NOTES ON DIOPHANTINE APPROXIMATION

Jan-Hendrik Evertse

November 28, 2007

10 The Subspace Theorem

Literature:
W.M. Schmidt, Diophantine approximation, Lecture Notes in Mathematics 785, Springer Verlag 1980, Chap.VI,VII,VIII

10.1 Statement of the result.

The Subspace Theorem is a generalization of Roth's Theorem to higher dimensions. We start with some definitions.

Let n be an integer $\geqslant 1$ and $r \leqslant n$. We say that linear forms $L_1 = \sum_{j=1}^n \alpha_{1j}X_j, \ldots, L_r = \sum_{j=1}^n \alpha_{nj}X_j$ with coefficients in $\mathbb{C}$ are linearly dependent if there are $c_1, \ldots, c_r \in \mathbb{C}$, not all 0, such that $c_1L_1 + \cdots + c_rL_r \equiv 0$. Otherwise, $L_1, \ldots, L_r$ are called linearly independent. If $r = n$, then $L_1, \ldots, L_n$ are linearly independent if and only if their coefficient determinant $\det(L_1, \ldots, L_n) = \det(\alpha_{ij})_{1\leqslant i,j\leqslant n} \neq 0$.

Recall that a linear subspace of $\mathbb{Q}^n$ is a set

$$T = \{\mathbf{x} \in \mathbb{Q}^n : L_1(\mathbf{x}) = 0, \ldots, L_r(\mathbf{x}) = 0\}$$

where $L_1, \ldots, L_r$ are linear forms in $X_1, \ldots, X_n$ with coefficients in $\mathbb{Q}$. If $L_1, \ldots, L_r$ are linearly independent, then T has dimension $n - r$.

The norm of $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ is given by

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

As an introduction to the Subspace Theorem, we give a "symmetric formulation" of Roth's Theorem. We mention that this and other results below deal with 'algebraic numbers in $\mathbb{C}$.' This includes the possibility that the algebraic numbers belong to $\mathbb{R}$.

Theorem 10.1.1 *Let $L_1 = \alpha X + \beta Y$, $L_2 = \gamma X + \delta Y$ be two linearly independent linear forms with algebraic coefficients in $\mathbb{C}$. Then the inequality*

$$|L_1(\mathbf{x})L_2(\mathbf{x})| \leqslant \max(|x|,|y|)^{-\varepsilon} \text{ in } \mathbf{x} = (x,y) \in \mathbb{Z}^2 \text{ with } gcd(x,y) = 1 \tag{1}$$

has only finitely many solutions.

Theorem 10.1.1$\Longrightarrow$Roth's Theorem. Let α be a real algebraic number of degree $n \geqslant 3$ and let $\kappa = 2 + \varepsilon > 2$. Consider $\xi \in \mathbb{Q}$ with

$$|\alpha - \xi| \leqslant H(\xi)^{-\kappa} \tag{2}$$

and write $\xi = x/y$ with $x, y \in \mathbb{Z}$, $\gcd(x,y) = 1$. Then we obtain

$$|y(x - \alpha y)| = y^2|\alpha - \xi| \leqslant \max(|x|,|y|)^{-\varepsilon}.$$

By Theorem 10.1.1 the latter has only finitely many solutions and therefore, (2) has only finitely many solutions.

Roth's Theorem$\Longrightarrow$Theorem 10.1.1. Let $\mathbf{x} = (x,y)$ be a solution of (1). By interchanging L_1, L_2 or x, y, we can achieve that $|L_1(\mathbf{x})| \leqslant |L_2(\mathbf{x})|$ and $|x| \leqslant |y|$. Since the linear forms L_1, L_2 are linearly independent, they span the vector space of all linear forms in X, Y with coefficients in $\mathbb{C}$. Hence X, Y can be expressed as linear combinations of L_1, L_2, i.e., $X = \alpha_1 L_1 + \alpha_2 L_2$, $Y = \alpha_3 L_1 + \alpha_4 L_2$ for certain constants $\alpha_i \in \mathbb{C}$. This implies

$$\max(|x|,|y|) \leqslant C \max(|L_1(\mathbf{x})|, |L_2(\mathbf{x})|) = C \cdot |L_2(\mathbf{x})|$$

where $C = \sum_{i=1}^{4} |\alpha_i|$. Combining this with (1) we obtain

$$|\alpha x + \beta y| \leqslant C \max(|x|,|y|)^{-1-\varepsilon}.$$

If $\alpha = 0$ then $\beta \neq 0$ and the latter inequality implies $|\beta| \cdot |y| \leqslant C \max(|x|,|y|)^{-1-\varepsilon}$ implying that $|y|$ is bounded. If $\alpha \neq 0$ the latter inequality can be rewritten as

$$\left|\frac{x}{y} + \frac{\beta}{\alpha}\right| \leqslant C|\alpha|^{-1}|y|^{-1} \max(|x|,|y|)^{-1-\varepsilon} = C' \max(|x|,|y|)^{-2-\varepsilon}$$

and this inequality has only finitely many solutions by Roth's Theorem. So (1) has only finitely many solutions with $|L_1(\mathbf{x})| \leqslant |L_2(\mathbf{x})|$, $|x| \leqslant |y|$. The cases $|L_1(\mathbf{x})| > |L_2(\mathbf{x})|$ and/or $|x| > |y|$ can be treated in the same way. □

The Subspace Theorem deals with a generalization of (1) with a product of n linearly independent linear forms in n variables.

Theorem 10.1.2 (Subspace Theorem, W.M. Schmidt, 1972). *Let $n \geqslant 2$, let*

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

be n linearly independent linear forms with algebraic coefficients in $\mathbb{C}$ and let $\varepsilon > 0$. Then the set of solutions of the inequality

$$|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| \leqslant \|\mathbf{x}\|^{-\varepsilon} \text{ in } \mathbf{x} \in \mathbb{Z}^n \tag{3}$$

is contained in a union $T_1 \cup \cdots \cup T_t$ of finitely many proper linear subspaces of $\mathbb{Q}^n$.

Remark. The proof of the Subspace Theorem is *ineffective*, i.e., it does not enable to determine the subspaces. There is however a quantitative version of the Subspace Theorem which gives an explicit upper bound for the number of subspaces. This is an important tool for estimating the number of solutions of various types of Diophantine equations.

Theorem 10.1.2$\Longrightarrow$ Theorem 10.1.1 (=Roth's Theorem). According to the Subspace Theorem, the set of solutions of (1) is contained in the union of finitely many proper linear subspaces of $\mathbb{Q}^2$ which all necessarily have dimension 1. Consider one of these subspaces, T, say. Notice that $T = \{\lambda(x_0, y_0) : \lambda \in \mathbb{Q}\}$, where (x_0, y_0) is a fixed vector in $\mathbb{Q}^2$. By multiplying (x_0, y_0) with a suitable scalar, we can achieve that x_0, y_0 are coprime integers. Then the only two solutions of (1) in T are $\pm(x_0, y_0)$. Hence (1) has only finitely many solutions. □

Example. We give an example showing that in general, if $n \geqslant 3$ the set of solutions of (3) need not be finite, not even if we restrict to solutions $\mathbf{x} = (x_1, \ldots, x_n)$ with $\gcd(x_1, \ldots, x_n) = 1$.
Let $0 < \varepsilon < 1$ and consider the inequality

$$|(x_1 + \sqrt{2}x_2 + \sqrt{3}x_3)(x_1 - \sqrt{2}x_2 + \sqrt{3}x_3)(x_1 - \sqrt{2}x_2 - \sqrt{3}x_3)| \leqslant \|\mathbf{x}\|^{-\varepsilon} \tag{4}$$

to be solved in $\mathbf{x} = (x_1, x_2, x_3) \in \mathbb{Z}^3$. Notice that the three linear forms on the left-hand side are linearly independent.

Consider the triples of integers $(x_1, x_2, x_3) \in \mathbb{Z}^3$ with $x_3 = 0, x_1 > 0, x_2 > 0$, satisfying the Pell equation $x_1^2 - 2x_2^2 = 1$. These triples have $\gcd(x_1, x_2, x_3) = 1$, there are infinitely many such triples, and for each such triple, the left-hand side of (4) equals

$$|(x_1 + \sqrt{2}x_2)(x_1 - \sqrt{2}x_2)^2| = \frac{1}{x_1 + \sqrt{2}x_2} \leqslant \|\mathbf{x}\|^{-\varepsilon}.$$

Hence (4) has infinitely many solutions with $\gcd(x_1, x_2, x_3) = 1$ lying in the subspace $x_3 = 0$.

The triples with $x_2 = 0$, $x_1 > 0, x_3 < 0$, $x_1^2 - 3x_3^2 = 1$ lead to infinitely many solutions of (4) with $\gcd(x_1, x_2, x_3) = 1$ in the subspace $x_2 = 0$, and the triples with $x_1 = 0$, $x_2 > 0$, $x_3 < 0$, $2x_2^2 - 3x_3^2 = -1$ to infinitely many solutions with $\gcd(x_1, x_2, x_3) = 1$ in the subspace $x_1 = 0$. The Subspace Theorem implies that the remaining solutions with $x_1x_2x_3 \neq 0$ lie in finitely many proper linear subspaces of $\mathbb{Q}^3$. With a more precise argument one shows that (4) has only finitely many solutions with $x_1x_2x_3 \neq 0$ (Exercise).

We give a generalization of the Subspace Theorem which may be useful for certain applications.

We say that a system of $r \geqslant n$ linear forms $L_1, \ldots, L_r$ in the variables $X_1, \ldots, X_n$ is *in general position* if each n-tuple of linear forms among $L_1, \ldots, L_n$ is linearly independent.

Theorem 10.1.3 *Let*

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

be r linear forms with algebraic coefficients in $\mathbb{C}$ in general position. Then the set of solutions of the inequality

$$|L_1(\mathbf{x}) \cdots L_r(\mathbf{x})| \leqslant \|\mathbf{x}\|^{r-n-\varepsilon} \text{ in } \mathbf{x} \in \mathbb{Z}^n \tag{5}$$

is contained in a union $T_1 \cup \cdots \cup T_t$ of finitely many proper linear subspaces of $\mathbb{Q}^n$.

Proof. This can be derived from the Subspace Theorem. Consider for instance those solutions $\mathbf{x}$ with $|L_1(\mathbf{x})| \leqslant \cdots \leqslant |L_r(\mathbf{x})|$. Let $i \geqslant n+1$. The linear forms $L_1, \ldots, L_{n-1}, L_i$ are linearly independent. By an argument similar to that in the deduction of Theorem 10.1.1 from Roth's Theorem, one shows that there is a constant $C_i > 0$ such that

$$\|\mathbf{x}\| \leqslant C_i \cdot \max(|L_1(\mathbf{x}|, \ldots, |L_{n-1}(\mathbf{x})|, |L_i(\mathbf{x})|) = C_i|L_i(\mathbf{x})|.$$

It is left as an exercise to work out the remaining details and to deduce Theorem 10.1.3. □

10.2 Applications

We deduce some generalizations of Roth's Theorem. We recall Dirichlet's Theorem:

Let $\alpha_1, \ldots, \alpha_n$ be reals which are linearly independent over the rationals. Then there is a constant $C > 0$ such that the inequality

$$|\alpha_1x_1 + \cdots + \alpha_nx_n| \leqslant C\|\mathbf{x}\|^{1-n} \text{ in } \mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n$$

has only finitely solutions.

In Exercise 6.4.4 this has been proved with $\alpha_1 = 1$. The above result can be reduced to this special case by dividing by $|\alpha_1|$. We show that the exponent $1-n$ is best possible if $\alpha_1, \ldots, \alpha_n$ are algebraic numbers.

Theorem 10.2.1 *Let $\alpha_1, \ldots, \alpha_n$ be real algebraic numbers and let $\varepsilon > 0$. Then the inequality*

$$0 < |\alpha_1 x_1 + \cdots + \alpha_n x_n| \leqslant \|\mathbf{x}\|^{1-n-\varepsilon} \text{ in } \mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n \tag{6}$$

has only finitely many solutions.

Proof. We proceed by induction on n. For $n = 1$ the assertion is trivial. (Here we use our assumption $\alpha_1 x_1 \neq 0$). Let $n > 1$ and suppose Theorem 10.2.1 is true for linear forms in fewer than n variables.

We apply the Subspace Theorem. We may assume that at least one of the coefficients $\alpha_1, \ldots, \alpha_n$ is non-zero, otherwise there are no solutions. Suppose that $\alpha_n \neq 0$. Then (6) implies

$$|(\alpha_1 x_1 + \cdots + \alpha_n x_n) x_2 \cdots x_n| \leqslant \|\mathbf{x}\|^{-\varepsilon}$$

and by the Subspace Theorem, the solutions of the latter lie in the union of finitely many proper linear subspaces $T_1, \ldots, T_t$ of $\mathbb{Q}^n$. We consider only solutions with $\alpha_1 x_1 + \cdots + \alpha_n x_n \neq 0$. Therefore, without loss of generality we may assume that $\alpha_1 x_1 + \cdots + \alpha_n x_n$ is not identically 0 on any of the spaces $T_1, \ldots, T_t$.

Consider the solutions of (6) in T_i. Choose a non-trivial linear form vanishing identically on T_i, $a_1 x_1 + \cdots + a_n x_n = 0$. Then one of the variables x_i can be expressed as a linear combination of the others. By substituting this into (6) we obtain a similar such inequality, with in the left-hand side a linear form in $n-1$ variables which is not identically 0. By the induction hypothesis, the latter inequality has only finitely many solutions. So T_i contains only finitely many solutions of (6). Applying this to $T_1, \ldots, T_t$ we obtain that (6) has only finitely many solutions. □

Let ξ be an algebraic number and $f(X) = a_0 X^n + \cdots + a_n \in \mathbb{Z}[X]$ the minimal polynomial of ξ. We may write

$$f(X) = a_0(X - \xi_1) \cdots (X - \xi_n) \text{ with } \xi_1 = \xi.$$

We define heights

$$H(\xi) := |a_0| \prod_{i=1}^{n} \max(1, |\xi_i|), \quad \tilde{H}(\xi) := \max(|a_0|, \ldots, |a_n|).$$

We state without proof that

$$(n+1)^{-1/2}H(\xi) \leqslant \tilde{H}(\xi) \leqslant 2^n H(\xi).$$

The upper bound is easy to prove but the lower bound requires a more involved argument.

Theorem 10.2.2 *Let α be a real algebraic number and n a positive integer. Further, let $\varepsilon > 0$. Then the inequality*

$$|\alpha - \xi| \leqslant \tilde{H}(\xi)^{-n-1-\varepsilon} \text{ in real algebraic numbers } \xi \text{ of degree } n \tag{7}$$

has only finitely many solutions.

Proof. Let ξ be a solution to (7) which is not conjugate to α (thus we exclude only finitely many solutions ξ). Let $f(X) = x_0X^n + x_1X^{n-1} + \cdots + x_n$ be the minimal polynomial of ξ, where $\mathbf{x} = (x_0, \ldots, x_n) \in \mathbb{Z}^{n+1}$. Notice that by the mean value theorem we have $|f(\alpha)| = |f'(\theta)| \cdot |\xi - \alpha|$ for some θ between ξ and α. Further, $f(\alpha) \neq 0$ since α is not equal to a conjugate of ξ. Using that

$$|\theta| \leqslant |\alpha| + |\theta - \alpha| \leqslant |\alpha| + |\xi - \alpha| \leqslant |\alpha| + 1,$$

we obtain

$$\begin{aligned} 0 < |x_0\alpha^n + \cdots + x_n| &= |f(\alpha)| = |f'(\theta)| \cdot |\xi - \alpha| \\ &\leqslant \sum_{i=0}^{n} ((n-i)|x_i| \cdot |\theta|^{n-i-1})|\xi - \alpha| \leqslant C\tilde{H}(\xi) \cdot |\xi - \alpha| \leqslant C\tilde{H}(\xi)^{-n-\varepsilon} \\ &= C\|\mathbf{x}\|^{-n-\varepsilon} \end{aligned}$$

for some constant $C > 0$. By the previous theorem (with $n+1$ instead of n), the latter inequality has only finitely many solutions. These give rise to finitely many minimal polynomials f, hence to finitely many algebraic numbers ξ. □

Remark. One can show that if α is real algebraic of degree $> n$, then the number of solutions of (7) becomes infinite if the exponent $-n-1-\varepsilon$ is replaced by $-n-1+\varepsilon$ for any $\varepsilon > 0$.

10.3 Exercises.

Exercise 10.3.1 *In this exercise, n is an integer $\geqslant 3$.*

(1) Let $M_1, \dots, M_n$ be n linearly independent linear forms in $X_1, \dots, X_n$ with coefficients in $\mathbb{C}$. Prove that there is a constant $C > 0$ such that for all $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{C}^n$ we have

$$\max(|x_1|, \dots, \mathbf{x}_n|) \leqslant C \max(|M_1(\mathbf{x})|, \dots, |M_n(\mathbf{x})|).$$

(2) Deduce Theorem 10.1.3 from Theorem 10.1.2.

Exercise 10.3.2 *Let $0 < \varepsilon < 1$ and consider the inequality*

$$|(x_1 + \sqrt{2}x_2 + \sqrt{3}x_3)(x_1 - \sqrt{2}x_2 + \sqrt{3}x_3)(x_1 - \sqrt{2}x_2 - \sqrt{3}x_3)| \leqslant \|\mathbf{x}\|^{-\varepsilon} \qquad (8)$$

to be solved in $\mathbf{x} = (x_1, x_2, x_3) \in \mathbb{Z}^3$.

(1) Let T be a one-dimensional linear subspace of $\mathbb{Q}^3$. Prove that T contains at most finitely many solutions from (8).

(2) Let $T = \{\mathbf{x} \in \mathbb{Q}^3 : a_1x_1 + a_2x_2 + a_3x_3 = 0\}$, where $a_1, a_2, a_3 \in \mathbb{Q}$ and at least two among a_1, a_2, a_3 are non-zero. Consider the solutions $\mathbf{x} = (x_1, x_2, x_3)$ of (8) in T and eliminate one of the variables x_1, x_2, x_3 by expressing it as a linear combination of the two others. Prove that after this elimination, the linear forms L_1, L_2, L_3 become a system of linear forms in two variables which is in general position. Distinguish between the cases $a_3 = 0$ giving $x_2 = -(a_1/a_2)x_1$, and $a_3 \neq 0$ giving $x_3 = -(a_1/a_3)x_1 - (a_2/a_3)x_2$.

(3) Prove that (8) has only finitely many solutions with $x_1x_2x_3 \neq 0$.

Remark. In 1989, Vojta proved the following refinement of the Subspace Theorem. Let again $L_1, \dots, L_n$ be n linearly independent linear forms with algebraic coefficients in $\mathbb{C}$ and $\varepsilon > 0$. Then there exist a finite collection $S_1, \dots, S_m$ of proper linear subspaces of $\mathbb{Q}^n$, which is effectively determinable and which is independent of ε, and a finite set F_ε which depends on ε, such that the set of solutions of

$$|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| \leqslant \|\mathbf{x}\|^{-\varepsilon} \text{ in } \mathbf{x} \in \mathbb{Z}^n$$

is contained in $S_1 \cup \cdots \cup S_m \cup F_\varepsilon$.

In example (8) one can take $S_1 = \{x_1 = 0\}$, $S_2 = \{x_2 = 0\}$, $S_3 = \{x_3 = 0\}$.

Exercise 10.3.3 *Let $L_1 = \alpha_1X_1 + \cdots + \alpha_nX_n$, $L_2 = \beta_1X_1 + \cdots + \beta_nX_n$ be two linearly independent linear forms with algebraic coefficients from $\mathbb{C}$. Let $\varepsilon > 0$. Prove that the system of inequalities*

$$0 < |L_1(\mathbf{x})| \leqslant \|\mathbf{x}\|^{1-n}, \ 0 < |L_2(\mathbf{x})| \leqslant \|\mathbf{x}\|^{1-\varepsilon} \text{ in } \mathbf{x} \in \mathbb{Z}^n$$

has only finitely many solutions.

Exercise 10.3.4 *Let $\alpha_1, \ldots, \alpha_n$ be real algebraic numbers such that $1, \alpha_1, \ldots, \alpha_n$ are linearly independent over $\mathbb{Q}$ and let $\varepsilon > 0$. Prove that the system of inequalities*

$$|\alpha_1 - \frac{x_1}{x_{n+1}}| \leqslant \|\mathbf{x}\|^{-1-\frac{1}{n}-\varepsilon}, \ldots, |\alpha_n - \frac{x_n}{x_{n+1}}| \leqslant \|\mathbf{x}\|^{-1-\frac{1}{n}-\varepsilon} \tag{9}$$

to be solved simultaneously in $\mathbf{x} = (x_1, \ldots, x_{n+1}) \in \mathbb{Z}^{n+1}$, has only finitely many solutions.

Hint. *Prove that the solutions lie in finitely many proper linear subspaces of $\mathbb{Q}^{n+1}$. Then give a direct proof, so without using the Subspace Theorem, that any proper subspace T of $\mathbb{Q}^n$ contains only finitely many solutions of (9).*
To this end, take a non-trivial equation $a_1x_1 + \cdots + a_nx_n + a_{n+1}x_{n+1} = 0$ vanishing identically on T, and assuming that T contains a non-zero solution $\mathbf{x} \in \mathbb{Z}^{n+1}$, estimate from above $|a_1\alpha_1 + \cdots + a_n\alpha_n + a_{n+1}|$.

Exercise 10.3.5 *Recall that if K is an algebraic number field of degree n, and $\sigma_1, \ldots, \sigma_n$ are the embeddings $K \to \mathbb{C}$, then the norm of $\alpha \in K$ is given by*

$$N_{K/\mathbb{Q}}(\alpha) := \prod_{i=1}^{n} \sigma_i(\alpha).$$

We have $N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Q}$ for $\alpha \in K$.

Let $K = \mathbb{Q}(\sqrt[5]{2})$. Thus, there are precisely five embeddings $\sigma_1, \ldots, \sigma_5 : K \to \mathbb{C}$, given by $\sigma_i(\sqrt[5]{2}) = \rho^{i-1}\sqrt[5]{2}$, where ρ is a primitive 5-th root of unity.

Consider the Diophantine equation

$$N_{K/\mathbb{Q}}(x_1 + x_2\sqrt[5]{2} + x_3(\sqrt[5]{2})^2) = 1 \text{ in } \mathbf{x} = (x_1, x_2, x_3) \in \mathbb{Z}^3\,. \tag{10}$$

(1) Prove that the left-hand side of (10) is a product of linear forms in general position (think of Vandermonde determinants).

(2) Let $\alpha, \beta \in K$ with $\beta \neq 0$ and $\alpha/\beta \notin \mathbb{Q}$. Prove that the linear forms $\sigma_i(\alpha)X + \sigma_i(\beta)Y$ $(i = 1, \ldots, 5)$ are in general position.

(3) Prove that (10) has only finitely many solutions.

Remark. Equation (10) is a special case of a so-called *norm form equation*. A norm form equation is an equation of the type

$$N_{K/\mathbb{Q}}(\alpha_1x_1 + \cdots + \alpha_nx_n) = c \text{ in } x_1, \ldots, x_n \in \mathbb{Z} \tag{11}$$

where K is an algebraic number field, $\alpha_1, \ldots, \alpha_n \in K$ and where c is a non-zero integer. In 1972, applying his Subspace Theorem, Schmidt gave a necessary and sufficient algebraic condition in terms of K, $\alpha_1, \ldots, \alpha_n$, such that (11) has only finitely many solutions for every non-zero integer c.