Results and open problems related to Schmidt's Subspace Theorem

Jan-Hendrik Evertse
Universiteit Leiden

29$^{\text{ièmes}}$ Journées Arithmétiques

July 6, 2015, Debrecen

Slides can be downloaded from
http://pub.math.leidenuniv.nl/∼evertsejh/lectures.shtml

Dirichlet's Theorem

Define the height of $\xi \in \mathbb{Q}$ by

$$H(\xi) = \max(|x|, |y|),$$

where x, y are coprime integers with $\xi = x/y$.

Theorem (Dirichlet, 1842, small variation)

For every irrational real number α there is $c(\alpha) > 0$ such that the inequality

$$|\alpha - \xi| \leq c(\alpha) H(\xi)^{-2}$$

has infinitely many solutions in $\xi \in \mathbb{Q}$.

Proof.

Dirichlet's box principle. $\square$

Roth's Theorem

Theorem (Roth, 1955)

Let α be a real algebraic number and $\delta > 0$. Then the inequality

$$|\alpha - \xi| \leq H(\xi)^{-2-\delta} \tag{1}$$

has only finitely many solutions in $\xi \in \mathbb{Q}$.

Roth's proof, and later proofs of his theorem, are *ineffective*, i.e., they do not give a method to determine the solutions.

Roth's proof and the later ones allow to give an explicit upper bound for the *number* of approximants ξ.

There is a *semi-effective version* of Roth's Theorem, which gives an upper bound for the heights $H(\xi)$ of the approximants ξ that is effective in terms of the height of α but ineffective in other parameters.

Number of approximants

The minimal polynomial of an algebraic number α is the irreducible polynomial $F \in \mathbb{Z}[X]$ with coprime coefficients such that $F(\alpha) = 0$.

We define the height $H(\alpha) := \max|\text{coeff. of } F|$.

Theorem (Bugeaud and Ev., 2008)

Let α be a real algebraic number of degree d and height H and $0 < \delta \leq 1$. Then the number of $\xi \in \mathbb{Q}$ with

$$|\alpha - \xi| \leq H(\xi)^{-2-\delta} \tag{1}$$

is at most $2^{25}\left(\delta^{-1}\log\log 4H + \delta^{-3}\log\delta^{-1}\log 4d\log\log 4d\right)$.

Results of this type with larger upper bounds in terms of δ, d, H were obtained earlier by Davenport and Roth (1955), Mignotte (1974), Bombieri and van der Poorten (1987), and Corvaja (1996).

Number of approximants

The minimal polynomial of an algebraic number α is the irreducible polynomial $F \in \mathbb{Z}[X]$ with coprime coefficients such that $F(\alpha) = 0$.

We define the height $H(\alpha) := \max |\text{coeff. of } F|$.

Theorem (Bugeaud and Ev., 2008)

Let α be a real algebraic number of degree d and height H and $0 < \delta \leq 1$. Then the number of $\xi \in \mathbb{Q}$ with

$$|\alpha - \xi| \leq H(\xi)^{-2-\delta} \tag{1}$$

is at most $2^{25}\big(\delta^{-1} \log\log 4H + \delta^{-3} \log \delta^{-1} \log 4d \log\log 4d\big)$.

Theorem (Mueller and Schmidt, 1989)

There are infinitely many real algebraic numbers α of degree $\leq d$ such that (1) has at least

$$\tfrac{1}{2}\delta^{-1}(\log\log 4H(\alpha) + \log 4d)$$

solutions $\xi \in \mathbb{Q}$.

A semi-effective Roth's Theorem

Theorem (Bombieri and van der Poorten, 1987)

Let $\delta > 0$, α *a real algebraic number,* $K = \mathbb{Q}(\alpha)$ *and* $[K : \mathbb{Q}] = d$*. Then for every* $\xi \in \mathbb{Q}$ *with*

$$|\alpha - \xi| \leq H(\xi)^{-2-\delta} \tag{1}$$

we have $H(\xi) \leq \max\left(B^{\mathrm{ineff}}(\delta, K),\ H(\alpha)^{c^{\mathrm{eff}}(\delta,d)}\right)$.

Here c^{eff}, B^{ineff} *are constants, effectively, resp. not effectively computable from the method of proof, depending on the parameters between the parentheses.*

A semi-effective Roth's Theorem

Theorem (Bombieri and van der Poorten, 1987)

Let $\delta > 0$, α a real algebraic number, $K = \mathbb{Q}(\alpha)$ and $[K : \mathbb{Q}] = d$. Then for every $\xi \in \mathbb{Q}$ with

$$(1) \qquad |\alpha - \xi| \leq H(\xi)^{-2-\delta}$$

we have $H(\xi) \leq \max\left(B^{\text{ineff}}(\delta, K),\ H(\alpha)^{c^{\text{eff}}(\delta,d)}\right)$.

Here c^{eff}, B^{ineff} are constants, effectively, resp. not effectively computable from the method of proof, depending on the parameters between the parentheses.

Equivalent formulation ("Roth's Theorem with moving targets")

(1) *has only finitely many solutions $(\xi, \alpha) \in \mathbb{Q} \times K$ with $H(\xi) > H(\alpha)^{c^{\text{eff}}(\delta,d)}$.*

A semi-effective Roth's Theorem

Theorem (Bombieri and van der Poorten, 1987)

Let $\delta > 0$, α *a real algebraic number,* $K = \mathbb{Q}(\alpha)$ *and* $[K : \mathbb{Q}] = d$. *Then for every* $\xi \in \mathbb{Q}$ *with*

$$(1) \qquad |\alpha - \xi| \leq H(\xi)^{-2-\delta}$$

we have $H(\xi) \leq \max\left(B^{\mathrm{ineff}}(\delta, K),\ H(\alpha)^{c^{\mathrm{eff}}(\delta,d)}\right)$.

Here c^{eff}, B^{ineff} *are constants, effectively, resp. not effectively computable from the method of proof, depending on the parameters between the parentheses.*

Equivalent formulation ("Roth's Theorem with moving targets")

(1) *has only finitely many solutions* $(\xi, \alpha) \in \mathbb{Q} \times K$ *with* $H(\xi) > H(\alpha)^{c^{\mathrm{eff}}(\delta,d)}$.

Similar results follow from work of Vojta (1995), Corvaja (1997), McQuillan ($c^{\mathrm{eff}}(\delta, d) = O(d(1 + \delta^{-2}))$, published ?).

Schmidt's Subspace Theorem

Let $\overline{\mathbb{Q}}$ denote the field of algebraic numbers in $\mathbb{C}$ and let

$$L_i(\mathbf{X}) = \alpha_{i1}X_1 + \cdots + \alpha_{in}X_n \quad (i = 1, \ldots, n)$$

be linearly independent linear forms with coefficients $\alpha_{ij} \in \overline{\mathbb{Q}}$.

For $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n$, put $\|\mathbf{x}\| := \max_i |x_i|$.

Subspace Theorem (W.M. Schmidt, 1972)

Let $\delta > 0$. Then the set of solutions of

$$|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| \le \|\mathbf{x}\|^{-\delta} \text{ in } \mathbf{x} \in \mathbb{Z}^n \tag{2}$$

is contained in finitely many proper linear subspaces of $\mathbb{Q}^n$.

There are generalizations where the unknowns are taken from a number field and various archimedean and non-archimedean absolute values are involved. (Schmidt, Schlickewei)

Subspace Theorem $\Longrightarrow$ Roth's Theorem

Let α be a real algebraic number and $\delta > 0$, and consider the solutions x_1/x_2 with $x_1, x_2 \in \mathbb{Z}$ of

$$|\alpha - x_1/x_2| < H(x_1/x_2)^{-2-\delta} = \max(|x_1|, |x_2|)^{-2-\delta}.$$

These satisfy

$$|(x_1 - \alpha x_2)x_2| < \max(|x_1|, |x_2|)^{-\delta}.$$

By the Subspace Theorem, the pairs (x_1, x_2) lie in finitely many one-dimensional subspaces of $\mathbb{Q}^2$.

These give rise to finitely many fractions x_1/x_2. $\square$

Systems of inequalities

By a combinatorial argument, the inequality (2) $|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| \leq \|\mathbf{x}\|^{-\delta}$ can be reduced to finitely many systems of inequalities of the shape

$$(3) \qquad |L_1(\mathbf{x})| \leq \|\mathbf{x}\|^{c_1}, \ldots, |L_n(\mathbf{x})| \leq \|\mathbf{x}\|^{c_n} \quad \text{in } \mathbf{x} \in \mathbb{Z}^n,$$

where $c_1 + \cdots + c_n < 0$.

Systems of inequalities

By a combinatorial argument, the inequality (2) $|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| \le \|\mathbf{x}\|^{-\delta}$ can be reduced to finitely many systems of inequalities of the shape

$$(3) \qquad |L_1(\mathbf{x})| \le \|\mathbf{x}\|^{c_1}, \ldots, |L_n(\mathbf{x})| \le \|\mathbf{x}\|^{c_n} \quad \text{in } \mathbf{x} \in \mathbb{Z}^n,$$

where $c_1 + \cdots + c_n < 0$.

Proof (idea).

There is a bounded subset $\mathcal{S}$ of $\mathbb{R}^n$ such that if $\mathbf{x} \in \mathbb{Z}^n$ is a solution of (2), then

$$|L_1(\mathbf{x})| \le \|\mathbf{x}\|^{c_1(\mathbf{x})}, \ldots, |L_n(\mathbf{x})| \le \|\mathbf{x}\|^{c_n(\mathbf{x})},$$

with $\mathbf{c}(\mathbf{x}) = (c_1(\mathbf{x}), \ldots, c_n(\mathbf{x})) \in \mathcal{S}$.

Cover $\mathcal{S}$ by a very fine, finite grid. Then $\mathbf{x}$ satisfies (3) with $\mathbf{c} = (c_1, \ldots, c_n)$ a grid point very close to $\mathbf{c}(\mathbf{x})$. $\square$

Systems of inequalities

By a combinatorial argument, the inequality (2) $|L_1(\mathbf{x})\cdots L_n(\mathbf{x})| \leq \|\mathbf{x}\|^{-\delta}$ can be reduced to finitely many systems of inequalities of the shape

$$(3) \qquad |L_1(\mathbf{x})| \leq \|\mathbf{x}\|^{c_1}, \ldots, |L_n(\mathbf{x})| \leq \|\mathbf{x}\|^{c_n} \quad \text{in } \mathbf{x} \in \mathbb{Z}^n,$$

where $c_1 + \cdots + c_n < 0$.

Thus, the following is equivalent to the Subspace Theorem:

Theorem

The solutions of (3) *lie in finitely many proper linear subspaces of* $\mathbb{Q}^n$.

A refinement of the Subspace Theorem

Let again $L_1, \ldots, L_n$ be linearly independent linear forms in $X_1, \ldots, X_n$ with coefficients in $\overline{\mathbb{Q}}$ and $c_1, \ldots, c_n$ reals with $c_1 + \cdots + c_n < 0$. Consider again

$$(3) \qquad |L_1(\mathbf{x})| \le \|\mathbf{x}\|^{c_1}, \ldots, |L_n(\mathbf{x})| \le \|\mathbf{x}\|^{c_n} \quad \text{in } \mathbf{x} \in \mathbb{Z}^n.$$

Theorem (Vojta (1989), Schmidt (1993), Faltings-Wüstholz (1994))

There is an effectively computable, proper linear subspace T^{exc} of $\mathbb{Q}^n$ such that (3) has only finitely many solutions outside T^{exc}.

The space T^{exc} belongs to a finite collection, which depends only on $L_1, \ldots, L_n$ and is independent of $c_1, \ldots, c_n$.

A refinement of the Subspace Theorem

Let again $L_1, \ldots, L_n$ be linearly independent linear forms in $X_1, \ldots, X_n$ with coefficients in $\overline{\mathbb{Q}}$ and $c_1, \ldots, c_n$ reals with $c_1 + \cdots + c_n < 0$. Consider again

$$(3) \qquad |L_1(\mathbf{x})| \leq \|\mathbf{x}\|^{c_1}, \ldots, |L_n(\mathbf{x})| \leq \|\mathbf{x}\|^{c_n} \quad \text{in } \mathbf{x} \in \mathbb{Z}^n.$$

Theorem (Vojta (1989), Schmidt (1993), Faltings-Wüstholz (1994))

There is an effectively computable, proper linear subspace T^{exc} of $\mathbb{Q}^n$ such that (3) has only finitely many solutions outside T^{exc}.

The space T^{exc} belongs to a finite collection, which depends only on $L_1, \ldots, L_n$ and is independent of $c_1, \ldots, c_n$.

This refinement can be deduced from Schmidt's basic Subspace Theorem, asserting that the solutions of (3) lie in only finitely many subspaces.

So it is in fact equivalent to Schmidt's basic Subspace Theorem.

About the exceptional subspace

Assume for simplicity that $L_1, \ldots, L_n$ have real algebraic coefficients.

For a linear subspace T of $\mathbb{Q}^n$, we say that a subset $\{L_{i_1}, \ldots, L_{i_m}\}$ of $\{L_1, \ldots, L_n\}$ is linearly independent on T if no non-trivial $\mathbb{R}$-linear combination of $L_{i_1}, \ldots, L_{i_m}$ vanishes identically on T.

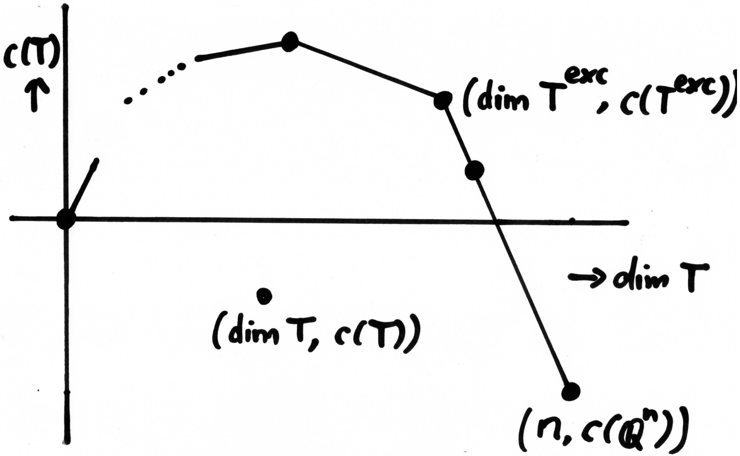
For a linear subspace T of $\mathbb{Q}^n$ define $c(T)$ to be the minimum of the quantities $c_{i_1} + \cdots + c_{i_m}$, taken over all subsets $\{L_{i_1}, \ldots, L_{i_m}\}$ of $\{L_1, \ldots, L_n\}$ of cardinality $m = \dim T$ that are linearly independent on T.

T^{exc} is the unique proper linear subspace T of $\mathbb{Q}^n$ such that

$$\frac{c(\mathbb{Q}^n) - c(T)}{n - \dim T} \text{ is minimal,}$$

subject to this condition, $\dim T$ is minimal.

About the exceptional subspace



An effective estimate

Lemma (Ev., Ferretti, 2013)

Suppose that the coefficients of $L_1, \dots, L_n$ have heights $\leq H$.

Then T^{exc} has a basis $\{\mathbf{x}_1, \dots, \mathbf{x}_m\} \subset \mathbb{Z}^n$ with

$$\|\mathbf{x}_i\| \leq (\sqrt{n} H^n)^{4^n} \quad (i = 1, \dots, m).$$

Open problem

Is there an efficient method to determine T^{exc} in general?

Easy combinatorial expression of T^{exc} in terms of $L_1, \dots, L_n$, $c_1, \dots, c_n$?

Examples

Let $n \geq 3$, $0 < \delta < 1/(n-1)$ and let $\alpha_1, \ldots, \alpha_{n-1} \in \overline{\mathbb{Q}}$ such that $1, \alpha_1, \ldots, \alpha_{n-1}$ are linearly independent over $\mathbb{Q}$. Consider the systems

$$(4) \qquad \begin{cases} |\alpha_1 x_1 + \cdots + \alpha_{n-1}x_{n-1} + x_n| \leq \|\mathbf{x}\|^{1-n-\delta}, \\ |x_1| \leq \|\mathbf{x}\|, \ldots, |x_{n-1}| \leq \|\mathbf{x}\|, \end{cases}$$

$$(5) \qquad \begin{cases} |\alpha_i x_n - x_i| \leq \|\mathbf{x}\|^{-(1+\delta)/(n-1)} \quad (i = 1, \ldots, n-1), \\ |x_n| \leq \|\mathbf{x}\| \end{cases}$$

in $\mathbf{x} \in \mathbb{Z}^n$.

For both systems, $T^{\text{exc}} = \{\mathbf{0}\}$.

Corollary (Schmidt, 1970)

Both systems (4) *and* (5) *have only finitely many solutions.*

Remarks

With the present methods of proof it is not possible to determine effectively the solutions of

$$(3) \qquad |L_1(\mathbf{x})| \leq \|\mathbf{x}\|^{c_1}, \ldots, |L_n(\mathbf{x})| \leq \|\mathbf{x}\|^{c_n} \quad \text{in } \mathbf{x} \in \mathbb{Z}^n$$

outside T^{exc}.

There is a semi-effective version of the Subspace Theorem comparable to that of Roth's Theorem.

The present methods of proof do not allow to give an explicit upper bound for the *number* of solutions of (3) outside T^{exc}.

However, it is possible to give an explicit upper bound for the minimal number of proper linear subspaces of $\mathbb{Q}^n$ containing the solutions of (3) (Schmidt (1989), Ev. (1995), Ev. and Schlickewei (2002), Ev. and Ferretti (2013)).

On the number of subspaces

Let $L_1, \dots, L_n$ be linearly independent linear forms in $X_1, \dots, X_n$ with complex algebraic coefficients and $c_1, \dots, c_n$ reals such that

- the coefficients of $L_1, \dots, L_n$ have heights $\leq H$ and generate a number field K of degree d;
- $c_i \leq 1$ for $i = 1, \dots, n$, $c_1 + \dots + c_n = -\delta$ with $0 < \delta \leq 1$.

Put $\Delta := |\det(L_1, \dots, L_n)|$ and consider

$$(6) \qquad |L_1(\mathbf{x})| \leq \Delta^{1/n} \|\mathbf{x}\|^{c_1}, \dots, |L_n(\mathbf{x})| \leq \Delta^{1/n} \|\mathbf{x}\|^{c_n} \quad \text{in } \mathbf{x} \in \mathbb{Z}^n.$$

Theorem (Ev. and Ferretti, 2013)

The set of solutions of (6) *is contained in the union of at most*

$$2^{35n}\Big(\delta^{-1} \log\log 4H \,+\, \delta^{-3}\big(\log(4\delta^{-1})\big)^2 \cdot \log 4d \log\log 4d\Big)$$

proper linear subspaces of $\mathbb{Q}^n$.

On the number of solutions

Let $n \geq 3$, $\delta > 0$ and $\alpha_1, \dots, \alpha_{n-1} \in \overline{\mathbb{Q}}$ such that $1, \alpha_1, \dots, \alpha_{n-1}$ are linearly independent over $\mathbb{Q}$.

Call $\mathbf{x} \in \mathbb{Z}^n$ *primitive* if its coordinates have gcd 1.

Proposition (variation on Schmidt, 1990)

Let $\mathbf{w} = (w_1, \dots, w_n) \in \mathbb{Z}^n$ *be a primitive solution to*

$$(7) \qquad |\alpha_i w_n - w_i| \leq \|\mathbf{w}\|^{-(2+\delta)/(n-2)} \quad (i = 1, \dots, n-1).$$

Then the inequality

$$(8) \qquad |\alpha_1 x_1 + \cdots + \alpha_{n-1} x_{n-1} + x_n| \leq \|\mathbf{x}\|^{1-n-\delta}$$

has $\gg^{\mathrm{eff}} \|\mathbf{w}\|^{1/(n-2)(n-1)}$ *primitive solutions* $\mathbf{x} \in \mathbb{Z}^n$ *lying in the subspace*

$$w_1 x_1 + \cdots + w_n x_n = 0.$$

On the number of solutions

Let $n \geq 3$, $\delta > 0$ and $\alpha_1, \ldots, \alpha_{n-1} \in \overline{\mathbb{Q}}$ such that $1, \alpha_1, \ldots, \alpha_{n-1}$ are linearly independent over $\mathbb{Q}$.

Call $\mathbf{x} \in \mathbb{Z}^n$ *primitive* if its coordinates have gcd 1.

Proposition (variation on Schmidt, 1990)

Let $\mathbf{w} = (w_1, \ldots, w_n) \in \mathbb{Z}^n$ be a primitive solution to

$$(7) \qquad |\alpha_i w_n - w_i| \leq \|\mathbf{w}\|^{-(2+\delta)/(n-2)} \quad (i = 1, \ldots, n-1).$$

Then the inequality

$$(8) \qquad |\alpha_1 x_1 + \cdots + \alpha_{n-1} x_{n-1} + x_n| \leq \|\mathbf{x}\|^{1-n-\delta}$$

has $\gg^{\mathrm{eff}} \|\mathbf{w}\|^{1/(n-2)(n-1)}$ primitive solutions $\mathbf{x} \in \mathbb{Z}^n$ lying in the subspace

$$w_1 x_1 + \cdots + w_n x_n = 0.$$

So an upper bound for the *number* of primitive solutions of (8) would imply an upper bound for the *sizes* of the primitive solutions of (7), i.e., we would be able to determine all primitive solutions of (7) effectively.

A semi-effective version of the Subspace Theorem

Let $L_1, \dots, L_n$ be linearly independent linear forms in $X_1, \dots, X_n$ with complex algebraic coefficients and $c_1, \dots, c_n$ reals such that:

• the coefficients of $L_1, \dots, L_n$ have heights $\leq H$ and generate a number field K of degree d;
• $c_1 + \cdots + c_n = -\delta < 0$.

Theorem

For every solution $\mathbf{x}$ of

$$(9) \qquad |L_1(\mathbf{x})| \leq \|\mathbf{x}\|^{c_1}, \dots, |L_n(\mathbf{x})| \leq \|\mathbf{x}\|^{c_n} \quad \text{with } \mathbf{x} \in \mathbb{Z}^n \setminus T^{\mathrm{exc}}$$

we have $\|\mathbf{x}\| \leq \max\left(B^{\mathrm{ineff}}(n, \delta, K), H^{c^{\mathrm{eff}}(n,\delta,d)}\right)$.

Proof.

Small modification of the proof of the Subspace Theorem. □

A semi-effective version of the Subspace Theorem

Let $L_1, \ldots, L_n$ be linearly independent linear forms in $X_1, \ldots, X_n$ with complex algebraic coefficients and $c_1, \ldots, c_n$ reals such that:

• the coefficients of $L_1, \ldots, L_n$ have heights $\leq H$ and generate a number field K of degree d;
• $c_1 + \cdots + c_n = -\delta < 0$.

Theorem

For every solution $\mathbf{x}$ *of*

$$(9) \qquad |L_1(\mathbf{x})| \leq \|\mathbf{x}\|^{c_1}, \ldots, |L_n(\mathbf{x})| \leq \|\mathbf{x}\|^{c_n} \quad \textit{with } \mathbf{x} \in \mathbb{Z}^n \setminus T^{\mathrm{exc}}$$

we have $\|\mathbf{x}\| \leq \max\left(B^{\mathrm{ineff}}(n, \delta, K), H^{c^{\mathrm{eff}}(n,\delta,d)}\right)$.

We may take $c^{\mathrm{eff}}(n, \delta, d) = \exp\left(10^{6n}(1 + \delta^{-3}) \log 4d \log\log 4d\right)$.

A conjectural improvement

Keep the assumptions

- $L_1, \dots, L_n$ are linearly independent linear forms in $X_1, \dots, X_n$ whose coefficients have heights $\le H$ and generate a number field of degree d;
- $c_1 + \cdots + c_n = -\delta < 0$.

Conjecture 1

There are an effectively computable constant $c^{\mathrm{eff}}(n, \delta, d) > 0$ and a constant $B'(n, \delta, d) > 0$ such that for every solution $\mathbf{x}$ of

$$(9) \qquad |L_1(\mathbf{x})| \le \|\mathbf{x}\|^{c_1}, \dots, |L_n(\mathbf{x})| \le \|\mathbf{x}\|^{c_n} \quad \text{with } \mathbf{x} \in \mathbb{Z}^n \setminus T^{\mathrm{exc}}$$

we have $\|\mathbf{x}\| \le \max\left(B'(n, \delta, d), H^{c^{\mathrm{eff}}(n,\delta,d)}\right)$.

So the ineffective constant B depending on the number field generated by the coefficients of $L_1, \dots, L_n$ is replaced by a constant B' depending on the degree of this field.

A conjectural improvement

Keep the assumptions

• $L_1, \dots, L_n$ are linearly independent linear forms in $X_1, \dots, X_n$ whose coefficients have heights $\leq H$ and generate a number field of degree d;
• $c_1 + \cdots + c_n = -\delta < 0$.

Conjecture 1

There are an effectively computable constant $c^{\mathrm{eff}}(n, \delta, d) > 0$ and a constant $B'(n, \delta, d) > 0$ such that for every solution $\mathbf{x}$ of

$$(9) \qquad |L_1(\mathbf{x})| \leq \|\mathbf{x}\|^{c_1}, \dots, |L_n(\mathbf{x})| \leq \|\mathbf{x}\|^{c_n} \quad \text{with } \mathbf{x} \in \mathbb{Z}^n \setminus T^{\mathrm{exc}}$$

we have $\|\mathbf{x}\| \leq \max\left(B'(n, \delta, d), H^{c^{\mathrm{eff}}(n,\delta,d)}\right)$.

This is hopeless with B' effective. Can this be proved with B' ineffective?

abc-inequalities

Let K be an algebraic number field of degree d and discriminant D_K.
Let $a, b, c \in O_K \setminus \{0\}$ with $a + b = c$.

Define $H_K(a, b, c) := \prod_{\sigma : K \hookrightarrow \mathbb{C}} \max(|\sigma(a)|, |\sigma(b)|, |\sigma(c)|)$.

Theorem 1 (Effective abc-inequality, Győry, 1978)

$H_K(a, b, c) \leq (2|N_{K/\mathbb{Q}}(abc)|)^{c_1(d)|D_K|^{c_2(d)}}$ with $c_1(d), c_2(d)$ effectively computable in terms of d.

Proof.

Baker-type logarithmic forms estimates. □

abc-inequalities

Let K be an algebraic number field of degree d and discriminant D_K.
Let $a, b, c \in O_K \setminus \{0\}$ with $a + b = c$.

Define $H_K(a, b, c) := \prod_{\sigma : K \hookrightarrow \mathbb{C}} \max(|\sigma(a)|, |\sigma(b)|, |\sigma(c)|)$.

Theorem 1 (Effective abc-inequality, Győry, 1978)

$H_K(a, b, c) \leq (2|N_{K/\mathbb{Q}}(abc)|)^{c_1(d)|D_K|^{c_2(d)}}$ with $c_1(d), c_2(d)$ effectively computable in terms of d.

Proof.

Baker-type logarithmic forms estimates. □

Theorem 2 (Semi-effective abc-inequality, well-known)

For every $\delta > 0$ we have $H_K(a, b, c) \leq C^{\mathrm{ineff}}(K, \delta)|N_{K/\mathbb{Q}}(abc)|^{1+\delta}$.

Proof.

Roth's Theorem over number fields. □

A very weak abc-conjecture

Let again K be a number field of degree d and discriminant D_K.

Conjecture 2 (Very weak abc-conjecture)

There are a constant $C(d,\delta) > 0$ and an effectively computable constant $c^{\mathrm{eff}}(d,\delta) > 0$ such that for all $a, b, c \in O_K \setminus \{0\}$ with $a + b = c$ and all $\delta > 0$ we have

$$H_K(a,b,c) \leq C(d,\delta)|D_K|^{c^{\mathrm{eff}}(d,\delta)}|N_{K/\mathbb{Q}}(abc)|^{1+\delta}.$$

A very weak abc-conjecture

Let again K be a number field of degree d and discriminant D_K.

Conjecture 2 (Very weak abc-conjecture)

There are a constant $C(d,\delta) > 0$ and an effectively computable constant $c^{\text{eff}}(d,\delta) > 0$ such that for all $a,b,c \in O_K \setminus \{0\}$ with $a+b=c$ and all $\delta > 0$ we have

$$H_K(a,b,c) \leq C(d,\delta)|D_K|^{c^{\text{eff}}(d,\delta)}|N_{K/\mathbb{Q}}(abc)|^{1+\delta}.$$

abc-conjecture over number fields

There is $C(d,\delta) > 0$ such that for all $a,b,c \in O_K \setminus \{0\}$ with $a+b=c$ and all $\delta > 0$ the following holds:

Let $\mathfrak{d} := (a,b,c)$ and $R := N_{K/\mathbb{Q}}(\prod \mathfrak{p})$, where the product is over all prime ideals $\mathfrak{p}$ of O_K with $\mathfrak{p} \supset abc\mathfrak{d}^{-3}$. Then

$$\begin{aligned} H_K(a,b,c) &\leq C(d,\delta)N_{K/\mathbb{Q}}(\mathfrak{d})|D_K|^{1+\delta} \cdot R^{1+\delta} \\ &\leq C(d,\delta)|D_K|^{1+\delta} \cdot |N_{K/\mathbb{Q}}(abc)|^{1+\delta}. \end{aligned}$$

A very weak abc-conjecture

Let again K be a number field of degree d and discriminant D_K.

Conjecture 2 (Very weak abc-conjecture)

There are a constant $C(d, \delta) > 0$ and an effectively computable constant $c^{\mathrm{eff}}(d, \delta) > 0$ such that for all $a, b, c \in O_K \setminus \{0\}$ with $a + b = c$ and all $\delta > 0$ we have

$$H_K(a, b, c) \leq C(d, \delta)|D_K|^{c^{\mathrm{eff}}(d,\delta)}|N_{K/\mathbb{Q}}(abc)|^{1+\delta}.$$

Conjecture 1 $\Longrightarrow$ Conjecture 2 (idea).

Choose a $\mathbb{Z}$-basis $\{\omega_1, \ldots, \omega_d\}$ of O_K with conjugates with absolute values bounded from above in terms of D_K. Write $a = \sum_{i=1}^{d} x_i\omega_i$, $b = \sum_{i=1}^{d} y_i\omega_i$ with $x_i, y_i \in \mathbb{Z}$. Then $\mathbf{x} = (x_1, \ldots, y_d)$ satisfies one of finitely many systems of inequalities of the type

$$|L_i(\mathbf{x})| \leq \|\mathbf{x}\|^{c_i} \quad (i = 1, \ldots, 2d)$$

where the L_i are linear forms whose coefficients lie in the Galois closure of K and have heights bounded above in terms of $|D_K|$. $\square$

Discriminants of binary forms

Definition

The discriminant of a binary form

$$F = a_0X^n + a_1X^{n-1}Y + \cdots + a_nY^n = \prod_{i=1}^{n}(\alpha_i X - \beta_i Y)$$

is given by $D(F) = \displaystyle\prod_{1\leq i<j\leq n}(\alpha_i\beta_j - \alpha_j\beta_i)^2$.

This is a homogeneous polynomial in $\mathbb{Z}[a_0, \ldots, a_n]$ of degree $2n - 2$.

Discriminants of binary forms

Definition

The discriminant of a binary form

$$F = a_0X^n + a_1X^{n-1}Y + \cdots + a_nY^n = \prod_{i=1}^{n}(\alpha_i X - \beta_i Y)$$

is given by $D(F) = \prod_{1 \le i < j \le n} (\alpha_i\beta_j - \alpha_j\beta_i)^2$.

This is a homogeneous polynomial in $\mathbb{Z}[a_0, \ldots, a_n]$ of degree $2n - 2$.

For a matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ we define $F_A(X, Y) = F(aX + bY, cX + dY)$.

Two binary forms $F, G \in \mathbb{Z}[X, Y]$ are called *equivalent* if $G = \pm F_A$ for some $A \in \mathrm{GL}(2, \mathbb{Z})$.

Equivalent binary forms have the same discriminant.

A finiteness result for binary forms of given discriminant

Theorem (Lagrange ($n = 2$, 1773), Hermite ($n = 3$, 1851), Birch and Merriman ($n \geq 4$, 1972))

For every $n \geq 2$ and $D \neq 0$, there are only finitely many equivalence classes of binary forms $F \in \mathbb{Z}[X, Y]$ of degree n and discriminant D.

The proofs of Lagrange and Hermite are effective (in that they allow to compute a full system of representatives for the equivalence classes), that of Birch and Merriman is ineffective.

An effective finiteness result

Define the height of $F = a_0X^n + a_1X^{n-1}Y + \cdots + a_nY^n \in \mathbb{Z}[X, Y]$ by $H(F) := \max_i |a_i|$.

Theorem 3 (Ev., Győry, recent improvement of result from 1991)

Let $F \in \mathbb{Z}[X, Y]$ be a binary form of degree $n \geq 4$ and discriminant $D \neq 0$. Then F is equivalent to a binary form G for which

$$H(G) \leq \exp\left((16n^3)^{25n^2}|D|^{5n-3}\right).$$

An effective finiteness result

Define the height of $F = a_0X^n + a_1X^{n-1}Y + \cdots + a_nY^n \in \mathbb{Z}[X, Y]$ by $H(F) := \max_i |a_i|$.

Theorem 3 (Ev., Győry, recent improvement of result from 1991)

Let $F \in \mathbb{Z}[X, Y]$ be a binary form of degree $n \geq 4$ and discriminant $D \neq 0$. Then F is equivalent to a binary form G for which

$$H(G) \leq \exp\left((16n^3)^{25n^2}|D|^{5n-3}\right).$$

More precise versions of the arguments of Lagrange and Hermite give a bound $H(G) \leq \text{constant} \cdot |D|$ in case that F has degree ≤ 3.

An effective finiteness result

Define the height of $F = a_0X^n + a_1X^{n-1}Y + \cdots + a_nY^n \in \mathbb{Z}[X,Y]$ by $H(F) := \max_i |a_i|$.

Theorem 3 (Ev., Győry, recent improvement of result from 1991)

Let $F \in \mathbb{Z}[X,Y]$ be a binary form of degree $n \geq 4$ and discriminant $D \neq 0$. Then F is equivalent to a binary form G for which

$$H(G) \leq \exp\left((16n^3)^{25n^2}|D|^{5n-3}\right).$$

Proof (idea).

Let L be the splitting field of F. Assume for convenience that $F = \prod_{i=1}^{n}(\alpha_i X - \beta_i Y)$ with $\alpha_i, \beta_i \in O_L\ \forall i$. Put $\Delta_{ij} := \alpha_i\beta_j - \alpha_j\beta_i$ and apply an explicit version of the effective abc-inequality (Theorem 1) to the identities

$$\Delta_{ij}\Delta_{kl} + \Delta_{jk}\Delta_{il} = \Delta_{ik}\Delta_{jl} \quad (1 \leq i,j,k,l \leq n). \qquad \square$$

A semi-effective finiteness result

Theorem 4 (Ev., 1993)

Let $F \in \mathbb{Z}[X,Y]$ be a binary form of degree $n \geq 4$, discriminant $D \neq 0$ and splitting field L. Then F is equivalent to a binary form G for which

$$H(G) \leq C^{\mathrm{ineff}}(n,L) \cdot |D|^{21/(n-1)}.$$

Proof (idea).

Apply the semi-effective abc-inequality Theorem 2 to the identities

$$\Delta_{ij}\Delta_{kl} + \Delta_{jk}\Delta_{il} = \Delta_{ik}\Delta_{jl} \quad (1 \leq i,j,k,l \leq n). \qquad \square$$

A conjecture

Conjecture 3

Let $F \in \mathbb{Z}[X,Y]$ be a binary form of degree $n \geq 4$ and discriminant $D \neq 0$. Then F is equivalent to a binary form G for which

$$H(G) \leq C_1(n)|D|^{c_2^{\mathrm{eff}}(n)}.$$

Conjecture 2 $\Longrightarrow$ Conjecture 3.

Let L be the splitting field of F. Following the proof of Theorem 4 and using the very weak abc-conjecture, one obtains that there is G equivalent to F such that

$$H(G) \leq C_3(n)|D_L|^{c_4^{\mathrm{eff}}(n)}|D|^{21/(n-1)}.$$

Use that D_L divides $D^{n!}$. $\square$

A conjecture

Conjecture 3

Let $F \in \mathbb{Z}[X, Y]$ be a binary form of degree $n \geq 4$ and discriminant $D \neq 0$. Then F is equivalent to a binary form G for which

$$H(G) \leq C_1(n)|D|^{c_2^{\mathrm{eff}}(n)}.$$

Problem

What is the right value of the exponent on $|D|$?

A function field analogue

Let k be an algebraically closed field of characteristic 0, $K = k(t)$, $R = k[t]$.
Define $|\cdot|$ on $k(t)$ by $|f/g| := e^{\deg f - \deg g}$ for $f, g \in R$.

Define the height of $F = a_0X^n + a_1X^{n-1}Y + \cdots + a_nY^n \in R[X, Y]$ by $H(F) := \max_i |a_i|$.

Call two binary forms $F, G \in R[X, Y]$ equivalent if $G = uF_A$ for some $u \in k^*$, $A \in \mathrm{GL}(2, R)$.

Theorem 5 (W. Zhuang)

Let $F \in R[X, Y]$ be a binary form of degree $n \geq 4$ and discriminant $D \neq 0$. Then F is equivalent to a binary form G for which

$$H(G) \leq e^{n^2+4n+14}|D|^{20+7/(n-2)}.$$

Proof.

Follow the proof over $\mathbb{Z}$ and apply Mason's abc-theorem for function fields. □

Approximation of algebraic numbers by algebraic numbers of bounded degree

Theorem (Schmidt, 1971)

Let $\alpha \in \overline{\mathbb{Q}}$, $d \in \mathbb{Z}_{>0}$ and $\delta > 0$. Then there are only finitely many $\xi \in \overline{\mathbb{Q}}$ of degree d such that

$$|\alpha - \xi| \leq H(\xi)^{-d-1-\delta}.$$

Proof.

Consequence of the Subspace Theorem. □

Wirsing (1969) proved this earlier with $-2d - \delta$ instead of $-d - 1 - \delta$, by a different method.

Approximation of algebraic numbers by algebraic numbers of bounded degree: Vojta's conjecture

For $\xi \in \overline{\mathbb{Q}}$, define $D(\xi)$ to be the discriminant of the number field $\mathbb{Q}(\xi)$.

Conjecture (Vojta, 1987)

Let $\alpha \in \overline{\mathbb{Q}}$, $d \in \mathbb{Z}_{>0}$ and $\delta > 0$. Then there are only finitely many $\xi \in \overline{\mathbb{Q}}$ of degree d such that

$$|\alpha - \xi| \leq |D(\xi)|^{-1} H(\xi)^{-2-\delta}.$$

This implies Wirsing's Theorem since $|D(\xi)| \ll H(\xi)^{2d-2}$.

Restricting to algebraic numbers ξ in a given number field K, we obtain Roth's Theorem over number fields.

Approximation of algebraic numbers by algebraic numbers of bounded degree: application of Conjecture 1

Our Conjecture 1 implies the following:

Conjecture 4

Let $\alpha \in \overline{\mathbb{Q}}$, $d \in \mathbb{Z}_{>0}$, $\delta > 0$, *and put* $m := [\mathbb{Q}(\alpha) : \mathbb{Q}]$. *There is an effectively computable number* $c^{\mathrm{eff}}(m, d, \delta) > 0$, *such that the inequality*

$$|\alpha - \xi| \leq |D(\xi)|^{-c^{\mathrm{eff}}(m,d,\delta)} H(\xi)^{-2-\delta}$$

has only finitely many solutions in algebraic numbers ξ *of degree* d.

Thank you for your attention!