Astérisque

YURI F. BILU

# The many faces of the subspace theorem [after Adamczewski, Bugeaud, Corvaja, Zannier...]

*Astérisque*, tome 317 (2008), Séminaire Bourbaki, exp. n° 967, p. 1-38
<http://www.numdam.org/item?id=AST_2008__317__1_0>

Séminaire BOURBAKI
59e année, 2006–2007, n° 967, p. 1 à 39

Novembre 2006

# THE MANY FACES OF THE SUBSPACE THEOREM
## [after Adamczewski, Bugeaud, Corvaja, Zannier...]

by **Yuri F. BILU***

*And we discovered subspace. It gave us our galaxy and it gave us the universe. And we saw other advanced life. And we subdued it or we crushed it... With subspace, our empire would surely know no boundaries.*

(From *The Great War* computer game)

## 1. INTRODUCTION

This is not a typical Bourbaki talk. A generic *exposé* on this seminar is, normally, a report on a recent seminal achievement, usually involving new technique. The principal character of this talk is the Subspace Theorem of Wolfgang Schmidt, known for almost forty years. All results I am going to talk about rely on this celebrated theorem (more precisely, on the generalization due to Hans Peter Schlickewei). Moreover, in all cases it is by far the most significant ingredient of the proof.

Of course, the last remark is not meant to belittle the work of the authors of the results I am going to speak about. Adapting the Subspace Theorem to a concrete problem is often a formidable task, requiring great imagination and ingenuity.

During the last decade the Subspace Theorem found several quite unexpected applications, mainly in the Diophantine Analysis and in the Transcendence Theory. Among the great variety of spectacular results, I have chosen several which are technically simpler and which allow one to appreciate how miraculously does the Subspace Theorem emerge in numerous situations, implying beautiful solutions to difficult problems hardly anybody hoped to solve so easily.

The three main topics discussed in this article are:

- the work of Adamczewski and Bugeaud on complexity of algebraic numbers;
- the work of Corvaja and Zannier on Diophantine equations with power sums;

– the work of Corvaja and Zannier on integral points on curves and surfaces, and the subsequent development due to Levin and Autissier.

In particular, we give a complete proof of the beautiful theorem of Levin and Autissier (see Theorem 5.8): *an affine surface with 4 (or more) properly intersecting ample divisors at infinity cannot have a Zariski dense set of integral points.*

Originally, Schmidt proved his theorem for the needs of two important subjects: norm form equations and exponential Diophantine equations (including the polynomial-exponential equations and linear recurrence sequences). These "traditional" applications of the Subspace Theorem form a vast subject, interesting on its own; we do not discuss it here (except for a few motivating remarks in Section 4). Neither do we discuss the quantitative aspect of the Subspace Theorem. For this, the reader should consult the fundamental work of Evertse and Schlickewei (see [**33, 34, 56, 52, 57**] and the references therein).

Some of the results stated here admit far-going generalizations, but I do not always mention them: the purpose of this talk is to exhibit ideas rather than to survey the best known results.

In Section 2 we introduce the Subspace Theorem. Sections 3, 4 and 5 are totally independent and can be read in any order.

## 2. THE SUBSPACE THEOREM

In this section we give a statement of the Subspace Theorem. Before formulating it in full generality, we consider several particular cases, to make the general case more motivated.

### 2.1. The Theorem of Roth

In 1955, K. F. Roth [**51**] proved that algebraic numbers cannot be "well approximated" by rationals.

THEOREM 2.1 (Roth). — *Let $\alpha$ be an irrational algebraic number. Then for any $\varepsilon > 0$ the inequality*

$$\left|\alpha - \frac{y}{x}\right| < \frac{1}{|x|^{2+\varepsilon}}$$

*has only finitely many solutions in non-zero $x, y \in \mathbb{Z}$.*

This result is, in a sense, best possible, because, by the Dirichlet approximation theorem, the inequality $|\alpha - y/x| \leq |x|^{-2}$ has infinitely many solutions.

The theorem of Roth has a glorious history. Already Liouville showed in 1844 the inequality $|\alpha - y/x| \geq c(\alpha)|x|^{-n}$, where $n$ is the degree of the algebraic number $\alpha$,

and used this to give first examples of transcendental numbers. However, Liouville's theorem was too weak for serious applications in the Diophantine Analysis. In 1909 A. Thue [**64**] made a breakthrough, proving that $|\alpha - y/x| \leq |x|^{-n/2-1-\varepsilon}$ has finitely many solutions. A series of refinements (the most notable being due to Siegel [**62**]) followed, and Roth made the final (though very important and difficult) step.

Kurt Mahler, who was a long proponent of $p$-adic Diophantine approximations, suggested to his student D. Ridout [**50**] to extend Roth's theorem to the non-archimedean domain. To state Ridout's result, we need to introduce some notation. For every prime number $p$, including the "infinite prime" $p = \infty$, we let $|\cdot|_p$ be the usual $p$-adic norm on $\mathbb{Q}$ (so that $|p|_p = p^{-1}$ if $p < \infty$ and $|2006|_\infty = 2006$), somehow extended to the algebraic closure $\bar{\mathbb{Q}}$. For a rational number $\xi = y/x$ with $\gcd(x, y) = 1$ we define its *height* by

$$H(\xi) = \max\{|x|, |y|\}. \tag{1}$$

One immediately verifies that

$$H(\xi) = \prod_p \max\{1, |\xi|_p\} = \left(\prod_p \min\{1, |\xi|_p\}\right)^{-1}, \tag{2}$$

where the products extend to all prime numbers, including the infinite prime.

Now let $S$ be a finite set of primes, including $p = \infty$, and for every $p \in S$ we fix an algebraic number $\alpha_p$. Ridout proved that for any $\varepsilon > 0$ the inequality

$$\prod_{p \in S} \min\left\{1, |\alpha_p - \xi|_p\right\} < \frac{1}{H(\xi)^{2+\varepsilon}}$$

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

While the theorem of Roth becomes interesting only when the degree of $\alpha$ is at least 3, the theorem of Ridout is quite non-trivial even when the "targets" $\alpha_p$ are rational. Moreover, one can also allow "infinite" targets, with the standard convention $\infty - \xi = \xi^{-1}$. The following particular case of Ridout's theorem is especially useful: given an algebraic number $\alpha$, a set $S$ of prime numbers, and $\varepsilon > 0$, the inequality

$$|\alpha - \xi| < H(\xi)^{-1-\varepsilon}$$

has finitely many solutions in $S$-integers [(1)] $\xi$. To prove this, consider the theorem of Ridout with $\alpha_\infty = \alpha$ and with $\alpha_p = \infty$ for $p \neq \infty$, and apply (2).

One consequence of this result is that the decimal expansion of an algebraic number cannot have "too long" blocks of zeros. More precisely, let $0.a_1a_2\ldots$ be the decimal expansion of an algebraic number, and for every $n$ define $\ell(n)$ as the minimal $\ell \geq 0$

(1) A rational number is called $S$-integer if its denominator is divisible only by the prime numbers from $S$.

such that $a_{n+\ell} \neq 0$; then $\ell(n) = o(n)$ as $n \to \infty$. To show this, apply the above-stated particular case of the theorem of Ridout with $S = \{2, 5, \infty\}$. More generally, the decimal expansion of an algebraic number cannot have "too long" periodic blocks.

S. Lang extended the theorem of Roth-Ridout to approximation of algebraic numbers by the elements of a given number field. We invite the reader to consult Chapter 7 of his book [**41**] or Part D of the more recent volume [**40**] for the statement and the proof of Lang's theorem.

### 2.2. The Statement of the Subspace Theorem

Now we have enough motivation to state the Subspace Theorem. We begin with the original theorem of Schmidt [**58**] (see also [**59**] for a very detailed proof).

THEOREM 2.2 (W. M. Schmidt). — *Let $L_1, \dots, L_m$ be linearly independent linear forms in $m$ variables with (real) algebraic coefficients. Then for any $\varepsilon > 0$ the solutions $\mathbf{x} = (x_1, \dots, x_m) \in \mathbb{Z}^m$ of the inequality*

$$|L_1(\mathbf{x}) \cdots L_m(\mathbf{x})| \leq \|\mathbf{x}\|^{-\varepsilon}$$

*are contained in finitely many proper linear subspaces of $\mathbb{Q}^m$. (Here $\|\mathbf{x}\| = \max_i\{|x_i|\}$.)*

Putting $m = 2$, $L_1(x, y) = x\alpha - y$ and $L_2(x, y) = x$, we recover the theorem of Roth.

The theorem of Schmidt is not sufficient for many applications. One needs a non-archimedean generalization of it, analogous to Ridout's generalization of Roth's theorem. This result was obtained by Schlickewei [**53, 54**]. As in the previous section, let $S$ be a finite set of prime numbers, including $p = \infty$, and pick an extension of every $p$-adic valuation to $\bar{\mathbb{Q}}$.

THEOREM 2.3 (H. P. Schlickewei). — *For every $p \in S$ let $L_{1,p}, \dots, L_{m,p}$ be linearly independent linear forms in $m$ variables with algebraic coefficients. Then for any $\varepsilon > 0$ the solutions $\mathbf{x} \in \mathbb{Z}^m$ of the inequality*

$$\prod_{p \in S} \prod_{i=1}^{m} |L_{i,p}(\mathbf{x})|_p \leq \|\mathbf{x}\|^{-\varepsilon}$$

*are contained in finitely many proper linear subspaces of $\mathbb{Q}^m$.*

It is usually more convenient to allow the variables $x_1, \dots, x_m$ to be $S$-integers rather than integers. To restate Schlickewei's theorem using the $S$-integer variables, one needs an adequate measure of the "size" of a vector with $S$-integer (or, more

generally, rational) coordinates; evidently, the sup-norm $\|\mathbf{x}\|$ cannot serve for this purpose. Thus, let $\mathbf{x}$ be a non-zero vector from $\mathbb{Q}^m$; we define its *height* by

$$H(\mathbf{x}) = \prod_p \|\mathbf{x}\|_p, \tag{3}$$

where $\|\mathbf{x}\|_p = \max\{|x_1|_p, \dots, |x_m|_p\}$, and the product extends to all rational primes, including $p = \infty$.

The height function, defined this way, is "projective": if $a \in \mathbb{Q}^*$ then $H(a\mathbf{x}) = H(\mathbf{x})$ (this is an immediate consequence of the product formula). When the coordinates $x_1, \dots, x_m$ are coprime integers, we have $H(\mathbf{x}) = \|\mathbf{x}\|$.

REMARK 2.4. — One piece of warning: the height of a rational number $\xi$, defined in (1) is *not* equal to the height of the "one-dimensional vector" with the coordinate $\xi$; in fact, the height of a non-zero one-dimensional vector is 1, by the product formula, while $H(\xi)$ is the height of the 2-dimensional vector $(1, \xi)$, according to (2). This abuse of notation is quite common and will not lead to any confusion.

Denote by $\mathbb{Z}_S$ the ring of $S$-integers. Now Theorem 2.3 can be re-stated as follows.

THEOREM 2.3′. — *In the set-up of Theorem 2.3, the solutions $\mathbf{x} \in \mathbb{Z}_S^m$ of the inequality*

$$\prod_{p \in S} \prod_{i=1}^{m} |L_{i,p}(\mathbf{x})|_p \le H(\mathbf{x})^{-\varepsilon}$$

*are contained in finitely many proper linear subspaces of $\mathbb{Q}^m$.*

It is very easy to deduce Theorem 2.3′ from Theorem 2.3; we leave this as an exercise for the reader. (One should use the "product formula" $\prod_p |a|_p = 1$, where $a \in \mathbb{Q}^*$ and the product extends to all rational primes, including $p = \infty$.)

Unfortunately, for many applications Theorem 2.3′ is insufficient as well: one needs to extend it to the case when the variables $x_1, \dots, x_m$ belong to an arbitrary number field. This was also done by Schlickewei [**55**]. Before stating the theorem, we need to make some conventions. Let $K$ be a number field of degree $d = [K : \mathbb{Q}]$ and let $M_K$ be the set of all absolute values on $K$. Recall that the set $M_K$ consists of infinitely many *finite* absolute values, corresponding to prime ideals of the field $K$, and finitely many *infinite* absolute values, corresponding to real embeddings of $K$ (real absolute values) and pairs of complex conjugate embeddings (complex absolute values).

We normalize the absolute values on $K$ as follows. If $v \in M_K$ is a $\mathfrak{p}$-adic absolute value, then we normalize it so that $|p|_v = p^{-d_v/d}$, where $p$ is the prime number below the prime ideal $\mathfrak{p}$ and $d_v = [K_v : \mathbb{Q}_p]$ is the local degree. If $v$ is an infinite absolute value, then we normalize it to have $|2006|_v = 2006^{d_v/d}$, where $d_v$ is again the local degree (that is, $d_v = 1$ if $v$ is real and $d_v = 2$ if $v$ is complex). With this normalization we have the product formula in the form $\prod_{v \in M_K} |a|_v = 1$, where $a \in K^*$.

We also need to define the height of a vector $\mathbf{x} \in K^m$. By analogy with (3) we put $H(\mathbf{x}) = \prod_{v \in M_K} \|\mathbf{x}\|_v$, where $\|\mathbf{x}\|_v = \max\{|x_1|_v, \dots, |x_m|_v\}$. An easy verification shows that for $\mathbf{x} \in \mathbb{Q}^m$ this definition agrees with (3).

Now we are ready to state the Subspace Theorem in its most general form. Let $K$ be a number field, and let $S$ be a finite set of absolute values of $K$ (normalized as above), including all the infinite absolute values. We denote by $\mathcal{O}_S$ the ring of $S$-integers [2] of the field $K$.

THEOREM 2.5 (H. P. Schlickewei). — *For every $v \in S$ let $L_{1,v}, \dots, L_{m,v}$ be linearly independent linear forms in $m$ variables with algebraic coefficients. Then for any $\varepsilon > 0$ the solutions $\mathbf{x} \in \mathcal{O}_S^m$ of the inequality*

$$\prod_{v \in S} \prod_{i=1}^{m} |L_{i,v}(\mathbf{x})|_v \leq H(\mathbf{x})^{-\varepsilon}$$

*are contained in finitely many proper linear subspaces of $K^m$.*

A complete proof of this theorem can be found, for instance, in Chapter 7 of the recent book [**9**] by Bombieri and Gubler (who use a slightly different definition of height).

## 3. COMPLEXITY OF ALGEBRAIC NUMBERS

Quite recently Adamczewski and Bugeaud applied the Subspace Theorem to the long-standing problem of complexity of algebraic numbers. In particular, they proved transcendence of irrational automatic numbers. This will be the first topic of this talk.

We need some definitions. Let $\mathcal{A}$ be a finite set. We call it an *alphabet*, and its elements will be referred to as *letters*. Let $U = (u_1, u_2, u_3, \dots)$ be an infinite sequence of letters from $\mathcal{A}$. For every positive integer $n$, we let $\rho(n) = \rho_U(n)$ be the number of distinct $n$-words occurring as $n$ successive elements of $U$:

$$\rho(n) = \big|\{u_k u_{k+1} \dots u_{k+n-1} \mid k = 1, 2, 3, \dots\}\big|.$$

Obviously, $1 \leq \rho(n) \leq |\mathcal{A}|^n$. The function $\rho(n)$, defined on the set of natural numbers, is called the *complexity function*, or simply *complexity* of the sequence $U$.

Now let $\alpha \in (0, 1)$ be a real number. For every integer $b \geq 2$ we can write the $b$-ary digital expansion of $\alpha$:

$$\alpha = u_1 b^{-1} + u_2 b^{-2} + u_3 b^{-3} + \dots, \tag{4}$$

[2] An element $\alpha \in K$ is called $S$-integer if $|\alpha|_v \leq 1$ for all $v \notin S$.

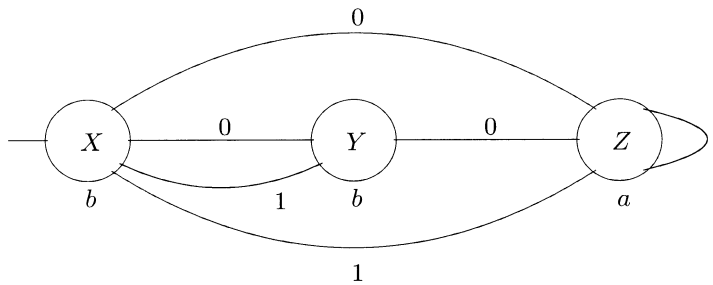


FIGURE 1. A finite automaton with 3 states

where $u_1, u_2, u_3, \cdots \in \{0, 1, \ldots, b-1\}$. One may ask about the complexity of the digital sequence $(u_1, u_2, u_3, \ldots)$. For instance, if $\alpha$ is rational, then the expansion is (eventually) periodic, and the complexity function is bounded. Adamczewski and Bugeaud proved that the complexity function of the $b$-ary expansion of an irrational algebraic number is strictly non-linear.

THEOREM 3.1 (Adamczewski, Bugeaud). — *Let $\alpha \in (0,1)$ be an irrational algebraic number, and let $b \geq 2$ be an integer. Then the complexity function $\rho(n)$ of the $b$-ary expansion of $\alpha$ satisfies $\lim_{n\to\infty} \rho(n)/n = \infty$.*

Previously, it was only known that $\rho(n) - n \to +\infty$, which follows from the results of [**36**].

It is widely believed since the work of Borel [**10, 11**] that irrational algebraic numbers are *normal*; that is, every $n$-word occurs in the $b$-ary expansion with the correct frequency $b^{-n}$. In particular, one should expect that $\rho(n) = b^n$. This conjecture (let alone Borel normality) is far beyond the capabilities of the modern mathematics.

An important consequence of this theorem is transcendence of irrational *automatic numbers*. Recall that a finite automaton consists of the following elements:

- the *input alphabet*, which is usually the set of $k \geq 2$ digits $\{0, 1, \ldots, k-1\}$;
- the set of *states* $\mathcal{Q}$, usually a finite set of 2 or more elements, with one element (called the *initial state*) singled out;
- the *transition map* $\mathcal{Q} \times \{0, 1, \ldots, k-1\} \to \mathcal{Q}$, which associates to every state a new state depending on the current input;
- the *output alphabet* $\mathcal{A}$, together with the *output map* $\mathcal{Q} \to \mathcal{A}$.

On Figure 1 one can see an example of a finite automaton with inputs $0, 1$, states $X, Y, Z$ with $X$ the initial state, and outputs $a, b$. The transition map is given by the arrows, and the output map is $X \mapsto b$, $Y \mapsto b$ and $Z \mapsto a$.

An input stream for a finite automaton is a word in the input alphabet. Let us take the word 00100. We start at the initial state $X$ and the first input 0 moves us to

the state $Y$. The next input 0 moves us further to $Z$, and the third input 1 tells us to stay in $Z$. With the fourth input 0 we return to $X$, and with the final fifth input we end up in $Y$. The output of $Y$ is $b$. Thus, the word 00100 produces output $b$.

If we input consecutively the binary expansion of natural numbers $0, 1, 2, 3, \ldots$ written from right to left (that is, $0, 1, 01, 11, 001, \ldots$), we obtain the sequence of outputs $b, a, b, a, a, \ldots$ called the *automatic sequence* generated by the automaton from Figure 1.

More generally, given an automaton with $K$ inputs $0, 1, \ldots, k-1$, the sequence generated by this automaton is the result of consecutive inputs of $k$-ary expansions of natural numbers written from right to left.

Probably, the most famous non-periodic automatic sequence is the *Thue-Morse sequence* $0, 1, 1, 0, 1, 0, 0, 1, \ldots$, the $n$-th term being the parity of the sum of digits of the binary expansion of $n$; it is generated by a finite automaton with 2 inputs, 2 states and 2 outputs.

A real number $\alpha \in (0, 1)$ is called *automatic* if the digits of its $b$-ary expansion (for some $b \geq 2$) form an automatic sequence.

For more information on automatic sequence, see the book of Allouche and Shallit [**5**].

It is well-known (see, for instance, [**17**] or [**5**, Section 10.3]) that the complexity of an automatic sequence satisfies $\rho(n) = O(n)$. Hence Theorem 3.1 implies the following remarkable result.

COROLLARY 3.2. — *An irrational automatic number is transcendental.*

Probably, the first one to conjecture this was Cobham [**16**]. Sometimes this is referred to as the *problem of Loxton and van der Poorten*, who obtained [**44, 45**] several results in favor of this conjecture.

Adamczewski and Bugeaud deduce Theorem 3.1 from a new transcendence criterion they obtained jointly with F. Luca. The proof of this criterion relies on the Subspace Theorem. We say that the infinite sequence $(u_n)$ has *long repetitions* if there exist a real $\varepsilon > 0$, and infinitely many natural $N$ such that the word $u_1 u_2 \ldots u_N$ has two disjoint equal subwords of length exceeding $\varepsilon N$.

In symbols, the phrase "the word $u_1 u_2 \ldots u_N$ has two disjoint equal subwords of length $\ell$" means the following: there exist $k$ and $n$ such that $k + \ell \leq n \leq N + 1 - \ell$ and

$$u_k = u_n, \quad u_{k+1} = u_{n+1}, \quad \ldots, \quad u_{k+\ell-1} = u_{n+\ell-1}.$$

THEOREM 3.3 (Adamczewski, Bugeaud, Luca). — *Assume that for some $b \geq 2$ the $b$-ary expansion of $\alpha \in (0, 1)$ has long repetitions. Then $\alpha$ is either rational or transcendental.*

In the introduction we remarked that the decimal expansion of an irrational algebraic number cannot have too long blocks of zeros (or too long periodic blocks), which is a relatively easy consequence of the theorem of Ridout. Theorem 3.3 is a far-going generalization of this observation.

Theorem 3.1 is a consequence of Theorem 3.3, due to the following simple lemma.

LEMMA 3.4. — *Assume that the complexity function of an infinite sequence* $(u_n)$ *satisfies* $\liminf_{n\to\infty} \rho(n)/n < \infty$. *Then* $(u_n)$ *has long repetitions.*

PROOF. — By the assumption, there exists $\kappa > 0$ such that $\rho(n) < \kappa n$ for infinitely many $n$. Fix such $n$ and put $N = \lceil (\kappa+1)n \rceil$. By the box principle, the word $u_1 u_2 \dots u_N$ contains two equal subwords of length $n$. If they are disjoint, then we are done, because $n \geq N/2(\kappa+1)$. Now assume they are not. This means that $u_1 u_2 \dots u_N$ contains a subword $W = ABC$, where the words $A$, $B$ and $C$ are non-empty and where $AB$ and $BC$ are equal words of length $n$.

Since the words $AB$ and $BC$ are equal, we have $W = AAB$, which means that $AA$ is a prefix [(3)] of $W$. If $\ell(AA) \leq n$ (where we denote by $\ell(X)$ the length of the word $X$) then $AA$ is a prefix of $AB$, which means that $AAA$ is a prefix of $W$. Continuing by induction, we see that $W$ has a prefix $\underbrace{A \dots A}_{k}$, where $k = \lfloor n/\ell(A) \rfloor + 1$ (in particular, $k \geq 2$ and $k\ell(A) > n$). This implies that there are two disjoint words equal to $\underbrace{A \dots A}_{\lfloor k/2 \rfloor}$. Since $k \geq 2$ we have $\lfloor k/2 \rfloor \geq k/3$, which implies that the length of these words is at least $n/3$. Hence the lemma is proved with $\varepsilon = 1/6(\kappa+1)$. □

PROOF OF THEOREM 3.3. — We assume that $\alpha$ is algebraic and show that it is rational. Write the $b$-ary expansion of $\alpha$ as in (4). By the hypothesis, there exist $\varepsilon > 0$ and infinitely many natural $N$ such that the initial $N$-segment $W_N = u_1 \dots u_N$ has two disjoint subwords of length at least $\varepsilon N$. Fix one such $N$. Then $W_N$ has a prefix $ABCB$, where $\ell(B) \geq \varepsilon N$ (the words $A$ and $C$ may be empty). Let $\xi$ be the rational number with the eventually periodic $b$-ary expansion $ABCBCBC\dots$. A straightforward calculation shows that

$$\xi = \frac{M}{b^r(b^s - 1)},$$

with $M \in \mathbb{Z}$, where $r = \ell(A)$ is the length of the non-periodic part, and $s = \ell(BC)$ is the length of the period. Notice that $s + r = \ell(ABC) \leq N$ and that $s \geq \ell(B) \geq \varepsilon N$.

(3) A *prefix* of the word $v_1 \dots v_m$ is any of the words $v_1 \dots v_s$ with $s \leq m$.