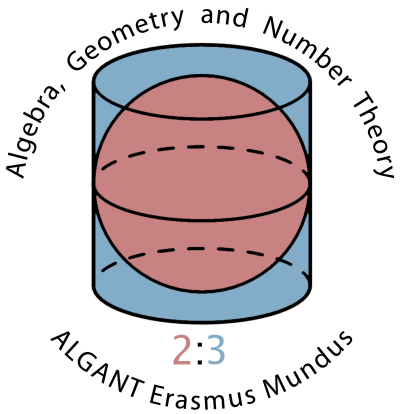

ALGANT MASTER THESIS

ON THE COMPLEXITY OF THE β-EXPANSIONS OF ALGEBRAIC NUMBERS

Alessandro PEZZONI

Advised by:
Dr. Jan-Hendrik EVERTSE

UNIVERSITÀ DEGLI STUDI
DI MILANO

UNIVERSITEIT
LEIDEN

27 August 2015

Contents

1 Introduction

Consider a (positive) real number α and an integer $b \geq 2$. Then we know that we can always find an integer m and a sequence $(a_k)_{k \geq -m}$ with terms in $\{0, \ldots, b-1\}$ such that

$$\begin{aligned} \alpha &= a_{-m} \ldots a_0 \, . \, a_1 a_2 a_3 \ldots \\ &:= \sum_{k=-m}^{\infty} a_k b^{-k}. \end{aligned}$$

The expression $a_{-m} \ldots a_0 \, . \, a_1 a_2 a_3 \ldots$ is called the *b-ary expansion* of α and the terms a_k are the *digits* of α in base b. Furthermore, recall that we can make the choice of b-ary expansion unique by excluding the expansions with a tail of $(b-1)$s.

We say that a real number α is *normal in base b* if for every $n \geq 1$, each of the b^n possible blocks of n digits from $\{0, \ldots, b-1\}$ occurs with frequency $1/b^n$ among all blocks of n consecutive digits of the b-ary expansion of α. In other words, for any fixed block of n digits $w = x_1 \ldots x_n$ with $x_i \in \{0, \ldots, b-1\}$, we define $N_r^b(\alpha, w)$ to be the number of occurrences of w among the blocks $a_{-m} \cdots a_{n-1-m}$, $a_{1-m} \cdots a_{n-m}$, $\ldots$, $a_{r+1-n-m} \cdots a_{r-m}$ and we say that α is normal in base b if

$$\lim_{r \to \infty} \frac{N_r^b(\alpha, w)}{r} = \frac{1}{b^n}.$$

Moreover, we say that α is *(absolutely) normal* if it is normal in every base $b \geq 2$. It is useful to observe that a real number α with sequence of digits $(a_k)_{k \geq -m}$ is normal (in base b) if and only if $(a_k)_{k \geq 1}$ is the sequence of digits of a normal (in base b) number in $[0, 1]$.

In 1909 Borel [9] used his strong law of large numbers to prove that almost every real number (with respect to the Lebesgue measure) is absolutely normal. Though his proof was faulty, it was fixed a year later by Faber [18] and various alternative proofs appeared since then.

The first known numbers normal in some base b were constructed by Champernowne [11] in 1933 by concatenating the b-ary expansions of the positive integers. For example

$$0.12345678910111213141516\ldots$$

in base 10. Furthermore, he conjectured that the number

$$0.23571113171923\ldots$$

obtained by concatenating the decimal expansion of all the prime numbers is normal in base 10, and this was proved by Copeland and Erdős [13] in 1946.

A few other examples of numbers normal in some base are known, and in 2002 Becher and Figueira [5] proved the existence of a computable absolutely normal number by following an old proof by Sierpinski of Borel's result. Despite the abundance of normal numbers, though, we currently don't know of any example which has not been constructed ad-hoc. In 1950 Borel [10] conjectured that every irrational algebraic number is absolutely normal, but an answer to this problem seems still out of reach. We don't even know if, say, 5 appears infinitely many times in the decimal expansion of $\sqrt{2}$.

1.1 β-expansions

This problem can be generalised as follows. Fix a real number $\beta > 1$ and consider the transformation on $[0,1]$ given by $T_\beta : x \mapsto \beta x \pmod 1$. Then we can define the β-*expansion* of a number $\alpha \in [0,1]$ as

$$0.x_1x_2\ldots := \sum_{k=1}^{\infty} x_k \beta^{-k}$$

where $x_k = \left\lfloor \beta T_\beta^{k-1}(x) \right\rfloor$ for every $k \geq 1$ and T_β^0 is the identity on $[0,1]$. Furthermore, we can extend this to every (positive) real number α by saying that the β-expansion of α is

$$\beta^n \sum_{k=1}^{\infty} x_k \beta^{-k}$$

where $n \geq 0$ is the smallest integer such that $\alpha/\beta^n \in [0,1]$ and x_k are the digits of the β-expansion of α/β^n. Note that the β-expansion of a real number is unique by construction.

Now, if β is an integer this is the same as the b-ary expansion defined above, otherwise the digits x_k are all elements of $\{0,\ldots,\lfloor\beta\rfloor\}$. We cannot naively extend the notion of normal number to non-integer bases, though. For example, if $\beta = \varphi$ is the golden ratio, then $1 + 1/\varphi = \varphi$ implies that the sequence 11 will never appear in the φ-expansion of a real number.

In 1957 Rényi [27] proved that T_β admits a unique ergodic invariant probability measure μ_β, which is absolutely continuous with respect to the Lebesgue measure on $[0,1]$. Furthermore, he showed that if β is an integer, then μ_β is just the Lebesgue measure on $[0,1]$.

Observe that if $0.x_1x_2x_3\ldots$ is the β-expansion of α, then $0.x_2x_3\ldots$ is the β-expansion of $T_\beta(\alpha)$. Now fix a sequence of digits $w = y_1\ldots y_n$ and consider the set I_w of numbers in $[0,1]$ whose β-expansion starts with $y_1\ldots y_n$. If χ_w is the characteristic function of

I_w, then by the pointwise ergodic theorem we know that for μ_β-almost every number $\alpha \in [0,1]$

$$\lim_{k\to\infty} \frac{1}{k} \sum_{i=1}^{k} \chi_w(T_\beta^{i-1}(\alpha)) = \int_{[0,1]} \chi_w \, d\mu_\beta = \int_{I_w} d\mu_\beta \tag{1.1}$$

and this generalises Borel's result on the normality in base b of almost every real number. Indeed, if β is an integer then μ_β is the Lebesgue measure, and if $w = y_1 \dots y_n$ then $\int_{I_w} d\mu_\beta = 1/\beta^n$.

As suggested by Adamczewski and Bugeaud in [1], a possible way to generalise Borel's conjecture on the normality of irrational algebraic numbers is to ask if identity (1.1) holds for every algebraic number in $[0,1]$ which is not a periodic point for the dynamical system $(T_\beta, [0,1], \mu_\beta)$. As for Borel's conjecture, this question is currently without answer, too.

No knowledge of Ergodic Theory is needed to understand the present work after this point. The interested reader is invited to consult [14, Chapters 2 and 4] or [37, Chapters 3 and 5] for an introduction to Ergodic Theory.

1.2 Complexity

Given two real numbers α and $\beta > 1$ define the *complexity function* of the β-expansion of α as the function $p_\alpha^\beta \colon \mathbb{Z}_{>0} \to \mathbb{Z}_{\geq 0}$ that assigns to each positive integer n the number of distinct (possibly overlapping) blocks of n consecutive digits that appear in the β-expansion of α.

Note that if α is normal in base b, then $p_\alpha^b(n) = b^n$ for every $n \geq 1$ (the converse isn't necessarily true). While even showing that $p_\alpha^b(n) = b^n$ for every irrational algebraic α is still out of reach, in 2007 Adamczewski and Bugeaud [2] proved that the complexity function p_α^b of every irrational algebraic number grows more than linearly (see corollary 1.3.2 below).

On the other hand, in 1965 Hartmanis and Stearns [19] proposed another notion of complexity for real numbers, based on a notion of computability introduced by Turing [39]. Namely, they said that a real number α is *computable in time* $T_\alpha(n)$ if there is a multitape Turing machine that can compute the first n terms of the binary expansion of α in at most $T_\alpha(n)$ operations. Further, they say that α is *computable in real time* if one can choose $T_\alpha(n) \in O(n)$.

Clearly all rational numbers are computable in real time, and Hartmanis and Stearns asked if there is any irrational algebraic number which is computable in real time. As far as the present author knows this question has yet to be answered, but in 1968 Cobham [12] proposed to restrict this problem to finite-state automata (see chapter 7 for a definition) and tried to solve it. Loxton and van der Poorten attacked this problem in 1982 [23], and in 1988 [24] they claimed to have proved that the b-ary expansion of any irrational

algebraic number cannot be generated by a finite-state automaton. While their proof was faulty (see Becker [6]), the restricted problem was finally solved by Adamczewski and Bugeaud in 2007 [2].

1.3 The present work

The aforementioned results from Adamczewski's and Bugeaud's paper [2] were based on the following:

Theorem 1.3.1. *Let $\beta > 1$ be a Pisot or Salem integer. Let $\mathbf{a} = (a_i)_{i\geq 1}$ be a bounded sequence of rational integers. If there exists a real number $w > 1$ such that $\mathbf{a}$ satisfies condition $(*)_w$ (see definition 5.0.9), then the real number*

$$\alpha := \sum_{i=1}^{\infty} \frac{a_i}{\beta^i}$$

either belongs to $\mathbb{Q}(\beta)$ or is transcendental.

The goal of the present work was to generalise this theorem, which we did with theorem 5.0.14, and possibly some of its consequences. While we later learned that after [2] Adamczewski and Bugeaud published a result similar to the one we obtained, our proof is original and some of the tools we developed are interesting in and of themselves, notably corollary 4.0.7.

In chapter 2 we recall some generalities about absolute values on a number field.

In chapter 3 we give a brief outline of the Subspace Theorem from Diophantine Approximation and its history. This Subspace Theorem is the main ingredient in the proofs of theorem 1.3.1 and of theorem 5.0.14.

In chapter 4 we develop the tools which we use in chapter 5 to prove our generalisation of theorem 1.3.1.

In chapter 6 we deduce corollary 6.0.19, which generalises some of the results from [2], for instance the following:

Corollary 1.3.2. *Let $b \geq 2$ be an integer. The complexity function of the b-ary expansion of every irrational algebraic number α satisfies*

$$\liminf_{n\to\infty} \frac{p_\alpha^b(n)}{n} = +\infty.$$

Other results from [2] that follow from our corollary 6.0.19 are the generalisation of corollary 1.3.2 to Pisot and Salem integers (corollary 6.0.21), as well as a p-adic analogue of corollary 1.3.2 (corollary 6.0.22).

Finally, in chapter 7 we use theorem 5.0.14 to prove that every k-automatic number is either rational or transcendental.

2 Places and heights

We start by recalling a few notions of algebraic number theory, which we will need to discuss our main results.

Definition 2.0.3. Let $\mathbb{K}$ be an infinite field. An *absolute value* on $\mathbb{K}$ is a function $|\cdot|\colon \mathbb{K} \to \mathbb{R}_{\geq 0}$ such that

1. $|x| = 0$ if and only if $x = 0$;
2. $|xy| = |x||y|$ for every $x, y \in \mathbb{K}$;
3. There is a constant $C \geq 1$ such that $|x+y| \leq C\max\{|x|, |y|\}$ for every $x, y \in \mathbb{K}$.

Further, the absolute value $|\cdot|$ is called *non-archimedean* if it satisfies (3) with $C = 1$, i.e. if it satisfies

$$|x+y| \leq \max\{|x|, |y|\} \quad \forall x, y \in \mathbb{K}.$$

This is called the *ultrametric inequality*. If $|\cdot|$ doesn't satisfy this inequality, then it is said to be *archimedean*.

Note that 2 implies that $|1_{\mathbb{K}}| = 1$, where $1_{\mathbb{K}}$ is the unit of $\mathbb{K}$. An absolute value such that $|x| = 1$ for every $x \in \mathbb{K} \setminus \{0\}$ is said to be *trivial* and from now on we will always assume absolute values to be non-trivial.

Remark 2.0.4. If $|\cdot|$ is non-archimedean and $1_{\mathbb{K}}$ is the unit of $\mathbb{K}$, then $|1_{\mathbb{K}}| = 1$ and the ultrametric inequality imply that $|n \cdot 1_{\mathbb{K}}| \leq 1$ for every $n \in \mathbb{Z}$.

An absolute value on $\mathbb{K}$ gives extra structure to $\mathbb{K}$, in particular it induces a topology on it, and we call the pair $(\mathbb{K}, |\cdot|)$ a *field with absolute value*. A morphism between two fields with absolute value $(\mathbb{K}_1, |\cdot|_1)$ and $(\mathbb{K}_2, |\cdot|_2)$ is just a field morphism $\varphi\colon \mathbb{K}_1 \to \mathbb{K}_2$ which preserves the extra structure, i.e. such that $|x|_1 = |\varphi(x)|_2$ for every $x \in \mathbb{K}_1$.

Definition 2.0.5. Two absolute values $|\cdot|_1$ and $|\cdot|_2$ on $\mathbb{K}$ are said to be *equivalent* if there is a constant $e > 0$ such that

$$|x|_1 = |x|_2^e$$

for every $x \in \mathbb{K}$.

Remark 2.0.6. Two absolute values on $\mathbb{K}$ are equivalent if and only if they induce the same topology on $\mathbb{K}$ (e.g. see [26, proposition II.3.3]).

Definition 2.0.7. Consider a field with absolute value $(\mathbb{K}, |\cdot|)$. An infinite sequence (a_n) with terms in $\mathbb{K}$ is said to *converge* (in $\mathbb{K}$, with respect to $|\cdot|$) if there is an $\alpha \in \mathbb{K}$ such that $\lim_{n\to\infty} |a_n - \alpha| = 0$. Furthermore, (a_n) is said to be *Cauchy* if $\lim_{m,n\to\infty} |a_m - a_n| = 0$, and we say that $(\mathbb{K}, |\cdot|)$ is *complete* if every Cauchy sequence with terms in $\mathbb{K}$ converges in $\mathbb{K}$.

Now, consider a field with absolute value $(\mathbb{K}, |\cdot|)$ which isn't complete and let R be the ring of all Cauchy sequences of $(\mathbb{K}, |\cdot|)$, where addition and multiplication are defined component-wise. The set $\mathfrak{m}$ of sequences converging to 0 is a maximal ideal of R, so the quotient $\widehat{\mathbb{K}} = R/\mathfrak{m}$ is a field. Note that we have a natural inclusion $\mathbb{K} \hookrightarrow \widehat{\mathbb{K}}$ given by sending an element x to the class of the constant sequence $(x, x, \dots)$. Furthermore, we can extend $|\cdot|$ to $\widehat{\mathbb{K}}$ as follows: for every $\alpha \in \widehat{\mathbb{K}}$ represented by a Cauchy sequence (a_n) let

$$|\alpha| := \lim_{n\to\infty} |a_n|$$

which is well defined because $||a_m| - |a_n|| \leq |a_m - a_n|$ implies that $(|a_n|)$ is a Cauchy sequence in $\mathbb{R}$ (with respect to the usual absolute value). Finally, it can be shown that $\widehat{\mathbb{K}}$ is complete with respect to $|\cdot|$ and that it is the smallest (with respect to inclusion of fields with absolute value) complete field containing $(\mathbb{K}, |\cdot|)$. Thus the field $(\widehat{K}, |\cdot|)$ is said to be the *completion* of $\mathbb{K}$ with respect to $|\cdot|$.

Remark 2.0.8. A theorem by Ostrowski shows that for every field $\mathbb{K}$ complete with respect to an archimedean absolute value $|\cdot|_{\mathbb{K}}$ there are a constant $s > 0$ and an injective homomorphism σ of $\mathbb{K}$ to either $\mathbb{R}$ or $\mathbb{C}$ such that $|x|_{\mathbb{K}} = |\sigma(x)|^s$ for every $x \in \mathbb{K}$ (e.g. see [26, theorem II.4.2]).

Example 2.0.9. Consider $\mathbb{K} = \mathbb{Q}$. For every $x \in \mathbb{Q}$ and for every prime number p define the absolute values

$$|x|_\infty := \max(x, -x)$$
$$|x|_p := p^{-\operatorname{ord}_p(x)}$$

where $\operatorname{ord}_p(x)$ is the unique integer such that $x = p^{\operatorname{ord}_p(x)} a/b$ with $a, b \in \mathbb{Z}$ and $p \nmid ab$, and where for every p we define $|0|_p = 0$.

We see that $|\cdot|_\infty$ is archimedean and the completion of $\mathbb{Q}$ with respect to it is $\mathbb{Q}_\infty := \mathbb{R}$, while for every prime p the absolute value $|\cdot|_p$ is non-archimedean and the completion of $\mathbb{Q}$ with respect to it is denoted by $\mathbb{Q}_p$ and called the field of *p-adic numbers*. Furthermore,

by another of Ostrowski's theorems we know that every absolute value on $\mathbb{Q}$ is equivalent to either $|\cdot|_\infty$ or $|\cdot|_p$ for some prime number p (e.g. see [26, proposition II.3.7]).

Finally, note that these absolute values satisfy the so-called *product formula*

$$|x|_\infty \prod_{p \text{ prime}} |x|_p = 1 \quad \forall x \in \mathbb{Q}^*.$$

Consider a field with absolute value $(\mathbb{K}, |\cdot|)$. If $\mathbb{L}$ is a field extension of $\mathbb{K}$, we say that an absolute value $|\cdot|_\mathbb{L}$ on $\mathbb{L}$ is an *extension* of $|\cdot|$ if its restriction to $\mathbb{K}$ coincides with $|\cdot|$. We have the following:

Proposition 2.0.10. *If $(\mathbb{K}, |\cdot|)$ is a complete field with absolute value and $\mathbb{L}$ is any algebraic extension of $\mathbb{K}$, then $|\cdot|$ can be extended in a unique way (up to equivalence) to $\mathbb{L}$. Furthermore, if $\mathbb{L}$ is finite over $\mathbb{K}$ we have that*

$$|x| = \left|N_{\mathbb{L}/\mathbb{K}}(x)\right|^{1/[\mathbb{L}:\mathbb{K}]}$$

for every $x \in \mathbb{L}$ and $\mathbb{L}$ is complete with respect to this absolute value.

On the other hand, if $\mathbb{L}$ is an algebraic closure of $\mathbb{K}$ we have $|x| = |\sigma(x)|$ for every $x \in \mathbb{L}$ and $\tau \in \mathrm{Gal}(\mathbb{L}, \mathbb{K})$.

Proof. See [26, theorem II.4.8]. □

Remark 2.0.11. Even if $(\mathbb{K}, |\cdot|)$ is not complete we can always extend $|\cdot|$ to any algebraic extension $\mathbb{L}$ of $\mathbb{K}$, because $\mathbb{L}$ is always contained in some algebraic extension of $\widehat{\mathbb{K}}$, but this absolute value may not be unique (up to equivalence).

For example consider $\mathbb{K} = \mathbb{Q}$, φ_1 and φ_2 the golden ratio and its conjugate, and $\mathbb{L} = \mathbb{Q}(\varphi_1)$. Then for $i = 1, 2$ let $\sigma_i \colon \mathbb{L} \to \mathbb{R}$ be the embedding such that $\varphi_1 \mapsto \varphi_i$ and observe that the absolute values $|\cdot|_1, |\cdot|_2$ on $\mathbb{L}$ defined by $|x|_i := |\sigma_i(x)|$ cannot be equivalent, because $|\varphi_1|_1 > 1$ but $|\varphi_1|_2 < 1$.

2.1 Places on a number field

From now on $\mathbb{K}$ will be an algebraic number field, unless otherwise stated.

Definition 2.1.1. A *real place* of $\mathbb{K}$ a set $\{\sigma\}$ where $\sigma \colon \mathbb{K} \to \mathbb{R}$ is a real embedding of $\mathbb{K}$, while a *complex place* of $\mathbb{K}$ is a set $\{\sigma, \bar{\sigma}\}$ where $\sigma, \bar{\sigma} \colon \mathbb{K} \to \mathbb{C}$ is a pair of conjugate complex embeddings of $\mathbb{K}$.

An *infinite place* of $\mathbb{K}$ is either a real or complex place, while a *finite place* of $\mathbb{K}$ is a non-zero prime ideal $\mathfrak{p}$ of $\mathscr{O}_\mathbb{K}$. We denote by $M_\mathbb{K}$, $M_\mathbb{K}^\infty$, and $M_\mathbb{K}^0$ the sets of places, infinite places, and finite places of $\mathbb{K}$, respectively.

Remark 2.1.2. If r_1 and r_2 are the numbers of real and complex places of $\mathbb{K}$, respectively, then we know that $r_1 + 2r_2 = [\mathbb{K} : \mathbb{Q}]$.

Similarly to what we did for $\mathbb{Q}$ in example 2.0.9, for each place v of $\mathbb{K}$ we can define an absolute value $|\cdot|_v$ as follows (for every $x \in \mathbb{K}$):

$$\begin{aligned} |x|_v &:= |\sigma(x)| && \text{if } v = \{\sigma\} \text{ is real} \\ |x|_v &:= |\sigma(x)|^2 = |\bar{\sigma}(x)|^2 && \text{if } v = \{\sigma, \bar{\sigma}\} \text{ is complex} \\ |x|_v &:= N_K(\mathfrak{p})^{-\operatorname{ord}_{\mathfrak{p}}(x)} && \text{if } v = \mathfrak{p} \text{ is finite} \end{aligned}$$

where $N_K(\mathfrak{p}) = |\mathscr{O}_{\mathbb{K}}/\mathfrak{p}|$ is the absolute norm of $\mathfrak{p}$, $\operatorname{ord}_{\mathfrak{p}}(x)$ is the exponent of $\mathfrak{p}$ in the prime factorisation of (x), and where for every $\mathfrak{p}$ we define $|0|_{\mathfrak{p}} = 0$.

Remark 2.1.3. Let $\rho : \mathbb{L} \to \mathbb{K}$ be an isomorphism of algebraic number fields and consider a place v of $\mathbb{K}$. Then we can define a place $v \circ \rho$ of $\mathbb{L}$ by

$$v \circ \rho := \begin{cases} \{\sigma\rho\} & \text{if } v = \{\sigma\} \text{ is real} \\ \{\sigma\rho, \bar{\sigma}\rho\} & \text{if } v = \{\sigma, \bar{\sigma}\} \text{ is complex} \\ \rho^{-1}(\mathfrak{p}) & \text{if } v = \mathfrak{p} \text{ is finite} \end{cases}$$

and the corresponding absolute value is $|x|_{v\circ\rho} = |\rho(x)|_v$ for every $x \in \mathbb{L}$.

Remark 2.1.4. It can be showed that every algebraic number field which is complete with respect to a non-archimedean absolute value is isomorphic (as a field with absolute value) to a finite extension of $\mathbb{Q}_p$ for some prime number p (e.g. see [26, proposition II.5.2]).

Note that for any pair of distinct places u, v of $\mathbb{K}$ the absolute values $|\cdot|_u$ and $|\cdot|_v$ cannot be equivalent. Moreover, using the results mentioned in remarks 2.0.8 and 2.1.4 one can prove that the completion $\mathbb{K}_v$ of $\mathbb{K}$ with respect to $|\cdot|_v$ is isomorphic to:

- $\mathbb{R}$ if v is a real place;
- $\mathbb{C}$ if v is a complex place;
- a finite extension of $\mathbb{Q}_p$ if $v = \mathfrak{p}$ is a finite place and $\mathfrak{p} \cap \mathbb{Z} = (p)$.

Remark 2.1.5. Any archimedean absolute value $|\cdot|_{\mathbb{K}}$ on $\mathbb{K}$ is equivalent to $|\cdot|_v$ for some $v \in M_{\mathbb{K}}^{\infty}$. Indeed, consider the completion $\widehat{\mathbb{K}}$ and the natural inclusion $\iota : \mathbb{K} \to \widehat{\mathbb{K}}$. Then by remark 2.0.8 we know that $\widehat{\mathbb{K}}$ is isomorphic to either $\mathbb{R}$ or $\mathbb{C}$: in the first case $|\cdot|_{\mathbb{K}}$ is equivalent to $|\iota(\cdot)| = |\cdot|_v$ with $v = \{\iota\}$ a real place, while in the second case $|\cdot|_{\mathbb{K}}$ is equivalent to $|\iota(\cdot)| = |\cdot|_v$ with $v = \{\iota, \bar{\iota}\}$ a complex place.

Remark 2.1.6. Let x be a non-zero element of $\mathbb{K}$. Then the Chinese Remainder Theorem and $|\mathscr{O}_{\mathbb{K}}/(p^e)| = p^{e[\mathbb{K}:\mathbb{Q}]}$ imply that $N_{\mathbb{K}}((x)) = |\mathscr{O}_{\mathbb{K}}/(x)| = \left|N_{\mathbb{K}|\mathbb{Q}}(x)\right|$. This, combined with the product formula for $\mathbb{Q}$, gives the *product formula* for $\mathbb{K}$:

$$\prod_{v \in M_{\mathbb{K}}} |x|_v = 1 \quad \forall x \in \mathbb{K}^*.$$

Remark 2.1.7. The following inequality is sometimes useful:

$$|x_1 + \cdots + x_n|_v \leq n^{e_v} \max(|x_1|_v, \ldots, |x_n|_v) \quad \forall v \in M_{\mathbb{K}} \quad \forall x_1, \ldots, x_n \in \mathbb{K}$$

where e_v is 1 if v is real, 2 if v is complex, and 0 if v is finite. In particular, $\sum_{v \in M_{\mathbb{K}}^{\infty}} e_v = [\mathbb{K} : \mathbb{Q}]$.

Definition 2.1.8. Consider a finite extension $\mathbb{L} \supset \mathbb{K}$ of number fields and places v, V of $\mathbb{K}, \mathbb{L}$, respectively. We say that V *lies above* v (or that v *lies below* V) if the restriction of $|\cdot|_V$ to $\mathbb{K}$ is a power of $|\cdot|_v$.

Remark 2.1.9. This happens precisely when v, V are archimedean and the embeddings of v are the restriction of the embeddings of V, or if $v = \mathfrak{p}$ and $V = \mathfrak{P}$ are prime ideals of $\mathscr{O}_{\mathbb{K}}$ and $\mathscr{O}_{\mathbb{L}}$, respectively, such that $\mathfrak{P} \supset \mathfrak{p}$.

Furthermore, if V lies over v the completion $\mathbb{L}_V$ is a finite extension of $\mathbb{K}_v$. Indeed, if v and V are infinite then $[\mathbb{L}_V : \mathbb{K}_v]$ is 1 or 2, while if $v = \mathfrak{p}$ and $V = \mathfrak{P}$ are finite we have $[\mathbb{L}_V : \mathbb{K}_v] = e(\mathfrak{P}|\mathfrak{p}) f(\mathfrak{P}|\mathfrak{p})$, where $e(\mathfrak{P}|\mathfrak{p})$ and $f(\mathfrak{P}|\mathfrak{p})$ denote the ramification index and residue class degree of $\mathfrak{P}$ over $\mathfrak{p}$.

Proposition 2.1.10. *Consider a finite extension $\mathbb{L} \supset \mathbb{K}$ of number fields. Further, let v be a place of $\mathbb{K}$ and let $V_1, \ldots, V_g$ be the places of $\mathbb{L}$ lying over v. Then*

$$|\alpha|_{V_k} = |\alpha|_v^{[\mathbb{L}_{V_k} : \mathbb{K}_v]} \quad \textit{for all } \alpha \in \mathbb{K}, k \in \{1, \ldots, g\} \tag{2.1}$$

$$\prod_{k=1}^{g} |\alpha|_{V_k} = \left|N_{\mathbb{L}/\mathbb{K}}(\alpha)\right|_v \quad \textit{for all } \alpha \in \mathbb{L} \tag{2.2}$$

$$\sum_{k=1}^{g} [\mathbb{L}_{V_k} : \mathbb{K}_v] = [\mathbb{L} : \mathbb{K}]. \tag{2.3}$$

Proof. This is clear if v and V are infinite, thus suppose that $v = \mathfrak{p}$ and $V_k = \mathfrak{P}_k$ ($k \in \{1, \ldots, g\}$) are finite, with $\mathfrak{P}_k \supset \mathfrak{p}$. Then (2.1) follows from the fact that for every $\alpha \in \mathbb{K}$ and $k \in \{1, \ldots, g\}$ we have

$$|\alpha|_{V_k} = N_L(\mathfrak{P}_k)^{-\operatorname{ord}_{\mathfrak{P}_k}(\alpha)} = N_K(\mathfrak{p})^{-e(\mathfrak{P}_k|\mathfrak{p}) f(\mathfrak{P}_k|\mathfrak{p}) \operatorname{ord}_{\mathfrak{P}_k}(\alpha)} = |\alpha|_v^{[\mathbb{L}_{V_k} : \mathbb{K}_v]}.$$

For the second identity see [21, Chapter II, section 6], while (2.3) follows from the other two identities, because for $\alpha \in \mathbb{K}^*$ we have

$$|\alpha|_v^{\sum_{k=1}^g [\mathbb{L}_{V_k}:\mathbb{K}_v]} = \prod_{k=1}^g |\alpha|_{V_k} = \left|N_{\mathbb{L}/\mathbb{K}}(\alpha)\right|_v = |\alpha|_v^{[\mathbb{L}:\mathbb{K}]}. \qquad \square$$

2.2 Heights and S-units

Definition 2.2.1. Let S be a finite set of places of $\mathbb{K}$ which contains all the infinite places. An $x \in \mathbb{K}$ is said to be an *S-integer* if $|x|_v \leq 1$ for every place not in S. The S-integers form a ring, denoted by $\mathscr{O}_S$. The units in $\mathscr{O}_S$ are called *S-units* and their group is denoted by $\mathscr{O}_S^*$.

Remark 2.2.2. If $S = M_{\mathbb{K}}^\infty$ then by remark 2.0.4 we know that $\mathscr{O}_S = \mathscr{O}_{\mathbb{K}}$ and $\mathscr{O}_S^* = \mathscr{O}_{\mathbb{K}}^*$. Otherwise $S = M_{\mathbb{K}}^\infty \cup \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ and $\mathscr{O}_S = \mathscr{O}_{\mathbb{K}}[(\mathfrak{p}_1 \cdots \mathfrak{p}_r)^{-1}]$, while the S-units are precisely the elements x of $\mathbb{K}$ such that all the prime factors of (x) are in $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$.

Example 2.2.3. If $\mathbb{K} = \mathbb{Q}$ and $S = \{\infty, p_1, \ldots, p_r\}$, then $\mathbb{Z}_S = \mathbb{Z}[(p_1 \cdots p_r)^{-1}]$ and

$$\mathbb{Z}_S^* = \{x = \pm p_1^{e_1} \cdots p_r^{e_r} \in \mathbb{Q} : e_1, \ldots, e_r \in \mathbb{Z}\}.$$

2.2.1 S-norm and S-height

Definition 2.2.4. Fix a set S as in definition 2.2.1. The *S-norm* of $x \in \mathbb{K}$ is

$$N_S(x) := \prod_{v \in S} |x|_v.$$

Observe that the S-norm is multiplicative. Moreover, suppose that $S = M_{\mathbb{K}}^\infty \cup \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ and consider an $x \in \mathbb{K}^*$. Then there are some integers $e_1, \ldots, e_r$ and a fractional ideal $\mathfrak{a}$ of $\mathscr{O}_{\mathbb{K}}$ such that

$$(x) = \mathfrak{p}_1^{e_1} \cdots p_r^{e_r} \mathfrak{a}$$

and $\mathfrak{p}_i \nmid \mathfrak{a}$ for every $i \in \{1, \ldots, r\}$. Thus by the product formula we have

$$N_S(x) = \prod_{v \notin S} |x|_v^{-1} = \prod_{\mathfrak{p} \in M_{\mathbb{K}}^0 \setminus \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}} N_{\mathbb{K}}(\mathfrak{p})^{\mathrm{ord}_{\mathfrak{p}}(x)} = N_{\mathbb{K}}(\mathfrak{a}).$$

Remark 2.2.5. In particular, if ε is an S-unit then $\mathfrak{a} = \mathscr{O}_{\mathbb{K}}$, so $N_S(\varepsilon) = 1$.

Now consider a finite extension $\mathbb{L}$ of $\mathbb{K}$ and

$$T = M_{\mathbb{L}}^{\infty} \cup P_1 \cup \cdots \cup P_r$$

where P_i is the set of prime ideals $\mathfrak{P}$ of $\mathscr{O}_{\mathbb{L}}$ lying above $\mathfrak{p}_i$, i.e. such that $\mathfrak{P} \cap \mathscr{O}_{\mathbb{K}} = \mathfrak{p}_i$, for every $i \in \{1, \ldots, r\}$. Then $\mathscr{O}_T$ is the integral closure in $\mathbb{L}$ of $\mathscr{O}_S$ and

$$N_T(x) = N_{\mathbb{L}}(\mathfrak{a}\mathscr{O}_{\mathbb{L}}) = N_{\mathbb{K}}(\mathfrak{a})^{[\mathbb{L}:\mathbb{K}]} = N_S(x)^{[\mathbb{L}:\mathbb{K}]}$$

for every $x \in \mathbb{K}^*$.

Definition 2.2.6. We define the *S-height* of $\mathbf{x} = (x_1, \ldots, x_n) \in \mathscr{O}_S^n$ as

$$H_S(\mathbf{x}) = H_S(x_1, \ldots, x_n) := \prod_{v \in S} \max(|x_1|_v, \ldots, |x_n|_v).$$

Note that if $n = 1$ then $H_S(x) = N_S(x)$.

Remark 2.2.7. For every $\varepsilon \in \mathscr{O}_S^*$ and for every $\mathbf{x} = (x_1, \ldots, x_n) \in \mathscr{O}_S^n$ we have

$$H_S(\varepsilon \mathbf{x}) = \prod_{v \in S} \max(|\varepsilon x_1|_v, \ldots, |\varepsilon x_n|_v) = N_S(\varepsilon) H_S(\mathbf{x}) = H_S(\mathbf{x}).$$

2.2.2 Absolute heights

In this section consider a fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$.

Definition 2.2.8. The *absolute (multiplicative) height* of a number $\alpha \in \overline{\mathbb{Q}}$ is defined as

$$H(\alpha) := \prod_{v \in M_{\mathbb{K}}} \max(1, |\alpha|_v)^{1/[\mathbb{K}:\mathbb{Q}]}$$

where $\mathbb{K} \subset \overline{\mathbb{Q}}$ is any number field containing α. Furthermore, the *absolute logarithmic height* of α is $h(\alpha) := \log H(\alpha)$.

Note that (2.2) from proposition 2.1.10 implies that $H(\alpha)$ is independent from the choice of field containing α.

Now fix a number field $\mathbb{K}$. Then for every $\alpha \in \mathbb{K}^*$ we immediately see that

$$h(\alpha) = \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_{v \in M_{\mathbb{K}}} \log\left(\max(1, |\alpha|_v)\right).$$

Lemma 2.2.9. *Consider $\alpha, \alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$, $m \in \mathbb{Z}$, and an automorphism σ of $\overline{\mathbb{Q}}$. Then*

1. $h(\sigma(\alpha)) = h(\alpha)$;

2. $h(\alpha_1 \cdots \alpha_n) \leq \sum_{i=1}^{n} h(\alpha_i)$;

3. $h(\alpha_1 + \cdots + \alpha_n) \leq \log(n) + \sum_{i=1}^{n} h(\alpha_i)$;

4. $h(\alpha^m) = |m| h(\alpha)$ *if* $\alpha \neq 0$.

Proof. The first property is a direct consequence of remark 2.1.3. The second follows from

$$\max(1, xy) \leq \max(1, x) \max(1, y)$$

for every $x, y > 0$. The fourth property follows from $\max(1, x^n) = \max(1, x)^n$ for every $x \in \mathbb{R}$. And finally the third property follows from remark2.1.7 because if $\mathbb{K}$ is an algebraic number field which contains $\alpha_1, \ldots, \alpha_n$, then

$$\begin{aligned}
h(\alpha_1 + \cdots + \alpha_n) &= \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_{v \in M_{\mathbb{K}}} \log\left(\max(1, |\alpha_1 + \cdots + \alpha_n|_v)\right) \\
&\leq \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_{v \in M_{\mathbb{K}}} \log\left(\max\left(1, n^{e_v} \max(|\alpha_1|_v, \ldots, |\alpha_n|_v)\right)\right) \\
&\leq \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_{v \in M_{\mathbb{K}}} e_v \log(n) + \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_{v \in M_{\mathbb{K}}} \log\left(\max(1, |\alpha_1|_v, \ldots, |\alpha_n|_v)\right) \\
&\leq \log(n) + \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_{v \in M_{\mathbb{K}}} \log\left(\max(1, |\alpha_1|_v) \cdots \max(1, |\alpha_n|_v)\right) \\
&= \log(n) + \sum_{i=1}^{n} h(\alpha_i).
\end{aligned}$$

□

3 The Subspace Theorem

For our main result we will need to prove a corollary of (one form of) a powerful and versatile theorem, known as the Subspace Theorem. Following the excellent Bourbaki talk [7] by Y. Bilu, to give it some context and motivation we will start with a few special cases.

From now on $\overline{\mathbb{Q}}$ is the set of algebraic numbers in $\mathbb{C}$ and for every absolute value on $\mathbb{Q}$ we choose an extension to $\overline{\mathbb{Q}}$. Furthermore, $\mathbb{K}$ is a fixed algebraic number field, $\overline{\mathbb{K}}$ a fixed algebraic closure of $\mathbb{K}$, and for every absolute value on $\mathbb{K}$ we choose an extension to $\overline{\mathbb{K}}$.

3.1 Roth's theorem

Recall that by Dirichlet's approximation theorem the inequality

$$\left|\alpha - \frac{x}{y}\right| \leq |y|^{-2}$$

has infinitely many solutions in coprime non-zero integers x, y whenever α is an irrational number. In 1955 K. F. Roth [29] showed that, in some sense, this is the best possible case when α is algebraic; namely, he proved the following:

Theorem 3.1.1 (Roth)**.** *If α is a real algebraic number of degree $d \geq 3$, then for every $\varepsilon > 0$ there is a constant $c(\alpha, \varepsilon) > 0$ such that*

$$\left|\alpha - \frac{x}{y}\right| \geq c(\alpha, \varepsilon) \max(|x|, |y|)^{-2-\varepsilon} \tag{3.1}$$

for every $x, y \in \mathbb{Z}$ with $y \neq 0$.

Remark 3.1.2. Note that Roth's theorem holds if α is rational or quadratic, too (as long as $\frac{x}{y} \neq \alpha$), but then it is weaker than (3.2) below. Also, it trivially holds even if $\alpha \in \mathbb{C} \setminus \mathbb{R}$, because then $|\alpha - \xi| \geq \mathrm{Im}(\alpha)$ for every $\xi \in \mathbb{Q}$.

This theorem has a long history. Already in 1855 Liouville proved the existence of a constant $c(\alpha) > 0$ such that

$$|\alpha - \xi| \geq c(\alpha) H(\xi)^{-d} \tag{3.2}$$

for every $\xi \in \mathbb{Q}$ with $\xi \neq \alpha$, where α is an algebraic number of degree d. Liouville's result is too weak for many applications in Diophantine Approximation, though. In 1909 A. Thue showed [38] the existence of a constant $c(\alpha,\varepsilon) > 0$ such that (3.1) holds for every $\varepsilon > d/2 - 1$ when α is an algebraic number of degree $d \geq 3$. In 1921 C. L. Siegel [36] refined this to $\varepsilon \geq 2\sqrt{d} - 2$, in 1949 A. O. Gel'fond and F. Dyson independently improved this to $\varepsilon > \sqrt{2d} - 2$, and in 1955 Roth made the final step. However, it should be noted that Liouville's result is effective, meaning that it gives a way to compute the constant $c(\alpha)$ explicitly, while those of Thue, Gel'fond, Dyson, and Roth are not.

In 1958 D. Ridout [28], then a student of K. Mahler, extended Roth's theorem to the case of non-archimedean absolute values by proving the following:

Theorem 3.1.3 (Ridout)**.** *Let S be a finite set of places of $\mathbb{Q}$ containing the infinite place and for each $v \in S$ fix an algebraic number α_v. Then for every $\varepsilon > 0$ the inequality*

$$\prod_{v \in S} \min\left\{1, \left|\alpha_v - \frac{x}{y}\right|_v\right\} < \max(|x|,|y|)^{-2-\varepsilon}$$

has at most finitely many solutions $x, y \in \mathbb{Z}$ with $y \neq 0$.

Finally, it is worth noting that S. Lang extended the theorems of Roth and Ridout to cover approximation of algebraic numbers by elements of a fixed number field. The interested reader may find the statement and proof of this theorem in Lang's classic book [22, Chapter 7] or in the more recent volume [20, Part D] by Hindry and Silverman.

3.2 Statement of the Subspace Theorem

Recall that n linear forms in m variables

$$L_1 = a_{1,1}X_1 + \cdots + a_{m,1}X_m\,,\ \ \ldots\,,\ \ L_n = a_{1,n}X_1 + \cdots + a_{m,n}X_m$$

with coefficients in some field F are said to be *linearly independent* if and only if the vectors

$$(a_{1,1},\ldots,a_{m,1})\,,\ \ \ldots\,,\ \ (a_{1,n},\ldots,a_{m,n})$$

are linearly independent in F^m.

In 1972 W. M. Schmidt [34] proved the following (see also his lecture notes [35])

Theorem 3.2.1 (Subspace Theorem, Schmidt)**.** *Fix $n \geq 2$ and consider linearly independent linear forms $L_1,\ldots,L_n$ in n variables with coefficients in $\overline{\mathbb{Q}}$. Then for every $C > 0$ and $\varepsilon > 0$ the solutions of*

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

lie in the union of finitely many proper subspaces of $\mathbb{Q}^n$, where $\|\mathbf{x}\| := \max(|x_1|,\ldots,|x_n|)$.

Note that with $n = 2$, $L_1(x,y) = x\alpha - y$, and $L_2(x,y) = x$ we recover Roth's theorem. Still, this result proved insufficient for many applications and it was later generalised by H. P. Schlickewei [30, 31], similarly to how Ridout generalised Roth's theorem.

Theorem 3.2.2 (Subspace Theorem, Schlickewei)**.** *Let S be a finite set of places of $\mathbb{Q}$, including the infinite place, and for every $v \in S$ let $L_{1,v}, \dots, L_{n,v}$ be linearly independent linear forms in n variables with coefficients in $\overline{\mathbb{Q}}$. Then for any fixed $\varepsilon > 0$ the solutions of*

$$\prod_{v \in S} \prod_{i=1}^{n} |L_{i,v}(\mathbf{x})|_v \leq H_S(\mathbf{x})^{-\varepsilon} \text{ with } \mathbf{x} \in \mathbb{Z}_S^n \setminus \{\mathbf{0}\}$$

lie in the union of finitely many proper linear subspaces of $\mathbb{Q}^n$.

Unfortunately, even this formulation proved insufficient for many applications: one needs to extend it to the case where the variables $x_1, \dots, x_n$ are chosen from an arbitrary number field. This, too, was done by Schlickewei [32].

Theorem 3.2.3 (p-adic Subspace Theorem)**.** *Let S be a finite set of places of $\mathbb{K}$ containing all the infinite places. Further for each $v \in S$ let $L_{1,v}, \dots, L_{n,v}$ be linearly independent linear forms in $X_1, \dots, X_n$ with coefficients from $\overline{\mathbb{K}}$. Then for any fixed $\varepsilon > 0$ the solutions of*

$$\prod_{v \in S} \prod_{i=1}^{n} |L_{i,v}(\mathbf{x})|_v \leq H_S(\mathbf{x})^{-\varepsilon} \text{ with } \mathbf{x} \in \mathscr{O}_S^n \setminus \{\mathbf{0}\} \tag{3.3}$$

lie in the union of finitely many proper linear subspaces of $\mathbb{K}^n$.

A detailed proof of this theorem can be found in the recent book [8] by E. Bombieri and W. Gubler. The interested reader is invited to consult this very book or Bilu's Bourbaki talk [7] for a flavour of the many interesting applications of this theorem.

Finally, it is important to mention that the proofs of all of these results are ineffective, in that they don't provide a way to actually determine the involved subspaces. There are some quantitative versions of the Subspace Theorem, though, obtained by J. H. Evertse, H. P. Schlickewei, and R. G. Ferretti that give an upper bound on the number of subspaces (see for example [17] or [16]).

4 A useful lemma

Again, in what follows $\mathbb{K}$ is assumed to be an algebraic number field.

Definition 4.0.4. Let $J_n = \{1,\dots,n\}$. A sum $y = x_1 + \ldots + x_n$ is said to be *non-degenerate* if it is non-zero and every subsum is non-zero, i.e. if for every non-empty subset $I \subseteq J_n$ we have $\sum_{i\in I} x_i \neq 0$. Further, given $I \subseteq J_n$ we shall call y an *I-sum* if $\sum_{i\in I} x_i$ is non-degenerate and equal to y.

Lemma 4.0.5 (Key)**.** *Let $\mathscr{S}$ be any finite set of places of $\mathbb{K}$. For each $v \in \mathscr{S}$ consider a linear form $L_v = \alpha_v(X_1 + \cdots + X_n) - X_{n+1}$ with α_v algebraic not in $\mathbb{K}$ and let $L_v = X_{n+1}$ for $v \in M_{\mathbb{K}}^{\infty} \setminus \mathscr{S}$. Further, let $S = M_{\mathbb{K}}^{\infty} \cup \mathscr{S}$. Then for any fixed $\varepsilon > 0$*

$$\prod_{v\in S} |L_v(\mathbf{x})|_v \leq H_S(\mathbf{x})^{-\varepsilon} \tag{4.1}$$

has, up to multiplication by S-units, only finitely many non-degenerate solutions $\mathbf{x} \in (\mathscr{O}_S^*)^n \times (\mathscr{O}_S \setminus \{0\})$, i.e. solutions such that $x_1 + \ldots + x_n$ is non-degenerate.

Proof. First note that, since $x_1,\dots,x_n$ are all S-units by hypothesis, (4.1) is equivalent to

$$\prod_{v\in S} |x_1 \cdots x_n L_v(\mathbf{x})|_v \leq H_S(\mathbf{x})^{-\varepsilon} \tag{4.2}$$

and that the solutions of (4.2) lie in the union of finitely many proper linear subspaces of $\mathbb{K}^{n+1}$ by the p-adic Subspace Theorem. Let T be one such subspace, with equation, say, $\theta_1 X_1 + \ldots + \theta_{n+1} X_{n+1} = 0$.

If $\theta_{n+1} \neq 0$ then we can assume without loss of generality that $\theta_{n+1} = -1$. Furthermore, since we are considering only solutions with $x_{n+1} \neq 0$, at least another one of $\theta_1,\dots,\theta_n$ must be non-zero, say θ_n. Also note that $\alpha_v - \theta_i \neq 0$ for every $i \in \{1,\dots,n\}$ and for every $v \in \mathscr{S}$ because $\alpha_v \notin \mathbb{K}$ by hypothesis. Now consider the linear forms

$$\begin{cases} L'_v = (\alpha_v - \theta_1)X_1 + \cdots + (\alpha_v - \theta_n)X_n & \text{if } v \in \mathscr{S} \\ L'_v = \theta_1 X_1 + \cdots + \theta_n X_n & \text{otherwise} \end{cases}$$

and observe that

$$\operatorname{rank}\{X_1,\dots,X_{n-1},L'_v\} = n \quad \text{for every } v \in S.$$

Moreover, if $\mathbf{x} = (x_1, \ldots, x_{n+1})$ is a solution of (4.2) in T, then $\mathbf{x}' = (x_1, \ldots, x_n)$ is a solution of

$$\prod_{v \in S} \left| x_1 \cdots x_{n-1} L'_v(\mathbf{x}') \right|_v \leq H_S(\mathbf{x}')^{-\varepsilon} \tag{4.3}$$

because $H_S(\mathbf{x}') \leq H_S(\mathbf{x})$. By the p-adic Subspace Theorem we know that the solutions of (4.3) lie in the union of finitely many proper linear subspaces of $\mathbb{K}^n$, and viewing any such subspace as a proper linear subspace of $\mathbb{K}^{n+1}$ we can then reduce to the following case:

If $\theta_{n+1} = 0$ then without loss of generality we may assume $\theta_n = 1$. Now, for every $j \in \{1, \ldots, n-1\}$ define $\theta'_j := 1 - \theta_j$ and note that at least one of the θ'_j must be non-zero because otherwise every solution in T would be degenerate. Further, up to adding finitely many finite places to S, we may assume that each non-zero θ'_j is an S-unit.

We proceed by induction on n, observing that there are no solutions in T for $n = 1$, because $u \neq 0$ for every $u \in \mathscr{O}_S^*$. Then suppose $n > 1$. For any non-empty subset $I \subseteq J_{n-1} = \{1, \ldots, n-1\}$ define an *I-solution* (of (4.1) in T) as a non-degenerate solution $\mathbf{x} \in T$ of (4.1) such that $\theta'_1 x_1 + \cdots + \theta'_{n-1} x_{n-1}$ is an I-sum. Further, let

$$\begin{cases} L_{v,I} = \alpha_v(\sum_I X_i) - X_{n+1} & \text{if } v \in \mathscr{S} \\ L_{v,I} = X_{n+1} & \text{otherwise.} \end{cases}$$

Now note that if $\mathbf{x} = (x_1, \ldots, x_{n+1})$ is a non-degenerate solution of (4.1), then there is a non-empty $I \subseteq J_{n-1}$ such that $\mathbf{x}$ is an I-solution. Hence $\mathbf{x}' = (\theta'_i x_i \, (i \in I); x_{n+1})$ is a non-degenerate solution of

$$\prod_{v \in S} \left| L_{v,I}(\mathbf{x}') \right|_v = \prod_{v \in S} |L_v(\mathbf{x})|_v \leq H_S(\mathbf{x})^{-\varepsilon} \ll_{\{\theta_i\}_I} H_S(\mathbf{x}')^{-\varepsilon}$$

so by the induction hypothesis we deduce that there are only finitely many possible values for $(\frac{x_i}{x_n})_{i \in I}$. Then fix a tuple $(d_i)_{i \in I}$ of such values and let $D = 1 + \sum_I d_i$. Further, observe that $D \neq 0$ because $\mathbf{x}$ is non-degenerate, so up to adding finitely many finite places to S we may assume $D \in \mathscr{O}_S^*$. Then let

$$\begin{cases} L_v^I = \alpha_v\big(\sum_{J_{n-1} \setminus I} X_j + X_n\big) - X_{n+1} & \text{if } v \in \mathscr{S} \\ L_v^I = X_{n+1} & \text{otherwise} \end{cases}$$

and note that $\mathbf{x}$ non-degenerate implies that $\mathbf{x}'' = (x_j, Dx_n, x_{n+1})_{j \in J_{n-1} \setminus I}$ is a non-degenerate solution of

$$\prod_{v \in S} \left| L_v^I(\mathbf{x}'') \right|_v = \prod_{v \in S} |L_v(\mathbf{x})|_v \leq H_S(\mathbf{x})^{-\varepsilon} \ll_D H_S(\mathbf{x}'')^{-\varepsilon}$$

hence, again by the induction hypothesis, we conclude that there are only finitely many possible choices for $\mathbf{x}$ up to multiplication by an S-unit. This is enough to prove the lemma because J_{n-1} has only finitely many (non-empty) subsets. □

Remark 4.0.6. Note that if $u \in \mathscr{O}_S^*$, then $L_v(u\mathbf{x}) = uL_v(\mathbf{x})$ for every $v \in S$. Hence if $\mathbf{x}$ is a solution of (4.1), then $u\mathbf{x}$ is a solution, too. Therefore if $\#S > 1$, then (4.1) has either infinitely many solutions (overall) or no solution at all.

Corollary 4.0.7. *Let S, T be finite sets of places of $\mathbb{K}$ such that S contains all the infinite places. Further, for every $v \in T$ fix an algebraic number α_v not in $\mathbb{K}$. Then for every fixed $\varepsilon > 0$ and $M > 0$*

$$\prod_{v \in T} \left| \alpha_v - \frac{x}{y} \right|_v < H_S(x,y)^{-1-\varepsilon} \tag{4.4}$$

has, up to multiplication by an S-unit, at most finitely many solutions in $x \in \mathscr{O}_S \setminus \{0\}$ and y a non-degenerate sum of at most M S-units.

Proof. First note that we may assume $T \subseteq S$. Indeed, $|x|_v \leq 1$ and $|y|_v \leq 1$ for every $v \in T \setminus S$ because $x, y \in \mathscr{O}_S$. Thus $H_S(x,y) \geq H_{S \cup T}(x,y)$.

Now suppose that x, y is a solution of (4.4) with y the non-degenerate sum of $u_1, \ldots, u_n \in \mathscr{O}_S^*$. Then from [15, theorem 2] follows that for any $v \in S$ and for any $\delta > 0$ we have

$$\max(|x|_v, |y|_v) \gg \max(|x|_v, |u_1|_v, \ldots, |u_n|_v) H_S(u)^{-\delta/\#S}$$

where $u = (u_1, \ldots, u_k)$ and where the constants implied by the Vinogradov symbol depend only on $\mathbb{K}, S, n$, and δ. Taking the product over all $v \in S$ this gives

$$H_S(x,y) \gg H_S(x, u_1, \ldots, u_n) H_S(u)^{-\delta} \gg H_S(x, u_1, \ldots, u_n)^{1-\delta}.$$

If we choose $0 < \delta < 1$, then $\varepsilon(1-\delta) > 0$ and $x, u_1, \ldots, u_n$ is a solution of

$$\begin{aligned} \prod_{v \in T} |\alpha_v y - x|_v \prod_{w \in S \setminus T} |x|_w &\leq H_S(x,y) \prod_{v \in T} \left| \alpha_v - \frac{x}{y} \right|_v \\ &\ll_{\mathbb{K}, S, n, \delta} H_S(x, u_1, \ldots, u_n)^{-\varepsilon(1-\delta)}. \end{aligned} \tag{4.5}$$

By the key lemma (4.5) has at most finitely many solutions up to multiplication by an S-unit, thus the result follows immediately by letting n range over the positive integers less than M. □

Note that this corollary gives an improvement on the theorems of Roth and Ridout for a special kind of solutions, in that here we have an exponent $-1-\varepsilon$ instead of $-2-\varepsilon$.

Remark 4.0.8. Corollary 4.0.7 implies that the decimal expansion of an algebraic number cannot have "too long" blocks of zeroes. More precisely, let $0.a_1a_2\dots$ be the decimal expansion of an (irrational) algebraic number α and for every integer $n > 0$ define $\ell(n)$ to be the minimal $\ell \geq 0$ such that $a_{n+\ell} \neq 0$. Then $\ell(n) = o(n)$ for $n \to \infty$.

Indeed, consider $\mathbb{K} = \mathbb{Q}$, $S = \{\infty, 2, 5\}$, $T = \infty$, and $M = 1$. Then corollary 4.0.7 gives that

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

has at most finitely many solutions in S-integers x; in particular in rational numbers x with terminating decimal expansion. Now suppose that $\limsup_{n\to\infty} \ell(n)/n > 0$, i.e. suppose that there are a constant $c > 0$ and a strictly increasing infinite sequence of integers $(n_k)_{k\geq 1}$ such that $\ell(n_k) > cn_k$. Further, let

$$x_k = 0.a_1a_2\dots a_{n_k} =: \frac{p}{10^{n_k}}.$$

Then $H(x_k) = \max(p, 10^{n_k}) = 10^{n_k}$, so there is an $\varepsilon > 0$ such that (for k large enough)

$$|\alpha - x_k| \leq 10^{-n_k-\ell(n_k)+1} < H(x_k)^{-1-\varepsilon}$$

contradicting corollary 4.0.7.

5 A transcendence criterion

We shall now introduce some notation, following [2]. Let $\mathscr{A}$ be a finite alphabet and consider a word W on $\mathscr{A}$. We denote by $|W|$ the length of W and for any positive integer n we write W^n for the concatenation of W with itself n times. Further, for any positive real number x, we write W^x for $W^{\lfloor x \rfloor} W'$, where W' is a prefix of W of length $\lceil (x - \lfloor x \rfloor)|W| \rceil$.

Definition 5.0.9. Let $\mathbf{a} = (a_i)_{i \geq 1}$ be a sequence of elements of $\mathscr{A}$, which we identify with the infinite word $a_1 a_2 \ldots$, and let $w > 1$ be a real number. We say that $\mathbf{a}$ satisfies *condition* $(*)_w$ if it is *not* eventually periodic and if there are two infinite sequences of finite words $(U_n), (V_n)$ such that:

1. For any index n the word $U_n V_n^w$ is a prefix of $\mathbf{a}$;
2. The sequence $\left(\frac{|U_n|}{|V_n|} \right)$ is bounded from above by a constant $D > 0$;
3. The sequence $(|V_n|)$ is strictly increasing.

Example 5.0.10. It is fairly straightforward to construct a sequence that satisfies condition $(*)_w$ for a given $w > 1$. For example, let $\mathscr{A} = \{0, 1\}$ and define the sequences (U_n) and (V_n) as follows: let $U_1 = 0$, $V_1 = 1$ and for every $n > 1$ consider

$$U_n = U_{n-1} V_{n-1}^w \quad \text{and} \quad V_n = \overbrace{dd \cdots d}^{|U_n| \text{ times}}$$

where $d = 0$ if n is even and $d = 1$ if n is odd. Then simply let (a_i) be the limit sequence of U_n for $n \to \infty$.

For a more interesting example, note that in corollary 7.0.29 we prove that every non-periodic k-automatic sequence satisfies condition $(*)_w$. In particular, the classic Thue-Morse sequence (see example 7.0.24) satisfies condition $(*)_w$ with $w = 3/2$.

Definition 5.0.11. Let $\mathbf{a}$ be a sequence satisfying condition $(*)_w$ for some $w > 1$ and write s_n and r_n for the lengths of U_n and V_n, respectively. Then we define the *n-th*

(ultimately) periodic approximant of $\mathbf{a}$ to be the sequence $\mathbf{b}^{(n)}$ given by

$$\begin{cases} b_i^{(n)} = a_i & \text{for } 1 \le i \le r_n \\ b_{r_n+i+hs_n}^{(n)} = a_{r_n+i} & \text{for } 1 \le i \le s_n \text{ and } h \ge 0. \end{cases}$$

Note. The n-th periodic approximant of $\mathbf{a}$ is indeed ultimately periodic, with preperiod U_n and period V_n.

Remark 5.0.12. Let $\mathbf{a}, \mathbf{b}^{(n)}, r_n, s_n$ as in definition 5.0.11 and assume that the terms of $\mathbf{a}$ are in $\mathbb{K}$. Then in $\mathbb{K}[[X]]$ we have

$$\begin{aligned} \sum_{i=1}^{\infty} b_i^{(n)} X^i &= \sum_{i=1}^{r_n} a_i X^i + \sum_{i=r_n+1}^{\infty} b_i^{(n)} X^i \\ &= \sum_{i=1}^{r_n} a_i X^i + X^{r_n} \left(\sum_{i=1}^{s_n} a_{r_n+i} X^i \right) \left(\sum_{h=0}^{\infty} X^{hs_n} \right) \\ &= \sum_{i=1}^{r_n} a_i X^i + \frac{X^{r_n}}{1 - X^{s_n}} \sum_{i=1}^{s_n} a_{r_n+i} X^i. \end{aligned} \tag{5.1}$$

Let v be a place of $\mathbb{K}$ and denote by $\mathbb{K}_v$ the completion of $\mathbb{K}$ at v. Further, let $(a_i)_{i\ge 0}$ be a sequence with terms in $\mathbb{K}_v$. To lighten the notation, we define

$$v\text{-}\sum_{i=0}^{\infty} a_i := \lim_{m\to\infty} \sum_{i=0}^{m} a_i \quad \text{with respect to } |\cdot|_v$$

provided the limit exists.

Remark 5.0.13. Consider a $\beta \in \mathbb{K}$ and a place v of $\mathbb{K}$ such that $|\beta|_v > 1$. If $(a_i)_{i\ge 0}$ is a sequence of elements of $\mathbb{K}$ such that there is a constant $C_v > 0$ with $|a_i|_v < C_v$ for every $i \ge 0$ then

$$v\text{-}\sum_{i=0}^{\infty} \frac{a_i}{\beta^i}$$

converges in $\mathbb{K}_v$. Indeed we just need to prove that the partial sums form a Cauchy sequence: for every $m > n \ge 0$ we have

If v is non-archimedean then by the ultrametric inequality

$$\left| \sum_{i=n}^{m} \frac{a_i}{\beta^i} \right|_v \le C_v |\beta|_v^{-n}.$$

If v is archimedean let d_v be 1 if v is real or 2 if v is complex. Then

$$\left|\sum_{i=n}^{m}\frac{a_i}{\beta^i}\right|_v \leq \left(\sum_{i=n}^{m}\left|\frac{a_i}{\beta^i}\right|_v^{1/d_v}\right)^{d_v} \leq C_v\frac{|\beta|_v^{-n}}{1-|\beta|_v^{-1/d_v}}.$$

Furthermore, this gives an upper bound for $\left|v\text{-}\sum_{i=0}^{\infty}\frac{a_i}{\beta^i}\right|_v$ in terms of just C_v and $|\beta|_v$.

Recall that the *absolute (multiplicative) height* of $\alpha \in \mathbb{K}$ is defined as

$$H(\alpha) := \prod_{v\in M_{\mathbb{K}}} \max(1,|\alpha|_v)^{1/[\mathbb{K}:\mathbb{Q}]}$$

and that the *absolute logarithmic height* of α is $h(\alpha) := \log H(\alpha)$.

Theorem 5.0.14. *Fix an algebraic number field $\mathbb{K}$. Then fix a non-zero $\beta \in \mathbb{K}$ and a place v of $\mathbb{K}$ such that $|\beta|_v > 1$. Now consider $\mathbf{a} = (a_i)$ a sequence with terms in a finite subset $\mathscr{A} \subseteq \mathscr{O}_{\mathbb{K}}$. If there is $w > 1$ such that $\mathbf{a}$ satisfies condition $(*)_w$ and*

$$1+\frac{w-1}{D+1} > [\mathbb{K}:\mathbb{Q}]\,\frac{h(\beta)}{\log|\beta|_v}$$

where $D > 0$ is the upper bound of the sequence $(|U_n|/|V_n|)$ from condition $(*)_w$, then

$$\alpha_v = v\text{-}\sum_{i=1}^{\infty}\frac{a_i}{\beta^i}$$

is either in $\mathbb{K}$ or transcendental.

Proof. Assume $\alpha_v \notin \mathbb{K}$ and write s_n and r_n for the lengths of U_n and V_n from the definition of condition $(*)_w$, respectively. Then for every positive integer n define

$$\alpha_v^{(n)} = v\text{-}\sum_{i=1}^{\infty}\frac{b_i^{(n)}}{\beta^i}$$

where $\mathbf{b}^{(n)}$ is the n-th periodic approximant of $\mathbf{a}$ and observe that

$$\alpha_v - \alpha_v^{(n)} = v\text{-}\sum_{i=r_n+\lceil ws_n\rceil+1}^{\infty}\frac{a_i-b_i^{(n)}}{\beta^i}.$$

Moreover, by substituting β^{-1} in (5.1) we have

$$\begin{aligned}\beta^{r_n}(\beta^{s_n}-1)\alpha_v^{(n)} &= \beta^{r_n+s_n}(1-\beta^{-s_n})\left(\sum_{i=1}^{r_n}\frac{a_i}{\beta^i}+\frac{\beta^{-r_n}}{1-\beta^{-s_n}}\sum_{i=1}^{s_n}\frac{a_{r_n+i}}{\beta^i}\right)\\ &= \sum_{i=1}^{r_n} a_i\beta^{r_n-i}(\beta^{s_n}-1)+\sum_{i=1}^{s_n} a_{r_n+i}\beta^{s_n-i}\\ &=: P_n(\beta).\end{aligned}$$

In particular, note that P_n is a polynomial of degree at most r_n+s_n-1. Now let

$$S := M_{\mathbb{K}}^{\infty}\cup\{u\in M_{\mathbb{K}} : |\beta|_u \neq 1\} \qquad \mathscr{S} := \{u\in S : |\beta|_u > 1\}$$

and observe that

$$|P_n(\beta)|_u \ll_{\mathscr{A},u} r_n+s_n$$

for every $u\in S\setminus\mathscr{S}$. Furthermore, by remark 5.0.13

$$\left|\alpha_v-\alpha_v^{(n)}\right|_v = \left|\alpha_v-\frac{P_n(\beta)}{\beta^{r_n+s_n}-\beta^{r_n}}\right|_v \ll_{\mathscr{A},\beta,v} |\beta|_v^{-r_n-ws_n-1}.$$

Since (s_n) is increasing by condition $(*)_w$ and we are assuming $\alpha_v\notin\mathbb{K}$, this implies that $\alpha_v^{(n)}$ admits infinitely many different values. Indeed, otherwise there would be an $N>0$ such that $\alpha_v=\alpha_v^{(N)}\in\mathbb{K}$. Now define $d_1 := \#(S\setminus\mathscr{S})$ and

$$\ell := [\mathbb{K}:\mathbb{Q}]\,\frac{h(\beta)}{\log|\beta|_v} = \frac{1}{\log|\beta|_v}\left(\sum_{u\in\mathscr{S}}\log|\beta|_u\right).$$

For $\mathbf{x}=(\beta^{r_n+s_n},-\beta^{r_n},P_n(\beta))$ we have

$$\begin{aligned}H_S(\mathbf{x}) &= \prod_{u\in S}\max(|\beta|_u^{r_n+s_n},|\beta|_u^{r_n},|P_n(\beta)|_u)\\ &\ll_{\mathscr{A},S\setminus\mathscr{S}} (r_n+s_n)^{d_1}\prod_{u\in\mathscr{S}}\max(|\beta|_u^{r_n+s_n},|\beta|_u^{r_n},|P_n(\beta)|_u)\\ &\ll_{\mathscr{A},\mathscr{S}} (r_n+s_n)^{d_1}\prod_{u\in\mathscr{S}}|\beta|_u^{r_n+s_n}\\ &= (r_n+s_n)^{d_1}|\beta|_v^{\ell(r_n+s_n)}.\end{aligned}$$

Thanks to corollary 4.0.7, this means that we're done if we can prove that there are constants $C,\varepsilon>0$ such that

$$C(r_n+s_n)^{\varepsilon d_1}|\beta|_v^{(1+\varepsilon)\ell(r_n+s_n)} \le |\beta|_v^{r_n+s_n+(w-1)s_n}.$$

Taking logarithms and rearranging, this is equivalent to

$$\log(C)+\varepsilon d_1\log(r_n+s_n)\leq\big((1-\ell(1+\varepsilon))(r_n+s_n)+(w-1)s_n\big)\log|\beta|_v.$$

Now, by hypothesis we know that $\frac{r_n}{s_n}$ is bounded from above by $D>0$, thus

$$\frac{(w-1)s_n}{r_n+s_n}=\frac{w-1}{\frac{r_n}{s_n}+1}\geq\frac{w-1}{D+1}.$$

Further, note that $\frac{\log(r_n+s_n)}{r_n+s_n}$ takes its maximum for $r_n+s_n=3$, thus it follows that it is enough to find $C',\varepsilon>0$ such that

$$\log(C')+\varepsilon d_1\frac{\log(3)}{3}\leq\left(1+\frac{w-1}{D+1}-\ell-\varepsilon\ell\right)\log|\beta|_v$$

which is indeed possible because by hypothesis $1+\frac{w-1}{D+1}-\ell>0$. □

In [1] Adamczewski and Bugeaud proved a similar statement with a more manageable hypothesis on **a**. Namely, they said that **a** satisfies condition $(*)_\rho$ for some real constant $\rho\geq 1$ if there are two sequences of finite words $(U_n),(V_n)$ and a sequence of positive real numbers (w_n) such that:

1. For any index n the word $U_nV_n^{w_n}$ is a prefix of **a**;
2. $|U_nV_n^{w_n}|/|U_nV_n|\geq\rho$ for any index n;
3. The sequence $(|V_n^{w_n}|)$ is strictly increasing.

Then they defined the *Diophantine exponent* of **a** as

$$\mathbb{D}(\mathbf{a}):=\sup\left\{\rho\in\mathbb{R}_{\geq 1}:\mathbf{a}\text{ satisfies condition }(*)_\rho\right\}$$

noting that for any sequence we have $1\leq\mathbb{D}(\mathbf{a})\leq+\infty$ and that $\mathbb{D}(\mathbf{a})=+\infty$ for every **a** eventually periodic.

Mimicking the proof of theorem 5.0.14, with the appropriate modifications in the setting and the final estimates, we can prove the following slightly more general statement than the one from [1]:

Theorem 5.0.15. *Fix an algebraic number field $\mathbb{K}$. Then fix a non-zero $\beta\in\mathbb{K}$ and a place v of $\mathbb{K}$ such that $|\beta|_v>1$. Now consider a sequence $\mathbf{a}=(a_i)$ with terms from a finite subset $\mathscr{A}\subseteq\mathscr{O}_\mathbb{K}$. If*

$$\mathbb{D}(\mathbf{a})>[\mathbb{K}:\mathbb{Q}]\,\frac{h(\beta)}{\log|\beta|_v}$$

then

$$\alpha_v=v\text{-}\sum_{i=1}^{\infty}\frac{a_i}{\beta^i}$$

is either in $\mathbb{K}$ or transcendental.

Proof. Since the supremum of a set is either itself in the set or is an accumulation point of that set, by hypothesis we can find a real number ρ such that

$$\rho > [\mathbb{K}:\mathbb{Q}]\,\frac{h(\beta)}{\log|\beta|_v} =: \ell$$

and such that $\mathbf{a}$ satisfies condition $(*)_\rho$. Let $(U_n),(V_n)$, and (w_n) as in the definition of condition $(*)_\rho$ and define r_n, s_n as the lengths of U_n, V_n respectively.

Suppose that $\alpha \notin \mathbb{K}$. Mimicking the proof of theorem 5.0.14 with w_n instead of w we can find an infinite sequence $(\alpha_v^{(n)})$ such that

$$\left|\alpha_v - \alpha_v^{(n)}\right|_v \ll_{\mathscr{A},\beta,v} |\beta|_v^{-r_n - w_n s_n - 1}$$

and

$$\alpha_v^{(n)} = \frac{P_n(\beta)}{\beta^{r_n+s_n} - \beta^{r_n}}$$

where P_n is a polynomial of degree at most $r_n + s_n - 1$ with coefficients in $\mathbb{K}$. Still following the proof of theorem 5.0.14 we see that for $\mathbf{x} = (\beta^{r_n+s_n}, -\beta^{r_n}, P_n(\beta))$ we have

$$H_S(\mathbf{x}) \ll_{\mathscr{A},\mathscr{S}} (r_n+s_n)^{d_1} |\beta|_v^{\ell(r_n+s_n)}$$

where $S := M_{\mathbb{K}}^\infty \cup \{u \in M_{\mathbb{K}} : |\beta|_u \neq 1\}$, $\mathscr{S} := \{u \in S : |\beta|_u > 1\}$, and $d_1 := \#(S \setminus \mathscr{S})$.

Thanks to corollary 4.0.7, this means that we're done if we can prove that there are constants $C, \varepsilon > 0$ such that with $\mathbf{x} = (\beta^{r_n+s_n}, -\beta^{r_n}, P_n(\beta))$ we have

$$C H_S(\mathbf{x})^{1+\varepsilon} \leq |\beta|_v^{r_n + w_n s_n + 1}$$

for every $n \geq 1$. Using the above estimate, taking logarithms, and rearranging we see that it is enough to find $C, \varepsilon > 0$ such that

$$\log(C) + (1+\varepsilon) d_1 \log(r_n+s_n) \leq \big(r_n + w_n s_n + 1 - \ell(1+\varepsilon)(r_n+s_n)\big) \log|\beta|_v.$$

Now observe that for every index n we have

$$\frac{r_n + w_n s_n + 1}{r_n + s_n} \geq \frac{r_n + \lceil w_n s_n \rceil}{r_n + s_n} = \frac{|U_n V_n^{w_n}|}{|U_n V_n|} \geq \rho$$

by condition $(*)_\rho$. Furthermore, note that $\frac{\log(r_n+s_n)}{r_n+s_n}$ takes its maximum for $r_n + s_n = 3$. Thus it follows that it is enough to find $C', \varepsilon > 0$ such that

$$\log(C') + (1+\varepsilon) d_1 \frac{\log(3)}{3} \leq \big(\rho - (1+\varepsilon)\ell\big) \log|\beta|_v$$

which is possible because by hypothesis $\rho > \ell$. □

Remark 5.0.16. In [3] Adamczewski and Bugeaud state that the hypothesis of theorem 5.0.15 is stronger than the one from theorem 5.0.14, but this doesn't seem to be the case.

Indeed, suppose that **a** is a non-eventually periodic sequence which satisfies condition $(*)_w$ for some $w > 1$. Now let $(U_n), (V_n), D$ as in the definition of condition $(*)_w$ and consider the constant sequence (w_n) with $w_n = w$. Then the first hypothesis of condition $(*)_\rho$ is clearly satisfied. Further, up to extracting a subsequence we have that $|V_n^w| = \lceil w|V_n| \rceil$ is strictly increasing, because $(|V_n|)$ is strictly increasing and $w > 1$. Finally, writing as usual $r_n = |U_n|$ and $s_n = |V_n|$, we have

$$\frac{|U_n V_n^w|}{|U_n V_n|} = \frac{r_n + \lceil w s_n \rceil}{r_n + s_n} = 1 + \frac{\lceil (w-1) s_n \rceil}{r_n + s_n} \geq 1 + \frac{w-1}{D+1} =: \rho > 1.$$

Thus if **a** satisfies the hypothesis of theorem 5.0.14, then it satisfies the hypothesis of theorem 5.0.15, too, so the latter is actually weaker than the former.

This author doesn't know if there is some case where theorem 5.0.15 is applicable but theorem 5.0.14 isn't, or if these two theorems are are actually equivalent. It is worth to point out that the problem in proving the latter doesn't lie in showing that if **a** satisfies condition $(*)_\rho$ for some $\rho > 1$ then it also satisfies condition $(*)_w$ for some $w > 1$, but it lies in showing that for any $c > 1$ if $\rho > c$, then we can choose w, (U_n), and (V_n) such that

$$1 + \frac{w-1}{D+1} > c$$

where D is defined as in condition $(*)_w$.

6 Some consequences

Definition 6.0.17. The *complexity function* of a sequence $\mathbf{a}$ is the number $p_{\mathbf{a}}(n)$ of distinct blocks of consecutive n terms of $\mathbf{a}$. In other words, if $\mathbf{a} = (a_i)_{i\geq 1}$, then $p_{\mathbf{a}}(n)$ is the number of distinct sequences among $(a_1,\dots,a_n),(a_2,\dots,a_{n+1}),\dots$.

Remark 6.0.18. Note that the complexity function of a periodic sequence is bounded.

Corollary 6.0.19. *Fix $\mathbb{K},\beta,v$ as in theorem 5.0.15, fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ such that $\mathbb{K}\subset\overline{\mathbb{Q}}$, and suppose that*

$$[\mathbb{K}:\mathbb{Q}]\,\frac{h(\beta)}{\log|\beta|_v} < 1+\frac{1}{c}$$

for some real constant $c>0$. Further, fix an algebraic number $\alpha\in\overline{\mathbb{Q}}\setminus\mathbb{K}$ and a finite subset $\mathscr{A}\subset\mathscr{O}_{\mathbb{K}}$. If $\mathbf{a}=(a_i)_{i\geq m}$ with $m\in\mathbb{Z}$ is a sequence with terms in $\mathscr{A}$ such that

$$\alpha = v\text{-}\sum_{i=1}^{\infty}\frac{a_i}{\beta^i}$$

then the complexity function $p_{\mathbf{a}}(n)$ of $\mathbf{a}$ satisfies

$$\liminf_{n\to\infty}\frac{p_{\mathbf{a}}(n)}{n} > c. \tag{6.1}$$

Proof. We follow the general idea of the proof of [1, theorem 3].

Suppose that $p_{\mathbf{a}}(n_k)\leq cn_k$ for some strictly increasing infinite sequence of positive integers (n_k). If, for any positive integer ℓ, we denote by $A(\ell)$ the prefix of $\mathbf{a}$ of length ℓ, then by the Pigeonhole Principle we know that there is (at least) a word W_k of length n_k which occurs (at least) twice in $A((c+1)n_k)$. Therefore we can find (possibly empty) words B_k,D_k,E_k and a non-empty word C_k such that

$$A((c+1)n_k) = B_kW_kD_kE_k = B_kC_kW_kE_k.$$

Now, if $|C_k|\geq|W_k|$, then we can find a (possibly empty) word F_k such that

$$A((c+1)n_k) = B_kW_kF_kW_kE_k.$$

Hence, setting $U_k = B_k$, $V_k = W_k F_k$, and $w_k = |W_k F_k W_k|/|W_k F_k|$ we have that $U_k V_k^{w_k} = B_k W_k F_k W_k$ is a prefix of $\mathbf{a}$, $\left|V_k^{w_k}\right| > n_k$, and

$$\frac{\left|U_k V_k^{w_k}\right|}{|U_k V_k|} = 1 + \frac{|W_k|}{|B_k W_k F_k|} \geq 1 + \frac{n_k}{c n_k} = 1 + \frac{1}{c}.$$

If, on the other hand, $|C_k| < |W_k|$, then C_k is a prefix of W_k and we can find a real $w_k > 0$ such that

$$C_k W_k = C_k^{w_k}.$$

Hence, setting $U_k = B_k$ and $V_k = C_k$ we have that $U_k V_k^{w_k} = B_k C_k W_k$ is a prefix of $\mathbf{a}$, $\left|V_k^{w_k}\right| = |C_k W_k| > n_k$, and

$$\frac{\left|U_k V_k^{w_k}\right|}{|U_k V_k|} = 1 + \frac{|W_k|}{|B_k C_k|} \geq 1 + \frac{n_k}{c n_k} = 1 + \frac{1}{c}.$$

Therefore in either case we found sequences $(U_k), (V_k), (w_k)$ such that

1. $U_k V_k^{w_k}$ is a prefix of $\mathbf{a}$;
2. $\left|U_k V_k^{w_k}\right|/|U_k V_k| > 1 + 1/c$ for every index k;
3. The sequence $\left(\left|V_k^{w_k}\right|\right)$ is strictly increasing.

Thus $\mathbf{a}$ satisfies condition $(*)_{1+1/c}$, hence $\mathbb{D}(\mathbf{a}) \geq 1 + 1/c$. Finally, from theorem 5.0.15 it follows that either α is in $\mathbb{K}$ or it is transcendental, against the hypothesis of the corollary. □

This result is especially interesting whenever $[\mathbb{K} : \mathbb{Q}] \frac{h(\beta)}{\log|\beta|_v} = 1$. For example, this happens when β is an imaginary quadratic integer, because then there is only one place v (archimedean, corresponding to the embedding $\beta \mapsto \beta$) for which $|\beta|_v \geq 1$. Thus we immediately deduce the following:

Corollary 6.0.20. *Fix an imaginary quadratic integer $\beta \in \mathbb{C}$ different from $\pm i$ or $\left((1 + i\sqrt{3})/2\right)^k$ for some $k \in \mathbb{Z}$, and consider an algebraic number $\alpha \in \mathbb{C} \setminus \mathbb{Q}(\beta)$. If $\mathbf{a} = (a_i)_{i \geq m}$ with $m \in \mathbb{Z}$ is a sequence with terms in a finite subset of $\mathcal{O}_{\mathbb{Q}(\beta)}$ such that*

$$\alpha = \sum_{i=1}^{\infty} \frac{a_i}{\beta^i}$$

(where the limit is taken in $\mathbb{C}$), then the complexity function $p_{\mathbf{a}}(n)$ of $\mathbf{a}$ satisfies

$$\liminf_{n \to \infty} \frac{p_{\mathbf{a}}(n)}{n} = +\infty.$$

Proof. Note that every imaginary quadratic integer β is either of the form $a+ib\sqrt{d}$ with $a,b,d \in \mathbb{Z}$, $b \neq 0$, and $d > 0$ squarefree (but possibly 1) if $d \not\equiv 3 \pmod 4$, or of the form $(a+ib\sqrt{d})/2$ with a,b both even or both odd if $d \equiv 3 \pmod 4$. Thus $|\beta| > 1$ unless β is one of $\pm i$ or $\left((1+i\sqrt{3})/2\right)^k$ for some $k \in \mathbb{Z}$, so we can apply the previous corollary. □

Another case where $[\mathbb{K} : \mathbb{Q}] \frac{h(\beta)}{\log|\beta|_v} = 1$ is when β is a Pisot (or Salem) integer, i.e. when β is a real algebraic integer greater than 1 and all of the conjugates of β different from it lie in the open (respectively, closed) complex unit disc. For example every integer greater than 1 is a Pisot number, as is the golden ratio.

This case is particularly relevant because if β is a Pisot integer, then a real α is in $\mathbb{Q}(\beta)$ if and only if it has an ultimately periodic β-expansion, which was proved by Schmidt in 1980 [33]. In general every number with a periodic β-expansion must lie in $\mathbb{Q}(\beta)$, but the converse may not hold. To the best of this author's knowledge there are no other known necessary or sufficient conditions on β for it to hold.

Corollary 6.0.21. *Fix a Pisot or Salem integer $\beta > 1$. If α is real algebraic number with non-periodic β-expansion, then the complexity function $p_{\mathbf{a}}(n)$ of its β-expansion satisfies*

$$\liminf_{n\to\infty} \frac{p_{\mathbf{a}}(n)}{n} = +\infty.$$

Proof. Observe that if a sequence is ultimately periodic, then its complexity function is bounded by a function of the lengths of its period and preperiod. Hence the conclusion immediately follows from corollary 6.0.19, thanks to Schmidt's result. □

Finally, consider a prime number p and the completion $\mathbb{Q}_p$ of $\mathbb{Q}$. Then recall that every number $\alpha \in \mathbb{Q}_p$ admits a p-adic expansion

$$\alpha = \sum_{k=-m}^{\infty} a_k p^k$$

with $m \in \mathbb{Z}$ and $a_k \in \{0,\dots,p-1\}$ for every $k \geq -m$, where the limit is taken with respect to $|\cdot|_p$. Moreover, $\alpha \in \mathbb{Q}$ if and only if the sequence $(a_k)_{k\geq -m}$ is ultimately periodic (e.g. see [26, chapter II, sections 1 and 2]).

Corollary 6.0.22. *Fix a prime number p and consider an infinite sequence $\mathbf{a} = (a_k)_{k\geq -m}$ with terms in $\{0,\dots,p-1\}$ which isn't ultimately periodic. If there is a $w > 1$ such that $\mathbf{a}$ satisfies condition $(*)_w$ (or if $\mathbb{D}(\mathbf{a}) > 1$), then the p-adic number*

$$\alpha = \sum_{k=-m}^{\infty} a_k p^k$$

is transcendental.

Proof. Note that

$$\alpha = \sum_{k=-m}^{\infty} a_k p^k = \sum_{k=-m}^{\infty} \frac{a_k}{(p^{-1})^k}$$

and since p is a rational integer we have that $h(1/p) = \sum_{v \in M_{\mathbb{Q}}} |1/p|_v = |1/p|_p = p$. Thus the statement follows from theorem 5.0.14 (or theorem 5.0.15) because **a** not ultimately periodic implies that $\alpha \notin \mathbb{Q}$. □

7 Automatic numbers

Given a finite alphabet $\mathscr{A}$, in what follows we will denote by $\mathscr{A}^*$ the free monoid generated by $\mathscr{A}$, i.e. the set of finite words on $\mathscr{A}$ with the operation of concatenation (where the identity is the empty word).

Consider an integer $k \geq 2$ and denote by Σ_k the set $\{0,\dots,k-1\}$. A *k-automaton* is a tuple

$$A = (Q, \Sigma_k, \delta, q_0, \Delta, \tau)$$

where Q and Δ are finite sets, $q_0 \in Q$, $\delta\colon Q \times \Sigma_k \to Q$, and $\tau\colon Q \to \Delta$. The set Q is the *set of states*, Σ_k and Δ are respectively the *input* and *output alphabets*, q_0 is the *initial state*, δ is the *transition function*, and τ is the *output function*.

Observe that, given a k-automaton A, we can extend δ to $Q \times \Sigma_k^*$. Indeed, consider a state $q \in Q$ and a finite word $W = w_1 w_2 \dots w_n$ on Σ_k. Then we can define $\delta(q, W)$ recursively as $\delta(\delta(q, w_1 \dots w_{n-1}), w_n)$.

Definition 7.0.23. A sequence $\mathbf{a} = (a_n)_{n\geq 0}$ is said to be k-automatic if there is a k-automaton A such that $a_n = \tau(\delta(q_0, W_n))$ for every $n \geq 0$, where W_n is the sequence of digits of the k-ary expansion of n.

Furthermore, a real number α is said to be *k-automatic* if there is an integer $b \geq 2$ such that the sequence of digits of the b-ary expansion of α is k-automatic. In this case we also say that α is *generated* by a finite automaton.

Informally, this means that a sequence (a_n) is k-automatic if we can compute a_n as a finite state function of the digits of n in base k.

Example 7.0.24. The Thue-Morse sequence counts the number of occurrences of 1 in the binary expansion of n, modulo 2. In other words, it is the sequence $(a_n)_{n\geq 0}$ where a_n is 0 if the sum of the digits in the binary expansion of n is even, and 0 otherwise. This sequence can be generated by the 2-automaton

$$(\{q_0, q_1\}, \{0,1\}, \delta, q_0, \{0,1\}, \tau)$$

where

$$\begin{aligned} \delta(q_0,0) = \delta(q_1,1) = q_0 \qquad &\text{and} \qquad \delta(q_0,1) = \delta(q_1,0) = q_1 \\ \tau(q_0) = 0 \qquad &\text{and} \qquad \tau(q_1) = 1. \end{aligned}$$

The first few terms of the sequence are

$$01101001100101101001 0\ldots.$$

Moreover, note that in 1929 Mahler showed that the real number whose binary expansion is the Thue-Morse sequence is transcendental [25].

Example 7.0.25. The Rudin-Shapiro sequence is a sequence $(a_n)_{n\geq 0}$ such that $a_n = 1$ if the number of (possibly overlapping) occurrences of 11 in the binary expansion of n is even, and $a_n = -1$ otherwise. This sequence can be generated by the finite automaton

$$(\{q_0,q_1,q_2,q_3\},\{0,1\},\delta,q_0,\{1,-1\},\tau)$$

where

$$\begin{aligned} \delta(q_0,0) = \delta(q_1,0) = q_0 \qquad & \delta(q_2,0) = \delta(q_3,0) = q_3 \\ \delta(q_0,1) = \delta(q_2,1) = q_1 \qquad & \delta(q_1,1) = \delta(q_3,1) = q_2 \\ \tau(q_0) = \tau(q_1) = 1 \qquad & \tau(q_2) = \tau(q_3) = -1. \end{aligned}$$

Informally, the states q_0 and q_1 represent a current even number of occurrences of 11, with the last digit 0 or 1, respectively, while the states q_2 and q_3 represent a current odd number of occurrences of 11, with last digit 1 or 0, respectively. The first few terms of the sequence are

$$1\,1\,1\,-1\,1\,1\,-1\,1\,1\,1\,1\,-1\,-1\,-1\,1\,1\,-1\ldots.$$

Consider two finite alphabets $\mathscr{A}$ and $\mathscr{B}$. A *morphism* from $\mathscr{A}^*$ to $\mathscr{B}^*$ is just a monoid homomorphism $\sigma\colon \mathscr{A}^* \to \mathscr{B}^*$, i.e. a map such that $\sigma(xy) = \sigma(x)\sigma(y)$ for every $x,y \in \mathscr{A}^*$. Note that every morphism from $\mathscr{A}^*$ to $\mathscr{B}^*$ is uniquely defined by its action on the letters of $\mathscr{A}$ and that every morphism can be uniquely extended to the infinite sequences with terms from $\mathscr{A}$.

Definition 7.0.26. Let $k \geq 1$ be an integer. A morphism σ from $\mathscr{A}^*$ to $\mathscr{B}^*$ is said to be *k-uniform* if $|\sigma(a)| = k$ for every letter $a \in \mathscr{A}$. A 1-uniform morphism is called a *coding*.

Now consider a finite alphabet $\mathscr{A}$. A morphism σ from $\mathscr{A}^*$ to itself is said to be *prolongable* (on a) if there is a letter $a \in \mathscr{A}$ such that $\sigma(a) = aW$, where W is a word such that $\sigma^k(W)$ is non-empty for every $k \geq 1$; in particular W itself must be non-empty because $\sigma(\varepsilon) = \varepsilon$. In this case the infinite word

$$\sigma^\omega(a) := aW\,\sigma(W)\,\sigma^2(W)\,\sigma^3(W)\cdots$$

is a fixed point of σ, in the sense that $\sigma(\sigma^\omega(a)) = \sigma^\omega(a)$, and we say that the word $\sigma^\omega(a)$ is *generated* by the morphism σ. Moreover, note that $\sigma^\omega(a)$ is the unique fixed point of σ that starts with a.

Example 7.0.27. If $\sigma\colon \{0,1\}^* \to \{0,1\}^*$ is the 2-uniform morphism defined by

$$0 \mapsto 01 \qquad 1 \mapsto 10$$

then it can be showed that $\sigma^\omega(0)$ is the Thue-Morse sequence.

Theorem 7.0.28 (Cobham)**.** *Fix an integer $k \geq 2$. A sequence (a_n) is k-automatic if and only if it is the image, under a coding, of a fixed point of a k-uniform morphism.*

Corollary 7.0.29. *Let k be a positive integer. Then every k-automatic number is either rational or transcendental.*

Proof. Consider an automatic number α. If it is rational we are done, otherwise let b,k be integers such that the sequence of digits of the b-ary expansion $\mathbf{a}$ of α is k-automatic. Also fix $\mathscr{A} = \{0,\dots,b-1\}$. Then by Cobham's theorem there are a finite alphabet $\mathscr{B}$, a coding φ from $\mathscr{B}^*$ to $\mathscr{A}^*$, and a k-uniform morphism σ from $\mathscr{B}^*$ to itself such that $\mathbf{a} = \varphi(\mathbf{u})$, where $\mathbf{u}$ is a fixed point of σ. Furthermore, since φ is a coding it follows that if $\mathbf{u}$ satisfies condition $(*)_w$, then $\mathbf{a}$ does, too.

Now, if $\mathscr{B}$ has r elements, then by the Pigeonhole Principle there is a letter $u \in \mathscr{B}$ that appears at least twice in the prefix of $\mathbf{u}$ of length $r+1$, which can thus be written as

$$A\,u\,B\,u\,C$$

where A,B,C are (possibly empty) finite words on $\mathscr{B}$. Then consider the two sequences $(U_n)_{n\geq 1}$ and $(V_n)_{n\geq 1}$ defined by $U_n = \sigma^n(A)$ and $V_n = \sigma^n(uB)$.

Note that, since σ is k-uniform, $|\sigma^n(W)| = k^n|W|$ for every finite word W on $\mathscr{B}$. In particular, $\sigma^n(u)$ is a prefix of V_n of length at least $|V_n|/r$ because by hypothesis $|uB| \leq r$, which gives

$$|\sigma^n(u)| = k^n = \frac{|V_n|}{|uB|} \geq \frac{|V_n|}{r}.$$

This means that $U_n V_n^{1+1/r}$ is a prefix of $\mathbf{u}$. Moreover, observe that

$$\frac{|U_n|}{|V_n|} = \frac{k^n|A|}{k^n|uB|} \leq |A| \leq r-1.$$

Since $|V_n| = k^n|uB| \geq k^n$, it follows that $\mathbf{u}$ satisfies condition $(*)_w$ with $w = 1+1/r$, so $\mathbf{a}$ does, too.

Finally, note that $b \in \mathbb{Z}$ implies $h(b) = \log|b|$, thus the hypotheses of theorem 5.0.14 are satisfied and α must be transcendental, as required. □

7.1 Proof of Cobham's theorem

We shall now give a short proof of Cobham's theorem, following [4, section 6.3]. To lighten the notation, in this section we will write $\langle n \rangle_k$ for the k-ary expansion of an integer n and $[w]_k$ for the integer n with k-ary expansion w, where w is a finite word on $\Sigma_k = \{0, \ldots, k-1\}$.

Lemma 7.1.1. *Consider a k-automatic morphism σ and an infinite word $\mathbf{a} = (a_n)_{n \geq 0}$ such that $\sigma(\mathbf{a}) = \mathbf{a}$. Then $\sigma(a_n) = a_{kn} a_{kn+1} \cdots a_{kn+k-1}$.*

Proof. Since σ is k-automatic and $\mathbf{a}$ is a fixed point of σ we have

$$\sigma(a_0 a_1 \cdots a_n) = a_0 a_1 \cdots a_{kn+k-1}.$$

We proceed by induction. For $n = 0$ we have $\sigma(a_0) = a_0 a_1 \cdots a_{k-1}$, which we know to be true. Now by induction hypothesis for $n > 0$ we have

$$\sigma(a_0 a_1 \cdots a_{n-1}) \sigma(a_n) = (a_0 a_1 \cdots a_{kn-1})(a_{kn} a_{kn+1} \cdots a_{kn+k-1})$$

and $\sigma(a_0 a_1 \cdots a_n) = \sigma(a_0 a_1 \cdots a_{n-1}) \sigma(a_n)$ implies the desired result. □

Proof of Cobham's theorem. First consider a finite alphabet $\mathscr{B}$, a k-uniform morphism σ from $\mathscr{B}^*$ to itself, and a coding φ from $\mathscr{B}^*$ to $\mathscr{A}^*$. Further, let $\mathbf{a} = \varphi(\mathbf{u})$ where $\mathbf{u} = (u_n)_{n \geq 0}$ is a fixed point of σ. Then let $q_0 = u_0$ and define a k-automaton $(\mathscr{B}, \Sigma_k, \delta, q_0, \mathscr{A}, \varphi)$ where $\delta(q, s)$ is the s-th letter of $\sigma(q)$.

Now we prove by induction that $\delta(q_0, \langle n \rangle_k) = u_n$ for all $n \geq 0$. For $n = 0$ this is clear, because we defined $q_0 = u_0$ and $\mathbf{u}$ is a fixed point of σ. Then assume the claim true for all $0 \leq r < n$ and write $\langle n \rangle_k = n_1 n_2 \cdots n_t$ and $n = kn' + n_t$. We have

$$\begin{aligned}
\delta(q_0, \langle n \rangle_k) &= \delta(q_0, n_1 n_2 \cdots n_t) \\
&= \delta(\delta(q_0, n_1 n_2 \cdots n_{t-1}), n_t) \\
&= \delta(\delta(q_0, \langle n' \rangle_k), n_t) \\
&= \delta(u_{n'}, n_t) && \text{(by induction)} \\
&= \text{the } n_t\text{-th letter of } \sigma(u_{n'}) \\
&= u_{kn'+n_t} && \text{(by lemma 7.1.1)} \\
&= u_n.
\end{aligned}$$

Conversely, consider a k-automatic sequence $\mathbf{a}$ which is generated by a k-automaton $(Q, \Sigma_k, \delta, q_0, \mathscr{A}, \varphi)$ and note that up to a permutation of Σ_k we may assume without loss of generality that $\delta(q_0, 0) = q_0$. Then define a k-uniform morphism σ from Q^* to itself by

$$\sigma(q) := \delta(q, 0) \delta(q, 1) \cdots \delta(q, k-1)$$

for each $q \in Q$ and let $\mathbf{u} = (u_n)_{n\geq 0}$ be a fixed point of σ, starting at q_0 (which exists because $\delta(q_0, 0) = q_0$). We will now prove that $\delta(q_0, y) = u_{[y]_k}$ for every $y \in \Sigma_k$ by induction on $|y|$.

For $|y| = 0$ this is clear because $\delta(q_0, \varepsilon) = q_0 = u_0$. Then assume the claim is true if $|y| < r$ and consider y with $|y| = r$. After writing $y = xa$ with $a \in \Sigma_k$ we have

$$\begin{aligned}
\delta(q_0, y) &= \delta(q_0, xa) \\
&= \delta(\delta(q_0, x), a) \\
&= \delta(u_{[x]_k}, a) && \text{(by induction)} \\
&= a\text{-th letter of } \sigma(u_{[x]_k}) && \text{(by definition of } \sigma) \\
&= u_{k[x]_k + a} && \text{(by lemma 7.1.1)} \\
&= u_{[xa]_k} = u_{[y]_k}.
\end{aligned}$$

Therefore $a_n = \varphi(\delta(q_0, \langle n \rangle_k)) = \varphi(u_n)$, so $\mathbf{a}$ is the image under the coding φ of a fixed point of σ, as required. □

Bibliography

[1] B. Adamczewski and Y. Bugeaud. Dynamics for β-shifts and Diophantine approximation. *Ergodic Theory Dynam. Systems*, 27(6):1695–1711, 2007.

[2] B. Adamczewski and Y. Bugeaud. On the complexity of algebraic numbers. I. Expansions in integer bases. *Ann. of Math. (2)*, 165(2):547–565, 2007.

[3] B. Adamczewski, Y. Bugeaud, and F. Luca. On the values of a class of analytic functions at algebraic points. *Acta Arith.*, 135(1):1–18, 2008.

[4] J.-P. Allouche and J. Shallit. *Automatic sequences. Theory, applications, generalizations.* Cambridge: Cambridge University Press, 2003.

[5] V. Becher and S. Figueira. An example of a computable absolutely normal number. *Theor. Comput. Sci.*, 270(1-2):947–958, 2002.

[6] P.-G. Becker. k-regular power series and Mahler-type functional equations. *J. Number Theory*, 49(3):269–286, 1994.

[7] Y. F. Bilu. The many faces of the subspace theorem [after Adamczewski, Bugeaud, Corvaja, Zannier...]. *Astérisque*, (317):Exp. No. 967, vii, 1–38, 2008. Séminaire Bourbaki. Vol. 2006/2007.

[8] E. Bombieri and W. Gubler. *Heights in Diophantine geometry*, volume 4 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2006.

[9] E. Borel. Les probabilités denombrables et leurs applications arithmétiques. *Rend. Circ. Mat. Palermo*, 27:247–271, 1909.

[10] E. Borel. Sur les chiffres decimaux de $\sqrt{2}$ et divers problèmes de probabilités en chaînes. *C. R. Acad. Sci., Paris*, 230:591–593, 1950.

[11] D. G. Champernowne. The construction of decimals normal in the scale of ten. *J. Lond. Math. Soc.*, 8:254–260, 1933.

[12] A. Cobham. On the hartmanis-stearns problem for a class of tag machines. *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*, 0:51–60, 1968.

[13] A. H. Copeland and P. Erdős. Note on normal numbers. *Bull. Am. Math. Soc.*, 52:857–860, 1946.

[14] M. Einsiedler and T. Ward. *Ergodic theory with a view towards number theory*, volume 259 of *Graduate Texts in Mathematics*. Springer-Verlag London, Ltd., London, 2011.

[15] J.-H. Evertse. On sums of S-units and linear recurrences. *Compositio Mathematica*, 53(2):225–244, 1984.

[16] J.-H. Evertse. On the quantitative subspace theorem. *Zap. Nauchn. Sem. S.-Petersburg. Otdel. Mat. Inst. Steklov. (POMI)*, 377(Issledovaniya po Teorii Chisel. 10):217–240, 245, 2010.

[17] J.-H. Evertse and H. P. Schlickewei. A quantitative version of the absolute subspace theorem. *J. Reine Angew. Math.*, 548:21–127, 2002.

[18] G. Faber. Über stetige Funktionen. (Zweite Abhandlung). *Math. Ann.*, 69:372–443, 1910.

[19] J. Hartmanis and R. E. Stearns. On the computational complexity of algorithms. *Trans. Amer. Math. Soc.*, 117:285–306, 1965.

[20] M. Hindry and J. H. Silverman. *Diophantine geometry: an introduction*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.

[21] G. J. Janusz. *Algebraic number fields*, volume 7 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, second edition, 1996.

[22] S. Lang. *Fundamentals of Diophantine geometry*. Springer-Verlag, New York, 1983.

[23] J. H. Loxton and A. J. van der Poorten. Arithmetic properties of the solutions of a class of functional equations. *J. Reine Angew. Math.*, 330:159–172, 1982.

[24] J. H. Loxton and A. J. van der Poorten. Arithmetic properties of automata: regular sequences. *J. Reine Angew. Math.*, 392:57–69, 1988.

[25] K. Mahler. Arithmetische Eigenschaften der Lösungen einer Klasse von Funktionalgleichungen. *Mathematische Annalen*, 101(1):342–366, 1929.

[26] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[27] A. Rényi. Representations for real numbers and their ergodic properties. *Acta Math. Acad. Sci. Hung.*, 8:477–493, 1957.

[28] D. Ridout. The p-adic generalization of the Thue-Siegel-Roth theorem. *Mathematika*, 5:40–48, 1958.

[29] K. F. Roth. Rational approximations to algebraic numbers. *Mathematika*, 2:1–20; corrigendum, 168, 1955.

[30] H. P. Schlickewei. Die $\mathfrak{p}$-adische Verallgemeinerung des Satzes von Thue-Siegel-Roth-Schmidt. *J. Reine Angew. Math.*, 288:86–105, 1976.

[31] H. P. Schlickewei. On products of special linear forms with algebraic coefficients. *Acta Arith.*, 31(4):389–398, 1976.

[32] H. P. Schlickewei. The p-adic Thue-Siegel-Roth-Schmidt theorem. *Arch. Math. (Basel)*, 29(3):267–270, 1977.

[33] K. Schmidt. On periodic expansions of Pisot numbers and Salem numbers. *Bull. London Math. Soc.*, 12(4):269–278, 1980.

[34] W. M. Schmidt. Norm form equations. *Ann. of Math. (2)*, 96:526–551, 1972.

[35] W. M. Schmidt. *Diophantine approximation*, volume 785 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

[36] C. L. Siegel. Über einige Anwendungen diophantischer Approximationen. *Abh. Preuß. Akad. Wiss., Phys.-Math. Kl.*, 1929(1):70 s., 1929.

[37] C. E. Silva. *Invitation to ergodic theory*, volume 42 of *Student Mathematical Library*. American Mathematical Society, Providence, RI, 2008.

[38] A. Thue. Über Annäherungswerte algebraischer Zahlen. *J. Reine Angew. Math.*, 135:284–305, 1909.

[39] A. Turing. On computable numbers, with an application to the Entscheidungsproblem. *Proc. Lond. Math. Soc. (2)*, 42:230–265, 1936.