Universality Beyond Quadratic Forms

Om Prakash
Charles University, Czechia

Squares in Dortmund, Germany
March 31, 2025
(Joint work with Vítězslav Kala)

Quadratic Forms

Quadratic forms: $Q(x_1, x_2, \ldots, x_n) = \sum_{1 \le i \le j \le n} a_{ij} x_i x_j, \quad a_{ij} \in \mathbb{Z}.$

- Q represents an integer c if there exists $x \in \mathbb{Z}^n$ satisfying $Q(x) = c$.

Quadratic Forms

Quadratic forms: $Q(x_1, x_2, \ldots, x_n) = \sum_{1 \le i \le j \le n} a_{ij} x_i x_j, \quad a_{ij} \in \mathbb{Z}.$

- Q represents an integer c if there exists $x \in \mathbb{Z}^n$ satisfying $Q(x) = c$.
- Q is positive definite if $Q(x) > 0$ for all $x \in \mathbb{Z}^n \setminus \{0\}$.

Quadratic Forms

Quadratic forms: $Q(x_1, x_2, \ldots, x_n) = \sum_{1 \le i \le j \le n} a_{ij} x_i x_j, \quad a_{ij} \in \mathbb{Z}.$

- Q represents an integer c if there exists $x \in \mathbb{Z}^n$ satisfying $Q(x) = c$.
- Q is positive definite if $Q(x) > 0$ for all $x \in \mathbb{Z}^n \setminus \{0\}$.

Which integers are represented by quadratic forms?

Example

Sums of squares (Fermat, Gauss and Lagrange):

- $p = x^2 + y^2 \iff p \equiv 1 \pmod 4$
- $n = x^2 + y^2 + z^2 \iff n \neq 4^a(8b + 7)$
- $x^2 + y^2 + z^2 + w^2$ represents all $\mathbb{Z}_{\ge 0}$.

Universal Quadratic Forms

- A quadratic form is called universal if it is *positive definite* and represents all positive integers.

Classification

- Ramanujan, Dickson (1916): classified all universal forms in four variables, e.g., $x^2 + 2y^2 + 4z^2 + dw^2$ with $d \leq 14$.
- 15-Theorem (Conway–Schneeberger): positive definite classical quadratic form is universal $\iff$ it represents $1, 2, \ldots, 15$.

Universal Quadratic Forms

- A quadratic form is called universal if it is *positive definite* and represents all positive integers.

Classification

- Ramanujan, Dickson (1916): classified all universal forms in four variables, e.g., $x^2 + 2y^2 + 4z^2 + dw^2$ with $d \leq 14$.
- 15-Theorem (Conway–Schneeberger): positive definite classical quadratic form is universal $\iff$ it represents $1, 2, \ldots, 15$.

290-Theorem (Bhargava-Hanke, 2011)

If a positive definite quadratic form Q represents

$$1, 2, 3, 5, 6, 7, 10, 13, 14, 15, 17, 19, 21, 22, 23, 26,$$
$$29, 30, 31, 34, 35, 37, 42, 58, 93, 110, 145, 203, \text{ and } 290,$$

then it is universal.

Sums of mth Powers

Waring's problem (1770): Can every positive integer be expressed as a sum of at most $g(m)$ mth powers of non-negative integers, where $g(m)$ depends only on m, not the number being represented? $g(3) = 9$? $g(4) = 19$?

Sums of mth Powers

Waring's problem (1770): Can every positive integer be expressed as a sum of at most $g(m)$ mth powers of non-negative integers, where $g(m)$ depends only on m, not the number being represented? $g(3) = 9$? $g(4) = 19$?

Theorem (Hilbert, 1909)

For each fixed $m \geq 1$, there exists $g(m) < \infty$ such that every positive integer can be expressed as a sum of at most $g(m)$ mth powers.

Estimates/Formulae for $g(m)$?

Bounds for $g(m)$

- $g(m) \geq 2^{m-1}$.
- Conjecture: $g(m) = 2^m + \lfloor (3/2)^m \rfloor - 2$ for every $m \geq 1$.
- Mahler (1957), there are at most finitely many exceptions. Verified for $m \leq 471,600,000$ by Kubina–Wunderlich (1990).

Bounds for $g(m)$

- $g(m) \geq 2^{m-1}$.
- Conjecture: $g(m) = 2^m + \lfloor (3/2)^m \rfloor - 2$ for every $m \geq 1$.
- Mahler (1957), there are at most finitely many exceptions. Verified for $m \leq 471,600,000$ by Kubina–Wunderlich (1990).
- Unconditionally it is known that

$$g(m) \leq 2^m + \lfloor (3/2)^m \rfloor - 2.$$

if $2^m\{(3/2)^m\} + \lfloor (3/2)^m \rfloor \leq 2^m$. Otherwise,

$$g(m) \leq 2^m + \lfloor (3/2)^m \rfloor + \lfloor (4/3)^m \rfloor - \epsilon,$$

where ϵ is 2 or 3 depending on $\lfloor (4/3)^m \rfloor \lfloor (3/2)^m \rfloor + \lfloor (4/3)^m \rfloor + \lfloor (3/2)^m \rfloor$ equals or exceeds 2^m.

Higher Degree Forms

Replace the sum of mth power, by a homogeneous polynomial of degree $m > 2$ (i.e. higher degree form).

Higher Degree Forms

Replace the sum of mth power, by a homogeneous polynomial of degree $m > 2$ (i.e. higher degree form).

Definition

Let m and n be positive integers. Then an m-ic form in n variables over $\mathbb{Z}$ is

$$Q(x_1, x_2, \ldots, x_n) = \sum_{\substack{i_1, \ldots, i_n \geq 0 \\ i_1 + i_2 + \cdots + i_n = m}} a_{i_1 i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n},$$

where $a_{i_1 i_2 \ldots i_n} \in \mathbb{Z}$. We call m the *degree* of Q and n its *rank*.

e.g. $x^4 + 2x^3y + 5z^4 + y^2z^2$

Positive Definite Forms

- An m-ic form Q is positive definite if $Q(x) > 0$ for all $x \in \mathbb{R}^n \setminus \{(0, 0, \ldots, 0)\}$.
- By homogeneity of Q, we have $Q(-x) = (-1)^m Q(x)$ for all x.

From now on, we assume that m is even.

- An m-ic form is universal if it is positive definite and represents all positive integers.

Positive Definite Forms

- An m-ic form Q is positive definite if $Q(x) > 0$ for all $x \in \mathbb{R}^n \setminus \{(0, 0, \ldots, 0)\}$.
- By homogeneity of Q, we have $Q(-x) = (-1)^m Q(x)$ for all x.

From now on, we assume that m is even.

- An m-ic form is universal if it is positive definite and represents all positive integers.

Question

1. Given an m-ic form Q, which integers are represented by Q?
2. Does there exists a finite set $\mathcal{A}$ of positive integers such that if an m-ic form represents all elements of $\mathcal{A}$ then it is universal?
   Such a set $\mathcal{A}$ is known as finite criterion set.

Question 1

- is hard.
- is related to *Hilbert's* 10*th problem.*
- Davis, Putnam, Robinson, and Matiyasevich (1973): may be undecidable.

Question 1

- is hard.
- is related to *Hilbert's* 10*th problem.*
- Davis, Putnam, Robinson, and Matiyasevich (1973): may be undecidable.

We'll answer Question 2 negatively.

No criterion set

Proposition (Kala-P., 2024)

Given a positive even integer $m > 2$ and a positive integer B, there is a positive definite, m-ic form Q that represents all the positive integers $\leq B$ but is not universal.

No criterion set

Proposition (Kala-P., 2024)

Given a positive even integer $m > 2$ and a positive integer B, there is a positive definite, m-ic form Q that represents all the positive integers $\leq B$ but is not universal.

Proof:

- $Q_1(x_1, x_2, \ldots, x_B) = \sum_{i=1}^{B} i x_i^m$.
- Let $c > B$ be mth powerfree.
- $Q(x_1, x_2, \ldots, x_B) = \sum_{i=1}^{B} i x_i^m + \sum_{1 \leq i < j \leq B} \delta x_i^2 x_j^{m-2}$.

$m > 2$ **is important.**

Here is a stronger result.

Theorem (Kala-P., 2024)

Let $\mathcal{A} \subset \mathbb{Z}_{>0}$ be finite. Then the following conditions are equivalent:

1. There exists a positive definite m-ic form Q that represents exactly $\mathbb{Z}_{\geq 0} \setminus \mathcal{A}$.
2. For all $a, b \in \mathbb{Z}$, we have that $ab^m \in \mathcal{A}$ implies $a \in \mathcal{A}$.

Moreover, Q can be chosen of rank $< (B+1)(2^{m+1}+1)$, where B is the largest element of $\mathcal{A}$.

Forms Over Number Fields

$$K = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}.$$

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}.$$

$$\mathcal{O}_K^+ = \mathbb{Z}[\sqrt{2}]^+ = \{a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}] : a + b\sqrt{2}, a - b\sqrt{2} > 0\}.$$

Forms Over Number Fields

$$K = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}.$$

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}.$$

$$\mathcal{O}_K^+ = \mathbb{Z}[\sqrt{2}]^+ = \{a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}] : a + b\sqrt{2}, a - b\sqrt{2} > 0\}.$$

- We want to study the representation of elements in $\mathbb{Z}[\sqrt{2}]^+$ by the forms over K, e.g. $\sqrt{2}x^4 + 5y^2z^2 + (1 + \sqrt{2})z^4$, i.e. homogeneous polynomials with coefficients in $\mathbb{Z}[\sqrt{2}]$.
- Q represents $\alpha \in \mathcal{O}_K^+ \iff$ it represents $\alpha\varepsilon^m$ for all $\varepsilon \in \mathcal{O}_K^\times$. So, need to consider $\mathcal{O}_K^+/{\mathcal{O}_K^\times}^m$.

Forms Over Number Fields

$$K = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}.$$

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}.$$

$$\mathcal{O}_K^+ = \mathbb{Z}[\sqrt{2}]^+ = \{a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}] : a + b\sqrt{2}, a - b\sqrt{2} > 0\}.$$

- We want to study the representation of elements in $\mathbb{Z}[\sqrt{2}]^+$ by the forms over K, e.g. $\sqrt{2}x^4 + 5y^2z^2 + (1 + \sqrt{2})z^4$, i.e. homogeneous polynomials with coefficients in $\mathbb{Z}[\sqrt{2}]$.
- Q represents $\alpha \in \mathcal{O}_K^+ \iff$ it represents $\alpha\varepsilon^m$ for all $\varepsilon \in \mathcal{O}_K^\times$. So, need to consider $\mathcal{O}_K^+/\mathcal{O}_K^{\times m}$.

Does there exists universal m-ic form over $\mathbb{Z}[\sqrt{2}]$?

Universal m-ic Form

Siegel (1945): Sums of mth powers can never be universal over $K \neq \mathbb{Q}$.

$$(a + b\sqrt{2})^2 = a^2 + 2b^2 + 2ab\sqrt{2}$$

e.g. $3 + \sqrt{2}$ can't be expressible as sums of mth powers.

Universal m-ic Form

Siegel (1945): Sums of mth powers can never be universal over $K \neq \mathbb{Q}$.

$$(a + b\sqrt{2})^2 = a^2 + 2b^2 + 2ab\sqrt{2}$$

e.g. $3 + \sqrt{2}$ can't be expressible as sums of mth powers.

- Sum of mth powers can only represent elements from $\mathbb{Z}[2\sqrt{2}]$.
- $[\mathbb{Z}[\sqrt{2}] : \mathbb{Z}[2\sqrt{2}]] = 2$, $\mathbb{Z}[\sqrt{2}]/\mathbb{Z}[2\sqrt{2}] = \{\alpha, \beta\}$

$$\alpha(\text{sums of } m\text{th powers}) + \beta(\text{sum of } m\text{th powers}) + \text{something}.$$

Theorem (Kala-P., 2024)

Given a totally real number field K and an even positive integer $m > 2$, there exists a universal m-ic form over K.

Remark. Above result is not always true in the case of totally real infinite extension of $\mathbb{Q}$.

Result over Number Fields

Theorem (Kala-P., 2024)

Let K be a totally real number field, $m > 2$ an even positive integer, and $\mathcal{A}_0$ a finite subset of $\mathcal{O}_K^+$. Set $\mathcal{A} = \mathcal{A}_0 \cdot \mathcal{O}_K^{\times m} = \{\delta\varepsilon^m \mid \delta \in \mathcal{A}_0, \varepsilon \in \mathcal{O}_K^\times\}$. Then the following conditions are equivalent:

1. There exists a totally positive definite m-ic form that represents exactly $\mathcal{O}_K^+ \setminus \mathcal{A}$.
2. For all $\alpha, \beta \in \mathcal{O}_K$ we have that $\alpha\beta^m \in \mathcal{A}$ implies $\alpha \in \mathcal{A}$.

Result over Number Fields

Theorem (Kala-P., 2024)

Let K be a totally real number field, $m > 2$ an even positive integer, and $\mathcal{A}_0$ a finite subset of $\mathcal{O}_K^+$. Set $\mathcal{A} = \mathcal{A}_0 \cdot \mathcal{O}_K^{\times m} = \{\delta\varepsilon^m \mid \delta \in \mathcal{A}_0, \varepsilon \in \mathcal{O}_K^\times\}$. Then the following conditions are equivalent:

1. There exists a totally positive definite m-ic form that represents exactly $\mathcal{O}_K^+ \setminus \mathcal{A}$.
2. For all $\alpha, \beta \in \mathcal{O}_K$ we have that $\alpha\beta^m \in \mathcal{A}$ implies $\alpha \in \mathcal{A}$.

Thank You for Your Attention!