Kala, Vitezslav; Yatsyna, Pavlo

On Kitaoka's conjecture and lifting problem for universal quadratic forms

Published in:
Bulletin of the London Mathematical Society

DOI:
10.1112/blms.12762

Published: 01/04/2023

Document Version
Peer-reviewed accepted author manuscript, also known as Final accepted manuscript or Post-print

Please cite the original version:
Kala, V., & Yatsyna, P. (2023). On Kitaoka's conjecture and lifting problem for universal quadratic forms. *Bulletin of the London Mathematical Society*, *55*(2), 854-864. https://doi.org/10.1112/blms.12762

ON KITAOKA'S CONJECTURE AND LIFTING PROBLEM FOR UNIVERSAL QUADRATIC FORMS

VÍTĚZSLAV KALA AND PAVLO YATSYNA

Abstract. For a totally positive definite quadratic form over the ring of integers of a totally real number field K, we show that there are only finitely many totally real field extensions of K of a fixed degree over which the form is universal (namely, those that have a short basis in a suitable sense). Along the way we give a general construction of a universal form of rank bounded by $D(\log D)^{d-1}$, where d is the degree of K over $\mathbb{Q}$ and D is its discriminant. Furthermore, for any fixed degree we prove (weak) Kitaoka's conjecture that there are only finitely many totally real number fields with a universal ternary quadratic form.

1. Introduction

Let F be a totally real number field with the ring of integers $\mathcal{O}_F$. A classical question asks when an algebraic integer $\alpha \in \mathcal{O}_F$ can be written as the sum of squares of elements of $\mathcal{O}_F$; an obvious necessary condition is that α is totally positive (i.e., all its conjugates are positive). This condition is also sufficient in the basic case $F = \mathbb{Q}$ by the four square theorem, and when $F = \mathbb{Q}(\sqrt{5})$. However, Siegel [Si2] proved that these are the only such totally real number fields, motivating the study of two natural generalizations.

The first one asks how many squares are required, provided that α is indeed representable as the sum of squares. This leads to the Pythagoras number, a constant well-studied also in other settings (see, e.g., [Le]). Yet, in the case of the ring of integers of a totally real number field, all that is known in general is that the Pythagoras number is finite [Sc] and bounded by the degree of the field [KY], but can grow arbitrarily large [Sc] (in the non-totally real case, the Pythagoras number ≤ 5 [Pe2]; for some small degree cases see [Pe1, Ti, KRS]). Furthermore, Siegel [Si1] proved that for each number field F there exists $m \in \mathbb{N}$ such that all totally positive integers divisible by m can be represented as the sum of squares.

The second generalization is to universal forms over F, i.e., quadratic forms that represent all the totally positive elements of $\mathcal{O}_F$. The smallest possible rank of a universal form is three, and this can happen only in number fields of even degree [EK]. Even for them, Kitaoka formulated his influential conjecture that there are only finitely many number fields F admitting a ternary universal form. The only known examples are in real quadratic fields [CKR] and Kitaoka's conjecture remains unproven, even though it seems that universal forms typically must have large ranks [BK, Ka, KKP, KT, Ya].

Indecomposable algebraic integers turned out to be one of the key tools in the recent advances on this topic. In this short paper, we first prove in Theorem 5 that each indecomposable has norm smaller or equal to the discriminant of F, significantly extending previous results in the quadratic and cubic cases [DS, KT, TV], as well as improving the previous general bound [Br], which is typically much worse than ours, as it depends on the regulator. Our result is also a substantial step towards answering [Nar, Problem 53].

Theorem 5 directly implies a construction of a universal quadratic form – giving the first completely general result in the train of thought started by B. M. Kim [Ki1]. The following theorem is more precisely formulated and proved as Theorem 6.

Date: October 5, 2022.

2010 *Mathematics Subject Classification.* 11E12, 11E20, 11E25, 11H06, 11R04.

Key words and phrases. universal quadratic form, totally real number field, extension of scalars, indecomposable algebraic integer.

Both authors were supported by the project PRIMUS/20/SCI/002 from Charles University. V.K. was supported by Czech Science Foundation (GAČR) grant 21-00420M and Charles University Research Centre program UNCE/SCI/022. P.Y. was supported by the Academy of Finland (grants 336005 and 351271, PI C. Hollanti), and by MATINE, Ministry of Defence of Finland (grant 2500M-0147, PI C. Hollanti).

Theorem 1. *Let F be a totally real number field of degree $d = [F : \mathbb{Q}]$ and discriminant Δ. Then there is a universal quadratic form over $\mathcal{O}_F$ of rank $\ll \Delta(\log \Delta)^{d-1}$.*

In the case when the number field F is monogenic (i.e., has integral power basis), contains no proper subfields, and has units of all signatures, there is also a lower bound [Ya, Theorem 1.4] on the rank of universal quadratic forms that depends on Δ. In particular, for such real quadratic number fields [Ya, Theorem 5.4], and for the simplest cubic fields [KT, Theorem 1.1], the rank of the universal quadratic form is $\gg \Delta^{1/2}$ or $\gg \Delta^{1/4}$, depending on whether the quadratic form is classical or not, respectively.

Then we move on to the main goal of this note, namely, to proving several finiteness results concerning the (non-)universality of certain quadratic forms (and, slightly more generally, $\mathcal{O}_F$-lattices).

Theorem 2. *Let F be a totally real number field, L an $\mathcal{O}_F$-lattice, and $d, m \in \mathbb{N}$. There are at most finitely many totally real number fields $K \supset F$ of degree $d = [K : \mathbb{Q}]$ such that $L \otimes \mathcal{O}_K$ represents all elements of $m\mathcal{O}_K^+$.*

This theorem includes, as a significant special case, a new result on the sum of squares, for one can take $F = \mathbb{Q}$ and $L = \mathbb{Z}^r$ equipped with the quadratic form $Q = x_1^2 + \cdots + x_r^2$. It also extends the previous results on the *lifting problem* (i.e., whether a form can be universal over a larger number field, see [KY] and *potentially universal quadratic forms* in [XZ]), and partly resolves an open question formulated in [KY]: As Corollary 9 we show that a given quadratic form is universal only over finitely many totally real number fields of degree d.

We further apply these results to prove a weak version of Kitaoka's conjecture:

Theorem 3. *For each $d \in \mathbb{N}$, there are only finitely many totally real number fields K of degree $d = [K : \mathbb{Q}]$ over which there is a ternary universal $\mathcal{O}_K$-lattice.*

For *classical* lattices, this theorem was previously proved by B. M. Kim in an unpublished manuscript [Ki2].

We begin the article by introducing notation and basic tools in the next section. Section 3 considers indecomposables and contains the proofs of Theorems 5 and 6. Theorem 2 is then proved in Section 4 as Theorem 7. There we also cover the cases of representations of $m\mathcal{O}_F^+$ by the sums of squares (Corollary 8) and the lifting problem for positive definite quadratic forms over $\mathbb{Z}$ (Corollary 9). Finally, Theorem 3 is proved in the last section as Theorem 12. There we use the existence of "universality criterion sets" (as introduced in [EKK]), which was a folklore result [Km], whose full proof appeared in the work of Chan and Oh [CO].

Acknowledgments

We are grateful to Byeong Moon Kim for sharing his manuscript [Ki2] with us, to Giacomo Cherubini and Dayoon Park for several useful discussions and comments, and to Jakub Krásenský for suggesting the specific formulation of Theorem 6 and for a number of helpful corrections. We are also thankful to the anonymous referee for several very useful suggestions.

2. Preliminaries

Let F be a totally real number field of degree d over $\mathbb{Q}$ and let $\mathcal{O}_F$ denote its ring of integers. Let $\sigma_1, \sigma_2, \dots, \sigma_d : K \hookrightarrow \mathbb{R}$ be the distinct real embeddings of F and let $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_d) : F \hookrightarrow \mathbb{R}^d$ be the corresponding embedding of F into the Minkowski space.

The *norm* and *trace* are $\mathrm{N}_{F/\mathbb{Q}}, \mathrm{Tr}_{F/\mathbb{Q}} : F \to \mathbb{R}$, $\mathrm{N}_{F/\mathbb{Q}}(\alpha) = \sigma_1(\alpha) \cdots \sigma_d(\alpha)$ and $\mathrm{Tr}_{F/\mathbb{Q}}(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_d(\alpha)$.

As a height function on F, we will primarily work with the *house* (also called *the maximum modulus of conjugates*), defined as $\overline{|\alpha|}_F = \overline{|\alpha|} = \max_i(|\sigma_i(\alpha)|)$. For $v = (v_1, \dots, v_n)^t \in F^n$, we further let $\overline{|v|}_F = \overline{|v|} = \max_j \overline{|v_j|}_F$. We have $\overline{|\alpha|} \geq 1$ for all $\alpha \in \mathcal{O}_F \setminus \{0\}$.

An element $\alpha \in F$ is *totally positive* if $\sigma_i(\alpha) > 0$ for all i. The set of all totally positive elements of F is denoted F^+. For $\alpha, \beta \in F$, α is *totally greater than* β (denoted $\alpha \succ \beta$) if $\alpha - \beta \in F^+$. If E is a subset of F, then $E^+ = E \cap F^+$.

An element $\alpha \in \mathcal{O}_F^+$ is *indecomposable* if there does not exist $\beta \in \mathcal{O}_F^+$ such that $\alpha \succ \beta$.

For a positive integer m, let $\sum^m \mathcal{O}_F^{(2)} = \{\sum^m \alpha_i^2 : \alpha_i \in \mathcal{O}_F\}$; also $\sum^\infty \mathcal{O}_F^{(2)} = \bigcup_m \sum^m \mathcal{O}_F^{(2)}$. We say that $n = \mathcal{P}(\mathcal{O}_F)$ is the *Pythagoras number* of $\mathcal{O}_F$ if it is the smallest positive integer (or ∞) such that $\sum^n \mathcal{O}_F^{(2)} = \sum^\infty \mathcal{O}_F^{(2)}$.

We follow the lattice-related terminologies and notations from [OM]. Specifically, let V be r-ary *quadratic space* over F with its symmetric *bilinear form* $B : V \times V \longrightarrow F$ and the corresponding *quadratic form* Q, i.e., $B(v,v) = Q(v)$. The *Gram matrix* of vectors $v_1, \ldots, v_k \in V$ is the $k \times k$ symmetric matrix $(B(v_i, v_j))$.

A *(quadratic) $\mathcal{O}_F$-lattice* L on V is a finitely generated $\mathcal{O}_F$-submodule of V such that $FL = V$, which we view equipped with the restrictions of B and Q; we often denote this by saying that (L, Q) is an $\mathcal{O}_F$-lattice. The *rank* of L is r.

The *scale* of L is $\mathfrak{s}L = \{B(v,w) : v, w \in L\}$, while the $\mathcal{O}_F$-module generated by $Q(L) = \{Q(v) : v \in L\}$, denoted by $\mathfrak{n}L$, is called the *norm* of L. Throughout the work we assume that $\mathfrak{n}L \subset \mathcal{O}_F$ (i.e., $Q(v) \in \mathcal{O}_F$ for all $v \in L$); then $\mathfrak{s}L \subset \frac{1}{2}\mathcal{O}_F$ and $2B(v,w) \in \mathcal{O}_F$ for all $v, w \in L$. We say that the scale is *integral* if $\mathfrak{s}L \subset \mathcal{O}_F$, in this case we say that the lattice is *classical*. By [OM, 81:3] there is a basis $v_1, \ldots, v_r$ of V and fractional ideals $\mathfrak{a}_i \subset F$ such that $L = \mathfrak{a}_1 v_1 + \cdots + \mathfrak{a}_r v_r$. The *volume* of L is $\mathfrak{v}L = \mathfrak{a}_1^2 \cdots \mathfrak{a}_r^2 \det(B(v_i, v_j))$.

The quadratic form Q (or, the lattice L) is *totally positive definite* if $Q(v) \succ 0$ for all non-zero $v \in V$. In that case we have the *Cauchy–Schwarz inequality* $Q(v)Q(w) \succeq B(v,w)^2$ for all $v, w \in V$ (that easily follows from the usual Cauchy–Schwarz inequality for quadratic forms over $\mathbb{R}$). We say that L (or Q) *represents* an algebraic integer α if there exists $v \in L$ such that $Q(v) = \alpha$. We say that a totally positive lattice is *universal* (over $\mathcal{O}_F$ or over F) if it represents all the elements of $\mathcal{O}_F^+$.

Given a field extension $K \supset F$ and an $\mathcal{O}_F$-lattice (L, Q), we have the *tensor product* $\mathcal{O}_K$-lattice $L \otimes \mathcal{O}_K$ defined as $L \otimes \mathcal{O}_K = \mathcal{O}_K\mathfrak{a}_1 v_1 + \cdots + \mathcal{O}_K\mathfrak{a}_r v_r$ equipped with the natural extensions of B and Q, e.g., if $x = \sum x_i v_i \in L \otimes \mathcal{O}_K$, then $Q(x) = x^t M x$ where we identify x with the column vector $(x_1, \ldots, x_r)^t$ and $M = (B(v_i, v_j))$ is the Gram matrix. If we moreover identify $V = F^r$, then $L \otimes \mathcal{O}_K \subset K^r$.

For a quadratic form $Q : \mathcal{O}_F^r \to \mathcal{O}_F$, we apply all the preceding terminology when it applies to the free $\mathcal{O}_F$-lattice $(\mathcal{O}_F^r, Q)$.

Convention. Whenever we talk about an *$\mathcal{O}_F$-lattice* throughout the paper, we always mean a totally positive definite quadratic $\mathcal{O}_F$-lattice satisfying $\mathfrak{n}L \subset \mathcal{O}_F$.

We shall also use the common asymptotic notations: If $f(x), g(x)$ are two positive real functions, then $f \ll g$ (and $g \gg f$) if there is a constant $C > 0$ such that $f(x) < Cg(x)$ for all x (that lie in the domains of f, g), and $f \asymp g$ if $f \ll g$ and $g \ll f$.

Let us now begin with the following lemma:

Lemma 4. *Let $K \supset F$ be totally real number fields and (L, Q) an $\mathcal{O}_F$-lattice. There is $C = C_{L,F} \in \mathbb{R}^+$ such that for all $v \in L \otimes \mathcal{O}_K$ we have $\overline{|v|}_K^2 \le C\overline{|Q(v)|}_K$.*

Note that the constant $C = C_{L,F}$ above depends on L, Q, F, and the choice of pseudo-basis $L = \mathfrak{a}_1 u_1 + \cdots + \mathfrak{a}_r u_r$, but **not** on K.

Proof. This follows from Rayleigh–Ritz Theorem (Rayleigh quotient) [HJ, Theorem 4.2.2], that says: *If M is a symmetric matrix with entries in $\mathbb{R}$ and $\lambda_1(M)$ is its smallest eigenvalue, then*

$$\lambda_1(M) \sum v_k^2 \le v^t M v \tag{1}$$

for any vector $v = (v_1, \ldots, v_d)^t \in \mathbb{R}^d$. Let $L = \mathfrak{a}_1 u_1 + \cdots + \mathfrak{a}_r u_r$ and let $M = (B(u_i, u_j))$ be the corresponding Gram matrix. Define $M_i = \sigma_i(M)$ for each embeddings of F in $\mathbb{R}$. In particular, M_i is a symmetric matrix with coefficients in F. For each embedding $\sigma_i : F \hookrightarrow \mathbb{R}$, let $\sigma_{ij} : K \hookrightarrow \mathbb{R}$ be all its extensions.

It now suffices to consider the inequality (1) with $C = \frac{1}{\lambda}$, where $\lambda = \min_i \lambda_1(M_i)$ (note that $\lambda > 0$, for L is totally positive definite, which implies that each matrix M_i is positive definite). That is,

$$\begin{aligned}\overline{|Q(v)|}_K &= \max_{i,j} \sigma_{ij}(v^t M v) = \max_{i,j} \left((\sigma_{ij} v)^t M_i (\sigma_{ij} v)\right) \ge \max_{i,j} \left(\lambda_1(M_i) \left(\sum (\sigma_{ij} v_k)^2\right)\right) \\ &\ge \frac{1}{C} \max_{i,j} \sigma_{ij} \left(\sum v_k^2\right) \ge \frac{1}{C} \overline{|v|}_K^2. \end{aligned}$$

□

3. Indecomposables

Let us start by proving a general bound on the norm of indecomposables.

Theorem 5. *Let K be a totally real number field with discriminant Δ. For every element $\alpha \in \mathcal{O}_K^+$ with $\mathrm{N}_{K/\mathbb{Q}}(\alpha) > \Delta$ there is $\beta \in \mathcal{O}_K$ such that $\alpha \succ \beta^2$. In particular, no such element α is indecomposable.*

Proof. Let K be of degree d over $\mathbb{Q}$. In the Minkowski space associated to K, consider the box defined by $|x_i| \le \sqrt{\sigma_i(\alpha)} - \varepsilon$, where σ_i are the embeddings of K into $\mathbb{R}$ and $\varepsilon > 0$ is small enough that

$$\prod_{i=1}^{d} (\sqrt{\sigma_i(\alpha)} - \varepsilon) > \sqrt{\Delta}.$$

This is possible because $\prod_{i=1}^d \sqrt{\sigma_i(\alpha)} = \sqrt{\mathrm{N}_{K/\mathbb{Q}}(\alpha)} > \sqrt{\Delta}$. Thus the volume of the box is bigger than $2^d\sqrt{\Delta}$. By Minkowski theorem (e.g., see Theorem III in Chapter III in [Ca]) there exists a non-zero lattice point in this box, which corresponds to an algebraic integer $\beta \in \mathcal{O}_K$. We have that $\sqrt{\sigma_i(\alpha)} > \sigma_i(\beta)$, and thus $\sigma_i(\alpha) > \sigma_i(\beta^2)$ for all i. Therefore $\alpha \succ \beta^2$, as was required to show. □

As an important corollary, we get the following general construction of a universal quadratic form.

Theorem 6. *Let K be a totally real number field of degree $d = [K : \mathbb{Q}]$ whose discriminant is Δ and Pythagoras number of the ring of integers $\mathcal{O}_K$ is $\mathcal{P}(\mathcal{O}_K) = P$. Fix a set of representatives $\mathcal{S}$ for classes of elements $\alpha \in \mathcal{O}_K^+$, $\mathrm{N}_{K/\mathbb{Q}}(\alpha) \le \Delta$, up to multiplication by squares of units in $\mathcal{O}_K$. Then the diagonal quadratic form*

$$Q = \sum_{\alpha \in \mathcal{S}} \alpha x_\alpha^2 + y_1^2 + \cdots + y_P^2$$

is universal and has rank $\#\mathcal{S} + P \ll \Delta(\log \Delta)^{d-1}$ (where the implied constant depends only on d).

Proof. Let $\gamma \in \mathcal{O}_K^+$. If $\mathrm{N}_{K/\mathbb{Q}}(\gamma) > \Delta$, then we can repeatedly use Theorem 5 to find elements $\gamma_0 \in \mathcal{O}_K^+, \beta_1, \dots, \beta_t \in \mathcal{O}_K$ such that $\gamma = \gamma_0 + \beta_1^2 + \cdots + \beta_t^2$ and $\mathrm{N}_{K/\mathbb{Q}}(\gamma_0) \le \Delta$. Then $\gamma_0 = \alpha x^2$ for some $\alpha \in \mathcal{S}$ and $x \in \mathcal{O}_K^\times$, and the sum of squares $\beta_1^2 + \cdots + \beta_t^2$ is represented as $y_1^2 + \cdots + y_P^2$ by the definition of the Pythagoras number P.

Now it remains to estimate $\#\mathcal{S} + P$: The size of $\mathcal{S}$ is at most 2^d-times the number of principal ideals of norm $\le \Delta$ (for in $\mathcal{S}$, we are considering elements up to *squares* of units). Counting all ideals I of norm $N(I) \le \Delta$, it is quite easy to see that their number is $\ll \Delta(\log \Delta)^{d-1}$:

Let a_n be the number of ideals in $\mathcal{O}_K$ of norm n and let b_n be defined by $\zeta(s)^d = \sum_{n \ge 1} b_n n^{-s}$ (where $\zeta(s)$ is the Riemann zeta-function). For each rational prime p, there are at most d prime ideals that divide p (and whose norm is a power of p), and so by comparing the Euler products of $\zeta_K(s) = \sum_{n \ge 1} a_n n^{-s}$ and $\zeta(s)^d$, we see that $a_n \le b_n$ for all n. Thus it suffices to obtain an upper bound for $\sum_{1 \le n \le \Delta} b_n$, which by the Tauberian theorem is easily seen to be $\ll \Delta(\log \Delta)^{d-1}$ as $\Delta \to \infty$ (where the implied constant depends only on d), as we wanted. (For the required background in analytic number theory, see, e.g., [Nar, Chapter 7 and Appendix II]).

As for the Pythagoras number P, in [KY, Corollary 3.3] we proved that P is bounded from above by a bound that depends only on the degree $d = [K : \mathbb{Q}]$. Specifically, the proof of [KY, Corollary 3.3] established that $P \le g(d)$, where $g(d)$ is the *g-invariant*, i.e., the smallest rational integer such that any quadratic form with $\mathbb{Z}$-coefficients of rank d that is represented by the sum of any number of squares is represented by the sum of $g(d)$ squares. Recently Beli, Chan, Icaza, and Liu [BC+, Theorem 1.1] showed an upper bound for the g-invariant that is exponential in $\sqrt{d}$, i.e., $g(d) \le c_1 \exp(c_2\sqrt{d})$. In any case, as our implied constant depends on d, we have $P \ll 1$. □

Note that the number of ideals in $\mathcal{O}_K$ of norm $\le X$ grows as $\asymp X$ as $X \to \infty$ (and an analogue of this is known even for *principal* ideals). But here the constants do depend on K, and in fact, even using finer versions of this asymptotics, it seems that for $X = \Delta$, the error term is often larger than the main term. Therefore in Theorem 6 we had to use the weaker bound $\ll \Delta(\log \Delta)^{d-1}$.

4. Weak Lifting Problem

We are now ready to prove our first main theorem concerning the general lifting problem.

Theorem 7. *Let F be a totally real number field, L an $\mathcal{O}_F$-lattice, and $d, m \in \mathbb{N}$. There are at most finitely many totally real number fields $K \supset F$ of degree $d = [K : \mathbb{Q}]$ such that $L \otimes \mathcal{O}_K$ represents all elements of $m\mathcal{O}_K^+$.*

Proof. Let C be the constant (for F and L) from Lemma 4 and take a totally real number field $K \supset F$ of degree $d = [K : \mathbb{Q}]$. Let $X > 1$ be such that

- $X > \overline{|\alpha_i|}_F = \overline{|\alpha_i|}_K$ for all elements α_i in a fixed integral basis of F, and
- $X > 3Cm$.

Consider the subfield $E \subset K$ generated (as a field) by all the elements $\alpha \in \mathcal{O}_K$ such that $\overline{|\alpha|}_K < X$. By our choice of X, we have $F \subset E$. There are only finitely many algebraic integers of bounded degree and house (in particular, of degree $\leq d$ and house $< X$), and so they generate only finitely many possible number fields E. In particular, there are (at most) finitely many possible fields K for which $E = K$ can happen. Excluding these Ks, we can assume that E is a proper subfield of K.

Let $Y \geq X$ be the minimum of $\overline{|\alpha|} = \overline{|\alpha|}_K$ for $\alpha \in \mathcal{O}_K \setminus \mathcal{O}_E$ (the minimum exists, as the set of algebraic integers of bounded degree and $\overline{|\alpha|}$ is finite). Let $\alpha \in \mathcal{O}_K \setminus \mathcal{O}_E$ be such that $\overline{|\alpha|} = Y$, and let $k \in \mathbb{Z}$ be the smallest rational integer such that $k + \alpha \succ 0$. We have $\overline{|k+\alpha|} < 2\overline{|\alpha|} + 1 \leq 3\overline{|\alpha|}$.

If $L \otimes \mathcal{O}_K$ represents all elements from $m\mathcal{O}_K^+$, then there exists $v \in L \otimes \mathcal{O}_K \subset K^r$ such that $Q(v) = m(k+\alpha)$. If $v = (v_j) \in E^r \subset K^r$, then $Q(v) \in E$ (as (L, Q) is an $\mathcal{O}_F$-lattice and $F \subset E$), and so also $\alpha \in E$, a contradiction. Thus there is j such that $v_j \notin E$, and so $\overline{|v|} \geq \overline{|v_j|} \geq Y$.

By Lemma 4 we then have

$$Y^2 \leq \overline{|v|}^2 \leq C\overline{|Q(v)|} = Cm\overline{|k+\alpha|} < 3Cm\overline{|\alpha|} = 3YCm.$$

Thus $X \leq Y < 3Cm$, which is a contradiction with our choice of X. □

Note that one could also consider the natural extension of Theorem 7 to representations of $\beta\mathcal{O}_K^+$ for fixed $\beta \in \mathcal{O}_F^+$. The corresponding statement follows immediately from the theorem, as $\beta\mathcal{O}_K^+ \subset m\mathcal{O}_K^+$ for $m = N_{F/\mathbb{Q}}(\beta)$.

Corollary 8. *For each $m, d \in \mathbb{N}$, there are only finitely many totally real number fields K of degree $d = [K : \mathbb{Q}]$ such that all elements in $m\mathcal{O}_K^+$ are sums of squares.*

Proof. The Pythagoras number of the ring of integers is bounded in terms of degree of the field extension [KY, Corollary 3.3], i.e., *there is a function $g(d)$ such that $\mathcal{P}(\mathcal{O}_F) \leq g(d)$ whenever $[F : \mathbb{Q}] = d$.* Thus, it suffices to consider the sum of a bounded number of squares $Q = x_1^2 + \cdots + x_{g(d)}^2$. Then the corollary is immediate from the previous theorem applied to the free $\mathcal{O}_F$-lattice $(\mathcal{O}_F^{g(d)}, Q)$. (See the end of the proof of Theorem 6 for more information on $g(d)$.) □

We get the subsequent strong addendum to Theorems 1.1 and 1.2 in [KY]:

Corollary 9. *For each $d, r \in \mathbb{N}$, there are only finitely many totally real number fields K of degree $d = [K : \mathbb{Q}]$ such that there is a positive definite quadratic form over $\mathbb{Z}$ of rank r that is universal over K.*

Proof. Let Q be a positive definite quadratic form over $\mathbb{Z}$ of rank r. By Theorem 1 in [CS] (possibly first taking $2Q$ to make the form classical), *there exists $m \in \mathbb{Z}$ (depending on r) such that mQ is the sum of squares of linear forms with $\mathbb{Z}$-coefficients.* Thus, if Q is universal over K, then every element of $m\mathcal{O}_K^+$ is the sum of squares. By Corollary 8 there are only finitely many such fields of given degree d. □

5. Weak Kitaoka's conjecture

Let us use the results obtained in the previous section to prove our Theorem 3. However, first we need to recall a (mostly well-known) fact concerning sublattices.

Lemma 10. *Let F be a totally real number field. Let $d, r \in \mathbb{N}$ and let ℓ be an $\mathcal{O}_F$-lattice of rank r. There exists a positive integer m such that for every totally real extension $K \supset F$ of degree d and $\mathcal{O}_K$-lattice M of rank r satisfying $\ell \otimes \mathcal{O}_K \subset M$ we have $mM \subset \ell \otimes \mathcal{O}_K$.*

Proof. Let $L_K = \ell \otimes \mathcal{O}_K$. By definition, we have $(\mathfrak{v}\ell)\mathcal{O}_K = \mathfrak{v}L_K$, and [OM, 82:11] gives

$$(\mathfrak{v}\ell)\mathcal{O}_K = \mathfrak{v}L_K = \mathfrak{a}^2\mathfrak{v}M, \tag{2}$$

where $\mathfrak{a}$ is an integral ideal (equal to the product of the *invariant factors* of L_K in M [OM, §81D]). As we assume that all lattices satisfy $\mathfrak{n}M \subset \mathcal{O}_K$, we can use [OM, 82:19] to obtain $\mathfrak{v}(2M) = 2^r(\mathfrak{v}M) \subset \mathcal{O}_K$.

By (2), the integral ideal $\mathfrak{v}(2M)$ divides $2^r(\mathfrak{v}\ell)\mathcal{O}_K$, and so there are only finitely many possibilities for it. [OM, 103:4] says that *there are only finitely many $\mathcal{O}_K$-lattices of given volume and integral scale.* As the $\mathcal{O}_K$-lattice $2M$ has integral scale and bounded volume, there are also only finitely many possibilities for M.

Thus there are only finitely many possibilities for the (subgroup) index $(M : L_K)$; taking m to be the least common divisor of all the possible indices, we get $mM \subset (M : L_K)M \subset L_K$ as we wanted. □

Our final tool will be the notion of a "universality criterion set":

Definition 11. Let K be a totally real number field. A *universality criterion set in K* is a finite set $S_K \subset \mathcal{O}_K^+$ such that if an $\mathcal{O}_K$-lattice represents all elements of S_K, then it is universal.

Note that in the definition, S_K is not required to be minimal or unique. As an example, let us mention that by the 290-Theorem by Bhargava and Hanke [BH] we can take $S_{\mathbb{Q}} = \{1, \dots, 290\}$.

The existence of a universality criterion set in any totally real number field was probably first mentioned by Kim, Kim, and Oh [KKO] (see also [Km, Section 6]), with the name coming from [EKK]. The existence was recently proved by Chan and Oh [CO, Corollary 5.8].

For a matrix M, let $K(M)$ be the number field extension of K generated by all the entries of M.

Theorem 12. *For each $d \in \mathbb{N}$, there are only finitely many totally real number fields K of degree $d = [K : \mathbb{Q}]$ over which there is a ternary universal $\mathcal{O}_K$-lattice.*

Proof. Most of the proof will consist of inductively defining finite sets $\mathcal{A}_i, \mathcal{F}_i, \mathcal{H}_i$ (throughout the proof, we view also the empty set as finite) of number fields of degree $\le d$ with the following property:

If K is a number field of degree $\le d$ that admits a ternary universal $\mathcal{O}_K$-lattice L, then

(1) $K \in \mathcal{A}_i$, or
(2) there is $F \in \mathcal{H}_i, F \subsetneq K$ with a ternary universal $\mathcal{O}_F$-lattice ℓ such that $\ell \otimes \mathcal{O}_K \subset L$, or
(3) there are $k_j \in \mathcal{F}_j, j = 0, \dots, i$, such that $k_0 \subsetneq k_1 \subsetneq \cdots \subsetneq k_i \subsetneq K$.

Let us denote the set of number fields K satisfying item *(2)* (item *(3)*, resp.) by $\mathcal{B}_i$ ($\mathcal{C}_i$, resp.). We do not claim (yet) that $\mathcal{B}_i$ or $\mathcal{C}_i$ is necessarily finite.

Let us start the construction with $\mathcal{A}_0 = \mathcal{H}_0 = \emptyset$ and $\mathcal{F}_0 = \{\mathbb{Q}\}$. Note that if K is a number field with a ternary universal $\mathcal{O}_K$-lattice, then $K \neq \mathbb{Q}$, and so K satisfies item *(3)* for $i = 0$, as $\mathbb{Q} = k_0 \subsetneq K$.

Let further $K \notin \mathcal{A}_i$ admit a ternary universal $\mathcal{O}_K$-lattice L. We do not need to consider fields $K \in \mathcal{B}_i$ (i.e., satisfying item *(2)* above), for we will have $\mathcal{H}_{i+1} \supset \mathcal{H}_i$ by our construction, and so $\mathcal{B}_i \subset \mathcal{B}_{i+1}$.

Thus consider $K \in \mathcal{C}_i$ and accordingly take some $k = k_i \in \mathcal{F}_i$ such that $k \subsetneq K$. Let S_k be the corresponding universality criterion set. The universal $\mathcal{O}_K$-lattice L represents all elements $s \in S_k$, i.e., there are $v_s \in L$ such that $Q(v_s) = s$. Let $M = (B(v_s, v_t))$ be the corresponding Gram matrix. Further let $B(v_s, v_t) = m_{st}/2$ for $s \neq t$ and $m_{ss} = s \in S_k$ so that $m_{st} \in \mathcal{O}_K$ for all s, t.

As L is totally positive definite, for each $s, t \in S_k$ we have the Cauchy–Schwarz inequality $m_{st}^2 \preceq 4st$, and so $\operatorname{Tr}_{K/\mathbb{Q}}(m_{st}^2) \le \max_{s,t\in S_k} 4 \operatorname{Tr}_{K/\mathbb{Q}}(st) \le \max_{s,t\in S_k} 4d \operatorname{Tr}_{k/\mathbb{Q}}(st)$ is bounded. Since m_{st} is an algebraic integer of degree $\le d$, there are only finitely many possibilities for it (that do not depend on K). Thus there are also only finitely many possibilities for the field $k(M) \subset K$.

Let us next distinguish three cases according to whether we have equality in any of the inclusions $k \subset k(M) \subset K$:

a) To deal with the case $k(M) = K$, *let $\mathcal{A}_{i+1}$ be the union of $\mathcal{A}_i$ with all these fields $k(M)$ as k runs through $\mathcal{F}_i$.* Therefore if moreover $K \notin \mathcal{A}_{i+1}$, then $k(M)$ is a proper subfield of K.

b) Assume now that $k(M) = k$ and consider the $\mathcal{O}_k$-span ℓ of all vectors v_s for $s \in S_k$ (as a subset of L). Then ℓ (equipped with the restrictions of B, Q) is an $\mathcal{O}_k$-lattice (for all entries of the Gram matrix M lie in k) that represents all elements of S_k. By the assumption that S_k is a universality criterion set for k, the $\mathcal{O}_k$-lattice ℓ is universal over k.

Then $\ell \otimes \mathcal{O}_K$ is a sublattice of the ternary lattice L, and so the rank of ℓ is also 3 (no universal lattice has rank ≤ 2, and rank of $\ell \leq$ rank of $L = 3$). Thus we can *let $\mathcal{H}_{i+1}$ be the union of $\mathcal{H}_i$ with all these fields $k(M) = k$ as k runs through $\mathcal{F}_i$.*

c) Finally, we are left with the case $k \subsetneq k(M) \subsetneq K$. Then *let $\mathcal{F}_{i+1}$ be the set of these fields $k_{i+1} = k(M)$*, i.e., $k \subsetneq k_{i+1} = k(M) \subsetneq K$.

Thus we have defined all the needed sets for $i+1$. As there were only finitely many possibilities for $k(M)$ (which did not depend on K but only on $k \in \mathcal{F}_i$), each of the new sets $\mathcal{A}_{i+1}$, $\mathcal{F}_{i+1}$, $\mathcal{H}_{i+1}$ is still finite, as we wanted.

Having constructed the desired sets $\mathcal{A}_i, \mathcal{F}_i, \mathcal{H}_i$, let us now consider them when $i = d$. Note that no field K satisfies *(3)* for $i = d$ (i.e., $\mathcal{C}_d = \emptyset$), for otherwise we would have $d = [K : \mathbb{Q}] \geq [k_d : \mathbb{Q}] + 1 \geq [k_{d-1} : \mathbb{Q}] + 2 \geq \cdots \geq [k_0 : \mathbb{Q}] + d + 1$, which is impossible.

There are finitely many fields K in the finite set $\mathcal{A}_d$, and so it remains to consider fields $K \in \mathcal{B}_d$. We will prove that there are also finitely many of them.

The set $\mathcal{H}_d$ is finite, and by Corollary 1 in [Ea], there are only finitely many ternary universal lattices over a fixed field $F \in \mathcal{H}_d$. Thus there are finitely many pairs (F, ℓ) that can appear in item *(2)*.

By Lemma 10 there is $m \in \mathbb{N}$ depending on (F, ℓ) and d, but not on the specific field K or lattice L, such that if $\ell \otimes \mathcal{O}_K \subset L$ (which is true by *(2)*), then $mL \subset \ell \otimes \mathcal{O}_K$.

As L is universal, $\ell \otimes \mathcal{O}_K$ represents all elements of $m\mathcal{O}_K^+$. But by Theorem 7, there are only finitely many such fields K (and for each of them, there are again at most finitely many ternary universal lattices L). Thus, for a fixed pair (F, ℓ), there are at most finitely many extensions (K, L) (of given degree d). Thus also item *(2)* gives only finitely many fields K, concluding the proof. □

Finally, note that essentially the same proof yields the following corollary for fields of odd degree (over which there never exists a ternary universal lattice). For *classical* lattices, this result was proved by Kim [Ki2].

Corollary 13. *For each* odd $d \in \mathbb{N}$*, there are only finitely many totally real number fields K of degree $d = [K : \mathbb{Q}]$ over which there is a quaternary universal $\mathcal{O}_K$-lattice.*

Proof. The proof is almost verbatim the same as the proof of Theorem 12, replacing "ternary" by "quaternary" everywhere in the proof (and adding the requirement that all number fields considered have odd degree). As K is assumed to have odd degree, all its subfields also have odd degree, and so do not admit a ternary universal lattice [EK, Lemma 3]. Thus the lattice ℓ considered in part b) of the preceding proof must have rank 4. Finally, towards the end of the proof one uses [EK, Theorem 1] instead of [Ea, Corollary 1]. □

References

[BC+] C. N. Beli, W. K. Chan, M. I. Icaza, J. Liu, *On a Waring's problem for integral quadratic and Hermitian forms*, Trans. Amer. Math. Soc. **371** (2019), 5505–5527

[BH] M. Bhargava, J. Hanke, *Universal quadratic forms and the 290-theorem*, preprint

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

[Br] H. Brunotte, *Zur Zerlegung totalpositiver Zahlen in Ordnungen totalreeller algebraischer Zahlkörper*, Arch. Math. (Basel) 41 (1983), 502–503

[Ca] J. W. S. Cassels, *An introduction to the geometry of numbers*, Springer-Verlag, Berlin, 1997

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

[CO] W. K. Chan, B.-K. Oh, *Can we recover an integral quadratic form by representing all its subforms?*, arxiv:2201.08957

[CS] J. H. Conway, N. J. A. Sloane, *Low-dimensional lattices. V. Integral coordinates for integral lattices*, Proc. Roy. Soc. London Ser. A **426** (1989), 211–232

[DS] A. Dress, R. Scharlau, *Indecomposable totally positive numbers in real quadratic orders*, J. Number Theory **14** (1982), 292–306

[Ea] A. G. Earnest, *Universal and regular positive quadratic lattices over totally real number fields*, in 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

[EKK] N. D. Elkies, D. M. Kane, S. D. Kominers, *Minimal $\mathcal{S}$-universality criteria may vary in size*, J. Théor. Nombres Bordeaux **25** (2013), 557–563

[HJ] R. A. Horn, C. R. Johnson, *Matrix analysis*, Cambridge University Press, Cambridge, 2013

[Ka] V. Kala, *Universal quadratic forms and elements of small norm in real quadratic fields*, Bull. Aust. Math. Soc. **94** (2016), 7–14
[KT] V. Kala, M. Tinková, *Universal Quadratic Forms, Small Norms, and Traces in Families of Number Fields*, Int. Math. Res. Not. IMRN (to appear), doi:10.1093/imrn/rnac073
[KY] V. Kala, P. Yatsyna, *Lifting problem for universal quadratic forms*, Adv. Math., **26**, (2020), 107497, 24 pp.
[Ki1] B. M. Kim, *Universal octonary diagonal forms over some real quadratic fields*, Comment. Math. Helv. **75** (2000), 410–414
[Ki2] B. M. Kim, *Positive Universal Forms over Totally Real Fields*, unpublished manuscript (2003)
[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, Contemp. Math. **344** (2004). Amer. Math. Soc., 215–228
[KKO] B. M. Kim, M.-H. Kim, B.-K. Oh, *A finiteness theorem for representability of quadratic forms by forms*, J. Reine Angew. Math. **581** (2005), 23–30
[KKP] B. M. Kim, M.-H. Kim, D. Park, *Real quadratic fields admitting universal lattices of rank 7*, J. Number Theory **233** (2022), 456–466
[KRS] J. Krásenský, M. Raška, E. Sgallová, *Pythagoras number in biquadratic fields*, Expo. Math. (to appear), doi:10.1016/j.exmath.2022.06.002
[Le] D. B. Leep, *A historical view of the Pythagoras numbers of fields*, in Quadratic forms—algebra, arithmetic, and geometry, Contemp. Math. **493** (2009), Amer. Math. Soc., 271–288
[Nar] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, 3rd Edition, Springer-Verlag, Berlin, 2004
[OM] O. T. O'Meara, *Introduction to Quadratic Forms*, Springer-Verlag, Berlin, 1973
[Pe1] M. Peters, *Quadratische Formen über Zahlringen*, Acta Arith. **24** (1973), 157–165
[Pe2] M. Peters, *Summen von Quadraten in Zahlringen*, J, reine angew. Math. **268** (1974), 318–323
[Sc] 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, *Darstellung total positiver Zahlen durch Quadrate*, Math. Z. **11** (1921), 246–275
[Si2] C. L. Siegel, *Sums of m-th powers of algebraic integers*, Ann. of Math. **46** (1945), 313–339
[Ti] M. Tinková, *On the Pythagoras number of the simplest cubic fields*, arxiv:2101.11384
[TV] M. Tinková, P. Voutier, *Indecomposable integers in real quadratic fields*, J. Number Theory **212** (2020), 458–482
[XZ] F. Xu, Y. Zhang, *On indefinite and potentially universal quadratic forms over number fields*, Trans. Amer. Math. Soc. (to appear), arxiv:2004.02090
[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. **94** 2019, 221–239

Charles University, Faculty of Mathematics and Physics, Department of Algebra, Sokolovská 83, 18600 Praha 8, Czech Republic
Email address: kala@karlin.mff.cuni.cz

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

Aalto University, Department of Mathematics and Systems Analysis, P.O. Box 11100, FI-00076, Finland
Email address: pavlo.yatsyna@aalto.fi