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>

© Société mathématique de France, 2008, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/
Publications/Asterisque/) implique l'accord avec les conditions générales d'uti-
lisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou
impression systématique est constitutive d'une infraction pénale. Toute copie
ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

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 α 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 $|\alpha - y/x| \le |x|^{-2}$ has infinitely many solutions.

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

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

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

One immediately verifies that

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

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 α_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 α is at least 3, the theorem of Ridout is quite non-trivial even when the "targets" α_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 α, 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] ξ. 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 $0.a_1 a_2 \ldots$ 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* $L_1, \ldots, L_m$ *be linearly independent linear forms in* m *variables with (real) algebraic coefficients. Then for any* $\varepsilon > 0$ *the solutions* $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{Z}^m$ *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* $L_{1,p}, \ldots, L_{m,p}$ *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 $x_1, \ldots, x_m$ 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

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

where $\|\mathbf{x}\|_p = \max\{|x_1|_p, \ldots, |x_m|_p\}$, 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 $x_1, \ldots, x_m$ are coprime integers, we have $H(\mathbf{x}) = \|\mathbf{x}\|$.

REMARK 2.4. — One piece of warning: the height of a rational number ξ, defined in (1) is *not* equal to the height of the "one-dimensional vector" with the coordinate ξ; 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 $x_1, \ldots, x_m$ 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 $\|\mathbf{x}\|_v = \max\{|x_1|_v, \ldots, |x_m|_v\}$. 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 $L_{1,v}, \ldots, L_{m,v}$ 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 $U = (u_1, u_2, u_3, \ldots)$ 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:

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

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 α:

(4) $\alpha = u_1 b^{-1} + u_2 b^{-2} + u_3 b^{-3} + \ldots,$

---

[2] An element $\alpha \in K$ is called S-integer if $|\alpha|_v \leq 1$ for all $v \notin S$.
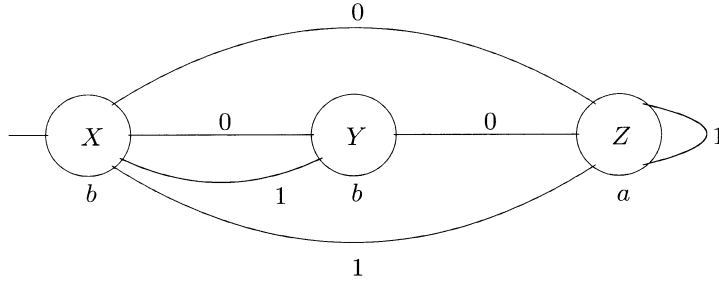
FIGURE 1. A finite automaton with 3 states

where $u_1, u_2, u_3, \dots \in \{0, 1, \dots, b-1\}$. One may ask about the complexity of the digital sequence $(u_1, u_2, u_3, \dots)$. For instance, if α 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 α 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 $\{0, 1, \dots, k-1\}$;
- 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* $\mathcal{Q} \times \{0, 1, \dots, k-1\} \to \mathcal{Q}$, 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 εN.

In symbols, the phrase "the word $u_1 u_2 \ldots u_N$ has two disjoint equal subwords of length ℓ" 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 α 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* $\liminf\limits_{n\to\infty} \rho(n)/n < \infty$. *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 $u_1 u_2 \ldots u_N$ 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 $u_1 u_2 \ldots u_N$ 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 $\underbrace{A \ldots A}_{k}$, 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 $\underbrace{A \ldots A}_{\lfloor k/2 \rfloor}$.

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 $\varepsilon = 1/6(\kappa + 1)$. $\qquad\square$

PROOF OF THEOREM 3.3. — We assume that α is algebraic and show that it is rational. Write the b-ary expansion of α as in (4). By the hypothesis, there exist $\varepsilon > 0$ and infinitely many natural N such that the initial N-segment $W_N = u_1 \ldots u_N$ has two disjoint subwords of length at least εN. 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 ξ be the rational number with the eventually periodic b-ary expansion $ABCBCBC \ldots$. 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 $v_1 \ldots v_m$ is any of the words $v_1 \ldots v_s$ with $s \leq m$.

The main point of the proof is that ξ is a good rational approximation for α. Indeed, the first $\ell(ABCB)$ digits of the b-ary expansions of α and ξ coincide. Since $\ell(ABCB) = r + s + \ell(B) \geq r + s + \varepsilon N$, we obtain

$$(5) \qquad\qquad |\alpha - \xi| \leq b^{-r-s-\varepsilon N}.$$

This is not sufficient to get a contradiction with Roth's or Ridout's theorems, but, as we shall see, the Subspace Theorem will do the job.

Rewrite (5) as

$$(6) \qquad\qquad \left| b^{r+s}\alpha - b^r\alpha - M \right| \leq b^{-\varepsilon N}.$$

Now it is the time to define the data for the Subspace Theorem: the set S of prime numbers and the linear forms $L_{i,p}$. Let S consist of the infinite prime and all the prime divisors of b. Further, for $p \in S$ we define the linear forms $L_{1,p}$, $L_{2,p}$ and $L_{3,p}$ in variables $\mathbf{x} = (x_1, x_2, x_3)$ as follows. For $p = \infty$ we put

$$L_{1,\infty}(\mathbf{x}) = x_1, \qquad L_{2,\infty}(\mathbf{x}) = x_2, \qquad L_{3,\infty}(\mathbf{x}) = \alpha x_1 - \alpha x_2 - x_3.$$

And for $p < \infty$ we put $L_{i,p}(\mathbf{x}) = x_i$ for $i = 1, 2, 3$.

We put $\mathbf{x} = (b^{r+s}, b^s, M)$. Since $\xi \in (0, 1)$, we have $|M| \leq b^{r+s}$. Thus,

$$(7) \qquad\qquad \|\mathbf{x}\| \leq b^{r+s} \leq b^N.$$

Now we have

$$\prod_{p \in S} \prod_{i=1}^{3} |L_{i,p}(\mathbf{x})|_p = \prod_{p \in S} |b^r|_p \prod_{p \in S} |b^{r+s}|_p \prod_{\substack{p \in S \\ p \neq \infty}} |M|_p \left| b^{r+s}\alpha - b^r\alpha - M \right|_\infty.$$

By our definition of S and the product formula we have $\prod_{p \in S} |b|_p = 1$. Further, since $M \in \mathbb{Z}$, we have $|M|_p \leq 1$ for each $p \neq \infty$. It follows that

$$(8) \qquad \prod_{p \in S} \prod_{i=1}^{3} |L_{i,p}(\mathbf{x})|_p \leq \left| b^{r+s}\alpha - b^r\alpha - M \right|_\infty \leq b^{-\varepsilon N} \leq \|\mathbf{x}\|^{-\varepsilon}.$$

(We used (6) and (7).)

We can repeat this argument for infinitely many N and find vectors $\mathbf{x} = \mathbf{x}(N)$ satisfying (8). Moreover, recall that $s(N) \geq \varepsilon N$, whence $s(N) \to \infty$ as $N \to \infty$, which means that among the vectors $\mathbf{x} = \mathbf{x}(N)$ infinitely many are distinct. Theorem 2.3 implies that these vectors $\mathbf{x}(N)$ lie on finitely many planes of the space $\mathbb{Q}^3$. Hence infinitely many of them lie on the same plane; that is, there exist $\lambda, \mu, \nu \in \mathbb{Q}$, not all 0 such that for infinitely many N we have

$$(9) \qquad\qquad \lambda b^{r(N)} + \mu b^{r(N)+s(N)} + \nu M(N) = 0.$$

Moreover, $\nu \neq 0$ because $s(N) \to \infty$. Dividing (9) by $b^{r(N)} \left(b^{s(N)} - 1 \right)$, we obtain

$$\frac{\lambda}{b^{s(N)} - 1} + \mu \frac{b^{s(N)}}{b^{s(N)} - 1} + \nu \xi(N) = 0.$$

Sending N to infinity, we conclude that $\mu + \nu \alpha = 0$, whence $\alpha \in \mathbb{Q}$. The theorem is proved. $\square$

As the reader could have noticed, it is quite irrelevant for the proof that the "digits" $u_1, u_2, \ldots$ belong to the set $\{0, 1, \ldots, b - 1\}$. In fact, any finite set of rational, or even algebraic numbers, would do. Also, b is not obliged to be a rational integer; one can assume it to be any Pisot or Salem number [4]. Thus, the result of Adamczewski and Bugeaud in the most general form sounds as follows: let $u_1, u_2, \ldots$ be a sequence of algebraic numbers with finitely many distinct terms, and with long repetitions, and let β be a Pisot or Salem number; then either $\alpha = u_1 \beta^{-1} + u_2 \beta^{-2} + \ldots$ belongs to the number field generated by β and by the "digits" $u_1, u_2, \ldots$, or α is transcendental.

In [1, 3] Adamczewski and Bugeaud exploit a different notion of complexity, based on continued fractions rather than b-ary expansions, and obtain several results in the same spirit.

The reader may consult Waldschmidt's survey [70] for more information on the Diophantine analysis of symbolic sequences.

Remark in conclusion that Adamczewski and Bugeaud were not the first to apply the Subspace Theorem in the transcendence; in [48, 15, 65, 21] it was used to prove transcendence of certain infinite sums. The argument of Troi and Zannier [65] is quite similar to that of Adamczewski and Bugeaud. See also [30] for a more recent application.

4. DIOPHANTINE EQUATIONS WITH POWER SUMS

In 1984 M. Laurent [42] applied the Subspace Theorem to study the solutions $\mathbf{x} = (x_1, \ldots, x_r) \in \mathbb{Z}^r$ of a polynomial-exponential equation

$$(10) \qquad\qquad \sum_{i=1}^{N} P_i(\mathbf{x}) \mathbf{a}_i^{\mathbf{x}} = 0,$$

where $P_1, \ldots, P_N \in \bar{\mathbb{Q}}[\mathbf{x}]$, $\mathbf{a}_1, \ldots, \mathbf{a}_N \in \bar{\mathbb{Q}}^r$ and $\mathbf{a}^{\mathbf{x}} := a_1^{x_1} \cdots a_r^{x_r}$. (Using a specialization argument, one can replace $\bar{\mathbb{Q}}$ by any field of characteristic 0.) His results imply, in particular, that, under certain natural condition, the following holds: with

---

[4] A real algebraic number $\beta > 1$ is called *Pisot number* if all its conjugates (except β itself) lie inside the unit disk of the complex plane; it is called *Salem number* if they lie inside or on the boundary of the unit disk.

finitely many exceptions, every solution of (10) is also a solution of a "strictly shorter" equation $\sum_{i \in I} P_i(\mathbf{x}) \mathbf{a}_i^{\mathbf{x}} = 0$, where I is a proper subset of $\{1, \ldots, N\}$. The above mentioned condition is the following: the only $\mathbf{x} \in \mathbb{Z}^r$ satisfying $\mathbf{a}_i^{\mathbf{x}} = \mathbf{a}_j^{\mathbf{x}}$ for all i, j is $\mathbf{x} = (0, \ldots, 0)$.

While the theorem of Laurent does not (and cannot) imply ultimate finiteness in general, it allows one to establish it in many special cases, usually by induction in N and/or elimination.

However, there are interesting polynomial-exponential equations for which the theorem of Laurent does not yield anything non-trivial. One of the simplest is $a^n + b^n = P(x)$ in $x, n \in \mathbb{Z}$, where P is a polynomial. (The equation $a^n = P(x)$ can be analyzed, for instance, by Baker's method.) For this equation $r = 2$ and the vectors $\mathbf{a}_i$ are $(a, 1)$, $(b, 1)$ and $(1, 1)$. For any such $\mathbf{a}_i$ and for any $\mathbf{x} = (0, x)$ we have $\mathbf{a}_i^{\mathbf{x}} = (1, 1)$, so that Laurent's condition is not satisfied.

Corvaja and Zannier studied these and more general equations in the important and largely underestimated article [**19**], as well as in the later article [**21**]. Let us introduce some terminology. Call *power sum* an expression of the form

$$(11) \qquad\qquad u(n) = b_1 a_1^n + \cdots + b_m a_m^n,$$

where $a_1, \ldots, a_m$ (the *roots*) and $b_1, \ldots, b_m$ (the *coefficients*) are complex numbers. Power sums can be viewed as a particular case of *linear recurrence sequences*

$$u(n) = b_1(n) a_1^n + \cdots + b_m(n) a_m^n,$$

where $b_1(n), \ldots, b_m(n)$ are polynomials in n; one may say that *power sums are linear recurrences with simple roots*.

If the roots and the coefficients belong to a ring A, then we call (11) an *A-power sum*, or a *power sum over A*.

Let $P(x, y) \in \mathbb{Q}[x, y]$ be an irreducible polynomial with $\deg_y P \geq 2$. Corvaja and Zannier studied the equation $P(u(n), y) = 0$, where u is a power sum. They were motivated by a question of Yasumoto about *universal Hilbert sets*, that is, sets A of rational integers with the following property:

(UHS)   for any irreducible (over $\mathbb{Q}$) polynomial $P(x, y) \in \mathbb{Q}[x, y]$, the specialized polynomial $P(a, y) \in \mathbb{Q}[y]$ is irreducible for all but finitely many $a \in A$.

Informally, a universal Hilbert set proves the Hilbert irreducibility theorem for every polynomial, and with finitely many exceptions.

A well-known elementary Galois-theoretic argument (see, for instance, [**8**, Section 2]) implies that A is a universal Hilbert set if and only if it has the following formally weaker property:

(UHS′)   for any absolutely irreducible $P(x, y) \in \mathbb{Q}[x, y]$ with $\deg_y P \geq 2$ the equation $P(a, y) = 0$ has only finitely many solutions (a, y) with $a \in A$ and $y \in \mathbb{Q}$.

Existence of universal Hilbert sets was shown by Gilmore and Robinson [**37**], and the first explicit example was suggested by Sprindzhuk [**63**] (see [**8, 32, 71, 72**] for further examples). Yasumoto [**71**] asked whether $\{2^n + 3^n\}$ is a universal Hilbert set. Dèbes and Zannier [**32**] managed to prove, using the theorem of Ridout, that $\{2^n + 5^n\}$ is a universal Hilbert set, but their argument fails for $\{2^n + 3^n\}$. In [**19**] this problem is solved, and even a much stronger result is obtained: values of any power sum $b_1 a_1^n + \cdots + b_m a_m^n$ with multiplicatively independent $a_1, \ldots, a_m$ form a universal Hilbert set (with $m \geq 2$ and $b_1, \ldots, b_m \neq 0$).

Another motivation for [**19**] was the celebrated problem of Pisot. A power series $f(t) = \sum_{n=0}^{\infty} u(n) t^n$ is called the *Hadamard q-th power* of the series $g(t) = \sum_{n=0}^{\infty} v(n) t^n$ if $u(n) = v(n)^q$ for $n = 0, 1, \ldots$; in this case the latter series is called an *Hadamard q-th root* of the former.

Let $f(t)$ be a rational power series (that is, a power series expansion of a rational function in t) with coefficients in $\mathbb{Q}$, and let q be a positive integer. Assume that $f(t)$ is the Hadamard q-th power of another series with coefficients in $\mathbb{Q}$. Pisot conjectured that in this case $f(t)$ is the Hadamard q-th power of another *rational* power series (with coefficients in $\mathbb{Q}$).

Since $f(t) = \sum_{n=0}^{\infty} u(n) t^n$ is a rational power series if and only if the coefficients $u(n)$ form a linear recurrence sequence, Pisot's conjecture can be stated as follows: assume that $\{u(n)\}$ is a linear recurrence sequence of rational numbers, such that every $u(n)$ is a q-th power in $\mathbb{Q}$; then $u(n) = v(n)^q$ for all n, where $v(n)$ is another linear recurrence sequence of rational numbers.

Zannier [**73**] proved Pisot's conjecture by a method independent of the Subspace Theorem. Now, let us ask a more difficult question: assume that

(12) $u(n)$ is a q-th power in $\mathbb{Q}$ for *infinitely many n*;

what can one say about the linear recurrence u? Since the work of Corvaja and Zannier applies to the particular equation $u(n) - y^q = 0$, it answers this question in the special case when u is a power sum (over $\mathbb{Q}$). It turns out that, while u itself is not obliged to be a q-th power of another $\mathbb{Q}$-power sum, this is true for the power sum obtained from u by letting n run through an arithmetical progression (see Corollary 4.2).

Below, we give a complete proof of this particular case of the theorem of Corvaja and Zannier. We shall also state the general theorem and sketch its proof.

4.1. Refined Pisot's Conjecture for Power Sums

The main result of Corvaja and Zannier concerns $\mathbb{Q}$-power sums with *positive* roots. For these power sums (12) implies that u is a q-th power of another power sum, but over $\overline{\mathbb{Q}}$. More precisely, we have the following.

THEOREM 4.1 (Corvaja, Zannier). — *Let u be a $\mathbb{Q}$-power sum with positive roots, and let q be a positive integer. Assume that $u(n)$ is a q-th power for infinitely many $n \in \mathbb{Z}$. Then $u(n) = a^{n+r}v(n)^q$ for all $n \in \mathbb{Z}$, where a is a non-zero rational number, r is an integer and v is a $\mathbb{Q}$-power sum. In particular, u is a q-th power of $\bar{\mathbb{Q}}$-power sum.*

COROLLARY 4.2. — *Let u be a $\mathbb{Q}$-power sum, and let q be a positive integer. Assume that $u(n)$ is a q-th power for infinitely many $n \in \mathbb{Z}$. Then there exist positive integers Q and R and a $\mathbb{Q}$-power sum w such that $u(Qn + R) = w(n)^q$ for all $n \in \mathbb{Z}$.*

In other words, though u itself is not necessarily a q-th power of a $\mathbb{Q}$-power sum, the power sum obtained from u by letting n run through a certain arithmetical progression is.

If u has positive roots then the corollary is immediate, with $Q = q$. In the general case one should consider the power sums $u(2n)$ and $u(2n + 1)$, both having positive roots, and the corollary follows with $Q = 2q$.

PROOF OF THEOREM 4.1. — We may assume that $u(n)$ is a q-th power for infinitely many *positive* integers n, replacing $u(n)$ by $u(-n)$, if necessary.

Write $u(n) = b_0 a_0^n + \cdots + b_m a_m^n$, where the roots $a_0, \ldots, a_m$ are positive rational numbers written in the decreasing order, so that $a_0 > a_1 > \cdots > a_m > 0$.

Assume first that $a_0 = 1$. Putting $b = b_0$ and $c_k = b_k/b$, we write

$$u(n) = b(1 + z(n))$$

with $z(n) = c_1 a_1^n + \cdots + c_m a_m^n$. Since the roots of the power sum z are strictly smaller than 1, we have [5] $|z(n)| \ll \theta^n$ for some $\theta \in (0, 1)$. Since $u(n)$ is infinitely often a rational q-th power, we have $b > 0$ when q is even. We may assume that $b > 0$ when q is odd as well, replacing u by $-u$, if necessary. Thus, for big positive n we have $u(n) > 0$, which implies that $u(n)$ has exactly one positive q-th root; we denote it by $y(n)$. For sufficiently large n we can express $y(n)$ using the binomial power series:

$$(13) \qquad y(n) = b^{1/q} \sum_{\ell=0}^{\Lambda-1} \binom{1/q}{\ell} z(n)^\ell + O(\theta^{n\Lambda}),$$

where the parameter Λ will be specified later.

The sum in (13) can be expressed as $\beta_1 \alpha_1^n + \cdots + \beta_\mu \alpha_\mu^n$, where $\alpha_1, \ldots, \alpha_\mu$ are pairwise distinct. Since $\alpha_1, \ldots, \alpha_\mu$ are multiplicative combinations of $a_1, \ldots, a_m$, they

---

[5] In this proof "$\ll$", "$\gg$" and $O(\cdot)$ imply constants depending on the power sum u and on the parameter Λ defined below, but independent of n.

are positive rational numbers. Thus, we have

$$\left| y(n) - b^{1/q} \sum_{k=1}^{\mu} \beta_k \alpha_k^n \right| \ll \theta^{n\Lambda}.$$

Now we are in a position to apply the Subspace Theorem. We let S to be a finite set of prime numbers, including the infinite prime, such that the numbers $a_1, \ldots, a_m$ are S-units, and $b_0, \ldots, b_m$ are S-integers. Then $u(n)$ is an S-integer for every n, and so is $y(n) = u(n)^{1/q}$ (as soon as $y(n) \in \mathbb{Q}$). Also, the numbers $\alpha_1, \ldots, \alpha_\mu$ are S-units, being multiplicative combinations of $a_1, \ldots, a_m$.

Next, for every $p \in S$ we define $\mu + 1$ independent linear forms in $\mu + 1$ variables as follows. For $p = \infty$ we put

$$L_{0,\infty}(\mathbf{x}) = x_0 - b^{1/q} \sum_{k=1}^{\mu} \beta_k x_k, \qquad L_{k,\infty}(\mathbf{x}) = x_k \quad (k = 1, \ldots, \mu).$$

And for a finite $p \in S$ we put $L_k(\mathbf{x}) = x_k$ for $k = 0, \ldots, \mu$.

Now let n be such that $y(n) \in \mathbb{Q}$. Then $\mathbf{x} = \mathbf{x}(n) = \big(y(n), \alpha_1^n, \ldots, \alpha_\mu^n\big)$ is a vector with S-integer coordinates. We have

(14)
$$\prod_{p \in S} \prod_{k=0}^{r} |L_{k,p}(\mathbf{x})|_p = \left| y(n) - b^{1/q} \sum_{k=1}^{\mu} \beta_k \alpha_k^n \right| \prod_{\substack{p \in S \\ p \neq \infty}} |y(n)|_p \prod_{k=1}^{r} \prod_{p \in S} |\alpha_k^n|_p \ll \theta^{\Lambda n} H(y(n)).$$

Indeed, the product formula implies that $\prod_{p \in S} |\alpha_k|_p = 1$ (because the numbers α_k are S-units), which means that the double product is 1. Also, the first product is bounded by $H(y(n))$, because $y(n)$ is an S-integer.

An obvious calculation shows that the height of the rational number $u(n)$ is $e^{O(n)}$. Since $y(n)^q = u(n)$, we have $H(y(n)) = H(u(n))^{1/q} = e^{O(n)}$. It follows that the right-hand side of (14) is bounded by $C^n \theta^{\Lambda n}$, where the constant C depends only on the power sum u.

Now specify the parameter Λ to have $C\theta^\Lambda \leq 1/2$. We obtain

$$\prod_{p \in S} \prod_{k=0}^{r} |L_{k,p}(\mathbf{x})|_p \ll 2^{-n}.$$

A routine estimate gives $H(\mathbf{x}) \leq e^{O(n)}$. We finally obtain

(15)
$$\prod_{p \in S} \prod_{k=0}^{r} |L_{k,p}(\mathbf{x})|_p < H(\mathbf{x})^{-\varepsilon}$$

with some $\varepsilon > 0$ (depending only on u).

By the assumption, there exist infinitely many positive integers n such that $y(n) \in \mathbb{Q}$. Hence (15) has infinitely many solutions in S-integer vectors $\mathbf{x} = \mathbf{x}(n)$. By Theorem 2.3′, all these solutions belong to finitely many proper subspaces of $\mathbb{Q}^{\mu+1}$.

It follows that infinitely many vectors $\mathbf{x}(n)$ belong to the same proper subspace. In other words, there exist rational numbers $\gamma_0, \ldots, \gamma_\mu$, not all 0, such that

$$\gamma_0 y(n) = b^{1/q} \left(\gamma_1 \alpha_1^n + \cdots + \gamma_\mu \alpha_\mu^n \right).$$

If $\gamma_0 = 0$ then $\gamma_1 \alpha_1^n + \cdots + \gamma_\mu \alpha_\mu^n$ would vanish for infinitely many n, which is impossible because $\alpha_1, \ldots, \alpha_\mu$ are pairwise distinct positive numbers. Thus, $\gamma_0 \neq 0$, and we may assume that $\gamma_0 = 1$.

We have shown that for infinitely many n we have $y(n) \in \mathbb{Q}$ and

$$y(n) = b^{1/q} \left(\gamma_1 \alpha_1^n + \cdots + \gamma_\mu \alpha_\mu^n \right).$$

Since $\gamma_1 \alpha_1^n + \cdots + \gamma_\mu \alpha_\mu^n \neq 0$ for large n, we have

$$b^{1/q} = \frac{y(n)}{\gamma_1 \alpha_1^n + \cdots + \gamma_\mu \alpha_\mu^n} \in \mathbb{Q}.$$

Thus, for infinitely many n we have $y(n) = v(n)$, where v is a $\mathbb{Q}$-power sum with positive roots. Since $u(n) - v(n)^q$ is a power sum with positive roots as well, it can vanish infinitely often only if it vanishes identically. Thus, $u(n) = v(n)^q$. This proves the theorem in the special case $a_0 = 1$.

The general case easily reduces to the special one. For some r there exist infinitely many positive integers n, congruent to $-r$ modulo q such that $u(n)$ is a q-th power in $\mathbb{Q}$. Replacing $u(n)$ by $a_0^{-n-r} u(n)$, we reduce the general case to the case $a_0 = 1$, already treated. $\qquad\square$

4.2. The General Equation

And here is the general theorem of Corvaja and Zannier.

THEOREM 4.3 (Corvaja, Zannier [**21**]). — *Let u be a $\mathbb{Q}$-power sum with positive roots, let S be a finite set of primes including the infinite prime, and let $P(x, y) \in \mathbb{Q}[x, y]$ be a polynomial non-constant in y. Assume that the equation $P(u(n), y) = 0$ has infinitely many solutions in integers n and S-integers y. Then there exists a $\bar{\mathbb{Q}}$-power sum v with positive real coefficients such that $P(u(n), v(n)) = 0$ for all $n \in \mathbb{Z}$.*

PROOF (a sketch). — As above, we may assume that there are infinitely many solutions with positive n. When $n \to +\infty$ we have $u(n) \to b \in \mathbb{Q} \cup \{-\infty, +\infty\}$. Replacing $u(n)$ by $-u(n)$ we may exclude the $-\infty$, and upon replacing $u(n)$ by $u(n) - b$ we may assume that in the finite case the limit is 0. Thus, $\lim\limits_{n \to +\infty} u(n) \in \{0, +\infty\}$.

Assume that $\lim_{n \to +\infty} u(n) = 0$. Then [6] $u(n) \ll \theta^n$ with some $\theta \in (0,1)$. By the assumption, for infinitely many positive integers n there exists an S-integer $y(n)$ such that $P(u(n), y(n)) = 0$. Let

$$(16) \qquad Y_i(x) = \sum_{k=-\kappa_i}^{\infty} c_{ki} x^{k/e_i} \qquad (i = 1, \dots, \deg_y P)$$

be the Puiseux expansion of the algebraic function y at 0, the coefficients c_{ki} being algebraic numbers. Since $u(n) \to 0$, for large n all the series (16) converge at $x = u(n)$, and one of the sums $Y_i(u(n))$ is $y(n)$. We fix i for which $Y_i(u(n)) = y(n)$ infinitely often, and omit the index i in the sequel. Thus, for infinitely many positive integers n we have

$$y(n) = \sum_{k=-\kappa}^{\infty} c_k u(n)^{k/e}.$$

Truncating the series, we find

$$y(n) = \sum_{k=-\kappa}^{\Lambda e - 1} c_k u(n)^{k/e} + O(\theta^{\Lambda n}).$$

Now write $u(n) = ba^n(1 + z(n))$, where a is the biggest root of u. Redefining θ, we may assume that $z(n) \ll \theta^n$ for positive n. Replacing each $u(n)^{k/e}$ by

$$b^{1/e} a^{n/e} \sum_{j=0}^{\Lambda - 1} \binom{k/e}{j} z(n)^j + O(\theta^{\Lambda n}),$$

we obtain $y(n) = \beta_1 \alpha_1^n + \cdots + \beta_\mu \alpha_\mu^n + O(\theta^{\Lambda n})$, where $\alpha_1, \dots, \alpha_\mu$ are positive real algebraic numbers, and $\beta_1, \dots, \beta_\mu$ are algebraic numbers.

Now applying the Subspace Theorem in the same way as we did in the proof of Theorem 4.1, we find that $y(n) = v(n)$ for infinitely many n, where v is a $\bar{\mathbb{Q}}$-power sum with positive real roots. Then $P(u(n), v(n))$ is a $\bar{\mathbb{Q}}$-power sum with positive real roots, which vanishes at infinitely many n. Hence it vanishes identically.

The case $u(n) \to +\infty$ is treated similarly, the Puiseux expansions at zero being replaced by those at infinity.   □

Among other consequences of this theorem, we have the following result mentioned above.

COROLLARY 4.4 (Corvaja, Zannier). — *Let $u(n) = b_1 a_1^n + \cdots + b_m a_m^n$ be a $\mathbb{Q}$-power sum. Assume that $m \geq 2$ and that the roots $a_1, \dots, a_m$ are multiplicatively independent. Then $\{u(n)\}$ is a universal Hilbert set.*

---

[6] Here implicit constants may depend on the power sum u, the polynomial $P(x, y)$ and the parameter Λ defined below, but not on n.

To prove the corollary, we need a purely algebraic lemma. Let K be a field of characteristic 0 and let Γ be a multiplicatively written torsion-free abelian group. Then the group ring $K[\Gamma]$ is an integral domain.

LEMMA 4.5. — *In the ring $K[\Gamma]$ consider an element $u = b_1\gamma_1 + \cdots + b_m\gamma_m$, where $b_1, \ldots, b_m \in K^*$ and $\gamma_1, \ldots, \gamma_m$ are multiplicatively independent elements of Γ. Assume that $m \geq 2$. Then the ring $K[u]$ is integrally closed in $K[\Gamma]$.*

Since this the lemma has nothing to do with our main subject, we prove it in the addendum to this section.

PROOF OF COROLLARY 4.4. — We apply the lemma with $K = \mathbb{C}$ and with Γ consisting of the functions $\mathbb{Z} \to \mathbb{R}$ defined by $n \mapsto a^n$ with a positive real a. Then $\mathbb{C}[\Gamma]$ is exactly the ring of power sums with complex coefficients and positive real roots.

Now let $u(n) = b_1 a_1^n + \cdots + b_m a_m^n$ be as in the corollary. We may assume that the roots $a_1, \ldots, a_m$ are positive, considering separately $u(2n)$ and $u(2n+1)$. By the lemma, the ring $\mathbb{C}[u]$ is integrally closed in $\mathbb{C}[\Gamma]$.

If $\{u(n)\}$ is not a universal Hilbert set then there exists a $\mathbb{Q}$-irreducible polynomial $P(x, y) \in \mathbb{Q}[x, y]$ with $\deg_y P \geq 2$ such that $P(u(n), y) = 0$ has infinitely many solutions in $n \in \mathbb{Z}$ and $y \in \mathbb{Q}$. We may assume the polynomial P absolutely irreducible [7] and monic [8] in y. Since P is monic, there exists a finite set of primes S such that for all solutions (n, y) as above, the number y is an S-integer. Applying Theorem 4.3, we find a power sum v with positive real roots such that $P(u(n), v(n)) = 0$. Since the polynomial $P(x, y)$ is absolutely irreducible, y-monic and of y-degree at least 2, the ring $\mathbb{C}[u, v]$ is a non-trivial integral extension of $\mathbb{C}[u]$. Hence $\mathbb{C}[u]$ is not integrally closed in $\mathbb{C}[\Gamma]$, a contradiction.   □

In fact, Corvaja and Zannier prove more. For instance, using Siegel's theorem (see Section 5), they show [9] the following: *in the set-up of Theorem 4.3 assume that P is $\mathbb{Q}$-irreducible and $\deg_y P \geq 2$; then either $u = f(v)$, where v is another power sum and f is a polynomial of degree at least 2, or the roots of u generate a cyclic multiplicative group (that is $u(n) = b_1 a^{\nu_1 n} + \cdots + b_m a^{\nu_m n}$ with some $a \in \mathbb{Q}^*$ and $\nu_1, \ldots, \nu_m \in \mathbb{Z}$).* This implies further examples of universal Hilbert power sums, like $2^n + 3^n + 6^n$, etc.

To conclude, we briefly discuss power sums over number fields. Theorems 4.1 and 4.3 stay true, with almost the same proof, if the assumption *the roots of u are positive* is replaced by *the roots of u generate a torsion-free multiplicative abelian*

---

[7] It is well-known and easy to show that if $P(x, y)$ is $\mathbb{Q}$-irreducible but $\mathbb{C}$-reducible then the equation $P(x, y) = 0$ can have only finitely many solutions in $x, y \in \mathbb{Q}$.

[8] Replace $P(x, y) = a_q(x)y^q + \cdots + a_1(x)y + 1$ by $a_q(x)^{q-1}P(x, y/a_q(x))$.

[9] In [19] they consider only power sums with integer roots, but the argument extends to rational roots without trouble.

group. One may attempt to extend Theorems 4.1 and 4.3, with this more general assumption, to K-power sums, with an arbitrary number field K. Unfortunately, this is done only under a certain technical assumption about our power sum. We say that a K-power sum u has an *upper* (respectively, *lower*) *dominant root* if there exists a root a of u and an absolute value $v \in M_K$ such that $|a|_v > |a'|_v$ (respectively, $|a|_v < |a'|_v$) for any other root a'.

Now let u be a K-power sum satisfying the following two conditions: *the roots of u generate a torsion-free multiplicative abelian group,* and *u has both an upper dominant root and a lower dominant root.* Then u satisfies both the analogues of Theorems 4.1 and 4.3 with $\mathbb{Q}$ replaced by K (with very similar proofs).

The existence of a "dominant root" is immediate [10] if the field K has at least one real embedding, but it may fail already for $K = \mathbb{Q}(i)$: the power sum

$$u(n) = (8+i)^n + (8-i)^n + (2+i)^n + (2-i)^n$$

has no upper dominant root.

Suppressing the "dominant root" assumption looks a difficult problem. It seems that at least one cardinal new idea is needed to handle power sums without dominant roots. See, however, [**20**].

Addendum: Proof of Lemma 4.5

We may assume that Γ is a division group; moreover, since it is torsion-free, every $\gamma \in \Gamma$ has a well-defined "n-th root" $\gamma^{1/n}$ for any non-zero integer n. It suffices to prove that $K[u]$ is integrally closed in the ring $K[\Delta]$, for any finitely generated subgroup Δ of Γ, containing $\gamma_1, \ldots, \gamma_m$. Replacing Δ by a bigger finitely generated subgroup, we may assume that it has a free $\mathbb{Z}$-basis consisting of $\gamma_1^{1/n}, \ldots, \gamma_m^{1/n}$ (with some positive integer n) and, perhaps, several more elements of Γ.

We have reduced the lemma to the following statement.

PROPOSITION 4.6. — *Let $R = K[x_1, \ldots, x_r]$ be the polynomial ring over a field K (of characteristic 0) and let n be a positive integer. Consider $u = b_1 x_1^n + \cdots + b_m x_m^n \in R$, where $2 \le m \le r$ and $b_1, \ldots, b_m \in K^*$. Then $K[u]$ is integrally closed in R.*

PROOF. — We may assume that K is algebraically closed and, by a linear change of variables we may assume that $b_1 = \cdots = b_m = 1$, so that $u = x_1^n + \cdots + x_m^n$. Let $\mathcal{O}$ be the integral closure of $K[u]$ in R. We want to prove that $\mathcal{O} = K[u]$.

The quotient field of $\mathcal{O}$ is contained in the purely transcendental field $K(x_1, \ldots, x_r)$. By the theorem of Luroth (see Remark 4.7) it itself must be purely transcendental. Thus, we may write this quotient field as $K(v)$, and the generator v may be chosen in the ring $\mathcal{O}$. We have $u = P(v)$, where, a priori, $P(X)$ is a rational function over K.

---

[10] Provided the roots generate a torsion-free abelian group.

Since both u and v are polynomials in $x_1, \ldots, x_r$, the rational function $P(X)$ must be a polynomial.

Specializing $x_1 = t$, $x_2 = \cdots = x_r = 0$, we obtain $t^n = P(Q(t))$, where $Q(t)$ is a polynomial over K. It follows that $P(X) = aX^\nu$ for some positive integer ν and some $a \in K^*$. Specializing $x_1 = t$, $x_2 = 1$, $x_3 = \cdots = x_r = 0$ (it is here where we use the assumption $m \geq 2$), we conclude that $t^n + 1$ is a ν-th power of yet another polynomial in t, which is possible only if $\nu = 1$. Thus, $u = av$, which proves the proposition. $\qquad\square$

REMARK 4.7. — We use here a slightly non-traditional form of Luroth's theorem: if $K \subset L \subset \Omega$ is a tower of fields of characteristic 0, with K algebraically closed, Ω purely transcendental over K and L of transcendence degree 1 over K, then L is purely transcendental. In standard textbooks one usually assumes that Ω is of transcendence degree 1 as well.

However, our "more general" version of Luroth's theorem easily follows from the traditional one. Indeed, geometrically, the "traditional" version means the following: if an algebraic curve C admits a non-constant rational dominant map $\mathbb{P}^1 \to C$, then it is isomorphic to $\mathbb{P}^1$. And in our version $\mathbb{P}^1$ should be replaced by $\mathbb{P}^r$. But if a curve admits a non-constant dominant map from a projective space, then it also admits one from the projective line.

5. INTEGRAL POINTS

5.1. Integral Points on Curves

It is well-known that a binary Diophantine equation $P(x, y) = 0$ of degree 1 or 2 has infinitely many solutions in integers unless it has an "obvious" reason (local obstruction) for having finitely many. Siegel proved [**62**], relying on the already mentioned work of A. Thue [**64**], that an equation of degree 3 or higher must have finitely many solutions, unless it has an "obvious" reason to have infinitely many (reduces to a linear or quadratic equation by a variable change).

Precisely speaking, Siegel proved that an irreducible equation $P(x, y) = 0$ (where $P(x, y) \in \mathbb{Q}[x, y]$) has at most finitely many solutions $x, y \in \mathbb{Z}$ if one of the following conditions is satisfied:

  – the genus of the plane curve $P(x, y) = 0$ is at least 1, or
  – this curve has at least 3 points at infinity.

More generally, let $\bar{C}$ be an absolutely irreducible projective curve defined over a number field K and let C be an affine subset of $\bar{C}$ embedded into the affine space $\mathbb{A}^\nu$. Further, let S be a finite set of absolute values of K, including all archimedean absolute values, and let $\mathcal{O}_S$ be the ring of S-integers of K. Again, Siegel's theorem (in the more general form due to Mahler and Lang) asserts that C has at most finitely many points in $\mathbb{A}^\nu(\mathcal{O}_S)$ if $\mathbf{g}(\bar{C}) \geq 1$ or if $\left| \bar{C} \setminus C \right| \geq 3$.

Of course, one should mention the celebrated result of Faltings, who proved that the set of rational points on a projective curve of genus 2 or higher is finite. We do not discuss Faltings' work here.

The conventional proof of Siegel's theorem, as in [**41**, Chapter 8] or [**40**, Section D.9], relies on the Theorem of Roth [11] and heavily depends on the existence of the Jacobian embedding $\bar{C} \hookrightarrow J(\bar{C})$, because it exploits high degree étale coverings of $\bar{C}$.

Recently Corvaja and Zannier [**22**] suggested a beautiful new proof, based on the Subspace Theorem rather than the Theorem of Roth, and using projective rather than Jacobian embeddings.

Corvaja and Zannier prove the following theorem.

THEOREM 5.1. — *In the above set-up assume that $\left|\bar{C} \setminus C\right| \geq 3$. Then C has at most finitely many points in $\mathbb{A}^\nu(\mathcal{O}_S)$.*

Siegel's theorem easily follows from Theorem 5.1. Indeed, if $\mathbf{g}(\bar{C}) \geq 1$ then there is an étale covering $\bar{C}' \to \bar{C}$ of degree 3. It induces the covering of affine curves $C' \to C$, and we have $\left|\bar{C}' \setminus C'\right| \geq 3$.

By the Chevalley-Weil principle, the set $\bar{C}(K)$ is covered by $\bar{C}'(K')$, where K' is a number field. Theorem 5.1 implies that the set of $\mathcal{O}_{S'}$-integral points on C' is finite (where S' is the extension of S to K'). Hence so is the set of S-integral points on C.

Existence of the covering $\bar{C}' \to \bar{C}$ of degree 3 is the only point in the new proof of Siegel's theorem which appeals to the Jacobian embedding: as we shall see, the proof of Theorem 5.1 is free of Jacobians.

PROOF OF THEOREM 5.1. — Write $\bar{C} \setminus C = \{Q_1, \ldots, Q_r\}$, where, by the assumption, $r \geq 3$. Extending the field K, we may assume that each of the points $Q_1, \ldots, Q_r$ is defined over K. Further, let $D = Q_1 + \cdots + Q_r$ be the "divisor at infinity".

Let n be a (big) positive integer, to be specified later. By the Riemann-Roch theorem, the dimension $\ell = \ell(nD)$ of the vector space

$$\mathcal{L} = \mathcal{L}(nD) = \{y \in K(C) : (y) + nD \geq 0\}$$

is given by $\ell = nr - O(1)$. In particular, for big n we have $\ell \sim nr$.

Pick a basis $y_1, \ldots, y_\ell$ of $\mathcal{L}$. Every y_j is integral over the ring $K[\mathbf{x}] = K[x_1, \ldots, x_\nu]$, where $x_1, \ldots, x_\nu$ are the coordinate functions on the affine curve $C \subset \mathbb{A}^\nu$. Multiplying each by a suitable non-zero constant, we may assume that they are integral over the ring $\mathcal{O}_S[\mathbf{x}]$. It follows that for every S-integral point P we have $y_j(P) \in \mathcal{O}_S$.

Now assume that there exist infinitely many distinct S-integral points $P_1, P_2, P_3, \ldots$. Since $\bar{C}$ is a projective curve, the set $\bar{C}(K_v)$ is compact in the v-adic topology for

_____

[11] At the time of Siegel Roth's theorem was not available, and Siegel had to use a weaker statement.

every v. Hence, replacing the sequence (P_i) by a suitable subsequence, we may assume that it converges in v-adic topology for every $v \in S$, and we denote by Q_v the corresponding limits. Now we partition our set S as $S = S' \cup S''$, letting S' consist of $v \in S$ such that $Q_v \in \bar{C} \setminus C$ and S'' of those v for which $Q_v \in C$.

We wish to estimate $|y_j(P_i)|_v$ for $i = 1, 2, \ldots$ and $v \in S$. For $v \in S''$ it is obvious that $|y_j(P_i)|_v$ are bounded independently of k. For $v \in S'$ fix a local parameter t_v at Q_v. Then $|y_j(P_i)|_v \ll |t_v(P_i)|_v^{-n}$, where here and below implicit constants are independent of i. Thus, for $\mathbf{y} = (y_1, \ldots, y_\ell)$ we obtain

$$\|\mathbf{y}(P_i)\|_v \ll \begin{cases} |t_v(P_i)|_v^{-n}, & \text{if } v \in S' \\ 1, & \text{if } v \in S''. \end{cases}$$

Since the numbers $y_j(P_i)$ are S-integers, we obtain

$$(17) \qquad H(\mathbf{y}(P_i)) = \prod_{v \in S} \|\mathbf{y}(P_i)\|_v \ll \prod_{v \in S'} |t_v(P_i)|_v^{-n}.$$

All this was just a preparation, and now we are coming to the heart of the Corvaja-Zannier argument. Fix $v \in S'$. If $z \in \mathcal{L}$ vanishes at Q_v, then $|z(P_i)|_v$ becomes "very small" as P_i approaches Q_v, which gives rise to v-adically small linear form. Since the vector space $\mathcal{L}$ contains "many" such z, we have many independent v-adically small linear forms. This would allow us to use the Subspace Theorem.

More specifically, elementary linear algebra shows that our space $\mathcal{L}$ has a basis [12] $z_1, \ldots, z_\ell$ satisfying

$$\mathrm{ord}_{Q_v} z_k \geq k - n - 1 \qquad (k = 1, \ldots, \ell).$$

Of course, not all of the functions z_k vanish at Q_v (some of them even have a pole at Q_v) but, "in average", they do. Indeed

$$(18) \qquad \sum_{k=1}^{\ell} \mathrm{ord}_{Q_v} z_k \geq \sum_{k=1}^{\ell} (k - n - 1) = \frac{1}{2} \ell(\ell - 2n - 1) =: A.$$

Since $\ell \sim rn$ for large n, and $r \geq 3$ by the assumption, we may specify n to have $A > 0$.

Express every z_k as a linear form in $\mathbf{y}$:

$$z_k = L_{k,v}(\mathbf{y}).$$

This defines independent linear forms $L_{1,v}, \ldots, L_{\ell,v}$ for $v \in S'$. For $v \in S''$ we simply put $L_{k,v}(\mathbf{y}) = y_k$.

We wish to estimate $|L_{k,v}(\mathbf{y}(P_i))|_v$ for all k and v. For $v \in S''$ we again have

$$|L_{k,v}(\mathbf{y}(P_i))|_v = |y_k(P_i)|_v \ll 1,$$

---

[12] It would be more correct to write $z_{1,v}, \ldots, z_{\ell,v}$, but this would make the notation too heavy.

and for $v \in S'$ we have

$$|L_{k,v}(\mathbf{y}(P_i))|_v = |z_k(P_i)|_v \ll |t_v(P_i)|_v^{\mathrm{ord}_{Q_v} z_k}.$$

Putting this together, we obtain

$$\prod_{v \in S} \prod_{k=1}^{\ell} |L_{k,v}(\mathbf{y}(P_i))|_v \ll \prod_{v \in S'} |t_v(P_i)|_v^{\sum_{k=1}^{\ell} \mathrm{ord}_{Q_v} z_k} \le \prod_{v \in S'} |t_v(P_i)|_v^A,$$

where $A > 0$ is defined in (18). Combining this with (17), we obtain

$$\prod_{v \in S} \prod_{k=1}^{\ell} |L_{k,v}(\mathbf{y}(P_i))|_v \ll H(\mathbf{y}(P_i))^{-\varepsilon}$$

with $\varepsilon = A/n$.

Now apply the Subspace Theorem in the form of Theorem 2.5. We obtain that there exist finitely many non-zero functions $u_1, \ldots, u_s$ from $\mathcal{L}$ such that every P_i is a zero of one of u_j. It follows that among the points P_i only finitely many are distinct, which contradicts the original assumption about the existence of an infinite sequence of distinct S-integral points. The theorem is proved. $\qquad\square$

Since this argument does not use Jacobians, one may expect to extend to higher dimensions. This is discussed in Subsection 5.2. Another useful aspect of the new proof of Siegel's theorem is that it allows, in many cases, to obtain good quantitative bounds for the number of integral points. This direction is exploited, in particular, in [**24**].

5.2. Integral Points on Surfaces

It is widely believed that an affine (respectively, projective) variety V of general type cannot have many integral (respectively, rational) points. Of course, one cannot have here ultimate finiteness, but it is expected that integral (or rational) points are not Zariski dense [13] on V. Faltings [**35**] did the case when V is a subvariety of an abelian variety, and Vojta extended his result to subvarieties of semiabelian varieties, but very little is known for general V.

Since the argument of Corvaja and Zannier does not use Jacobians, it is very likely to extend to certain surfaces and varieties of higher dimension, the assumption *there exists at least* 3 *points at infinity* being replaced by something like *the divisor at infinity is "sufficiently reducible"*. Vojta [**66, 68**] used the Subspace Theorem to show that integral points on an irreducible affine variety of dimension d are not Zariski dense if the divisor at infinity has at least $d + \rho + 1$ components, where ρ is the rank of the Néron-Severi group (see also [**49**]).

---

[13] Recall that a subset of an algebraic variety is *not Zariski dense* if it lies on a proper closed subvariety.

In the article [**26**] Corvaja and Zannier applied their argument to integral points on surfaces. Let $\bar{X}$ be a non-singular projective surface and $X \subset \mathbb{A}^\nu$ a non-empty affine subset of $\bar{X}$. We let $C_1, \ldots, C_r$ be the irreducible components of $\bar{X} \setminus X$ and we may define the "divisor at infinity" $D = C_1 + \cdots + C_r$. Corvaja and Zannier, however, use the divisor

$$D = a_1 C_1 + \cdots + a_r C_r$$

with some positive integers $a_1, \ldots, a_r$ ("weights"). This approach is much more flexible, because the weights can be chosen in a certain "optimal" way.

Recall that in the case of curves we could apply the Subspace Theorem because for every point at infinity Q and for a sufficiently large n we found a basis $z_1, \ldots, z_\ell$ of the space $\mathcal{L}(nD)$ such that

$$\sum_{j=1}^{\ell} \operatorname{ord}_Q(z_j) > 0.$$

Similarly, in the surface case, we must find, for every curve C_i and for a sufficiently large n, a basis $z_1, \ldots, z_\ell$ of the space $H^0(\bar{X}, nD)$ such that

$$\sum_{j=1}^{\ell} \operatorname{ord}_{C_i}(z_j) > 0.$$

We want to express this property in terms of the divisor D. In the subsequent paragraph we write C for C_i and a for a_i.

Consider the filtration of the space $H^0(\bar{X}, nD)$

$$(19) \qquad H^0(\bar{X}, nD) \supseteq H^0(\bar{X}, nD - C) \supseteq H^0(\bar{X}, nD - 2C) \supseteq \ldots,$$

and let $z_1, \ldots, z_\ell$ be a basis of this filtration [14]. For this basis we have

$$\sum_{j=1}^{\ell} \operatorname{ord}_C(z_j) = \sum_{k=0}^{\infty} (k - an)\Big(h^0\big(nD - kC\big) - h^0\big(nD - (k+1)C\big)\Big)$$

$$= -anh^0(nD) + \sum_{k=0}^{\infty} h^0(nD - kC)$$

(of course, the infinite sums have only finitely many non-zero terms).

Thus, the basic condition to be satisfied is that the inequalities

$$(20) \qquad \frac{\sum_{k=0}^{\infty} h^0(nD - kC_i)}{nh^0(nD)} > a_i \qquad (i = 1, \ldots, r)$$

hold for a certain n.

---

[14] A basis of a filtration $W_0 \supseteq W_1 \supseteq W_2 \supseteq \ldots$ of vector spaces is, by definition, a basis of W_0 which contains a basis of every W_i.

THEOREM 5.2 (Corvaja, Zannier). — *Let $\bar{X}$ be a non-singular projective surface defined over a number field K and let $X \subset \mathbb{A}^\nu$ be a non-empty affine subset of $\bar{X}$. Let $C_1, \ldots, C_r$ be effective divisors[15] supported at $\bar{X} \setminus X$. Assume that $C_1, \ldots, C_r$ intersect properly (that is, no 2 of them have a common component and no 3 of them have a common point). Further, assume that for some choice of positive integers $a_1, \ldots, a_r$ the r inequalities (20) (with $D = a_1 C_1 + \cdots + a_r C_r$) hold for certain n. Then for any finite set $S \subset M_K$ the set $X \cap \mathbb{A}^\nu(\mathcal{O}_S)$ of S-integral points on X is not Zariski dense.*

PROOF. — It is quite analogous to the proof of Theorem 5.1. We may assume that every C_i is defined over K. Let n be such that the inequalities (20) hold. As we have seen above, this implies existence of a positive B such that

$$\sum_{k=1}^{\ell} \mathrm{ord}_C z_k \geq B,$$

where C is any of $C_1, \ldots, C_r$ and $z_1, \ldots, z_\ell$ is a basis of the filtration (19).

To prove the theorem, it suffices to show that every infinite sequence of S-integral points has a subsequence contained on a curve defined over K. Indeed, since there are only countably many K-curves, a Zariski-dense set contains a sequence with finitely many elements on every K-curve.

Thus, let $P_1, P_2, P_3 \ldots$ be a sequence of S-integral points. Replacing it by a subsequence, we may assume that it v-adically converges for every $v \in S$, and denote the limit by Q_v. Now we have 3 cases: either $Q_v \in X$ or Q_v belongs exactly to one of the C_i (call it C_v), or it belongs to exactly two of them (call them C_v and C'_v). (By the assumption, Q_v cannot belong to three or more C_i.) Let S_0, S_1 and S_2 be the corresponding subsets of S.

Fix a basis $y_1, \ldots, y_\ell$ of the space $H^0(\bar{X}, nD)$. We may assume that $y_j(P) \in \mathcal{O}_S$ for any S-integral point P.

Now, for each $v \in S$ we shall define a new basis $z_1 = z_{1,v}, \ldots, z_\ell = z_{\ell,v}$ of the same space, and we let $L_{1,v}, \ldots, L_{\ell,v}$ be the linear forms such that $z_k = L_{k,v}(\mathbf{y})$. Then we shall apply the Subspace Theorem to these forms evaluated at $\mathbf{y}(P_i)$.

If $v \in S_0$ then, as in the proof of Theorem 5.1, we define the z-basis just putting $z_j = y_j$. We have plainly

(21) $$\|\mathbf{y}(P_i)\|_v \ll 1,$$

(22) $$\prod_{k=1}^{\ell} |L_{k,v}(\mathbf{y}(P_i))|_v \ll 1.$$

---

[15] We do not assume the divisors $C_1, \ldots, C_r$ irreducible.

Next, assume that $v \in S_1$ and let $z_1, \ldots, z_\ell$ be a basis of the filtration (19) with $C = C_v$. If t_v is a local parameter of C_v near Q_v then for any function u regular on X the function $t_v^{-\operatorname{ord}_{C_v} u} u$ is regular in a neighborhood of Q_v. It follows

$$|u(P_i)|_v \ll |t_v(P_i)|_v^{\operatorname{ord}_{C_v} u} \qquad (i = 1, 2, \ldots).$$

Applying this with $u = y_1, \ldots, y_\ell$ and with $u = z_1, \ldots, z_\ell$, we find that

$$(23) \qquad \|\mathbf{y}(P_i)\|_v \ll |t_v(P_i)|_v^{\min_{1 \le j \le \ell} \operatorname{ord}_{C_v} y_j} \le |t_v(P_i)|_v^{-An},$$

$$(24) \qquad \prod_{k=1}^\ell |L_{k,v}(\mathbf{y}(P_i))|_v \ll |t_v(P_i)|_v^{\sum_{k=1}^\ell \operatorname{ord}_{C_v} z_k} \le |t_v(P_i)|_v^B,$$

where $A = \max\{a_1, \ldots, a_r\}$ and $B > 0$ is defined in the beginning of the proof.

Finally, assume that $v \in S_2$. In this case Corvaja and Zannier use the following nice elementary lemma.

LEMMA 5.3. — *Let*

$$(25) \qquad W = W_0 \supseteq W_1 \supseteq W_2 \supseteq \ldots, \qquad W = W_0' \supseteq W_1' \supseteq W_2' \supseteq \ldots$$

be two filtrations of a finitely dimensional vector space W. Then there exists a common basis for the two filtrations (that is, there exists a basis of W containing bases for every W_i and for every W_i'.)

(The proof is by induction in $\dim W$. Without loss of generality we may assume that W_1 is a hyperplane in W. Put $W_i'' = W_1 \cap W_i'$. By induction, there exists a common basis $w_1, \ldots, w_{d-1}$ for the filtrations $W_1 \supseteq W_2 \supseteq \ldots$ and $W_1 = W_0'' \supseteq W_1'' \supseteq W_2'' \supseteq \ldots$. Now let k be the smallest index for which $W_k' \not\subseteq W_1$ (the set of such indices is non-empty because it includes 0). Then W_i'' is a hyperplane in W_i' for $i \le k$ and $W_i' = W_i''$ for $i > k$. Now, picking a $w_d \in W_k' \setminus W_k''$, we obtain a basis $w_1, \ldots, w_{d-1}, w_d$ of both filtrations (25), which proves the lemma.)

Using the lemma, we find a common basis $z_1, \ldots, z_\ell$ for both the filtrations (19) with $C = C_v$ and $C = C_v'$.

Now let t_v and t_v' be local parameters near Q_v at C_v and C_v', respectively. Then for any function u regular on X the function $t_v^{-\operatorname{ord}_{C_v} u} (t_v')^{-\operatorname{ord}_{C_v'} u} u$ is regular in a neighborhood of Q_v, whence

$$|u(P_i)|_v \ll |t_v(P_i)|_v^{\operatorname{ord}_{C_v} u} |t_v'(P_i)|_v^{\operatorname{ord}_{C_v'} u} \qquad (i = 1, 2, \ldots).$$

Applying this with $u = y_1, \ldots, y_\ell$ and with $u = z_1, \ldots, z_\ell$, we obtain

$$(26) \quad \|\mathbf{y}(P_i)\|_v \ll |t_v(P_i)|_v^{\min_{1 \le j \le \ell} \operatorname{ord}_{C_v} y_j} |t_v'(P_i)|_v^{\min_{1 \le j \le \ell} \operatorname{ord}_{C_v'} y_j} \le |t_v(P_i) t_v'(P_i)|_v^{-An},$$

(27)
$$\prod_{k=1}^\ell |L_{k,v}(\mathbf{y}(P_i))|_v \ll |t_v(P_i)|_v^{\sum_{k=1}^\ell \operatorname{ord}_{C_v} z_k} |t_v'(P_i)|_v^{\sum_{k=1}^\ell \operatorname{ord}_{C_v'} z_k} \le |t_v(P_i) t_v'(P_i)|_v^B.$$

Combining the inequalities (21, 23, 26) with (22, 24, 27), we find

$$\prod_{v \in S} \prod_{k=1}^{\ell} |L_{k,v}(\mathbf{y}(P_i))|_v \ll H(\mathbf{y}(P_i))^{-\varepsilon} \qquad (i = 1, 2, \dots)$$

with $\varepsilon = B/An$. Now we complete the proof using the Subspace Theorem in the same manner as we did in the proof of Theorem 5.1. □

REMARK 5.4. — Using Vojta's refinement [**67**] of the Subspace Theorem, Levin [**43**] shows that, under the hypothesis of Theorem 5.2 there exists a (possibly, reducible) affine curve on X, depending only on X, but independent on K and S, such that all but finitely many S-integral points from X belong to this curve. (The exceptional finite set may, however, depend on K and S.) The same is true for the consequences of Theorem 5.2: Corollaries 5.6 and 5.7 and Theorem 5.8.

Imposing on our divisors C_i additional assumption (like ampleness), we can estimate from below the quantity on the left of (20) asymptotically (as $n \to \infty$), using the Riemann-Roch theorem on surfaces. This would express our condition in terms of the intersection numbers of the divisors $C_1, \dots, C_r$ and the weights $a_1, \dots, a_r$. The Riemann-Roch theorem applies through the following lemma, proved in the addendum to this section.

LEMMA 5.5. — *Let C be an ample divisor and D an effective divisor on a nonsingular projective surface, and let n and k be positive integers such that $k \leq \alpha n$, where $\alpha = (D \cdot C)/C^2$. Then*

$$(28) \qquad\qquad h^0(nD - kC) \geq \frac{1}{2}(nD - kC)^2 - O(n).$$

Let us look closer at this lemma. We have

$$(nD - kC)^2 = D^2 n^2 - 2(D \cdot C)nk + C^2 k^2.$$

The quadratic form

$$q(\xi, \tau) = D^2 \xi^2 - 2(D \cdot C)\xi\tau + C^2 \tau^2$$

is not positive definite by the Hodge index theorem. Hence the polynomial $q(1, \tau)$ has two real roots, γ and γ'. They are, obviously, positive, and we assume that $\gamma \leq \gamma'$. In fact, $\gamma \leq \alpha \leq \gamma'$ because $\alpha = (\gamma + \gamma')/2$.

Thus, we have $q(\xi, \tau) < 0$ if $\gamma\xi < \tau < \gamma'\xi$, and $q(\xi, \tau) \geq 0$ otherwise. In particular, (28) remains true for $k \leq \gamma'n$, but it is uninteresting for $\gamma n < k < \gamma'n$ and becomes interesting only for $k \leq \gamma n$.

Applying the lemma in our situation, we bound the numerator on the left of (20) as (we write C instead of C_i)

$$(29) \qquad \sum_{k=0}^{\infty} h^0(nD - kC) \geq \sum_{k \leq \theta n} \frac{1}{2} q(n, k) - O(n^2)$$

$$= \left(\frac{1}{2} \theta D^2 - \frac{1}{2} \theta^2 (D \cdot C) + \frac{1}{6} \theta^3 C^2 \right) n^3 - O(n^2),$$

where θ is any real number satisfying $0 \leq \theta \leq \gamma'$. Also, the Riemann-Roch theorem gives for the denominator in (20) the asymptotics

$$n h^0(nD) = \frac{1}{2} n^3 D^2 + O(n^2).$$

Hence the left-hand side of (20) is bounded from below by $F(\theta) + O(1/n)$, where

$$F(\theta) = \theta \left(1 - \theta \frac{D \cdot C}{D^2} + \frac{1}{3} \theta^2 \frac{C^2}{D^2} \right).$$

It remains to select the parameter θ in the optimal way.

The estimate in (29) is best possible if the sum on the right of (29) contains all positive terms $q(n, k)$ and no negative terms. It follows that the optimal choice is $\theta = \gamma$. We obtain the following consequence.

COROLLARY 5.6 (Corvaja, Zannier). — *Let $\bar{X}$ be a non-singular projective surface defined over a number field K and let $X \subset \mathbb{A}^{\nu}$ be a non-empty affine subset of $\bar{X}$. Let $C_1, \ldots, C_r$ be properly intersecting effective ample divisors supported at $\bar{X} \setminus X$. Further, assume that for some choice of positive integers $a_1, \ldots, a_r$ the r inequalities*

$$(30) \qquad \gamma_i \left(1 - \gamma_i \frac{D \cdot C_i}{D^2} + \frac{1}{3} \gamma_i^2 \frac{C_i^2}{D^2} \right) > a_i \qquad (i = 1, \ldots r)$$

hold, where $D = a_1 C_1 + \cdots + a_r C_r$ and where γ_i is the smallest positive root of the polynomial $D^2 - 2(D \cdot C_i)T + C_i^2 T^2$. Then for any finite set $S \subset M_K$ the S-integral points are not Zariski dense on X.

By choosing suitable weights, Corvaja and Zannier showed that integral points are not Zariski-dense if they satisfy some conditions, for instance if $r \geq 4$ and the intersection matrix of $C_1, \ldots, C_r$ is of rank 1.

Autissier [7] suggested to take $\theta = \beta/2$, where $\beta = D^2/(D \cdot C)$. (Notice that $\beta/2 < \gamma$ and $\gamma \approx \beta/2$ when γ' is very large.) Since

$$F\left(\frac{\beta}{2} \right) = \frac{\beta}{2} \left(1 - \frac{\beta}{2} \frac{D \cdot C}{D^2} + \frac{\beta^2}{12} \frac{C^2}{D^2} \right) = \frac{1}{4} \frac{D^2}{D \cdot C} \left(1 + \frac{1}{6} \frac{D^2 C^2}{(D \cdot C)^2} \right),$$

we obtain the following result.

COROLLARY 5.7 (Autissier). — *In the set-up of Corollary 5.6, assume that for some choice of positive integers* $a_1, \ldots, a_r$ *the* r *inequalities*

$$(31) \qquad \frac{D^2}{D \cdot C_i} \left(1 + \frac{1}{6} \frac{D^2 C_i^2}{(D \cdot C_i)^2} \right) > 4a_i \qquad (i = 1, \ldots, r)$$

hold. Then for any finite set $S \subset M_K$ *the* S-*integral points are not Zariski dense on* X.

This result is formally weaker, than Corollary 5.6, but it is more practical, because inequality (31) is much easier to handle, than (30).

Levin [**43**] and, independently, Autissier [**7**] observed that a "nearly optimal" choice of the weights $a_1, \ldots, a_r$ implies that 4 ample divisors at infinity would suffice. More precisely, they prove the following.

THEOREM 5.8 (Levin, Autissier). — *Let* $\bar{X}$ *be a non-singular projective surface defined over a number field* K *and let* $X \in \mathbb{A}^\nu$ *be a non-empty affine subset of* $\bar{X}$. *Let* $C_1, \ldots, C_r$ *be properly intersecting effective ample divisors supported at* $\bar{X} \setminus X$. *Assume that* $r \geq 4$. *Then for any finite set* $S \subset M_K$ *the* S-*integral points on* X *are not Zariski dense.*

REMARK 5.9. — In Theorem 5.8 one can relax the assumption that the divisors C_i are ample (see [**43**, Theorem 11.5A]), but one cannot just assume that C_i are effective and intersect properly. As an example take $\bar{X} = \mathbb{P}^1 \times \mathbb{P}^1$ and $X = \mathbb{G}_m \times \mathbb{G}_m$, where $\mathbb{G}_m$ is obtained by removing the 0-point and the ∞-point from $\mathbb{P}^1$. Then $\bar{X} \setminus X$ consists of 4 curves. The map $(x, y) \to (x, x^{-1}, y, y^{-1})$ defines an affine embedding $X \to \mathbb{A}^4$, and the set of S-integral points with respect to this embedding is $\mathcal{O}_S^\times \times \mathcal{O}_S^\times$, which is Zariski-dense in general.

To prove Theorem 5.8 we need one more elementary lemma.

LEMMA 5.10. — *Let* $M = [\mu_{ij}]_{1 \leq i,j \leq r}$ *be a symmetric* $r \times r$-*matrix with positive real entries. Consider the linear forms*

$$L_i(\mathbf{x}) = \mu_{i1} x_1 + \cdots + \mu_{ir} x_r \qquad (i = 1, \ldots, r)$$

and the quadratic form $Q(\mathbf{x}) = \mathbf{x}^t M \mathbf{x}$. *Then for any* $\varepsilon > 0$ *there exist positive integers* $a_1, \ldots, a_r$ *such that*

$$(32) \qquad (1 - \varepsilon) Q(\mathbf{a}) < r a_i L_i(\mathbf{a}) < (1 + \varepsilon) Q(\mathbf{a}) \qquad (i = 1, \ldots, r),$$

where $\mathbf{a} = (a_1, \ldots, a_r)$.

PROOF. — We follow the elegant argument of Autissier [**7**, Proposition 2.3]. Notice that

$$Q(\mathbf{x}) = x_1 L_1(\mathbf{x}) + \cdots + x_r L_r(\mathbf{x}).$$

Hence we have to find a point $\mathbf{a}$ with positive *integral* coordinates such that the r numbers $a_i L_i(\mathbf{a})$ are *approximately* equal. We first find a point with positive *real* coordinates where these numbers are *exactly* equal.

Let Δ be the simplex

(33) $$x_1 + \cdots + x_r = 1, \qquad 0 \le x_i \le 1 \qquad (i = 1, \ldots, r).$$

Consider the map $\Delta \to \Delta$ defined by

$$\mathbf{x} \mapsto \left(L_1(\mathbf{x})^{-1}, \ldots, L_r(\mathbf{x})^{-1} \right) \left(\sum_{i=1}^r L_i(\mathbf{x})^{-1} \right)^{-1}.$$

The map is well-defined because the entries of our matrix M are positive numbers. By the Brower theorem, our map has a fixed point $\mathbf{a} \in \Delta$. For this point we have

$$a_1 L_1(\mathbf{a}) = \cdots = a_r L_r(\mathbf{a}).$$

Since none of the $L_i(\mathbf{a})$ vanishes, none of the a_i does; in other words, the real numbers $a_1, \ldots, a_r$ are strictly positive. Replacing each by a suitable rational approximation, we obtain positive rational numbers $a_1, \ldots, a_r$ satisfying (32). Multiplying them by the common denominator, we arrive to the desired integers $a_1, \ldots, a_r$. $\qquad \square$

PROOF OF THEOREM 5.8. — First of all, remark that the term

(34) $$\frac{1}{6} \frac{D^2 C_i^2}{(D \cdot C_i)^2},$$

occurring in (31), is bounded from below, uniformly in $\mathbf{a}$, by a positive constant. Indeed, (34) defines a homogeneous positive real function on non-zero vectors $\mathbf{a} \in (\mathbb{Z}_{\ge 0})^r$. But, since it is a quotient of quadratic forms with positive coefficients, it extends to a positive real continuous function on the non-zero vectors of $(\mathbb{R}_{\ge 0})^r$. By homogeneity, it suffices to consider this function on the compact Δ defined by (33), where it is bounded away from 0.

Thus, to ensure (31), we must find positive integers $a_1, \ldots, a_r$ such that for some $\varepsilon > 0$ the inequalities

$$D^2 (1 + \varepsilon) > 4a_i (D \cdot C_i) \qquad (i = 1, \ldots, r)$$

hold. Applying Lemma 5.10 to the intersection matrix of $C_1, \ldots, C_r$, we find $a_1, \ldots, a_r$ such that

$$D^2 (1 + \varepsilon) > r a_i (D \cdot C_i) \qquad (i = 1, \ldots, r).$$

Since $r \ge 4$, we are done. $\qquad \square$

In his fundamental article [**43**], Levin extends Theorem 5.8 to varieties of arbitrary dimension, without assuming proper intersection. One difficulty he has to overcome is that Lemma 5.3 is no longer true for three or more filtrations.

Levin gives a thorough analysis of the argument of Corvaja and Zannier and, probably, reaches its "natural limitations". In addition, he accompanies every Diophantine result with an analogous statement about holomorphic maps, in accordance with Vojta's philosophy.

For more Diophantine applications of the Subspace Theorem, see [**25, 31**].

Addendum: Proof of Lemma 5.5

We deduce Lemma 5.5 from the Theorem of Riemann-Roch and the following proposition.

PROPOSITION 5.11. — *Let B, C and D be divisors on a non-singular projective surface X. Assume that C is very ample, that D is effective and that $C^2 \le C \cdot D$. Then*
$$h^0(B - D + C) \le B \cdot C + h^0(B) + 1.$$

PROOF. — By the Theorem of Bertini we may assume that C is an irreducible smooth curve. The exact sequence of sheaves
$$0 \to \mathcal{O}_X(B - D) \to \mathcal{O}_X(B - D + C) \to \mathcal{O}_X(B - D + C)|_C \to 0,$$
implies the exact sequence of cohomologies
$$0 \to H^0(X, B - D) \to H^0(X, B - D + C) \to H^0(C, \Delta) \to \dots,$$
where Δ is the divisor $(B - D + C)|_C$ on C. It follows that
$$(35) \qquad h^0(X, B - D + C) \le h^0(X, B - D) + h^0(C, \Delta).$$
We have $\deg \Delta = (B - D + C) \cdot C \le B \cdot C$ because $C^2 \le C \cdot D$. It remains to observe that $h^0(C, \Delta) \le \deg \Delta + 1$ and that $h^0(X, B - D) \le h^0(X, B)$, because D is effective. $\square$

PROOF OF LEMMA 5.5. — By the theorem of Riemann-Roch,
$$h^0(nD - kC) \ge \frac{1}{2}(nD - kC)^2 - \frac{1}{2}\big((nD - kC) \cdot K\big) - h^0(K - nD + kC) + O(1),$$
where K is the canonical divisor. Since $(nD - kC) \cdot K = O(n)$, we have to prove that $h^0(K - nD + kC) = O(n)$.

We may assume k so large that kC is very ample. Applying Proposition 5.11 with $B = K$ and with kC, nD instead of C and D, the condition $(kC)^2 \le kC \cdot nD$ being assured by the assumption $k \le \alpha n$, we find

$$h^0(K - nD + kC) \leq k(K \cdot C) + h^0(K) + 1 = O(n),$$

as wanted.   □

I thank Ivan Cheltsov for explanations concerning this lemma.

6. CONCLUSION

As it was indicated in the introduction, the recent remarkable applications of the Subspace Theorem are not limited to the results discussed above. Without any claim for exhaustiveness, let me just quote several more works that I personally find attractive.

Mahler [46] showed, using the theorem of Ridout, that if α is a positive rational number, but not integer, and $0 < \theta < 1$ then the inequality $|\alpha^n - m| \leq \theta^n$ has finitely many solutions in positive integers n and m. He asked for which irrational algebraic numbers a similar statement is true, observing that it is false, for instance, if $\alpha = \left(1 + \sqrt{5}\right)/2$, and, more generally, if α is a Pisot number [16]. Corvaja and Zannier answered this question, showing that the corresponding statement is true for all irrational algebraic numbers except the roots of Pisot numbers (and for the latter it is obviously false).

In the same article they answered a question of Mendès France [47] on the period length of the periodic continued fraction for α^n, where α is a quadratic irrationality. Corvaja and Zannier showed that the period tends to infinity with n unless α is a square root of a rational number or a unit. See also [14, 29, 61].

Corvaja and Zannier [20] gave a complete answer to Pisot's question on when the quotient $u(n)/v(n)$ of two power sums (and, more generally, of two linear recurrences) is infinitely often an integer. By the way, this is one of the rare cases when the authors managed to overcome the difficulty stemming from the absence of the "dominant root" (see the end of Section 4).

Corvaja and Zannier [23] and, independently, Hernández and Luca [39] proved that $(ab + 1)(ac + 1)(bc + 1)$ cannot have only small prime divisors, confirming a conjecture of Győry, Sárközy and Stewart [38]. See [13] for a quantitative version of this result.

Bugeaud, Corvaja and Zannier proved [12] that $a^n - 1$ and $b^n - 1$ cannot have a large common divisor. This was extended by Corvaja and Zannier [23, 28].

---

[16] See footnote 4 on page 11.

Corvaja, Rudnick and Zannier [**18**] showed that (with obvious exceptions) the multiplicative order of an integral matrix mod N grows quicker than $\log N$ as $N \to \infty$. This result is essentially the best possible.

And there are numerous contributions that I failed to mention, because of lack of space or time or because of my ignorance.

REFERENCES

[1] B. ADAMCZEWSKI & Y. BUGEAUD – "On the complexity of algebraic numbers. II. Continued fractions", *Acta Math.* **195** (2005), p. 1–20.

[2] ———, "On the complexity of algebraic numbers. I. Expansions in integer bases", *Ann. of Math. (2)* **165** (2007), p. 547–565.

[3] _____ , "On the Maillet-Baker continued fractions", *J. reine angew. Math.* **606** (2007), p. 105–121.

[4] B. ADAMCZEWSKI, Y. BUGEAUD & F. LUCA – "Sur la complexité des nombres algébriques", *C. R. Math. Acad. Sci. Paris* **339** (2004), p. 11–14.

[5] J.-P. ALLOUCHE & J. SHALLIT – *Automatic sequences. Theory, applications, generalizations*, Cambridge University Press, 2003.

[6] F. AMOROSO & U. ZANNIER (eds.) – *Diophantine approximation*, Lectures from the C.I.M.E. Summer School held in Cetraro, June 28–July 6, 2000. Lecture Notes in Mathematics **1819**, Springer, 2003.

[7] P. AUTISSIER – "Géométrie des surfaces algébriques et points entiers", arXiv:math.NT/0606184.

[8] Y. BILU – "A note on universal Hilbert sets", *J. reine angew. Math.* **479** (1996), p. 195–203.

[9] E. BOMBIERI & W. GUBLER – *Heights in Diophantine geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, 2006.

[10] É. BOREL – "Les probabilités dénombrables et leurs applications arithmétiques", *Palermo Rend.* **27** (1909), p. 247–271.

[11] _____ , "Sur les chiffres décimaux de $\sqrt{2}$ et divers problèmes de probabilités en chaîne", *C. R. Acad. Sci. Paris* **230** (1950), p. 591–593.

[12] Y. BUGEAUD, P. CORVAJA & U. ZANNIER – "An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$", *Math. Z.* **243** (2003), p. 79–84.

[13] Y. BUGEAUD & F. LUCA – "A quantitative lower bound for the greatest prime factor of $(ab + 1)(bc + 1)(ca + 1)$", *Acta Arith.* **114** (2004), p. 275–294.

[14] _____ , "On the period of the continued fraction expansion of $\sqrt{2^{2n+1} + 1}$", *Indag. Math. (N.S.)* **16** (2005), p. 21–35.

[15] P. BUNDSCHUH & A. PETHŐ – "Zur Transzendenz gewisser Reihen", *Monatsh. Math.* **104** (1987), p. 199–223.

[16] A. COBHAM – "On the Hartmanis-Stearns problem for a class of tag machines", in *IEEE Conference Record of 1968 Ninth Annual Symposium on Switching and Automata Theory, Schenectady*, 1968, p. 51–60.

[17] _____ , "Uniform tag sequences", *Math. Systems Theory* **6** (1972), p. 164–192.

[18] P. CORVAJA, Z. RUDNICK & U. ZANNIER – "A lower bound for periods of matrices", *Comm. Math. Phys.* **252** (2004), p. 535–541.

[19] P. CORVAJA & U. ZANNIER – "Diophantine equations with power sums and universal Hilbert sets", *Indag. Math. (N.S.)* **9** (1998), p. 317–332.

[20] _____ , "Finiteness of integral values for the ratio of two linear recurrences", *Invent. Math.* **149** (2002), p. 431–451.

[21] ———, "Some new applications of the subspace theorem", *Compositio Math.* **131** (2002), p. 319–340.

[22] ———, "A subspace theorem approach to integral points on curves", *C. R. Math. Acad. Sci. Paris* **334** (2002), p. 267–271.

[23] ———, "On the greatest prime factor of $(ab + 1)(ac + 1)$", *Proc. Amer. Math. Soc.* **131** (2003), p. 1705–1709.

[24] ———, "On the number of integral points on algebraic curves", *J. reine angew. Math.* **565** (2003), p. 27–42.

[25] ———, "On a general Thue's equation", *Amer. J. Math.* **126** (2004), p. 1033–1055.

[26] ———, "On integral points on surfaces", *Ann. of Math. (2)* **160** (2004), p. 705–726.

[27] ———, "On the rational approximations to the powers of an algebraic number: solution of two problems of Mahler and Mendès France", *Acta Math.* **193** (2004), p. 175–191.

[28] ———, "A lower bound for the height of a rational function at S-unit points", *Monatsh. Math.* **144** (2005), p. 203–224.

[29] ———, "On the length of the continued fraction for values of quotients of power sums", *J. Théor. Nombres Bordeaux* **17** (2005), p. 737–748.

[30] ———, "S-unit points on analytic hypersurfaces", *Ann. Sci. École Norm. Sup. (4)* **38** (2005), p. 76–92.

[31] ———, "On the integral points on certain surfaces", *Int. Math. Res. Not.* (2006), Art. ID 98623.

[32] P. Dèbes & U. Zannier – "Universal Hilbert subsets", *Math. Proc. Cambridge Philos. Soc.* **124** (1998), p. 127–134.

[33] J.-H. Evertse & H. P. Schlickewei – "The absolute subspace theorem and linear equations with unknowns from a multiplicative group", in *Number theory in progress, Vol. 1 (Zakopane-Kościelisko, 1997)*, de Gruyter, 1999, p. 121–142.

[34] ———, "A quantitative version of the absolute subspace theorem", *J. reine angew. Math.* **548** (2002), p. 21–127.

[35] G. Faltings – "Diophantine approximation on abelian varieties", *Ann. of Math. (2)* **133** (1991), p. 549–576.

[36] S. Ferenczi & C. Mauduit – "Transcendence of numbers with a low complexity expansion", *J. Number Theory* **67** (1997), p. 146–161.

[37] P. C. Gilmore & A. Robinson – "Metamathematical considerations on the relative irreducibility of polynomials", *Canad. J. Math.* **7** (1955), p. 483–489.

[38] K. Győry. A. Sárközy & C. L. Stewart – "On the number of prime factors of integers of the form $ab + 1$", *Acta Arith.* **74** (1996), p. 365–385.

[39] S. HERNÁNDEZ & F. LUCA – "On the largest prime factor of $(ab+1)(ac+1)(bc+1)$", *Bol. Soc. Mat. Mexicana (3)* **9** (2003), p. 235–244.

[40] M. HINDRY & J. H. SILVERMAN – *Diophantine geometry, an introduction*, Graduate Texts in Mathematics, vol. 201, Springer, 2000.

[41] S. LANG – *Fundamentals of Diophantine geometry*, Springer, 1983.

[42] M. LAURENT – "Équations diophantiennes exponentielles", *Invent. Math.* **78** (1984), p. 299–327.

[43] A. LEVIN – "Generalizations of Siegel's and Picard's theorems", arXiv:math.NT/0503699, to appear.

[44] J. H. LOXTON & A. J. VAN DER POORTEN – "Arithmetic properties of the solutions of a class of functional equations", *J. reine angew. Math.* **330** (1982), p. 159–172.

[45] _____ , "Arithmetic properties of automata: regular sequences", *J. reine angew. Math.* **392** (1988), p. 57–69.

[46] K. MAHLER – "On the fractional parts of the powers of a rational number. II", *Mathematika* **4** (1957), p. 122–124.

[47] M. MENDÈS FRANCE – "Remarks and problems on finite and periodic continued fractions", *Enseign. Math. (2)* **39** (1993), p. 249–257.

[48] M. MIGNOTTE – "An application of W. Schmidt's theorem: transcendental numbers and golden number", *Fibonacci Quart.* **15** (1977), p. 15–16.

[49] J. NOGUCHI & J. WINKELMANN – "Holomorphic curves and integral points off divisors", *Math. Z.* **239** (2002), p. 593–610.

[50] D. RIDOUT – "The p-adic generalization of the Thue-Siegel-Roth theorem", *Mathematika* **5** (1958), p. 40–48.

[51] K. F. ROTH – "Rational approximations to algebraic numbers", *Mathematika* **2** (1955), p. 1–20; corrigendum, 168.

[52] H. P. SCHLICKEWEI – "The subspace theorem and applications", in *Proceedings of the International Congress of Mathematicians, Vol. II (Berlin, 1998)*, vol. Extra Vol. II, *Doc. Math.*, 1998, Extra Vol. II, p. 197–205 (electronic).

[53] _____ , "Die p-adische Verallgemeinerung des Satzes von Thue-Siegel-Roth-Schmidt", *J. reine angew. Math.* **288** (1976), p. 86–105.

[54] _____ , "On products of special linear forms with algebraic coefficients", *Acta Arith.* **31** (1976), p. 389–398.

[55] _____ , "The $\mathfrak{p}$-adic Thue-Siegel-Roth-Schmidt theorem", *Arch. Math. (Basel)* **29** (1977), p. 267–270.

[56] _____ , "Multiplicities of recurrence sequences", *Acta Math.* **176** (1996), p. 171–243.

[57] _____ , "Approximation of algebraic numbers", in *Diophantine approximation (Cetraro, 2000)*, Lecture Notes in Math., vol. 1819, Springer, 2003, p. 107–170.

[58] W. M. SCHMIDT – "Norm form equations", *Ann. of Math. (2)* **96** (1972), p. 526–551.

[59] _____ , *Diophantine approximation*, Lecture Notes in Mathematics, vol. 785, Springer, 1980.

[60] _____ , *Diophantine approximations and Diophantine equations*, Lecture Notes in Mathematics, vol. 1467, Springer, 1991.

[61] A. SCREMIN – "On the period of the continued fraction for values of the square root of power sums", *Acta Arith.* **123** (2006), p. 297–312.

[62] C. L. SIEGEL – "Über einige Anwendungen Diophantischer Approximationen", *Abh. Preuss Akad. Wiss. Phys.-Math. Kl.* **1** (1929), p. 209–266.

[63] V. G. SPRINDZHUK – "Diophantine equations with prime unknowns (Russian)", *Trudy Mat. Inst. Steklov.* **158** (1981), p. 180–196; English translation: *Proc. Steklov Inst. Math.* 1983, **4**, p. 197–214.

[64] A. THUE – "Über Annäherungswerte algebraischer Zahlen", *J. reine angew. Math.* **135** (1909), p. 284–305.

[65] G. TROI & U. ZANNIER – "Note on the density constant in the distribution of self-numbers. II", *Boll. Unione Mat. Ital. Sez. B Artic. Ric. Mat. (8)* **2** (1999), p. 397–399.

[66] P. VOJTA – *Diophantine approximations and value distribution theory*, Lecture Notes in Mathematics, vol. 1239, Springer, 1987.

[67] _____ , "A refinement of Schmidt's subspace theorem", *Amer. J. Math.* **111** (1989), p. 489–518.

[68] _____ , "Integral points on subvarieties of semiabelian varieties. I", *Invent. Math.* **126** (1996), p. 133–181.

[69] _____ , "Integral points on subvarieties of semiabelian varieties. II", *Amer. J. Math.* **121** (1999), p. 283–313.

[70] M. WALDSCHMIDT – "Diophantine analysis and words", in *Diophantine analysis and related fields 2006 (in honor of Prof. Iekata Shiokawa)*, Sem. Math. Sci., vol. 35, Keio Univ., 2006, p. 203–221.

[71] M. YASUMOTO – "Hilbert irreducibility sequences and nonstandard arithmetic", *J. Number Theory* **26** (1987), p. 274–285.

[72] U. ZANNIER – "Note on dense universal Hilbert sets", *C. R. Acad. Sci. Paris Sér. I Math.* **322** (1996), p. 703–706.

[73] _____ , "A proof of Pisot's *d*-th root conjecture", *Ann. of Math. (2)* **151** (2000), p. 375–383.

[74] _____ , "Some applications of diophantine approximation to diophantine equations (with special emphasis on the Schmidt subspace theorem)", Forum, Udine, 2003.

Yuri F. BILU

Université Bordeaux I
UFR de Mathématiques et Informatique
A2X : Laboratoire de Théorie des Nombres
et d'Algorithmique Arithmétique
(UMR 5465 du CNRS)
351 cours de la Libération
F-33405 Talence Cedex
E-mail : yuri@math.u-bordeaux1.fr