Universal quadratic forms, small norms and traces in families of number fields

Magdaléna Tinková

Joint work with Vítězslav Kala.

February 8, 2022

Outline

1. Universal quadratic forms
2. Indecomposable integers
3. The simplest cubic fields

Quadratic forms

- Lagrange: Every positive integer can be written as a sum of four squares.
- Take some $n \in \mathbb{N}$.
- We can find $x, y, z, w \in \mathbb{Z}$ such that

$$n = x^2 + y^2 + z^2 + w^2.$$

- We say that the quadratic form

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

is universal over $\mathbb{Z}$.

Universal quadratic forms over $\mathbb{Z}$

- There is no universal quadratic form in three variables over $\mathbb{Z}$.
- Up to equivalence, we know all universal quadratic forms in four variables over $\mathbb{Z}$ (Ramanujan, 1917; Dickson, 1927).

$\rightarrow$ We want to generalize this problem.

- K totally real number field, $\mathcal{O}_K$ its ring of algebraic integers
- $\mathcal{O}_K^+$ set of totally positive elements $\alpha \in \mathcal{O}_K$, i.e., all conjugates of α are positive
- quadratic form $Q(x_1, \ldots, x_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} x_i x_j$ with $a_{ij} \in \mathcal{O}_K$ is
  - *classical* if $2 | a_{ij}$ for all $i \neq j$,
  - *totally positive definite* if $Q(\gamma_1, \ldots, \gamma_n) \in \mathcal{O}_K^+$ for all $\gamma_i \in \mathcal{O}_K$ not all zero,
  - *universal* over $\mathcal{O}_K$ if it is classical, totally positive definite and represents all elements in $\mathcal{O}_K^+$

Results on universal quadratic forms

- The sum of 3 squares is universal for $K = \mathbb{Q}(\sqrt{5})$ (Maaß, 1941).
- Sums of squares can be universal only for $K = \mathbb{Q}, \mathbb{Q}(\sqrt{5})$ (Siegel, 1945).
- There always exists a universal quadratic form for every totally real field (Hsia, Kitaoka, Kneser, 1978).

$\rightarrow$ We are interested in the minimal number of variables of universal quadratic forms.

Results on universal quadratic forms

Conjecture (Kitaoka)

There are only finitely many fields which admit universal quadratic forms in three variables.

- verified for classical quadratic forms in quadratic fields (Chan, Kim, Raghavan, 1996), fields of odd degrees (Earnest, Khosravani, 1997) and biquadratic fields (Krásenský, T., Zemková, 2020)

Results on universal quadratic forms

Theorem (Blomer, Kala, 2015; Kala 2016)

For each M, there are infinitely many real quadratic fields that do not admit universal quadratic forms in M variables.

- the same is true for multiquadratic fields (Kala, Svoboda, 2019), cubic fields (Yatsyna, 2019) and fields of degrees divisible by 2 or 3 (Kala, 2022+)

Motivation

- let $Q(x,y) = \alpha x^2 + \beta y^2$ for some $\alpha, \beta \in \mathbb{N}$
- We want to represent 1 by Q – it means that $\alpha x^2 = 1$ or $\beta y^2 = 1$, let $\alpha x^2 = 1$.
- It implies that $\alpha = 1$.
- 1 cannot be written as a sum of two positive integers
- We say that 1 is indecomposable in $\mathbb{Z}$.

Definition

We say that $\alpha \in \mathcal{O}_K^+$ is indecomposable in $\mathcal{O}_K$ if it cannot be written as $\alpha = \beta + \gamma$ for any $\beta, \gamma \in \mathcal{O}_K^+$.

- only one indecomposable integer in $\mathbb{Z}$, namely 1
- we can use indecomposable integers to find bounds on the minimal number of variables of universal quadratic forms

Results on indecomposable integers

- We know the precise structure of indecomposable integers in quadratic fields $\mathbb{Q}(\sqrt{D})$, where they can be described using the continued fraction of $\sqrt{D}$ or $\frac{\sqrt{D}-1}{2}$ (Perron, 1913; Dress, Scharlau, 1982).
- some partial results for biquadratic fields (Čech, Lachman, Svoboda, T., Zemková, 2019; Krásenský, T., Zemková, 2020)
- Their norm is bounded in each field (Brunotte, 1983).
- Their norm is bounded by the discriminant of the field (Kala, Yatsyna, 2022+).
- sharper estimates on this bound for quadratic fields (Dress, Scharlau, 1982; Jang, Kim, 2016; T., Voutier, 2020) and some families of cubic fields (T., 2022+)

Method for determination of indecomposable integers

- up to multiplication by totally positive units, there are only finitely many indecomposable integers
- consider the fundamental domain for the action of multiplication by totally positive units
- by Shintani's Unit Theorem, we can choose a polyhedric cone as this fundamental domain
- a polyhedric cone is a finite disjoint union of simplicial cones
- for every indecomposable integers $\alpha \in \mathcal{O}_K$, there exists a totally positive unit ε such that $\alpha\varepsilon$ lies in one of these simplical cones

Method for determination of indecomposable integers – cubic case

- let $\mathcal{C}(\alpha_1,\dots,\alpha_r)=\mathbb{R}^+\alpha_1+\dots+\mathbb{R}^+\alpha_r$
- let $\overline{\mathcal{C}}(\alpha_1,\dots,\alpha_r)=\mathbb{R}_0^+\alpha_1+\dots+\mathbb{R}_0^+\alpha_r$
- let ε_1 and ε_2 be two totally positive units with some special properties (they are *proper* in the sense of Thomas and Vasquez, 1980)
- then our polyhedric cone can be chosen as

$$\mathcal{C}(1,\varepsilon_1,\varepsilon_2)\sqcup\mathcal{C}(1,\varepsilon_1,\varepsilon_1\varepsilon_2^{-1})\sqcup\mathcal{C}(1,\varepsilon_1)\sqcup\mathcal{C}(1,\varepsilon_2)\sqcup\mathcal{C}(1,\varepsilon_1\varepsilon_2^{-1})\sqcup\mathcal{C}(1)$$

$$\subset\overline{\mathcal{C}}(1,\varepsilon_1,\varepsilon_2)\cup\overline{\mathcal{C}}(1,\varepsilon_1,\varepsilon_1\varepsilon_2^{-1})$$

- $\sqcup$ denotes disjoint union

Method for determination of indecomposable integers – cubic case

- let $\mathcal{D}(\alpha_1,\alpha_2,\alpha_3)=[0,1]\alpha_1+[0,1]\alpha_2+[0,1]\alpha_3$
- if α is indecomposable and lies in $\overline{\mathcal{C}}(1,\varepsilon_1,\varepsilon_2)$, then it lies in $\mathcal{D}(1,\varepsilon_1,\varepsilon_2)$
- to determine indecomposable integers in $\mathcal{O}_K$, it suffices to study elements in $\mathcal{D}(1,\varepsilon_1,\varepsilon_2)$ and $\mathcal{D}(1,\varepsilon_1,\varepsilon_1\varepsilon_2^{-1})$
- however, these sets can contain decomposable integers

Method for determination of indecomposable integers – codifferent

- let $\mathcal{O}_K^\vee = \{\delta \in K, \mathrm{Tr}(\alpha\delta) \in \mathbb{Z} \text{ for all } \alpha \in \mathcal{O}_K\}$ be the codifferent of K
- if $\mathcal{O}_K = \mathbb{Z}[\rho]$, f minimal polynomial of ρ

$$\Rightarrow \mathcal{O}_K^\vee = f'(\rho)^{-1}\mathbb{Z}[\rho]$$

- if for $\alpha \in \mathcal{O}_K^+$, there exists $\delta \in \mathcal{O}_K^{\vee,+}$ such that $\mathrm{Tr}(\alpha\delta) = 1$, then α is indecomposable in $\mathcal{O}_K$

The simplest cubic fields

- introduced by Shanks (1974)
- $K=\mathbb{Q}(\rho)$ where ρ is a root of $f(x)=x^3-ax^2-(a+3)x-1$ with $a\geq -1$
- advantages:
  - they are Galois extension,
  - they posses units of all signatures; every totally positive unit is a square,
  - the system of fundamental units is formed by ρ and ρ' where ρ' is a conjugate of ρ,
  - $\mathcal{O}_K=\mathbb{Z}[\rho]$ for infinitely many cases of a

Indecomposable integers in the simplest cubic fields

Theorem

Let K be the simplest cubic field with $a \geq -1$ such that $\mathcal{O}_K = \mathbb{Z}[\rho]$. The elements 1, $1+\rho+\rho^2$, and

$$\alpha(v,w) = -v - w\rho + (v+1)\rho^2$$

where $0 \leq v \leq a$ and $v(a+2)+1 \leq w \leq (v+1)(a+1)$ are, up to multiplication by totally positive units, all the indecomposable integers in $\mathbb{Q}(\rho)$.

Minimal traces

- we can also study the value of $\min_{\delta\in\mathcal{O}_K^{\vee,+}} \mathrm{Tr}(\alpha\delta)$ for α indecomposable
- it is equal to 1 for all indecomposable integers in quadratic fields
- $\min_{\delta\in\mathcal{O}_K^{\vee,+}} \mathrm{Tr}(\alpha(v,w)\delta) = 1$
- $\min_{\delta\in\mathcal{O}_K^{\vee,+}} \mathrm{Tr}((1+\rho+\rho^2)\delta) = 2$
- for cubic orders, it can attain arbitrarily large values (Tinková, 2022+)

Small norms

- for $X \in \mathbb{R}$, let $\mathcal{P}_a(X)$ be the number of primitive principal ideals I with norm $N(I) \leq X$

Theorem

Let K be the simplest cubic field with the parameter $a \geq -1$ such that $\mathcal{O}_K = \mathbb{Z}[\rho]$. Let $s \in [0,1]$. Then $\mathcal{P}_a(a^{1+s}) \asymp a^{2s/3}$.

- we use the knowledge of the structure of indecomposable integers in $\mathcal{O}_K$

Universal quadratic forms – upper bound

- let S be a set of representatives of indecomposable integers in $\mathcal{O}_K$ up to multiplication by squares of units
- let $s = s(\mathcal{O}_K)$ be the Pythagoras number of $\mathcal{O}_K$, i.e., the minimal number of squares for which every sum of squares of elements in $\mathcal{O}_K$ is representable as the sum of at most $s(\mathcal{O}_K)$ squares.

Proposition

The quadratic form $\sum_{\sigma \in S} \sigma(x_{1,\sigma}^2 + \cdots + x_{s,\sigma}^2)$ is universal over $\mathcal{O}_K$ (and has rank $s \cdot \#S$).

Proof

- every $\alpha \in \mathcal{O}_K^+$ can be written as a sum of indecomposable integers
- thus we can write $\alpha = \sum_{\sigma \in S} \sigma\beta_\sigma$ where β_σ is a sum of squares of units
- β_σ as a sum of squares from $\mathcal{O}_K$ is representable by the sum of s squares
- thus $\sum_{\sigma \in S} \sigma(x_{1,\sigma}^2 + \cdots + x_{s,\sigma}^2)$ represents α

Upper bound for the simplest cubic fields

- every totally positive unit in $\mathbb{Q}(\rho)$ is a square, thus we can choose $S = \{1, 1+\rho+\rho^2, \alpha(v,w)\}$, and thus $\#S = \frac{a^2+3a+6}{2}$
- if K is a totally real cubic field, then $s(\mathcal{O}_K) \leq 6$ (Kala, Yatsyna, 2021)
- thus $s \cdot \#S \leq 3(a^2+3a+6)$, i.e., we get a universal quadratic form in at most $3(a^2+3a+6)$ variables!

Universal quadratic forms – lower bound

- let $\delta \in \mathcal{O}_K^{\vee,+}$
- assume that there exist elements $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K^+$ such that $\mathrm{Tr}(\alpha_i \delta) = 1$ for each i
- let d be the degree of K

Proposition

Every universal quadratic form over $\mathcal{O}_K$ has rank at least n/d.

- simplest cubic fields: this is true for elements $\alpha(v, w)$ and three totally positive units, thus $n/d = (a^2 + 3a + 8)/6$

Universal quadratic forms over the simplest cubic fields

Theorem

Let K be the simplest cubic field with $a \geq -1$ such that $\mathcal{O}_K = \mathbb{Z}[\rho]$. Then

- *there is a universal quadratic form of rank $3(a^2+3a+6)$ over K,*
- *every universal classical quadratic form over K has rank at least $\frac{a^2+3a+8}{6}$.*

Work in progress/Future plans

- generalization to fields of higher degrees
- indecomposable integers in other signatures
- Pythagoras number
- connection to multidimensional continued fractions

Thank you for your attention.