha)(\mathcal{O}_K^\varphi)^{-1}),$$
where
\[ \sigma(I) = \sum_{J \in I} N(J) \]

and \((\alpha)\) denotes the fractional ideal \(\alpha \mathcal{O}_K\).

Putting together (5.2) and (5.3), we get
\[ (5.4) \quad \sum_{\alpha \in \mathcal{O}_K^{\mathbb{Z}} / T_{\alpha} = 1} \sigma((\alpha)(\mathcal{O}_K^{\mathbb{Z}})^{-1}) = \frac{(-1)^d}{b_d}|\Delta_K|^{3/2} \left( \frac{1}{4\pi^2} \right)^d \zeta_K(2). \]

Note that \(|\zeta_K(2)|\) is bounded in terms of the degree \(d\) of \(K\).

We can now use this formula to prove our main result that greatly restricts possible number fields of small degrees with a universal \(\mathbb{Z}\)-form.

**Theorem 14.** There does not exist a totally real number field \(K\) of degree 2, 3, 4, 5 or 7, with a principal codifferent ideal and a universal \(\mathbb{Z}\)-form defined over it, unless \(K = \mathbb{Q}(\sqrt{5})\) or \(\mathbb{Q}(\zeta_7 + \zeta_7^{-1})\).

**Proof.** Since \(d \leq 7 < 43\), by Theorem 8 the form \(t_d\) is of \(E\)-type. Hence we can use the results of Section 4. Let us assume that there exists a universal \(\mathbb{Z}\)-form over \(\mathcal{O}_K\). By Corollary 11 there are units of all signatures in \(\mathcal{O}_K\). By the assumption that \(\mathcal{O}_K^{\mathbb{Z}}\) is a principal ideal, there exists some \(\delta \in K\) such that \(\mathcal{O}_K^{\mathbb{Z}} = (\delta)\). Without loss of generality, let \(\delta > 0\).

By Lemma 12, if \(\alpha = \delta \in \mathcal{O}_K^{\mathbb{Z}}\) is such that \(\text{Tr}(\alpha) = 1\), then \(\alpha' \in \mathcal{O}_K^{\mathbb{Z}}\). As then \((\alpha) = (\delta) = \mathcal{O}_K^{\mathbb{Z}}\), we deduce that
\[ \sigma((\alpha)(\mathcal{O}_K^{\mathbb{Z}})^{-1}) = \sigma(\mathcal{O}_K^{\mathbb{Z}}(\mathcal{O}_K^{\mathbb{Z}})^{-1}) = \sigma(\mathcal{O}_K) = 1. \]

Therefore, the left-hand side of (5.4) is equal to the number of \(\alpha \in \mathcal{O}_K^{\mathbb{Z}}\) that have \(\text{Tr}(\alpha) = 1\). As \(\zeta_K(2) \neq 0\), this in particular implies that there is at least one such \(\alpha \in \mathcal{O}_K^{\mathbb{Z}}\) and that \(\min(t_\delta) = 1\).

To a given \(\alpha = \delta \in \mathcal{O}_K^{\mathbb{Z}}\) correspond two minimal vectors of \(t_\delta\), say \(\pm \varepsilon\). Because \(t_\delta(x)\) is a classical quadratic form of rank \(d\), it has at most \(2d\) minimal vectors. Therefore,
\[ d \geq \#\{\alpha \in \mathcal{O}_K^{\mathbb{Z}} | \text{Tr}(\alpha) = 1\} = \sum_{\alpha \in \mathcal{O}_K^{\mathbb{Z}} \atop \text{Tr}(\alpha) = 1} \sigma((\alpha)(\mathcal{O}_K^{\mathbb{Z}})^{-1}). \]

Rearranging equation (5.4) and using the fact that \(\zeta_K(2) > 1\), we get
\[ |\Delta_K| < \left( \frac{4\pi^2}{d} \right)^{2/3}. \]

In the table below we summarize the resulting bounds:

| \(d\) | \(\Delta_K\) | \(\mathcal{O}_K\) |
|-------|-------------|----------------|
| 2     | 5.6...      |                |
| 3     | 51.2...     |                |
| 4     | 742.8...    |                |
| 5     | 14886.9...  |                |
| 7     | 12386158.6... |               |

From online database of number fields (described in [JR]; cf. also [Vo]) we find that there are only a few totally real number fields \(K = \mathbb{Q}(\alpha)\) that satisfy the above bounds:

| \(d\) | Minimal polynomial of \(\alpha\) | \(\Delta_K\) | Narrow class number |
|-------|---------------------------------|-------------|--------------------|
| 2     | \(x^2 - x - 1\)                | 5           | 1                  |
| 3     | \(x^3 - x^2 - 2x + 1\)         | 49          | 1                  |
| 4     | \(x^4 - x^3 - 3x^2 + x + 1\)   | 725         | 1                  |
| 5     | \(x^5 - x^4 - 4x^3 + 3x^2 + 3x - 1\) | 14641     | 1                  |

First, note that there does not exist a number field satisfying the above bound for degree 7. Quadratic, cubic, and quintic number fields correspond to the maximal real subfields of cyclotomic fields. In particular, we have \(\mathbb{Q}(\zeta_5 + \zeta_5^{-1})\), \(\mathbb{Q}(\zeta_7 + \zeta_7^{-1})\), and \(\mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})\), respectively. We need to exclude the cases in degrees \(d = 4\) and 5.
$d = 4$. Let $K = \mathbb{Q}(\beta)$, where $\beta$ is a root of $f(x) = x^4 - x^3 - 3x^2 + x + 1$. Given that $\Delta_f = \Delta_K$ (where $\Delta_f$ is the discriminant of the polynomial $f$), we have $\mathcal{O}_K = \mathbb{Z}[\beta]$. The totally positive integer $\beta + 2$ has norm 11, and so it is indecomposable by Lemma 3, and from Proposition 13 it follows that there is no universal classical $\mathbb{Z}$-form. However, we also need to exclude non-classical forms.

Assume that there is a universal (non-classical) $\mathbb{Z}$-form over $\mathcal{O}_K$. In particular it represents $\beta + 2$, and so by Proposition 4, this element is represented by a $\mathbb{Z}$-form $Q'$ of rank $\leq 4$. But then $2(\beta + 2)$ is represented by the classical $\mathbb{Z}$-form $2Q'$, which in turn is represented as sum of squares [CS, Theorem 1].

Hence it suffices to show that $2(\beta + 2)$ cannot be represented as a sum of squares; assume that $2(\beta + 2) \geq \alpha^2$ for some $\alpha$, without loss of generality $\alpha > 0$. $2(\beta + 2)$ is not a square, and so $2(\beta + 2) = \alpha^2 + \gamma$ with $\gamma > 0$. Then by Lemma 3 we have

$$N(\alpha)^{1/2} + 1 \leq N(\alpha)^{1/2} + N(\gamma)^{1/4} \leq N(2(\beta + 2))^{1/2} = 2 \cdot 11^{1/4},$$

and so $N(\alpha) < 7$. We can easily check in Magma that the only elements of norm less than 11 in $\mathcal{O}_K$ are units, and so if $2(\beta + 2)$ is a sum of squares, then it is a sum of squares of units. From the bound of Lemma 3 it follows that there are at most three summands. The trace of $2(\beta + 2)$ is 18, thus by checking all the combinations of totally positive units of a small trace, we confirm that $2(\beta + 2)$ cannot be represented as a sum of squares.

$d = 5$. Let $\alpha = \zeta_{11} + \zeta_{11}^{-1}$ and $K = \mathbb{Q}(\alpha)$. There (again) exists a totally positive integer of norm 11 in $\mathcal{O}_K$, i.e., $\beta = \alpha + 2$. Given that $N(\beta) = 11 < 2^5$, Lemma 3 implies that $\beta$ is indecomposable. Furthermore, $\beta | 11 | \Delta_K$, and thus $\beta^{-1} \in \mathcal{O}_K^{+*}$ [Nar, Theorem 4.24]. If there exists a universal $\mathbb{Z}$-form $Q$ over $K$, then

$$\min(t_{\beta^{-1}}) \min(Q) = \min(t_{\beta^{-1}} \otimes Q) \leq 5,$$

as $Q$ represents $\beta$. Since $\mathbb{Z}[\alpha] = \mathcal{O}_K$, we compute in Magma the integer matrix corresponding to $t_{\beta^{-1}}$ with respect to the basis $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4\}$:

$$\begin{pmatrix}
5 & -5 & 11 & -13 & 30 \\
-5 & 11 & -13 & 30 & -35 \\
11 & -13 & 30 & -35 & 86 \\
-13 & 30 & -35 & 86 & -94 \\
30 & -35 & 86 & -94 & 252
\end{pmatrix}.$$

Using this, we check (in Magma again) that $\min(t_{\beta^{-1}}) = 5$. Thus by Proposition 10 it follows that $\beta$ is a square, which is impossible given that the norm of $\beta$ is 11. Therefore, there does not exist universal $\mathbb{Z}$-form over $\mathcal{O}_K$. \hfill $\square$

We note that the argument in the proof fails for $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$. Even though we can find an indecomposable element $\beta$ of norm 7, we have that $\min(t_{\beta^{-1}}) = 2$, and so $\beta$ does not correspond to a minimal vector.

6. Existence of universal forms

In the previous sections we have proved in a number of cases that there does not exist a universal $\mathbb{Z}$-form. Let us now turn our attention to the opposite problem, namely, of proving the existence of a universal $\mathbb{Z}$-form over $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$.

**Lemma 15.** Let $K = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$. Then the binary quadratic form $Q = x^2 + xy + y^2$ represents all indecomposable integers of $K$.

**Proof.** All totally positive units are squares in $\mathcal{O}_K$, thus $Q$ represents all of them, as $Q$ represents 1. Using the bounds from Table 1 in [Br], we compute in Magma that the only non-unit indecomposable integer of $K$ (up to multiplication by totally positive units) is an element of norm 7, which can be written as

$$(\zeta_7^2 + \zeta_7^{-2} + 2) - (\zeta_7 + \zeta_7^{-1}) + 1.$$
And we have that
\[ (\zeta_7^2 + \zeta_7^{-2} + 2) - (\zeta_7 + \zeta_7^{-1}) + 1 = (\zeta_7 + \zeta_7^{-1})^2 - (\zeta_7 + \zeta_7^{-1}) + 1 = x^2 + xy + y^2, \]
where \( x = \zeta_7 + \zeta_7^{-1} \) and \( y = -1 \).

This lemma gives us some clues concerning the possible shape of a universal \( \mathbb{Z} \)-form over \( \mathbb{Q}(\zeta_7 + \zeta_7^{-1}) \).

Theorem 16. Let \( K = \mathbb{Q}(\zeta_7 + \zeta_7^{-1}) \). Then the quadratic form \( Q = x^2 + y^2 + z^2 + w^2 + xy + xz + xw + zw \) is universal over \( \mathcal{O}_K \).

Proof. The proof consists in using the mass formula for the class number of \( O \) over \( K \). We will not introduce all the relevant notions here and instead refer the reader to [Si4] as a general reference.

Let \( L \) be the \( \mathbb{Z} \)-lattice corresponding to the \( \mathbb{Z} \)-form \( Q \). In Magma we compute that the class number of \( L \) over \( \mathbb{Q}(\zeta_7 + \zeta_7^{-1}) \) is 1, as the mass of \( L \) is \( 1 / 1152 \) and the order of the automorphism group of \( L \) is 1152. Therefore it suffices to show that \( L \) is universal locally.

There are three archimedean places, all of them real, and \( Q \) clearly represents all positive elements over each of them. Over all the non-dyadic places, \( 2 \) is a unit, and so \( L \) is unimodular. As the rank of \( L \) is 4, by [OMI, 92:1] it follows that \( L \) is universal there too.

Finally, \( 2 \) is inert in \( L \). We directly check that \( L \) represents all the square classes (there are 32 of them) over the 2-adic completion of \( K \). Hence \( Q \) is indeed universal over \( \mathcal{O}_K \). \( \square \)

From Hilbert reciprocity law it follows that there cannot exist a universal quadratic form over \( \mathbb{Q}(\zeta_7 + \zeta_7^{-1}) \) of smaller rank than 4 [EK, Lemma 3].

Let us also remark that another quaternary quadratic form, \( Q' = x^2 + xy + y^2 + z^2 + zw + w^2 \), that was also considered by Deutsch [De1], appears to be universal over \( \mathbb{Q}(\zeta_7 + \zeta_7^{-1}) \) as well. However, this form has class number 2, and so we haven’t proved its universality. Deutsch proved the universality of \( Q' \) over \( \mathbb{Q}(\sqrt{5}) \) and also showed that it is not universal over several real quadratic fields of small discriminant. By our Theorem 1 it now follows that it is not universal over any other real quadratic field.

Finally, let us show a general proposition that provides a way of constructing a universal form from a quadratic form that represents all indecomposable integers.

Proposition 17. Let \( K \) be a totally real field of degree \( d \) and \( Q \) a totally positive definite quadratic form over \( \mathcal{O}_K \) of rank \( r \) that represents all indecomposable integers. Then there is \( m \in \mathbb{N} \) such that \( Q^m \) is universal over \( \mathcal{O}_K \).

In particular, if there is a \( \mathbb{Z} \)-form that represents all indecomposables such as in Lemma 15, then there is a universal \( \mathbb{Z} \)-form over \( \mathcal{O}_K \). So if we were interested only in the existence of a universal \( \mathbb{Z} \)-form, we could have used this proposition instead of the specific (and much stronger!) construction of Theorem 16.

Proof. This is an easy application of [HKK, Theorem 3]. The form \( Q \) represents every indecomposable, and so in particular it represents 1. Thus the form \( Q^m \) represents the sum of squares form \( x_1^2 + \cdots + x_n^2 \).

If \( n \) is sufficiently large, this form is universal over every completion of \( K \), and so by [HKK, Theorem 3] it represents every totally positive integer of large enough trace \( T \) for some \( T \in \mathbb{N} \). Each of the remaining integers of trace \( \leq T \) is the sum of at most \( T \) indecomposables, and so it is represented by the form \( Q^T \). Taking \( m = \max(n, T) \), we conclude that \( Q^m \) is indeed universal. \( \square \)

Let us conclude by noting that in the case of \( K = \mathbb{Q}(\zeta_7 + \zeta_7^{-1}) \), one can do much better than this proposition even without using the mass formula as in Theorem 14. In the proof of Lemma 15, we have seen that, up to multiplication by units, there are exactly two indecomposables, 1 and \( \beta = \zeta_7^2 + \zeta_7^{-2} - \zeta_7 + \zeta_7^{-1} + 3 \). Every totally positive integer \( \alpha \) can be written as a sum of indecomposables, and so also as \( \alpha = 1 \cdot \sigma_1 + \beta \cdot \sigma_2 \), where \( \sigma_1 \) and \( \sigma_2 \) are sums of totally positive units. Every totally positive unit in \( \mathcal{O}_K \) is square, thus \( \sigma_1 \) and \( \sigma_2 \) are sums of squares. Now we can use Corollary 5 to
deduce that $\sigma_1$ and $\sigma_2$ are each sum of just 6 squares. Denoting by $I_6$ the sum of 6 squares quadratic form, we conclude that $\alpha$ is represented by the quadratic form $Q' = I_6 \perp \beta I_6$, which is therefore universal over $K$. Finally, since 1 and $\beta$ are both represented by the $\mathbb{Z}$-form $Q = x^2 + xy + y^2$, we see that $Q'$ is represented by the $\mathbb{Z}$-form $Q^{\perp 12}$, which is thus universal over $K$ as well.

REFERENCES

[Bh] M. Bhargava, On the Conway-Schneeberger Fifteen Theorem, Contemp. Math. 272 (1999), 27-37

[BH] M. Bhargava, J. Hanke, Universal quadratic forms and the 290-theorem, Invent. Math., to appear

[BK1] V. Blomer, V. Kala, Number fields without universal n-ary quadratic forms, Math. Proc. Cambridge Philos. Soc. 159 (2015), 239–252

[BK2] V. Blomer, V. Kala, On the rank of universal quadratic forms over real quadratic fields, Doc. Math. 23 (2018), 15–34

[BCP] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language

[CKR] W. K. Chan, M.-H. Kim, S. Raghavan, On the rank of universal quadratic forms over real quadratic fields

[CI] W. K. Chan, M. I. Icaza, Positive definite almost regular ternary quadratic forms over totally real number fields

[CL+] M. Čech, D. Lachman, C. Playoust, The Magma algebra system. I. The user language

[Br] H. Brunotte, The Computation of a Certain Metric Invariant of an Algebraic Number Field, Math. Comput 38 (1982), 627–632

[CL+] M. Čech, D. Lachman, J. Svoboda, M. Tinková, K. Zemková, Universal Quadratic Forms and Indecomposables over Biquadratic Fields, arXiv:1802.07811

[CI] W. K. Chan, M. I. Icaza, Positive definite almost regular ternary quadratic forms over totally real number fields, Bull. Lond. Math. Soc. 40 (2008), 1025-1037.

[CKR] W. K. Chan, M.-H. Kim, S. Raghavan, Ternary universal integral quadratic forms, Japan. J. Math. 22 (1996), 263–273

[CS] J. H. Conway, N. J. A. Sloane, Low-dimensional lattices. V. Integral coordinates for integral lattices

[De1] J. I. Deutsch, Universality of a non-classical integral quadratic form over $\mathbb{Q}(\sqrt{15})$, Acta Arith. 136 (2009), 229-242

[De2] J. I. Deutsch, A non-classical quadratic form of Hessian discriminant $4$ is universal over $\mathbb{Q}(\sqrt{3})$, Integers 16 (2016), # A19

[DS] A. Dress, R. Scharlau, Indecomposable totally positive numbers in real quadratic orders, J. Number Theory 46 (1992), 211–232

[EA] A. G. Earnest, Universal and regular positive quadratic lattices over totally real number fields, Integral quadratic forms and lattices (Seoul, 1998), Contemp. Math. 249 (1999), Amer. Math. Soc., 17-27.

[EK] A. G. Earnest, A. Khosravani, Universal positive quaternary quadratic lattices over totally real number fields, Mathematika 44 (1997), 342–347

[EH] D. R. Estes, J. S. Hsia, Sums of three integer squares in complex quadratic fields, Proc. Amer. Math. Soc. 89 (1983), 211–214

[Ho] D. Hoffmann, Pythagoras numbers of fields, J. Amer. Math. Soc. 12 (1999), 839–848

[HKK] J.S. Hsia, Y. Kitaoka, M. Kneser, Representations of positive definite quadratic forms, J. Reine Angew. Math. 301 (1978), 132–141

[Ic] M.I. Icaza, Sums of squares of integral linear forms, Acta Arith. 74 (1996), 231–240

[JK] S. W. Jang, B. M. Kim, A refinement of the Dress-Scharlau theorem, J. Number Theory 158 (2016), 234–243

[JR] J. W. Jones, D. P. Roberts, A database of number fields

[Ka1] V. Kala, Universal quadratic forms and elements of small norm in real quadratic fields

[Ka2] V. Kala, Norms of indecomposable integers in real quadratic fields, J. Number Theory 166 (2016), 193–207

[KS] V. Kala, J. Svoboda, Universal quadratic forms over multiquadratic fields, Ramanujan J., to appear, arXiv:1703.03185

[Ki1] B. M. Kim, Finiteness of real quadratic fields which admit positive integral diagonal septenary universal forms, Manuscr. Math. 99 (1999), 181–184

[Ki2] B. M. Kim, Universal octonary diagonal forms over some real quadratic fields, Commentarii Math. Helv. 75 (2000), 410–414

[Km] M. H. Kim, Recent developments on universal forms, In Algebraic and arithmetic theory of quadratic forms, In Algebraic and arithmetic theory of quadratic forms, 344 of Contemp. Math., pages 215228. Amer. Math. Soc., Providence, RI, 2004.

[Kt1] Y. Kitaoka, Arithmetic of quadratic forms, Cambridge Tracts in Mathematics 106, Cambridge University Press 1993

[Kt2] Y. Kitaoka, Tensor products of positive definite quadratic forms, Proc. Japan Acad. 52 (1976), 498–500

[Kt3] Y. Kitaoka, Scalar extension of quadratic lattices, Nagoya Math. J., 66, (1977), 139–149

[Ko] C. Ko, On the representation of a quadratic form as a sum of squares of linear forms, Q. J. Math. 1 (1937), 81–98

[Le] Y.M. Lee, Universal forms over $\mathbb{Q}(\sqrt{5})$, Ramanujan J. 16 (2008), 97–104

[Ma] H. Maaß, Über die Darstellung total positiver Zahlen des Körpers $R(\sqrt{5})$ als Summe von drei Quadraten, Abh. Math. Sem. Univ. Hamburg 14 (1941), 185–191

[MH] J. Milnor, D. Husemoller, Symmetric Bilinear Forms, Springer-Verlag, New York, 1973

[Mo1] L.J. Mordell, On the representation of a binary quadratic form as a sum of squares of linear forms, Math. Z. 35 (1932), 1–15
LIFTING PROBLEM FOR UNIVERSAL QUADRATIC FORMS 13

[Mo2] L.J. Mordell, *The Representation of a Definite Quadratic Form as a Sum of Two Others*, Ann. Math. 38 (1937), 751–757

[Nar] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, 3rd Edition, Springer-Verlag, Berlin, 2004

[New] M. Newman, *Units in arithmetic progression in an algebraic number field*, Proc. Amer. Math. Soc. 43, (1974), 266–268

[OM1] O. T. O’Meara, *Introduction to Quadratic Forms*, Springer-Verlag, Berlin, 1973

[OM2] O. T. O’Meara, *On indecomposable quadratic forms*, J. Reine Angew. Math. 317, (1980), 120–156

[Pe] M. Peters, *Summen von Quadraten in Zahlringen*, J. Reine Angew. Math. 268/269, (1974), 318–323

[Sa] H. Sasaki, *Quaternary universal forms over $Q[\sqrt{13}]$*, Ramanujan J. 18 (2009), 73–80

[Sch] R. Scharlau, *On the Pythagoras number of orders in totally real number fields*, J. Reine Angew. Math. 316, (1980), 208–210

[Si1] C. L. Siegel, *Berechnung von Zetafunktionen an ganzzahligen Stellen*, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II (1969), 87–102

[Si2] C. L. Siegel, *Darstellung total positiver Zahlen durch Quadrate*, Math. Z. 11 (1921), 246–275

[Si3] C. L. Siegel, *Sums of m-th powers of algebraic integers*, Ann. of Math. 46 (1945), 313–339

[Si4] C. L. Siegel, *Über die analytische Theorie der quadratischen Formen III.*, Ann. of Math. 38 (1937), 212–291

[Vo] J. Voight, *Enumeration of totally real number fields of bounded root discriminant*, in Algorithmic number theory 5011, Springer, Berlin 2008, 268–281

[Ya] P. Yatsyna, *A lower bound for the rank of a universal quadratic form with integer coefficients in a totally real field*, Comment. Math. Helvet., to appear, arXiv:1808.01441

[Ze] D. Zagier, *On the values at negative integers of the zeta-function of a real quadratic field*, Enseignement Math. (2), 22 (1976), 55–95

Charles University, Faculty of Mathematics and Physics, Department of Algebra, Sokolovská 83, 18600 Praha 8, Czech Republic

E-mail address: vita.kala@gmail.com

E-mail address: pvyatsyna@gmail.com