On the possible ranks of universal quadratic forms over totally real number fields

Daniel Gil Muñoz

Charles University in Prague
Department of Algebra

Barcelona, October 2021

Table of contents

Table of contents

A quadratic form on a K-vector space V is a map $Q\colon V \longrightarrow K$ such that:

- $Q(\lambda u) = \lambda^2 Q(u)$ for every $\lambda \in K$ and $v \in V$.
- $B\colon V \times V \longrightarrow K$, $B(u,v) = \frac{1}{2}(Q(u+v) - Q(u) - Q(v))$ is K-bilinear.

A quadratic form on an R-module M is a map $Q\colon M \longrightarrow R$ such that:

- $Q(\lambda u) = \lambda^2 Q(u)$ for every $\lambda \in R$ and $v \in M$.
- $B\colon M \times M \longrightarrow \frac{1}{2}R$, $B(u,v) = \frac{1}{2}(Q(u+v) - Q(u) - Q(v))$ is R-bilinear.

A quadratic form on an R-module M is a map $Q\colon M \longrightarrow R$ such that:

- $Q(\lambda u) = \lambda^2 Q(u)$ for every $\lambda \in R$ and $v \in M$.
- $B\colon M \times M \longrightarrow \frac{1}{2}R$, $B(u,v) = \frac{1}{2}(Q(u+v) - Q(u) - Q(v))$ is R-bilinear.

B is the unique bilinear symmetric form whose **associated quadratic form** is Q.

A quadratic form on an R-module M is a map $Q\colon M \longrightarrow R$ such that:

- $Q(\lambda u) = \lambda^2 Q(u)$ for every $\lambda \in R$ and $v \in M$.
- $B\colon M \times M \longrightarrow \frac{1}{2}R$, $B(u,v) = \frac{1}{2}(Q(u+v) - Q(u) - Q(v))$ is R-bilinear.

B is the unique bilinear symmetric form whose **associated quadratic form** is Q.

$$Q(u) = B(u,u)$$

A quadratic form on an R-module M is a map $Q\colon M \longrightarrow R$ such that:

- $Q(\lambda u) = \lambda^2 Q(u)$ for every $\lambda \in R$ and $v \in M$.
- $B\colon M \times M \longrightarrow \frac{1}{2}R$, $B(u,v) = \frac{1}{2}(Q(u+v) - Q(u) - Q(v))$ is R-bilinear.

B is the unique bilinear symmetric form whose **associated quadratic form** is Q.

$$Q(u) = B(u,u)$$

Assume that M is R-free and fix an R-basis. Let $A = (b_{ij})_{i,j=1}^n$ be the (symmetric) matrix of B. Then:

A quadratic form on an R-module M is a map $Q\colon M \longrightarrow R$ such that:

- $Q(\lambda u) = \lambda^2 Q(u)$ for every $\lambda \in R$ and $v \in M$.
- $B\colon M \times M \longrightarrow \frac{1}{2}R$, $B(u,v) = \frac{1}{2}(Q(u+v) - Q(u) - Q(v))$ is R-bilinear.

B is the unique bilinear symmetric form whose **associated quadratic form** is Q.

$$Q(u) = B(u,u)$$

Assume that M is R-free and fix an R-basis. Let $A = (b_{ij})_{i,j=1}^n$ be the (symmetric) matrix of B. Then:

$$Q(u) = u^t A u = \sum_{1 \le i \le j \le n} a_{ij} u_i u_j.$$

A n-ary **quadratic form** over a ring R is an homogeneous polynomial $Q \in R[X_1, \ldots, X_n]$ of degree 2.

A n-ary **quadratic form** over a ring R is an homogeneous polynomial $Q \in R[X_1, \ldots, X_n]$ of degree 2.

$$Q(X_1, \ldots, X_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} X_i X_j, \; a_{ij} \in R.$$

A n-ary **quadratic form** over a ring R is an homogeneous polynomial $Q \in R[X_1, \ldots, X_n]$ of degree 2.

$$Q(X_1, \ldots, X_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} X_i X_j, \ a_{ij} \in R.$$

The integer number n is the **arity** or the **rank** of Q.

A n-ary **quadratic form** over a ring R is an homogeneous polynomial $Q \in R[X_1, \ldots, X_n]$ of degree 2.

$$Q(X_1, \ldots, X_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} X_i X_j,\ a_{ij} \in R.$$

The integer number n is the **arity** or the **rank** of Q.

In arithmetic, we are interested in the case $R = \mathbb{Z}$.

A n-ary **quadratic form** over a ring R is an homogeneous polynomial $Q \in R[X_1, \dots, X_n]$ of degree 2.

$$Q(X_1, \dots, X_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} X_i X_j,\ a_{ij} \in R.$$

The integer number n is the **arity** or the **rank** of Q.

In arithmetic, we are interested in the case $R = \mathbb{Z}$.

We say that Q is:

A n-ary **quadratic form** over a ring R is an homogeneous polynomial $Q \in R[X_1, \dots, X_n]$ of degree 2.

$$Q(X_1, \dots, X_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} X_i X_j, \; a_{ij} \in R.$$

The integer number n is the **arity** or the **rank** of Q.

In arithmetic, we are interested in the case $R = \mathbb{Z}$.

We say that Q is:

- **Positive definite** if $Q(X) > 0$ for every $X \in \mathbb{Z}^n - \{0\}$.

A n-ary **quadratic form** over a ring R is an homogeneous polynomial $Q \in R[X_1, \ldots, X_n]$ of degree 2.

$$Q(X_1, \ldots, X_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} X_i X_j, \; a_{ij} \in R.$$

The integer number n is the **arity** or the **rank** of Q.

In arithmetic, we are interested in the case $R = \mathbb{Z}$.

We say that Q is:

- **Positive definite** if $Q(X) > 0$ for every $X \in \mathbb{Z}^n - \{0\}$.
- **Diagonal** if $a_{ij} = 0$ for $i \neq j$.

A n-ary **quadratic form** over a ring R is an homogeneous polynomial $Q \in R[X_1, \ldots, X_n]$ of degree 2.

$$Q(X_1, \ldots, X_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} X_i X_j,\ a_{ij} \in R.$$

The integer number n is the **arity** or the **rank** of Q.

In arithmetic, we are interested in the case $R = \mathbb{Z}$.

We say that Q is:

- **Positive definite** if $Q(X) > 0$ for every $X \in \mathbb{Z}^n - \{0\}$.
- **Diagonal** if $a_{ij} = 0$ for $i \neq j$.
- **Classical** if 2 divides a_{ij} for $i \neq j$.

A n-ary **quadratic form** over a ring R is an homogeneous polynomial $Q \in R[X_1, \ldots, X_n]$ of degree 2.

$$Q(X_1, \ldots, X_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} X_i X_j, \; a_{ij} \in R.$$

The integer number n is the **arity** or the **rank** of Q.

In arithmetic, we are interested in the case $R = \mathbb{Z}$.

We say that Q is:

- **Positive definite** if $Q(X) > 0$ for every $X \in \mathbb{Z}^n - \{0\}$.
- **Diagonal** if $a_{ij} = 0$ for $i \neq j$.
- **Classical** if 2 divides a_{ij} for $i \neq j$.

Recall that $Q(X) = X^t A X$, with $A \in \mathcal{M}_n(\mathbb{Q})$ symmetric.

A n-ary **quadratic form** over a ring R is an homogeneous polynomial $Q \in R[X_1, \ldots, X_n]$ of degree 2.

$$Q(X_1, \ldots, X_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} X_i X_j, \; a_{ij} \in R.$$

The integer number n is the **arity** or the **rank** of Q.

In arithmetic, we are interested in the case $R = \mathbb{Z}$.

We say that Q is:

- **Positive definite** if $Q(X) > 0$ for every $X \in \mathbb{Z}^n - \{0\}$.
- **Diagonal** if $a_{ij} = 0$ for $i \neq j$.
- **Classical** if 2 divides a_{ij} for $i \neq j$.

Recall that $Q(X) = X^t AX$, with $A \in \mathcal{M}_n(\mathbb{Q})$ symmetric.
If Q is classical, then $A \in \mathcal{M}_n(\mathbb{Z})$.

We care about the degree 2 diophantine equation

$$Q(X_1, \ldots, X_n) = a,\ a \in \mathbb{Z}.$$

We care about the degree 2 diophantine equation

$$Q(X_1, \ldots, X_n) = a,\ a \in \mathbb{Z}.$$

Definition

A quadratic form Q represents an integer $a \in \mathbb{Z}$ *if there is some* $X \in \mathbb{Z}^n - \{0\}$ *such that* $Q(X) = a$.

We care about the degree 2 diophantine equation

$$Q(X_1, \ldots, X_n) = a, \; a \in \mathbb{Z}.$$

Definition

A quadratic form Q represents an integer $a \in \mathbb{Z}$ if there is some $X \in \mathbb{Z}^n - \{0\}$ such that $Q(X) = a$.

Example

- Pythagorean theorem: The ternary quadratic form $x^2 + y^2 - z^2$ represents 0 (in infinitely many ways).

We care about the degree 2 diophantine equation

$$Q(X_1, \dots, X_n) = a,\ a \in \mathbb{Z}.$$

Definition

A quadratic form Q represents an integer $a \in \mathbb{Z}$ if there is some $X \in \mathbb{Z}^n - \{0\}$ such that $Q(X) = a$.

Example

- Pythagorean theorem: The ternary quadratic form $x^2 + y^2 - z^2$ represents 0 (in infinitely many ways).
- Pell's equation: If $n \in \mathbb{Z}_{>0}$, 1 is represented by the form $x^2 - ny^2$ (in infinitely many ways).

Definition

We say that a quadratic form Q is ***universal*** *if it represents all positive integers.*

Definition

*We say that a quadratic form Q is **universal** if it represents all positive integers.*

Example

- **Langrange's four-square theorem, 1770**: The sum of four squares $x^2 + y^2 + z^2 + t^2$ is universal.

Definition

*We say that a quadratic form Q is **universal** if it represents all positive integers.*

Example

- **Langrange's four-square theorem, 1770**: The sum of four squares $x^2 + y^2 + z^2 + t^2$ is universal.
- **Legendre's three-square theorem, 1790**: The sum of three squares $x^2 + y^2 + z^2$ is not universal.

Definition

We say that a quadratic form Q is ***universal*** *if it represents all positive integers.*

Example

- **Langrange's four-square theorem, 1770**: The sum of four squares $x^2 + y^2 + z^2 + t^2$ is universal.
- **Legendre's three-square theorem, 1790**: The sum of three squares $x^2 + y^2 + z^2$ is not universal.
- If $4 \nmid d$, the ternary quadratic form $x^2 - y^2 + dz^2$ is universal.

Theorem (Bhargava - Hanke, 2011)

Let Q be a positive definite quadratic form over $\mathbb{Z}$. If Q represents the twenty nine integers

$$1, 2, 3, 5, 6, 7, 10, 13, 14, 15, 17, 19, 21, 22, 23, 26,$$

$$29, 30, 31, 34, 35, 37, 42, 58, 93, 110, 145, 203, 290,$$

then Q is universal.

Moreover, this set is minimal for that property.

More general situation: $R = \mathcal{O}_K$, number ring of a totally real number field K.

More general situation: $R = \mathcal{O}_K$, number ring of a totally real number field K.

Let K be a number field, $d = [K : \mathbb{Q}]$

More general situation: $R = \mathcal{O}_K$, number ring of a totally real number field K.

Let K be a number field, $d = [K : \mathbb{Q}] \implies$
there are d embeddings $\sigma_1, \ldots \sigma_d \colon K \longrightarrow \mathbb{C}$.

More general situation: $R = \mathcal{O}_K$, number ring of a totally real number field K.

Let K be a number field, $d = [K : \mathbb{Q}] \Longrightarrow$
there are d embeddings $\sigma_1, \ldots \sigma_d : K \longrightarrow \mathbb{C}$.
K is **totally real** if $\mathrm{Im}(\sigma_i) \subseteq \mathbb{R}$ for all $1 \leq i \leq d$.

More general situation: $R = \mathcal{O}_K$, number ring of a totally real number field K.

Let K be a number field, $d = [K : \mathbb{Q}] \Longrightarrow$
there are d embeddings $\sigma_1, \ldots \sigma_d \colon K \longrightarrow \mathbb{C}$.
K is **totally real** if $\mathrm{Im}(\sigma_i) \subseteq \mathbb{R}$ for all $1 \leq i \leq d$.

$$Q(X_1, \ldots, X_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} X_i X_j,\ a_{ij} \in \mathcal{O}_K.$$

More general situation: $R = \mathcal{O}_K$, number ring of a totally real number field K.

Let K be a number field, $d = [K : \mathbb{Q}] \Longrightarrow$
there are d embeddings $\sigma_1, \dots \sigma_d \colon K \longrightarrow \mathbb{C}$.
K is **totally real** if $\mathrm{Im}(\sigma_i) \subseteq \mathbb{R}$ for all $1 \leq i \leq d$.

$$Q(X_1, \dots, X_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} X_i X_j, \; a_{ij} \in \mathcal{O}_K.$$

$\alpha \prec \beta$ if and only if $\sigma_i(\alpha) < \sigma_i(\beta)$ for all i.

More general situation: $R = \mathcal{O}_K$, number ring of a totally real number field K.

Let K be a number field, $d = [K : \mathbb{Q}] \Longrightarrow$
there are d embeddings $\sigma_1, \ldots \sigma_d \colon K \longrightarrow \mathbb{C}$.
K is **totally real** if $\mathrm{Im}(\sigma_i) \subseteq \mathbb{R}$ for all $1 \leq i \leq d$.

$$Q(X_1, \ldots, X_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} X_i X_j, \; a_{ij} \in \mathcal{O}_K.$$

$\alpha \prec \beta$ if and only if $\sigma_i(\alpha) < \sigma_i(\beta)$ for all i.

We say that Q is:

- **Positive definite** if $Q(X) > 0$ for every $X \in \mathbb{Z}^n - \{0\}$.
- **Diagonal** if $a_{ij} = 0$ for $i \neq j$.
- **Classical** if 2 divides a_{ij} for $i \neq j$.

More general situation: $R = \mathcal{O}_K$, number ring of a totally real number field K.

Let K be a number field, $d = [K : \mathbb{Q}] \Longrightarrow$
there are d embeddings $\sigma_1, \ldots \sigma_d \colon K \longrightarrow \mathbb{C}$.
K is **totally real** if $\mathrm{Im}(\sigma_i) \subseteq \mathbb{R}$ for all $1 \leq i \leq d$.

$$Q(X_1, \ldots, X_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} X_i X_j,\ a_{ij} \in \mathcal{O}_K.$$

$\alpha \prec \beta$ if and only if $\sigma_i(\alpha) < \sigma_i(\beta)$ for all i.

We say that Q is:

- **Positive definite** if $Q(X) \succ 0$ for every $X \in \mathcal{O}_K^n - \{0\}$.
- **Diagonal** if $a_{ij} = 0$ for $i \neq j$.
- **Classical** if 2 divides a_{ij} for $i \neq j$.

An (algebraic) integer $\alpha \in \mathcal{O}_K$ is **totally positive** if $\alpha \succ 0$.

An (algebraic) integer $\alpha \in \mathcal{O}_K$ is **totally positive** if $\alpha \succ 0$.

Definition

*A quadratic form Q is **universal** if it represents all totally positive integers of $\mathcal{O}_K$.*

An (algebraic) integer $\alpha \in \mathcal{O}_K$ is **totally positive** if $\alpha \succ 0$.

Definition

*A quadratic form Q is **universal** if it represents all totally positive integers of $\mathcal{O}_K$.*

Recall that the sum of three squares is not universal over $\mathbb{Q}$.

An (algebraic) integer $\alpha \in \mathcal{O}_K$ is **totally positive** if $\alpha \succ 0$.

Definition

*A quadratic form Q is **universal** if it represents all totally positive integers of $\mathcal{O}_K$.*

Recall that the sum of three squares is not universal over $\mathbb{Q}$.

Theorem (Maaß, 1941)

The sum of three squares is universal over $\mathbb{Q}(\sqrt{5})$.

An (algebraic) integer $\alpha \in \mathcal{O}_K$ is **totally positive** if $\alpha \succ 0$.

Definition

A quadratic form Q is ***universal*** *if it represents all totally positive integers of* $\mathcal{O}_K$*.*

Recall that the sum of three squares is not universal over $\mathbb{Q}$.

Theorem (Maaß, 1941)

The sum of three squares is universal over $\mathbb{Q}(\sqrt{5})$*.*

Theorem (Siegel, 1945)

If the sum of n squares is universal over K, then $K = \mathbb{Q}$ *or* $\mathbb{Q}(\sqrt{5})$*.*

Table of contents

Theorem (Hsia - Kitaoka - Kresner, 1978)

For every totally real number field K, there exists a universal quadratic form over K.

Theorem (Hsia - Kitaoka - Kresner, 1978)

For every totally real number field K, there exists a universal quadratic form over K.

Problem

Let K be a totally real field. What is the minimal $n \in \mathbb{Z}_{>0}$ for which there is a universal quadratic form over K of rank n?

Theorem (Hsia - Kitaoka - Kresner, 1978)

For every totally real number field K, there exists a universal quadratic form over K.

Problem

Let K be a totally real field. What is the minimal $n \in \mathbb{Z}_{>0}$ for which there is a universal quadratic form over K of rank n?

We ask for the value of

$$m(K) \equiv \text{minimal rank of a universal form over } K.$$

Theorem (Hsia - Kitaoka - Kresner, 1978)

For every totally real number field K, there exists a universal quadratic form over K.

Problem

Let K be a totally real field. What is the minimal $n \in \mathbb{Z}_{>0}$ for which there is a universal quadratic form over K of rank n?

We ask for the value of

$$m(K) \equiv \text{minimal rank of a universal form over } K.$$

There are not universal forms of ranks 1 or 2, i.e. $m(K) \geq 3$.

Theorem (Hsia - Kitaoka - Kresner, 1978)

For every totally real number field K, there exists a universal quadratic form over K.

Problem

Let K be a totally real field. What is the minimal $n \in \mathbb{Z}_{>0}$ for which there is a universal quadratic form over K of rank n?

We ask for the value of

$$m(K) \equiv \text{minimal rank of a universal form over } K.$$

There are not universal forms of ranks 1 or 2, i.e. $m(K) \geq 3$.

Conjecture (Kitaoka)

$m(K) = 3$ *only for finitely many totally real fields K.*

In 2015, Blomer and Kala introduced a strategy to determine families of number fields without universal quadratic forms of few unknowns.

In 2015, Blomer and Kala introduced a strategy to determine families of number fields without universal quadratic forms of few unknowns.

They applied it successfully to the case of totally real quadratic fields.

In 2015, Blomer and Kala introduced a strategy to determine families of number fields without universal quadratic forms of few unknowns.

They applied it successfully to the case of totally real quadratic fields.

This approach is partly based on these ideas:

In 2015, Blomer and Kala introduced a strategy to determine families of number fields without universal quadratic forms of few unknowns.

They applied it successfully to the case of totally real quadratic fields.

This approach is partly based on these ideas:

- Number fields with many **indecomposable elements** do not have universal quadratic forms of few variables.

In 2015, Blomer and Kala introduced a strategy to determine families of number fields without universal quadratic forms of few unknowns.

They applied it successfully to the case of totally real quadratic fields.

This approach is partly based on these ideas:

- Number fields with many **indecomposable elements** do not have universal quadratic forms of few variables.
- One can construct indecomposable elements of a quadratic field $K = \mathbb{Q}(\sqrt{D})$ from the **continued fraction expansion** of $\sqrt{D}$.

Definition

*A totally positive element $\alpha \in \mathcal{O}_K$ is said to be **indecomposable** if $\alpha \neq \beta + \gamma$ for all totally positive $\beta, \gamma \in \mathcal{O}_K$.*

Definition

*A totally positive element $\alpha \in \mathcal{O}_K$ is said to be **indecomposable** if $\alpha \neq \beta + \gamma$ for all totally positive $\beta, \gamma \in \mathcal{O}_K$.*

Suppose that α is indecomposable and represented by a (positive definite) diagonal quadratic form

$$\alpha = \sum_{i=1}^{n} a_{ii} x_i^2.$$

Definition

A totally positive element $\alpha \in \mathcal{O}_K$ is said to be ***indecomposable*** *if $\alpha \neq \beta + \gamma$ for all totally positive $\beta, \gamma \in \mathcal{O}_K$.*

Suppose that α is indecomposable and represented by a (positive definite) diagonal quadratic form

$$\alpha = \sum_{i=1}^{n} a_{ii} x_i^2.$$

Necessarily, for some $1 \leq i_0 \leq n$,

$$\alpha = a_{i_0 i_0} x_{i_0}^2.$$

Definition

A totally positive element $\alpha \in \mathcal{O}_K$ is said to be ***indecomposable*** *if $\alpha \neq \beta + \gamma$ for all totally positive $\beta, \gamma \in \mathcal{O}_K$.*

Suppose that α is indecomposable and represented by a (positive definite) diagonal quadratic form

$$\alpha = \sum_{i=1}^{n} a_{ii} x_i^2.$$

Necessarily, for some $1 \leq i_0 \leq n$,

$$\alpha = a_{i_0 i_0} x_{i_0}^2.$$

Then the rank of a diagonal universal quadratic form is at least the number of indecomposables modulo squares.

Let γ be a positive real number.

Let γ be a positive real number. The expansion of γ as a **continued fraction** is the expression

$$\gamma = u_0 + \frac{1}{u_1 + \frac{1}{u_2 + \dots}}, \; u_i \in \mathbb{Z}_{>0}.$$

Let γ be a positive real number. The expansion of γ as a **continued fraction** is the expression

$$\gamma = u_0 + \frac{1}{u_1 + \frac{1}{u_2 + \dots}}, \ u_i \in \mathbb{Z}_{>0}.$$

We will write $\gamma = [u_0, u_1, \dots]$.

Let γ be a positive real number. The expansion of γ as a **continued fraction** is the expression

$$\gamma = u_0 + \cfrac{1}{u_1 + \frac{1}{u_2 + \dots}}, \; u_i \in \mathbb{Z}_{>0}.$$

We will write $\gamma = [u_0, u_1, \dots]$.

Example

- $\frac{415}{93} = 4 + \frac{1}{2+\frac{1}{6+\frac{1}{7}}} = [4, 2, 6, 7]$.

Let γ be a positive real number. The expansion of γ as a **continued fraction** is the expression

$$\gamma = u_0 + \cfrac{1}{u_1 + \frac{1}{u_2 + \dots}}, \; u_i \in \mathbb{Z}_{>0}.$$

We will write $\gamma = [u_0, u_1, \dots]$.

Example

- $\frac{415}{93} = 4 + \frac{1}{2 + \frac{1}{6 + \frac{1}{7}}} = [4, 2, 6, 7]$.
- $\sqrt{2} = [1, 2, 2, 2, \dots] = [1, \overline{2}]$.

Let γ be a positive real number. The expansion of γ as a **continued fraction** is the expression

$$\gamma = u_0 + \frac{1}{u_1 + \frac{1}{u_2 + \dots}}, \; u_i \in \mathbb{Z}_{>0}.$$

We will write $\gamma = [u_0, u_1, \dots]$.

Example

- $\frac{415}{93} = 4 + \frac{1}{2+\frac{1}{6+\frac{1}{7}}} = [4, 2, 6, 7]$.
- $\sqrt{2} = [1, 2, 2, 2, \dots] = [1, \overline{2}]$.
- $\pi = [3, 7, 15, 1, 292, \dots]$

$$\gamma = u_0 + \cfrac{1}{u_1 + \frac{1}{u_2 + \dots}}, \; u_i \in \mathbb{Z}.$$

$$\gamma = u_0 + \cfrac{1}{u_1 + \frac{1}{u_2 + \dots}}, \ u_i \in \mathbb{Z}.$$

For $i \in \mathbb{Z}_{\geq 0}$, $\frac{p_i}{q_i} = [u_0, \dots, u_i]$ is the i-th **convergent** of γ.

$$\gamma = u_0 + \frac{1}{u_1 + \frac{1}{u_2 + \dots}}, \ u_i \in \mathbb{Z}.$$

For $i \in \mathbb{Z}_{\geq 0}$, $\frac{p_i}{q_i} = [u_0, \dots, u_i]$ is the i-th **convergent** of γ.

Basic properties

- $p_{i+2} = u_{i+2}p_{i+1} + p_i$, $q_{i+2} = u_{i+2}q_{i+1} + q_i$.

$$\gamma = u_0 + \cfrac{1}{u_1 + \frac{1}{u_2 + \dots}}, \; u_i \in \mathbb{Z}.$$

For $i \in \mathbb{Z}_{\geq 0}$, $\frac{p_i}{q_i} = [u_0, \dots, u_i]$ is the i-th **convergent** of γ.

Basic properties

- $p_{i+2} = u_{i+2}p_{i+1} + p_i$, $q_{i+2} = u_{i+2}q_{i+1} + q_i$.
- $p_{i+1}q_i - p_i q_{i+1} = (-1)^{i+1}$.

$$\gamma = u_0 + \frac{1}{u_1 + \frac{1}{u_2 + \ldots}}, \ u_i \in \mathbb{Z}.$$

For $i \in \mathbb{Z}_{\geq 0}$, $\frac{p_i}{q_i} = [u_0, \ldots, u_i]$ is the i-th **convergent** of γ.

Basic properties

- $p_{i+2} = u_{i+2}p_{i+1} + p_i$, $q_{i+2} = u_{i+2}q_{i+1} + q_i$.
- $p_{i+1}q_i - p_iq_{i+1} = (-1)^{i+1}$.
- Given $i \in \mathbb{Z}_{\geq}0$,

$$\frac{1}{(u_{i+1}+2)q_i^2} < \left|\frac{p_i}{q_i} - \gamma\right| < \frac{1}{u_{i+1}q_i^2}.$$

Let $D \in \mathbb{Z}_{>0}$ be squarefree. Then,

$$\sqrt{D} = [u_0, \overline{u_1, \ldots, u_{s-1}, 2u_0}],$$

where the sequence $(u_1, \ldots, u_{s-1})$ is symmetric.

Let $D \in \mathbb{Z}_{>0}$ be squarefree. Then,

$$\sqrt{D} = [u_0, \overline{u_1, \ldots, u_{s-1}, 2u_0}],$$

where the sequence $(u_1, \ldots, u_{s-1})$ is symmetric.

Let us define

$$\alpha_i = p_i + q_i\sqrt{D}.$$

Then, $\alpha_{i+2} = u_{i+2}\alpha_{i+1} + \alpha_i$.

Let $D \in \mathbb{Z}_{>0}$ be squarefree. Then,

$$\sqrt{D} = [u_0, \overline{u_1, \ldots, u_{s-1}, 2u_0}],$$

where the sequence $(u_1, \ldots, u_{s-1})$ is symmetric.

Let us define

$$\alpha_i = p_i + q_i\sqrt{D}.$$

Then, $\alpha_{i+2} = u_{i+2}\alpha_{i+1} + \alpha_i$.

Theorem

The elements

$$\alpha_{i,r} = r\alpha_{i+1} + \alpha_i,\ 0 \leq r \leq u_{i+2},\ i \text{ odd}$$

and their conjugates are all indecomposables > 1 of $K = \mathbb{Q}(\sqrt{D})$.

Let $D \in \mathbb{Z}_{>0}$ be squarefree. Then,

$$\sqrt{D} = [u_0, \overline{u_1, \ldots, u_{s-1}, 2u_0}],$$

where the sequence $(u_1, \ldots, u_{s-1})$ is symmetric.

Let us define

$$\alpha_i = p_i + q_i\sqrt{D}.$$

Then, $\alpha_{i+2} = u_{i+2}\alpha_{i+1} + \alpha_i$.

Theorem

The elements

$$\alpha_{i,r} = r\alpha_{i+1} + \alpha_i,\ 0 \le r \le u_{i+2},\ i \text{ odd}$$

and their conjugates are all indecomposables > 1 *of* $K = \mathbb{Q}(\sqrt{D})$.

In particular, the elements α_i, i odd, are indecomposables.

Conversely, we can obtain $\sqrt{D}$ from symmetric sequences of integers:

Conversely, we can obtain $\sqrt{D}$ from symmetric sequences of integers:

Theorem (Friesen, 1988)

Let $(u_1, u_2, \dots, u_{s-1})$ be symmetric and such that

$$q_{s-2} \quad \text{or} \quad \frac{q_{s-2}^2 - (-1)^s}{q_{s-1}} \quad \text{is even.}$$

Then there are infinitely many square-free D such that

$$\sqrt{D} = [u_0, \overline{u_1, u_2, \dots, u_{s-1}, 2u_0}],$$

where $u_0 = \lfloor \sqrt{D} \rfloor$.

Choosing the coefficients u_i suitably, we can construct infinitely many $K = \mathbb{Q}(\sqrt{D})$ with many indecomposable elements. This led to the following:

Choosing the coefficients u_i suitably, we can construct infinitely many $K = \mathbb{Q}(\sqrt{D})$ with many indecomposable elements. This led to the following:

Theorem (Blomer - Kala, 2015)

For every $n \in \mathbb{Z}_{>0}$, there are infinitely many real quadratic fields $K = \mathbb{Q}(\sqrt{D})$ such that every classical universal quadratic form over K has rank at least n.

Choosing the coefficients u_i suitably, we can construct infinitely many $K = \mathbb{Q}(\sqrt{D})$ with many indecomposable elements. This led to the following:

Theorem (Blomer - Kala, 2015)

For every $n \in \mathbb{Z}_{>0}$, there are infinitely many real quadratic fields $K = \mathbb{Q}(\sqrt{D})$ such that every classical universal quadratic form over K has rank at least n.

Theorem (Kala, 2016)

For every $n \in \mathbb{Z}_{>0}$, there are infinitely many real quadratic fields $K = \mathbb{Q}(\sqrt{D})$ such that every universal quadratic form over K has rank at least n, i.e. $m(K) \geq n$.

If we restrict to diagonal quadratic form, there are more explicit bounds available:

If we restrict to diagonal quadratic form, there are more explicit bounds available:

Theorem (Blomer - Kala, 2018)

Let $K = \mathbb{Q}(\sqrt{D})$. We have

$$\max\left(\frac{M_D}{\kappa s}, C_\epsilon M^*_{D,\epsilon}\right) \leq m_{\mathrm{diag}}(K) \leq 8M_D$$

for any $\epsilon \geq 0$, where C_ϵ is a constant depending on ϵ and $\kappa = 2$ if s is odd and $\kappa = 1$ otherwise.

If we restrict to diagonal quadratic form, there are more explicit bounds available:

Theorem (Blomer - Kala, 2018)

Let $K = \mathbb{Q}(\sqrt{D})$. We have

$$\max\left(\frac{M_D}{\kappa s}, C_\epsilon M_{D,\epsilon}^*\right) \leq m_{\text{diag}}(K) \leq 8M_D$$

for any $\epsilon \geq 0$, where C_ϵ is a constant depending on ϵ and $\kappa = 2$ if s is odd and $\kappa = 1$ otherwise.

$$M_D = \begin{cases} u_1 + u_3 + \cdots + u_{s-1} & \text{if } s \text{ is even,} \\ 2u_0 + u_1 + u_2 + \cdots + u_{s-1} & \text{if } s \text{ is odd and } D \not\equiv 1\,(4), \\ 2u_0 + u_1 + u_2 + \cdots + u_{s-1} - 1 & \text{if } s \text{ is odd and } D \equiv 1\,(4). \end{cases}$$

For number fields of higher degree, there are similar results:

For number fields of higher degree, there are similar results:

Theorem (Kala - Svoboda, 2019)

For every $n, k \in \mathbb{Z}_{>0}$, there are infinitely many multiquadratic fields $K = \mathbb{Q}(\sqrt{D_1}, \ldots, \sqrt{D_k})$ of degree 2^k such that $m(K) \geq n$.

For number fields of higher degree, there are similar results:

Theorem (Kala - Svoboda, 2019)

For every $n, k \in \mathbb{Z}_{>0}$, there are infinitely many multiquadratic fields $K = \mathbb{Q}(\sqrt{D_1}, \ldots, \sqrt{D_k})$ of degree 2^k such that $m(K) \geq n$.

Theorem (Yatsyna, 2019)

For every $n \in \mathbb{Z}_{>0}$, there are infinitely many cubic fields K such $m(K) \geq n$.

For number fields of higher degree, there are similar results:

Theorem (Kala - Svoboda, 2019)

For every $n, k \in \mathbb{Z}_{>0}$, there are infinitely many multiquadratic fields $K = \mathbb{Q}(\sqrt{D_1}, \dots, \sqrt{D_k})$ of degree 2^k such that $m(K) \geq n$.

Theorem (Yatsyna, 2019)

For every $n \in \mathbb{Z}_{>0}$, there are infinitely many cubic fields K such $m(K) \geq n$.

Theorem (Kala, 2021)

For every $n, m \in \mathbb{Z}_{>0}$ with m divisible by 2 or 3, there are infinitely many totally real fields K of degree m such that $m(K) \geq n$.

We have also bounds for a special type of cubic fields.

We have also bounds for a special type of cubic fields.

Definition

*The **simplest cubic fields** are those cubic fields K_a generated by a polynomial of the form*

$$f_a(x) = x^3 - ax^2 - (a+3)x - 1,\ a \in \mathbb{Z}_{\geq 0}.$$

We have also bounds for a special type of cubic fields.

Definition

The ***simplest cubic fields*** *are those cubic fields K_a generated by a polynomial of the form*

$$f_a(x) = x^3 - ax^2 - (a+3)x - 1,\ a \in \mathbb{Z}_{\geq 0}.$$

Theorem (Kala - Tinková, 2020)

Let K_a be a simplest cubic field. Then:

- $m(K_a) \leq 3(a^2 + 3a + 6)$.
- *If* $a \geq 21$, $m(K_a) \geq \frac{\sqrt{a^2+3a+8}}{3\sqrt{2}}$.

- M. Bhargava, J. Hanke; *Universal quadratic forms and the 290-theorem*, Invent. Math., 2005.
- V. Blomer, V. Kala; *Number fields without n-ary universal quadratic forms*, Math. Proc. Cambridge Philos. Soc. **159** (2015), 239-252.
- V. Blomer, V. Kala; *On the rank of universal quadratic forms over real quadratic fields*, Doc. Math. **23** (2018), 15-34.
- V. Kala; *Universal quadratic forms and elements of small norm in real quadratic fields*, Bull. Aust. Math. Soc. **94** (2016), 7-14.

- V. Kala; *Number fields without universal quadratic forms of small rank exist in most degrees*, Preprint.
- V. Kala, J. Svoboda; *Universal quadratic forms over multiquadratic fields*, Ramanujan J. **48** (2019), 151-157.
- V. Kala, M. Tinková; *Universal quadratic forms, small norms and traces in families of number fields*, Preprint.
- 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.

Thank you for your attention