ON THE SUBSPACE THEOREM

Jan-Hendrik Evertse (Leiden)

Winter school on
Explicit Methods in Number Theory

Debrecen, January 30, 2009

DIRICHLET'S THEOREM

Rational numbers are represented as x/y, where x, y are integers such that $\gcd(x, y) = 1$, $y > 0$.

Theorem 1 (Dirichlet, 1842)
Let α be an irrational real number. Then there are infinitely many rational numbers x/y such that

$$|\alpha - (x/y)| \leqslant y^{-2}.$$

ROTH'S THEOREM

Theorem 2 (Roth, 1955)
Let α be a real algebraic number. Let $\delta > 0$. Then there are only finitely many rational numbers x/y such that

$$|\alpha - (x/y)| \leqslant y^{-2-\delta}.$$

This result is the outgrow of earlier work of Thue (1909), Siegel (1921), Dyson, Gel'fond (1949).

THE SUBSPACE THEOREM

For $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ define

$$\|\mathbf{x}\| := \max(|x_1|, \ldots, |x_n|).$$

Let

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

be n linear forms with (real or complex) algebraic coefficients.

Suppose that $L_1, \ldots, L_n$ are *linearly independent*, i.e., $\det(\alpha_{ij}) \neq 0$.

Theorem 3 (Subspace Theorem, W.M. Schmidt, 1972)
For every $\delta > 0$, there are a finite number $T_1, \ldots, T_t$ of proper linear subspaces of $\mathbb{Q}^n$ such that the set of solutions of the inequality

$$(1) \qquad |L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| \leqslant \|\mathbf{x}\|^{-\delta} \quad \textit{in } \mathbf{x} \in \mathbb{Z}^n$$

is contained in $T_1 \cup \cdots \cup T_t$.

SUBSPACE THM $\Longrightarrow$ ROTH'S THM

Consider

$(*)$ $\qquad |\alpha - (x/y)| \leqslant y^{-2-\delta}$ in $x/y \in \mathbb{Q}$

where α is algebraic and $\delta > 0$. Then

$$|y(x - \alpha y)| \leqslant y^{-\delta} \ll \max(|x|, |y|)^{-\delta}.$$

By the Subspace Theorem, the solutions $(x, y) \in \mathbb{Z}^2$ lie in finitely many one-dimensional proper linear subspaces of $\mathbb{Q}^2$.

Each of these subspaces gives rise to one rational number x/y.

Hence (*) has only finitely many solutions.

AN EXAMPLE WITH INFINITELY MANY SOLUTIONS

Let $0 < \delta < 1$ and consider

(2)

$$|(x_1+\sqrt{2}x_3)(x_1-\sqrt{2}x_3)(x_2-\sqrt{2}x_3)| \leqslant \|\mathbf{x}\|^{-\delta}.$$

Inequality (2) has infinitely many solutions $\mathbf{x} = (x_1, x_2, x_3) \in \mathbb{Z}^3$ in the following four subspaces:

- $x_1 = x_2$ (e.g., with $x_1 = x_2$, $x_1x_3 \geqslant 0$ and satisfying the Pell equation $|x_1^2 - 2x_3^2| = 1$);
- $x_1 = -x_2$, (e.g., with $x_1 = -x_3$, $x_1x_3 \leqslant 0$, $|x_1^2 - 2x_3^2| = 1$);
- $x_1 = x_3 = 0$;
- $x_2 = x_3 = 0$.

Exercise. Inequality (2) has only finitely many solutions outside these four subspaces, each satisfying $\|\mathbf{x}\| \leqslant 10^{1/\delta}$.

REMARKS

1) In general, the available methods of proof of the Subspace Theorem are *ineffective* in that they do not provide an algorithm to determine the subspaces $T_1, \ldots, T_t$ containing the solutions of

$$|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| \leqslant \|\mathbf{x}\|^{-\delta}.$$

2) It is possible to estimate from above the *number* t of subspaces. This leads to quantitative versions of the Subspace Theorem.

VOJTA'S REFINEMENT

Let again $L_1, \ldots, L_n$ be linearly independent linear forms in n variables with algebraic coefficients and $\delta > 0$. Consider again the inequality

(1) $\qquad |L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| \leqslant \|\mathbf{x}\|^{-\delta}$ in $\mathbf{x} \in \mathbb{Z}^n$.

Theorem 4 (Vojta, 1989)
There is a finite, effectively determinable collection $U_1, \ldots, U_r$ of proper linear subspaces of $\mathbb{Q}^n$, independent of δ, such that (1) *has only finitely many solutions outside $U_1 \cup \cdots \cup U_r$.*

Remark. With Vojta's method of proof it is not possible to determine the solutions outside $U_1 \cup \cdots \cup U_r$ effectively.
Nor is it possible to estimate from above the number of solutions outside $U_1 \cup \cdots \cup U_r$.

ABSOLUTE VALUES ON $\mathbb{Q}$

For $a \in \mathbb{Q}$ we define $|a|_\infty := |a|$ and

$$|a|_p := \begin{cases} 0 & \text{if } a = 0; \\ p^{-r} & \text{if } a = p^r b/c \text{ where } b, c \in \mathbb{Z},\ p \nmid bc \end{cases}$$

for every prime number p.

We fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$.

For every $p \in \{\infty\} \cup \{\text{prime numbers}\}$, we choose an extension of $|\cdot|_p$ to $\overline{\mathbb{Q}}$.

Thus, the absolute values $|\cdot|_p$ are all defined on $\overline{\mathbb{Q}}$.

Product Formula:
Let $a \in \mathbb{Q} \setminus \{0\}$ composed of primes $p_1, \ldots, p_t$ and $S = \{\infty, p_1, \ldots, p_t\}$. Then

$$\prod_{p \in S} |a|_p = 1.$$

THE P-ADIC SUBSPACE THEOREM

Theorem 5 (Schlickewei, 1977)
Let $S = \{\infty, p_1, \ldots, p_t\}$, $n \geqslant 2$, $\delta > 0$.

For each $p \in S$, *let* $L_{1p}, \ldots, L_{np}$ *be* n *linearly independent linear forms in* n *variables with coefficients in* $\overline{\mathbb{Q}}$.

Then the set of solutions of
(3)
$$\prod_{p \in S} |L_{1p}(\mathbf{x}) \cdots L_{np}(\mathbf{x})|_p \leqslant \|\mathbf{x}\|^{-\delta} \quad \text{in } \mathbf{x} \in \mathbb{Z}^n$$
is contained in a union of finitely many proper linear subspaces of $\mathbb{Q}^n$.

There is a more general result in which the solutions $\mathbf{x}$ have their coordinates in a given algebraic number field instead of $\mathbb{Z}$ (Schmidt, Schlickewei).

THE QUANTITATIVE SUBSPACE THEOREM: HISTORY

Quantitative versions of the Subspace Theorem give an explicit upper bound for the number of subspaces.

In 1989, Schmidt gave the first quantitative version of his basic Subspace Theorem (Theorem 3).

In 1991, Schlickewei generalized this to the p-adic case.

There were subsequent improvements and generalizations by Ev. (1995) and Schlickewei and Ev. (2002).

The result of Schlickewei and Ev. was recently improved by Ferretti and Ev. (in preparation).

Quantitative versions of the p-adic Subspace Theorem are important tools to derive good explicit upper bounds for the number of solutions of Diophantine equations from several classes.

There are recent applications by Adamczewski, Bugeaud et.al. to complexity measures of expansions of algebraic numbers, and to transcendence measures.

SPLITTING THE PRODUCT

Let $S = \{\infty, p_1, \ldots, p_t\}$.

The quantitative version of the Subspace Theorem of Ferretti and Ev. does not give an explicit upper bound for the number of subspaces containing the solutions of

$$\prod_{p \in S} |L_{1p}(\mathbf{x}) \cdots L_{np}(\mathbf{x})|_p \leqslant \|\mathbf{x}\|^{-\delta} \tag{3}$$

but instead for the number of subspaces containing the solutions of a system of inequalities

$$|L_{ip}(\mathbf{x})|_p \leqslant \|\mathbf{x}\|^{c_{ip}} \ (p \in S,\ i = 1, \ldots, n) \tag{4}$$

in $\mathbf{x} \in \mathbb{Z}^n$, where the c_{ip} are fixed reals with

$$\sum_{p \in S} \sum_{i=1}^{n} c_{ip} < 0.$$

REMARKS

One can reduce inequality (3) to a finite number of systems of type (4).

For a system (4) we have a much sharper upper bound for the number of subspaces of solutions than for an inequality (3).

In many Diophantine applications one obtains sharper results by making a reduction to systems (4) instead of inequalities of type (3).

THE QUANTITATIVE P-ADIC SUBSPACE THEOREM

Let $S = \{\infty, p_1, \ldots, p_t\}$.

Let L_{ip}, c_{ip} $(p \in S, i = 1, \ldots, n)$ be linear forms in n variables with coefficients in $\overline{\mathbb{Q}}$, resp. reals satisfying

$$|\det(L_{1p}, \ldots, L_{np})|_p = 1 \quad \text{for } p \in S,$$

$$\sum_{p \in S} \sum_{i=1}^{n} c_{ip} \leqslant -\delta \quad \text{with } 0 < \delta < 1.$$

Theorem 6 (Ferretti, Ev., 201?)
The set of solutions $\mathbf{x} \in \mathbb{Z}^n$ *of*

(4) $\quad |L_{ip}(\mathbf{x})|_p \leqslant \|\mathbf{x}\|^{c_{ip}} \quad (p \in S,\, i = 1, \ldots, n)$

is contained in a union of at most

$$C(\{L_{ip}\}) \cdot c_1^n \delta^{-3} (\log \delta^{-1})^2$$

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

Here c_1 *is an absolute constant, and* $C(\{L_{ip}\})$ *depends only on the set of linear forms* $\{L_{ip} : p \in S, i = 1, \ldots, n\}$ *and is independent of* $p_1, \ldots, p_t$ *and the* c_{ip}.

Previously, Schlickewei and Ev. (2002) had obtained a bound

$$C(\{L_{ip}\}) \cdot c^{n^2} \delta^{-n-4}.$$

AN APPLICATION

Let $a_0, \ldots, a_n$ be non-zero integers, and $B_0, \ldots, B_n$ pairwise coprime integers $\geqslant 2$.

Consider the equation

$$a_0 B_0^{z1} + \cdots + a_n B_n^{z_n} = 0 \quad \text{in } z_0, \ldots, z_n \in \mathbb{Z}_{>0}. \tag{5}$$

Theorem 7
Eq. (5) *has at most*

$$(c_2 n)^{c_3 n^2}$$

solutions, where c_2, c_3 *are absolute constants, independent of* $a_0, \ldots, a_n, B_0, \ldots, B_n$.

A QUALITATIVE PROOF (I)

Let $S = \{\infty, p_1, \ldots, p_t\}$, where $p_1, \ldots, p_t$ are the primes occurring in the factorizations of $a_0, \ldots, a_n$, $B_0, \ldots, B_n$.

For a solution $(z_0, \ldots, z_n)$ of (5), write

$$x_i := a_i B_i^{z_i} \quad (i = 0, \ldots, n).$$

Notice that $x_1, \ldots, x_n$ and $x_0 = -x_1 - \cdots - x_n$ are linear forms in $\mathbf{x} = (x_1, \ldots, x_n)$.

For $p \in S$, choose $i_p \in \{0, \ldots, n\}$ for which $|x_{i_p}|_p$ is maximal. Thus,

$$|x_{i_\infty}|_\infty = \|\mathbf{x}\|, \quad |x_{i_p}|_p \gg 1 \ (p = p_1, \ldots, p_t).$$

Then using $\prod_{p \in S} |x_i|_p = 1$ for $i = 0, \ldots, n$ we infer

$$\prod_{p \in S} \prod_{\substack{i=0 \\ i \neq i_p}}^{n} |x_i|_p \ll \|\mathbf{x}\|^{-1}.$$

A QUALITATIVE PROOF (II)

By the p-adic Subspace Theorem, the vectors $\mathbf{x} = (x_1, \ldots, x_n)$ lie in finitely many proper linear subspaces of $\mathbb{Q}^n$.

Consider the solutions $\mathbf{x}$ in one of these subspaces. Then we can eliminate one of the variables and make a reduction to an equation in fewer variables.

By induction, (5) has only finitely many solutions. $\square$

DEDUCTION OF THE UPPER BOUND

It can be shown that there is a collection of at most $(c_4 n)^{c_5 n}$ systems of type (4) with

$$\delta = \frac{1}{2}, \quad L_{ip} \in \left\{ X_1, \ldots, X_n, -\sum_{i=1}^{n} X_i \right\} \ \forall i, p$$

such that each vector $\mathbf{x} = (a_1 B_1^{z_1}, \ldots, a_n B_n^{z_n})$ corresponding to a solution $(z_0, \ldots, z_n)$ of (5) satisfies one of these systems.

By the QPST, the vectors $\mathbf{x}$ satisfying a single system lie in at most c_6^n proper linear subspaces of $\mathbb{Q}^n$.

Thus, the whole set of vectors $\mathbf{x}$ is contained in at most $(c_7 n)^{c_8 n}$ proper linear subspaces of $\mathbb{Q}^n$.

By induction, the total number of solutions of (5) is at most $(c_2 n)^{c_3 n^2}$.

A MORE GENERAL RESULT (I)

Let

$$\Gamma := \{\alpha_1^{z_1} \cdots \alpha_r^{z_r} : z_1, \ldots, z_r \in \mathbb{Z}\}$$

where $\alpha_1, \ldots, \alpha_r$ are non-zero complex numbers.

Define the *division group* of Γ by

$$\begin{aligned} \overline{\Gamma} &:= \{x \in \mathbb{C}^* : \exists m \in \mathbb{Z}_{>0} \text{ with } x^m \in \Gamma\} \\ &= \left\{ \sqrt[m]{\alpha_1^{z_1} \cdots \alpha_r^{z_r}} : m \in \mathbb{Z}_{>0},\, z_1, \ldots, z_r \in \mathbb{Z} \right\}. \end{aligned}$$

Theorem 8 (Beukers, Schlickewei, 1996)
Let a_1, a_2 be non-zero complex numbers. Then the equation

$$a_1 x_1 + a_2 x_2 = 1 \quad \textit{in } x_1, x_2 \in \overline{\Gamma}$$

has at most $2^{16(r+1)}$ solutions.

DEGENERATE SOLUTIONS

Now let $n \geqslant 3$ and consider

(6) $\quad a_1x_1 + \cdots + a_nx_n = 1$ in $x_1, \ldots, x_n \in \overline{\Gamma}$.

A solution $(x_1, \ldots, x_n)$ of (6) is called *degenerate* if there is a vanishing subsum

$$\sum_{i \in I} a_i x_i = 0 \quad \text{for some } I \subset \{1, \ldots, n\}$$

and *non-degenerate* otherwise.

From such a degenerate solution $(x_1, \ldots, x_n)$ we may construct infinitely many other solutions $(x'_1, \ldots, x'_n)$ of the shape

$$x'_i = x \cdot x_i \ (i \in I), \quad x'_i = x_i \ (i \notin I)$$

with $x \in \overline{\Gamma}$.

A MORE GENERAL RESULT (II)

Theorem 9 (Schlickewei, Schmidt, Ev., 2002)
Let $\Gamma = \{\alpha_1^{z_1} \cdots \alpha_r^{z_r} : z_1, \ldots, z_n \in \mathbb{Z}\}$ *where* $\alpha_1, \ldots, \alpha_n \in \mathbb{C}^*$, *denote by* $\overline{\Gamma}$ *the division group of* Γ, *and let* $n \geqslant 3$, $a_1, \ldots, a_n \in \mathbb{C}^*$.

Then the equation

$$a_1 x_1 + \cdots + a_n x_n = 1 \text{ in } x_1, \ldots, x_n \text{ in } \overline{\Gamma}$$

has at most $c(n, r)$ *non-degenerate solutions.*

Schlickewei, Schmidt, Ev. proved this with $c(n, r) = e^{(6n)^{4n}(r+1)}$.

This was very recently improved by Amoroso and Viada to $c(n, r) = (9n)^{8n^5(r+1)}$.

INGREDIENTS OF THE PROOF

• A specialization argument from algebraic geometry, to make a reduction to the case that the generators $\alpha_1, \ldots, \alpha_r$ of Γ are algebraic.

• A strong general quantitative version of the Subspace Theorem, where the unknowns may be algebraic numbers instead of rational integers (Schlickewei, Ev., 2002).

• Upper bounds for the number of algebraic points of small height on an algebraic variety. This was a development which started with S. Zhang (1996). Recently Amoroso and Viada obtained a new sharpening leading to their improvement of $c(n, r)$.

A TRANSCENDENCE RESULT

We consider gap series

$$\xi = \sum_{k=1}^{\infty} b^{-n_k}$$

where $b \geqslant 2$ and $0 < n_1 < n_2 < n_3 < \cdots$ are integers.

Theorem 10 (Schneider, 1957)
Suppose

$$\limsup_{k \to \infty} \frac{n_{k+1}}{n_k} > 1.$$

Then ξ is transcendental.

AN IMPROVEMENT

We consider again numbers $\xi = \sum_{k=1}^{\infty} b^{-n_k}$ with integers $b \geqslant 2$, $0 < n_1 < n_2 < \cdots$.

Theorem 11 (Bugeaud, Ev., 2008)
Suppose that $n_{k+1}/n_k \downarrow 1$ *monotonically.*

Further suppose that for some $\varepsilon > 0$ *there are infinitely many* k *such that*

$$\frac{n_{k+1}}{n_k} > 1 + \frac{1}{k^{(1/3)-\varepsilon}}.$$

Then ξ *is transcendental.*

Example. $\displaystyle\sum_{k=1}^{\infty} b^{-2^{[k^\eta]}}$ with $\eta > 2/3$.

PROOF OF THEOREM 11 (I)

Assume that ξ is algebraic.

Fix δ with $0 < \delta < 1$, and consider the set

$$A(\delta) := \left\{ k : \frac{n_{k+1}}{n_k} \geqslant 1 + \delta \right\}.$$

Let $k \in A(\delta)$. Define

$$x_k := b^{n_k}, \quad y_k := b^{n_k} \sum_{i=1}^{k} b^{-n_i}, \quad \mathbf{x}_k := (x_k, y_k).$$

Then $x_k, y_k \in \mathbb{Z}_{>0}$, $\gcd(x_k, y_k) = 1$,
$\|\mathbf{x}_k\| \ll b^{n_k}$ and

$$\begin{aligned} |x_k\xi - y_k| &= b^{n_k} \sum_{i=k+1}^{\infty} b^{-n_i} \\ &\ll b^{n_k - n_{k+1}} = (b^{n_k})^{-\delta} \ll \|\mathbf{x}_k\|^{-\delta}. \end{aligned}$$

PROOF OF THEOREM 11 (II)

Let $S = \{\infty, p_1, \ldots, p_t\}$, where $p_1, \ldots, p_t$ are the primes dividing b. Then

(7)
$$\begin{cases} |x_k\xi - y_k|_\infty \ll \|\mathbf{x}_k\|^{-\delta}, & |x_k|_\infty \leqslant \|\mathbf{x}_k\|, \\ |x_k|_p \ll \|\mathbf{x}_k\|^{\log|b|_p/\log b}, & |y_k|_p \leqslant 1 \end{cases}$$

for $p = p_1, \ldots, p_t$.

The sum of the exponents is $-\delta$.

So by the QPST, the solutions of (7) lie in $\ll \delta^{-3}(\log\delta^{-1})^2$ one-dimensional subspaces of $\mathbb{Q}^2$, each of which gives rise to at most one value of k.

PROOF OF THEOREM 11 (III)

So for all δ with $0 < \delta < 1$,

$$\#A(\delta) = \#\left\{k : \frac{n_{k+1}}{n_k} \geqslant 1 + \delta\right\} \ll \delta^{-3}(\log \delta^{-1})^2.$$

Hence

$$\frac{n_{k+1}}{n_k} - 1 \ll \frac{(\log k)^{2/3}}{k^{1/3}}$$

for every sufficiently large k, contrary to our assumption. □

COMPLEXITY OF ALGEBRAIC NUMBERS (I)

Let ξ be an irrational algebraic number with $0 < \xi < 1$ and b an integer $\geqslant 2$. Consider the b-ary expansion of ξ,

$$\xi = \sum_{n=1}^{\infty} a_n b^{-n} \quad \text{with } a_n \in \{0, \ldots, b-1\}.$$

We measure the complexity of ξ by estimating its number of digit changes up to N,

$$\text{nbdc}(\xi, b; N) := \#\{n \leqslant N : \, a_{n+1} \neq a_n\}.$$

COMPLEXITY OF ALGEBRAIC NUMBERS (II)

Assuming that the digits of the b-ary expansion of an irrational real algebraic number ξ behave like a random sequence, one should expect $\mathrm{nbdc}(\xi, b; N)$ to be linear in N.

Theorem 12 (Bugeaud, Ev., 2008)
For any real, irrational algebraic number ξ and any integer $b \geqslant 2$ we have

$$\mathrm{nbdc}(\xi, b; N) \gg_{\xi,b} \frac{(\log N)^{3/2}}{\log\log N} \text{ as } N \to \infty.$$

The proof is similar to that of the previous transcendence result.