Bounds on the number of number fields of given degree and bounded discriminant

Robert J. Lemke Oliver
Tufts University

(joint w/ Frank Thorne)

Preprint: https://arxiv.org/abs/2005.14110
Slides: https://rlemke01.math.tufts.edu/slides/nf-bounds.pdf

Number fields

A number field K of degree n is formed by an irreducible poly.:

$$K := \mathbb{Q}[x]/(f(x)) \simeq \mathbb{Q}(\alpha)$$

Number fields

A number field K of degree n is formed by an irreducible poly.:

$$K := \mathbb{Q}[x]/(f(x)) \simeq \mathbb{Q}(\alpha)$$

Central Question: How many degree n number fields are there w/ $\mathrm{Disc}(K) \leq X$?

Number fields

A number field K of degree n is formed by an irreducible poly.:

$$K := \mathbb{Q}[x]/(f(x)) \simeq \mathbb{Q}(\alpha)$$

Central Question: How many degree n number fields are there w/ $\mathrm{Disc}(K) \leq X$?

Conjecture: $\sim c_n X$ as $X \to \infty$

Number fields

A number field K of degree n is formed by an irreducible poly.:

$$K := \mathbb{Q}[x]/(f(x)) \simeq \mathbb{Q}(\alpha)$$

Central Question: How many degree n number fields are there w/ $\mathrm{Disc}(K) \leq X$?

Conjecture: $\sim c_n X$ as $X \to \infty$

Open Problem: How many degree 6 number fields are there w/ $\mathrm{Disc}(K) \leq X$?

Number fields

A number field K of degree n is formed by an irreducible poly.:

$$K := \mathbb{Q}[x]/(f(x)) \simeq \mathbb{Q}(\alpha)$$

Central Question: How many degree n number fields are there w/ $\mathrm{Disc}(K) \leq X$?

Conjecture: $\sim c_n X$ as $X \to \infty$

Open Problem: How many degree 6 number fields are there w/ $\mathrm{Disc}(K) \leq X$?

Best known upper bound: $O(X^2)$

Irreducible polynomials

Theorem (Hilbert Irreducibility)

"100% *of monic integer polynomials of degree* n *are irreducible.*"

Irreducible polynomials

Theorem (Hilbert Irreducibility)

"100% *of monic integer polynomials of degree* n *are irreducible.*"

True for $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ with:

- each $|a_i| \leq H$, as $H \to \infty$;

Irreducible polynomials

Theorem (Hilbert Irreducibility)

"100% of monic integer polynomials of degree n are irreducible."

True for $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ with:

- each $|a_i| \leq H$, as $H \to \infty$;
- each $|a_i| \leq H^i$, as $H \to \infty$.

Irreducible polynomials

Theorem (Hilbert Irreducibility)

"100% *of monic integer polynomials of degree n are irreducible.*"

True for $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ with:

- each $|a_i| \leq H$, as $H \to \infty$;
- each $|a_i| \leq H^i$, as $H \to \infty$.

(Lots of other cases/families too!)

Irreducible polynomials

Theorem (Hilbert Irreducibility)

"100% of monic integer polynomials of degree n are irreducible."

True for $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ with:

- each $|a_i| \leq H$, as $H \to \infty$;
- each $|a_i| \leq H^i$, as $H \to \infty$.

(Lots of other cases/families too!)

Naive thought: If it's easy to write down irreducible polynomials, shouldn't it be easy to write down number fields?

Rings of integers

Let $\mathcal{O}_K$ be the ring of integers of K.

Rings of integers

Let $\mathcal{O}_K$ be the ring of integers of K. Then

$$\mathrm{Disc}(K) := \mathrm{Disc}(\mathcal{O}_K).$$

Rings of integers

Let $\mathcal{O}_K$ be the ring of integers of K. Then

$$\mathrm{Disc}(K) := \mathrm{Disc}(\mathcal{O}_K).$$

If $\mathcal{O}_K = \mathbb{Z}[\alpha]$, then $\mathrm{Disc}(\mathcal{O}_K) = \mathrm{Disc}(f_\alpha(x))$.

Rings of integers

Let $\mathcal{O}_K$ be the ring of integers of K. Then

$$\mathrm{Disc}(K) := \mathrm{Disc}(\mathcal{O}_K).$$

If $\mathcal{O}_K = \mathbb{Z}[\alpha]$, then $\mathrm{Disc}(\mathcal{O}_K) = \mathrm{Disc}(f_\alpha(x))$.

Problem: Usually $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$ for any α!

Rings of integers

Let $\mathcal{O}_K$ be the ring of integers of K. Then

$$\mathrm{Disc}(K) := \mathrm{Disc}(\mathcal{O}_K).$$

If $\mathcal{O}_K = \mathbb{Z}[\alpha]$, then $\mathrm{Disc}(\mathcal{O}_K) = \mathrm{Disc}(f_\alpha(x))$.

Problem: Usually $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$ for any α!

Definition: If $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some α, K is called monogenic.

Rings of integers

Let $\mathcal{O}_K$ be the ring of integers of K. Then

$$\mathrm{Disc}(K) := \mathrm{Disc}(\mathcal{O}_K).$$

If $\mathcal{O}_K = \mathbb{Z}[\alpha]$, then $\mathrm{Disc}(\mathcal{O}_K) = \mathrm{Disc}(f_\alpha(x))$.

Problem: Usually $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$ for any α!

Definition: If $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some α, K is called monogenic.

Typically, K is **not** monogenic

Rings of integers

Let $\mathcal{O}_K$ be the ring of integers of K. Then

$$\mathrm{Disc}(K) := \mathrm{Disc}(\mathcal{O}_K).$$

If $\mathcal{O}_K = \mathbb{Z}[\alpha]$, then $\mathrm{Disc}(\mathcal{O}_K) = \mathrm{Disc}(f_\alpha(x))$.

Problem: Usually $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$ for any α!

Definition: If $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some α, K is called monogenic.

Typically, K is **not** monogenic $\Rightarrow \mathcal{O}_K = \mathbb{Z}[\alpha_1, \ldots, \alpha_m]$

Rings of integers

Let $\mathcal{O}_K$ be the ring of integers of K. Then

$$\mathrm{Disc}(K) := \mathrm{Disc}(\mathcal{O}_K).$$

If $\mathcal{O}_K = \mathbb{Z}[\alpha]$, then $\mathrm{Disc}(\mathcal{O}_K) = \mathrm{Disc}(f_\alpha(x))$.

Problem: Usually $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$ for any α!

Definition: If $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some α, K is called monogenic.

Typically, K is **not** monogenic $\Rightarrow \mathcal{O}_K = \mathbb{Z}[\alpha_1, \ldots, \alpha_m]$
$\Rightarrow \mathrm{Disc}(K)$ more complicated (need all α_i, not just one)

Rings of integers

Let $\mathcal{O}_K$ be the ring of integers of K. Then

$$\mathrm{Disc}(K) := \mathrm{Disc}(\mathcal{O}_K).$$

If $\mathcal{O}_K = \mathbb{Z}[\alpha]$, then $\mathrm{Disc}(\mathcal{O}_K) = \mathrm{Disc}(f_\alpha(x))$.

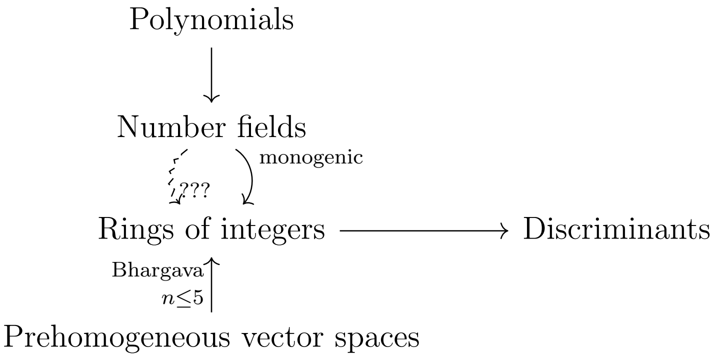
Problem: Usually $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$ for any α!

Definition: If $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some α, K is called monogenic.

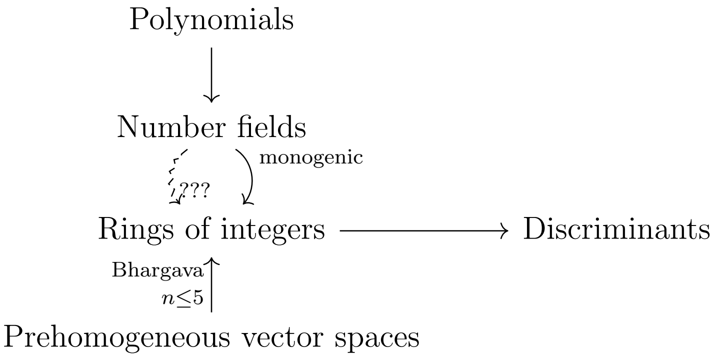
Typically, K is **not** monogenic $\Rightarrow \mathcal{O}_K = \mathbb{Z}[\alpha_1, \ldots, \alpha_m]$
$\Rightarrow \mathrm{Disc}(K)$ more complicated (need all α_i, not just one)

Example: $K = \mathbb{Q}[x]/(x^3 + 4x^2 + 3x + 8)$ needs $m = 2$

A schematic

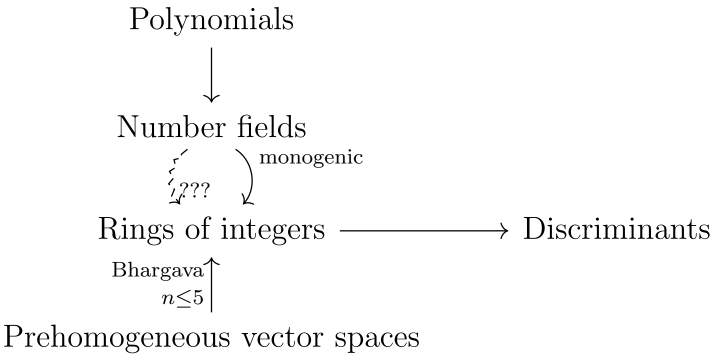

Polynomials
Number fields
???
monogenic
Rings of integers
Discriminants
Bhargava
$n \leq 5$
Prehomogeneous vector spaces

A schematic



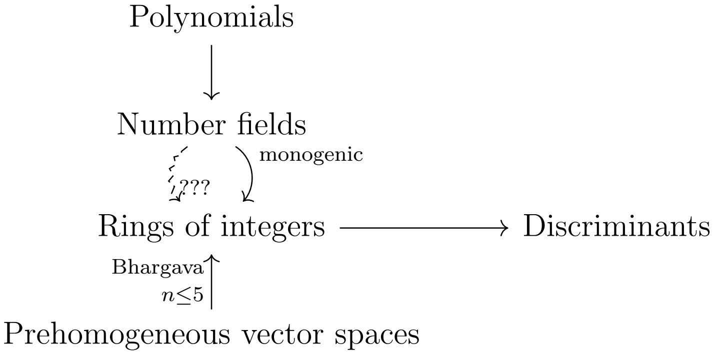
Key Obstacle: We “run out” of prehomogeneous vector spaces

A schematic



Key Obstacle: We "run out" of prehomogeneous vector spaces
$\Rightarrow$ No direct route to discriminants for $n \geq 6$.

A schematic



Key Obstacle: We "run out" of prehomogeneous vector spaces

$\Rightarrow$ No direct route to discriminants for $n \geq 6$.

Upshot: We have to settle for upper and lower bounds when $n \geq 6$

Bounds on number fields

For $n \geq 2$, let $N_n(X) := \#\{K/\mathbb{Q} : [K : \mathbb{Q}] = n, |\mathrm{Disc}(K)| \leq X\}$.

Bounds on number fields

For $n \geq 2$, let $N_n(X) := \#\{K/\mathbb{Q} : [K : \mathbb{Q}] = n, |\mathrm{Disc}(K)| \leq X\}$.

Conjecture: $N_n(X) \sim c_n X$ for some $c_n > 0$.

Bounds on number fields

For $n \geq 2$, let $N_n(X) := \#\{K/\mathbb{Q} : [K : \mathbb{Q}] = n, |\mathrm{Disc}(K)| \leq X\}$.

Conjecture: $N_n(X) \sim c_n X$ for some $c_n > 0$.

Known only for $n \leq 5$. (Davenport–Heilbronn; Bhargava)

Bounds on number fields

For $n \geq 2$, let $N_n(X) := \#\{K/\mathbb{Q} : [K : \mathbb{Q}] = n, |\mathrm{Disc}(K)| \leq X\}$.

Conjecture: $N_n(X) \sim c_n X$ for some $c_n > 0$.

Known only for $n \leq 5$. (Davenport–Heilbronn; Bhargava)

Lower bounds: $N_n(X) \gg_n X^{\frac{1}{2}+\frac{1}{n}}$.

Bounds on number fields

For $n \geq 2$, let $N_n(X) := \#\{K/\mathbb{Q} : [K : \mathbb{Q}] = n, |\mathrm{Disc}(K)| \leq X\}$.

Conjecture: $N_n(X) \sim c_n X$ for some $c_n > 0$.

Known only for $n \leq 5$. (Davenport–Heilbronn; Bhargava)

Lower bounds: $N_n(X) \gg_n X^{\frac{1}{2}+\frac{1}{n}}$.

Uses monogenic fields. (Bhargava–Shankar–Wang)

Bounds on number fields

For $n \geq 2$, let $N_n(X) := \#\{K/\mathbb{Q} : [K:\mathbb{Q}] = n, |\mathrm{Disc}(K)| \leq X\}$.

Conjecture: $N_n(X) \sim c_n X$ for some $c_n > 0$.

Known only for $n \leq 5$. (Davenport–Heilbronn; Bhargava)

Lower bounds: $N_n(X) \gg_n X^{\frac{1}{2}+\frac{1}{n}}$.

Uses monogenic fields. (Bhargava–Shankar–Wang)

Upper bounds: This talk!

Bounds on number fields

For $n \geq 2$, let $N_n(X) := \#\{K/\mathbb{Q} : [K : \mathbb{Q}] = n, |\mathrm{Disc}(K)| \leq X\}$.

Conjecture: $N_n(X) \sim c_n X$ for some $c_n > 0$.

Known only for $n \leq 5$. (Davenport–Heilbronn; Bhargava)

Lower bounds: $N_n(X) \gg_n X^{\frac{1}{2}+\frac{1}{n}}$.

Uses monogenic fields. (Bhargava–Shankar–Wang)

Upper bounds: This talk!

Much further from expected answer.

Bounds on number fields

For $n \geq 2$, let $N_n(X) := \#\{K/\mathbb{Q} : [K : \mathbb{Q}] = n, |\mathrm{Disc}(K)| \leq X\}$.

Conjecture: $N_n(X) \sim c_n X$ for some $c_n > 0$.

Known only for $n \leq 5$. (Davenport–Heilbronn; Bhargava)

Lower bounds: $N_n(X) \gg_n X^{\frac{1}{2}+\frac{1}{n}}$.

Uses monogenic fields. (Bhargava–Shankar–Wang)

Upper bounds: This talk!

Much further from expected answer.

Previous work of Schmidt, Ellenberg–Venkatesh, Couveignes.

Upper bounds on number fields

Recall: $N_n(X) := \#\{K/\mathbb{Q} : [K : \mathbb{Q}] = n, |\mathrm{Disc}(K)| \leq X\}$

- **Schmidt** (1995): $N_n(X) \ll_n X^{\frac{n+2}{4}}$.

Upper bounds on number fields

Recall: $N_n(X) := \#\{K/\mathbb{Q} : [K:\mathbb{Q}] = n, |\mathrm{Disc}(K)| \leq X\}$

- **Schmidt** (1995): $N_n(X) \ll_n X^{\frac{n+2}{4}}$.
- **Ellenberg–Venkatesh** (2006): $N_n(X) \ll_n X^{e^{c\sqrt{\log n}}}$.

Upper bounds on number fields

Recall: $N_n(X) := \#\{K/\mathbb{Q} : [K:\mathbb{Q}] = n, |\mathrm{Disc}(K)| \leq X\}$

- **Schmidt** (1995): $N_n(X) \ll_n X^{\frac{n+2}{4}}$.
- **Ellenberg–Venkatesh** (2006): $N_n(X) \ll_n X^{e^{c\sqrt{\log n}}}$.
- **Couveignes** (2019): $N_n(X) \ll_n X^{c(\log n)^3}$.

Upper bounds on number fields

Recall: $N_n(X) := \#\{K/\mathbb{Q} : [K : \mathbb{Q}] = n, |\mathrm{Disc}(K)| \leq X\}$

- **Schmidt** (1995): $N_n(X) \ll_n X^{\frac{n+2}{4}}$.
- **Ellenberg–Venkatesh** (2006): $N_n(X) \ll_n X^{e^{c\sqrt{\log n}}}$.
- **Couveignes** (2019): $N_n(X) \ll_n X^{c(\log n)^3}$.

Theorem (L.O.–Thorne; 2020)

$N_n(X) \ll_n X^{c(\log n)^2}$.

Upper bounds on number fields

Recall: $N_n(X) := \#\{K/\mathbb{Q} : [K:\mathbb{Q}] = n, |\mathrm{Disc}(K)| \leq X\}$

- **Schmidt** (1995): $N_n(X) \ll_n X^{\frac{n+2}{4}}$.
- **Ellenberg–Venkatesh** (2006): $N_n(X) \ll_n X^{e^{c\sqrt{\log n}}}$.
- **Couveignes** (2019): $N_n(X) \ll_n X^{c(\log n)^3}$.

Theorem (L.O.–Thorne; 2020)

$N_n(X) \ll_n X^{c(\log n)^2}$.

This improves on Schmidt for large n (in fact, $n \geq 95$).

Upper bounds on number fields

Recall: $N_n(X) := \#\{K/\mathbb{Q} : [K : \mathbb{Q}] = n, |\mathrm{Disc}(K)| \le X\}$

- **Schmidt** (1995): $N_n(X) \ll_n X^{\frac{n+2}{4}}$.
- **Ellenberg–Venkatesh** (2006): $N_n(X) \ll_n X^{e^{c\sqrt{\log n}}}$.
- **Couveignes** (2019): $N_n(X) \ll_n X^{c(\log n)^3}$.

Theorem (L.O.–Thorne; 2020)

$N_n(X) \ll_n X^{c(\log n)^2}$.

This improves on Schmidt for large n (in fact, $n \geq 95$).

- **AIM** (2022+; in progress): Improve Schmidt for all n
  - Lose to LO–Thorne for n sufficiently large (e.g., $n \geq 100$)

Schmidt's Idea

Idea: Every field is cut out by a polynomial.

Schmidt's Idea

Idea: Every field is cut out by a polynomial.

Question: Given K, what's the "smallest" polynomial $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ s.t. $K \simeq \mathbb{Q}(x)/(f(x))$?

Schmidt's Idea

Idea: Every field is cut out by a polynomial.

Question: Given K, what's the "smallest" polynomial $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ s.t. $K \simeq \mathbb{Q}(x)/(f(x))$?

Factoring $f(x) = (x - \alpha_1) \ldots (x - \alpha_n)$ over $\mathbb{C}$,

Schmidt's Idea

Idea: Every field is cut out by a polynomial.

Question: Given K, what's the "smallest" polynomial $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ s.t. $K \simeq \mathbb{Q}(x)/(f(x))$?

Factoring $f(x) = (x - \alpha_1) \ldots (x - \alpha_n)$ over $\mathbb{C}$, we obtain:

Nearly equivalent question: Given K, what's the smallest $\alpha \in \mathcal{O}_K$ measured by $\max\{|\alpha_1|, \ldots, |\alpha_n|\} =: ||\alpha||$?

Schmidt's Idea

Idea: Every field is cut out by a polynomial.

Question: Given K, what's the "smallest" polynomial $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ s.t. $K \simeq \mathbb{Q}(x)/(f(x))$?

Factoring $f(x) = (x - \alpha_1) \dots (x - \alpha_n)$ over $\mathbb{C}$, we obtain:

Nearly equivalent question: Given K, what's the smallest $\alpha \in \mathcal{O}_K$ measured by $\max\{|\alpha_1|, \dots, |\alpha_n|\} =: ||\alpha||$?

Minkowski embedding: $\mathcal{O}_K$ is a lattice in $\mathbb{R}^n$,

Schmidt's Idea

Idea: Every field is cut out by a polynomial.

Question: Given K, what's the "smallest" polynomial $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ s.t. $K \simeq \mathbb{Q}(x)/(f(x))$?

Factoring $f(x) = (x - \alpha_1) \ldots (x - \alpha_n)$ over $\mathbb{C}$, we obtain:

Nearly equivalent question: Given K, what's the smallest $\alpha \in \mathcal{O}_K$ measured by $\max\{|\alpha_1|, \ldots, |\alpha_n|\} =: ||\alpha||$?

Minkowski embedding: $\mathcal{O}_K$ is a lattice in $\mathbb{R}^n$, covolume $\sqrt{|\mathrm{Disc}(K)|}$,

Schmidt's Idea

Idea: Every field is cut out by a polynomial.

Question: Given K, what's the "smallest" polynomial $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ s.t. $K \simeq \mathbb{Q}(x)/(f(x))$?

Factoring $f(x) = (x - \alpha_1) \ldots (x - \alpha_n)$ over $\mathbb{C}$, we obtain:

Nearly equivalent question: Given K, what's the smallest $\alpha \in \mathcal{O}_K$ measured by $\max\{|\alpha_1|, \ldots, |\alpha_n|\} =: ||\alpha||$?

Minkowski embedding: $\mathcal{O}_K$ is a lattice in $\mathbb{R}^n$, covolume $\sqrt{|\mathrm{Disc}(K)|}$, shortest vector $\asymp_n 1$,

Schmidt's Idea

Idea: Every field is cut out by a polynomial.

Question: Given K, what's the "smallest" polynomial $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ s.t. $K \simeq \mathbb{Q}(x)/(f(x))$?

Factoring $f(x) = (x - \alpha_1) \ldots (x - \alpha_n)$ over $\mathbb{C}$, we obtain:

Nearly equivalent question: Given K, what's the smallest $\alpha \in \mathcal{O}_K$ measured by $\max\{|\alpha_1|, \ldots, |\alpha_n|\} =: ||\alpha||$?

Minkowski embedding: $\mathcal{O}_K$ is a lattice in $\mathbb{R}^n$, covolume $\sqrt{|\mathrm{Disc}(K)|}$, shortest vector $\asymp_n 1$,

$$\Rightarrow \exists \alpha \in \mathcal{O}_K \text{ with } ||\alpha|| \ll_n |\mathrm{Disc}(K)|^{\frac{1}{2n-2}}.$$

Schmidt's Idea, pt. 2

Just saw $\exists \alpha \in \mathcal{O}_K$ with $||\alpha|| \ll_n |\mathrm{Disc}(K)|^{\frac{1}{2n-2}}$.

Schmidt's Idea, pt. 2

Just saw $\exists \alpha \in \mathcal{O}_K$ with $||\alpha|| \ll_n |\mathrm{Disc}(K)|^{\frac{1}{2n-2}}$.

In fact, $\exists \alpha \in \mathcal{O}_K$ with $||\alpha|| \ll_n |\mathrm{Disc}(K)|^{\frac{1}{2n-2}}$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = 0$.

Schmidt's Idea, pt. 2

Just saw $\exists \alpha \in \mathcal{O}_K$ with $||\alpha|| \ll_n |\mathrm{Disc}(K)|^{\frac{1}{2n-2}}$.

In fact, $\exists \alpha \in \mathcal{O}_K$ with $||\alpha|| \ll_n |\mathrm{Disc}(K)|^{\frac{1}{2n-2}}$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = 0$.

Then $f_\alpha(x) = x^n + a_2 x^{n-2} + \cdots + a_n$, with

$$a_i \ll_n |\mathrm{Disc}(K)|^{\frac{i}{2n-2}}$$

Schmidt's Idea, pt. 2

Just saw $\exists \alpha \in \mathcal{O}_K$ with $||\alpha|| \ll_n |\mathrm{Disc}(K)|^{\frac{1}{2n-2}}$.

In fact, $\exists \alpha \in \mathcal{O}_K$ with $||\alpha|| \ll_n |\mathrm{Disc}(K)|^{\frac{1}{2n-2}}$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = 0$.

Then $f_\alpha(x) = x^n + a_2 x^{n-2} + \cdots + a_n$, with

$$a_i \ll_n |\mathrm{Disc}(K)|^{\frac{i}{2n-2}} \leq X^{\frac{i}{2n-2}}.$$

Schmidt's Idea, pt. 2

Just saw $\exists \alpha \in \mathcal{O}_K$ with $||\alpha|| \ll_n |\mathrm{Disc}(K)|^{\frac{1}{2n-2}}$.

In fact, $\exists \alpha \in \mathcal{O}_K$ with $||\alpha|| \ll_n |\mathrm{Disc}(K)|^{\frac{1}{2n-2}}$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = 0$.

Then $f_\alpha(x) = x^n + a_2 x^{n-2} + \cdots + a_n$, with

$$a_i \ll_n |\mathrm{Disc}(K)|^{\frac{i}{2n-2}} \leq X^{\frac{i}{2n-2}}.$$

There are $\ll_n X^{\frac{2}{2n-2} + \cdots + \frac{n}{2n-2}} = X^{\frac{n+2}{4}}$ such polynomials in $\mathbb{Z}[x]$,

Schmidt's Idea, pt. 2

Just saw $\exists \alpha \in \mathcal{O}_K$ with $||\alpha|| \ll_n |\mathrm{Disc}(K)|^{\frac{1}{2n-2}}$.

In fact, $\exists \alpha \in \mathcal{O}_K$ with $||\alpha|| \ll_n |\mathrm{Disc}(K)|^{\frac{1}{2n-2}}$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = 0$.

Then $f_\alpha(x) = x^n + a_2 x^{n-2} + \cdots + a_n$, with

$$a_i \ll_n |\mathrm{Disc}(K)|^{\frac{i}{2n-2}} \leq X^{\frac{i}{2n-2}}.$$

There are $\ll_n X^{\frac{2}{2n-2} + \cdots + \frac{n}{2n-2}} = X^{\frac{n+2}{4}}$ such polynomials in $\mathbb{Z}[x]$,
$\Rightarrow$ there are $\ll_n X^{\frac{n+2}{4}}$ fields.

Schmidt's Idea, pt. 2

Just saw $\exists\alpha \in \mathcal{O}_K$ with $||\alpha|| \ll_n |\mathrm{Disc}(K)|^{\frac{1}{2n-2}}$.

In fact, $\exists\alpha \in \mathcal{O}_K$ with $||\alpha|| \ll_n |\mathrm{Disc}(K)|^{\frac{1}{2n-2}}$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = 0$.

Then $f_\alpha(x) = x^n + a_2x^{n-2} + \cdots + a_n$, with

$$a_i \ll_n |\mathrm{Disc}(K)|^{\frac{i}{2n-2}} \leq X^{\frac{i}{2n-2}}.$$

There are $\ll_n X^{\frac{2}{2n-2}+\cdots+\frac{n}{2n-2}} = X^{\frac{n+2}{4}}$ such polynomials in $\mathbb{Z}[x]$,
$\Rightarrow$ there are $\ll_n X^{\frac{n+2}{4}}$ fields.

This is Schmidt's theorem.

Schmidt's Idea, pt. 2

Just saw $\exists \alpha \in \mathcal{O}_K$ with $||\alpha|| \ll_n |\mathrm{Disc}(K)|^{\frac{1}{2n-2}}$.

In fact, $\exists \alpha \in \mathcal{O}_K$ with $||\alpha|| \ll_n |\mathrm{Disc}(K)|^{\frac{1}{2n-2}}$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = 0$.

Then $f_\alpha(x) = x^n + a_2 x^{n-2} + \cdots + a_n$, with

$$a_i \ll_n |\mathrm{Disc}(K)|^{\frac{i}{2n-2}} \leq X^{\frac{i}{2n-2}}.$$

There are $\ll_n X^{\frac{2}{2n-2} + \cdots + \frac{n}{2n-2}} = X^{\frac{n+2}{4}}$ such polynomials in $\mathbb{Z}[x]$,
$\Rightarrow$ there are $\ll_n X^{\frac{n+2}{4}}$ fields.

This is Schmidt's theorem.

(**Caution:** Slight issue: what if $K \neq \mathbb{Q}(\alpha)$?

Schmidt's Idea, pt. 2

Just saw $\exists \alpha \in \mathcal{O}_K$ with $||\alpha|| \ll_n |\mathrm{Disc}(K)|^{\frac{1}{2n-2}}$.

In fact, $\exists \alpha \in \mathcal{O}_K$ with $||\alpha|| \ll_n |\mathrm{Disc}(K)|^{\frac{1}{2n-2}}$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = 0$.

Then $f_\alpha(x) = x^n + a_2 x^{n-2} + \cdots + a_n$, with

$$a_i \ll_n |\mathrm{Disc}(K)|^{\frac{i}{2n-2}} \leq X^{\frac{i}{2n-2}}.$$

There are $\ll_n X^{\frac{2}{2n-2} + \cdots + \frac{n}{2n-2}} = X^{\frac{n+2}{4}}$ such polynomials in $\mathbb{Z}[x]$,
$\Rightarrow$ there are $\ll_n X^{\frac{n+2}{4}}$ fields.

This is Schmidt's theorem.

(**Caution:** Slight issue: what if $K \neq \mathbb{Q}(\alpha)$? Schmidt inducts,

Schmidt's Idea, pt. 2

Just saw $\exists \alpha \in \mathcal{O}_K$ with $||\alpha|| \ll_n |\mathrm{Disc}(K)|^{\frac{1}{2n-2}}$.

In fact, $\exists \alpha \in \mathcal{O}_K$ with $||\alpha|| \ll_n |\mathrm{Disc}(K)|^{\frac{1}{2n-2}}$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = 0$.

Then $f_\alpha(x) = x^n + a_2 x^{n-2} + \cdots + a_n$, with

$$a_i \ll_n |\mathrm{Disc}(K)|^{\frac{i}{2n-2}} \leq X^{\frac{i}{2n-2}}.$$

There are $\ll_n X^{\frac{2}{2n-2} + \cdots + \frac{n}{2n-2}} = X^{\frac{n+2}{4}}$ such polynomials in $\mathbb{Z}[x]$,
$\Rightarrow$ there are $\ll_n X^{\frac{n+2}{4}}$ fields.

This is Schmidt's theorem.

(**Caution:** Slight issue: what if $K \neq \mathbb{Q}(\alpha)$? Schmidt inducts, details not important for this talk.)

Ellenberg–Venkatesh's idea

Ellenberg–Venkatesh's idea

What if we instead consider **pairs** $\alpha, \beta \in \mathcal{O}_K$?

Ellenberg–Venkatesh's idea

What if we instead consider **pairs** $\alpha, \beta \in \mathcal{O}_K$?

Bad idea: Could write down $f_\alpha(x)$ and $f_\beta(x)$ following Schmidt.

Ellenberg–Venkatesh's idea

What if we instead consider **pairs** $\alpha, \beta \in \mathcal{O}_K$?

Bad idea: Could write down $f_\alpha(x)$ and $f_\beta(x)$ following Schmidt.

$$f_\alpha(x) \Longleftrightarrow (\mathrm{Tr}_{K/\mathbb{Q}}(\alpha), \mathrm{Tr}_{K/\mathbb{Q}}(\alpha^2), \ldots, \mathrm{Tr}_{K/\mathbb{Q}}(\alpha^n)) \in \mathbb{Z}^n$$

Ellenberg–Venkatesh's idea

What if we instead consider **pairs** $\alpha, \beta \in \mathcal{O}_K$?

Bad idea: Could write down $f_\alpha(x)$ and $f_\beta(x)$ following Schmidt.

$$f_\alpha(x) \Longleftrightarrow (\mathrm{Tr}_{K/\mathbb{Q}}(\alpha), \mathrm{Tr}_{K/\mathbb{Q}}(\alpha^2), \ldots, \mathrm{Tr}_{K/\mathbb{Q}}(\alpha^n)) \in \mathbb{Z}^n$$

$$f_\beta(x) \Longleftrightarrow (\mathrm{Tr}_{K/\mathbb{Q}}(\beta), \mathrm{Tr}_{K/\mathbb{Q}}(\beta^2), \ldots, \mathrm{Tr}_{K/\mathbb{Q}}(\beta^n)) \in \mathbb{Z}^n$$

Ellenberg–Venkatesh's idea

What if we instead consider **pairs** $\alpha, \beta \in \mathcal{O}_K$?

Bad idea: Could write down $f_\alpha(x)$ and $f_\beta(x)$ following Schmidt.

$$f_\alpha(x) \Longleftrightarrow (\mathrm{Tr}_{K/\mathbb{Q}}(\alpha), \mathrm{Tr}_{K/\mathbb{Q}}(\alpha^2), \ldots, \mathrm{Tr}_{K/\mathbb{Q}}(\alpha^n)) \in \mathbb{Z}^n$$

$$f_\beta(x) \Longleftrightarrow (\mathrm{Tr}_{K/\mathbb{Q}}(\beta), \mathrm{Tr}_{K/\mathbb{Q}}(\beta^2), \ldots, \mathrm{Tr}_{K/\mathbb{Q}}(\beta^n)) \in \mathbb{Z}^n$$

Good idea: Let α and β mingle.

Ellenberg–Venkatesh's idea

What if we instead consider **pairs** $\alpha, \beta \in \mathcal{O}_K$?

Bad idea: Could write down $f_\alpha(x)$ and $f_\beta(x)$ following Schmidt.

$$f_\alpha(x) \Longleftrightarrow (\mathrm{Tr}_{K/\mathbb{Q}}(\alpha), \mathrm{Tr}_{K/\mathbb{Q}}(\alpha^2), \ldots, \mathrm{Tr}_{K/\mathbb{Q}}(\alpha^n)) \in \mathbb{Z}^n$$

$$f_\beta(x) \Longleftrightarrow (\mathrm{Tr}_{K/\mathbb{Q}}(\beta), \mathrm{Tr}_{K/\mathbb{Q}}(\beta^2), \ldots, \mathrm{Tr}_{K/\mathbb{Q}}(\beta^n)) \in \mathbb{Z}^n$$

Good idea: Let α and β mingle. Consider $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j) \in \mathbb{Z}$.

Invariants of pairs α, β

Suppose $\alpha, \beta \in \mathcal{O}_K$. Then

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j) = \alpha_1^i \beta_1^j + \alpha_2^i \beta_2^j + \cdots + \alpha_n^i \beta_n^j.$$

Invariants of pairs α, β

Suppose $\alpha, \beta \in \mathcal{O}_K$. Then

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j) = \alpha_1^i \beta_1^j + \alpha_2^i \beta_2^j + \cdots + \alpha_n^i \beta_n^j.$$

There are $\binom{n+2}{2} \approx \frac{n^2}{2}$ "mixed traces" $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j)$ with $i + j \leq n$.

Invariants of pairs α, β

Suppose $\alpha, \beta \in \mathcal{O}_K$. Then

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j) = \alpha_1^i \beta_1^j + \alpha_2^i \beta_2^j + \cdots + \alpha_n^i \beta_n^j.$$

There are $\binom{n+2}{2} \approx \frac{n^2}{2}$ "mixed traces" $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j)$ with $i + j \leq n$.

Idea: If "enough" $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j)$ are specified, can solve for $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$.

Invariants of pairs α, β

Suppose $\alpha, \beta \in \mathcal{O}_K$. Then

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j) = \alpha_1^i \beta_1^j + \alpha_2^i \beta_2^j + \cdots + \alpha_n^i \beta_n^j.$$

There are $\binom{n+2}{2} \approx \frac{n^2}{2}$ "mixed traces" $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j)$ with $i + j \leq n$.

Idea: If "enough" $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j)$ are specified, can solve for $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$.

Ellenberg–Venkatesh: $\approx 8n$ mixed traces are enough.

Invariants of pairs α, β

Suppose $\alpha, \beta \in \mathcal{O}_K$. Then

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j) = \alpha_1^i \beta_1^j + \alpha_2^i \beta_2^j + \cdots + \alpha_n^i \beta_n^j.$$

There are $\binom{n+2}{2} \approx \frac{n^2}{2}$ "mixed traces" $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j)$ with $i + j \leq n$.

Idea: If "enough" $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j)$ are specified, can solve for $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$.

Ellenberg–Venkatesh: $\approx 8n$ mixed traces are enough.

L.O.–Thorne: The $2n$ mixed traces with smallest $i + j$ are enough.

Invariants of pairs α, β

Suppose $\alpha, \beta \in \mathcal{O}_K$. Then

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j) = \alpha_1^i \beta_1^j + \alpha_2^i \beta_2^j + \cdots + \alpha_n^i \beta_n^j.$$

There are $\binom{n+2}{2} \approx \frac{n^2}{2}$ "mixed traces" $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j)$ with $i + j \leq n$.

Idea: If "enough" $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j)$ are specified, can solve for $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$.

Ellenberg–Venkatesh: $\approx 8n$ mixed traces are enough.

L.O.–Thorne: The $2n$ mixed traces with smallest $i + j$ are enough. (More on this later!)

Consequences for field counting

The $2n$ traces $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j)$ with smallest $i + j$ are "enough."

Consequences for field counting

The $2n$ traces $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j)$ with smallest $i + j$ are "enough."

$\Rightarrow i + j \approx 2\sqrt{n}$

Consequences for field counting

The $2n$ traces $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j)$ with smallest $i+j$ are “enough.”

$\Rightarrow i + j \approx 2\sqrt{n}$

If $||\alpha||, ||\beta|| \ll_n Y$, then $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j) \ll_n Y^{i+j}$

Consequences for field counting

The $2n$ traces $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j)$ with smallest $i + j$ are "enough."

$\Rightarrow i + j \approx 2\sqrt{n}$

If $||\alpha||, ||\beta|| \ll_n Y$, then $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j) \ll_n Y^{i+j} = Y^{O(n^{1/2})}$.

Consequences for field counting

The $2n$ traces $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j)$ with smallest $i + j$ are "enough."

$\Rightarrow i + j \approx 2\sqrt{n}$

If $||\alpha||, ||\beta|| \ll_n Y$, then $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j) \ll_n Y^{i+j} = Y^{O(n^{1/2})}$.

$2n$ different invariants $\Rightarrow$ there are $\ll_n Y^{O(n^{3/2})}$ choices for α, β

Consequences for field counting

The $2n$ traces $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j)$ with smallest $i + j$ are "enough."

$\Rightarrow i + j \approx 2\sqrt{n}$

If $||\alpha||, ||\beta|| \ll_n Y$, then $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j) \ll_n Y^{i+j} = Y^{O(n^{1/2})}$.

$2n$ different invariants $\Rightarrow$ there are $\ll_n Y^{O(n^{3/2})}$ choices for α, β

$\Rightarrow Y^{O(n^{3/2})}$ choices for K

Consequences for field counting

The $2n$ traces $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j)$ with smallest $i + j$ are "enough."

$\Rightarrow i + j \approx 2\sqrt{n}$

If $||\alpha||, ||\beta|| \ll_n Y$, then $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j) \ll_n Y^{i+j} = Y^{O(n^{1/2})}$.

$2n$ different invariants $\Rightarrow$ there are $\ll_n Y^{O(n^{3/2})}$ choices for α, β

$\Rightarrow Y^{O(n^{3/2})}$ choices for K

Schmidt: $Y = X^{\frac{1}{2n-2}}$.

Consequences for field counting

The $2n$ traces $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i\beta^j)$ with smallest $i+j$ are "enough."
$\Rightarrow i+j \approx 2\sqrt{n}$

If $||\alpha||, ||\beta|| \ll_n Y$, then $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i\beta^j) \ll_n Y^{i+j} = Y^{O(n^{1/2})}$.

$2n$ different invariants $\Rightarrow$ there are $\ll_n Y^{O(n^{3/2})}$ choices for α, β
$\Rightarrow Y^{O(n^{3/2})}$ choices for K

Schmidt: $Y = X^{\frac{1}{2n-2}}$. For "technical reasons," we take $Y = X^{\frac{1}{n}}$.

Consequences for field counting

The $2n$ traces $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j)$ with smallest $i + j$ are "enough."

$\Rightarrow i + j \approx 2\sqrt{n}$

If $||\alpha||, ||\beta|| \ll_n Y$, then $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j) \ll_n Y^{i+j} = Y^{O(n^{1/2})}$.

$2n$ different invariants $\Rightarrow$ there are $\ll_n Y^{O(n^{3/2})}$ choices for α, β

$\Rightarrow Y^{O(n^{3/2})}$ choices for K

Schmidt: $Y = X^{\frac{1}{2n-2}}$. For "technical reasons," we take $Y = X^{\frac{1}{n}}$.

Theorem: $N_n(X) \ll_n X^{\frac{8}{3}\sqrt{n}}$.

Going further

Going further

We can apply the same idea to triples $\alpha, \beta, \gamma \in \mathcal{O}_K$, looking at $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j \gamma^k) \in \mathbb{Z}$.

Going further

We can apply the same idea to triples $\alpha, \beta, \gamma \in \mathcal{O}_K$, looking at $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j \gamma^k) \in \mathbb{Z}$.

Or, more generally, to r-tuples $\alpha_1, \ldots, \alpha_r \in \mathcal{O}_K$, looking at $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_1^{i_1} \ldots \alpha_r^{i_r}) \in \mathbb{Z}$.

Going further

We can apply the same idea to triples $\alpha, \beta, \gamma \in \mathcal{O}_K$, looking at $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j \gamma^k) \in \mathbb{Z}$.

Or, more generally, to r-tuples $\alpha_1, \ldots, \alpha_r \in \mathcal{O}_K$, looking at $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_1^{i_1} \ldots \alpha_r^{i_r}) \in \mathbb{Z}$.

Ellenberg–Venkatesh: $\approx 2^{2r-1} n$ mixed traces are "enough" to determine $\alpha_1, \ldots, \alpha_r$ (and therefore K).

Going further

We can apply the same idea to triples $\alpha, \beta, \gamma \in \mathcal{O}_K$, looking at $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j \gamma^k) \in \mathbb{Z}$.

Or, more generally, to r-tuples $\alpha_1, \ldots, \alpha_r \in \mathcal{O}_K$, looking at $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_1^{i_1} \ldots \alpha_r^{i_r}) \in \mathbb{Z}$.

Ellenberg–Venkatesh: $\approx 2^{2r-1}n$ mixed traces are "enough" to determine $\alpha_1, \ldots, \alpha_r$ (and therefore K).

L.O.–Thorne: $r \cdot n$ traces with "small" $i_1 + \cdots + i_r$ are enough.

Going further

We can apply the same idea to triples $\alpha, \beta, \gamma \in \mathcal{O}_K$, looking at $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j \gamma^k) \in \mathbb{Z}$.

Or, more generally, to r-tuples $\alpha_1, \ldots, \alpha_r \in \mathcal{O}_K$, looking at $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_1^{i_1} \ldots \alpha_r^{i_r}) \in \mathbb{Z}$.

Ellenberg–Venkatesh: $\approx 2^{2r-1} n$ mixed traces are "enough" to determine $\alpha_1, \ldots, \alpha_r$ (and therefore K).

L.O.–Thorne: $r \cdot n$ traces with "small" $i_1 + \cdots + i_r$ are enough.

Main theorem uses $r \approx \log n$.

Going further

We can apply the same idea to triples $\alpha, \beta, \gamma \in \mathcal{O}_K$, looking at $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^i \beta^j \gamma^k) \in \mathbb{Z}$.

Or, more generally, to r-tuples $\alpha_1, \ldots, \alpha_r \in \mathcal{O}_K$, looking at $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_1^{i_1} \ldots \alpha_r^{i_r}) \in \mathbb{Z}$.

Ellenberg–Venkatesh: $\approx 2^{2r-1} n$ mixed traces are "enough" to determine $\alpha_1, \ldots, \alpha_r$ (and therefore K).

L.O.–Thorne: $r \cdot n$ traces with "small" $i_1 + \cdots + i_r$ are enough.

Main theorem uses $r \approx \log n$.

Question: How do we actually show a set of traces is enough?

Enough is enough: an example

Suppose $n = 3$ and $r = 2$.

Enough is enough: an example

Suppose $n = 3$ and $r = 2$. Replace "variables" α_i by x_i and β_i by y_i.

Enough is enough: an example

Suppose $n = 3$ and $r = 2$. Replace "variables" α_i by x_i and β_i by y_i. We're considering the equations

$$\begin{aligned} T_{1,0}\colon x_1 + x_2 + x_3 &= \mathrm{Tr}(\alpha), & T_{0,1}\colon y_1 + y_2 + y_3 &= \mathrm{Tr}(\beta), \\ T_{2,0}\colon x_1^2 + x_2^2 + x_3^2 &= \mathrm{Tr}(\alpha^2), & T_{1,1}\colon x_1 y_1 + x_2 y_2 + x_3 y_3 &= \mathrm{Tr}(\alpha\beta), \\ T_{0,2}\colon y_1^2 + y_2^2 + y_3^2 &= \mathrm{Tr}(\beta^2), & T_{3,0}\colon x_1^3 + x_2^3 + x_3^3 &= \mathrm{Tr}(\alpha^3). \end{aligned}$$

Enough is enough: an example

Suppose $n = 3$ and $r = 2$. Replace "variables" α_i by x_i and β_i by y_i. We're considering the equations

$$\begin{aligned} T_{1,0}\colon x_1 + x_2 + x_3 &= \mathrm{Tr}(\alpha), & T_{0,1}\colon y_1 + y_2 + y_3 &= \mathrm{Tr}(\beta), \\ T_{2,0}\colon x_1^2 + x_2^2 + x_3^2 &= \mathrm{Tr}(\alpha^2), & T_{1,1}\colon x_1 y_1 + x_2 y_2 + x_3 y_3 &= \mathrm{Tr}(\alpha\beta), \\ T_{0,2}\colon y_1^2 + y_2^2 + y_3^2 &= \mathrm{Tr}(\beta^2), & T_{3,0}\colon x_1^3 + x_2^3 + x_3^3 &= \mathrm{Tr}(\alpha^3). \end{aligned}$$

We want to show we can "solve" for $x_1, \ldots, y_3$ given the traces.

Enough is enough: an example

Suppose $n = 3$ and $r = 2$. Replace "variables" α_i by x_i and β_i by y_i. We're considering the equations

$$\begin{aligned} T_{1,0}\colon x_1 + x_2 + x_3 &= \mathrm{Tr}(\alpha), & T_{0,1}\colon y_1 + y_2 + y_3 &= \mathrm{Tr}(\beta), \\ T_{2,0}\colon x_1^2 + x_2^2 + x_3^2 &= \mathrm{Tr}(\alpha^2), & T_{1,1}\colon x_1 y_1 + x_2 y_2 + x_3 y_3 &= \mathrm{Tr}(\alpha\beta), \\ T_{0,2}\colon y_1^2 + y_2^2 + y_3^2 &= \mathrm{Tr}(\beta^2), & T_{3,0}\colon x_1^3 + x_2^3 + x_3^3 &= \mathrm{Tr}(\alpha^3). \end{aligned}$$

We want to show we can "solve" for $x_1, \ldots, y_3$ given the traces.

Actual goal: Want to show the variety cut out by these eq'ns has dimension 0.

Computing dimensions

Goal: Show that dim $V\,(T_{1,0}, T_{0,1}, T_{2,0}, T_{1,1}, T_{0,2}, T_{3,0}) = 0$.

Computing dimensions

Goal: Show that dim $V\,(T_{1,0}, T_{0,1}, T_{2,0}, T_{1,1}, T_{0,2}, T_{3,0}) = 0$.

Compute the tangent space, i.e. the kernel of the 6×6 matrix

$$D := \begin{pmatrix} \nabla T_{1,0} \\ \nabla T_{0,1} \\ \nabla T_{2,0} \\ \nabla T_{1,1} \\ \nabla T_{0,2} \\ \nabla T_{3,0} \end{pmatrix}.$$

Computing dimensions

Goal: Show that $\dim V\,(T_{1,0}, T_{0,1}, T_{2,0}, T_{1,1}, T_{0,2}, T_{3,0}) = 0$.

Compute the tangent space, i.e. the kernel of the 6×6 matrix

$$D := \begin{pmatrix} \nabla T_{1,0} \\ \nabla T_{0,1} \\ \nabla T_{2,0} \\ \nabla T_{1,1} \\ \nabla T_{0,2} \\ \nabla T_{3,0} \end{pmatrix}.$$

Hope $\ker D = 0$,

Computing dimensions

Goal: Show that $\dim V\,(T_{1,0}, T_{0,1}, T_{2,0}, T_{1,1}, T_{0,2}, T_{3,0}) = 0$.

Compute the tangent space, i.e. the kernel of the 6×6 matrix

$$D := \begin{pmatrix} \nabla T_{1,0} \\ \nabla T_{0,1} \\ \nabla T_{2,0} \\ \nabla T_{1,1} \\ \nabla T_{0,2} \\ \nabla T_{3,0} \end{pmatrix}.$$

Hope $\ker D = 0$, i.e. $\det D \neq 0$.

Computing dimensions

Goal: Show that $\dim V\,(T_{1,0}, T_{0,1}, T_{2,0}, T_{1,1}, T_{0,2}, T_{3,0}) = 0$.

Compute the tangent space, i.e. the kernel of the 6×6 matrix

$$D := \begin{pmatrix} \nabla T_{1,0} \\ \nabla T_{0,1} \\ \nabla T_{2,0} \\ \nabla T_{1,1} \\ \nabla T_{0,2} \\ \nabla T_{3,0} \end{pmatrix}.$$

Hope $\ker D = 0$, i.e. $\det D \neq 0$. In fact,

$$\det D = -12(x_1-x_2)(x_1-x_3)(x_2-x_3)(x_1y_2-x_1y_3-x_2y_1+x_2y_3+x_3y_1-x_3y_2).$$

Back to number fields

Upshot: $\det D$ is a non-zero polynomial

Back to number fields

Upshot: $\det D$ is a non-zero polynomial such that if $\det D(\vec{\alpha}, \vec{\beta}) \neq 0$,

Back to number fields

Upshot: $\det D$ is a non-zero polynomial such that if $\det D(\vec{\alpha}, \vec{\beta}) \neq 0$, then the traces $\mathrm{Tr}(\alpha), \mathrm{Tr}(\beta), \mathrm{Tr}(\alpha^2), \mathrm{Tr}(\alpha\beta), \mathrm{Tr}(\beta^2), \mathrm{Tr}(\alpha^3)$ determine K.

Back to number fields

Upshot: $\det D$ is a non-zero polynomial such that if $\det D(\vec{\alpha}, \vec{\beta}) \neq 0$, then the traces $\mathrm{Tr}(\alpha), \mathrm{Tr}(\beta), \mathrm{Tr}(\alpha^2), \mathrm{Tr}(\alpha\beta), \mathrm{Tr}(\beta^2), \mathrm{Tr}(\alpha^3)$ determine K.

Lemma

If $P\colon (\mathbb{C}^n)^r \to \mathbb{C}$ *is a non-zero polynomial and* $[K : \mathbb{Q}] = n$*,*

Back to number fields

Upshot: $\det D$ is a non-zero polynomial such that if $\det D(\vec{\alpha}, \vec{\beta}) \neq 0$, then the traces $\mathrm{Tr}(\alpha), \mathrm{Tr}(\beta), \mathrm{Tr}(\alpha^2), \mathrm{Tr}(\alpha\beta), \mathrm{Tr}(\beta^2), \mathrm{Tr}(\alpha^3)$ determine K.

Lemma

If $P\colon (\mathbb{C}^n)^r \to \mathbb{C}$ is a non-zero polynomial and $[K : \mathbb{Q}] = n$, then there exist $\alpha_1, \ldots, \alpha_r \in \mathcal{O}_K$ with each $||\alpha_i|| \ll_{n,P} |\mathrm{Disc}(K)|^{1/n}$ such that $P(\vec{\alpha_1}, \ldots, \vec{\alpha_r}) \neq 0$.

Back to number fields

Upshot: $\det D$ is a non-zero polynomial such that if $\det D(\vec{\alpha}, \vec{\beta}) \neq 0$, then the traces $\mathrm{Tr}(\alpha), \mathrm{Tr}(\beta), \mathrm{Tr}(\alpha^2), \mathrm{Tr}(\alpha\beta), \mathrm{Tr}(\beta^2), \mathrm{Tr}(\alpha^3)$ determine K.

Lemma

If $P\colon (\mathbb{C}^n)^r \to \mathbb{C}$ is a non-zero polynomial and $[K:\mathbb{Q}] = n$, then there exist $\alpha_1, \ldots, \alpha_r \in \mathcal{O}_K$ with each $||\alpha_i|| \ll_{n,P} |\mathrm{Disc}(K)|^{1/n}$ such that $P(\vec{\alpha_1}, \ldots, \vec{\alpha_r}) \neq 0$.

Applied to $\det D$ with $n = 3$, $r = 2$, we find:

$$N_3(X) \ll X^{\frac{1+1+2+2+2+3}{3}}$$

Back to number fields

Upshot: $\det D$ is a non-zero polynomial such that if $\det D(\vec{\alpha}, \vec{\beta}) \neq 0$, then the traces $\mathrm{Tr}(\alpha), \mathrm{Tr}(\beta), \mathrm{Tr}(\alpha^2), \mathrm{Tr}(\alpha\beta), \mathrm{Tr}(\beta^2), \mathrm{Tr}(\alpha^3)$ determine K.

Lemma

If $P \colon (\mathbb{C}^n)^r \to \mathbb{C}$ is a non-zero polynomial and $[K : \mathbb{Q}] = n$, then there exist $\alpha_1, \ldots, \alpha_r \in \mathcal{O}_K$ with each $||\alpha_i|| \ll_{n,P} |\mathrm{Disc}(K)|^{1/n}$ such that $P(\vec{\alpha_1}, \ldots, \vec{\alpha_r}) \neq 0$.

Applied to $\det D$ with $n = 3$, $r = 2$, we find:

$$N_3(X) \ll X^{\frac{1+1+2+2+2+3}{3}} = X^{11/3}.$$

Back to number fields

Upshot: $\det D$ is a non-zero polynomial such that if $\det D(\vec{\alpha}, \vec{\beta}) \neq 0$, then the traces $\mathrm{Tr}(\alpha), \mathrm{Tr}(\beta), \mathrm{Tr}(\alpha^2), \mathrm{Tr}(\alpha\beta), \mathrm{Tr}(\beta^2), \mathrm{Tr}(\alpha^3)$ determine K.

Lemma

If $P\colon (\mathbb{C}^n)^r \to \mathbb{C}$ is a non-zero polynomial and $[K : \mathbb{Q}] = n$, then there exist $\alpha_1, \ldots, \alpha_r \in \mathcal{O}_K$ with each $||\alpha_i|| \ll_{n,P} |\mathrm{Disc}(K)|^{1/n}$ such that $P(\vec{\alpha_1}, \ldots, \vec{\alpha_r}) \neq 0$.

Applied to $\det D$ with $n = 3$, $r = 2$, we find:

$$N_3(X) \ll X^{\frac{1+1+2+2+2+3}{3}} = X^{11/3}.$$

In general, we've transformed the problem into showing a (horrible!) determinant is a non-zero polynomial.

Determinants when $r = 2$

Theorem (LO–Thorne; $r = 2$)

If D is the $2n \times 2n$ matrix of partial derivatives of the first $2n$ functions $T_{1,0}, T_{0,1}, T_{2,0}, T_{1,1}, \ldots$, with

$$T_{a,b} := \sum_{i=1}^{n} x_i^a y_i^b,$$

then $\det D$ *is a non-zero polynomial in $x_1, \ldots, y_n$.*

Determinants when $r = 2$

Theorem (LO–Thorne; $r = 2$)

If D is the $2n \times 2n$ matrix of partial derivatives of the first $2n$ functions $T_{1,0}, T_{0,1}, T_{2,0}, T_{1,1}, \ldots,$ with

$$T_{a,b} := \sum_{i=1}^{n} x_i^a y_i^b,$$

then $\det D$ *is a non-zero polynomial in $x_1, \ldots, y_n$.*

Proof.

Induction. $n \mapsto n + 1$ gives two new rows and two new columns.
Cofactor expansion $\Rightarrow$ new 2×2 contribution not canceled. □

Determinants when $r = 2$

Theorem (LO–Thorne; $r = 2$)

If D is the $2n \times 2n$ matrix of partial derivatives of the first $2n$ functions $T_{1,0}, T_{0,1}, T_{2,0}, T_{1,1}, \ldots$, with

$$T_{a,b} := \sum_{i=1}^{n} x_i^a y_i^b,$$

then $\det D$ *is a non-zero polynomial in $x_1, \ldots, y_n$.*

Proof.

Induction. $n \mapsto n+1$ gives two new rows and two new columns. Cofactor expansion $\Rightarrow$ new 2×2 contribution not canceled. □

Leads to the bound $N_n(X) \ll X^{\frac{8}{3}\sqrt{n}}$.

Determinants when $r > 2$

Theorem (LO–Thorne; $r > 2$)

Let $n \geq 6$ and $r \geq 3$.

Determinants when $r > 2$

Theorem (LO–Thorne; $r > 2$)

Let $n \geq 6$ and $r \geq 3$. Suppose d is such that $\binom{d+r-1}{r-1} \geq r \cdot n$, and that $(d, r, n) \neq (3, 5, 7), (4, 5, 14)$.

Determinants when $r > 2$

Theorem (LO–Thorne; $r > 2$)

Let $n \geq 6$ and $r \geq 3$. Suppose d is such that $\binom{d+r-1}{r-1} \geq r \cdot n$, and that $(d, r, n) \neq (3, 5, 7), (4, 5, 14)$. Then there is a set of $r \cdot n$ functions of the form $T_{a_1,\ldots,a_r}$ with $a_1 + \cdots + a_r = d$ such that $\det D$ is a non-zero polynomial.

Determinants when $r > 2$

Theorem (LO–Thorne; $r > 2$)

Let $n \geq 6$ and $r \geq 3$. Suppose d is such that $\binom{d+r-1}{r-1} \geq r \cdot n$, and that $(d, r, n) \neq (3, 5, 7), (4, 5, 14)$. Then there is a set of $r \cdot n$ functions of the form $T_{a_1,\ldots,a_r}$ with $a_1 + \cdots + a_r = d$ such that $\det D$ is a non-zero polynomial.

Proof.

Uses a hammer from algebraic geometry, the Alexander–Hirschowitz theorem. □

Determinants when $r > 2$

Theorem (LO–Thorne; $r > 2$)

Let $n \geq 6$ and $r \geq 3$. Suppose d is such that $\binom{d+r-1}{r-1} \geq r \cdot n$, and that $(d, r, n) \neq (3, 5, 7), (4, 5, 14)$. Then there is a set of $r \cdot n$ functions of the form $T_{a_1, \ldots, a_r}$ with $a_1 + \cdots + a_r = d$ such that $\det D$ is a non-zero polynomial.

Proof.

Uses a hammer from algebraic geometry, the Alexander–Hirschowitz theorem. □

Leads to the bound $N_n(X) \ll_n (X^{\frac{d}{n}})^{rn} = X^{dr}$

Determinants when $r > 2$

Theorem (LO–Thorne; $r > 2$)

Let $n \geq 6$ and $r \geq 3$. Suppose d is such that $\binom{d+r-1}{r-1} \geq r \cdot n$, and that $(d, r, n) \neq (3, 5, 7), (4, 5, 14)$. Then there is a set of $r \cdot n$ functions of the form $T_{a_1,\ldots,a_r}$ with $a_1 + \cdots + a_r = d$ such that $\det D$ is a non-zero polynomial.

Proof.

Uses a hammer from algebraic geometry, the Alexander–Hirschowitz theorem. □

Leads to the bound $N_n(X) \ll_n (X^{\frac{d}{n}})^{rn} = X^{dr} = X^{O(r^2 n^{\frac{1}{r-1}})}$.

Summary

Theorem (LO–Thorne; explicit version)

1) Let d be the least integer for which $\binom{d+2}{2} \geq 2n+1$. *Then*

$$N_n(X) \ll_n X^{2d - \frac{d(d-1)(d+4)}{6n}} \ll X^{\frac{8\sqrt{n}}{3}}.$$

2) Let $3 \leq r \leq n$ *and let d be such that* $\binom{d+r-1}{r-1} \geq rn$. *Then* $N_n(X) \ll_{n,r,d} X^{dr}$.

Summary

Theorem (LO–Thorne; explicit version)

1) Let d be the least integer for which $\binom{d+2}{2} \geq 2n+1$. Then

$$N_n(X) \ll_n X^{2d - \frac{d(d-1)(d+4)}{6n}} \ll X^{\frac{8\sqrt{n}}{3}}.$$

2) Let $3 \leq r \leq n$ and let d be such that $\binom{d+r-1}{r-1} \geq rn$. Then $N_n(X) \ll_{n,r,d} X^{dr}$.

Theorem (LO–Thorne; asymptotic version)

There is a constant $c > 0$ such that $N_n(X) \ll_n X^{c(\log n)^2}$. In fact, $c = 1.564$ is admissible.

Thank you!