A singular approach to solving quintic equations

Trevor D. Wooley

University of Bristol

Toronto 05/04/2008

*Supported in part by a Royal Society Wolfson Research Merit Award

1. Solving cubic equations

Consider

$$F(\mathbf{x}) = \sum_{1 \le i \le j \le k \le s} c_{ijk} x_i x_j x_k \in \mathbb{Z}[\mathbf{x}],$$

a homogeneous cubic form with (fixed) integer coefficients c_{ijk}, and having s variables.

1. Solving cubic equations

Consider

$$F(\mathbf{x}) = \sum_{1 \le i \le j \le k \le s} c_{ijk} x_i x_j x_k \in \mathbb{Z}[\mathbf{x}],$$

a homogeneous cubic form with (fixed) integer coefficients c_{ijk}, and having s variables.

The **1950's** ... a race to solve the:

Problem

Is it true that with some $s_0 < \infty$, the equation

$$F(\mathbf{x}) = 0$$

is always soluble with $\mathbf{x} \in \mathbb{Z}^s \setminus \{\mathbf{0}\}$, provided only that $s \ge s_0$?

1. Solving cubic equations

Consider

$$F(\mathbf{x}) = \sum_{1 \le i \le j \le k \le s} c_{ijk} x_i x_j x_k \in \mathbb{Z}[\mathbf{x}],$$

a homogeneous cubic form with (fixed) integer coefficients c_{ijk}, and having s variables.

The **1950's** ... a race to solve the:

Problem

Is it true that with some $s_0 < \infty$, the equation

$$F(\mathbf{x}) = 0$$

is always soluble with $\mathbf{x} \in \mathbb{Z}^s \setminus \{\mathbf{0}\}$, provided only that $s \ge s_0$?

Why do we care?

1. Solving cubic equations

Consider

$$F(\mathbf{x}) = \sum_{1 \le i \le j \le k \le s} c_{ijk} x_i x_j x_k \in \mathbb{Z}[\mathbf{x}],$$

a homogeneous cubic form with (fixed) integer coefficients c_{ijk}, and having s variables.

The **1950's** ... a race to solve the:

Problem

Is it true that with some $s_0 < \infty$, the equation

$$F(\mathbf{x}) = 0$$

is always soluble with $\mathbf{x} \in \mathbb{Z}^s \setminus \{\mathbf{0}\}$, provided only that $s \ge s_0$?

Why do we care?

All part of the great quest to solve equations (over the integers).

Observation (Linear equations (easy!))

The equation

$$a_1x_1 + \cdots + a_sx_s = 0 \quad \textit{(fixed } a_i \in \mathbb{Z}\textit{)}$$

is soluble with $\mathbf{x} \in \mathbb{Z}^s \setminus \{\mathbf{0}\}$ *whenever* $s \geq 2$*.*

Observation (Linear equations (easy!))

The equation

$$a_1x_1 + \cdots + a_sx_s = 0 \quad \textit{(fixed } a_i \in \mathbb{Z}\textit{)}$$

is soluble with $\mathbf{x} \in \mathbb{Z}^s \setminus \{\mathbf{0}\}$ *whenever* $s \geq 2$.

Theorem (Quadratic equations (Meyer, 1880's; Hasse, 1924))

Provided that

$$\sum_{i=1}^{s}\sum_{j=1}^{s} a_{ij}x_ix_j = 0 \quad \textit{(fixed } a_{ij} \in \mathbb{Z}\textit{)}$$

possesses a solution $\mathbf{x} \in \mathbb{R}^s \setminus \{\mathbf{0}\}$ *and* $s \geq 5$, *then this equation is soluble with* $\mathbf{x} \in \mathbb{Z}^s \setminus \{\mathbf{0}\}$.

Observation (Linear equations (easy!))

The equation

$$a_1x_1 + \cdots + a_sx_s = 0 \quad \textit{(fixed } a_i \in \mathbb{Z}\textit{)}$$

is soluble with $\mathbf{x} \in \mathbb{Z}^s \setminus \{\mathbf{0}\}$ *whenever* $s \geq 2$*.*

Theorem (Quadratic equations (Meyer, 1880's; Hasse, 1924))

Provided that

$$\sum_{i=1}^{s} \sum_{j=1}^{s} a_{ij}x_ix_j = 0 \quad \textit{(fixed } a_{ij} \in \mathbb{Z}\textit{)}$$

possesses a solution $\mathbf{x} \in \mathbb{R}^s \setminus \{\mathbf{0}\}$ *and* $s \geq 5$*, then this equation is soluble with* $\mathbf{x} \in \mathbb{Z}^s \setminus \{\mathbf{0}\}$*.*

Cubics have non-trivial solutions over $\mathbb{R}$, but what about other local solubility conditions?

Theorem (Demyanov, 1950; Lewis, 1952)

Let $F(\mathbf{x}) \in \mathbb{Z}[x_1, \ldots, x_s]$ *be a cubic form. Then whenever* $s > 9$*, the equation* $F(\mathbf{x}) = 0$ *has a non-trivial solution* $\mathbf{x} \in \mathbb{Q}_p^s \setminus \{\mathbf{0}\}$.

Theorem (Demyanov, 1950; Lewis, 1952)

Let $F(\mathbf{x}) \in \mathbb{Z}[x_1, \ldots, x_s]$ *be a cubic form. Then whenever* $s > 9$, *the equation* $F(\mathbf{x}) = 0$ *has a non-trivial solution* $\mathbf{x} \in \mathbb{Q}_p^s \setminus \{\mathbf{0}\}$.

(Equivalent to $F(\mathbf{x}) \equiv 0 \pmod{p^h}$ having a primitive solution for all $h \in \mathbb{N}$.)

Theorem (Demyanov, 1950; Lewis, 1952)

Let $F(\mathbf{x}) \in \mathbb{Z}[x_1, \ldots, x_s]$ be a cubic form. Then whenever $s > 9$, the equation $F(\mathbf{x}) = 0$ has a non-trivial solution $\mathbf{x} \in \mathbb{Q}_p^s \setminus \{\mathbf{0}\}$.

(Equivalent to $F(\mathbf{x}) \equiv 0 \pmod{p^h}$ having a primitive solution for all $h \in \mathbb{N}$.)

The problem concerning solubility of cubic equations:

Problem

Is it true that with some $s_0 < \infty$, the equation

$$F(\mathbf{x}) = 0$$

is always soluble with $\mathbf{x} \in \mathbb{Z}^s \setminus \{\mathbf{0}\}$, provided only that $s \geq s_0$?

Theorem (Demyanov, 1950; Lewis, 1952)

Let $F(\mathbf{x}) \in \mathbb{Z}[x_1, \ldots, x_s]$ be a cubic form. Then whenever $s > 9$, the equation $F(\mathbf{x}) = 0$ has a non-trivial solution $\mathbf{x} \in \mathbb{Q}_p^s \setminus \{\mathbf{0}\}$.

(Equivalent to $F(\mathbf{x}) \equiv 0 \pmod{p^h}$ having a primitive solution for all $h \in \mathbb{N}$.)

The problem concerning solubility of cubic equations:

Problem

Is it true that with some $s_0 < \infty$, the equation

$$F(\mathbf{x}) = 0$$

is always soluble with $\mathbf{x} \in \mathbb{Z}^s \setminus \{\mathbf{0}\}$, provided only that $s \geq s_0$?

was solved in 1957 more or less simultaneously by Birch, Davenport and Lewis.

Mathematatika, vol. 4, December 1957:

"Editorial note — It is a curious coincidence that a problem which has been known for many years should have been solved independently in a matter of months by three mathematicians, namely (in order of priority) D. J. Lewis, H. Davenport and B. J. Birch. Birch's paper, which follows this one, is of greater generality in that it treats forms of any odd degree. Davenport's work, submitted to Phil. Trans. Royal Soc. (A) is limited to cubic forms with rational coefficients; it establishes that any such form in 32 *or more variables represents zero properly."*

Mathematatika, vol. 4, December 1957:

"Editorial note — It is a curious coincidence that a problem which has been known for many years should have been solved independently in a matter of months by three mathematicians, namely (in order of priority) D. J. Lewis, H. Davenport and B. J. Birch. Birch's paper, which follows this one, is of greater generality in that it treats forms of any odd degree. Davenport's work, submitted to Phil. Trans. Royal Soc. (A) is limited to cubic forms with rational coefficients; it establishes that any such form in 32 *or more variables represents zero properly."*

Historical Note: The Editor of Mathematika at this time was Harold Davenport

2. Davenport and the circle method

Write

$$f(\alpha) = \sum_{\mathbf{x} \in [-B,B]^s} e(\alpha F(\mathbf{x})) \quad (\alpha \in \mathbb{R}),$$

where $e(z) := e^{2\pi i z}$ and $B > 0$ is large (in terms of the coefficients of F).

2. Davenport and the circle method

Write

$$f(\alpha) = \sum_{\mathbf{x} \in [-B,B]^s} e(\alpha F(\mathbf{x})) \quad (\alpha \in \mathbb{R}),$$

where $e(z) := e^{2\pi i z}$ and $B > 0$ is large (in terms of the coefficients of F).

Then

$$\int_0^1 f(\alpha)\, d\alpha = \mathrm{card}\{\mathbf{x} \in [-B, B]^s \cap \mathbb{Z}^s \, : \, F(\mathbf{x}) = 0\}.$$

2. Davenport and the circle method

Write

$$f(\alpha) = \sum_{\mathbf{x} \in [-B,B]^s} e(\alpha F(\mathbf{x})) \quad (\alpha \in \mathbb{R}),$$

where $e(z) := e^{2\pi i z}$ and $B > 0$ is large (in terms of the coefficients of F).

Then

$$\int_0^1 f(\alpha)\, d\alpha = \mathrm{card}\{\mathbf{x} \in [-B,B]^s \cap \mathbb{Z}^s \,:\, F(\mathbf{x}) = 0\}.$$

Idea

Show that when $s \geq 32$ one has

$$\int_0^1 f(\alpha)\, d\alpha \gg B^{s-3}$$

by obtaining an asymptotic formula.

Theorem (Davenport, 1963)

Whenever $s \geq 16$ *and* $F(\mathbf{x}) \in \mathbb{Z}[x_1, \ldots, x_s]$ *is a homogeneous cubic, then the equation*

$$F(\mathbf{x}) = 0$$

has a solution $\mathbf{x} \in \mathbb{Z}^s \setminus \{\mathbf{0}\}$.

Theorem (Davenport, 1963)

Whenever $s \geq 16$ and $F(\mathbf{x}) \in \mathbb{Z}[x_1, \ldots, x_s]$ is a homogeneous cubic, then the equation

$$F(\mathbf{x}) = 0$$

has a solution $\mathbf{x} \in \mathbb{Z}^s \setminus \{\mathbf{0}\}$.

In particular, one has $s_0 \leq 16$.

Theorem (Davenport, 1963)

Whenever $s \geq 16$ *and* $F(\mathbf{x}) \in \mathbb{Z}[x_1, \ldots, x_s]$ *is a homogeneous cubic, then the equation*

$$F(\mathbf{x}) = 0$$

has a solution $\mathbf{x} \in \mathbb{Z}^s \setminus \{\mathbf{0}\}$.

In particular, one has $s_0 \leq 16$.

Recently this has been improved by Heath-Brown (to appear) so that $s_0 \leq 14$.

Theorem (Davenport, 1963)

Whenever $s \geq 16$ *and* $F(\mathbf{x}) \in \mathbb{Z}[x_1, \dots, x_s]$ *is a homogeneous cubic, then the equation*

$$F(\mathbf{x}) = 0$$

has a solution $\mathbf{x} \in \mathbb{Z}^s \setminus \{\mathbf{0}\}$*.*

In particular, one has $s_0 \leq 16$.

Recently this has been improved by Heath-Brown (to appear) so that $s_0 \leq 14$.

When $F(\mathbf{x}) = 0$ defines a non-singular hypersurface, then the analogue of s_0 satisfies $s_0 = 10$ (Heath-Brown, 1983)

Theorem (Davenport, 1963)

Whenever $s \geq 16$ *and* $F(\mathbf{x}) \in \mathbb{Z}[x_1, \ldots, x_s]$ *is a homogeneous cubic, then the equation*

$$F(\mathbf{x}) = 0$$

has a solution $\mathbf{x} \in \mathbb{Z}^s \setminus \{\mathbf{0}\}$.

In particular, one has $s_0 \leq 16$.

Recently this has been improved by Heath-Brown (to appear) so that $s_0 \leq 14$.

When $F(\mathbf{x}) = 0$ defines a non-singular hypersurface, then the analogue of s_0 satisfies $s_0 = 10$ (Heath-Brown, 1983)

Non-singular cubics in 9 or more variables satisfy the Hasse Principle (Hooley, 1988).

3. Birch and diagonalisation methods

Observation

Diagonal polynomials

$$a_1x_1^d + \cdots + a_sx_s^d$$

are relatively easy to handle (by means of straightforward applications of the circle method).

3. Birch and diagonalisation methods

Observation

Diagonal polynomials

$$a_1x_1^d + \cdots + a_sx_s^d$$

are relatively easy to handle (by means of straightforward applications of the circle method). So try to "diagonalise" general forms.

3. Birch and diagonalisation methods

Observation

Diagonal polynomials

$$a_1 x_1^d + \cdots + a_s x_s^d$$

are relatively easy to handle (by means of straightforward applications of the circle method). So try to "diagonalise" general forms.

Strategy

Find $\mathbf{u}_1, \ldots, \mathbf{u}_t \in \mathbb{Z}^s$ *so that*

$$F(z_1\mathbf{u}_1 + \cdots + z_t\mathbf{u}_t) = F(\mathbf{u}_1)z_1^3 + \cdots + F(\mathbf{u}_t)z_t^3$$

(in general t *will be much smaller than* s*!).*

Definition

When K is a field, denote by $\phi_d(K)$ the least integer s_1 such that, whenever $s > s_1$ and $b_1, \ldots, b_s \in \mathbb{K}$, then the equation

$$b_1 x_1^d + \cdots + b_s x_s^d = 0$$

has a solution $\mathbf{x} \in K^s \setminus \{\mathbf{0}\}$.

Definition

When K is a field, denote by $\phi_d(K)$ the least integer s_1 such that, whenever $s > s_1$ and $b_1, \ldots, b_s \in \mathbb{K}$, then the equation

$$b_1 x_1^d + \cdots + b_s x_s^d = 0$$

has a solution $\mathbf{x} \in K^s \setminus \{\mathbf{0}\}$.

Example

In all fields K, one has $\phi_1(K) = 1$ (linear algebra — the equation $a_1 x_1 + a_2 x_2 = 0$ is always soluble).

Definition

When K is a field, denote by $\phi_d(K)$ the least integer s_1 such that, whenever $s > s_1$ and $b_1, \ldots, b_s \in \mathbb{K}$, then the equation

$$b_1 x_1^d + \cdots + b_s x_s^d = 0$$

has a solution $\mathbf{x} \in K^s \setminus \{\mathbf{0}\}$.

Example

In all fields K, one has $\phi_1(K) = 1$ (linear algebra — the equation $a_1 x_1 + a_2 x_2 = 0$ is always soluble).

Example

One has $\phi_2(\mathbb{Q}) = +\infty$ and $\phi_2(\mathbb{R}) = +\infty$ (consider the definite forms $x_1^2 + \cdots + x_s^2$.)

Definition

When K is a field, denote by $\phi_d(K)$ the least integer s_1 such that, whenever $s > s_1$ and $b_1, \dots, b_s \in \mathbb{K}$, then the equation $b_1 x_1^d + \dots + b_s x_s^d = 0$ has a solution $\mathbf{x} \in K^s \setminus \{\mathbf{0}\}$.

Definition

When K is a field, denote by $\phi_d(K)$ the least integer s_1 such that, whenever $s > s_1$ and $b_1, \ldots, b_s \in \mathbb{K}$, then the equation $b_1 x_1^d + \cdots + b_s x_s^d = 0$ has a solution $\mathbf{x} \in K^s \setminus \{\mathbf{0}\}$.

Theorem (Davenport and Lewis, 1963)

For each $d \in \mathbb{N}$, one has $\phi_d(\mathbb{Q}_p) \leq d^2$.

Definition

When K is a field, denote by $\phi_d(K)$ the least integer s_1 such that, whenever $s > s_1$ and $b_1, \ldots, b_s \in \mathbb{K}$, then the equation $b_1 x_1^d + \cdots + b_s x_s^d = 0$ has a solution $\mathbf{x} \in K^s \setminus \{\mathbf{0}\}$.

Theorem (Davenport and Lewis, 1963)

For each $d \in \mathbb{N}$, one has $\phi_d(\mathbb{Q}_p) \leq d^2$.

Definition

When K is a field, denote by $v_d(K)$ the least s_2 such that, whenever $s > s_2$ and $F(\mathbf{x}) \in K[x_1, \ldots, x_s]$ is homogeneous of degree d, then the equation $F(\mathbf{x}) = 0$ has a solution $\mathbf{x} \in K^s \setminus \{\mathbf{0}\}$.

Definition

When K is a field, denote by $\phi_d(K)$ the least integer s_1 such that, whenever $s > s_1$ and $b_1, \ldots, b_s \in \mathbb{K}$, then the equation $b_1 x_1^d + \cdots + b_s x_s^d = 0$ has a solution $\mathbf{x} \in K^s \setminus \{\mathbf{0}\}$.

Theorem (Davenport and Lewis, 1963)

For each $d \in \mathbb{N}$, one has $\phi_d(\mathbb{Q}_p) \leq d^2$.

Definition

When K is a field, denote by $v_d(K)$ the least s_2 such that, whenever $s > s_2$ and $F(\mathbf{x}) \in K[x_1, \ldots, x_s]$ is homogeneous of degree d, then the equation $F(\mathbf{x}) = 0$ has a solution $\mathbf{x} \in K^s \setminus \{\mathbf{0}\}$.

Theorem (Brauer, 1945)

Let K be a field, and suppose that $\phi_i(K) < \infty$ for $2 \leq i \leq d$.

Definition

When K is a field, denote by $\phi_d(K)$ the least integer s_1 such that, whenever $s > s_1$ and $b_1, \ldots, b_s \in \mathbb{K}$, then the equation $b_1 x_1^d + \cdots + b_s x_s^d = 0$ has a solution $\mathbf{x} \in K^s \setminus \{\mathbf{0}\}$.

Theorem (Davenport and Lewis, 1963)

For each $d \in \mathbb{N}$, one has $\phi_d(\mathbb{Q}_p) \leq d^2$.

Definition

When K is a field, denote by $v_d(K)$ the least s_2 such that, whenever $s > s_2$ and $F(\mathbf{x}) \in K[x_1, \ldots, x_s]$ is homogeneous of degree d, then the equation $F(\mathbf{x}) = 0$ has a solution $\mathbf{x} \in K^s \setminus \{\mathbf{0}\}$.

Theorem (Brauer, 1945)

Let K be a field, and suppose that $\phi_i(K) < \infty$ for $2 \leq i \leq d$. Then one has $v_d(K) < \infty$.

Definition

When K is a field, denote by $v_d(K)$ the least s_2 such that, whenever $s > s_2$ and $F(\mathbf{x}) \in K[x_1, \ldots, x_s]$ is homogeneous of degree d, then the equation $F(\mathbf{x}) = 0$ has a solution $\mathbf{x} \in K^s \setminus \{\mathbf{0}\}$.

Theorem (Brauer, 1945)

Let K be a field, and suppose that $\phi_i(K) < \infty$ for $2 \leq i \leq d$. Then one has $v_d(K) < \infty$.

Definition

When K is a field, denote by $v_d(K)$ the least s_2 such that, whenever $s > s_2$ and $F(\mathbf{x}) \in K[x_1, \ldots, x_s]$ is homogeneous of degree d, then the equation $F(\mathbf{x}) = 0$ has a solution $\mathbf{x} \in K^s \setminus \{\mathbf{0}\}$.

Theorem (Brauer, 1945)

Let K be a field, and suppose that $\phi_i(K) < \infty$ for $2 \le i \le d$. Then one has $v_d(K) < \infty$.

Theorem (W., 1998)

One has

$$v_d(K) \le 2\phi_d(K)^{2^{d-2}} \prod_{i=2}^{d-1} (\phi_i(K) + 1)^{2^{i-2}}.$$

Definition

When K is a field, denote by $v_d(K)$ the least s_2 such that, whenever $s > s_2$ and $F(\mathbf{x}) \in K[x_1, \dots, x_s]$ is homogeneous of degree d, then the equation $F(\mathbf{x}) = 0$ has a solution $\mathbf{x} \in K^s \setminus \{\mathbf{0}\}$.

Theorem (Brauer, 1945)

Let K be a field, and suppose that $\phi_i(K) < \infty$ for $2 \le i \le d$. Then one has $v_d(K) < \infty$.

Theorem (W., 1998)

One has

$$v_d(K) \le 2\phi_d(K)^{2^{d-2}} \prod_{i=2}^{d-1} (\phi_i(K) + 1)^{2^{i-2}}.$$

Corollary

For each natural number d one has $v_d(\mathbb{Q}_p) \le d^{2^d}$.

Definition

When K is a field, denote by $v_d(K)$ the least s_2 such that, whenever $s > s_2$ and $F(\mathbf{x}) \in K[x_1, \dots, x_s]$ is homogeneous of degree d, then the equation $F(\mathbf{x}) = 0$ has a solution $\mathbf{x} \in K^s \setminus \{\mathbf{0}\}$.

Theorem (W., 1998)

One has

$$v_d(K) \le 2\phi_d(K)^{2^{d-2}} \prod_{i=2}^{d-1} (\phi_i(K) + 1)^{2^{i-2}}.$$

Corollary

For each natural number d one has $v_d(\mathbb{Q}_p) \le d^{2^d}$.

Definition

When K is a field, denote by $v_d(K)$ the least s_2 such that, whenever $s > s_2$ and $F(\mathbf{x}) \in K[x_1, \dots, x_s]$ is homogeneous of degree d, then the equation $F(\mathbf{x}) = 0$ has a solution $\mathbf{x} \in K^s \setminus \{\mathbf{0}\}$.

Theorem (W., 1998)

One has

$$v_d(K) \leq 2\phi_d(K)^{2^{d-2}} \prod_{i=2}^{d-1} (\phi_i(K) + 1)^{2^{i-2}}.$$

Corollary

For each natural number d one has $v_d(\mathbb{Q}_p) \leq d^{2^d}$.

(This just uses the bound $\phi_i(\mathbb{Q}_p) \leq i^2$ due to Davenport and Lewis (1963).)

Corollary (Peck, 1949)

Suppose that L is a purely imaginary field extension of $\mathbb{Q}$ (e.g. $\mathbb{Q}(\sqrt{-1})$). Then $v_d(L) < \infty$.

Corollary (Peck, 1949)

Suppose that L is a purely imaginary field extension of $\mathbb{Q}$ (e.g. $\mathbb{Q}(\sqrt{-1})$). Then $v_d(L) < \infty$.

Uses Siegel's version of the circle method for number fields — this shows that $\phi_d(L) < \infty$, but there is dependence on $[L : \mathbb{Q}]$.

Corollary (Peck, 1949)

Suppose that L is a purely imaginary field extension of $\mathbb{Q}$ (e.g. $\mathbb{Q}(\sqrt{-1})$). Then $v_d(L) < \infty$.

Uses Siegel's version of the circle method for number fields — this shows that $\phi_d(L) < \infty$, but there is dependence on $[L : \mathbb{Q}]$.

Theorem (W., 1998)

One has $v_d(L) \leq e^{2^{d+2}(\log d)^2}$.

Idea (diagonalisation)

Suppose that $F(\mathbf{x}) \in K[x_1, \ldots, x_s]$ *is homogeneous of degree* d.

Idea (diagonalisation)

Suppose that $F(\mathbf{x}) \in K[x_1, \ldots, x_s]$ is homogeneous of degree d. Observe that

$$F(t\mathbf{u} + w\mathbf{v}) = t^d F(\mathbf{u}) + w^d F(\mathbf{v}) + \sum_{i=1}^{d-1} t^i w^{d-i} G_i(\mathbf{u}, \mathbf{v}),$$

where the polynomials $G_i(\mathbf{u}, \mathbf{v}) \in K[\mathbf{u}, \mathbf{v}]$ are bihomogeneous of degree i in terms of $\mathbf{u}$, and degree $d - i$ in terms of $\mathbf{v}$.

Idea (diagonalisation)

Suppose that $F(\mathbf{x}) \in K[x_1, \ldots, x_s]$ *is homogeneous of degree* d. *Observe that*

$$F(t\mathbf{u} + w\mathbf{v}) = t^d F(\mathbf{u}) + w^d F(\mathbf{v}) + \sum_{i=1}^{d-1} t^i w^{d-i} G_i(\mathbf{u}, \mathbf{v}),$$

where the polynomials $G_i(\mathbf{u}, \mathbf{v}) \in K[\mathbf{u}, \mathbf{v}]$ *are bihomogeneous of degree* i *in terms of* $\mathbf{u}$, *and degree* $d - i$ *in terms of* $\mathbf{v}$.

Fix $\mathbf{u} \in K^s \setminus \{\mathbf{0}\}$, *and try to solve the system of equations*

$$G_i(\mathbf{u}, \mathbf{v}) = 0 \quad (1 \leq i \leq d - 1)$$

for $\mathbf{v}$

Idea (diagonalisation)

Suppose that $F(\mathbf{x}) \in K[x_1, \ldots, x_s]$ *is homogeneous of degree* d. *Observe that*

$$F(t\mathbf{u} + w\mathbf{v}) = t^d F(\mathbf{u}) + w^d F(\mathbf{v}) + \sum_{i=1}^{d-1} t^i w^{d-i} G_i(\mathbf{u}, \mathbf{v}),$$

where the polynomials $G_i(\mathbf{u}, \mathbf{v}) \in K[\mathbf{u}, \mathbf{v}]$ *are bihomogeneous of degree* i *in terms of* $\mathbf{u}$, *and degree* $d - i$ *in terms of* $\mathbf{v}$.

Fix $\mathbf{u} \in K^s \setminus \{\mathbf{0}\}$, *and try to solve the system of equations*

$$G_i(\mathbf{u}, \mathbf{v}) = 0 \quad (1 \le i \le d-1)$$

for $\mathbf{v}$ *(one equation of degree* $d-1$*,... , one equation of degree* 1*).*

Idea (diagonalisation)

Suppose that $F(\mathbf{x}) \in K[x_1, \ldots, x_s]$ *is homogeneous of degree* d. *Observe that*

$$F(t\mathbf{u} + w\mathbf{v}) = t^d F(\mathbf{u}) + w^d F(\mathbf{v}) + \sum_{i=1}^{d-1} t^i w^{d-i} G_i(\mathbf{u}, \mathbf{v}),$$

where the polynomials $G_i(\mathbf{u}, \mathbf{v}) \in K[\mathbf{u}, \mathbf{v}]$ *are bihomogeneous of degree* i *in terms of* $\mathbf{u}$, *and degree* $d - i$ *in terms of* $\mathbf{v}$.

Fix $\mathbf{u} \in K^s \setminus \{\mathbf{0}\}$, *and try to solve the system of equations*

$$G_i(\mathbf{u}, \mathbf{v}) = 0 \quad (1 \le i \le d - 1)$$

for $\mathbf{v}$ *(one equation of degree* $d - 1$*,... , one equation of degree* 1*).*

This system is of "smaller" degree than the original equation.

Idea (diagonalisation)

Suppose that $F(\mathbf{x}) \in K[x_1, \ldots, x_s]$ is homogeneous of degree d. Observe that

$$F(t\mathbf{u} + w\mathbf{v}) = t^d F(\mathbf{u}) + w^d F(\mathbf{v}) + \sum_{i=1}^{d-1} t^i w^{d-i} G_i(\mathbf{u}, \mathbf{v}),$$

where the polynomials $G_i(\mathbf{u}, \mathbf{v}) \in K[\mathbf{u}, \mathbf{v}]$ are bihomogeneous of degree i in terms of $\mathbf{u}$, and degree $d - i$ in terms of $\mathbf{v}$.

Fix $\mathbf{u} \in K^s \setminus \{\mathbf{0}\}$, and try to solve the system of equations

$$G_i(\mathbf{u}, \mathbf{v}) = 0 \quad (1 \leq i \leq d-1)$$

for $\mathbf{v}$ (one equation of degree $d-1$,... , one equation of degree 1).

This system is of "smaller" degree than the original equation. If we can solve this "smaller" system, then we can "diagonalise" $F(\mathbf{x})$ to

$$F(t\mathbf{u} + w\mathbf{v}) = t^d F(\mathbf{u}) + w^d F(\mathbf{v}).$$

Idea

So far ...

$$F(t\mathbf{u}+w\mathbf{v})=t^dF(\mathbf{u})+w^dF(\mathbf{v})$$

Idea

So far ...

$$F(t\mathbf{u} + w\mathbf{v}) = t^d F(\mathbf{u}) + w^d F(\mathbf{v})$$

Now use linear spaces, more variables, induction ...

$$F(t_1\mathbf{u}_1 + \cdots + t_m\mathbf{u}_m) = t_1^d F(\mathbf{u}_1) + \cdots + t_m^d F(\mathbf{u}_m)$$

(for $s \geq s_3(d, m)$, say).

Idea

So far ...

$$F(t\mathbf{u} + w\mathbf{v}) = t^d F(\mathbf{u}) + w^d F(\mathbf{v})$$

Now use linear spaces, more variables, induction ...

$$F(t_1\mathbf{u}_1 + \cdots + t_m\mathbf{u}_m) = t_1^d F(\mathbf{u}_1) + \cdots + t_m^d F(\mathbf{u}_m)$$

(for $s \geq s_3(d, m)$, say).
Take $m = \phi_d(K) + 1$, and then we can solve

$$t_1^d F(\mathbf{u}_1) + \cdots + t_m^d F(\mathbf{u}_m) = 0$$

for $\mathbf{t} \in K^m \setminus \{\mathbf{0}\}$, whence also

$$F(t_1\mathbf{u}_1 + \cdots + t_m\mathbf{u}_m) = 0.$$

Idea

So far ...

$$F(t\mathbf{u} + w\mathbf{v}) = t^d F(\mathbf{u}) + w^d F(\mathbf{v})$$

Now use linear spaces, more variables, induction ...

$$F(t_1\mathbf{u}_1 + \cdots + t_m\mathbf{u}_m) = t_1^d F(\mathbf{u}_1) + \cdots + t_m^d F(\mathbf{u}_m)$$

(for $s \geq s_3(d, m)$, say).

Take $m = \phi_d(K) + 1$, and then we can solve

$$t_1^d F(\mathbf{u}_1) + \cdots + t_m^d F(\mathbf{u}_m) = 0$$

for $\mathbf{t} \in K^m \setminus \{\mathbf{0}\}$, whence also

$$F(t_1\mathbf{u}_1 + \cdots + t_m\mathbf{u}_m) = 0.$$

Now the argument involves induction on the degree, and on the dimension of linear spaces of solutions, with the basis for the induction starting from systems of linear equations.

Obstruction to making such an argument work over $\mathbb{Q}$:

$$\phi_{2k}(\mathbb{Q}) = +\infty \quad (k \in \mathbb{N}).$$

Obstruction to making such an argument work over $\mathbb{Q}$:

$$\phi_{2k}(\mathbb{Q}) = +\infty \quad (k \in \mathbb{N}).$$

Theorem (Birch, 1957)

Let K be a field, and let d be an odd natural number. Suppose that $\phi_i(K) < \infty$ for each odd number i with $3 \leq i \leq d$. Then $v_d(K) < \infty$.

Theorem (Birch, 1957)

Let K be a field, and let d be an odd natural number. Suppose that $\phi_i(K) < \infty$ for each odd number i with $3 \le i \le d$. Then $v_d(K) < \infty$.

Theorem (Birch, 1957)

Let K be a field, and let d be an odd natural number. Suppose that $\phi_i(K) < \infty$ for each odd number i with $3 \le i \le d$. Then $v_d(K) < \infty$.

Idea

One has

$$\begin{aligned} F(t\mathbf{u} + w\mathbf{v}) =& t^d F(\mathbf{u}) + w^d F(\mathbf{v}) \\ &+ \sum_{\substack{i=1 \\ i \text{ odd}}}^{d-1} t^i w^{d-i} G_i(\mathbf{u}, \mathbf{v}) \\ &+ \sum_{\substack{j=1 \\ j \text{ even}}}^{d-1} t^j w^{d-j} G_j'(\mathbf{u}, \mathbf{v}), \end{aligned}$$

where each $G_i(\mathbf{u}, \mathbf{v})$ is bihomogeneous in $(\mathbf{u}, \mathbf{v})$ of bidegree $(i, d-i)$, and each $G_j'(\mathbf{u}, \mathbf{v})$ is bihomogeneous in $(\mathbf{u}, \mathbf{v})$ of bidegree $(j, d-j)$.

Idea

One has

$$\begin{aligned} F(t\mathbf{u}+w\mathbf{v}) =& t^d F(\mathbf{u}) + w^d F(\mathbf{v}) \\ & + \sum_{\substack{i=1 \\ i \text{ odd}}}^{d-1} t^i w^{d-i} G_i(\mathbf{u},\mathbf{v}) + \sum_{\substack{j=1 \\ j \text{ even}}}^{d-1} t^j w^{d-j} G_j'(\mathbf{u},\mathbf{v}), \end{aligned}$$

where each $G_i(\mathbf{u},\mathbf{v})$ is bihomogeneous in $(\mathbf{u},\mathbf{v})$ of bidegree $(i, d-i)$, and each $G_j'(\mathbf{u},\mathbf{v})$ is bihomogeneous in $(\mathbf{u},\mathbf{v})$ of bidegree $(j, d-j)$.

Idea

One has

$$\begin{aligned} F(t\mathbf{u}+w\mathbf{v}) =& t^d F(\mathbf{u}) + w^d F(\mathbf{v}) \\ & + \sum_{\substack{i=1 \\ i \text{ odd}}}^{d-1} t^i w^{d-i} G_i(\mathbf{u},\mathbf{v}) + \sum_{\substack{j=1 \\ j \text{ even}}}^{d-1} t^j w^{d-j} G'_j(\mathbf{u},\mathbf{v}), \end{aligned}$$

where each $G_i(\mathbf{u},\mathbf{v})$ *is bihomogeneous in* $(\mathbf{u},\mathbf{v})$ *of bidegree* $(i, d-i)$*, and each* $G'_j(\mathbf{u},\mathbf{v})$ *is bihomogeneous in* $(\mathbf{u},\mathbf{v})$ *of bidegree* $(j, d-j)$*.*

But i *and* $d-j$ *are both odd when* d *is odd,* i *is odd, and* j *is even.*

Idea

One has

$$\begin{aligned} F(t\mathbf{u}+w\mathbf{v}) =& t^d F(\mathbf{u}) + w^d F(\mathbf{v}) \\ & + \sum_{\substack{i=1 \\ i \text{ odd}}}^{d-1} t^i w^{d-i} G_i(\mathbf{u},\mathbf{v}) + \sum_{\substack{j=1 \\ j \text{ even}}}^{d-1} t^j w^{d-j} G_j'(\mathbf{u},\mathbf{v}), \end{aligned}$$

where each $G_i(\mathbf{u},\mathbf{v})$ is bihomogeneous in $(\mathbf{u},\mathbf{v})$ of bidegree $(i, d-i)$, and each $G_j'(\mathbf{u},\mathbf{v})$ is bihomogeneous in $(\mathbf{u},\mathbf{v})$ of bidegree $(j, d-j)$.

But i and $d-j$ are both odd when d is odd, i is odd, and j is even. So we can restrict to using odd degree equations only.

Idea

One has

$$\begin{aligned} F(t\mathbf{u}+w\mathbf{v}) =& t^d F(\mathbf{u}) + w^d F(\mathbf{v}) \\ &+ \sum_{\substack{i=1 \\ i \text{ odd}}}^{d-1} t^i w^{d-i} G_i(\mathbf{u},\mathbf{v}) + \sum_{\substack{j=1 \\ j \text{ even}}}^{d-1} t^j w^{d-j} G_j'(\mathbf{u},\mathbf{v}), \end{aligned}$$

where each $G_i(\mathbf{u},\mathbf{v})$ is bihomogeneous in $(\mathbf{u},\mathbf{v})$ of bidegree $(i, d-i)$, and each $G_j'(\mathbf{u},\mathbf{v})$ is bihomogeneous in $(\mathbf{u},\mathbf{v})$ of bidegree $(j, d-j)$.

But i and $d-j$ are both odd when d is odd, i is odd, and j is even. So we can restrict to using odd degree equations only.

Birch: *"Bounds (are) not even astronomical".*

Definition

Define

$$\psi^{(0)}(x) = \exp(x),$$

and for $n \geq 1$,

$$\psi^{(n)}(x) = \psi^{(n-1)}_{42 \log x}(x),$$

in which $f_r(x)$ means $f(f(\dots f(x) \dots))$, with the number of iterations equal to $[r]$.

Definition

Define

$$\psi^{(0)}(x) = \exp(x),$$

and for $n \geq 1$,

$$\psi^{(n)}(x) = \psi^{(n-1)}_{42 \log x}(x),$$

in which $f_r(x)$ means $f(f(\dots f(x)\dots))$, with the number of iterations equal to $[r]$.

Theorem (W., 1998)

When d is odd with $d \geq 7$, one has $v_d(\mathbb{Q}) < \psi^{((d-5)/2)}(d)$.

Definition

Define

$$\psi^{(0)}(x) = \exp(x),$$

and for $n \geq 1$,

$$\psi^{(n)}(x) = \psi^{(n-1)}_{42 \log x}(x),$$

in which $f_r(x)$ means $f(f(\ldots f(x)\ldots))$, with the number of iterations equal to $[r]$.

Theorem (W., 1998)

When d is odd with $d \geq 7$, one has $v_d(\mathbb{Q}) < \psi^{((d-5)/2)}(d)$.

As a side note (W., 1997), if one has a system of r quintic forms in s variables defined over $\mathbb{Q}$, then their solution set contains a non-trivial linear space of rational solutions of dimension m whenever

$$s > \exp(10^{32}((m+1)r\log(3r))^{5.872}\log(3r(m+1))).$$

Definition

Define

$$\psi^{(0)}(x) = \exp(x),$$

and for $n \geq 1$,

$$\psi^{(n)}(x) = \psi^{(n-1)}_{42 \log x}(x),$$

in which $f_r(x)$ means $f(f(\ldots f(x)\ldots))$, with the number of iterations equal to $[r]$.

Theorem (W., 1998)

When d is odd with $d \geq 7$, one has $v_d(\mathbb{Q}) < \psi^{((d-5)/2)}(d)$.

As a side note (W., 1997), if one has a system of r quintic forms in s variables defined over $\mathbb{Q}$, then their solution set contains a non-trivial linear space of rational solutions of dimension m whenever

$$s > \exp(10^{32}((m+1)r\log(3r))^{5.872}\log(3r(m+1))).$$

In particular, one has $v_5(\mathbb{Q}) < 10^{10^{32}}$.

4. Lewis and pulling points back from field extensions

4. Lewis and pulling points back from field extensions

Definition

When K is a field, and r and m are non-negative integers, let $\gamma_K(r;m)$ denote the least integer s such that, whenever $s > \gamma_K(r;m)$ and $f_i(\mathbf{x}) \in K[x_1,\dots,x_s]$ $(1 \le i \le r)$ are cubic forms, then the system

$$f_i(\mathbf{x}) = 0 \quad (1 \le i \le r)$$

has a solution set that contains a linear subspace of K^s of projective dimension m.

4. Lewis and pulling points back from field extensions

Definition

When K is a field, and r and m are non-negative integers, let $\gamma_K(r;m)$ denote the least integer s such that, whenever $s > \gamma_K(r;m)$ and $f_i(\mathbf{x}) \in K[x_1,\dots,x_s]$ $(1 \le i \le r)$ are cubic forms, then the system

$$f_i(\mathbf{x}) = 0 \quad (1 \le i \le r)$$

has a solution set that contains a linear subspace of K^s of projective dimension m.

Note: One has $v_3(K) = \gamma_K(1;0)$.

4. Lewis and pulling points back from field extensions

Definition

When K is a field, and r and m are non-negative integers, let $\gamma_K(r;m)$ denote the least integer s such that, whenever $s > \gamma_K(r;m)$ and $f_i(\mathbf{x}) \in K[x_1, \ldots, x_s]$ $(1 \le i \le r)$ are cubic forms, then the system

$$f_i(\mathbf{x}) = 0 \quad (1 \le i \le r)$$

has a solution set that contains a linear subspace of K^s of projective dimension m.

Note: One has $v_3(K) = \gamma_K(1;0)$.

Theorem (Lewis, 1957)

One has

$$\gamma_K(r;m) < \infty$$

for each field extension K of $\mathbb{Q}$, and for each r and m.

Definition

When K is a field, and r and m are non-negative integers, let $\gamma_K(r;m)$ denote the least integer s such that, whenever $s > \gamma_K(r;m)$ and $f_i(\mathbf{x}) \in K[x_1, \ldots, x_s]$ $(1 \le i \le r)$ are cubic forms, then the system

$$f_i(\mathbf{x}) = 0 \quad (1 \le i \le r)$$

has a solution set that contains a linear subspace of K^s of projective dimension m.

Note: One has $v_3(K) = \gamma_K(1;0)$.

Theorem (Lewis, 1957)

One has

$$\gamma_K(r;m) < \infty$$

for each field extension K of $\mathbb{Q}$, and for each r and m.

Definition

When K is a field, and r and m are non-negative integers, let $\gamma_K(r;m)$ denote the least integer s such that, whenever $s > \gamma_K(r;m)$ and $f_i(\mathbf{x}) \in K[x_1, \ldots, x_s]$ $(1 \le i \le r)$ are cubic forms, then the system

$$f_i(\mathbf{x}) = 0 \quad (1 \le i \le r)$$

has a solution set that contains a linear subspace of K^s of projective dimension m.

Note: One has $v_3(K) = \gamma_K(1;0)$.

Theorem (Lewis, 1957)

One has

$$\gamma_K(r;m) < \infty$$

for each field extension K of $\mathbb{Q}$, and for each r and m.

Corollary

One has $v_3(\mathbb{Q}) < \infty$.

Strategy

Try to solve cubic in $K(\sqrt{-1})$ (a purely imaginary field extension of $\mathbb{Q}$) in place of K, and then pull points back to K.

Strategy

Try to solve cubic in $K(\sqrt{-1})$ *(a purely imaginary field extension of* $\mathbb{Q}$*) in place of* K*, and then pull points back to* K*.*

One can apply Peck's Theorem to solve the cubic over $K(\sqrt{-1})$*. Now use some simple geometry to pull points back to* K *by considering conjugates.*

Strategy

Try to solve cubic in $K(\sqrt{-1})$ (a purely imaginary field extension of $\mathbb{Q}$) in place of K, and then pull points back to K.

One can apply Peck's Theorem to solve the cubic over $K(\sqrt{-1})$. Now use some simple geometry to pull points back to K by considering conjugates.

Idea

Solving equations in purely imaginary field extensions of $\mathbb{Q}$ is **"easier"** *than solving in fields that are not purely imaginary — every equation is indefinite.*

Some notation.

Some notation.

Write

$$f(\mathbf{x}) = \sum_{1 \leq i \leq j \leq k \leq s} c_{ijk} x_i x_j x_k.$$

Some notation.

Write

$$f(\mathbf{x}) = \sum_{1\le i\le j\le k\le s} c_{ijk} x_i x_j x_k.$$

Then put

$$T(\mathbf{x},\mathbf{y},\mathbf{z}) = \sum_{1\le i\le j\le k\le s} c_{ijk} x_i y_j z_k,$$

Some notation.

Write

$$f(\mathbf{x}) = \sum_{1 \le i \le j \le k \le s} c_{ijk} x_i x_j x_k.$$

Then put

$$T(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \sum_{1 \le i \le j \le k \le s} c_{ijk} x_i y_j z_k,$$

and then

$$f_{21}(\mathbf{x}, \mathbf{y}) = T(\mathbf{x}, \mathbf{x}, \mathbf{y}) + T(\mathbf{x}, \mathbf{y}, \mathbf{x}) + T(\mathbf{y}, \mathbf{x}, \mathbf{x}),$$

$$f_{12}(\mathbf{x}, \mathbf{y}) = f_{21}(\mathbf{y}, \mathbf{x}),$$

$$\begin{aligned} f_{111}(\mathbf{x}, \mathbf{y}, \mathbf{z}) = {} & T(\mathbf{x}, \mathbf{y}, \mathbf{z}) + T(\mathbf{x}, \mathbf{z}, \mathbf{y}) + T(\mathbf{y}, \mathbf{z}, \mathbf{x}) \\ & + T(\mathbf{y}, \mathbf{x}, \mathbf{z}) + T(\mathbf{z}, \mathbf{x}, \mathbf{y}) + T(\mathbf{z}, \mathbf{y}, \mathbf{x}). \end{aligned}$$

Lemma

Let K be a field, let $d \in K$ and suppose that $\sqrt{d} \notin K$. Suppose that a cubic form $f(\mathbf{x}) \in K[x_1, \ldots, x_s]$ possesses linearly independent zeros $\mathbf{v}_1, \ldots, \mathbf{v}_n \in K^s$ with the property that for each $t_1, \ldots, t_n$ one has

$$f(t_1\mathbf{v}_1 + \cdots + t_n\mathbf{v}_n) = 0.$$

Lemma

Let K be a field, let $d \in K$ and suppose that $\sqrt{d} \notin K$. Suppose that a cubic form $f(\mathbf{x}) \in K[x_1, \ldots, x_s]$ possesses linearly independent zeros $\mathbf{v}_1, \ldots, \mathbf{v}_n \in K^s$ with the property that for each $t_1, \ldots, t_n$ one has

$$f(t_1\mathbf{v}_1 + \cdots + t_n\mathbf{v}_n) = 0.$$

If the system of equations

$$f(\mathbf{x}) = f_{12}(\mathbf{v}_i, \mathbf{x}) = f_{21}(\mathbf{v}_i, \mathbf{x}) = f_{111}(\mathbf{v}_i, \mathbf{v}_j, \mathbf{x}) = 0,$$

with $1 \le i, j \le n$, has a solution over $K(\sqrt{d})$ which is linearly independent of $\mathbf{v}_1, \ldots, \mathbf{v}_n$ over $K(\sqrt{d})$,

Lemma

Let K be a field, let $d \in K$ and suppose that $\sqrt{d} \notin K$. Suppose that a cubic form $f(\mathbf{x}) \in K[x_1, \dots, x_s]$ possesses linearly independent zeros $\mathbf{v}_1, \dots, \mathbf{v}_n \in K^s$ with the property that for each $t_1, \dots, t_n$ one has

$$f(t_1\mathbf{v}_1 + \cdots + t_n\mathbf{v}_n) = 0.$$

If the system of equations

$$f(\mathbf{x}) = f_{12}(\mathbf{v}_i, \mathbf{x}) = f_{21}(\mathbf{v}_i, \mathbf{x}) = f_{111}(\mathbf{v}_i, \mathbf{v}_j, \mathbf{x}) = 0,$$

with $1 \le i, j \le n$, has a solution over $K(\sqrt{d})$ which is linearly independent of $\mathbf{v}_1, \dots, \mathbf{v}_n$ over $K(\sqrt{d})$, then $f(\mathbf{x})$ possesses linearly independent zeros $\mathbf{w}_0, \mathbf{w}_1, \dots, \mathbf{w}_n \in K^s$ with the property that for each $y_0, \dots, y_n$, one has

$$f(y_0\mathbf{w}_0 + \cdots + y_n\mathbf{w}_n) = 0.$$

Lemma

Let K be a field, let $d \in K$ and suppose that $\sqrt{d} \notin K$. Suppose that a cubic form $f(\mathbf{x}) \in K[x_1, \ldots, x_s]$ possesses linearly independent zeros $\mathbf{v}_1, \ldots, \mathbf{v}_n \in K^s$ with the property that for each $t_1, \ldots, t_n$ one has $f(t_1\mathbf{v}_1 + \cdots + t_n\mathbf{v}_n) = 0$. If the system of equations

$$f(\mathbf{x}) = f_{12}(\mathbf{v}_i, \mathbf{x}) = f_{21}(\mathbf{v}_i, \mathbf{x}) = f_{111}(\mathbf{v}_i, \mathbf{v}_j, \mathbf{x}) = 0,$$

with $1 \leq i, j \leq n$, has a solution over $K(\sqrt{d})$ which is linearly independent of $\mathbf{v}_1, \ldots, \mathbf{v}_n$ over $K(\sqrt{d})$, then $f(\mathbf{x})$ possesses linearly independent zeros $\mathbf{w}_0, \mathbf{w}_1, \ldots, \mathbf{w}_n \in K^s$ with the property that for each $y_0, \ldots, y_n$, one has $f(y_0\mathbf{w}_0 + \cdots + y_n\mathbf{w}_n) = 0$.

Lemma

Let K be a field, let $d \in K$ and suppose that $\sqrt{d} \notin K$. Suppose that a cubic form $f(\mathbf{x}) \in K[x_1, \ldots, x_s]$ possesses linearly independent zeros $\mathbf{v}_1, \ldots, \mathbf{v}_n \in K^s$ with the property that for each $t_1, \ldots, t_n$ one has $f(t_1\mathbf{v}_1 + \cdots + t_n\mathbf{v}_n) = 0$. If the system of equations

$$f(\mathbf{x}) = f_{12}(\mathbf{v}_i, \mathbf{x}) = f_{21}(\mathbf{v}_i, \mathbf{x}) = f_{111}(\mathbf{v}_i, \mathbf{v}_j, \mathbf{x}) = 0,$$

with $1 \leq i, j \leq n$, has a solution over $K(\sqrt{d})$ which is linearly independent of $\mathbf{v}_1, \ldots, \mathbf{v}_n$ over $K(\sqrt{d})$, then $f(\mathbf{x})$ possesses linearly independent zeros $\mathbf{w}_0, \mathbf{w}_1, \ldots, \mathbf{w}_n \in K^s$ with the property that for each $y_0, \ldots, y_n$, one has $f(y_0\mathbf{w}_0 + \cdots + y_n\mathbf{w}_n) = 0$.

Idea

We have 1 cubic, n quadratics and $\frac{1}{2}n(n+3)$ linear equations to solve. Either K is purely imaginary already, and we may apply Peck, or else $K(\sqrt{d})$ can be used instead as above.

Theorem (Dietmann and W., 2003)

Let L be an algebraic extension of $\mathbb{Q}$ (possibly $\mathbb{Q}$ itself). Then

$$\gamma_L(1; m) \leq \tfrac{1}{2}(5m^2 + 33m + 34).$$

Theorem (Dietmann and W., 2003)

Let L be an algebraic extension of $\mathbb{Q}$ (possibly $\mathbb{Q}$ itself). Then

$$\gamma_L(1; m) \le \tfrac{1}{2}(5m^2 + 33m + 34).$$

Now use an idea applied in Lewis' work from 1957 — find a large dimensional rational linear space on one cubic, and solve the second cubic inside this space.

Theorem (Dietmann and W., 2003)

Let L be an algebraic extension of $\mathbb{Q}$ (possibly $\mathbb{Q}$ itself). Then

$$\gamma_L(1; m) \leq \tfrac{1}{2}(5m^2 + 33m + 34).$$

Now use an idea applied in Lewis' work from 1957 — find a large dimensional rational linear space on one cubic, and solve the second cubic inside this space.

Corollary

One has $\gamma_{\mathbb{Q}}(2; 0) \leq 827$.

Theorem (Dietmann and W., 2003)

Let L be an algebraic extension of $\mathbb{Q}$ (possibly $\mathbb{Q}$ itself). Then

$$\gamma_L(1; m) \leq \tfrac{1}{2}(5m^2 + 33m + 34).$$

Now use an idea applied in Lewis' work from 1957 — find a large dimensional rational linear space on one cubic, and solve the second cubic inside this space.

Corollary

One has $\gamma_{\mathbb{Q}}(2; 0) \leq 827$.

Can now obtain $\gamma_{\mathbb{Q}}(2; 0) \leq 654$, possibly $\gamma_{\mathbb{Q}}(2; 0) \leq 626$.

Theorem (Dietmann and W., 2003)

Let L be an algebraic extension of $\mathbb{Q}$ (possibly $\mathbb{Q}$ itself). Then

$$\gamma_L(1; m) \leq \tfrac{1}{2}(5m^2 + 33m + 34).$$

Now use an idea applied in Lewis' work from 1957 — find a large dimensional rational linear space on one cubic, and solve the second cubic inside this space.

Corollary

One has $\gamma_{\mathbb{Q}}(2; 0) \leq 827$.

Can now obtain $\gamma_{\mathbb{Q}}(2; 0) \leq 654$, possibly $\gamma_{\mathbb{Q}}(2; 0) \leq 626$.
Can compare this to earlier work of Schmidt that had $\gamma_{\mathbb{Q}}(2; 0) \leq 5139$ using the circle method.

Theorem (Dietmann and W., 2003)

Let L be an algebraic extension of $\mathbb{Q}$ (possibly $\mathbb{Q}$ itself). Then

$$\gamma_L(1;m) \le \tfrac{1}{2}(5m^2 + 33m + 34).$$

Now use an idea applied in Lewis' work from 1957 — find a large dimensional rational linear space on one cubic, and solve the second cubic inside this space.

Corollary

One has $\gamma_{\mathbb{Q}}(2;0) \le 827$.

Can now obtain $\gamma_{\mathbb{Q}}(2;0) \le 654$, possibly $\gamma_{\mathbb{Q}}(2;0) \le 626$.
Can compare this to earlier work of Schmidt that had $\gamma_{\mathbb{Q}}(2;0) \le 5139$ using the circle method.

(Also refines a result of W. (1997) to the effect that $\gamma_{\mathbb{Q}}(2;0) \le 855$.)

What about quintics? So far we have only $v_5(\mathbb{Q}) < 10^{10^{32}}$.

5. Quintic forms

When $F(\mathbf{x}) \in \mathbb{Q}[x_1, \ldots, x_s]$ is a form of degree $d > 1$, write $h(F)$ for the least number h such that F may be written in the form

$$F = A_1 B_1 + A_2 B_2 + \cdots + A_h B_h,$$

with A_i, B_i forms in $\mathbb{Q}[\mathbf{x}]$ of positive degree $(1 \leq i \leq h)$.

$h(F) :=$ the least number h such that F may be written in the form

$$F = A_1 B_1 + A_2 B_2 + \cdots + A_h B_h,$$

with A_i, B_i forms in $\mathbb{Q}[\mathbf{x}]$ of positive degree $(1 \leq i \leq h)$.

$h(F) :=$ the least number h such that F may be written in the form

$$F = A_1 B_1 + A_2 B_2 + \cdots + A_h B_h,$$

with A_i, B_i forms in $\mathbb{Q}[\mathbf{x}]$ of positive degree $(1 \leq i \leq h)$.

Theorem (Schmidt, 1984)

Let d be an integer exceeding 1, and write $\chi(d) = d2^{4d}d!$.

$h(F) :=$ the least number h such that F may be written in the form

$$F = A_1 B_1 + A_2 B_2 + \cdots + A_h B_h,$$

with A_i, B_i forms in $\mathbb{Q}[\mathbf{x}]$ of positive degree ($1 \le i \le h$).

Theorem (Schmidt, 1984)

Let d be an integer exceeding 1, and write $\chi(d) = d2^{4d}d!$. Let $F(\mathbf{x}) \in \mathbb{Z}[x_1, \ldots, x_s]$ be homogeneous of degree d, and suppose that

$$h(F) \ge \chi(d) \max_p v_d(\mathbb{Q}_p).$$

$h(F) :=$ the least number h such that F may be written in the form

$$F = A_1 B_1 + A_2 B_2 + \cdots + A_h B_h,$$

with A_i, B_i forms in $\mathbb{Q}[\mathbf{x}]$ of positive degree $(1 \le i \le h)$.

Theorem (Schmidt, 1984)

Let d be an integer exceeding 1, and write $\chi(d) = d2^{4d}d!$. Let $F(\mathbf{x}) \in \mathbb{Z}[x_1, \ldots, x_s]$ be homogeneous of degree d, and suppose that

$$h(F) \ge \chi(d) \max_p v_d(\mathbb{Q}_p).$$

Then one has

$$\mathit{card}(\{\mathbf{x} \in [-B, B]^s \cap \mathbb{Z}^s \ : \ F(\mathbf{x}) = 0\}) \sim CB^{s-d},$$

where C denotes the "product of local densities" within the box $[-B, B]^s$

$h(F) :=$ the least number h such that F may be written in the form

$$F = A_1 B_1 + A_2 B_2 + \cdots + A_h B_h,$$

with A_i, B_i forms in $\mathbb{Q}[\mathbf{x}]$ of positive degree ($1 \le i \le h$).

Theorem (Schmidt, 1984)

Let d be an integer exceeding 1, and write $\chi(d) = d2^{4d}d!$. Let $F(\mathbf{x}) \in \mathbb{Z}[x_1, \ldots, x_s]$ be homogeneous of degree d, and suppose that

$$h(F) \ge \chi(d) \max_p v_d(\mathbb{Q}_p).$$

Then one has

$$card(\{\mathbf{x} \in [-B, B]^s \cap \mathbb{Z}^s \ : \ F(\mathbf{x}) = 0\}) \sim CB^{s-d},$$

where C denotes the "product of local densities" within the box $[-B, B]^s$ (under the hypotheses at hand, this is positive and bounded away from zero).

Strategy

Given a quintic form F, either $h(F)$ is large enough to apply the above theorem, or else $h(F)$ is "small".

Strategy

Given a quintic form F, either $h(F)$ is large enough to apply the above theorem, or else $h(F)$ is "small".

But then F may be rewritten in the shape

$$F = A_1 B_1 + \cdots + A_h B_h$$

wherein each polynomial A_i has degree either 3 or 1.

Strategy

Given a quintic form F, either $h(F)$ is large enough to apply the above theorem, or else $h(F)$ is "small".

But then F may be rewritten in the shape

$$F = A_1 B_1 + \cdots + A_h B_h$$

wherein each polynomial A_i has degree either 3 or 1. Now solve the system

$$A_1 = A_2 = \cdots = A_h = 0$$

over $\mathbb{Q}$.

Strategy

Given a quintic form F, either $h(F)$ is large enough to apply the above theorem, or else $h(F)$ is "small".

But then F may be rewritten in the shape

$$F = A_1 B_1 + \cdots + A_h B_h$$

wherein each polynomial A_i has degree either 3 or 1. Now solve the system

$$A_1 = A_2 = \cdots = A_h = 0$$

over $\mathbb{Q}$.

The above system might consist entirely of cubics, and then the number of variables required to guarantee success is something like $(10h)^5$.

Strategy

Given a quintic form F, either $h(F)$ is large enough to apply the above theorem, or else $h(F)$ is "small".

But then F may be rewritten in the shape

$$F = A_1 B_1 + \cdots + A_h B_h$$

wherein each polynomial A_i has degree either 3 or 1. Now solve the system

$$A_1 = A_2 = \cdots = A_h = 0$$

over $\mathbb{Q}$.

The above system might consist entirely of cubics, and then the number of variables required to guarantee success is something like $(10h)^5$.

Such an approach yields a bound roughly

$$v_5(\mathbb{Q}) \leq 10^{194}.$$

Instead seek singular solutions on the quintic hypersurface defined by $F = 0$.

Instead seek singular solutions on the quintic hypersurface defined by $F = 0$.

A theorem of Birch (1962) shows that when the number of variables exceeds the dimension of the singular locus by at least 128, and there is a non-singular p-adic point for each prime p, then the expected asymptotic formula holds for the number of integral solutions.

Instead seek singular solutions on the quintic hypersurface defined by $F = 0$.

A theorem of Birch (1962) shows that when the number of variables exceeds the dimension of the singular locus by at least 128, and there is a non-singular p-adic point for each prime p, then the expected asymptotic formula holds for the number of integral solutions.

But when the quintic is highly singular, one has little useful control.

Instead seek singular solutions on the quintic hypersurface defined by $F = 0$.

A theorem of Birch (1962) shows that when the number of variables exceeds the dimension of the singular locus by at least 128, and there is a non-singular p-adic point for each prime p, then the expected asymptotic formula holds for the number of integral solutions.

But when the quintic is highly singular, one has little useful control.

Strategy (Mk 2)

Given a quintic form F, either $h(F)$ is large enough to apply the above theorem, or else $h(F)$ is "small".

Instead seek singular solutions on the quintic hypersurface defined by $F = 0$.

A theorem of Birch (1962) shows that when the number of variables exceeds the dimension of the singular locus by at least 128, and there is a non-singular p-adic point for each prime p, then the expected asymptotic formula holds for the number of integral solutions.

But when the quintic is highly singular, one has little useful control.

Strategy (Mk 2)

Given a quintic form F, either $h(F)$ is large enough to apply the above theorem, or else $h(F)$ is "small".

But then F may be rewritten in the shape

$$F = A_1 B_1 + \cdots + A_h B_h$$

wherein each polynomial A_i has degree either 3 or 1.

Strategy (Mk 2)

Given a quintic form F, either $h(F)$ is large enough to apply the above theorem, or else $h(F)$ is "small".

But then F may be rewritten in the shape

$$F = A_1 B_1 + \cdots + A_h B_h$$

wherein each polynomial A_i has degree either 3 or 1.

Strategy (Mk 2)

Given a quintic form F, either $h(F)$ is large enough to apply the above theorem, or else $h(F)$ is "small".

But then F may be rewritten in the shape

$$F = A_1 B_1 + \cdots + A_h B_h$$

wherein each polynomial A_i has degree either 3 or 1.

Now solve the system

$$A_1 = B_1 = A_2 = B_2 = \cdots = A_h = B_h = 0$$

over $\mathbb{Q}(\sqrt{-1})$.

Strategy (Mk 2)

Given a quintic form F, either $h(F)$ is large enough to apply the above theorem, or else $h(F)$ is "small".

But then F may be rewritten in the shape

$$F = A_1B_1 + \cdots + A_hB_h$$

wherein each polynomial A_i has degree either 3 or 1.

Now solve the system

$$A_1 = B_1 = A_2 = B_2 = \cdots = A_h = B_h = 0$$

over $\mathbb{Q}(\sqrt{-1})$.

We can assume without loss that the A_i are all cubic and the B_i all quadratic, and then the number of variables required to guarantee the existence of a solution is relatively low (because the underlying field is purely imaginary) — requires roughly $18h^4$ variables (W., 1998).

Have a solution $\mathbf{x}$ of the system

$$A_1 = B_1 = A_2 = B_2 = \cdots = A_h = B_h = 0$$

over $\mathbb{Q}(\sqrt{-1})$.

Have a solution **x** of the system

$$A_1 = B_1 = A_2 = B_2 = \cdots = A_h = B_h = 0$$

over $\mathbb{Q}(\sqrt{-1})$.

Such a solution is necessarily singular, since

$$\frac{\partial F}{\partial x_i} = \sum_{j=1}^{h} \left(A_j \frac{\partial B_j}{\partial x_i} + B_j \frac{\partial A_j}{\partial x_i} \right) = 0 \quad (1 \le i \le s),$$

for any such solution.

Have a solution **x** of the system

$$A_1 = B_1 = A_2 = B_2 = \cdots = A_h = B_h = 0$$

over $\mathbb{Q}(\sqrt{-1})$.

Such a solution is necessarily singular, since

$$\frac{\partial F}{\partial x_i} = \sum_{j=1}^{h} \left(A_j \frac{\partial B_j}{\partial x_i} + B_j \frac{\partial A_j}{\partial x_i} \right) = 0 \quad (1 \le i \le s),$$

for any such solution.

Now apply our geometrical argument to pull this back to a $\mathbb{Q}$-point.

A further refinement comes from a similar geometrical argument that shows that whenever a quintic form has a p-adic point and enough variables, then either it has a non-singular p-adic point, or else it is degenerate.

A further refinement comes from a similar geometrical argument that shows that whenever a quintic form has a p-adic point and enough variables, then either it has a non-singular p-adic point, or else it is degenerate.

This allows the Schmidt argument to be substantially sharpened.

A further refinement comes from a similar geometrical argument that shows that whenever a quintic form has a p-adic point and enough variables, then either it has a non-singular p-adic point, or else it is degenerate.

This allows the Schmidt argument to be substantially sharpened.

Theorem (W., 2008)

One has $v_5(\mathbb{Q}) \leq 1.38 \times 10^{14}$.

A further refinement comes from a similar geometrical argument that shows that whenever a quintic form has a p-adic point and enough variables, then either it has a non-singular p-adic point, or else it is degenerate.

This allows the Schmidt argument to be substantially sharpened.

Theorem (W., 2008)

One has $v_5(\mathbb{Q}) \leq 1.38 \times 10^{14}$.

This comes from the best known bound for the number of variables required to solve 1664 simultaneous cubics and quadratics over $\mathbb{Q}(\sqrt{-1})$.

Other ideas:

(1) Think about decompositions of the shape

$$F = A_1 B_1 C_1 + \cdots + A_h B_h C_h$$

in the context of Schmidt's method? Higher order singularities?

Other ideas:

(1) Think about decompositions of the shape

$$F = A_1 B_1 C_1 + \cdots + A_h B_h C_h$$

in the context of Schmidt's method? Higher order singularities?

(2) Work with higher degree field extensions and pull the points back (cf. Coray for cubics).