On Cobham’s theorem

Fabien Durand\textsuperscript{1} and Michel Rigo\textsuperscript{2}

\textsuperscript{1}LAMFA - Université de Picardie Jules Verne - CNRS UMR 6140
33 rue Saint Leu, F-80039 Amiens cedex 1, France
email: fabien.durand@u-picardie.fr

\textsuperscript{2}Université de Liège, Institut de Mathématiques
12 Allée de la découverte (B37), B-4000 Liège, Belgique
email: M.Rigo@ulg.ac.be

2010 Mathematics Subject Classification: 68Q45, 68R15, 11B85, 11A67, 11U05, 37B20

Key words: Numeration systems, recognizable sets of integers, Cobham’s theorem, ultimate periodicity, substitutions, dynamical systems.

Contents

1 Introduction 897
2 Numeration basis 899
3 Automatic sequences 903
4 Multidimensional extension and first-order logic 905
\hspace{.5cm} 4.1 Subsets of \( \mathbb{N}^d \) \hspace{.5cm} 905
\hspace{.5cm} 4.2 Logic and \( k \)-definable sets \hspace{.5cm} 906
5 Numeration systems and substitutions 908
\hspace{.5cm} 5.1 Substitutive sets and abstract numeration systems \hspace{.5cm} 908
\hspace{.5cm} 5.2 Cobham’s theorem for substitutive sets \hspace{.5cm} 910
\hspace{.5cm} 5.3 Density, syndeticity and bounded gaps \hspace{.5cm} 914
\hspace{.5cm} \hspace{.5cm} 5.3.1 The length of the iterates \hspace{.5cm} 914
\hspace{.5cm} \hspace{.5cm} 5.3.2 Letters and words appear with bounded gaps \hspace{.5cm} 915
\hspace{.5cm} 5.4 Ultimate periodicity \hspace{.5cm} 917
\hspace{.5cm} 5.5 The case of fixed points \hspace{.5cm} 918
\hspace{.5cm} 5.6 Back to numeration systems \hspace{.5cm} 919
\hspace{.5cm} \hspace{.5cm} 5.6.1 Polynomially-growing abstract numeration systems \hspace{.5cm} 919
\hspace{.5cm} \hspace{.5cm} 5.6.2 Bertrand basis and \( \omega_{\alpha} \)-substitutive words \hspace{.5cm} 919
6 Cobham’s theorem in various contexts 920
\hspace{.5cm} 6.1 Regular sequences \hspace{.5cm} 920
\hspace{.5cm} 6.2 Algebraic setting and quasi-automatic functions \hspace{.5cm} 920
1 Introduction

In this chapter we essentially focus on the representation of non-negative integers in a given numeration system. The main role of such a system — like the usual integer base-$k$ numeration system — is to replace numbers, or more generally sets of numbers, by their corresponding representations, i.e., by words or languages. First we consider integer base numeration systems to present the main concepts, but rapidly we will introduce non-standard systems and their relationship with substitutions.

Let $k \in \mathbb{N}_{\geq 2}$ be an integer, where $\mathbb{N}_{\geq 2}$ denotes the set of non-negative integers greater than or equal to 2. The set $\{0, \ldots, k\}$ is denoted by $[0,k]$. If we do not allow leading zeroes when representing numbers, the function mapping a non-negative integer $n$ onto its $k$-ary representation $\text{rep}_k(n) \in [0,k-1]^*$ is a one-to-one correspondence. In particular, 0 is assumed to be represented by the empty word $\varepsilon$. In the literature, one also finds notation such as $\langle n \rangle_k$, $(n)_k$, or $\rho_k(n)$ instead of $\text{rep}_k(n)$. Hence every subset $X \subseteq \mathbb{N}$ is associated with the language $\text{rep}_k(X)$ consisting of the $k$-ary representations of the elements of $X$.

It is natural to study the relation between the arithmetic or number-theoretic properties of integers and the syntactical properties of the corresponding representations in a given numeration system. We focus on those sets $X \subseteq \mathbb{N}$ for which a finite automaton can be used to decide, for any given word $w$ over $[0,k-1]$, whether or not $w$ belongs to $\text{rep}_k(X)$. Sets having the property that $\text{rep}_k(X)$ is regular\footnote{We use the terminology of regular language, instead of rational language.} are called $k$-recognizable sets. Such a set can be considered as a particularly simple set, because using the $k$-ary numeration system it has a somehow elementary algorithmic description. In the framework of infinite-state system verification, one also finds the terminology of Number Decision Diagram or NDD [130].

The essence of Cobham’s theorem is to express that the property of being recognizable by a finite automaton strongly depends on the choice of the base and more generally on the considered numeration system. Naturally, this fact leads to and motivates the introduction and the study of recognizable sets in non-standard numeration systems. Considering alternative numeration systems may provide new recognizable sets and these non-standard systems also have applications in computer arithmetic [63]. Last but not least, the proof
of Cobham’s theorem is non-trivial and relies on quite elaborate arguments.

Now let us state Cobham’s celebrated result from 1969 and give all the needed details and definitions. Several surveys have been written on the same subject; see [25, 26, 29, 28, 104].

**Definition 1.1.** Let \( \alpha, \beta > 1 \) be two real numbers. If the equation \( \alpha^m = \beta^n \) with \( m, n \in \mathbb{N} \) has only the trivial integer solution \( m = n = 0 \), then \( \alpha \) and \( \beta \) are said to be **multiplicatively independent**. Otherwise, \( \alpha \) and \( \beta \) are said to be **multiplicatively dependent**.

**Definition 1.2.** A subset of \( \mathbb{N} \) is **ultimately periodic** if it is the union of a finite set and a finite number of infinite arithmetic progressions. In particular, \( X \) is ultimately periodic if and only if there exist \( N \geq 0 \) and \( p \geq 1 \) such that for all \( n \geq N \), \( n \in X \iff n + p \in X \).

Recall that an arithmetic progression is a set of the form \( a\mathbb{N} + b := \{an + b \mid n \geq 0\} \).

**Theorem 1.1** (Cobham’s theorem [37]). Let \( k, \ell \geq 2 \) be two multiplicatively independent integers. A set \( X \subseteq \mathbb{N} \) is both \( k \)-recognizable and \( \ell \)-recognizable if and only if it is ultimately periodic.

In the various contexts that we will describe, showing that an ultimately periodic set is recognizable is always the easy direction to prove (see Remark 1.3). So we focus on the other direction.

Let \( k, \ell \geq 2 \) be two integers. Notice that \( k \) and \( \ell \) are multiplicatively independent if and only if \( \log k / \log \ell \) is irrational. Note that for \( k \) and \( \ell \) to be multiplicatively dependent, it is not enough that \( k \) and \( \ell \) share exactly the same prime factors occurring in their decomposition. For instance, 6 and 18 are multiplicatively independent. But coprime integers are multiplicatively independent.

The irrationality of \( \log k / \log \ell \) is a crucial point in the proof of Cobham’s theorem (see Subsection 5.3). Recall that if \( \theta > 0 \) is irrational, then the set \( \{\{n\theta\} \mid n > 0\} \) of fractional parts of the multiples of \( \theta \) is dense in \([0, 1]\). For a proof of the so-called Kronecker theorem; see [70].

**Remark 1.2.** Multiplicative dependence is an equivalence relation \( \mathfrak{M} \) over \( \mathbb{N}_{\geq 2} \). If \( k \) and \( \ell \) are multiplicatively dependent, then there exist a minimal \( q \geq 2 \) and two positive integers \( m, n \) such that \( k = q^m \) and \( \ell = q^n \). Let us give the first (with respect to their minimal element) few equivalence classes for \( \mathfrak{M} \) partitioning \( \mathbb{N}_{\geq 2} : [2]_{\mathfrak{M}}, [3]_{\mathfrak{M}}, [5]_{\mathfrak{M}}, [6]_{\mathfrak{M}}, [7]_{\mathfrak{M}}, [10]_{\mathfrak{M}}, [11]_{\mathfrak{M}}, [12]_{\mathfrak{M}}, \ldots \).

**Remark 1.3.** We show that if a set \( X \subseteq \mathbb{N} \) is ultimately periodic then, for all \( k \geq 2 \), \( X \) is \( k \)-recognizable. In the literature, one also finds the terminology of a **recognizable set** \( X \) (without any mention to a base), meaning that \( X \) is \( k \)-recognizable for all \( k \geq 2 \). Note that a finite union of regular languages is again a regular language. Hence it is enough to check that \( \text{rep}_k(a\mathbb{N} + b) \) is regular with \( 0 \leq b < a \). We can indeed assume that \( b < a \) because if we add a finite number of words to a regular language or if we or remove a finite number of words from a regular language, we still have a regular language. Consider a DFA having \( Q = [0, a - 1] \) as its set of states. For all state \( i \in Q \) and \( d \in [0, k - 1] \), the
transitions are given by
\[ i \xrightarrow{d} ki + d \mod a. \]
The initial state is 0 and the unique final state is \( b \). As an example, a DFA accepting exactly the binary representations of the integers congruent to 3 mod 4 is given in Figure 1. A study of the minimal automaton recognizing such divisibility criteria expressed in an integer base is given in [3]. Also see the discussion in [117, Prologue]. The fact that a divisibility criterion exists in every base for any fixed divisor was already observed by Pascal in [103, pp. 84–89].

### 2 Numeration basis

It is remarkable that the recognizability of ultimately periodic sets extends to wider contexts (see Proposition 2.6 and Theorem 5.1). Let us introduce our first generalization of the integer base numeration system.

**Definition 2.1.** A **numeration basis** is a sequence \( U = (U_n)_{n \geq 0} \) of integers such that \( U \) is increasing, \( U_0 = 1 \) and that the set \( \{U_{i+1}/U_i \mid i \geq 0\} \) is bounded. This latter condition ensures the finiteness of the alphabet of digits used to represent integers. If \( w = w_\ell \cdots w_0 \) is a word over a finite alphabet \( A \subset \mathbb{Z} \) then the numerical value of \( w \) is
\[
\pi_{A,U}(w) = \sum_{i=0}^{\ell} w_i U_i.
\]
Using the greedy algorithm [61], any integer \( n \) has a unique (normal) \( U \)-representation \( \text{rep}_U(n) = w_\ell \cdots w_0 \), which is a finite word over a minimal finite alphabet called the **canonical alphabet** of \( U \) and denoted by \( A_U \). The normal \( U \)-representation satisfies
\[
\pi_{A_U}(\text{rep}_U(n)) = n \quad \text{and} \quad i \in [0, \ell - 1], \pi_{A_U}(w_\ell \cdots w_0) < U_{i+1} \text{ for all } i \in [0, \ell - 1].
\]
Again, \( \text{rep}_U(0) = \varepsilon \). See [90, Chapter 7] or Ch. Frougny and J. Sakarovitch’s chapter in [12, Chapter 2]. A subset \( X \subseteq \mathbb{N} \) is **\( U \)-recognizable** if \( \text{rep}_U(X) \) is accepted by a finite automaton. Let \( B \subset \mathbb{Z} \) be a finite alphabet. If \( w \in B^* \) is such that \( \pi_{B,U}(w) \geq 0 \), then the function mapping \( w \) onto \( \text{rep}_U(\pi_{B,U}(w)) \) is called **normalization**.
Definition 2.2. A numeration basis $U$ is said to be linear if there exist $k \in \mathbb{N} \setminus \{0\}$, $d_1, \ldots, d_k \in \mathbb{Z}$, $d_k \neq 0$, such that, for all $n \geq k$, $U_n = d_1U_{n-1} + \cdots + d_kU_{n-k}$. The polynomial $P_U(X) = X^k - d_1X^{k-1} - \cdots - d_{k-1}X - d_k$ is called the characteristic polynomial of $U$.

Definition 2.3. Recall that a Pisot-Vijayaraghavan number is an algebraic integer $\beta > 1$ whose Galois conjugates have modulus strictly less than one. We say that $U = (U_n)_{n \geq 0}$ is a Pisot numeration system if the numeration basis $U$ is linear and $P_U(X)$ is the minimal polynomial of a Pisot number $\beta$. Integer base numeration systems are particular cases of Pisot systems. For instance, see [27] where it is shown that most properties related to $k$-recognizable sets, $k \in \mathbb{N}_{\geq 2}$, can be extended to Pisot systems. In such a case, there exists some $c > 0$ such that $|U_n - c\beta^n| \to 0$, as $n$ tends to infinity.

Example 2.1. Consider the Fibonacci sequence defined by $U_0 = 1$, $U_1 = 2$ and $U_{n+2} = U_{n+1} + U_n$ for all $n \geq 0$. A word over $\{0, 1\}$ is a $U$-representation if and only if it belongs to the language $L = \{0, 1\}^* \cup \{\varepsilon\}$. For instance, the word 10110 is not a $U$-representation. Since $\pi_{A_U,U}(10110) = 13$, the normalization maps 10110 to $\text{rep}_U(13) = 100000$. The characteristic polynomial of this linear numeration basis is the minimal polynomial of the Pisot number $(1 + \sqrt{5})/2$. This Pisot numeration system is presented in [131].

The following result is an easy exercise, but also can be carried out in a wider context.

Theorem 2.1. [123] Let $U$ be a numeration basis. If $\mathbb{N}$ is $U$-recognizable, then $U$ is linear.

Definition 2.4. [13] A Bertrand numeration basis $U$ is a numeration basis satisfying the following property: $w \in \text{rep}_U(\mathbb{N})$ if and only if, for all $n \in \mathbb{N}$, $w0^n \in \text{rep}_U(\mathbb{N})$. It is a natural condition satisfied by all integer base $k \geq 2$ systems. For instance, the sequence defined by $U_0 = 1$, $U_1 = 3$ and, for all $n \geq 0$, $U_{n+2} = U_{n+1} + U_n$ is not a Bertrand numeration basis because $\text{rep}_U(2) = 2$, but $\pi_{A_U,U}(20) = 6$ and $\text{rep}_U(6) = 102$.

Let $\alpha > 1$ be a real number. The notion of $\alpha$-expansion was introduced by Parry in [102] (also see Rényi’s paper [111]), or again see [90, Chapter 7]. All $x \in [0, 1]$ can be uniquely written in the following way:

$$x = \sum_{n \geq 1} a_n\alpha^{-n}, \tag{2.1}$$

with $x_1 = x$ and for all $n \geq 1$, $a_n = \lfloor \alpha x_n \rfloor$ and $x_{n+1} = \{\alpha x_n\}$, where $\lfloor \cdot \rfloor$ stands for the integer part. The sequence $d_\alpha(x) = (a_n)_{n \geq 1}$ is the $\alpha$-expansion of $x$ and $L(\alpha)$ denotes the set of finite words having an occurrence in some sequence $d_\alpha(x)$, $x \in [0, 1]$. Let $d_\alpha(1) = (t_n)_{n \geq 1}$. If there exist $N \geq 0$, $p > 0$ such that, for all $n \geq N$, we have $t_{n+p} = t_n$, then $\alpha$ is said to be a Parry number, sometimes called a $\beta$-number (for more details about these numbers, see [102] or [62]). Observe that integers greater or equal to 2 are Parry numbers.

The following result relates Bertrand numeration systems to languages defined by some real number.
**Theorem 2.2** (A. Bertrand-Mathis [14]). Let $U$ be a numeration basis. It is a Bertrand numeration basis if and only if there exists a real number $\alpha > 1$ such that $\text{rep}_U(\mathbb{N}) = L(\alpha)$. In this case, if $U$ is linear then $\alpha$ is a root of the characteristic polynomial of $U$.

**Theorem 2.3** (A. Bertrand-Mathis [13]). Let $\alpha > 1$ be a real number. The language $L(\alpha)$ is regular if and only if $\alpha$ is a Parry number.

Associated with a Parry number $\beta$, one can define the notion of beta-polynomial. For details, see [72] or [12, Chapter 2]. First we define the canonical beta-polynomial. If $d_\beta(1)$ is eventually constant and equal to 0: $d_\beta(1) = t_1 \cdots t_m 0^\omega$, with $t_m \neq 0$, then we set $G_\beta(X) = X^m - \sum_{i=1}^m t_i X^{m-i}$ and $r = m$. Otherwise, $d_\beta(1)$ is eventually periodic: $d_\beta(1) = t_1 \cdots t_m (t_{m+1} \cdots t_{m+p})^\omega$, with $m$ and $p$ being minimal. Then we set $G_\beta(X) = X^{m+p} - \sum_{i=1}^{m+p} t_i X^{m+p-i} - X^m + \sum_{i=1}^m t_i X^{m-i}$ and $r = p$. Let $\beta$ be a Parry number. An extended beta-polynomial is a polynomial of the form $H_\beta(X) = G_\beta(X)(1 + X^r + \cdots + X^{rk}) X^n$ for $k, n \in \mathbb{N}$.

**Proposition 2.4.** [72] Let $U$ be a linear numeration basis with dominant root $\beta$, i.e., $\lim_{n \to \infty} U_{n+1}/U_n = \beta$ for some $\beta > 1$. If $\text{rep}_U(\mathbb{N})$ is regular, then $\beta$ is a Parry number.

**Theorem 2.5** (M. Hollander [72]). Let $U$ be a linear numeration basis whose dominant root $\beta$ is a Parry number.

- If $d_\beta(1)$ is infinite and eventually periodic, then $\text{rep}_U(\mathbb{N})$ is regular if and only if $U$ satisfies an extended beta-polynomial for $\beta$.
- If $d_\beta(1)$ is finite of length $m$, then: if $U$ satisfies an extended beta-polynomial for $\beta$ then $\text{rep}_U(\mathbb{N})$ is regular; and conversely if $\text{rep}_U(\mathbb{N})$ is regular, then $U$ satisfies either an extended beta-polynomial for $\beta$, $H_\beta(X)$, or a polynomial of the form $(X^m - 1)H_\beta(X)$.

Ultimately periodic sets are recognizable for any linear numeration basis.

**Proposition 2.6** (Folklore [12, 90]). Let $a, b \geq 0$. If $U = (U_n)_{n \geq 0}$ is a linear numeration basis, then

$$\pi^{-1}_{A_U, U}(a N + b) = \left\{ c_\ell \cdots c_0 \in A_U^* \mid \sum_{k=0}^{\ell} c_k U_k \in a N + b \right\}$$

is accepted by a DFA that can be effectively constructed. In particular, if $\mathbb{N}$ is $U$-recognizable, then any ultimately periodic set is $U$-recognizable.

To conclude this section, consider again the integer base numeration systems.

**Example 2.2.** The set $P_2 = \{2^n \mid n \geq 0\}$ of powers of two is trivially 2-recognizable because $\text{rep}_2(P_2) = 10^*$. Since the difference between any two consecutive elements in $P_2$ is of the form $2^n$, the set $P_2$ is not ultimately periodic. As a consequence of Cobham’s theorem, the set $P_2$ is, for instance, neither 3-recognizable nor 5-recognizable.

One could also consider the case when the two bases $k$ and $\ell$ are multiplicatively dependent. This case is much easier and can be considered as an exercise.
Proposition 2.7. Let $k, \ell \geq 2$ be two multiplicatively dependent integers. A set $X \subseteq \mathbb{N}$ is $k$-recognizable if and only if it is $\ell$-recognizable.

The theorem of Cobham implies that ultimately periodic sets are the only infinite sets that are $k$-recognizable for every $k \geq 2$. We have seen so far that there exist sets (like the set $P_2$ of powers of two) that are only recognizable for some specific bases: exactly all bases belonging to a unique equivalence class for the equivalence relation $\equiv$ over $\mathbb{N}_{\geq 2}$. To see that a given infinite ordered set $X = \{x_0 < x_1 < x_2 < \cdots \}$ is $k$-recognizable for no base $k \geq 2$ at all, we can use results like the following one, where the behavior of the ratio (resp., difference) of any two consecutive elements in $X$ is studied through the quantities

$$R_X = \limsup_{i \to \infty} \frac{x_{i+1}}{x_i} \quad \text{and} \quad D_X = \limsup_{i \to \infty} (x_{i+1} - x_i).$$

Theorem 2.8 (Gap theorem [38]). Let $k \geq 2$. If $X \subseteq \mathbb{N}$ is a $k$-recognizable infinite subset of $\mathbb{N}$, then either $R_X > 1$ or $D_X < +\infty$.

Corollary 2.9. Let $a \in \mathbb{N}_{\geq 2}$. The set of primes and the set $\{n^a \mid n \geq 0\}$ are not $k$-recognizable for any integer base $k \geq 2$.

Proofs of the gap theorem and its corollary can also be found in [55]. For more results on primes; also see Chapter 25 “Automata in number theory” of this handbook.

Definition 2.5. An infinite ordered set $X = \{x_0 < x_1 < x_2 < \cdots \}$ such that $D_X < +\infty$ is said to be syndetic or with bounded gaps: there exists $C > 0$ such that for all $n \geq 0$, $x_{n+1} - x_n < C$. In particular, any ultimately periodic set is syndetic. The converse does not hold; see, for instance Example 3.1.

Remark 2.10. Note that syndeticity occurs in various contexts, such as ergodic theory. As an example, a subset of an Abelian group $G$ is said to be syndetic if finitely many translates of it cover $G$. The term “syndetic” was first used in [66]. Note that in [68] the following result is proved. Let $\alpha, \beta > 1$ be multiplicatively independent real numbers. If a set $X \subseteq \mathbb{N}$ is $\alpha$-recognizable and $\beta$-recognizable, for the Bertrand numeration systems based, respectively, on the real numbers $\alpha$ and $\beta$ in the sense of [14] and Theorem 2.2, then $X$ is syndetic.

Cobham’s original proof of Theorem 1.1 appeared in [37] and we quote [55]: “The proof is correct, long and hard. It is a challenge to find a more reasonable proof of this fine theorem”. Then G. Hansel provided a simpler presentation in [67], and one can see [104] or the dedicated chapter in [9] for an expository presentation. Prior to these last two references, one should read [116]. Usually the first step to prove Cobham’s theorem is to show the syndeticity of the considered set. See Section 5.3. T. Krebs recently presented a short proof of Cobham’s theorem without using Kronecker theorem [82].
3 Automatic sequences

As explained in Corollary 3.3 presented in this section, the formalism of $k$-recognizable
sets is equivalent to that of $k$-automatic sequences\footnote{We indifferently use the terms sequence and infinite word.}. Let us recall briefly what they are.

An infinite word $x = (x_n)_{n \geq 0} \in B^\mathbb{N}$ over an alphabet $B$ is said to be $k$-automatic if there exists a DFAO (deterministic finite automaton with output) over the alphabet $[0, k - 1]$, $(Q, [0, k - 1], \cdot, q_0, B, \tau)$ such that, for all $n \geq 0$,

$$x_n = \tau(q_0 \cdot \text{rep}_k(n)) .$$

The transition function is $\cdot : Q \times [0, k - 1] \to Q$ and can easily be extended to $Q \times [0, k - 1]^*$ by $q \cdot \varepsilon = q$ and $q \cdot wa = (q \cdot w) \cdot a$. The output function is $\tau : Q \to B$. Roughly speaking, the $n$th term of the sequence is obtained by feeding a DFAO with the $k$-ary representation of $n$. For a complete and comprehensive exposition on $k$-automatic sequences and their applications, see the book [9]. We equally use the terms of sequences or (right-) infinite words. For more information about combinatorics on words, see [89, 90] or also J. Cassaigne and F. Nicolas’ chapter in [12, Chapter 4].

**Definition 3.1.** Let $\sigma : A^* \to A^*$ be a morphism, i.e., $\sigma(uv) = \sigma(u)\sigma(v)$ for all $u, v \in A^*$. Naturally such a map can be defined on $A^\omega$. A finite or infinite word $x$ such that $\sigma(x) = x$ is said to be a fixed point of $\sigma$. A morphism $\sigma : A^* \to A^*$ is completely determined by the images of the letters in $A$. In particular, if there exists $k \geq 0$ such that $|\sigma(a)| = k$ for all $a \in A$, then $\sigma$ is said to be of $k$-uniform or simply uniform. A 1-uniform morphism is called a coding. If there exist a letter $a \in A$ and a word $u \in A^*$ such that $\sigma(a) = au$ and moreover, if $\lim_{n \to +\infty} |\sigma^n(a)| = +\infty$, then $\sigma$ is said to be prolongable on $a$ or to be a substitution. Let $\sigma : A^* \to A^*$ be a morphism prolongable on $a$. We have

$$\sigma(a) = au, \quad \sigma^2(a) = au\sigma(u), \quad \sigma^3(a) = au\sigma(u)\sigma^2(u), \ldots.$$ 

Since for all $n \in \mathbb{N}$, $\sigma^n(a)$ is a prefix of $\sigma^{n+1}(a)$ and because $|\sigma^n(a)|$ tends to infinity when $n \to +\infty$, the sequence $(\sigma^n(a))_{n \geq 0}$ converges (for the usual product topology on words — see, for instance (6.2)) to an infinite word denoted by $\sigma^\infty(a)$ and given by

$$\sigma^\infty(a) := \lim_{n \to +\infty} \sigma^n(a) = au\sigma(u)\sigma^2(u)\sigma^3(u)\cdots .$$

This infinite word is a fixed point of $\sigma$. An infinite word obtained by iterating a prolongable morphism in this way is said to be purely substitutive (or pure morphic). If $\sigma : A^* \to B^*$ is a non-erasing morphism, it can be extended to a map from $A^\mathbb{N}$ to $B^\mathbb{N}$ as follows. If $x = x_0x_1\cdots$ is an infinite word over $A$, then the sequence of words $(\sigma(x_0\cdots x_{n-1}))_{n \geq 0}$ is easily seen to converge to an infinite word over $B$. Its limit is denoted by $\sigma(x) = \sigma(x_0)\sigma(x_1)\sigma(x_2)\cdots$. If $x \in A^\mathbb{N}$ is purely substitutive and if $\tau : A \to B$ is a coding, then the word $y = \tau(x)$ is said to be substitutive.

Another result due to A. Cobham is the following; see [38]. The idea is to associate a DFA over $[0, k - 1]$ with every $k$-uniform morphism.
Theorem 3.1. Let $k \geq 2$. A sequence $x = (x_n)_{n \geq 0} \in B^N$ is $k$-automatic if and only if there exist a $k$-uniform morphism $\sigma : A^* \to A^*$ prolongable on a letter $a \in A$ and a coding $\tau : A \to B$ such that $x = \tau(\sigma^\infty(a))$.

Theorem 3.2 (Eilenberg [55]). A sequence $x = (x_n)_{n \geq 0}$ is $k$-automatic if and only if its $k$-kernel $N_k(x) = \{(x_{k^e + d})_{n \geq 0} \mid e \geq 0, 0 \leq d < k^e\}$ is finite.

Definition 3.2. The characteristic sequence $\|X\| \in \{0, 1\}^N$ of a set $X \subseteq N$ is defined by $\|X\|(n) = 1$ if and only if $n \in X$.

An infinite word $x \in A^\omega$ is ultimately periodic if there exist two finite words $u, v \in A^+$ such that $x = uv^\omega$. If $u = \varepsilon$, then $x$ is periodic. Obviously, a set $X \subseteq N$ is ultimately periodic if and only if $\|X\|$ is an ultimately periodic word over $\{0, 1\}$. In that case, there exist two finite words $u \in \{0, 1\}^*$ and $v \in \{0, 1\}^+$ such that $\|X\| = uv^\omega$. In particular, $|v|$ is a period of $X$. If $u$ and $v$ are chosen of minimal length, then $|u|$ (resp., $|v|$) is said to be the preperiod or index of $X$ (resp., the period of $X$). If $u = \varepsilon$, then $X$ is (purely) periodic. Periodic sets are, in particular, ultimately periodic.

Corollary 3.3. Let $k \geq 2$. If $x = (x_n)_{n \geq 0} \in B^N$ is a $k$-automatic sequence, then the set $\{ n \geq 0 \mid x_n = b \}$ is $k$-recognizable for all $b \in B$. Conversely, if a set $X \subseteq N$ is $k$-recognizable, then its characteristic sequence is $k$-automatic.

Theorem 3.4 (Cobham’s theorem, version 2). Let $k, \ell \geq 2$ be two multiplicatively independent integers. An infinite word $x = (x_n)_{n \geq 0} \in B^N$ is both $k$-automatic and $\ell$-automatic if and only if it is ultimately periodic.

Remark 3.5. Using the framework of $k$-automatic sequences instead of the formalism of $k$-recognizable sets turns out to be useful. For instance, consider the complexity function of an infinite word $x$, which maps $n \in N$ onto the number $p_x(n)$ of distinct factors of length $n$ occurring in $x$. The Morse–Hedlund theorem states that $x$ is ultimately periodic if and only if $p_x$ is bounded by some constant. This result appeared first in [96]. Proofs can be found in classical textbooks such as [9, 89].

It is also well known that for a $k$-automatic sequence $x$, $p_x \in O(n)$; again see the seminal paper [38]. This latter result can be used to show that particular sets are not $k$-recognizable for any $k \geq 2$: for instance, those sets whose characteristic sequence $\|X\|$ has a complexity function such that $\lim_{n \to +\infty} p_{1X}(n)/n = +\infty$. For the behavior of $p_x$ in the substitutive case, see the survey [4] or [12, Chapter 4].

Example 3.1. Iterating the morphism $\sigma : 0 \mapsto 01, 1 \mapsto 10$, we get the Thue–Morse word $(t_n)_{n \geq 0} = \sigma^\infty(0) = 01101001100110100101101100110 \cdots$. For an account of this celebrated word, see [8] and [60, Chapter 2]. It is a 2-automatic word; the $n$th letter in the word is 0 if and only if $\text{rep}_2(n)$ contains an even number of 1’s. This word is generated by the DFAO represented in Figure 2. In particular, the set

$$X_2 = \left\{ n \in N \mid \text{rep}_2(n) = c_1 \cdots c_0 \text{ and } \sum_{i=0}^t c_i \equiv 0 \pmod 2 \right\}$$
4 Multidimensional extension and first-order logic

4.1 Subsets of $\mathbb{N}^d$

To extend the concept of $k$-recognizability to subsets of $\mathbb{N}^d$, $d \geq 2$, it is natural to consider $d$-tuples of $k$-ary representations. To be self-contained, we repeat the discussions of Chapter 25 “Automata in number theory” of this handbook. To get $d$ words of the same length that have to be read simultaneously by an automaton, the shortest ones are padded with leading zeroes. We extend the definition of $\text{rep}_k$ to a map of domain $\mathbb{N}^d$ as follows. If $n_1, \ldots, n_d$ are non-negative integers, then we consider the word

$$\text{rep}_k(n_1, \ldots, n_d) := \begin{pmatrix} 0^{m-\|\text{rep}_k(n_1)\|} \text{rep}_k(n_1) \\ \vdots \\ 0^{m-\|\text{rep}_k(n_d)\|} \text{rep}_k(n_d) \end{pmatrix} \in ([0, k-1]^d)^*$$

where $m = \max\{|\text{rep}_k(n_1)|, \ldots, |\text{rep}_k(n_d)|\}$. A subset $X$ of $\mathbb{N}^d$ is $k$-recognizable if the corresponding language $\text{rep}_k(X)$ is accepted by a finite automaton over the alphabet $[0, k-1]^d$ which is the Cartesian product of $d$ copies of $[0, k-1]$. This automaton is reading $d$ digits at a time (one for each component): this is why we need $d$ words of the same length.

Example 4.1. Consider the automaton depicted in Figure 3 (the sink is not represented). It accepts $(\varepsilon, \varepsilon)$ and all pairs of words of the form $(u0, 0u)$ where $u \in 1 \{0, 1\}^*$. This means that the set $\{(2n, n) \mid n \geq 0\}$ is 2-recognizable.

Note that the notion of $k$-automatic sequence and Theorem 3.1 have been extended accordingly in [119, 120] where the images by a morphism of letters are $d$-dimensional cubes of size $k$.

Extending the concept of ultimately periodic sets to subsets of $\mathbb{N}^d$, with $d \geq 2$, is at first glance not so easy. We use bold face letters to represent elements in $\mathbb{N}^d$. For instance, one could take the following definition of a (purely) periodic subset $X \subseteq \mathbb{N}^d$. 

\[ X = \{(n, k) \mid k \geq 0\} \]
There exists a non-zero element $p \in \mathbb{N}^d$ such that $x \in X$ if and only if $x + p \in X$. As we will see (Remark 4.2, Proposition 6.9 and Theorem 6.11), it turns out that this definition is not compatible with the extension of Cobham’s theorem in $d$ dimensions. Therefore we will consider sets definable in $\langle \mathbb{N}, + \rangle$. Let us mention Nivat’s conjecture connecting such a notion of periodicity in higher dimensions with the notion of block complexity as introduced in Remark 3.5: let $X \subset \mathbb{Z}^2$. If there exist positive integers $n_1, n_2$ such that $p_X(n_1, n_2) \leq n_1 n_2$, then $X$ is periodic, where $p_X(n_1, n_2)$ counts the number of distinct blocks of size $n_1 \times n_2$ occurring in $X$. See [98] and, in particular, [109] for details and pointers to the existing bibliography. The reference [53] establishes a connection with the next section.

4.2 Logic and $k$-definable sets

The formalism of first-order logic is probably the best suited to present a natural extension (in the sense of Cobham’s theorem) of the definition of ultimately periodic sets in $d$ dimensions. See [107, 108] or the survey [16]. For a textbook presentation, see [114]. In Presburger arithmetic $\langle \mathbb{N}, + \rangle$, the variables range over $\mathbb{N}$ and we have at our disposal the connectives $\land, \lor, \neg, \rightarrow, \leftrightarrow$, the equality symbol $=$ and the quantifiers $\forall$ and $\exists$ that can only be applied to variables. This is the reason we speak of first-order logic; in second-order logic, quantifiers can be applied to relations, and in monadic second-order logic, only variables and unary relations, i.e., sets, may be quantified. If a variable is not within the scope of any quantifier, then this variable is said to be free. Formulas are built inductively from terms and atomic formulas. Here details have been omitted; see, for instance [29, 28, Section 3.1]. For example, order relations $<$, $\leq$, $\geq$ and $>$ can be added to the language by noticing that $x \leq y$ is equivalent to

\[(\exists z)(y = x + z).\]  \hfill (4.1)

In the same way, constants can also be added. For instance, $x = 0$ is equivalent to $(\forall y)(x \leq y)$ and $x = 1$ is equivalent to $\neg(x = 0)$ $\land$ $\forall y)(\neg(y = 0)$ $\rightarrow$ $(x \leq y)$. In general, the successor function $S(x) = y$ of $x$ is defined by

\[(x < y) \land (\forall z)((x < z) \rightarrow (y \leq z)).\]

For a complete account on the interactions between first-order logic and $k$-recognizable sets, see the excellent survey [29, 28].
**Remark 4.1.** We mainly discuss the case \( \langle \mathbb{N}, + \rangle \), but similar results are obtained for \( \langle \mathbb{Z}, +, \leq \rangle \). Note that if the variables belong to \( \mathbb{Z} \), then it is no longer possible to define \( \leq \) as in (4.1). So this order relation has to be added to the structure. The constant 0 can be defined by \( x + x = x \).

Let \( \varphi(x_1, \ldots, x_d) \) be a formula with \( d \) free variables \( x_1, \ldots, x_d \). Interpreting \( \varphi \) in \( \langle \mathbb{N}, + \rangle \) permits one to define the set of \( d \)-tuples of non-negative integers for which the formulas hold:

\[
\{(r_1, \ldots, r_d) \mid \langle \mathbb{N}, + \rangle \models \varphi[r_1, \ldots, r_d]\}.
\]

We write \( \langle \mathbb{N}, + \rangle \models \varphi[r_1, \ldots, r_d] \) whenever \( \varphi(x_1, \ldots, x_d) \) is satisfied in \( \langle \mathbb{N}, + \rangle \) when interpreting \( x_i \) by \( r_i \) for all \( i \in \{1, \ldots, d\} \). For the reader having no background in logic and model theory, the first chapters of [54] are worth reading.

**Remark 4.2.** The ultimately periodic sets of \( \mathbb{N} \) are exactly the sets that are definable in Presburger arithmetic. It is obvious that ultimately periodic sets of \( \mathbb{N} \) are definable. For instance, the set of even integers can be defined by \( \varphi(x) \equiv (\exists y)(x = y + y) \). Since constants can easily be defined, it is easy to write a formula for any arithmetic progression.

As an example, the formula \( \varphi(x) \equiv (\exists y)(x = S(S(y + y + y))) \) defines the progression \( 3\mathbb{N} + 2 \). In particular, multiplication by a fixed constant is definable in \( \langle \mathbb{N}, + \rangle \). Note that it is a classical result that the theory of \( \langle \mathbb{N}, +, \times \rangle \) is undecidable; see, for instance [15].

Adding congruences modulo any integer \( m \) permits quantifier elimination, which means that any formula expressed in Presburger arithmetic is equivalent to a formula using only \( \land, \lor, =, < \) and congruences; see [107, 108]. Presentations can also be found in [56, 85].

**Theorem 4.3** (Presburger). The structure \( \langle \mathbb{N}, +, <, (\equiv_m)_{m \geq 0} \rangle \) admits elimination of quantifiers.

This result can be used to prove that the theory of \( \langle \mathbb{N}, + \rangle \) is decidable. This can be done using the formalism of automata; see, for instance [29, 28].

**Corollary 4.4.** Any formula \( \varphi(x) \) in Presburger arithmetic \( \langle \mathbb{N}, + \rangle \) defines an ultimately periodic set of \( \mathbb{N} \).

Let \( k \geq 2 \). We add to the structure \( \langle \mathbb{N}, + \rangle \) a function \( V_k \) defined by \( V_k(0) = 1 \) and for all \( x > 0 \), \( V_k(x) \) is the greatest power of \( k \) dividing \( x \). As an example, we have \( V_2(6) = 2 \), \( V_2(20) = 4 \) and \( V_2(2^n) = 2^n \) for all \( n \geq 0 \). Again the theory of \( \langle \mathbb{N}, +, V_k \rangle \) can be shown to be decidable [29, 28]. The next result shows that, as for the \( k \)-automatic sequences, the logical framework within the richer structure \( \langle \mathbb{N}, +, V_k \rangle \) gives an equivalent presentation of the \( k \)-recognizable sets in any dimension. Proofs of the next three theorems can again be found in [29, 28], where a full account of the different approaches used to prove Theorem 4.5 is presented. For Büchi’s original paper; see [30].

**Theorem 4.5** (Büchi theorem). Let \( k \geq 2 \) and \( d \geq 1 \). A set \( X \subseteq \mathbb{N}^d \) is \( k \)-recognizable if and only if it can be defined by a first-order formula \( \varphi(x_1, \ldots, x_d) \) of \( \langle \mathbb{N}, +, V_k \rangle \).
For instance, the set $P_2$ introduced in Example 2.2 can be defined by the formula $\varphi(x) \equiv V_2(x) = x$. Note that Theorem 4.5 holds for Pisot numeration systems given in Definition 2.3; see [27] where the function $V_k$ is modified accordingly. This is partially based on the fact that in a Pisot numeration system the normalization function is realized by a finite automaton (see [62]), which allows one to consider addition of integers: first perform addition digit-wise without any carry, then normalize the result.

**Theorem 4.6** (Cobham’s theorem, version 3). Let $k, \ell \geq 2$ be two multiplicatively independent integers. A set $X \subseteq \mathbb{N}$ can be defined by a first-order formula in $\langle \mathbb{N}, +, V_k \rangle$ and by a first-order formula in $\langle \mathbb{N}, +, V_\ell \rangle$ if and only if it can be defined by a first-order formula in $\langle \mathbb{N}, + \rangle$.

This theorem still holds in higher dimensions, and is called the Cobham–Semenov theorem. In this respect, the notion of subset of $\mathbb{N}^d$ definable in Presburger arithmetic $\langle \mathbb{N}, + \rangle$ is the right extension of periodicity in a multidimensional setting. For Semenov’s original paper; see [121].

**Theorem 4.7** (Cobham–Semenov theorem). Let $k, \ell \geq 2$ be two multiplicatively independent integers. A set $X \subseteq \mathbb{N}^d$ can be defined by a first-order formula in $\langle \mathbb{N}, +, V_k \rangle$ and by a first-order formula in $\langle \mathbb{N}, +, V_\ell \rangle$ if and only if it can be defined by a first-order formula in $\langle \mathbb{N}, + \rangle$.

Subsets of $\mathbb{N}^d$ defined by a first-order formula in $\langle \mathbb{N}, + \rangle$ are characterized in [65]. The nice criterion of Muchnik appeared first in 1991 and is given in [97]. See Proposition 6.9 for its precise statement. Using this latter characterization, a proof of Theorem 4.7 is presented in [29, 28]. The logical framework has given rise to several works. Let us mention chronologically [126, 127] and [93, 94]. In [94, Section 5] the authors interestingly show how to reduce Semenov’s theorem to Cobham’s theorem: “Nothing new in higher dimensions”. Also extensions to non-standard numeration systems are considered in [105] and [15]. In this latter paper, the Cobham–Semenov theorem is proved for two Pisot numeration systems.

## 5 Numeration systems and substitutions

### 5.1 Substitutive sets and abstract numeration systems

In Sections 4.1 and 4.2, we have mainly extended the notion of recognizability to subsets of $\mathbb{N}^d$. Now we consider another extension of recognizability. In Corollary 3.3, we have seen that a $k$-recognizable set has a characteristic sequence generated by a uniform substitution and the application of an extra coding. It is rather easy to define sets of integers encoded by a characteristic sequence generated by an arbitrary substitution and an extra coding; that is, those for which the characteristic sequence is morphic. This generalization permits one to obtain a larger class of infinite words, and hence a larger class of sets of integers.
Example 5.1. Consider the morphism $\sigma : \{a, b, c\}^* \to \{a, b, c\}^*$ given by $\sigma(a) = abcc$, $\sigma(b) = bcec$, $\sigma(c) = c$ and the coding $\tau : a, b \mapsto 1, c \mapsto 0$. We get

$$\sigma^\infty(a) = abecbecebecccccccccccccccedbecccbececccccccccccccbecc \ldots$$

and $\tau(\sigma^\infty(a)) = 0100100001000001000000010000000000100000000001000000000010000000000100 \ldots$. Using the special form of the images by $\sigma$ of $b$ and $c$, it is not difficult to see that the difference between the position of the $n$th and $(n + 1)$st $b$ in $\sigma^\infty(a)$ is $2n + 1$. Hence $\tau(\sigma^\infty(a))$ is the characteristic sequence of the set of squares and it is substitutive. From Corollary 2.9 the set of squares is never $k$-recognizable for any integer base $k$.

**Definition 5.1.** As a natural extension of the concept of recognizability, we may consider sets $X \subseteq \mathbb{N}$ having a characteristic sequence $\mathbb{1}_X$ which is (purely) substitutive. Such a set is said to be a (purely) substitutive set. In particular, $k$-recognizable sets are substitutive.

With Theorem 5.2 it will turn out that the formalism of substitutive sets is equivalent to the one of abstract numeration systems.

**Definition 5.2.** [86] An abstract numeration system (or ANS) is a triple $\mathcal{S} = (L, A, \prec)$ where $L$ is an infinite regular language over a totally ordered alphabet $(A, \prec)$. The map $\text{rep}_\mathcal{S} : \mathbb{N} \to L$ is the one-to-one correspondence mapping $n \in \mathbb{N}$ onto the $(n + 1)$th word in the genealogically ordered language $L$, which is called the $\mathcal{S}$-representation of $n$. In particular, a set $X \subseteq \mathbb{N}$ is $\mathcal{S}$-recognizable if $\text{rep}_\mathcal{S}(X)$ is regular, and $\mathbb{N}$ is trivially $\mathcal{S}$-recognizable because $\text{rep}_\mathcal{S}(\mathbb{N}) = L$. Recall that in the genealogical order (also called radix or military order), words are first ordered by increasing length and for words of the same length, one uses the lexicographic ordering induced by the order $\prec$ on $A$.

Example 5.2. Consider the language $L = a^*b^* \cup a^*c^*$ with $a < b < c$. The first few words in $L$ are $\varepsilon, a, b, c, aa, ab, ac, bb, cc, aaa, aab, aac, abb, \ldots$. This means that for the ANS $\mathcal{S}$ built on $L$, the integer 0 is represented by $\varepsilon$, the integer 1 by $a$, the integer 2 by $b$, the integer 3 by $c$, the integer 4 by $aa$, etc. Since $L$ contains exactly $2n + 1$ words of length $n$ for all $n \geq 0$, we have that $n^2$ is represented by $a^n$ for all $n \geq 0$. In particular, the set $\{n^2 \mid n \geq 0\}$ is $\mathcal{S}$-recognizable because $a^*$ is regular. It is well known that in a regular language $L$, the set of the lexicographically first words of each length in the genealogically ordered language $L$ is regular; see [123].

Pisot numeration systems are special cases of ANS. Indeed, if the numeration basis $U = (U_n)_{n \geq 0}$ defines a Pisot numeration system, then $\text{rep}_U(\mathbb{N})$ is regular.

Example 5.3. Consider the Fibonacci sequence and the language $L = 1\{0, 01\}^* \cup \{\varepsilon\}$ defined in Example 2.1. To get the representation of an integer $n$, one can either decompose $n$ using the greedy algorithm or, order the words in $L$ genealogically and take the $(n + 1)$th element.

Theorem 5.1. [86] Let $\mathcal{S} = (L, A, \prec)$ be an abstract numeration system. Any ultimately periodic set is $\mathcal{S}$-recognizable.
Note that in [83], it is, in particular, proved that this latter result cannot be extended to context-free languages. Specific cases of $S$-recognizable sets are discussed in P. Lecomte and M. Rigo’s chapter in [12, Chapter 3]. We have an extension of Theorem 3.1.

**Theorem 5.2.** Let $x = (x_n)_{n \geq 0}$ be an infinite word over an alphabet $B$. This word is substitutive if and only if there exists an abstract numeration system $S = (L, A, <)$ such that $x$ is $S$-automatic, i.e., there exists a DFAO $(Q, A, \cdot, \{q_0\}, B, \tau)$ such that for all $n \geq 0$, $x_n = \tau(\rep_S(n))$.

A proof of this result is given in [112, 115] and a comprehensive treatment is given in [12, Chapter 3]. In that respect, we also obtain an extension of Corollary 3.3.

**Corollary 5.4.** Let $x = (x_n)_{n \geq 0}$ be an infinite substitutive word over an alphabet $B$. There exists an ANS $S$ such that for all $b \in B$, $\{n \geq 0 \mid x_n = b\}$ is $S$-recognizable. Conversely, if a set $X \subseteq \mathbb{N}$ is $S$-recognizable, then its characteristic sequence is $S$-automatic.

**Corollary 5.3.** A set $X \subseteq \mathbb{N}$ is substitutive if and only if there exists an ANS $S$ such that $X$ is $S$-recognizable.

### 5.2 Cobham’s theorem for substitutive sets

In the context of substitutive sets of integers, how could a Cobham-like theorem be expressed, i.e., what is playing the role of a base? Assume that there exist two purely substitutive infinite words $x \in A^\omega$ and $y \in B^\omega$, respectively, generated by the morphisms $\sigma : A^* \rightarrow A^*$ prolongable on $a \in A$ and $\tau : B^* \rightarrow B^*$ prolongable on $b \in B$, i.e., $\sigma^\infty(a) = x$ and $\tau^\infty(b) = y$. Consider two codings $\lambda : A \rightarrow \{0, 1\}$ and $\mu : B \rightarrow \{0, 1\}$ such that $\lambda(x) = \mu(y)$. This situation corresponds to the case where a set (here, given by its characteristic word) is recognizable in two a priori different numeration systems.

If $A = B$ and $\tau = \sigma^m$ for some $m \geq 1$, then nothing particular can be said about the infinite word $\lambda(x)$: iterating $\sigma$ or $\sigma^m$ from the same prolongable letter leads to the same fixed point. So we must introduce a notion analogous to the one of multiplicatively independent bases related to the substitutions $\sigma$ and $\lambda$.

**Definition 5.3.** Let $\sigma : A^* \rightarrow A^*$ be a substitution over an alphabet $A$. The matrix $M_{\sigma} \in \mathbb{N}^{A \times A}$ associated with $\sigma$ is called the incidence matrix of $\sigma$ and is defined as follows:

$$\text{for all } a, b \in A, \ (M_{\sigma})_{a,b} = |\sigma(b)|_a.$$ 

A square matrix $M \in \mathbb{R}^{n \times n}$ with entries in $\mathbb{R}_{\geq 0}$ is irreducible if, for all $i, j$, there exists $k$ such that $(M^k)_{i,j} > 0$. A square matrix $M \in \mathbb{R}^{n \times n}$ with entries in $\mathbb{R}_{\geq 0}$ is primitive if there exists $k$ such that, for all $i, j$, we have $(M^k)_{i,j} > 0$. Similarly, a substitution over the alphabet $A$ is irreducible (resp., primitive) if its incidence matrix is irreducible (resp., primitive). Otherwise stated, a substitution $\sigma : A^* \rightarrow A^*$ is primitive if there exists an integer $n \geq 1$ such that, for all $a \in A$, all the letters in $A$ appear in the image of $\sigma^n(a)$. 

Let us denote by $\mathbf{P}$ the abelianisation map (or Parikh map) that maps a word $w$ over $A = \{a_1, \ldots, a_r\}$ to the $r$-tuple $(|w|_{a_1}, \ldots, |w|_{a_r})$. The matrix $M_\sigma$ can be defined by its columns:

$$M_\sigma = (\mathbf{P}(\sigma(a_1)) \cdots \mathbf{P}(\sigma(a_r))),$$

and it satisfies the condition

for all $w \in A^*$, $\mathbf{P}(\sigma(w)) = M_\sigma \mathbf{P}(w)$.

**Remark 5.5.** If a matrix $M$ is primitive, the celebrated theorem of Perron can be used; see standard textbooks [76] or [64, 122]. A presentation is also given in [88]. To recap some of the key points, $M$ has a unique dominant real eigenvalue $\beta > 0$ and there exists an eigenvector with positive entries associated with $\beta$. Also, for all $i, j$, there exists $c_{i,j}$ such that $(M^n)_{i,j} = c_{i,j} \beta^n + o(\beta^n)$. For instance, primitivity of $M_\sigma$ implies the existence of the frequency of any factor occurring in any fixed point of $\sigma$. Note that

$$\text{if } \mathbf{P}(w) = ^t(p_1, \ldots, p_r), \text{ then } |w| = \sum_{i=1}^{r} p_i. \quad (5.1)$$

Hence, the value $|\sigma^n(a_j)|$ is obtained by summing up the entries in the $j$th column of $M_\sigma^n$ for all $n \geq 0$. If $\sigma$ is primitive, then there exists some $C_j$ such that $|\sigma^n(a_j)| = C_j \beta^n + o(\beta^n)$. In particular, if $\sigma$ is prolongable on $a$, then $|\sigma^n(a)| \sim C \beta^n$, for some $C > 0$.

In the general case of a matrix $M$ with non-negative entries, one can use the Perron–Frobenius theorem for each of the irreducible components of $M$ (they correspond to the strongly connected components of the associated graph and are also called communicating classes). Thus any non-negative matrix $M$ has a real eigenvalue $\alpha$ which is greater or equal to the modulus of any other eigenvalue. We call $\alpha$ the *dominant eigenvalue* of $M$. Moreover, if we exclude the case where $\alpha = 1$, then there exists a positive integer $p$ such that $M_p$ has a dominant eigenvalue $\alpha_p$ which is a Perron number; see [88, p. 369]. A *Perron number* is an algebraic integer $\alpha > 1$ such that all its algebraic conjugates have modulus less than $\alpha$. In particular, if we replace a prolongable substitution $\sigma$ such that $M_\sigma$ has a dominant eigenvalue $\alpha > 1$, with a convenient power $\sigma^p$ of $\sigma$, then we can assume that the dominant eigenvalue of $\sigma$ is a Perron number.

**Definition 5.4.** Let $\sigma : A^* \to A^*$ be a substitution prolongable on $a \in A$ such that all letters of $A$ have an occurrence in $\sigma^\infty(a)$. Let $\alpha > 1$ be the dominant eigenvalue of the incidence matrix of $\sigma$. Let $\phi : A \to B^*$ be a coding. We say $\phi(\sigma^\infty(a))$ is an $\alpha$-substitutive infinite word (with respect to $\sigma$). In view of Definition 5.1, this notion can be applied to subsets of $\mathbb{N}$. If, moreover, $\sigma$ is primitive, then $\phi(\sigma^\infty(a))$ is said to be a *primitive $\alpha$-substitutive infinite word* (w.r.t. $\sigma$).

Observe that $k$-automatic infinite words are $k$-substitutive infinite words.

**Example 5.4.** Consider the substitution $\sigma$ defined by $\sigma(a) = aa0a$, $\sigma(0) = 01$ and $\sigma(1) = 10$. Its dominant eigenvalue is 3. It is prolongable on $a$, 0 and 1. The fixed point $x$ of $\sigma$ starting with 0 is the Thue-Morse sequence (see Example 3.1). Definition 5.4 does not imply that $x$ is 3-substitutive because $a$ does not appear in $x$. But the fixed point $y$ of $\sigma$ starting with $a$ is 3-substitutive.
Example 5.5. Consider the so-called Tribonacci word, which is the unique fixed point of \( \sigma : a \mapsto ab, b \mapsto ac, c \mapsto a \). See [125, 60]. The incidence matrix of \( \sigma \) is

\[
M_\sigma = \begin{pmatrix}
1 & 1 & 1 \\
1 & 0 & 0 \\
0 & 1 & 0
\end{pmatrix}.
\]

One can check that \( M_\sigma^3 \) contains only positive entries. So the matrix is primitive. Let \( \alpha_T \approx 1.839 \) be the unique real root of the characteristic polynomial \( -X^3 + X^2 + X + 1 \) of \( M_\sigma \). The Tribonacci word \( T = abacabaab \cdots \) is primitive \( \alpha_T \)-substitutive. Let \( \tau : a \mapsto 1, b, c \mapsto 0 \) be a coding. The word \( \tau(T) \) is the characteristic sequence of a primitive \( \alpha_T \)-substitutive set of integers \( \{0, 2, 4, 6, 7, \ldots \} \).

To explain the substitutive extension of Cobham’s theorem we need the following definition.

Definition 5.5. Let \( S \) be a set of prolongable substitutions and \( x \) be an infinite word. If \( x \) is an \( \alpha \)-substitutive infinite word w.r.t. a substitution \( \sigma \) belonging to \( S \), then \( x \) is said to be \( \alpha \)-substitutive with respect to \( S \).

Let us consider the following Cobham-like statement depending on two sets \( S \) and \( S' \) of prolongable substitutions. It is useful to chronologically describe known results generalizing Cobham’s theorem in terms of substitutions leading to the most general statement for all substitutions.

Statement \((S, S')\). Let \( S \) and \( S' \) be two sets of prolongable substitutions. Let \( \alpha \) and \( \beta \) be two multiplicatively independent Perron numbers. Let \( x \in A^\omega \) where \( A \) is a finite alphabet. Then the following are equivalent:

1. the infinite word \( x \) is both \( \alpha \)-substitutive w.r.t. \( S \) and \( \beta \)-substitutive w.r.t. \( S' \);
2. the infinite word \( x \) is ultimately periodic.

Note that this statement excludes 1-substitutions, i.e., substitutions with a dominant eigenvalue equal to 1, because Perron numbers are larger than 1. The case of 1-substitutive infinite words will be mentioned in Subsection 5.6. Also notice that the substitutions we are dealing with can be erasing, i.e., at least one letter is sent onto the empty word. But from a result in [36, 9, 75], we can assume that the substitutions are non-erasing. Note that \( \alpha \) and \( \alpha^k \) are multiplicatively dependent.

Proposition 5.6. [52] Let \( x \) be an \( \alpha \)-substitutive infinite word. Then there exists an integer \( k \geq 1 \) such that \( x \) is \( \alpha^k \)-substitutive with respect to a non-erasing substitution.

The implication \((2) \Rightarrow (1)\) in the above general statement is not difficult to obtain, as mentioned in Remark 1.3 for the uniform situation.

Proposition 5.7. [48] Let \( x \) be an infinite word over a finite alphabet and \( \alpha \) be a Perron number. If \( x \) is periodic (resp., ultimately periodic), then \( x \) is primitive \( \alpha \)-substitutive (resp., \( \alpha \)-substitutive).
**Definition 5.6.** Let \( \sigma : A^* \to A^* \) and \( \tau : B^* \to B^* \) be two substitutions. We say that \( \sigma \) projects on \( \tau \) if there exists a coding \( \phi : A \to B \) such that

\[
\phi \circ \sigma = \tau \circ \phi.
\]  

(5.2)

The implication \((1) \Rightarrow (2)\) in Statement \((S, S')\) is known in many cases described below:

(i) When \( S = S' \) is the set of uniform substitutions, this is the classical theorem of Cobham.

(ii) In [57] S. Fabre proves the statement when \( S \) is the set of uniform substitutions and \( S' \) is a set of non-uniform substitutions related to some non-standard numeration systems.

(iii) When \( S = S' \) is the set of primitive substitutions, the statement is proved in [45]. The proof is based on a characterization of primitive substitutive sequences using the notion of return word [44]. A word \( w \) is a return word to \( u \) if \( wu \in L(x) \), \( u \) is a prefix of \( wu \) and \( u \) has exactly two occurrences in \( wu \).

(iv) When \( S = S' \) is the set of substitutions projecting on primitive substitutions, the statement is proved in [46]. This result is applied to generalize (ii). Using a characterization of \( U \)-recognizable sets of integers for a Bertrand numeration basis \( U \) [58], the main result of [46] extends Cobham’s theorem for a large family of non-standard numeration systems. This latter result includes a result obtained previously in [15] for Pisot numeration systems.

(v) Definition 5.8 and Theorem 5.17 describe the situation where \( S = S' = S_{\text{good}} \) (defined later). It includes all known and previously described situations for substitutions.

(vi) In [50], Statement \((S, S')\) is proven for the most general case that is \( S \) and \( S' \) are both the set of all substitutions. The final argument is based on a careful study of return words for non-primitive substitutive sequences.

**Example 5.6.** The Tribonacci word \( T \) is purely substitutive, but is \( k \)-automatic for no integer \( k \geq 2 \). Proceed by contradiction. Assume that there exists an integer \( k \geq 2 \) such that \( T \) is \( k \)-automatic. Then \( T \) is both \( k \)-substitutive and primitive \( \alpha_T \)-substitutive. By Theorem 5.17, \( T \) must be ultimately periodic, but it is not the case. The factor complexity of \( T \) is \( p_T(n) = 2n + 1 \). By the Morse–Hedlund theorem (see Remark 3.5), \( T \) is not ultimately periodic.

Let \( L(x) \) be the set of all factors of the infinite word \( x \). In [59], the following generalization of Cobham’s theorem is proved.

**Theorem 5.8.** Let \( k, \ell \geq 2 \) be two multiplicatively independent integers. Let \( x \) be a \( k \)-automatic infinite word and \( y \) be a \( \ell \)-automatic infinite word. If \( L(x) \subseteq L(y) \), then \( x \) is ultimately periodic.

The same result is valid in the primitive case.

**Theorem 5.9.** [45] Let \( x \) and \( y \) be, respectively, a primitive \( \alpha \)-substitutive infinite word and a primitive \( \beta \)-substitutive infinite word such that \( L(x) = L(y) \). If \( \alpha \) and \( \beta \) are multiplicatively independent, then \( x \) and \( y \) are periodic.
Note that under the hypothesis of Theorem 5.9, \(x\) and \(y\) are primitive substitutive infinite words. Thus \(L(x) = L(y)\) whenever \(L(x) \subset L(y)\). Observe that if \(y\) is the fixed point starting with \(a\), and \(x\) the fixed point starting with \(0\) of the substitution \(\sigma\) defined in Example 5.4, then \(L(x) \subset L(y)\), but \(x\) is not ultimately periodic.

In Sections 5.3 and 5.4 we give the main arguments to prove Statement \((S_{\text{good}}, S_{\text{good}})\).

### 5.3 Density, syndeticity and bounded gaps

The proofs of most of the generalizations of Cobham’s theorem are divided into two parts.

(i) Dealing with a subset \(X\) of integers, we have to prove that \(X\) is syndetic. Equivalently, dealing with an infinite word \(x\), we have to prove that the letters occurring infinitely many times in \(x\) appear with bounded gaps.

(ii) In the second part, the proof of the ultimate periodicity of \(X\) or \(x\) has to be carried out.

This section is devoted to the description of the main arguments that lead to the complete treatment of (i).

In the original proof of Cobham’s theorem one of the main arguments is that as \(k\) and \(\ell\) are multiplicatively independent (we refer to Theorem 1.1) the set \(\{k^n/\ell^m \mid n, m \in \mathbb{N}\}\) is dense in \([0, +\infty)\). In the uniform case, these powers refer to the length of the iterates of the substitutions. Indeed, suppose \(\sigma : A^* \rightarrow A^*\) is a \(k\)-uniform substitution. Then for every \(a \in A\) we have \(|\sigma^n(a)| = k^n\). Unsurprisingly, to be able to treat the non-uniform case, it is important to know that the set

\[
\left\{ \frac{|\sigma^n(a)|}{|\tau^m(b)|} \mid n, m \in \mathbb{N} \right\}
\]

is dense in \([0, +\infty)\), for some \(a, b \in A\). We explain below that \(|\sigma^n(a)|\) and \(|\tau^m(b)|\) are governed by the dominant eigenvalue of their incidence matrices. First we focus on part (i) and consider infinite words.

#### 5.3.1 The length of the iterates

The length of the iterates are described in the following lemma. Note that it includes erasing substitutions and substitutions with a dominant eigenvalue equal to \(1\). Observe that for the substitution \(\sigma\) defined by \(0 \mapsto 001\) and \(1 \mapsto 11\) we have \(|\sigma^n(0)| = (n + 2)2^{n-1}\) and \(|\sigma^n(1)| = 2^n\), showing that the situation is different from the uniform case. It can easily be described using the Jordan normal form of the incidence matrix \(M_\sigma\). Discussion of the following result can be found in [12, Section 4.7.3].

**Lemma 5.10** (Chapter III.7 in [118]). Let \(\sigma : A^* \rightarrow A^*\) be a substitution. For all \(a \in A\) one of the two following situations occurs

1. there exists \(N \in \mathbb{N}\) such that for all \(n > N\), \(|\sigma^n(a)| = 0\), or,
2. there exist \(d(a) \in \mathbb{N}\) and real numbers \(c(a), \theta(a)\) such that

\[
\lim_{n \to +\infty} \frac{|\sigma^n(a)|}{c(a)^n d(a)^n \theta(a)^n} = 1.
\]
Moreover, in the case (2), for all \( i \in \{0, \ldots, d(a)\} \) there exists a letter \( b \in A \) appearing in \( \sigma^i(a) \) for some \( j \in \mathbb{N} \) and such that

\[
\lim_{n \to +\infty} \frac{|\sigma^n(b)|}{e(b)n^d \lambda(a)n} = 1.
\]

**Definition 5.7.** Let \( \sigma \) be a non-erasing substitution. For all \( a \in A \), the pair \((d(a), \lambda(a))\) defined in Lemma 5.10 is called the growth type of \( A \). If \((d, \lambda)\) and \((e, \beta)\) are two growth types, then we say that \((d, \lambda)\) is less than \((e, \beta)\) (or \((d, \lambda) < (e, \beta)\)) whenever \( \lambda < \beta \) or, \( \theta = \beta \) and \( d < e \).

Consequently, if the growth type of \( a \in A \) is less than the growth type of \( b \in A \), then \( \lim_{n \to +\infty} |\sigma^n(a)|/|\sigma^n(b)| = 0 \). We say that \( a \in A \) is a growing letter if \((d(a), \lambda(a)) > (0, 1)\) or equivalently, if \( \lim_{n \to +\infty} |\sigma^n(a)| = +\infty \).

We set \( \Theta := \max\{\theta(a) \mid a \in A\} \), \( D := \max\{d(a) \mid \forall a \in A : \theta(a) = \Theta \} \) and \( A_{\text{max}} := \{a \in A \mid \theta(a) = \Theta, d(a) = D\} \). The dominant eigenvalue of \( M_{\sigma} \) is \( \Theta \). We say that the letters of \( A_{\text{max}} \) are of maximal growth and that \((D, \Theta)\) is the growth type of \( \sigma \). Consequently, we say that a substitutive infinite word \( y \) is \((D, \Theta)\)-substitutive if the underlying substitution is of growth type \((D, \Theta)\). Observe that, due to Lemma 5.10, any substitutive sequence is \((D, \Theta)\)-substitutive for some pair \((D, \Theta)\).

Observe that if \( \Theta = 1 \), then in view of the last part of Lemma 5.10, there exists at least one non-growing letter of growth type \((0, 1)\). Otherwise stated, if a letter has polynomial growth, then there exists at least one non-growing letter. Consequently \( \sigma \) is growing (i.e., all its letters are growing) if and only if \( \theta(a) > 1 \) for all \( a \in A \). We define

\[
\lambda_{\sigma} : A^* \to \mathbb{R}, \ u_0 \cdots u_{n-1} \mapsto \sum_{i=0}^{n-1} c(u_i) \mathbb{1}_{A_{\text{max}}}(u_i),
\]

where \( c : A \to \mathbb{R}_+ \) is defined in Lemma 5.10. From Lemma 5.10 we deduce the following lemma.

**Lemma 5.11.** For all \( u \in A^* \), we have \( \lim_{n \to +\infty} |\sigma^n(u)|/n^D \Theta^n = \lambda_{\sigma}(u) \).

We say that the word \( u \in A^* \) is of maximal growth if \( \lambda_{\sigma}(u) \neq 0 \).

**Corollary 5.12.** Let \( \sigma \) be a substitution of growth type \((D, \Theta)\). For all \( k \geq 1 \), the growth type of \( \sigma^k \) is \((D, \Theta^k)\).

### 5.3.2 Letters and words appear with bounded gaps

Recall that the first step in the proof of Cobham’s theorem is to prove that the letters occurring infinitely many times appear with bounded gaps. In our context, this implies the same property for words. Moreover, we can relax the multiplicative independence hypothesis in order to include 1-substitutions. Note that 1 and \( \alpha > 1 \) are multiplicatively dependent.

**Theorem 5.13.** [52] Let \( d, e \in \mathbb{N} \setminus \{0\} \) and \( \alpha, \beta \in [1, +\infty) \) such that \((d, \alpha) \neq (e, \beta)\) and satisfying one of the following three conditions:

(i) \( \alpha \) and \( \beta \) are multiplicatively independent;
(ii) $\alpha, \beta > 1$ and $d \neq e$;
(iii) $(\alpha, \beta) \neq (1, 1)$ and, $\beta = 1$ and $e \neq 0$, or, $\alpha = 1$ and $d \neq 0$.

Let $C$ be a finite alphabet. If $x \in C^\omega$ is both $(d, \alpha)$-substitutive and $(e, \beta)$-substitutive, then the words occurring infinitely many times in $x$ appear with bounded gaps.

The main argument used to prove this in [52] is the following.

**Theorem 5.14.** Let $d, e \in \mathbb{N}$ and $\alpha, \beta \in [1, +\infty)$. The set
\[
\Omega = \left\{ \frac{\alpha^n n^d}{\beta^m m^e} \mid n, m \in \mathbb{N} \right\}
\]
is dense in $[0, +\infty)$ if and only if one of the following three conditions holds:

(i) $\alpha$ and $\beta$ are multiplicatively independent;
(ii) $\alpha, \beta > 1$ and $d \neq e$;
(iii) $\beta = 1$ and $e \neq 0$, or, $\alpha = 1$ and $d \neq 0$.

**Sketch of the proof of Theorem 5.13.** We only consider the case where $\alpha$ and $\beta$ are multiplicatively independent.

Let $\sigma : A^* \to A^*$ be a substitution prolongable on a letter $a'$ having growth type $(d, \alpha)$. Let $\tau : B^* \to B^*$ be a substitution prolongable on a letter $b'$ having growth type $(e, \beta)$. Let $\phi : A \to C$ and $\psi : B \to C$ be two codings such that $\phi(\sigma^\infty(a')) = \psi(\tau^\infty(b')) = x$. Using Proposition 5.6 we may assume that $\sigma$ and $\tau$ are non-erasing. Suppose there is a letter $a$ having infinitely many occurrences in $x$, but that appears with unbounded gaps. Then the letters in $\phi^{-1}(\{a\})$ appear with unbounded gaps. To avoid extra technicalities (a complete treatment is considered in [52]), we assume that there is a letter $a$ having infinitely many occurrences in $x$, that does not contain any letter of $\phi^{-1}(\{a\})$. On the other hand, using a kind of pumping lemma for substitutions, one can show that there is a letter of $\psi^{-1}(\{a\})$ in $z$ at the index $c_3 n^e \beta n$.

Therefore, using Theorem 5.14, the letter $a$ appears in a word $\phi(w_n)$ for some $n$. This is not possible.

Now let us explain how to extend this result for a single letter to words. It uses what is called in [110] the substitutions of the words of length $n$. Let $u$ be a word of length $n$ occurring infinitely often in $x$. To prove that $u$ appears with bounded gaps in $x$, it suffices to prove that the letter 1 appears with bounded gaps in the infinite word $t \in \{0, 1\}^\mathbb{N}$ defined by
\[
t_i = \begin{cases} 1, & \text{if } x_i \cdots x_{i+n-1} = u; \\ 0, & \text{otherwise.} \end{cases}
\]

Let $A^n$ be the set of words of length $n$ over $A$. The infinite word $y^{(n)} = (y_n \cdots y_{i+n-1})_{i \geq 0}$ over the alphabet $A^n$ is a fixed point of the substitution $\sigma_n : (A^n)^* \to (A^n)^*$ defined, for all $(a_1 \cdots a_n) \in A^n$, by
\[
\sigma_n((a_1 \cdots a_n)) = (b_1 \cdots b_n)(b_2 \cdots b_{n+1}) \cdots (b_{|\sigma(a_1)|} \cdots b_{|\sigma(a_1)|+n-1})
\]
where $\sigma(a_1 \cdots a_n) = b_1 \cdots b_k$. For details; see Section V.4 in [110].
Let $\rho : A^n \to A^*$ be the coding defined by $\rho((b_1 \cdots b_n)) = b_1$ for all $(b_1 \cdots b_n) \in A^n$. We have $\rho \circ \sigma_n = \sigma \circ \rho$, and then $\rho \circ \sigma_n^k = \sigma^k \circ \rho$. Hence, if $\sigma$ is of growth type $(d, \alpha)$, then $y^{(n)}$ is $(d, \alpha)$-substitutive. Let $f : A^n \to \{0, 1\}$ be the coding defined by
\[
f((b_1 \cdots b_n)) = \begin{cases} 1, & \text{if } b_1 \cdots b_n = u; \\ 0, & \text{otherwise}. \end{cases}
\]
It is easy to see that $f(y^{(n)}) = t$, and hence $t$ is $(d, \alpha)$-substitutive. Then one proceeds in the same way with $\tau$ and uses the result for letters to conclude the proof.

5.4 Ultimate periodicity

**Definition 5.8.** Let $\sigma : A^* \to A^*$ be a substitution. If there exists a sub-alphabet $B \subseteq A$ such that for all $b \in B$, $\sigma(b) \in B^*$, then the substitution $\tau : B^* \to B^*$ defined by the restriction $\tau(b) = \sigma(b)$, for all $b \in B$, is a sub-substitution of $\sigma$. Note that $\sigma$ is, in particular, a sub-substitution of itself.

The substitution $\sigma$ having $\alpha$ as dominant eigenvalue is a "good" substitution if it has a primitive sub-substitution whose dominant eigenvalue is $\alpha$. So let us stress the fact that to be a "good" substitution, the sub-substitution has to be primitive and have the same dominant eigenvalue as the original substitution. We let $S_{\operatorname{good}}$ denote the set of good substitutions.

**Remark 5.15.** For all growing substitutions $\sigma$, there exists an integer $k$ such that $\sigma^k$ has a primitive sub-substitution. Hence by taking a convenient power of $\sigma$, the substitution can always be assumed to have a primitive sub-substitution.

Note that primitive substitutions and uniform substitutions are good substitutions. Now consider the substitution $\sigma : \{a, 0, 1\}^* \to \{a, 0, 1\}^*$ given by $\sigma : a \mapsto aa0, 0 \mapsto 01, 1 \mapsto 0$. Its dominant eigenvalue is 2 and it has only one primitive sub-substitution $(0 \mapsto 01, 1 \mapsto 0)$ whose dominant eigenvalue is $(1 + \sqrt{5})/2$, and hence it is not a good substitution.

**Remark 5.16.** Let $\sigma : A^* \to A^*$ and $\tau : B^* \to B^*$ be two substitutions such that $\sigma$ projects on $\tau$; recall (5.2) for the definition of projection. There exists a coding $\phi : A \to B$ such that $\phi \circ \sigma = \tau \circ \phi$. Note that $\phi \circ \sigma^n = \tau^n \circ \phi$. If $\tau$ is primitive, then it follows that $\sigma$ belongs to $S_{\operatorname{good}}$.

**Theorem 5.17.** Let $\alpha$ and $\beta$ be two multiplicatively independent Perron numbers. Let $x \in A^\omega$ where $A$ is a finite alphabet. Then the following are equivalent:

(i) the infinite word $x$ is both $\alpha$-substitutive w.r.t. $S_{\operatorname{good}}$ and $\beta$-substitutive w.r.t. $S_{\operatorname{good}}$;

(ii) the infinite word $x$ is ultimately periodic.

**Proof.** Let $\sigma : B^* \to B^*$ (resp. $\tau : C^* \to C^*$) be a substitution in $S_{\operatorname{good}}$ having $\alpha$ (resp., $\beta$) as its dominant eigenvalue and $\phi$ (resp., $\psi$) be a coding such that $x = \phi(\sigma^\infty(b))$ for some $b \in B$ (resp., $x = \psi(\tau^\infty(c))$ for some $c \in C$).

Let us first suppose that both substitutions are growing. In this way, taking a power if needed, we can suppose that they have primitive sub-substitutions.
By Theorem 5.13, the factors occurring infinitely many times in \( x \) appear with bounded gaps. Hence for any primitive and growing sub-substitutions \( \sigma \) and \( \tau \) of \( \sigma \) and of \( \tau \) respectively, we have \( \phi(L(\sigma)) = \psi(L(\tau)) = L \). Using Theorem 5.9 it follows that \( L \) is periodic, i.e., there exists a shortest word \( u \), appearing infinitely many times in \( x \), such that \( L = L(u^\infty) \). Thus \( u \) appears with bounded gaps. Let \( \mathcal{R}_u \) be the set of return words to \( u \). We recall that a word \( w \) is a return word to \( u \) if \( wu \) belongs to \( L(x) \), \( u \) is a prefix of \( wu \) and \( u \) has exactly two occurrences in \( wu \). Since \( u \) appears with bounded gaps, the set \( \mathcal{R}_u \) is finite. There exists an integer \( N \) such that all letters of \( A \) appear in \( \sigma^N \). For the second case it suffices to use a one-letter word \( v \) and \( \omega \) respectively, that \( \sigma^N \) and \( \tau^N \) belong to \( \mathcal{R}_u \). Hence \( \sigma^N \) and \( \tau^N \) are periodic sequences, and there exists a shortest word \( u \) such that all words \( \sigma^N \) and \( \tau^N \) appear with bounded gaps in \( x \). We set \( t = x_N x_{N+1} \cdots \) and we will prove that \( t \) is periodic. Consequently \( x \) would be ultimately periodic. We can suppose that \( u \) is a prefix of \( t \). Then \( t \) is a concatenation of return words to \( u \). Let \( w \) be a return word to \( u \). It appears with bounded gaps; hence it appears in some \( \phi(\sigma^N(a)) \), where \( \sigma \) is a primitive and growing sub-substitution, and there exist two words, \( p \) and \( q \), and an integer \( i \) such that \( wu = pn^i q \). As \( |u| \) is the least period of \( L \), it must be that \( wu = u^i \). It follows that \( t = u^\omega \).

If, for example, \( \sigma \) is non-growing, then a result of J.-J. Pansiot [100] asserts that either by modifying \( \sigma \) and \( \phi \) in a suitable way (in that case \( \alpha \) could be replaced by a power of \( \alpha \)) we can suppose \( \sigma \) is growing or \( L(\sigma^\infty(b)) \) contains the language of a periodic infinite word. We have treated the first case before. For the second case it suffices to use Theorem 5.13.

Suppose \( \alpha \) and \( \beta \) are multiplicatively independent real numbers and that \( x \) is a \( \alpha \)-substitutive infinite word w.r.t. \( S_{\text{good}} \) and \( y \) is a \( \beta \)-substitutive infinite word w.r.t. \( S_{\text{good}} \) satisfying \( L(x) \subset L(y) \). Then the conclusion of Theorem 5.8 is far from true. It suffices to look at Example 5.4 and the observation made after Theorem 5.9.

**Remark 5.18.** The Statement \((S,S')\) remains open when \( S \) is the set of substitutions which are not good. Nevertheless there are cases where we can say more. For example, if \( x \) is both \( \alpha \)-substitutive and \( \beta \)-substitutive (with \( \alpha \) and \( \beta \) being multiplicatively independent), and \( L(x) \) contains the language of a periodic sequence, then, from Theorem 5.13, we deduce that \( x \) is ultimately periodic.

Moreover, as we will see in the next section, this statement holds in the purely substitutive context.

### 5.5 The case of fixed points

Now let restrict ourselves to the purely substitutive case. In this setting Cobham’s theorem holds. Note that in the statement of the following result, \( \alpha \) and \( \beta \) are necessarily Perron numbers. Moreover, since the substitutions are growing, then \( \alpha \) and \( \beta \) must be larger than one.

**Theorem 5.19.** Let \( \sigma : A^* \to A^* \) and \( \tau : A^* \to A^* \) be two non-erasing growing substitutions prolongable on \( \alpha \in A \) with respective dominant eigenvalues \( \alpha \) and \( \beta \). Suppose that all letters of \( A \) appear in \( \sigma^\infty(a) \) and in \( \tau^\infty(a) \) and that \( \alpha \) and \( \beta \) are multiplicatively independent. If \( x = \sigma^\infty(a) \) and \( \tau^\infty(a) \), then \( x \) is ultimately periodic.
Proof. Thanks to Remark 5.15, we may assume that $\sigma$ has a primitive sub-substitution. Using Theorem 5.13, the letters appearing infinitely often in $x$ appear with bounded gaps. Let $\sigma : \mathcal{A} \to \mathcal{A}$ be a primitive sub-substitution of $\sigma$. Let $c \in \mathcal{A}$. Suppose that there exists a letter $b$, appearing infinitely many times in $x$, which does not belong to $\mathcal{A}$. Then the word $\sigma^n(c) = \sigma^m(c)$ does not contain $b$ and $b$ could not appear with bounded gaps. Consequently all letters (and, in particular, a letter of maximal growth) appearing infinitely often in $x$ belong to $\mathcal{A}$. Hence $\sigma$ also has $\alpha$ as dominant eigenvalue and $\sigma$ is a “good” substitution. In the same way $\tau$ is a “good” substitution. Theorem 5.17 concludes the proof.

5.6 Back to numeration systems

Let $S$ be an abstract numeration system. There is no reason for the substitutions describing characteristic words of $S$-recognizable sets (see Corollary 5.4) to be primitive. To obtain a Cobham-type theorem for families of abstract numeration systems, one has to interpret Theorem 5.17 in this formalism.

5.6.1 Polynomially-growing abstract numeration systems. Here we only mention the following result. The paper [42] is also of interest. It is well-known that the growth function counting the number of words of length $n$ in a regular language is either polynomial, i.e., in $O(n^k)$ for some integer $k$ or exponential, i.e., in $\Omega(\theta^n)$ for some $\theta > 1$.

Proposition 5.20. [52] Let $S = (L, A, <)$ (resp., $T = (M, B, <)$) be an abstract numeration system where $L$ is a polynomial regular language (resp., $M$ is an exponential regular language). A set $X$ of integers is both $S$-recognizable and $T$-recognizable if and only if $X$ is ultimately periodic.

5.6.2 Bertrand basis and $\omega_\alpha$-substitutive words. Let $U$ be a Bertrand numeration basis such that $\text{rep}_U(\mathbb{N}) = L(\alpha)$ where $\alpha$ is a Parry number which is not an integer. In [58] a substitution denoted by $\omega_\alpha$ is defined. The importance of this substitution is justified by Theorem 5.21. If $d_\alpha(1) = t_1 \cdots t_n 0^\omega$, $t_n \neq 0$, then $\omega_\alpha$ is defined on the alphabet $\{1, \ldots, n\}$ by

$$1 \mapsto 1^{t_1} 2, \ldots, n - 1 \mapsto 1^{t_{n-1}} n, \quad n \mapsto 1^n.$$ 

If $d_\alpha(1) = t_1 \cdots t_n (t_{n+1}, \ldots, t_{n+m})^\omega$, where $n$ and $m$ are minimal and where $t_{n+1} + t_{n+2} + \cdots + t_{n+m} \neq 0$, then $\omega_\alpha$ is defined on the alphabet $\{1, \ldots, n + m\}$ by

$$1 \mapsto 1^{t_1} 2, \ldots, n + m - 1 \mapsto 1^{t_{n+m-1}} (n + m), \quad n + m \mapsto 1^{t_{n+m}} (n + 1).$$

In both cases the substitution $\omega_\alpha$ is primitive and has $\alpha$ as dominant eigenvalue. A substitution that projects (see Definition 5.6) on $\omega_\alpha$ is called a $\omega_\alpha$-substitution, and we call each infinite word which is the image under a coding of a fixed point of a $\omega_\alpha$-substitution a $\omega_\alpha$-substitutive infinite word (ax-automatic infinite word in [58]).

Theorem 5.21. [58, Corollary 1] Let $U$ be a Bertrand numeration basis such that $\text{rep}_U(\mathbb{N}) = L(\alpha)$ where $\alpha$ is a Parry number. A set $X \subset \mathbb{N}$ is $U$-recognizable if and only if its characteristic sequence $\| X$ is $\omega_\alpha$-substitutive.
Remark 5.16 and Theorem 5.17 imply the following result.

**Theorem 5.22.** [46] Let $U$ and $V$ be two Bertrand numeration systems. Let $\alpha$ and $\beta$ be two multiplicatively independent Parry numbers such that $\text{rep}_U(N) = L(\alpha)$ and $\text{rep}_V(N) = L(\beta)$. A set $X \subseteq \mathbb{N}$ is $U$-recognizable and $V$-recognizable if and only if $X$ is ultimately periodic.

## 6 Cobham’s theorem in various contexts

### 6.1 Regular sequences

Regular sequences as presented in [6, 7, 9] are a generalization of automatic sequences to sequences taking infinitely many values. Many examples of such sequences are given in the first two references. Also see [43] for a generalization of the notion of automaticity in the framework of group actions. Let $R$ be a commutative ring. Let $k \geq 2$. Consider a sequence $x = (x_n)_{n \geq 0}$ taking values in some $R$-module. If the $R$-module generated by all sequences in the $k$-kernel $N_k(x)$ is finitely generated (recall Theorem 3.2), then the sequence $x$ is said to be $(R,k)$-regular.

**Theorem 6.1** (Cobham–Bell theorem [10]). Let $R$ be a commutative ring. Let $k, \ell$ be two multiplicatively independent integers. If a sequence $x \in R^\mathbb{N}$ is both $(R,k)$-regular and $(R,\ell)$-regular, then it satisfies a linear recurrence over $R$.

### 6.2 Algebraic setting and quasi-automatic functions

In [34] G. Christol characterized $p$-recognizable sets in terms of formal power series.

**Theorem 6.2.** Let $p$ be a prime number and $\mathbb{F}_p$ be the field with $p$ elements. A subset $A \subset \mathbb{N}$ is $p$-recognizable if and only if $f(X) = \sum_{n \in A} X^n \in \mathbb{F}_p[[X]]$ is algebraic over $\mathbb{F}_p(X)$.

This was applied to Cobham’s theorem in [35] to obtain an algebraic version.

**Theorem 6.3.** Let $A$ be a finite alphabet, $x \in A^\mathbb{N}$, and, $K_1$ and $K_2$ be two finite fields with different characteristics. Let $\alpha_1 : A \to K_1$ and $\alpha_2 : A \to K_2$ be two one-to-one maps. If $f(X) = \sum_{n \in \mathbb{N}} \alpha_1(x_n) X^n \in K_1[[X]]$ is algebraic over $K_1(X)$ and $f(X) = \sum_{n \in \mathbb{N}} \alpha_2(x_n) X^n \in K_2[[X]]$ is algebraic over $K_2(X)$, then $f(X)$ is rational.

Quasi-automatic functions were introduced by Kedlaya in [78]. Also see [79], where Christol’s theorem is generalized to Hahn’s generalized power series. In this algebraic setting, an extension of Cobham’s theorem is proved by Adamczewski and Bell in [1]. Details are given in the chapter “Automata in number theory” of this handbook.

---

3Note that in [6] the ground ring $R$ is assumed to be Noetherian (every ideal in $R$ is finitely generated), but this extra assumption is not needed in the above statement.
6.3 Real numbers and verification of infinite-state systems

Sets of numbers recognized by finite automata arise when analyzing systems with unbounded mixed variables taking integer or real values. Therefore systems such as timed or hybrid automata are considered [17]. One needs to develop data structures representing sets manipulated during the exploration of infinite state systems. For instance, it is often needed to compute the set of reachable configurations of such a system. Let \( k \geq 2 \) be an integer. Considering separately integer and fractional parts, a real number \( x > 0 \) can be decomposed as

\[
x = \sum_{i=0}^{d} c_i k^i + \sum_{i=1}^{\infty} c_{-i} k^{-i}, \quad c_i \in [0, k-1], \quad i \leq d,
\]

and gives rise to the infinite word \( c_d \cdots c_0 \star c_{-1}c_{-2} \cdots \) over \([0, k-1] \cup \{\star\}\), which is a \( k \)-ary representation of \( x \). Note that rational numbers of the form \( p/k^n \) have two \( k \)-ary representations, one ending with \( 0^\omega \) and one with \( (k-1)^\omega \). For the representation of negative elements, one can consider base \( k \)-complements or signed number representations [81], the sign being determined by the most significant digit which is thus \( 0 \) or \( k-1 \) (and this digit may be repeated an arbitrary number of times). For definition of Büchi and Muller automata, see the first part of this handbook.

**Definition 6.1.** A set \( X \subseteq \mathbb{R} \) is \( k \)-recognizable if there exists a Büchi automaton accepting all the \( k \)-ary representations of the elements in \( X \). Such an automaton is called a Real Number Automaton or RNA.

These notions extend naturally to subsets of \( \mathbb{R}^d \) and to Real Vector Automata or RVA. Also the Büchi theorem 4.5 holds for a suitable structure \( \langle \mathbb{R}, \mathbb{Z}, +, < \rangle \); see [22].

**Theorem 6.4.** [21] If \( X \subseteq \mathbb{R}^d \) is definable by a first-order formula in \( \langle \mathbb{R}, \mathbb{Z}, +, < \rangle \), then \( X \) written in base \( k \geq 2 \) is accepted by a weak deterministic RVA \( \mathcal{A} \).

Weakness means that each strongly connected component of \( \mathcal{A} \) contains only accepting states or only non-accepting states.

**Theorem 6.5.** [18] Let \( k, \ell \geq 2 \) be two multiplicatively independent integers. If \( X \subseteq \mathbb{R} \) is both \( k \)- and \( \ell \)-recognizable by two weak deterministic RVA, then it is definable in \( \langle \mathbb{R}, \mathbb{Z}, +, < \rangle \).

The extension of the Cobham–Semenov theorem for subsets of \( \mathbb{R}^d \) in this setting is discussed in [20]; also see [24] for a comprehensive presentation. The case of two coprime bases was first considered in [18]. Surprisingly, if the multiplicatively independent bases \( k, \ell \geq 2 \) share the same prime factors, then there exists a subset of \( \mathbb{R} \) that is both \( k \)- and \( \ell \)-recognizable, but not definable in \( \langle \mathbb{R}, \mathbb{Z}, +, < \rangle \); see [19]. This shows the main difference between recognizability of subsets of real numbers written in base \( k \) for (general) Büchi automata and weak deterministic RVA. Though written in a completely different language, a similar result was independently obtained in [2]. This latter paper is motivated by the study of some fractal sets. For extension to non-integer bases and graph directed iterated systems; see [32].
6.4 Dynamical systems and subshifts

In this section we would like to express a Cobham-type theorem in terms of dynamical systems called substitutive subshifts. Theorem 5.9 will appear as a direct corollary.

We first need some definitions.

A dynamical system is a pair $(X, S)$ where $X$ is a compact metric space and $S$ a continuous map from $X$ onto itself. The dynamical system $(X, S)$ is minimal whenever $X$ and the empty set are the only $S$-invariant closed subsets of $X$, that is, $S(X) = X$. We say that a minimal system $(X, S)$ is periodic whenever $X$ is finite.

Let $(X, S)$ and $(Y, T)$ be two dynamical systems. We say that $(Y, T)$ is a factor of $(X, S)$, or that $(X, S)$ factorizes to $(Y, T)$, if there is a continuous and onto map $\phi : X \to Y$ such that $\phi \circ S = T \circ \phi$ (\phi \text{ is called a factor map}). If $\phi$ is one-to-one we say that $\phi$ is an isomorphism and that $(X, S)$ and $(Y, T)$ are isomorphic.

Let $A$ be an alphabet. We endow $A^\omega$ with the infinite product of the discrete topologies. It is a metric space where the metric is given by

$$d(x, y) = \frac{1}{2^n} \text{ with } n = \inf\{k \mid x_k \neq y_k\},$$

(6.2)

where $x = (x_n)_{n \geq 0}$ and $y = (y_n)_{n \geq 0}$ are two elements of $A^\omega$. A subshift on $A$ is a pair $(X, T|_X)$ where $X$ is a closed $T$-invariant subset of $A^\omega$ and $T$ is the shift transformation $T : A^\omega \to A^\omega$, $(x_n)_{n \geq 0} \mapsto (x_{n+1})_{n \geq 0}$.

Let $u$ be a word over $A$. The set $[u]_X = \{x \in X \mid x_0 \cdots x_{|u|-1} = u\}$ is a cylinder. The family of these sets is a base of the induced topology on $X$. When there is no misunderstanding, we write $[u]$ and $T$ instead of $[u]_X$ and $T|_X$.

Let $x \in A^\omega$. The set $\{y \in A^\omega \mid L(y) \subseteq L(x)\}$ is denoted $\Omega(x)$. It is clear that $(\Omega(x), T)$ is also a subshift. We say that $(\Omega(x), T)$ is the subshift generated by $x$. When $x$ is a sequence, we have $\Omega(x) = \{T^nx \mid n \in \mathbb{N}\}$. Observe that $(\Omega(x), T)$ is minimal if and only if $x$ is uniformly recurrent, i.e., all its factors occur infinitely often in $x$ and for each factor $u$ of $x$, there exists a constant $K$ such that the distance between two consecutive occurrences of $u$ in $x$ is bounded by $K$.

Let $\phi$ be a factor map from the subshift $(X, T)$ on the alphabet $A$ onto the subshift $(Y, T)$ on the alphabet $B$. Here $x[i, j]$ denotes the word $x_i \cdots x_j$, $i \leq j$. The Curtis–Hedlund–Lyndon theorem [88, Thm. 6.2.9] asserts that $\phi$ is a sliding block code; there exists an r-block map $f : A^r \to B$ such that $(\phi(x))_i = f(x[i, i+r-1])$ for all $i \in \mathbb{N}$ and $x \in X$. We shall say that $f$ is a block map associated to $\phi$ and that $f$ defines $\phi$. If $u = u_0u_1 \cdots u_{n-1}$ is a word of length $n \geq r$, then we define $f(u)$ by $f(u)_i = f(u[i, i+r-1])$, $i \in \{0, 1, \cdots, n-r+1\}$. Let $C$ denote the alphabet $A'$ and $Z = \{(x[i, i+r-1])_{|u|} \mid (x_n)_{n \geq 0} \in X\}$. It is easy to check that the subshift $(Z, T)$ is isomorphic to $(X, T)$ and that $f$ induces a $1$-block map (a coding) from $C$ onto $B$ which defines a factor map from $(Z, T)$ onto $(Y, T)$.

We can now state a Cobham-type theorem for subshifts generated by substitutive sequences. Observe that it implies Theorem 5.9 and Statement (S, $S'$) when $S = S'$ is the set of primitive substitutions.

**Theorem 6.6.** Let $(X, T)$ and $(Y, T)$ be two subshifts generated, respectively, by a primitive $\alpha$-substitutive sequence $x$ and by a primitive $\beta$-substitutive sequence $y$. Suppose $(X, T)$ and $(Y, T)$ both factorize to the subshift $(Z, T)$. If $\alpha$ and $\beta$ are multiplicatively
independent, then $(Z, T)$ is periodic.

Below we give a sketch of the proof, which involves the concept of an ergodic measure. An invariant measure for the dynamical system $(X, S)$ is a probability measure $\mu$, on the $\sigma$-algebra $B(X)$ of Borel sets, with $\mu(S^{-1}B) = \mu(B)$ for all $B \in B(X)$; the measure is ergodic if every $S$-invariant Borel set has measure 0 or 1. The set of invariant measures for $(X, S)$ is denoted by $\mathcal{M}(X, S)$. The system $(X, S)$ is uniquely ergodic if $\#(\mathcal{M}(X, S)) = 1$. For expository books on subshifts and/or ergodic theory, see [39, 80, 88, 110, 84].

It is well known that the subshifts generated by primitive substitutive sequences are uniquely ergodic [110].

Let $\phi : X \to Z$ and $\psi : Y \to Z$ be two factor maps. Suppose that $(Z, T)$ is not periodic. We will prove that $\alpha$ and $\beta$ are multiplicatively independent.

Let $\mu$ and $\lambda$ be the unique ergodic measures of $(X, T)$ and $(Y, T)$ respectively. It is not difficult to see that $(Z, T)$ is also generated by a primitive substitutive sequence and consequently is uniquely ergodic. Let $\delta$ be its unique ergodic measure. Let us give more details about both measures in order to conclude the proof.

**Theorem 6.7.** Let $(\Omega, T)$ be a subshift generated by a primitive purely $\gamma$-substitutive sequence and $m$ be its unique ergodic measure. Then, the measures of cylinders in $\Omega$ lie in a finite union of geometric progressions. There exists a finite set $F$ of positive real numbers such that

$$\{m(C) \mid C \text{ cylinder of } X\} \subset \bigcup_{n \in \mathbb{N}} \gamma^{-n} F.$$

In conjunction with the next result and using the pigeonhole principle we will conclude the proof.

**Proposition 6.8.** Let $(\Omega, T)$ be a subshift generated by a primitive substitutive sequence on the alphabet $A$. There exists a constant $K$ such that for any block map $f : A^{2r+1} \to B$, we have $\#(f^{-1}(\{u\})) \leq K$ for all $u$ appearing in some sequence of $f(\Omega)$.

From these last two results we deduce that there exist two sets of numbers $F_X$ and $F_Y$ such that

$$\{\delta(C) \mid C \text{ cylinder of } Z\} = \{\mu(\phi^{-1}(C)) \mid C \text{ cylinder of } X\}$$
$$= \{\lambda(\psi^{-1}(C)) \mid C \text{ cylinder of } X\} 
$$
$$\subset \left(\bigcup_{n \in \mathbb{N}} \alpha^{-n} F_X\right) \cap \left(\bigcup_{n \in \mathbb{N}} \beta^{-n} F_Y\right).$$

The sets $F_X$ and $F_Y$ being finite, there exist two cylinder sets $U$ and $V$ of $Z$, $a \in F_X$, $b \in F_Y$ and $n, m, r, s$ four distinct positive integers, such that

$$a\alpha^{-n} = \delta(U) = b\beta^{-m} \quad \text{and} \quad a\alpha^{-r} = \delta(V) = b\beta^{-s}.$$
Consequently $\alpha$ and $\beta$ are multiplicatively dependent.

6.5 Tilings

6.5.1 From definable sets Let $A$ be a finite alphabet. An array in $\mathbb{N}^d$ is a map $T : \mathbb{N}^d \to A$. It can be viewed as a tiling of $\mathbb{R}^d_+$. The collection of all these arrays is $A^\mathbb{N}^d$. For all $x \in \mathbb{N}^d$, let $|x|$ denote the sum of the coordinates of $x$ and $B(x, r)$ be the set $\{(y_1, \ldots, y_d) \in \mathbb{N}^d \mid 0 \leq y_i - x_i < r, 1 \leq i \leq d\}$.

We say $T$ is periodic (resp., ultimately periodic) if there exists $p \in \mathbb{N}^d$ such that $T(x + p) = T(x)$ for all $x \in \mathbb{N}^d$ (resp., for all large enough $x$). We also need another notion of periodicity. We say that $Z \subset \mathbb{N}^d$ is $p$-periodic inside $X \subset \mathbb{N}^d$ if for any $x \in X$ with $x + p \in X$ we have

$$x \in Z \text{ if and only if } x + p \in Z.$$ We say that $Z$ is locally periodic if there exists a non-empty finite set $V \subset \mathbb{N}^d$ of non-zero vectors such that for some $K > \max\{|v| \mid v \in V\}$ and $L \geq 0$ one has

$$(\forall x \in \mathbb{N}^d, |x| \geq L)(\exists v \in V)(Z \text{ is } v\text{-periodic inside } B(x, K)).$$

Observe that for $d = 1$, local periodicity is equivalent to ultimate periodicity. We say $T$ is pseudo-periodic if for all $a \in A$, $T^{-1}(a)$ is locally periodic and every $(d - 1)$-section of $T^{-1}(a)$, say $S(i, n) = \{x \in T^{-1}(a) \mid x_i = n\}$, $1 \leq i \leq d$ and $n \in \mathbb{N}$, is pseudo-periodic (ultimately periodic when $d - 1 = 1$). The following criterion is due to Muchnik; see [97] for the proof.

**Proposition 6.9.** Let $E \subset \mathbb{N}^d$ and $T : \mathbb{N}^d \to \{0, 1\}$ be its characteristic function. The following are equivalent:

(i) $E$ is definable in Presburger arithmetic;

(ii) $T$ is pseudo-periodic;

(iii) for all $a \in \{0, 1\}$, there exist $n \in \mathbb{N}$, $v_i \in \mathbb{N}^d$ and finite sets $V_i \subset \mathbb{N}^d$, $0 \leq i \leq n$ such that

$$T^{-1}(a) = V_0 \cup \bigcup_{1 \leq i \leq n} \left( v_i + \sum_{v \in V_i} \mathbb{N}v \right).$$

Let $p$ be a positive integer and $A$ be a finite alphabet. A $p$-substitution (or substitution if we do not need to specify $p$) is a map $S : A \to A^{d^p}$ where $B_p = B(0, p) = \Pi_{i=1}^d \{0, \ldots, p - 1\}$. The substitution $S$ can be considered as a function from $A^\mathbb{N}^d$ into itself by setting

$$S((T(x)) = [S(T(y))](z), \text{ for all } T \in A^\mathbb{N}^d$$

where $y \in \mathbb{N}^d$ and $z \in B_p$ are the unique vectors satisfying $x = py + z$.

In the same way, we can define $S : A^{B_p^n} \to A^{B_p^{n+1}}$. We remark that $S^n(a) = S(S^{n-1}(a))$ for all $a \in A$ and $n > 0$. We say $T$ is generated by a $p$-substitution if there exist a coding $\phi$ and a fixed point $T_0$ of a $p$-substitution such that $T = \phi \circ T_0$.

In [31] the authors proved the following theorem, which is analogous to Theorem 3.1.
**Theorem 6.10.** Let \( p \geq 2 \) and \( d \geq 1 \). A set \( E \subset \mathbb{N}^d \) is \( p \)-recognizable if and only if the characteristic function of \( E \) is generated by a \( p \)-substitution.

Hence we can reformulate the Cobham–Semenov theorem as follows [121].

**Theorem 6.11** (Cobham–Semenov theorem, Version 2). Let \( p \) and \( q \) be two multiplicatively independent integers greater or equal to 2. Then the array \( T \) is generated by both a \( p \)-substitution and a \( q \)-substitution if and only if \( T \) is pseudo-periodic.

A dynamical proof of this can be given as for the unidimensional case; see [49] for the primitive case.

### 6.5.2 Self-similar tilings

In [40], a Cobham-like theorem is expressed in terms of self-similar tilings of \( \mathbb{R}^d \) with a proof using ergodic measures; see [124] for more about self-similar tilings. From the point of view of dynamical systems, the main result in [99] is also a Cobham-like theorem for self-similar tilings.

### 6.6 Toward Cobham’s theorem for the Gaussian integers

I. Kátai and J. Szabó proved [77] that the sequences \( ((-p + i)^n)_{n \geq 0} \) and \( ((-p - i)^n)_{n \geq 0} \) give rise to numeration systems whose set of digits is \( \{0, 1, \ldots, p^2\} \), \( p \in \mathbb{N} \setminus \{0\} \). It is an exercise to check that when \( p \in \mathbb{N} \setminus \{0\} \) and \( q \in \mathbb{N} \setminus \{0\} \) are different then \(-p + i\) and \(-q + i\) are multiplicatively independent. Therefore one could expect a Cobham-type theorem for the set of Gaussian integers \( \mathbb{G} = \{a + ib \mid a, b \in \mathbb{Z}\} \). A subset \( S \subset \mathbb{G} \) is periodic if there exists \( h \in \mathbb{G} \) such that, for all \( g \in \mathbb{G} \), \( s \in S \) if and only if \( s + gh \in S \).

G. Hansel and T. Safer conjectured the following [69]:

**Conjecture 6.12.** Let \( p \) and \( q \) be two different positive integers and \( S \in \mathbb{G} \). Then the following are equivalent.

(i) The set \( S \) is \((-p + i)\)-recognizable and \((-q + i)\)-recognizable;

(ii) There exists a periodic set \( P \) such that the symmetric difference set \( S \Delta P \) is finite.

The proof that (ii) implies (i) is easy. They tried to prove the other implication using the following (classical) steps:

1. \( D_{p,q} = \left\{ \frac{(-p + i)^n}{(-q + i)^m} \mid n, m \in \mathbb{Z} \right\} \) is dense in \( \mathbb{C} \).
2. \( S \) is syndetic.
3. \( S \) is periodic up to some finite set.

They succeeded in proving (ii) as given by the next result.

**Theorem 6.13.** Let \( p \) and \( q \) be two positive integers such that the set \( D_{p,q} \) is dense in \( \mathbb{C} \). Let \( S \subset \mathbb{G} \) be \((-p + i)\)-recognizable and \((-q + i)\)-recognizable. Then, \( S \) is syndetic.

Let us make some observations about the density of the set \( D_{p,q} \). Let \(-p + i = a e^{i \theta}\) and \(-q + i = b e^{i \theta}\).
Proposition 6.14. The following are equivalent.

(i) The set $D_{p,q}$ is dense in $\mathbb{C}$;
(ii) The set $D_{p,q}$ is dense on the circle: $\{e^{i\theta} \mid \theta \in \mathbb{R}\} \subset D_{p,q}$;
(iii) The following numbers are rationally independent (or linearly dependent over $\mathbb{Q}$):
\[
\frac{\ln b}{\ln a}, \frac{\theta \ln b}{2\pi \ln a}, \frac{\phi}{2\pi}, 1.
\]

The equivalence between (i) and (iii) is proven in [69] from an easy computation. The equivalence between (i) and (ii) comes from the fact that $p^2 + 1$ and $q^2 + 1$ are multiplicatively independent; see [69, Prop. 2]. As an example, take $p = 1$ and $q = 2$. Then, $a = \sqrt{2}, b = \sqrt{5}, \theta = \frac{3\pi}{4}$ and $\phi = \arctan(-\frac{1}{2})$. Proving the density of $D_{1,2}$ is equivalent to proving that $\ln 5/\ln 2$, $\arctan(1/2)/\pi$ and $1$ are rationally independent. In [69] the authors observe that the four exponentials conjecture (see [128]) would imply that $D_{p,q}$ is dense in $\mathbb{C}$.

Conjecture 6.15 ("four exponentials conjecture"). Let $\{\lambda_1, \lambda_2\}$ and $\{x_1, x_2\}$ be two pairs of rationally independent complex numbers. Then, one of the numbers $e^{\lambda_1 x_1}$, $e^{\lambda_1 x_2}$, $e^{\lambda_2 x_1}$, $e^{\lambda_2 x_2}$ is transcendental.

6.7 Recognizability over $\mathbb{F}_q[X]$

Using the analogy existing between $\mathbb{Z}$ and the ring of polynomials over a finite field $\mathbb{F}_q$ of positive characteristic, one can easily define $B$-recognizable sets of polynomials [113]. In [129, 106] characterization of these sets in a convenient logical structure analogous to Theorem 4.5 is given. A family of sets of polynomials recognizable in all polynomial bases is described in [113, 129]. Again, we can conjecture a Cobham-like theorem.

7 Decidability issues

So far we have seen that ultimately periodic sets have a very special status in the context of numeration systems (recall Proposition 2.6, Theorem 5.1 or Theorems 5.17 and 5.19). They can be described using a finite amount of data (two finite words for the preperiodic and the periodic parts). Let us settle down once more to the usual integer base numeration system. Let $X \subseteq \mathbb{N}$ be a $k$-recognizable set of integers given by a DFA accepting $\operatorname{rep}_k(X)$. Is there an algorithmic decision procedure which permits one to decide for any such set $X$, whether or not $X$ is ultimately periodic? For an integer base, the problem was solved positively in [74]. The main ideas are the following ones. Given a DFA $A$ accepting a $k$-recognizable set $X \subseteq \mathbb{N}$, the number of states of $A$ gives an upper bound on the possible index and period for $X$. Consequently, there are finitely many candidates to check. For each such pair $(i, p)$ of candidates, produce a DFA for all possible corresponding ultimately periodic sets and compare it with $A$. Using non-deterministic finite automata, the same problem was solved in [5]. With the formalism of first-order logic the problem becomes trivial. If a set $X \subseteq \mathbb{N}$ is $k$-recognizable, then using Theorem 4.5
it is definable by a formula $\varphi(x)$ in $\langle \mathbb{N}, +, V_k \rangle$ and $X$ is ultimately periodic if and only if $(\exists p)(\exists N)(\forall x)(x \geq N \land (\varphi(x) \leftrightarrow \varphi(x + p)))$. Since we have a decidable theory, it is decidable whether this latter sentence is true [29, Prop. 8.2]. The problem can be extended to $\mathbb{Z}^d$ and was discussed in [97]. It is solved in polynomial time in [87]. In view of Theorem 5.1 the question is extended to any abstract numeration system. Let $S$ be an abstract numeration system. Given a DFA accepting an $S$-recognizable set $X \subseteq \mathbb{N}$, decide whether or not $X$ is ultimately periodic. Some special cases have been solved positively in [33, 11]. Using Corollary 5.3, the same question can be asked in terms of morphisms. Given a morphism $\sigma : A^* \to A^*$ prolongable on a letter $a$ and a coding $\tau : A \to B$, decide whether or not $\tau(\sigma^\infty(a))$ is ultimately periodic. The is the HDOL (ultimate) periodicity problem. The purely substitutive case was solved independently in [101] and [71]. The general substitutive case is solved positively in [51] and [95]. Also see [91, 92] where decidability questions about almost-periodicity are considered. A word is almost periodic if factors occurring infinitely often have a bounded distance between occurrences (but some factors may occur only finitely often).

8 Acknowledgments

We would like to warmly thank Valérie Berthé, Alexis Bès, Véronique Bruyère, Christiane Frougny, Julien Leroy, Narad Rampersad, and Jeffrey Shallit for their useful comments after reading a preliminary version of this work.

References


On Cobham’s theorem


On Cobham’s theorem


[103] B. Pascal. *Œuvres complètes*. Seuil, 1963. The treatise *De numeris multiplicantibus*, written with the other arithmetical treatises before 1654, was published by Guillaume Desprez in 1665. 899


On Cobham’s theorem


