



**HAL**  
open science

## The carry propagation of the successor function

Valerie Berthe, Christiane Frougny, Michel Rigo, Jacques Sakarovitch

► **To cite this version:**

Valerie Berthe, Christiane Frougny, Michel Rigo, Jacques Sakarovitch. The carry propagation of the successor function. *Advances in Applied Mathematics*, 2020, 120, pp.102062. 10.1016/j.aam.2020.102062 . hal-03379583

**HAL Id: hal-03379583**

**<https://hal.science/hal-03379583>**

Submitted on 27 Oct 2021

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# The carry propagation of the successor function

Valérie Berthé \*    Christiane Frougny \*    Michel Rigo †  
Jacques Sakarovitch ‡§

April 30, 2020

## Abstract

Given any numeration system, we call *carry propagation* at a number  $N$  the number of digits that are changed when going from the representation of  $N$  to the one of  $N + 1$ , and *amortized carry propagation* the limit of the mean of the carry propagations at the first  $N$  integers, when  $N$  tends to infinity, if this limit exists.

In the case of the usual base  $p$  numeration system, it can be shown that the limit indeed exists and is equal to  $p/(p - 1)$ . We recover a similar value for those numeration systems we consider and for which the limit exists.

We address the problem of the existence of the amortized carry propagation in non-standard numeration systems of various kinds: abstract numeration systems, rational base numeration systems, greedy numeration systems and beta-numeration. We tackle the problem with three different types of techniques: combinatorial, algebraic, and ergodic. For each kind of numeration systems that we consider, the relevant method allows for establishing sufficient conditions for the existence of the carry propagation and examples show that these conditions are close to being necessary conditions.

## 1 Introduction

The *carry propagation* is a nightmare for schoolchildren and a headache for computer engineers: not only could the addition of two digits produce a carry, but this carry itself, when added to the next digit on the left<sup>1</sup> could give rise to another carry, and so on, and this may happen arbitrarily many times. Since the beginnings of computer science, the evaluation of the carry propagation length has been the subject of many works and it is known that the average carry propagation length for the addition of two uniformly distributed  $n$ -digit binary numbers is:  $\log_2(n) + O(1)$  (see [13, 20, 28]).

---

\*IRIF, CNRS/Université de Paris

†Université de Liège, Département de Mathématiques

‡IRIF, CNRS/Université de Paris and LTCI, Telecom, Institut Polytechnique de Paris

§Corresponding author

<sup>1</sup>We write numbers under MSDF (Most Significant Digit First) convention.

Many published works address the design of numeration systems in which the carry does not indeed propagate — through the use of supplementary digits — which allow the design of circuits where addition is performed ‘in parallel’ for numbers of large, but fixed, length [2, 14].

We consider here the problem of carry propagation from a more theoretical perspective and in an seemingly elementary case. We investigate the amortized carry propagation of the *successor function* in various numeration systems. The central case of integer base numeration system is a clear example of the issue. Let us take an integer  $p$  greater than 1 as a base. In the representations of the succession of the integers — which is exactly what the successor function achieves — the least digit changes at every step, the penultimate digit changes every  $p$  steps, the ante-penultimate digit changes every  $p^2$  steps, and so on. Consequently, the average carry propagation of the successor function, computed over the first  $N$  integers, should tend to the quantity:

$$1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \dots = \frac{p}{p-1} \quad , \quad (1)$$

when  $N$  tends to infinity. It can be shown that it is indeed the case. Following on our previous works on various non-standard numeration systems, we investigate here the questions of evaluating and computing the amortized carry propagation in those systems. We thus consider several such numeration systems which are different from the classical integer base numeration systems: the greedy numeration systems and the  $\beta$ -numeration systems (see [17]) which are a specific case of the former, the rational base numeration systems (introduced in [1]) which are not greedy numeration systems, and the abstract numeration systems (defined in [22]) which are a generalization of the classical *positional numeration systems*.

In [7], we already reported that the approach of *abstract numeration systems* of [21], namely the study of a numeration system via the properties of the set of expansions of the natural integers is appropriate for this problem. Such systems consist of a totally ordered alphabet  $A$  — hence, without loss of generality, an initial section  $\{0, 1, \dots, p-1\}$  of the non-negative integers  $\mathbb{N}$  — and a language  $L$  of  $A^*$ , ordered by the *radix order* deduced from the ordering on  $A$ . The representation of an integer  $n$  is then the  $(n+1)$ -th word<sup>2</sup> of  $L$  in the radix order. This definition is consistent with every classical standard and non-standard numeration system, that is, the representation of  $n$  in such a system is the  $(n+1)$ -th word (in the radix order) of the set of representations of all integers in the system.

Given a numeration system defined by a language  $L$  ordered by radix order, we denote by  $\text{cp}_L(i)$  the carry propagation in the computation from the representation of  $i$  in  $L$  to that of  $i+1$ . The (*amortized*) *carry propagation* of  $L$ , which we denote by  $\text{CP}_L$ , is the limit, *if it exists*, of the mean of the carry propagation

---

<sup>2</sup>The ‘+1’ gives room for the representation of 0 by the first word of  $L$ .

at the first  $N$  words of  $L$ :

$$\text{CP}_L = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{i=0}^{N-1} \text{cp}_L(i) . \quad (2)$$

This quantity, introduced by Barucci, Pinzani and Poneti in [5], is the main object of study of the present paper whose aim is to investigate cases where the carry propagation exists or not, and suggests ways to compute it.

A common further hypothesis is to consider *prefix-closed* and *right-extendable* languages, called ‘PCE’ languages in the sequel: every left-factor of a word of  $L$  is a word of  $L$  and every word of  $L$  is a left-factor of a longer word of  $L$ . Hence,  $L$  is the branch language of an infinite labeled tree  $\mathcal{T}_L$  and, once again, every classical standard and non-standard numeration system meets that hypothesis.

We move on to prove two simple properties of the carry propagation of PCE languages. First,  $\text{CP}_L$  does not depend upon the labeling of  $\mathcal{T}_L$ , but only on its ‘shape’ which is completely defined by the infinite sequence of the degrees of the nodes visited in a breadth-first traversal of  $\mathcal{T}_L$ , and which we call the *signature* of  $\mathcal{T}_L$  (or of  $L$ ) [25]. For instance, the signature of the language of the representations of the integers in base  $p$  is the constant sequence  $p^\omega$ . Next, let us denote by  $\mathbf{u}_L(\ell)$  the number of words of  $L$  of length  $\ell$ . We call the limit, *if it exists*, of the ratio  $\mathbf{u}_L(\ell + 1)/\mathbf{u}_L(\ell)$  the *local growth rate* of a language  $L$ , and we denote it by  $\gamma_L$ . And we show (Corollary 3.16) that *if  $\text{CP}_L$  exists, then  $\gamma_L$  exists* and

$$\text{CP}_L = \frac{\gamma_L}{\gamma_L - 1} \quad (3)$$

holds, which is an obvious generalization of (1). On the other hand, an example shows that  $\gamma_L$  may exist while  $\text{CP}_L$  does not (Example 3.17).

By virtue of (3), the *computation* of  $\text{CP}_L$  is usually not an issue. The problem lies in proving its *existence*. We develop *three different methods* for the proofs of existence, whose domains of application are pairwise incomparable, that is to say, we have examples of numeration systems for which the existence of  $\text{CP}_L$  is established by one method and not by the other two. These methods: *combinatorial*, *algebraic*, and *ergodic*, are built upon very different mathematical backgrounds.

We first show by a combinatorial method that languages with an *eventually periodic signature* have a carry propagation (Theorem 3.23). It is known that these languages are essentially the rational base numeration systems, possibly with non-canonical alphabets of digits [25].

We next consider the *rational abstract numeration systems*, that is, those systems which are defined by languages accepted by *finite automata*.<sup>3</sup> Examples of such systems are the Fibonacci numeration system and, more generally,  $\beta$ -numeration systems where  $\beta$  is a *Parry number* [17], and of course many other

---

<sup>3</sup>In this context where we deal with both languages and formal power series, we say *rational* rather than *regular* for languages accepted by finite automata.

systems which greatly differ from  $\beta$ -numeration. Theorem 4.1 states that *if a rational PCE language  $L$  has a local growth rate, and if all its quotients also have a local growth rate, then  $L$  therefore has a carry propagation*. The proof is based on a property of rational power series with positive coefficients which is reminiscent of the Perron-Frobenius Theorem. A tighter sufficient condition may even be established (Theorem 4.10) but a remarkable fact is that the existence of the local growth rate *is not* a sufficient condition for the existence of carry propagation *even for rational* PCE languages (Example 4.11).

The definition of carry propagation by Equation (2) inevitably brings to mind the Ergodic Theorem. Finally, we consider the so-called *greedy numeration systems* [15] —  $\beta$ -numeration systems, with any  $\beta > 1$ , are one example but they can be much more general. The language of greedy expansions in such a system is embedded into a compact set, and the successor function is extended as an action, called the odometer, on that compactification. In this setting, the odometer is just the addition of 1. This gives a dynamical system, introduced in [19, 4]. Tools from ergodic theory developed only recently (in [3]) allow us to prove the existence of the carry propagation for greedy systems with exponential growth (Theorem 5.17), and thus for  $\beta$ -numeration in general. The difficulty is that the odometer is not continuous in general and the Ergodic Theorem does not directly apply.

The substantial length of the paper is due to the fact that it borrows results from different chapters of mathematics (in relation with formal language theory) which we had to present as we wished the paper to be as self-contained as possible. It is organized as follows.

In Section 2, after reviewing some definitions on words, we present the notion of *abstract numeration systems*. Section 3 is devoted to the combinatorial point of view. Here we more precisely define the notion of carry propagation, present its relationship with the local growth rate, and give, as mentioned above, a first example of a language with local growth rate which does not have a carry propagation. We then define the signature of a language and establish the aforementioned quoted result for languages with eventually periodic signature. Note that neither the algebraic nor the ergodic methods apply to these languages (except of course for the integer-base numeration systems).

In Section 4, we study the carry propagation of *rational* abstract numeration systems by means of algebraic methods. We first recall the definitions of *generating function*, of *modulus* of a language, of *languages with dominating eigenvalue* (DEV languages), and give the description, due to Berstel, of the ‘leading terms’ of generating functions of rational languages. We are then able to introduce the notion of *languages with almost dominating eigenvalues* (ADEV languages) and to show that it is a necessary and sufficient condition for a rational language to have a local growth rate (Theorem 4.9). As already said, it is not a sufficient

condition for the existence of the carry propagation. But the counter-example directly leads to a sufficient condition for a rational language to have a carry propagation (Theorem 4.10).

Section 5 is devoted to the study of the question of the carry propagation of a language by means of tools from ergodic theory. Even though it seems to be quite a natural approach, it requires some elaborate new results and is, so far, applicable to the family of greedy numeration systems only. We first recall Birkhoff's Ergodic Theorem and follow [19] for the description of a framework in which we can turn a numeration system and its successor function into a dynamical system. We then focus on greedy numeration systems that have been studied by Barat and Grabner [3]. The carry propagation in these systems is not the uniform limit of its truncated approximations but the properties of greedy numeration systems allow us to establish that it is regular enough to be in the scope of the Ergodic Theorem. We end with some examples of  $\beta$ -numeration systems which are at the crossroads of algebraic and ergodic methods, thus allowing two different ways for the computation of the carry propagation.

It should be noted that the inspiration for this current work was initiated by a paper where the *amortized algorithmic complexity* of the successor function for some  $\beta$ -numeration systems was studied [5]. Whatever the chosen computation model, the (amortized) algorithmic complexity, that is, the limit of the mean of the *number of operations* necessary to compute the successor of the first  $N$  integers, is greater than the (amortized) carry propagation, hence can be seen as the sum of two quantities: the carry propagation itself and an *overload*. The study of carry propagation leads to quite unexpected and winding developments that form a subject on its own and that we present here. But this paper is only the first step in solving the original problem which consists in describing the *complexity* of the successor function.

Addressing complexity implies the definition of a computational model and ours is based on the use of sequential transducers. This explains the particular attention we pay in this paper to *rational* abstract numeration systems. The sequel of this work [8] is in the preparation phase and will hopefully be completed in a not too distant future.

## Acknowledgments

We are grateful to Christophe Reutenauer for helpful discussions on the proof of Theorem 4.1, and for pointing us to results from his treatise on rational series [6]. We would like to thank Peter Grabner who drew our attention to the ergodic nature of the notion of carry propagation and advised us on using the results of his recent work [3]. We are also grateful to our colleagues David Madore and Hugues Randriam for the numerous helpful and fruitful discussions we had with

them during the long development process of this paper. We finally thank the referee for his precise reading and his many corrections in order to improve the paper quality.

We are also pleased to acknowledge support from the French Agence Nationale de la Recherche through the ANR projects **DynA3S** (ANR-13-BS02-0003) and **CODYS** (ANR-18-CE40-0007).

## 2 Preliminary notions

We review more or less classical basic notions on languages that we will use throughout this work. More specific notions and notation will be introduced at the point they are needed, even when classical.

### 2.1 Words on ordered alphabets

In this paper,  $A$  denotes a *totally ordered* finite alphabet, and the order is denoted by  $<$ . Without loss of generality, we can always assume that  $A$  consists of consecutive integers starting with 0 and naturally ordered:  $A = \{0, 1, \dots, r-1\}$ . The set of all words over  $A$  is denoted by  $A^*$ . The empty word is denoted by  $\varepsilon$ . The length of a word  $w$  of  $A^*$  is denoted by  $|w|$ . The set of words of length less than or equal to  $n$  is denoted by  $A^{\leq n}$ .

If  $w = uv$ ,  $u$  is a *prefix* (or a *left-factor*) of  $w$ , *strict prefix* if  $v$  is non-empty, and  $v$  is a *suffix* (or a *right-factor*) of  $w$ , *strict suffix* if  $u$  is non-empty. The set of prefixes of  $w$  is denoted by  $\text{Pre}(w)$ .

The *lexicographic order*, denoted by  $\preceq$ , extends the order on  $A$  onto  $A^*$  and is defined as follows. Let  $v$  and  $w$  be two words in  $A^*$  and  $u$  their longest common prefix. Then,  $v \preceq w$  if  $v = w$  or, if  $v = uas$ ,  $w = ubt$  with  $a$  and  $b$  in  $A$ , and  $a < b$ . The *radix order* (also called the *genealogical order* or the *short-lex order*), denoted by  $\sqsubseteq$ , is defined as follows:  $v \sqsubseteq w$  if  $|v| < |w|$  or  $|v| = |w|$  and  $v \preceq w$  (that is, for two words of same length, the radix order coincides with the lexicographic order). In contrast with lexicographic order, radix order is a *well-order*, that is, every non-empty subset has a minimal element. For instance, the set  $a^+b = \{a^n b \mid n > 0\}$  has no minimal element for the lexicographic order.

### 2.2 Languages and Abstract Numeration Systems

In all what follows,  $L$  denotes a *language over  $A$* , that is, any subset of  $A^*$ . A language  $L$  is said to be *prefix-closed* if every prefix of a word of  $L$  is in  $L$ . A language  $L$  is said to be (*right*) *extendable* if every word of  $L$  is a strict prefix of another word of  $L$ .

**Definition 2.1.** *A language  $L$  is called a PCE language if it is both prefix-closed and right extendable.*

**Definition 2.2.** *Every infinite language  $L$  over  $A$  is totally ordered by the radix order on  $A^*$ . The successor of a word  $w$  of  $L$  is the least of all words of  $L$  greater than  $w$ , a well-defined word since radix order is a well-order, and denoted by  $\text{Succ}_L(w)$ .*

Hence  $\text{Succ}_L$  is a map from  $A^*$  into itself, whose domain is  $L$  and image is  $L \setminus \{w_0\}$ , where  $w_0$  is the least word in  $L$  for the radix order.

Languages over totally ordered alphabets have been called *Abstract Numeration Systems* (ANS for short) and studied, for instance, in [21] or [22].<sup>4</sup> Of course, such a language  $L$  can be totally ordered:  $w_0$  is the least word of  $L$ ,  $w_1$  is the least word of  $L \setminus \{w_0\}$ ,  $w_2$  the least word of  $L \setminus \{w_0, w_1\}$ ,  $w_{i+1}$  the least word of  $L \setminus \{w_0, w_1, \dots, w_i\}$ , and so on:

$$L = \{w_0 \sqsubseteq w_1 \sqsubseteq w_2 \sqsubseteq \dots \sqsubseteq w_i \sqsubseteq \dots\} .$$

By definition,  $w_i$ , the  $(i+1)$ -th word of  $L$  in that enumeration, is *the  $L$ -representation* of the integer  $i$  and is denoted by  $\langle i \rangle_L$  — hence  $w_0$  is the representation of 0. Conversely, we let  $\pi_L(w)$  denote the integer represented by the word  $w$  of  $L$ :  $\langle \pi_L(w) \rangle_L = w$ . In this setting, the successor function behaves as expected, that is, for every non-negative integer  $i$ ,

$$\text{Succ}_L(\langle i \rangle_L) = \langle i+1 \rangle_L .$$

The notion of ANS is consistent with that of *positional* numeration systems in the sense that the language of representations of integers in such systems, seen as an ANS, gives the same representation for every integer.

**Example 2.3. The integer base numeration systems.** Let  $p$  be an integer,  $p > 1$ , taken as a base. We write  $\langle n \rangle_p$  for the representation of  $n$  in base  $p$  (the  $p$ -representation of  $n$ ). Let  $A_p = \{0, 1, \dots, p-1\}$  be the alphabet of digits used to write integers in base  $p$  and  $L_p = \{\varepsilon\} \cup \{1, \dots, p-1\}A_p^*$  the set of  $p$ -representations of the integers.<sup>5</sup> The consistency claimed above reads:

$$\forall n \in \mathbb{N} \quad \langle n \rangle_p = \langle n \rangle_{L_p} .$$

Other examples such as *rational base numeration systems* are presented in Example 3.20 and *greedy numeration systems* in Sec. 5.3.1.

---

<sup>4</sup>To tell the truth, ANS are supposed to be *rational* (or regular) languages in these references [21, 22]. Although it will be met in most instances in this work, this hypothesis of being rational is not necessary for the basic definitions in ANS and we indeed also consider ANS which are *not* rational.

<sup>5</sup>For consistency with the whole theory we present here, the integer 0 is represented by  $\varepsilon$  even though, in reality, its  $p$ -representation is ‘0’.



### 2.3 The language tree

A prefix-closed language  $L$  of  $A^*$  is the *branch language* of a labeled tree  $\mathcal{T}_L$ , that we call the *language tree* of  $L$ .

The nodes of  $\mathcal{T}_L$  are indifferently seen as labeled by the words of  $L$  or by the non-negative integers: the root of  $\mathcal{T}_L$  is associated with  $\varepsilon$  and with  $0 = \langle \varepsilon \rangle_L$ ; a node labeled by  $w$  (and by  $n = \langle w \rangle_L$ ) has as many children as there are letters  $a_1, a_2, \dots, a_k$  in  $A$  such that  $wa_1, wa_2, \dots, wa_k$  are words in  $L$  and the edge between the node  $w$  (or  $n$ ) and the node  $wa_i$  (or  $m = \langle wa_i \rangle_L$ ) is labeled by  $a_i$ . It follows that the tree  $\mathcal{T}_L$  is naturally an *ordered tree* in the sense that the children  $wa_1, wa_2, \dots, wa_k$  are ordered by  $a_1 < a_2 < \dots < a_k$ .

The *breadth-first traversal* of the ordered tree  $\mathcal{T}_L$  amounts to enumerating the words of  $L$  in the radix order. We come back to this fact in Sec. 3.4.

If  $L$  is (right) extendable, then  $\mathcal{T}_L$  has no leaf and every branch of  $\mathcal{T}_L$  is infinite.

**Example 2.4** (Example 2.3 continued). The first nodes of the tree  $\mathcal{T}_{L_p}$ , that we rather write  $\mathcal{T}_p$ , are represented in Figure 1(a) for the case  $p = 3$ .

**Example 2.5. The Fibonacci numeration system.** The Fibonacci numeration system is a positional numeration system based on the sequence of Fibonacci numbers, that is, the linear recurrence sequence  $(F_n)_{n \geq 0}$  where  $F_0 = 1$ ,  $F_1 = 2$  and  $F_{n+2} = F_{n+1} + F_n$  for all  $n \geq 0$ . The set of representations of the natural integers in that system is known to be the set of words of  $\{0, 1\}^*$  that do not contain two consecutive 1's, that is,  $L_F = \{\varepsilon\} \cup 1\{0, 1\}^* \setminus \{0, 1\}^*11\{0, 1\}^*$  or simply  $L_F = \{\varepsilon\} \cup 1\{0, 01\}^*$ . The first nodes of the language tree  $\mathcal{T}_F$  are represented in Figure 1(b). For a general reference on non-standard numeration systems, see *e.g.* [17].

**Example 2.6. The Fina numeration system.** The sequence of Fibonacci numbers of *even rank* is also a linear recurrence sequence, defined by  $E_0 = 1$ ,  $E_1 = 3$  and  $E_{n+2} = 3E_{n+1} - E_n$  for all  $n \geq 0$ . The positional numeration system based on the sequence  $(E_n)_{n \geq 0}$ , which we call *Fina*, is known to give the integers representations that are the words of  $\{0, 1, 2\}^*$  which do not contain factors in the language  $21^*2$ . The first nodes of the language tree  $\mathcal{T}_E$  of  $E$  are represented in Figure 1(c).

### 2.4 Automata

We essentially follow the definitions and notation of [17, 32] for automata.

An *automaton over  $A$* ,  $\mathcal{A} = \langle A, Q, I, E, T \rangle$ , is a directed graph with edges labeled by elements of  $A$ . The set of vertices, traditionally called *states*, is denoted by  $Q$ ,  $I \subset Q$  is the set of *initial* states,  $T \subset Q$  is the set of *terminal* states and  $E \subset Q \times A \times Q$  is the set of labeled *edges*. If  $(p, a, q) \in E$ , we write  $p \xrightarrow{a} q$ . The

automaton is *finite* if  $Q$  is finite. The automaton  $\mathcal{A}$  is *deterministic* if  $E$  is the graph of a (partial) function from  $Q \times A$  to  $Q$ , and if there is a unique initial state. It is *trim* if every state is *accessible* and *co-accessible*.

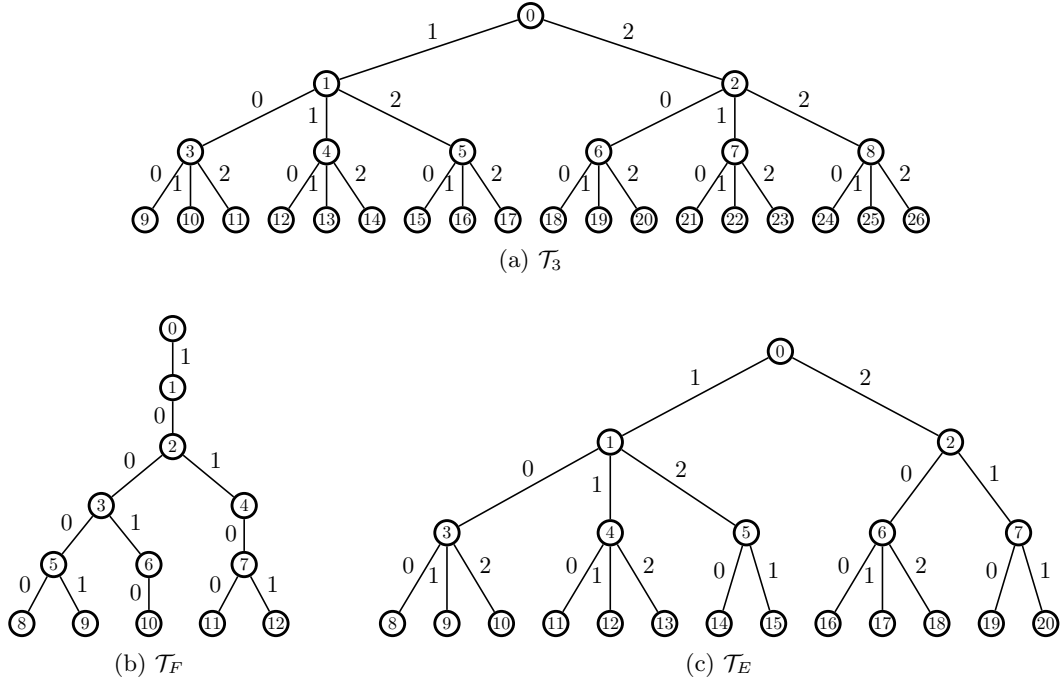


Figure 1: First levels of three language trees.

A language  $L$  of  $A^*$  is said to be *recognizable by a finite automaton* or *rational* if there exists a finite automaton  $\mathcal{A}$  such  $L$  is equal to the set  $L(\mathcal{A})$  of labels of paths starting in an initial state and ending in a terminal state. The set of rational languages over the alphabet  $A$  is denoted by  $\text{Rat } A^*$ . Note that the automata defined below implicitly read words *from left to right*.

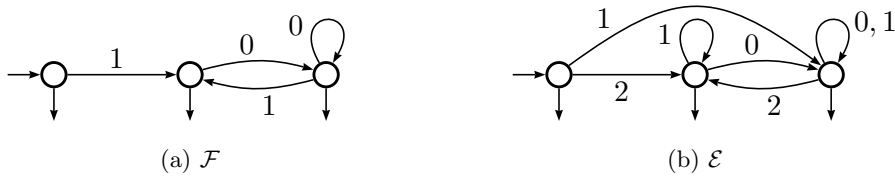


Figure 2: Two automata for representation languages.

## 2.5 A calculus classic

The general following statement will be used several times in the paper.

**Lemma 2.7.** Let  $(x(n))_{n \in \mathbb{N}}$  be an increasing sequence of positive numbers and  $(y(n))_{n \in \mathbb{N}}$  the sequence of the sums of initial segments:  $y(n) = \sum_{i=0}^n x(i)$  for every  $n$ . Then, the following statements are equivalent:

- (i)  $\lim_{n \rightarrow \infty} \frac{x(n+1)}{x(n)}$  exists and is equal to  $\gamma > 1$ ;
- (ii)  $\lim_{n \rightarrow \infty} \frac{y(n+1)}{y(n)}$  exists and is equal to  $\gamma > 1$ ;
- (iii)  $\lim_{n \rightarrow \infty} \frac{y(n)}{x(n)}$  exists and is equal to  $\frac{\gamma}{\gamma-1}$ .

*Proof.* Let us recall a classical result [12, Chap. V.4, Prop. 2]. Let  $(u_n)_{n \in \mathbb{N}}$  and  $(v_n)_{n \in \mathbb{N}}$  be two sequences of non-negative numbers. If the series  $\sum_{j=0}^{+\infty} v_j$  is divergent, then  $u_n \sim v_n$  implies that  $\sum_{j=0}^n u_j \sim \sum_{j=0}^n v_j$ . This result is sometimes referred to as Stolz–Cesàro Theorem.

(i) implies (ii): by the ratio test, the series  $\sum_{j=0}^{+\infty} x(j)$  is divergent. Apply the above result with  $(u_n)_{n \in \mathbb{N}} = (x(n+1))_{n \in \mathbb{N}}$  and  $(v_n)_{n \in \mathbb{N}} = (\gamma x(n))_{n \in \mathbb{N}}$ . We obtain that

$$\sum_{j=0}^n u_j = \sum_{j=1}^{n+1} x(j) = y(n+1) - x(0) \sim \sum_{j=0}^n v_j = \gamma \sum_{j=0}^n x(j) = \gamma y(n)$$

and the conclusion follows.

(ii) implies (i): from (ii) we have:

$$\lim_{n \rightarrow \infty} \frac{y(n) + x(n+1)}{y(n)} = \gamma$$

and thus  $\frac{x(n+1)}{y(n)} \rightarrow \gamma - 1$ . Since

$$\frac{x(n+1)}{x(n)} = \frac{x(n+1)}{y(n)} \frac{y(n)}{y(n-1)} \frac{y(n-1)}{x(n)},$$

the result follows.

(ii) implies (iii): since  $y(n) = y(n-1) + x(n)$  dividing both sides by  $y(n-1)$  and letting  $n$  tends to infinity, leads to

$$\gamma = 1 + \lim_{n \rightarrow \infty} \frac{x(n)}{y(n)} \frac{y(n)}{y(n-1)}.$$

We conclude that  $\frac{x(n)}{y(n)} \rightarrow \frac{\gamma-1}{\gamma}$ .

(iii) implies (ii): again since  $y(n) = y(n-1) + x(n)$ , observe that

$$\lim_{n \rightarrow \infty} \frac{y(n)}{x(n)} = \frac{\gamma}{\gamma-1} \quad \text{if and only if} \quad \lim_{n \rightarrow \infty} \frac{y(n-1)}{x(n)} = \frac{1}{\gamma-1}.$$

Since  $\frac{y(n)}{y(n-1)} = \frac{y(n)}{x(n)} \frac{x(n)}{y(n-1)}$ , the result follows. □

### 3 The carry propagation of a language: a combinatorial point of view

We first define the carry propagation of a language  $L$  and show that it does not always exist. Sufficient conditions for its existence, and for its computation are then investigated in terms, first, of growth rates of the language and, then, of the notion of signature associated with the language tree of  $L$ , by stressing the fact that what counts for carry propagation is the shape of the tree and not its labeling.

#### 3.1 First definitions for the carry propagation

We write  $u \wedge v$  for the *longest common left factor* of two words  $u$  and  $v$  of  $A^*$ . If two words  $u$  and  $v$  of  $A^*$  have the *same length*, we write  $\Delta(u, v)$  for the (common) length of the left quotient of  $u$  (or  $v$ ) by  $u \wedge v$ :

$$\Delta(u, v) = |u| - |u \wedge v| = |v| - |u \wedge v| .$$

If  $u$  and  $v$  do *not* have the same length, we set

$$\Delta(u, v) = \max\{|u|, |v|\} ,$$

which is the same as  $\Delta(u', v')$  where  $u'$  and  $v'$  are obtained from  $u$  and  $v$  by padding the shorter word *on the left* with a symbol which is not in  $A$  and so that  $|u'| = |v'|$ .

**Definition 3.1.** *Let  $A$  be an ordered alphabet and  $L$  a language of  $A^*$ , ordered by radix order. The carry propagation at a word  $w$  of  $L$ , and with respect to  $L$ , is the quantity:*

$$\text{cp}_L(w) = \Delta(w, \text{Succ}_L(w)) .$$

*We naturally consider a language over an ordered alphabet as an abstract numeration system and we also write, for every integer  $i$ ,*

$$\text{cp}_L(i) = \text{cp}_L(\langle i \rangle_L) = \Delta(\langle i \rangle_L, \langle i + 1 \rangle_L) .$$

**Example 3.2** (Example 2.5 continued). In the Fibonacci numeration system,  $\langle 9 \rangle_F = 10001$  and  $\langle 10 \rangle_F = 10010$ , hence  $\text{cp}_F(9) = 2$ . We also have  $\langle 12 \rangle_F = 10101$  and  $\langle 13 \rangle_F = 100000$ . Thus  $\text{cp}_F(12) = 6$ .

From the definition of the carry propagation at a word, we derive the carry propagation *of a language*. We first denote by  $\text{scp}_L(N)$  the *sum of the carry propagations at the first  $N$  words of the language  $L$* :

$$\text{scp}_L(N) = \sum_{i=0}^{N-1} \text{cp}_L(i) . \tag{4}$$

**Definition 3.3** ([5]). *The carry propagation of a language  $L \subseteq A^*$ , which we denote by  $\text{CP}_L$ , is the amortized carry propagation at the words of the language, that is, the limit, if it exists, of the mean of the carry propagation at the first  $N$  words of the language:*

$$\text{CP}_L = \lim_{N \rightarrow \infty} \frac{1}{N} \text{scp}_L(N) .$$

### 3.2 The language tree and the carry propagation

We denote by  $\mathbf{u}_L(\ell)$  (resp.  $\mathbf{v}_L(\ell)$ ) the number of words of  $L$  of length  $\ell$  (resp. of length less than, or equal to,  $\ell$ ):

$$\mathbf{u}_L(\ell) = \text{card} \left( L \cap A^\ell \right) \quad \text{and} \quad \mathbf{v}_L(\ell) = \text{card} \left( L \cap A^{\leq \ell} \right) = \sum_{i=0}^{\ell} \mathbf{u}_L(i) .$$

The set of words of  $L$  of each length that are maximal in the radix (or lexicographic) order is denoted by  $\text{Maxlg}(L)$ . We have:

$$\begin{aligned} \text{Maxlg}(L) &= \{ \langle \mathbf{v}_L(\ell) - 1 \rangle_L \mid \ell \in \mathbb{N} \} \quad \text{and} \\ L \cap A^\ell &= \{ u \in L \mid \mathbf{v}_L(\ell - 1) \leq \pi_L(u) < \mathbf{v}_L(\ell) \} . \end{aligned}$$

The carry propagation  $\text{CP}_L$  is more easily evaluated when the terms  $\text{cp}_L(i)$  of the sum  $\text{scp}_L(N)$  are first *aggregated* in *partial sums* corresponding to *words of fixed length*. In particular, we can state:

**Proposition 3.4.** *If  $L$  is a PCE language, then, for every integer  $\ell$ ,*

$$\sum_{\substack{w \in L \\ |w| = \ell}} \text{cp}_L(w) = \sum_{i=\mathbf{v}_L(\ell-1)}^{\mathbf{v}_L(\ell)-1} \text{cp}_L(i) = \mathbf{v}_L(\ell) . \quad (5)$$

This proposition is indeed an instance of the more precise Theorem 3.6 that will be used in subsequent proofs and that requires a definition.

Let  $\mathcal{T}_L$  be the language tree of  $L$  and  $w$  a word of  $L$  of length  $\ell$ . Let us denote by  $\mathcal{T}_L^{(\ell)}$  the part of  $\mathcal{T}_L$  which consists of words of  $L$  of length less than, or equal to,  $\ell$ . And let us see  $\text{Pre}(w)$ , the set of prefixes of  $w$  that form the unique path from  $w$  to  $\varepsilon$ , as a river that flows from  $w$  to  $\varepsilon$ ; it determines two subsets of  $\mathcal{T}_L^{(\ell)}$ : the ‘left bank’ of  $w$ ,  $\text{LB}_L(w)$ , and the ‘right bank’ of  $w$ ,  $\text{RB}_L(w)$ , which consists respectively of the nodes on the left and on the right of  $\text{Pre}(w)$  as depicted in Figure 3. Together,  $\text{LB}_L(w)$ ,  $\text{Pre}(w)$  and  $\text{RB}_L(w)$  form a partition of  $\mathcal{T}_L^{(\ell)}$  and we have:

$$\text{LB}_L(w) = \{ u \in L \mid |u| \leq |w| \quad \text{and} \quad u \preceq w \} \setminus \text{Pre}(w) .$$

**Example 3.5** (Example 2.5 continued). In  $\mathcal{T}_F$ , we have:

$$\begin{aligned} \text{LB}_F(10010) &= \{1000, 10000, 10001\} \quad \text{and} \\ \text{LB}_F(10100) &= \text{LB}_F(10010) \cup \{100, 1001, 10010\} . \end{aligned}$$

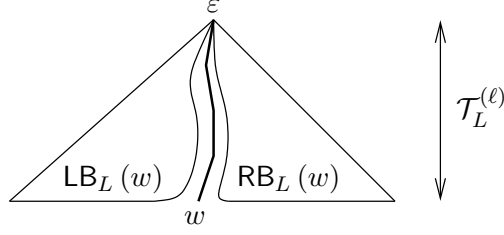


Figure 3: The tree  $\mathcal{T}_L^{(\ell)}$  and the three sets  $\text{LB}_L(w)$ ,  $\text{Pre}(w)$  and  $\text{RB}_L(w)$ .

The statement we are aiming at gives the sum of the carry propagation at all words of the same length  $\ell$  as a word  $u$  and less than or equal to  $u$  in the lexicographic order. We recall that  $\text{Maxlg}(L) = \{\langle \mathbf{v}_L(\ell) - 1 \rangle_L \mid \ell \in \mathbb{N}\}$ .

**Theorem 3.6.** *Let  $L$  be a PCE language,  $u$  in  $L$  of length  $\ell$  and  $N = \pi_L(u)$ . Then, we have:*

$$\sum_{i=\mathbf{v}_L(\ell-1)}^N \text{cp}_L(i) = \begin{cases} \text{card}(\text{LB}_L(\text{Succ}_L(u))) & \text{if } u \notin \text{Maxlg}(L) , \\ \mathbf{v}_L(\ell) & \text{if } u \in \text{Maxlg}(L) . \end{cases} \quad (6)$$

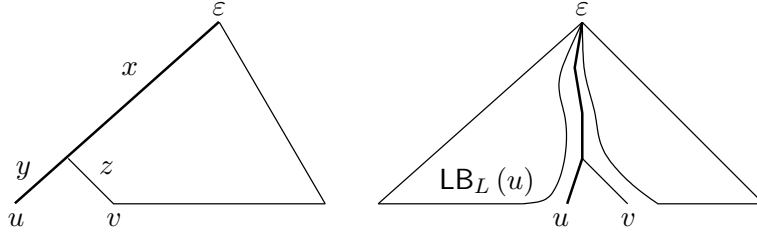


Figure 4: Illustrations of the first two cases of the proof of Theorem 3.6.

*Proof.* The proof works by induction on  $N$ . Let  $u = \langle N \rangle_L$  and  $\ell = |u|$ . Hence  $\mathbf{v}_L(\ell - 1) \leq N \leq \mathbf{v}_L(\ell) - 1$ .

(i) We first assume  $N = \mathbf{v}_L(\ell - 1)$ . The word  $u$  is the smallest word of  $L$  of length  $\ell$  (in the lexicographic order). Let  $v = \text{Succ}_L(u)$ . We first suppose that  $u$  is not in  $\text{Maxlg}(L)$ . Then (as depicted on the left part of Figure 4):

$$u = xy, \quad v = xz \quad \text{and} \quad \text{cp}_L(N) = \Delta(u, v) = |y| = |z| .$$

But, since  $L$  is prefix-closed,  $|y|$  is exactly the number of nodes in  $\text{LB}_L(v)$ .

Now, if  $u = \langle \mathbf{v}_L(\ell - 1) \rangle_L$  is in  $\text{Maxlg}(L)$ , then there is only one word in  $L$  for every length  $k$ ,  $0 \leq k \leq \ell$  and we have at the same time  $\text{cp}_L(u) = \ell + 1$  and  $\mathbf{v}_L(\ell) = \ell + 1$ , hence (6) still holds in this case.

(ii) We now assume  $\mathbf{v}_L(\ell - 1) < N < \mathbf{v}_L(\ell) - 1$ . Hence  $v = \text{Succ}_L(u)$  is of length  $\ell$  and as above there exist  $x, y$  and  $z$  such that  $u = xy$  and  $v = xz$ . The

same reasoning as above applies (see the right part of Figure 4):

$$\sum_{i=\mathbf{v}_L(\ell-1)}^N \text{cp}_L(i) = \sum_{i=\mathbf{v}_L(\ell-1)}^{N-1} \text{cp}_L(i) + \text{cp}_L(N) = \text{card}(\text{LB}_L(u)) + \text{cp}_L(u) = \text{card}(\text{LB}_L(u)) + |y| .$$

But, since  $L$  is prefix-closed,  $|y|$  is the number of nodes in  $\text{LB}_L(v) \setminus \text{LB}_L(u)$ .

(iii) Finally, assume  $N = \mathbf{v}_L(\ell) - 1$ . Then  $u = \langle N \rangle_L$  belongs to  $\text{Maxlg}(L)$ . In this case,

$$\text{cp}_L(u) = \ell + 1, \quad \text{LB}_L(u) \cup \text{Pre}(u) = \mathcal{T}_L^{(\ell)} \quad \text{and} \\ \sum_{i=\mathbf{v}_L(\ell-1)}^N \text{cp}_L(i) = \text{card}(\text{LB}_L(u)) + (\ell + 1) = \text{card}(\mathcal{T}_L^{(\ell)}) = \mathbf{v}_L(\ell) . \quad \square$$

Proposition 3.4 is the instance of Theorem 3.6 when  $N = \mathbf{v}_L(\ell) - 1$ . By grouping the sum of carry propagations by words of the same length, Theorem 3.6 also yields an evaluation of the sum (4) of the carry propagations at the first  $N$  words of a PCE language:

**Corollary 3.7.** *Let  $L$  be a PCE language,  $u$  in  $L$  of length  $\ell$  and  $N = \pi_L(u)$ . We then have:*

$$\text{scp}_L(N) = \sum_{i=0}^{\ell-1} \mathbf{v}_L(i) + \text{card}(\text{LB}_L(\text{Succ}_L(u))) .$$

**Example 3.8** (Example 2.3 continued). Let  $p$  be an integer,  $p > 1$ , and  $L_p$  the set of  $p$ -representations of the integers. In order to lighten the notation, we write  $\mathbf{u}_p(\ell)$  instead of  $\mathbf{u}_{L_p}(\ell)$ ,  $\mathbf{v}_p(\ell)$  instead of  $\mathbf{v}_{L_p}(\ell)$ ,  $\text{Succ}_p(u)$  instead of  $\text{Succ}_{L_p}(u)$ ,  $\text{CP}_p$  instead of  $\text{CP}_{L_p}$ , etc. As a first application of Theorem 3.6, Proposition 3.9 below allows one to recover the value  $\frac{p}{p-1}$  for the carry propagation.

**Proposition 3.9.** *Let  $p$  be an integer,  $p > 1$ , and  $L_p$  the set of  $p$ -representations of the integers. The carry propagation  $\text{CP}_p$  exists and is equal to  $\frac{p}{p-1}$ .*

*Proof.* Let  $N$  in  $\mathbb{N}$  and  $u = \langle N \rangle_p$ ; we have:  $\mathbf{v}_p(\ell-1) \leq N < \mathbf{v}_p(\ell)$  with  $\ell = |u|$ . And then, by Corollary 3.7:

$$\text{scp}_p(N) = \sum_{i=0}^{\ell-1} \mathbf{v}_p(i) + \text{card}(\text{LB}_p(\text{Succ}_p(u))) . \quad (7)$$

First, and since  $\mathbf{v}_p(k) = p^k$ , for every  $k$ , then, by Lemma 2.7,

$$\lim_{\ell \rightarrow \infty} \frac{1}{\mathbf{v}_p(\ell-1)} \sum_{i=0}^{\ell-1} \mathbf{v}_p(i) = \frac{p}{p-1}$$

which can be written as:

$$\sum_{i=0}^{\ell-1} \mathbf{v}_p(i) = \mathbf{v}_p(\ell-1) \left( \frac{p}{p-1} + \varepsilon(\ell) \right) \quad \text{with } \lim_{\ell \rightarrow \infty} \varepsilon(\ell) = 0 . \quad (8)$$

Second, we turn to the evaluation of  $\text{card}(\text{LB}_p(\text{Succ}_p(u)))$ . Let  $v = \text{Succ}_p(u)$ ; we exclude the case where  $N = \mathbf{v}_p(\ell) - 1$  and  $|v| = \ell + 1$  (which corresponds to  $\text{scp}_p(N) = \sum_{i=0}^{\ell} \mathbf{v}_p(i)$ ) and we write

$$N = \mathbf{v}_p(\ell-1) + (M-1) \quad \text{with } 1 \leq M < \mathbf{u}_p(\ell) .$$

We write  $\mathcal{T}_p$  for the language tree of  $L_p$ ,  $\mathcal{T}_p^{(\ell)}$  for its truncation to length  $\ell$ . Every node of  $\mathcal{T}_p$ , every internal node of  $\mathcal{T}_p^{(\ell)}$ , is of degree  $p$ , but the root, which is of degree  $p-1$ .

Since  $\langle \mathbf{v}_p(\ell-1) \rangle_p$  is the smallest word of  $L_p$  of length  $\ell$ ,  $v$  is the  $(M+1)$ -th word of  $L_p$  of length  $\ell$  and  $\text{card}(\text{LB}_p(v) \cap A^\ell) = M$ . We suppose that  $\ell > 1$  (which is not a restriction since we want  $\ell$  to tend to infinity). Since every internal node of  $\mathcal{T}_p^{(\ell)}$  at level  $\ell-1$  is of degree  $p$ :

$$\text{card}(\text{LB}_p(v) \cap A^{\ell-1}) = \left\lfloor \frac{M}{p} \right\rfloor .$$

By induction on  $k$ ,  $1 \leq k < \ell-1$ , and with the same argument:

$$\text{card}(\text{LB}_p(v) \cap A^{\ell-k}) = \left\lfloor \frac{M}{p^k} \right\rfloor .$$

From the inequalities  $\frac{M}{p^k} - 1 \leq \left\lfloor \frac{M}{p^k} \right\rfloor \leq \frac{M}{p^k}$ , we first get

$$M + \sum_{k=1}^{\ell-1} \left\lfloor \frac{M}{p^k} \right\rfloor \geq M + \sum_{k=1}^{\ell-1} \frac{M}{p^k} - (\ell-1) = M \frac{p}{p-1} - \ell + 1 - \frac{M}{p^{\ell-1}(p-1)}$$

and since  $M < p^\ell$ ,  $1 - M/(p^{\ell-1}(p-1)) \geq -1$ , it leads to the lower and upper bounds

$$M \frac{p}{p-1} - (\ell+1) \leq \text{card}(\text{LB}_p(v)) \leq M \frac{p}{p-1} .$$

Together with (8), they yield the bounds

$$(N+1) \frac{p}{p-1} + \mathbf{v}_p(\ell-1) \varepsilon(\ell) - (\ell+1) \leq \text{scp}_p(N) \leq (N+1) \frac{p}{p-1} + \mathbf{v}_p(\ell-1) \varepsilon(\ell) .$$

If we divide by  $N$ , both the lower and upper bounds tend to  $\frac{p}{p-1}$  when  $N$  tends to infinity, hence  $\frac{1}{N} \text{scp}_p(N)$  has a limit, and this limit is  $\frac{p}{p-1}$ .  $\square$

After Proposition 3.4, it is natural to extract from the sequence of means of carry propagations up to the first  $N$  words of  $L$ , those that correspond to the first  $\mathbf{v}_L(\ell)$  words of  $L$ .



**Definition 3.10.** For a language  $L$ , we call the *limit*, if it exists, of the mean of the carry propagation at the first  $\mathbf{v}_L(\ell)$  words of  $L$  the length-filtered carry propagation of  $L$ , and we denote it by  $\text{FCP}_L$ :

$$\text{FCP}_L = \lim_{\ell \rightarrow \infty} \frac{1}{\mathbf{v}_L(\ell)} \text{scp}_L(\mathbf{v}_L(\ell)) = \lim_{\ell \rightarrow \infty} \frac{1}{\mathbf{v}_L(\ell)} \sum_{i=0}^{\ell} \mathbf{v}_L(i) . \quad (9)$$

**Remark 3.11.** Of course, if  $\text{CP}_L$  exists, then  $\text{FCP}_L$  exists and  $\text{CP}_L = \text{FCP}_L$  but the converse does not hold as we shall see with Example 3.17. On the other hand, an easy way for showing that  $\text{CP}_L$  does not exist is to prove that  $\text{FCP}_L$  does not exist.

### 3.3 The local growth rate and the carry propagation

From Proposition 3.4 it also follows that the carry propagation of a language  $L$  is closely related to other growth measures of  $L$ . It is the case in particular of the growth rates.

First, the *global growth rate*  $\eta_L$  of a language  $L$  (called *growth rate* in [34] for instance) is classically defined by:

$$\eta_L = \limsup_{\ell \rightarrow \infty} \sqrt[\ell]{\mathbf{u}_L(\ell)} .$$

A language  $L$  is said to have *exponential growth* if  $\eta_L > 1$  and *polynomial growth* if  $\mathbf{u}_L(\ell) \leq P(\ell)$  for some polynomial  $P$  and all large enough  $\ell$ .

**Example 3.12. Languages with polynomial growth.** Let  $L$  be a PCE language such that  $\mathbf{u}_L(\ell) = P(\ell)$  for some polynomial  $P$  of degree  $d$ . Then  $\mathbf{v}_L(\ell)$  is a polynomial of degree  $d+1$  and by Proposition 3.4,  $\text{scp}_L(\mathbf{v}_L(\ell))$  is a polynomial of degree  $d+2$ . Hence  $\lim_{\ell \rightarrow \infty} \frac{1}{\mathbf{v}_L(\ell)} \text{scp}_L(\mathbf{v}_L(\ell)) = +\infty$  and  $\text{FCP}_L$  does not exist.

**Definition 3.13.** We call the *limit*, if it exists, of the ratio between the number of words of a language  $L$  of length  $\ell$  and the number of words of  $L$  of length  $\ell+1$ , when  $\ell$  tends to infinity, the *local growth rate* of  $L$ , and we denote it by  $\gamma_L$ :

$$\gamma_L = \lim_{\ell \rightarrow +\infty} \frac{\mathbf{u}_L(\ell+1)}{\mathbf{u}_L(\ell)} .$$

**Remark 3.14.** Observe that the quantity  $\eta_L$  always exists since it is defined by an upper limmit. If the local growth rate  $\gamma_L$  exists, then  $\gamma_L = \eta_L$ .

The definition of length-filtered carry propagation (see Definition 3.10) together with Proposition 3.4 directly implies the following.

**Proposition 3.15.** Let  $L$  be a PCE language with exponential growth. Then,  $\text{FCP}_L$  exists if and only if  $\gamma_L$  exists and, in this case,  $\text{FCP}_L = \frac{\gamma_L}{\gamma_L - 1}$  holds.

*Proof.* Using Lemma 2.7, if  $\lim_{\ell \rightarrow \infty} \frac{\mathbf{u}_L(\ell+1)}{\mathbf{u}_L(\ell)} = \gamma_L$ , then  $\lim_{\ell \rightarrow \infty} \frac{\mathbf{v}_L(\ell+1)}{\mathbf{v}_L(\ell)} = \gamma_L$ . Using again Lemma 2.7, the latter limit exists if and only if

$$\text{FCP}_L = \lim_{\ell \rightarrow \infty} \frac{1}{\mathbf{v}_L(\ell)} \sum_{i=0}^{\ell} \mathbf{v}_L(i) = \frac{\gamma_L}{\gamma_L - 1} . \quad \square$$

From Remark 3.11, the following holds, which extends the case of numeration in base  $p$  described in Proposition 3.9.

**Corollary 3.16.** *If the carry propagation  $\text{CP}_L$  exists, then the local growth  $\gamma_L$  exists and  $\text{CP}_L = \frac{\gamma_L}{\gamma_L - 1}$ .*

However, the existence of  $\gamma_L$ , and hence of  $\text{FCP}_L$ , does not imply in general the existence of the carry propagation  $\text{CP}_L$  of a language, as witnessed by the following example.

**Example 3.17. A language with an unbalanced tree.** Let  $A = \{a, b, c\}$ . The PCE language  $H$  we build will be such that  $\mathbf{u}_H(\ell) = 2^\ell$ , for every  $\ell$ . We denote by  $H_\ell$  the set  $H \cap A^\ell$  and by  $H'_\ell$  (resp.  $H''_\ell$ ) the first (resp. the last)  $2^{\ell-1}$  words of length  $\ell$  in the radix ordered language  $H_\ell$ . Set  $H_1 = \{a, c\}$ . For all  $\ell > 0$ ,  $H_{\ell+1} = \{H'_\ell\}A \cup \{H''_\ell\}b$ . Thus we get  $H_2 = \{aa, ab, ac, cb\}$ ,  $H_3 = \{aaa, aab, aac, aba, abb, abc, acb, cbb\}$  and it is clear that  $\mathbf{u}_H(\ell) = 2^\ell$  and  $\mathbf{v}_H(\ell) = 2^{\ell+1} - 1$ . Hence  $\gamma_H = 2$  and  $\text{FCP}_H = 2$  by Proposition 3.15.

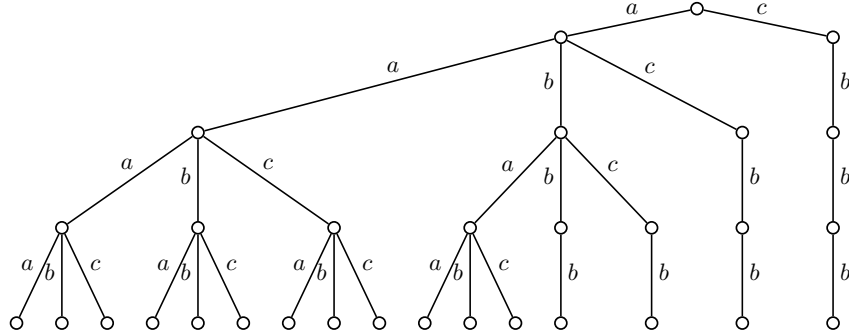


Figure 5: The first 5 levels of  $\mathcal{T}_H$ .

Let, for every  $\ell$ ,  $M(\ell) = 2^{\ell+1} - 1 + 2^\ell$  and let us evaluate  $\text{scp}_H(M(\ell))$ .

(i) The contribution to  $\text{scp}_H(M(\ell))$  of the words of length less than, or equal to,  $\ell$  is equal to  $C = \sum_{i=0}^{\ell} \mathbf{v}_H(i) = \sum_{i=0}^{\ell} (2^{i+1} - 1) = 2^{\ell+2} - \ell - 2$ .

(ii) By construction of  $H$ , the elements of  $H'_{\ell+1}$  are the leftmost  $2^\ell$  leaves of a ternary tree of height  $k$  such that  $3^k > 2^\ell$ . Since the carry propagation in base 3 is equal to  $3/2$  (as seen in the proof of Proposition 3.9), the contribution of the elements of  $H'_{\ell+1}$  to  $\text{scp}_H(M(\ell))$  is less than  $D = 2^\ell \times 3/2 = 2^{\ell-1} \times 3$ . We have:

$$\frac{1}{M(\ell)} \text{scp}_H(M(\ell)) < \frac{C + D}{2^{\ell+1} + 2^\ell} = \frac{2^{\ell+2} - \ell - 2 + 2^{\ell-1} \times 3}{2^{\ell+1} + 2^\ell} .$$

Hence

$$\lim_{\ell \rightarrow \infty} \frac{1}{M(\ell)} \text{scp}_H(M(\ell)) \leq \frac{11}{6} \neq \lim_{\ell \rightarrow \infty} \frac{1}{\mathbf{v}_H(\ell)} \text{scp}_H(\mathbf{v}_H(\ell)) = \text{FCP}_H = 2 .$$

The quantity  $\frac{1}{N} \text{scp}_H(N)$  has no limit when  $N$  tends to infinity and  $\text{CP}_H$  does not exist.

In view of Sec. 4 where we prove that the existence of the local growth rate of a language and its quotients (see Theorem 4.1) is a sufficient condition for a *rational* language to have a carry propagation, let us add that this language  $H$  is easily seen not to be rational. Indeed let  $m = m(n)$  be the smallest integer such that  $a^n b^m a$  is not in  $H$ . Then for every  $n' > n$ ,  $a^{n'} b^m a$  is an element of  $H$ , thus the words  $a^n$  have all distinct sets of right contexts for  $H$ .

### 3.4 The signature and the carry propagation

Theorem 3.6 and its proof make clear that the actual words of a language  $L$ , that is, the *labeling* of the language tree  $\mathcal{T}_L$ , have no impact on the carry propagation of  $L$ , its existence or its value, but what only counts is the *shape* of  $\mathcal{T}_L$  or, in one more precise word, its *signature*, introduced in [24, 25], and that we now define.

First, we introduce a slightly different look at trees that proves to be technically fit to the description and study of language trees associated with languages seen as abstract numeration systems (see Sec. 2.2 and 2.3).

Given a tree, we consider that in addition to all edges, the root is also a *child of itself*, that is, bears a loop onto itself.<sup>6</sup> We call such a structure an *i-tree*.<sup>7</sup> It is so close to a tree that we pass from one to the other with no further ado. When a tree is usually denoted by  $\mathcal{T}_x$  for some index  $x$ , the associated i-tree is denoted by  $\mathcal{I}_x$ , and conversely.

If the tree  $\mathcal{T}_x$  is labeled by letters of an ordered alphabet  $A$ , we want the loop on the root of the i-tree  $\mathcal{I}_x$  to be labeled by a letter less than the labels of all other edges going out of the root in  $\mathcal{T}_x$ . Either there exists a letter in  $A$  which meets the condition and it can be chosen as label for the loop, or such a letter does not exist in  $A$  and we enlarge the alphabet  $A$  with a new symbol, less than all letters of  $A$ . Figure 6 shows the language tree of the representation language in the Fibonacci numeration system and the associated i-tree.

The *degree* of a node in a tree, or in an i-tree, is the number of its children. The *signature*  $\mathbf{s}_x$  of a tree  $\mathcal{T}_x$  is the sequence of the degrees of the nodes of the associated i-tree  $\mathcal{I}_x$  in the breadth-first traversal. For instance, the signature of  $\mathcal{T}_F$  is  $\mathbf{s}_F = 21221212 \cdots$ , the signature of  $\mathcal{T}_p$  for the numeration in base  $p$  is the constant sequence  $\mathbf{s}_p = p^\omega$  for any base  $p > 1$ .

<sup>6</sup>This convention is sometimes taken when implementing tree-like structures (for instance in the Unix/Linux file system).

<sup>7</sup>The terminology comes indeed from the terminology for *inodes* in the Unix/Linux file system.

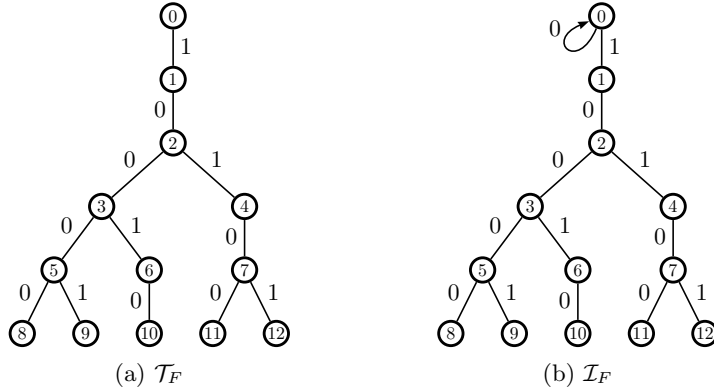


Figure 6: Tree and i-tree associated with the Fibonacci numeration system.

Conversely, we call *signature* any sequence  $\mathbf{s}$  of non-negative integers:  $\mathbf{s} = s_0 s_1 s_1 \cdots$  and a signature is *valid* if the following condition holds:

$$\forall j \in \mathbb{N} \quad \sum_{i=0}^j s_i > j + 1 .$$

Infinite trees and valid signatures are then in a 1-to-1 correspondence as expressed by the following.

**Proposition 3.18** ([24]). *The signature of an infinite tree is valid and a valid signature is the signature of a unique (i-)tree (up to the labeling).*

By extension, the signature of a (prefix-closed) language  $L$  is the signature of the language tree  $\mathcal{T}_L$ . The language  $L$  is extendable (or  $\mathcal{T}_L$  has no finite branch) if and only if its signature contains no ‘0’. As said above, *the carry propagation of a PCE language  $L$  is entirely determined by its signature* which determines the ‘shape’ of  $\mathcal{T}_L$ . In view of the next statements, we have to give two further definitions.

**Definition 3.19.** *Let  $p$  and  $q$  be two integers with  $p > q \geq 1$ .*

(i) *We call a  $q$ -tuple  $\mathbf{r}$  of non-negative integers whose sum is  $p$  a rhythm of directing parameter  $(q, p)$ :*

$$\mathbf{r} = (r_0, r_1, \dots, r_{q-1}) \quad \text{and} \quad \sum_{i=0}^{q-1} r_i = p .$$

(ii) *A signature  $\mathbf{s}$  is periodic if there exists a rhythm  $\mathbf{r}$  such that  $\mathbf{s} = \mathbf{r}^\omega$ . A signature  $\mathbf{s}$  is eventually periodic if there exists a rhythm  $\mathbf{r}$  such that there exist a finite sequence  $\mathbf{t}$  of non-negative integers and a rhythm  $\mathbf{r}$  such that  $\mathbf{s} = \mathbf{t}\mathbf{r}^\omega$ .*

Languages with periodic signatures were considered and characterized in [25] in the study of rational base numeration systems that we define as follows.

**Example 3.20. The rational base numeration systems.** Let  $\frac{p}{q}$  be a rational number, where  $p > q \geq 1$  are two *co-prime* integers.

In [1], it has been shown how to define a numeration system with  $\frac{p}{q}$  as a base and where nevertheless integers have finite representations. Let  $N$  be any positive integer; let us write  $N_0 = N$  and, for  $i \geq 0$ , let

$$qN_i = pN_{i+1} + a_i \quad (10)$$

where  $a_i$  is the remainder of the division of  $qN_i$  by  $p$ , and thus belongs to the digit-alphabet  $A_p = \{0, \dots, p-1\}$ . Since  $N_{i+1}$  is less than  $N_i$ , the division (10) can be repeated only a finite number of times, until eventually  $N_{k+1} = 0$  for some  $k$ . This algorithm produces the digits  $a_0, a_1, \dots, a_k$ , and:

$$N = \sum_{i=0}^k \frac{a_i}{q} \left(\frac{p}{q}\right)^i.$$

We will say that the word  $a_k \dots a_0$ , computed from  $N$  from right to left, that is to say, *least significant digit first*, is a  $\frac{p}{q}$ -*expansion* of  $N$ . It is known that this representation is indeed unique and we denote it by  $\langle N \rangle_{\frac{p}{q}}$ . We define the language  $L_{\frac{p}{q}}$  of  $A_p^*$  as the set of  $\frac{p}{q}$ -expansions of the integers:

$$L_{\frac{p}{q}} = \left\{ \langle n \rangle_{\frac{p}{q}} \mid n \in \mathbb{N} \right\}$$

and accordingly, we denote by  $\mathcal{T}_{\frac{p}{q}}$  the tree of the language  $L_{\frac{p}{q}}$ . When  $q = 1$ , we recover the usual numeration system in base  $p$  and  $L_{\frac{p}{q}} = L_p$ ; in the following,  $q \neq 1$ . Figure 7 shows the case  $p = 3$  and  $q = 2$ .

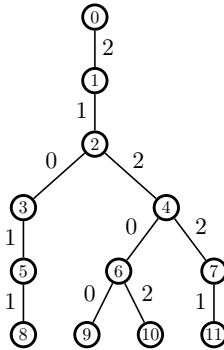


Figure 7: The first 6 levels of  $\mathcal{T}_{\frac{3}{2}}$ .

**Remark 3.21.** This definition is *not* the one corresponding to  $\beta$ -expansions with  $\beta = \frac{p}{q}$  (see Sec. 5.4). In particular, the digits are *not* the integers less than  $\frac{p}{q}$  but rather the integers less than  $p$ , hence those whose quotient by  $q$  is less than  $\frac{p}{q}$ .

From the classical theory of formal languages point of view, the language  $L_{\frac{p}{q}}$  is complex and difficult to understand. It can be shown not to meet any kind of iteration property (and thus not to be rational nor context-free) and such that any two distinct subtrees of  $\mathcal{T}_{\frac{p}{q}}$  are never isomorphic (cf. [1]). On the other hand, it is easy to verify the following property that expresses a certain kind of ‘regularity’ (and that has indeed been the motivation for the definition of signatures).

**Proposition 3.22** ([25]). *The signature of  $L_{\frac{p}{q}}$  is periodic and its period is a rhythm of directing parameter  $(q, p)$ .*

Note that having a periodic signature is even a characterization of rational base numeration systems (possibly using a non-canonical alphabet), according to [25, Theorem 2]. We now can state the main result of this section.

**Theorem 3.23.** *If a PCE language  $L$  has an eventually periodic signature with rhythm of parameter  $(q, p)$ , then  $\text{CP}_L$  exists and*

$$\text{CP}_L = \frac{p}{p - q} .$$

*Proof.* Let  $\mathbf{s} = \mathbf{tr}^\omega$  be the signature of  $\mathcal{T}_L$ . Let  $\mathbf{t} = t_0 t_1 \cdots t_k$  and  $\sum_{i=0}^k t_i = P$ . In the following, we always choose  $\ell$  larger than  $\ell_0$  such that  $\mathbf{v}_L(\ell - 1) > P$  and  $N$  larger than  $\mathbf{v}_L(\ell_0)$ , that is, we consider nodes and levels of  $\mathcal{T}_L$  where the signature is in its periodic part.

We first observe that at any given level  $\ell$ , the  $q$  leftmost nodes have  $p$  children at level  $\ell + 1$  and moreover for any  $k$  such that  $kq \leq \mathbf{u}_L(\ell)$ , the  $kq$  leftmost nodes have  $kp$  children at level  $\ell + 1$ . Conversely, the  $p$  leftmost nodes at level  $\ell$  are the children of the  $q$  leftmost nodes at level  $\ell - 1$  and for any  $k$  such that  $kp \leq \mathbf{u}_L(\ell)$ , the  $kp$  leftmost nodes at level  $\ell$  are the children of the  $kq$  leftmost nodes at level  $\ell - 1$ .

The first observation implies that for every  $\ell$  (greater than  $\ell_0$ ), we have:

$$p \left\lfloor \frac{\mathbf{u}_L(\ell)}{q} \right\rfloor \leq \mathbf{u}_L(\ell + 1) \leq p \left\lfloor \frac{\mathbf{u}_L(\ell)}{q} \right\rfloor + (p - 1) ,$$

hence 
$$\frac{p}{q} \mathbf{u}_L(\ell) - p \leq \mathbf{u}_L(\ell + 1) \leq \frac{p}{q} \mathbf{u}_L(\ell) + (p - 1) .$$

And since  $\lim_{\ell \rightarrow \infty} \mathbf{u}_L(\ell) = +\infty$ , it follows that

$$\lim_{\ell \rightarrow \infty} \frac{\mathbf{u}_L(\ell + 1)}{\mathbf{u}_L(\ell)} = \frac{p}{q} . \quad (11)$$

We then take the same notation as in the proof of Proposition 3.9: let  $N$  in  $\mathbb{N}$ ,  $u = \langle N \rangle_L$ , and  $\ell = |u|$ ; then  $\mathbf{v}_L(\ell - 1) \leq N < \mathbf{v}_L(\ell)$ . As in Corollary 3.7:

$$\text{scp}_L(N) = \sum_{i=0}^{\ell-1} \mathbf{v}_L(i) + \text{card}(\text{LB}_L(\text{Succ}_L(u))) . \quad (12)$$

From (11) and Lemma 2.7, it follows that  $\lim_{\ell \rightarrow \infty} \frac{\mathbf{v}_L(\ell+1)}{\mathbf{v}_L(\ell)} = \frac{p}{q}$  and then:

$$\lim_{\ell \rightarrow \infty} \frac{1}{\mathbf{v}_L(\ell-1)} \sum_{i=0}^{\ell-1} \mathbf{v}_L(i) = \frac{p}{p-q}$$

which can be written as:

$$\sum_{i=0}^{\ell-1} \mathbf{v}_L(i) = \mathbf{v}_L(\ell-1) \left( \frac{p}{p-q} + \varepsilon(\ell) \right) \quad \text{with } \lim_{\ell \rightarrow \infty} \varepsilon(\ell) = 0 . \quad (13)$$

Let  $v = \text{Succ}_L(u)$ . The evaluation of  $\text{card}(\text{LB}_L(v))$  goes as follows: the case where  $N = \mathbf{v}_L(\ell) - 1$  and  $|v| = \ell + 1$  (which corresponds to  $\text{scp}_L(N) = \sum_{i=0}^{\ell} \mathbf{v}_L(i)$ ) is excluded; we write  $N = \mathbf{v}_L(\ell-1) + (M-1)$  with  $1 \leq M < \mathbf{u}_L(\ell)$  and:

$$\text{card}(\text{LB}_L(v) \cap A^\ell) = M .$$

The second observation above implies then the evaluation at level  $\ell-1$ :

$$\frac{q}{p} M - q < q \left\lfloor \frac{M}{p} \right\rfloor \leq \text{card}(\text{LB}_L(v) \cap A^{\ell-1}) \leq q \left\lfloor \frac{M}{p} \right\rfloor + (q-1) < \frac{q}{p} M + q ,$$

at level  $\ell-2$ :

$$\left( \frac{q}{p} \right)^2 M - q \frac{q}{p} - q < \text{card}(\text{LB}_L(v) \cap A^{\ell-2}) < \left( \frac{q}{p} \right)^2 M + q \frac{q}{p} + q ,$$

and at level  $\ell-k$ :

$$\left( \frac{q}{p} \right)^k M - q \sum_{i=1}^k \left( \frac{q}{p} \right)^{k-i} < \text{card}(\text{LB}_L(v) \cap A^{\ell-k}) < \left( \frac{q}{p} \right)^k M + q \sum_{i=1}^k \left( \frac{q}{p} \right)^{k-i} .$$

Let us write  $B = \bigcup_{j=\ell_0}^{\ell} A^j$  and  $h = \ell - \ell_0$ . The summation of the above inequalities from  $k=0$  to  $k=h$  yields the following lower and upper bounds (after some simplifications):

$$\frac{p}{p-q} \left[ M \left( 1 - \left( \frac{q}{p} \right)^{h+1} \right) - qh \right] < \text{card}(\text{LB}_L(v) \cap B) < \frac{p}{p-q} [M + qh] .$$

Let  $Q = \sum_{i=0}^{\ell_0-1} \mathbf{v}_L(i)$ . We bound  $\text{card}(\text{LB}_L(v) \cap A^{<\ell_0})$  from below by 0 and from above by  $Q$  and we get then:

$$\frac{p}{p-q} \left[ M \left( 1 - \left( \frac{q}{p} \right)^{h+1} \right) - qh \right] < \text{card}(\text{LB}_L(v)) < \frac{p}{p-q} [M + qh] + Q .$$

As in the proof of Proposition 3.9, these inequalities together with (13) yields

$$\begin{aligned} (N+1) \frac{p}{p-q} + \mathbf{v}_p(\ell-1) \varepsilon(\ell) - M \frac{q}{p-q} \left( \frac{q}{p} \right)^h - qh \frac{p}{p-q} < \\ \text{scp}_p(N) < (N+1) \frac{p}{p-q} + \mathbf{v}_p(\ell-1) \varepsilon(\ell) + Q + qh \frac{p}{p-q} . \end{aligned}$$

If we divide by  $N$ , both the lower and upper bounds tend to  $\frac{p}{p-q}$  when  $N$  tends to infinity, hence  $\frac{1}{N} \text{scp}_p(N)$  has a limit, and this limit is  $\frac{p}{p-q}$ .  $\square$

## 4 The carry propagation of rational languages: an algebraic point of view

Even in the case of rational (PCE) languages, the existence of the local growth is not sufficient to insure the existence of the carry propagation, but we could say it is ‘almost’ sufficient. Recall that if  $L$  is a language of  $A^*$  and  $w$  a word of  $A^*$ , the *quotient* of  $L$  by  $w$  is the language  $w^{-1}L = \{v \in A^* \mid wv \in L\}$  and that a language is rational if and only if it has a finite number of distinct quotients (see for instance [32], [31] or any book on formal language theory). The aim of this section is the proof of the following result.

**Theorem 4.1.** *Let  $L$  be a rational PCE language with local growth rate  $\gamma_L$ . If the local growth rate of every quotient of  $L$  exists, then the carry propagation  $\text{CP}_L$  exists and is equal to  $\frac{\gamma_L}{\gamma_L - 1}$ .*

We prove indeed the existence of carry propagation for rational languages under somewhat more general hypotheses, the statement of which is more technical and requires some developments (Theorem 4.10). In any case, rationality *does not* imply the existence of the local growth rate, as seen with the example below.

**Example 4.2.** Let  $K_1 = (\{a\}\{a, b, c, d\})^*\{a, \varepsilon\}$  be the rational PCE language of  $\{a, b, c, d\}^*$  accepted by the automaton  $\mathcal{A}_1$  in Figure 8.

We have:  $\mathbf{u}_{K_1}(0) = 1$ ,  $\mathbf{u}_{K_1}(2\ell+1) = \mathbf{u}_{K_1}(2\ell)$  and  $\mathbf{u}_{K_1}(2\ell+2) = 4 \mathbf{u}_{K_1}(2\ell+1)$ , hence  $\gamma_{K_1}$  does not exist.

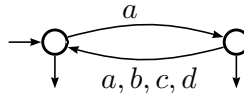


Figure 8: The minimal automaton  $\mathcal{A}_1$  of  $K_1 = (\{a\}\{a, b, c, d\})^*\{a, \varepsilon\}$ .

The proof of Theorem 4.1 and of other results of the same kind goes in two main steps. We first prove with Theorem 4.9 in Sec. 4.2 that the local growth rate of a rational language exists if and only if the language has an *almost dominating eigenvalue*, as defined in Sec. 4.1. In Sec. 4.3, we prove that if  $L$  has an almost dominating eigenvalue, then the carry propagation of  $L$  exists under some additional hypotheses on the eigenvalues of the quotients of  $L$  (Theorem 4.10). Theorem 4.1 is just a corollary of Theorem 4.10.

In Sec. 5.4 we will see that the hypothesis of Theorem 4.1 are fulfilled in the case of the so-called Parry beta-numeration (Corollary 5.39).

### 4.1 Generating functions and dominating eigenvalues

Let  $L$  be a language of  $A^*$ . The *generating function* of  $L$ ,  $\mathbf{g}_L(z)$ , is the (formal power) series in one indeterminate whose  $\ell$ -th coefficient is the number of words



of  $L$  of length  $\ell$ , that is, with our notation:

$$\mathbf{g}_L(z) = \sum_{\ell=0}^{\infty} \mathbf{u}_L(\ell) z^\ell .$$

Let  $L$  be a rational language of  $A^*$  and  $\mathcal{A} = \langle A, Q, I, E, T \rangle$  a deterministic automaton of ‘dimension’  $Q$  that accepts  $L$ :  $L = L(\mathcal{A})$ . We identify  $I$  and  $T$ , subsets of  $Q$ , with their characteristic functions in  $\mathbb{N}$ , and we write them as vectors of dimension  $Q$ , respectively row- and column-vectors:

$$\forall p \in Q \quad I_p = \begin{cases} 1, & \text{if } p \text{ is initial;} \\ 0, & \text{otherwise;} \end{cases} \quad T_p = \begin{cases} 1, & \text{if } p \text{ is final;} \\ 0, & \text{otherwise.} \end{cases}$$

The *adjacency matrix*  $M_{\mathcal{A}}$  of  $\mathcal{A}$  is the  $Q \times Q$ -matrix the  $(p, q)$ -entry of which is the *number* of transitions in  $\mathcal{A}$  that go from state  $p$  to state  $q$  (that is, the entries of  $M_{\mathcal{A}}$  are in  $\mathbb{N}$ ):

$$\forall p, q \in Q \quad (M_{\mathcal{A}})_{p,q} = \text{card}(\{a \in A \mid (p, a, q) \in E\}) .$$

Since  $\mathcal{A}$  is deterministic (the hypothesis ‘unambiguous’ would indeed be sufficient), the adjacency matrix allows the computation of  $\mathbf{u}_L(\ell)$ , the number of words of  $L$  of length  $\ell$ , as:

$$\forall \ell \in \mathbb{N} \quad \mathbf{u}_L(\ell) = I \cdot (M_{\mathcal{A}})^\ell \cdot T .$$

That is,  $\mathbf{g}_L(z)$  is an  $\mathbb{N}$ -rational series since the above equation precisely states that it is realized by the representation  $\langle I, \mu, T \rangle$ , with  $\mu(z) = M_{\mathcal{A}}$ . The  $\mathbb{N}$ -rationality of  $\mathbf{g}_L(z)$  implies a number of properties which eventually allow us to establish Theorem 4.10 and then Theorem 4.1.

The semiring  $\mathbb{N}$  is embedded in the *field*  $\mathbb{Q}$  (and, further on, in the *algebraically closed field*  $\mathbb{C}$ ) and in the remaining of the subsection, we essentially derive an expression of the coefficients  $\mathbf{u}_L(\ell)$  from the fact that  $\mathbf{g}_L(z)$  is a  $\mathbb{Q}$ -rational series (or even a  $\mathbb{C}$ -rational series). The very special properties of rational series with non-negative coefficients come into play in the next subsection. We rely on the treatise [6] of Berstel–Reutenauer (Sec. 6.1, 6.2, 8.1, and 8.3) for this exposition.

The Cayley–Hamilton Theorem implies that the sequence  $(\mathbf{u}_L(\ell))_{\ell \in \mathbb{N}}$  satisfies the *linear recurrence relation* defined by the *characteristic polynomial*  $\mathbf{P}_{\mathcal{A}}$  of  $M_{\mathcal{A}}$ , the zeroes of which are the *eigenvalues* of  $M_{\mathcal{A}}$ . The sequence  $(\mathbf{u}_L(\ell))_{\ell \in \mathbb{N}}$  satisfies indeed a *shortest* linear recurrence relation associated with a polynomial  $\mathbf{P}_L$ , the *minimal polynomial* of  $\mathbf{g}_L(z)$ , which is a divisor of  $\mathbf{P}_{\mathcal{A}}$ . The zeroes of  $\mathbf{P}_L$  are called the *eigenvalues* of  $\mathbf{g}_L(z)$  and of  $L$ . The *multiplicities* of these eigenvalues are those of these zeroes.

**Definition 4.3.** *We call the maximum of the moduli of the eigenvalues of a rational language  $L$  the modulus of  $L$ . It is the multiplicative inverse of the radius of convergence of the series  $\mathbf{g}_L(z)$ .*

A rational language  $L$  is said to have a dominating eigenvalue, or, for short, to be DEV, if there is, among the eigenvalues of  $L$ , a unique eigenvalue of maximal modulus, which is called the dominating eigenvalue of  $L$ .

With the next two examples, we stress the difference between the eigenvalues of the adjacency matrix of an automaton  $\mathcal{A}$  that recognizes  $L$  and the eigenvalues of  $L$ .

**Example 4.4** (Example 4.2 continued). The adjacency matrix of  $\mathcal{A}_1$  shown in Figure 8 is  $M_{\mathcal{A}_1} = \begin{pmatrix} 0 & 1 \\ 4 & 0 \end{pmatrix}$ , its characteristic polynomial is  $P_{\mathcal{A}_1} = X^2 - 4$ , the zeroes of which are 2 and  $-2$ . This polynomial is also the minimal polynomial of the linear recurrence satisfied by the coefficients of  $\mathbf{g}_{K_1}(z)$ :

$$\mathbf{u}_{K_1}(0) = 1, \quad \mathbf{u}_{K_1}(1) = 1, \quad \mathbf{u}_{K_1}(\ell + 2) = 4 \mathbf{u}_{K_1}(\ell),$$

hence  $\forall \ell \geq 0 \quad \mathbf{u}_{K_1}(\ell) = \frac{3}{4} 2^\ell + \frac{1}{4} (-2)^\ell,$

and  $K_1$  is thus not DEV.

**Example 4.5.** The adjacency matrix of the automaton  $\mathcal{A}_2$  in Figure 9 is  $M_{\mathcal{A}_2} = \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}$ , its characteristic polynomial is  $P_{\mathcal{A}_2} = X^2 - 4$  as above. But in this case, the *minimal polynomial of the linear recurrence* satisfied by the coefficients of  $\mathbf{g}_{K_2}(z)$ ,  $\mathbf{u}_{K_2}(\ell) = 2^\ell$ , is  $P_{K_2} = X - 2$ , with 2 as a unique zero and  $K_2$  is DEV.

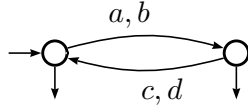


Figure 9: The minimal automaton  $\mathcal{A}_2$  of  $K_2 = (\{a, b\}\{c, d\})^*\{a, b, \varepsilon\}$ .

As stated in [6], the rational function  $\mathbf{g}_L(z)$  may be written, in a unique way, as:

$$\mathbf{g}_L(z) = T(z) + \frac{R(z)}{S(z)}$$

where  $T(z)$ ,  $R(z)$  and  $S(z)$  are polynomials in  $\mathbb{Q}[z]$ ,  $\deg R < \deg S$  and  $S(0) \neq 0$ . It can be shown that  $P_L$  is the *reciprocal polynomial* of  $S$ :  $P_L(z) = S(\frac{1}{z}) z^{\deg S}$ . It follows that if  $\lambda_1, \lambda_2, \dots, \lambda_t$  are the zeroes of  $P_L$ , the coefficients  $\mathbf{u}_L(\ell)$  of  $\mathbf{g}_L(z)$  can be written as:

$$\forall \ell \in \mathbb{N} \quad \mathbf{u}_L(\ell) = \sum_{j=1}^t \lambda_j^\ell P_j(\ell), \quad (14)$$

where every  $P_j$  is a polynomial (which depends on  $L$  even though it does not appear in the writing) *whose degree is equal to the multiplicity of the zero  $\lambda_j$  in  $P_L$  minus 1*, and is determined by the first values of the sequence  $(\mathbf{u}_L(\ell))_{\ell \in \mathbb{N}}$ .

## 4.2 From local growth rate to dominating eigenvalue

The properties of rational series with positive coefficients allow us to characterize the generating functions of rational languages with local growth rate. Let us first recall the theorem due to Berstel on such series.

**Theorem 4.6** (Theorem 8.1.1 and Lemma 8.1.2 in [6]).

Let  $f(z)$  be an  $\mathbb{R}_+$ -rational function which is not a polynomial and  $\lambda$  the maximum of the moduli of its eigenvalues. Then:

- (a)  $\lambda$  is an eigenvalue of  $f(z)$  (hence an eigenvalue in  $\mathbb{R}_+$ ).
- (b) Every eigenvalue of  $f(z)$  of modulus  $\lambda$  is of the form  $\lambda e^{i\theta}$  where  $e^{i\theta}$  is a root of unity.
- (c) The multiplicity of any eigenvalue of modulus  $\lambda$  is at most that of  $\lambda$ .

We express the consequences of this result (and of Equation (14)) in the following way. Let  $L$  be a rational language and  $\mathbf{g}_L(z)$  its generating function, an  $\mathbb{R}_+$ -rational function. Let  $\lambda = \lambda_1, \lambda_2, \dots, \lambda_k$  be the eigenvalues of maximal modulus  $\lambda$  of  $\mathbf{g}_L(z)$  and  $d$  the degree of the polynomial  $P_1$  in (14). For  $j = 2, \dots, k$ , we write  $\lambda_j = \lambda e^{i\theta_j}$ ;  $e^{i\theta_j}$  is a root of unity, hence  $\theta_j = 2\pi/h_j$  where  $h_j$  is an integer and let  $r$  be the least common multiple of all the  $h_j$ .

There exist  $k$  (possibly complex) numbers  $\delta_1, \delta_2, \dots, \delta_k$ , with  $\delta_1$  in  $\mathbb{R}$  and different from 0, such that (14) can be given the following asymptotic form:

$$\forall \ell \text{ large enough} \quad \mathbf{u}_L(\ell) = \lambda^\ell \ell^d \left( \delta_1 + \sum_{j=2}^k \delta_j e^{i\ell\theta_j} \right) + o(\lambda^\ell \ell^d) . \quad (15)$$

(It is understood that  $\delta_j$  is not zero if the polynomial  $P_j$  in (14) is of degree  $d$ , it is equal to 0 if this polynomial is of degree less than  $d$  — and by Theorem 4.6 (c) no such polynomial has degree greater than  $d$ .)

One can say that the description of  $\mathbf{u}_L(\ell)$  given in (14) is *ordered by eigenvalues* whereas the description in (15) is *ordered by moduli* of eigenvalues. Since for every  $j = 2, \dots, k$  and every  $p$  in  $\mathbb{N}$  we have  $e^{i p r \theta_j} = 1$ , it follows that

$$\lim_{p \rightarrow \infty} \frac{\mathbf{u}_L(p r)}{\lambda^{p r} (p r)^d} = \sum_{j=1}^k \delta_j .$$

**Definition 4.7.** Let  $f(z)$  be an  $\mathbb{R}_+$ -rational function which is not a polynomial and  $\lambda$  the maximum of the moduli of its eigenvalues. We say that  $f(z)$  has an almost dominating eigenvalue, or is ADEV, if the multiplicity of any non-real eigenvalue of modulus  $\lambda$  is strictly less than that of the eigenvalue  $\lambda$ .

Accordingly, we say that a rational language  $L$  is ADEV if  $\mathbf{g}_L(z)$  is ADEV. Using the above notation,  $L$  is ADEV if and only if all the  $\delta_j$ ,  $j = 2, \dots, k$ , but  $\delta_1$  in (15) are equal to 0, that is, if and only if (15) takes the following form:

$$\forall \ell \text{ large enough} \quad \mathbf{u}_L(\ell) = \lambda^\ell \ell^d \delta_1 + o(\lambda^\ell \ell^d) . \quad (16)$$

**Example 4.8.** The rational PCE language  $K_3$  accepted by the automaton  $\mathcal{A}_3$  shown in Figure 10 is ADEV without being DEV. The zeroes of the characteristic polynomial of  $M_{\mathcal{A}_3}$  are 2 with multiplicity 2 and  $-2$  (with multiplicity 1). The zeroes of  $\mathbb{P}_{K_3} = (X^2 - 4)(2 - X)$  are the same as we have

$$\forall \ell \in \mathbb{N} \quad \mathbf{u}_L(\ell) = \left(\frac{1}{4}\ell + \frac{7}{8}\right) 2^\ell + \frac{1}{8}(-2)^\ell . \quad (17)$$

On the other hand, the language  $K_1$  from Example 4.2, which is not DEV, is not ADEV either.

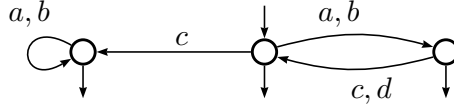


Figure 10: The minimal automaton  $\mathcal{A}_3$  of  $K_3 = (\{a, b\}\{c, d\})^*\{a, b, \varepsilon\} \cup c\{a, b\}^*$ .

**Theorem 4.9.** A rational language  $L$  is ADEV if and only if the local growth rate  $\gamma_L$  exists. In this case, the modulus of  $L$  is equal to  $\gamma_L$ .

*Proof.* If  $L$  is ADEV, the asymptotic expression (16) shows that the condition is sufficient since

$$\frac{\mathbf{u}_L(\ell + 1)}{\mathbf{u}_L(\ell)} = \lambda \left(\frac{\ell + 1}{\ell}\right)^d (1 + o(1))$$

implies that

$$\lim_{\ell \rightarrow \infty} \frac{\mathbf{u}_L(\ell + 1)}{\mathbf{u}_L(\ell)} = \lambda , \quad (18)$$

which states both that  $\gamma_L$  exists and is equal to  $\lambda$ .

Conversely, let us suppose that the limit of  $\frac{\mathbf{u}_L(\ell + 1)}{\mathbf{u}_L(\ell)}$  exists and is equal to  $\gamma_L$  when  $\ell$  tends to infinity. For the ease of writing, and in view of the use of (15), let us set:

$$w(\ell) = \delta_1 + \sum_{j=2}^k \delta_j e^{i\ell\theta_j} .$$

The function  $w(\ell)$  is periodic of period  $r$ , and for every integer  $s$ ,  $0 \leq s < r$ , the hypothesis, and (15), imply

$$\begin{aligned} \lim_{p \rightarrow \infty} \frac{\mathbf{u}_L(pr + s + 1)}{\mathbf{u}_L(pr + s)} &= \\ &= \lim_{p \rightarrow \infty} \left( \lambda \left(\frac{pr + s + 1}{pr + s}\right)^d \frac{w(s + 1)}{w(s)} (1 + o(1)) \right) = \lambda \frac{w(s + 1)}{w(s)} = \gamma_L . \end{aligned}$$

Hence, there exists an  $x$  in  $\mathbb{R}_+$  such that

$$\forall s \in \mathbb{N}, 0 \leq s < r \quad \frac{w(s + 1)}{w(s)} = x .$$

Moreover, since  $w(0) = w(r)$  and

$$\frac{w(0)}{w(0)} = \frac{w(1)}{w(0)} \frac{w(2)}{w(1)} \cdots \frac{w(0)}{w(r-1)} = x^r = 1 \quad ,$$

it follows that  $x = 1$ ,  $\lambda = \gamma_L$  and

$$\forall s \in \mathbb{N}, 0 \leq s < r \quad w(s) = w(0) = \delta_1 = \delta_1 + \sum_{j=2}^k \delta_j e^{is\theta_j} \quad .$$

We conclude that the vector  $(0 \ \delta_2 \ \cdots \ \delta_k)$  is a solution of the Vandermonde linear system (for the sake of completeness, we set  $\theta_1 = 0$ ):

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ e^{i\theta_1} & e^{i\theta_2} & \cdots & e^{i\theta_k} \\ e^{i2\theta_1} & e^{i2\theta_2} & \cdots & e^{i2\theta_k} \\ \vdots & \vdots & & \vdots \\ e^{i(k-1)\theta_1} & e^{i(k-1)\theta_2} & \cdots & e^{i(k-1)\theta_k} \end{pmatrix} \begin{pmatrix} \zeta_1 \\ \zeta_2 \\ \vdots \\ \zeta_k \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad (19)$$

hence identically zero: all  $\delta_j$ ,  $j = 2, \dots, k$ , are equal to 0 and  $L$  is ADEV.  $\square$

### 4.3 From dominating eigenvalue to the carry propagation

With the notions of modulus and of dominating eigenvalue of a rational language, we can now state a result that is more general and of which Theorem 4.1 is an obvious corollary.

**Theorem 4.10.** *Let  $L$  be an ADEV rational PCE language and  $\lambda$  its modulus. If every quotient of  $L$  whose modulus is equal to  $\lambda$  is ADEV, then  $L$  has a carry propagation and  $\text{CP}_L = \frac{\lambda}{\lambda - 1}$ .*

Indeed, previous results show that if a rational PCE language  $L$  is ADEV and of modulus  $\lambda$ , then  $\gamma_L$  exists and  $\gamma_L = \lambda$  and if the carry propagation  $\text{CP}_L$  exists, then  $\text{CP}_L = \frac{\lambda}{\lambda - 1}$ . The hypothesis on the quotients of  $L$  is necessary as shown by the following example.

**Example 4.11.** Let  $K_4$  be the language accepted by the automaton  $\mathcal{A}_4$  shown in Figure 11. It has first the property of being a DEV (and not only an ADEV) language, of modulus 2.

On the other hand,  $K_4 = \varepsilon \cup aK_1 \cup bK_1 \cup cK'_1$  where  $K_1$  is the language of Example 4.2 and  $K'_1$  the one accepted by the automaton  $\mathcal{A}'_1$  obtained from the automaton  $\mathcal{A}_1$  of Figure 8 by changing the initial state. The language  $K_1$  is a quotient of  $K_4$ :  $K_1 = a^{-1}K_4$ ; it has modulus 2 and *is not* ADEV.

We have seen that  $\mathbf{u}_{K_1}(\ell) = \frac{3}{4}2^\ell + \frac{1}{4}(-2)^\ell$ ; similarly  $\mathbf{u}_{K'_1}(\ell) = \frac{3}{2}2^\ell - \frac{1}{2}(-2)^\ell$ . Hence  $\mathbf{u}_{K_4}(0) = 1$  and  $\mathbf{u}_{K_4}(\ell + 1) = 2\mathbf{u}_{K_1}(\ell) + \mathbf{u}_{K'_1}(\ell) = 3 \cdot 2^\ell$ . From which one deduces  $\mathbf{v}_{K_4}(0) = 1$  and  $\mathbf{v}_{K_4}(\ell + 1) = 3 \cdot 2^{\ell+1} - 2$  and

$$\mathbf{w}_{K_4}(\ell + 1) = 1 + \sum_{j=0}^{\ell} \mathbf{v}_{K_4}(j + 1) = 3 \cdot 2^{\ell+2} - 2\ell - 7 .$$

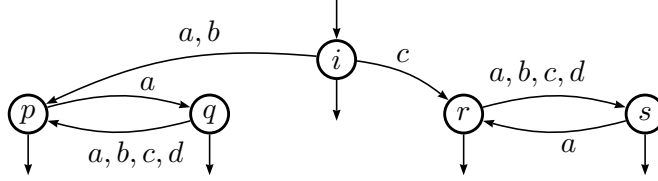


Figure 11: The automaton  $\mathcal{A}_4$

We show that  $\text{CP}_{K_4}$  does not exist with the same argument as the one developed in Example 3.17. We choose a sequence of words  $u_\ell$  and then a sequence of numbers  $N(\ell) = \pi_{K_4}(u_\ell)$  and show that the ratio  $\text{scp}_{K_4}(N(\ell))/N(\ell)$  does not have 2 as limit (and even that it has no limit).

We choose the words in  $b \text{Maxlg}(b^{-1}K_4) = \text{Maxlg}(bK_1)$ . It follows that

$$\begin{aligned} N(\ell + 2) &= \mathbf{v}_{K_4}(\ell + 1) + 2\mathbf{u}_{K_4}(\ell + 1) \quad \text{and} \\ \text{scp}_{K_4}(N(\ell + 2)) &= \mathbf{w}_{K_4}(\ell + 1) + \text{card}\left(\text{LB}_{K_4}\left(\text{Succ}_{K_4}\left(\langle N(\ell + 2) \rangle_{K_4}\right)\right)\right) \\ &= \mathbf{w}_{K_4}(\ell + 1) + 2\mathbf{v}_{K_4}(\ell + 1) . \end{aligned}$$

We then have:

$$\begin{aligned} N(2k + 2) &= 2 \cdot 2^{2k+2} - 2 \quad \text{and} \quad N(2k + 3) = \frac{5}{2}2^{2k+3} - 2 , \\ \text{scp}_{K_4}(N(2k + 2)) &\sim \frac{13}{3}2^{2k+2} \quad \text{and} \quad \text{scp}_{K_4}(N(2k + 3)) \sim \frac{14}{3}2^{2k+3} , \\ \text{hence} \quad \lim_{\ell \rightarrow +\infty} \frac{\text{scp}_L(N(2\ell))}{N(2\ell)} &= \frac{13}{6} \quad \text{and} \quad \lim_{\ell \rightarrow +\infty} \frac{\text{scp}_L(N(2\ell + 1))}{N(2\ell + 1)} = \frac{28}{15} , \end{aligned}$$

which complete the proof of the non-existence of  $\text{CP}_{K_4}$ .

The proof of Theorem 4.10 requires a new description of the ‘left bank’ of a word (recall the definition p.12), a description for which we introduce some notation. In order to keep these new symbols readable, we simplify some of those already in use.

For the remaining of the section, the ADEV rational PCE language  $L$  is fixed and kept implicit in most cases: the number of words of  $L$  of length  $\ell$  (resp. of length less than or equal to  $\ell$ ) is now denoted by  $\mathbf{u}(\ell)$  (resp. by  $\mathbf{v}(\ell)$ ) and the minimal polynomial of  $L$  is now denoted by  $\mathbf{P}$ .

Let  $\mathcal{A} = \langle A, Q, q_0, \delta, T \rangle$  be a deterministic finite automaton that accepts  $L$  (and which is also kept implicit in what follows). For every  $q$  in  $Q$  and  $w$  in  $A^*$ , we write  $q \cdot w$  for the state reached by the computation of  $\mathcal{A}$  starting in  $q$  and

labeled with  $w$ . For every state  $q$  in  $Q$ , we denote by  $L_q$  the language accepted by the automaton  $\mathcal{A}_q = \langle A, Q, q, \delta, T \rangle$ , that is,  $L_q = \{w \in A^* \mid q \cdot w \in T\}$  and, for every  $\ell$  in  $\mathbb{N}$ , by  $\mathbf{u}_q(\ell)$  the number of words of  $L_q$  of length  $\ell$  and by  $\mathbf{v}_q(\ell)$  the number of words of  $L_q$  of length less than or equal to  $\ell$  (in particular,  $\mathbf{u}(\ell) = \mathbf{u}_{q_0}(\ell)$  and  $\mathbf{v}(\ell) = \mathbf{v}_{q_0}(\ell)$ ).<sup>8</sup>

For every  $q$  in  $Q$ , there exists a word  $w_q$  of length  $\ell_q$  such that  $q_0 \cdot w_q = q$  and then  $L_q = w_q^{-1}L$ :  $L_q$  is a *quotient* of  $L$ . It then follows

$$\forall q \in Q, \forall \ell \in \mathbb{N}, \ell \geq \ell_q \quad \mathbf{u}(\ell + \ell_q) \geq \mathbf{u}_q(\ell) . \quad (20)$$

If  $w = a_1 a_2 \cdots a_{\ell+1}$  is a word of  $A^*$ , we denote by  $w_{[j]}$  the *prefix of length  $j$*  of  $w$ :  $w_{[j]} = a_1 a_2 \cdots a_j$ ;  $w_{[0]} = \varepsilon$  and  $w_{[\ell+1]} = w$ . (The formulas to come are simpler if the length of  $w$  is written as  $\ell + 1$  rather than  $\ell$ .) Suppose  $w$  is in  $L$ . The left bank of  $w$ ,  $\text{LB}_L(w)$ , is, by definition, for each length  $j$ ,  $1 \leq j \leq \ell + 1$ , the set of words of  $L$  of length  $j$  that are less than  $w_{[j]}$  in the lexicographic order. This is a description by *horizontal layers*. The same set can be given a decomposition by *subtrees* of  $\mathcal{T}_L$ . For every  $j$ ,  $0 \leq j \leq \ell$ , the prefix of  $w$  of length  $j + 1$  is  $w_{[j+1]} = w_{[j]} a_{j+1}$ . Then, for every  $j$ ,  $0 \leq j \leq \ell$  and for every  $a$ ,  $a < a_{j+1}$ ,  $\text{LB}_L(w)$  contains all words of  $L_{q_0 \cdot w_{[j]} a}$  of length less than, or equal to,  $\ell - j$  concatenated on the left with  $w_{[j]} a$ . Moreover, these subsets form a *partition* of  $\text{LB}_L(w)$ :

$$\text{LB}_L(w) = \bigcup_{j=0}^{\ell} \left[ \bigcup_{a < a_{j+1}} w_{[j]} a \left( L_{q_0 \cdot w_{[j]} a} \cap A^{\leq \ell - j} \right) \right] , \quad (21)$$

where the unions are pairwise disjoint and can then be used for counting the elements of  $\text{LB}_L(w)$ .

*Proof of Theorem 4.10.* Let  $\lambda$  be the modulus of  $L$ . Let  $N$  be an integer and  $\langle N \rangle_L = w = a_1 a_2 \cdots a_{\ell+1}$  its  $L$ -representation (see Sec. 2.2). By definition,  $N$  is equal to the number of words of  $L$  that are less than  $w$  in the radix order, that is, in the line<sup>9</sup> of the decomposition (21):

$$N = \mathbf{v}(\ell) + \sum_{j=0}^{\ell} \left[ \sum_{a < a_{j+1}} \mathbf{u}_{q_0 \cdot w_{[j]} a}(\ell - j) \right] . \quad (22)$$

On the other hand, Corollary 3.7 and (21) yield the following expression for the sum of the carry propagations at the first  $N$  words of  $L$ :

$$\text{scp}_L(N) = \sum_{j=0}^{\ell} \mathbf{v}(j) + \sum_{j=0}^{\ell} \left[ \sum_{a < a_{j+1}} \mathbf{v}_{q_0 \cdot w_{[j]} a}(\ell - j) \right] . \quad (23)$$

<sup>8</sup>These definitions hide some technicalities: for  $q \cdot w$  to be defined for all  $q$  and  $w$ ,  $\mathcal{A}$  needs to be not necessarily trim but possibly endowed with a sink state  $s$ ; then  $L_s$  will be empty and  $\mathbf{u}_s(\ell)$  equal to 0 for every  $\ell$ .

<sup>9</sup>This is a reformulation of Lemma 3 in [21].

By Proposition 3.15 and Theorem 4.9, if the carry propagation

$$\text{CP}_L = \lim_{N \rightarrow \infty} \frac{1}{N} \text{scp}_L(N)$$

of  $L$  exists, it must be equal to  $\frac{\lambda}{\lambda-1}$ . We thus evaluate

$$\lim_{N \rightarrow \infty} \left( \frac{1}{N} \text{scp}_L(N) - \frac{\lambda}{\lambda-1} \right)$$

and show it exists and is equal to 0, using both (22) and (23). We write:

$$\begin{aligned} \frac{1}{N} \left( \text{scp}_L(N) - \frac{\lambda}{\lambda-1} N \right) &= \frac{1}{N} \left( \sum_{j=0}^{\ell} \mathbf{v}(j) - \frac{\lambda}{\lambda-1} \mathbf{v}(\ell) \right) \\ &\quad + \frac{1}{N} \left( \sum_{j=0}^{\ell} \left( \sum_{a < a_{j+1}} \left( \mathbf{v}_{q_0 \cdot w_{[j]a}(\ell-j)} - \frac{\lambda}{\lambda-1} \mathbf{u}_{q_0 \cdot w_{[j]a}(\ell-j)} \right) \right) \right) . \end{aligned}$$

The two parts of the right-hand side of the equation are evaluated separately. We first note that  $\ell$  tends to infinity with  $N$  and recall that, by (18),

$$\lim_{\ell \rightarrow \infty} \frac{\mathbf{u}(\ell+1)}{\mathbf{u}(\ell)} = \lambda .$$

Since  $N \geq \mathbf{v}(\ell)$ , we have:

$$\frac{1}{N} \left| \sum_{j=0}^{\ell} \mathbf{v}(j) - \frac{\lambda}{\lambda-1} \mathbf{v}(\ell) \right| \leq \left| \frac{1}{\mathbf{v}(\ell)} \left( \sum_{j=0}^{\ell} \mathbf{v}(j) \right) - \frac{\lambda}{\lambda-1} \right|$$

which, by Lemma 2.7, tends to 0 when  $\ell$  tends to infinity.

The second term requires some more work. For the ease of writing, let us set, for every  $q$  in  $Q$  and every  $\ell$  in  $\mathbb{N}$ ,

$$\mathbf{z}_q(\ell) = \left( \mathbf{v}_q(\ell) - \frac{\lambda}{\lambda-1} \mathbf{u}_q(\ell) \right) .$$

The term we have to evaluate reads then

$$\frac{1}{N} \left| \sum_{j=0}^{\ell} \left( \sum_{a < a_{j+1}} \left( \mathbf{z}_{q_0 \cdot w_{[j]a}(\ell-j)} \right) \right) \right| \quad (24)$$

and is (loosely) bounded by

$$(\text{card}(A) - 1) \frac{1}{\mathbf{v}(\ell)} \sum_{j=0}^{\ell} \left( \sum_{q \in Q} |\mathbf{z}_q(j)| \right) . \quad (25)$$



Indeed, the range of every inner sum in (24) is a subset of the alphabet  $A$  made of letters less than a given one, hence every such sum contains at most  $(\text{card}(A) - 1)$  terms. Moreover, we have replaced every term

$$\mathbf{z}_{q_0 \cdot w_{[j]a}}(\ell - j) \quad \text{by the sum} \quad \sum_{q \in Q} |\mathbf{z}_q(\ell - j)| \ .$$

This is of course a loose upper bound but it allows us to get rid of the problem of taking the limit of quantities that are different when  $N$  tends to infinity. Finally, we permute the two summations in (25) and it remains to show that, for every state  $q$  in  $Q$ ,

$$\lim_{\ell \rightarrow \infty} \frac{1}{\mathbf{v}(\ell)} \left( \sum_{j=0}^{\ell} |\mathbf{z}_q(j)| \right) = 0 \ , \quad (26)$$

and we need to go more into details for that purpose.

For every  $q$  in  $Q$ ,  $L_q$  is accepted by  $\mathcal{A}_q$ , the accessible part of which is a subautomaton of  $\mathcal{A}$ . Hence, the sequence  $(\mathbf{u}_q(\ell))_{\ell \in \mathbb{N}}$  satisfies a linear recurrence relation whose minimal polynomial  $P_q$  is, as is  $P$ , a factor of  $P_{\mathcal{A}}$ . However, the zeroes of  $P_q$  are not necessarily a subset of those of  $P$  and we base the comparison between  $(\mathbf{u}_q(\ell))_{\ell \in \mathbb{N}}$  and  $(\mathbf{u}(\ell))_{\ell \in \mathbb{N}}$  on the asymptotic behaviour.

The series  $\mathbf{g}_q(z) = \sum_{\ell=0}^{\infty} \mathbf{u}_q(\ell) z^{\ell}$  is an  $\mathbb{N}$ -rational series and, for the same reasons as above, it has a real eigenvalue of maximal modulus  $\mu_q$  and of multiplicity  $d_q + 1$ , and one can write:

$$\forall \ell \text{ large enough} \quad \mathbf{u}_q(\ell) = \mu_q^{\ell} \ell^{d_q} \left( \delta_{q,1} + \sum_{j=2}^k \delta_{q,j} e^{i\ell\theta_{q,j}} \right) + o(\mu_q^{\ell} \ell^{d_q}) \ , \quad (27)$$

where  $d_q$ , the  $\delta_{q,j}$ 's and the  $\theta_{q,j}$ 's play the same role as  $d$ , the  $\delta_j$ 's and the  $\theta_j$ 's play in Equation (15).

There are two cases: either  $\mu_q$  is less than  $\lambda$ , or  $\mu_q$  is equal to  $\lambda$ . It cannot be larger than  $\lambda$  for otherwise  $\mathbf{u}_q(\ell)$  would not be bounded by  $\mathbf{u}(\ell)$  (Equation (20)). In the first case, the quantity  $|\mathbf{z}_q(j)| = \left| \mathbf{v}_q(j) - \frac{\lambda}{\lambda - 1} \mathbf{u}_q(j) \right|$  is of the order of  $\mu_q^{\ell}$ , in the second case, of the order of  $o(\lambda^{\ell} \ell^d)$ , hence, in both cases, (26) holds. More precisely, the computations go as follows. The reader will see that the hypothesis on the quotient plays its role in the second case only.

Case 1:  $\mu_q < \lambda$ . The case  $\mu_q = 1$  corresponds to sequences  $\mathbf{u}_q(\ell)$  and thus  $\mathbf{v}_q(\ell)$  having a polynomial growth. In which case, (26) directly holds. In the following, we assume that  $\mu_q > 1$ .

The quantity  $w_q(\ell) = \delta_{q,1} + \sum_{j=2}^k \delta_{q,j} e^{i\ell\theta_{q,j}}$  is periodic (with some period  $h_q$ ) and, *since the sequence  $(\mathbf{u}_q(\ell))_{\ell \in \mathbb{N}}$  is monotonically increasing*, there exist bounds  $\alpha_q$  and  $\beta_q$ ,  $0 < \alpha_q \leq \beta_q$ , such that

$$\forall \ell \in \mathbb{N} \quad \alpha_q \leq w_q(\ell) \leq \beta_q \ .$$

It follows that

$$\forall \ell \in \mathbb{N} \quad \mu_q^\ell \ell^{d_q} \alpha_q + o(\mu_q^\ell \ell^{d_q}) \leq \mathbf{u}_q(\ell) \leq \mu_q^\ell \ell^{d_q} \beta_q + o(\mu_q^\ell \ell^{d_q}) \quad ,$$

and

$$\forall \ell \in \mathbb{N} \quad \frac{\mu_q}{\mu_q - 1} \mu_q^\ell \ell^{d_q} \alpha_q + o(\mu_q^\ell \ell^{d_q}) \leq \mathbf{v}_q(\ell) \leq \frac{\mu_q}{\mu_q - 1} \mu_q^\ell \ell^{d_q} \beta_q + o(\mu_q^\ell \ell^{d_q}) \quad ,$$

hence

$$\forall \ell \in \mathbb{N} \quad \mu_q^\ell \ell^{d_q} \alpha'_q + o(\mu_q^\ell \ell^{d_q}) \leq \left| \mathbf{v}_q(\ell) - \frac{\lambda}{\lambda - 1} \mathbf{u}_q(\ell) \right| \leq \mu_q^\ell \ell^{d_q} \beta'_q + o(\mu_q^\ell \ell^{d_q}) \quad ,$$

where

$$\alpha'_q = \frac{\mu_q}{\mu_q - 1} \left( \alpha_q - \frac{\lambda}{\lambda - 1} \beta_q \right) \quad \text{and} \quad \beta'_q = \frac{\mu_q}{\mu_q - 1} \left( \beta_q - \frac{\lambda}{\lambda - 1} \alpha_q \right) \quad .$$

It follows that the quantity

$$\sum_{j=0}^{\ell} \left| \mathbf{v}_q(j) - \frac{\lambda}{\lambda - 1} \mathbf{u}_q(j) \right|$$

is also of the order of  $\mu_q^\ell$  and since  $\mathbf{v}(\ell)$  is of the order of  $\lambda^\ell$ , (26) holds.

Case 2:  $\mu_q = \lambda$ . In this case, and since by hypothesis,  $L_q$  is ADEV, every  $\delta_{q,j} = 0$ ,  $2 \leq j \leq k$ , and it holds:

$$\forall \ell \text{ large enough} \quad \mathbf{u}_q(\ell) = \lambda^\ell \ell^{d_q} \delta_{q,1} + o(\lambda^\ell \ell^{d_q}) \quad .$$

It follows that  $\left| \mathbf{v}_q(\ell) - \frac{\lambda}{\lambda - 1} \mathbf{u}_q(\ell) \right|$  is a  $o(\lambda^\ell \ell^{d_q})$  with  $d_q \leq d$  and (26) holds again, which completes the proof.  $\square$

## 5 The carry propagation of a language: an ergodic point of view

The definition of the carry propagation of a language:

$$\text{CP}_L = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{i=0}^{N-1} \text{cp}_L(i) \quad , \quad (28)$$

especially if we write it as:

$$\text{CP}_L = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{i=0}^{N-1} \text{cp}_L(\text{Succ}_L^i(\varepsilon)) \quad ,$$

inevitably reminds one of the *Ergodic Theorem* (that we recall right below). In this section, we explain how to set the carry propagation problem in terms relevant to ergodic theory and we study under which conditions and to what extent the Ergodic Theorem allows us to conclude the existence of the carry propagation. We begin with a very brief account of ergodic theory; for more detailed definitions, see [27] for instance.

## 5.1 Birkhoff's Ergodic Theorem

A *dynamical system*  $(\mathcal{K}, \tau)$  is a compact set  $\mathcal{K}$ , equipped with a map  $\tau$  from  $\mathcal{K}$  into itself, called the *action* of the system. A probability measure  $\mu$  on  $\mathcal{K}$  is  $\tau$ -invariant if  $\tau$  is measurable and if  $\mu(\tau^{-1}(B)) = \mu(B)$  for every measurable set  $B$ . The dynamical system  $(\mathcal{K}, \tau)$  is said to be *ergodic* if  $\tau^{-1}(B) = B$  implies  $\mu(B) = 0$  or 1, for every  $\tau$ -invariant measure  $\mu$ . It is *uniquely ergodic* if it admits a unique  $\tau$ -invariant measure (if there exists only one  $\tau$ -invariant measure, then it is ergodic). The Ergodic Theorem then reads.

**Theorem 5.1.** *Let  $(\mathcal{K}, \tau)$  be a dynamical system,  $\mu$  a  $\tau$ -invariant measure on  $\mathcal{K}$  and  $f: \mathcal{K} \rightarrow \mathbb{R}$  a function<sup>10</sup> in  $L^1(\mu)$ . If  $(\mathcal{K}, \tau)$  is ergodic then, for  $\mu$ -almost all  $s$  in  $\mathcal{K}$ ,*

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{i=0}^{N-1} f(\tau^i(s)) = \int_{\mathcal{K}_G} f d\mu . \quad (29)$$

*Moreover, if  $(\mathcal{K}, \tau)$  is uniquely ergodic and if  $f$  and  $\tau$  are continuous, then (29) holds for all  $s$  in  $\mathcal{K}$ .*

This theorem states indeed two results: it says first that the limit of the left hand-side of (29) *exists*, and, second, it gives the value of this limit. What is really of interest for us is *the existence of the limit* since, in most cases, if we know that  $\text{CP}_L$  exists, we already have other means to compute it.

We have thus to explain how to turn the language  $L$  into a compact set, and how to transform the successor function into a map of this compact set into itself. The hypotheses of the classic formulation of the Ergodic Theorem are rather restrictive for our case of study. We shall rely on more recent and technical works [3] which significantly widen the scope of this theorem.

## 5.2 Turning a numeration system into a dynamical system

Let  $L \subseteq A^*$  be a numeration system, that is, once again, the set of representations of the natural integers. The purpose is the embedding of  $L$  into a compact set, and extending the successor function into an action on that set. Since we use the *radix order* on words in order to map  $L$  onto the set of integers or, which amounts to the same thing, since we use the *most significant digit first* (MSDF) convention for the representation of integers (assuming a left-to-right reading), we build the compact set by considering *left* infinite words.

Note that the authors from whom we borrow the results rather use the *least significant digit first* (LSDF) representation of integers, and *right* infinite words to build the same compact set ([19, 3]). Going from one convention to the other is routine and requires just suppleness of mind (or a mirror).

---

<sup>10</sup>That is,  $f$  is absolutely (Lebesgue)  $\mu$ -integrable.

### 5.2.1 Compactification of the numeration system

The set of left infinite words over  $A$  is denoted by  ${}^\omega A$ . As we did for the words of  $A^*$ , the left infinite words are indexed from right to left (fortunately): if  $s$  is in  ${}^\omega A$ , we write  $s = \cdots s_2 s_1 s_0$ , and for  $0 \leq j \leq \ell \leq +\infty$ , we denote by  $s_{[\ell, j]}$  the word  $s_{[\ell, j]} = s_\ell s_{\ell-1} \cdots s_j$ .

As assumed since the beginning of this paper, the alphabet  $A$  is an alphabet of digits, starting with 0:  $A = \{0, 1, \dots, r-1\}$ . In order to embed finite words into (left) infinite ones, we need the following assumption.

**Assumption 5.2.** No word of  $L$  begins with 0, that is,  $L \subseteq (A \setminus \{0\}) A^*$ .

This assumption is naturally fulfilled by the classical numeration systems in integer bases, the Fibonacci system, *etc.* Under this assumption, the map from  $A^*$  to  ${}^\omega A$  defined by  $w \mapsto {}^\omega 0 w$  is a *bijection* between  $L$  and  ${}^\omega 0 L$ , that is,  $L$  embeds in  ${}^\omega A$  and can be identified with  ${}^\omega 0 L$ .

The set  ${}^\omega A$  is classically equipped with the *product topology* or topology of *simple convergence*, that is, the topology induced by the *distance* between elements defined by  $d(s, t) = 2^{-e(s, t)}$  where  $e(s, t)$  is the length of the longest common right-factor of  $s$  and  $t$ . Under this topology,  ${}^\omega A$  is a *compact set*, and so is any closed subset of  ${}^\omega A$ .

**Definition 5.3.** The compactification of  $L$  is the closure of  ${}^\omega 0 L$  under the topology of  ${}^\omega A$  and is denoted by  $\mathcal{K}_L$ :

$$\mathcal{K}_L = \overline{{}^\omega 0 L} = \left\{ s \in {}^\omega A \mid \forall j \in \mathbb{N} \quad \exists w^{(j)} \in 0^* L \quad s_{[j, 0]} \text{ is a right-factor of } w^{(j)} \right\} .$$

The topology on  $\mathcal{K}_L$  is the one induced by the topology on  ${}^\omega A$ . For every word  $w$  in  $A^*$ , we call the set of elements  $s$  in  $\mathcal{K}_L$  of which  $w$  is a right-factor the *cylinder generated by  $w$* , and denote it by  $[w]$ :<sup>11</sup>

$$[w] = \left\{ s \in \mathcal{K}_L \mid s_{[|w|-1, 0]} = w \right\} = {}^\omega A w \cap \mathcal{K}_L .$$

The set of cylinders is a base of open sets of  $\mathcal{K}_L$ . Given any two words  $u$  and  $v$  in  $A^*$ , with  $|u| \leq |v|$ , either  $[v] \subseteq [u]$ , a case that holds if and only if  $u$  is a right-factor of  $v$ , or  $[u] \cap [v] = \emptyset$ .

### 5.2.2 Definition of the odometer

Let  $L \subseteq A^*$  be a language which satisfies Assumption 5.2. The successor function  $\text{Succ}_L: L \rightarrow L$  is naturally transformed into a function  $\text{Succ}_L: {}^\omega 0 L \rightarrow {}^\omega 0 L$  by setting  $\text{Succ}_L({}^\omega 0 w) = {}^\omega 0 \text{Succ}_L(w)$ .

<sup>11</sup>It should be noted that although the *notation*  $[w]$  does not bear any reference to  $L$ , the *set*  $[w]$  does depend on  $L$ .

**Definition 5.4.** We call a function from  $\mathcal{K}_L$  into itself that extends  $\text{Succ}_L$  an odometer on  $L$ , and we denote it by  $\tau_L$ .

This definition silently implies that the uniqueness of the odometer is not guaranteed. A particular odometer is chosen in the case where  $\text{Succ}_L$  is continuous:

**Definition 5.5.** Let  $L$  be a language with the property that  $\text{Succ}_L: {}^\omega 0L \rightarrow {}^\omega 0L$  is continuous. Then the odometer  $\tau_L$  is the unique continuous function from  $\mathcal{K}_L$  into itself that extends  $\text{Succ}_L$ .

Uniqueness in the above definition follows from the fact that  ${}^\omega 0L$  is dense in  $\mathcal{K}_L$ . If  $\text{Succ}_L$  is not continuous, one has to find other means to define  $\tau_L$ , and they depend on the cases, and on the authors (see for instance [19], [10]). We give such a construction, following [19], in Sec. 5.3.2.

### 5.2.3 Extension of the carry propagation

We extend the map  $\Delta$  defined in Sec. 3 on pairs of finite words to pairs of elements of  ${}^\omega A$ . Let  $s$  and  $t$  in  ${}^\omega A$ ; then:

$$\Delta(s, t) = \begin{cases} \min \left\{ j \in \mathbb{N} \mid s_{[\infty, j]} = t_{[\infty, j]} \right\} & \text{if } \left\{ j \in \mathbb{N} \mid s_{[\infty, j]} = t_{[\infty, j]} \right\} \neq \emptyset, \\ +\infty & \text{otherwise.} \end{cases}$$

Conversely, the definition of  $\Delta$  on  $((A \setminus \{0\})A^*)^2$  can be deduced from the one on  $({}^\omega A)^2$  which is simpler and we have, for  $u$  and  $v$  in  $(A \setminus \{0\})A^*$ ,

$$\Delta({}^\omega 0u, {}^\omega 0v) = \Delta(u, v) .$$

When the odometer  $\tau_L$  will be defined, we shall set, as in Definition 3.1:

$$\forall s \in {}^\omega A \quad \text{cp}_L(s) = \Delta(s, \tau_L(s)) .$$

**Proposition 5.6.** If  $\tau_L$  is continuous, then  $\text{cp}_L$  is continuous at any point where it takes finite values.

*Proof.* Indeed, let  $s$  in  $\mathcal{K}_L$  with  $\text{cp}_L(s) < +\infty$  and  $(s_n)_{n \in \mathbb{N}}$  be a sequence of elements of  $\mathcal{K}_L$  such that  $d(s, s_n)$  tends to 0. It means that  $e(s, s_n)$ , the length of the longest common right factor of  $s$  and  $s_n$ , takes arbitrarily large values. Since  $\tau_L$  is continuous,  $e(\tau_L(s), \tau_L(s_n))$  is arbitrarily large as well. Let  $j > \text{cp}_L(s)$ . For large enough  $n$ ,  $s_{[j, 0]} = (s_n)_{[j, 0]}$  and similarly  $\tau_L(s)_{[j, 0]} = \tau_L(s_n)_{[j, 0]}$ . Thus  $\text{cp}_L(s) = \text{cp}_L(s_n)$ .  $\square$

If we write  $0 = {}^\omega 0$ ,  $\text{CP}_L$ , the carry propagation of  $L$ , can be written, if the limit exists, as:

$$\text{CP}_L = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{i=0}^{N-1} \text{cp}_L(\tau_L^i(0)) ,$$

which is the transformation of (28) we were aiming at in order to engage with the use of the Ergodic Theorem.

**Example 5.7.** Let  $p$  be an integer. The completion  $\mathcal{K}_p$  of  ${}^{\omega}0L_p$  is the ring  $\mathbb{Z}_p$  of the  $p$ -adic integers (a non-integral one if  $p$  is not a prime).

The ring  $\mathbb{Z}_p$  is a topological group, and the odometer  $\tau_p$  is the addition of 1, and thus a group rotation and a continuous function. By Proposition 5.6 the carry propagation  $\text{cp}_p$  is continuous. The system  $(\mathcal{K}_p, \tau_p)$  is uniquely ergodic, see [29] for instance. By applying the (second part of) Ergodic Theorem, we get an ‘ergodic proof’ of Proposition 3.9.

### 5.3 The dynamics of greedy numeration systems

In this section, we consider a case where the odometer is not defined by continuity but rather by a combinatorial property of the representation languages. The greedy numeration systems have indeed the property that the language of the representations of the natural integers is closed under right-factors, and this will allow a meaningful definition of the odometer, even when it is not continuous. Our study is based on recent results due to Barat and Grabner [3].

#### 5.3.1 Greedy algorithm and greedy numeration systems

Greedy numeration systems (GNS, for short) are a generalization of the integer base numeration systems. The base is replaced by a *basis* (also called *scale*) which is an infinite sequence of positive integers and which plays the role of the sequence of the powers of the integer base. The classical example is the Fibonacci numeration system where the basis consists of the sequence of Fibonacci numbers. These systems have been first defined and studied in full generality by A. Fraenkel [15] and we have given large accounts on this subject in some previous works of ours [17, 31].

A *basis* is a strictly increasing sequence of integers  $G = (G_\ell)_{\ell \in \mathbb{N}}$  with  $G_0 = 1$ . The *greedy  $G$ -expansion* of a natural integer is the result of a so-called *greedy algorithm* — described in this context in [15] — for the definition of which we take a new notation. Given two integers  $m$  and  $p$ , we write  $m \div p$  and  $m \% p$  for the *quotient* and the *remainder* of the Euclidean division of  $m$  by  $p$  respectively.

**Definition 5.8.** *The greedy algorithm goes as follows: given  $N$  in  $\mathbb{N}$ ,*

- (i) *let  $k$  be defined by the condition  $G_k \leq N < G_{k+1}$ .*
- (ii) *let  $x_k = N \div G_k$  and  $r_k = N \% G_k$ ;*
- (iii) *for every  $i$ , from  $i = k - 1$  to  $i = 0$ , let  $x_i = r_{i+1} \div G_i$  and  $r_i = r_{i+1} \% G_i$ .*

*We then have:  $N = x_k G_k + x_{k-1} G_{k-1} + \dots + x_0 G_0$ .*

The sequence of digits  $x_k x_{k-1} \cdots x_1 x_0$  is called the (*greedy*)  $G$ -*expansion* of  $N$  and is denoted by  $\langle N \rangle_G$ . The set of  $G$ -expansions is denoted by  $L_G$ :

$$L_G = \{ \langle N \rangle_G \mid N \in \mathbb{N} \} .$$

The language  $L_G$  is characterized by the following:

$$\begin{aligned} x_k x_{k-1} \cdots x_0 \in L_G &\iff \\ \forall i, 0 \leq i \leq k, \quad x_i G_i + x_{i-1} G_{i-1} + \cdots + x_0 G_0 &< G_{i+1} . \end{aligned} \quad (30)$$

The  $G$ -expansion maps the natural order on  $\mathbb{N}$  onto the *radix order* on  $L_G$ , that is,  $N \leq M$  holds if and only if  $\langle N \rangle_G \sqsubseteq \langle M \rangle_G$  holds and  $L_G$  may also be considered as an ANS. Equation (30) becomes:

$$x_k x_{k-1} \cdots x_0 \in L_G \iff \forall i, 0 \leq i \leq k, \quad x_i x_{i-1} \cdots x_0 \sqsubseteq \langle G_{i+1} - 1 \rangle_G . \quad (31)$$

It follows that for every  $\ell$  in  $\mathbb{N}$ , we have:

$$G_\ell = \mathbf{v}_{L_G}(\ell) .$$

For readability, we write  $g_\ell = \langle G_\ell - 1 \rangle_G$ , and it follows from (31) that

$$\text{Maxlg}(L_G) = \{ g_\ell \mid \ell \in \mathbb{N} \} .$$

By construction, the language  $L_G$  satisfies Assumption 5.2 and the language  $0^* L_G$  is *closed under right-factor*. Note that  $L_G$  is not PCE in general (*cf.* Remark 5.28 below).

If the sequence of the quotients  $G_{\ell+1}/G_\ell$  of successive terms of  $G$  is bounded, with  $r = \limsup \lceil \frac{G_{\ell+1}}{G_\ell} \rceil$ , then all  $G$ -expansions are words over the alphabet  $A_G = \{0, 1, \dots, r-1\}$ . In the following, we silently assume that this condition holds and that  $L_G$  is thus a language over the finite alphabet  $A_G$ . (For instance, we exclude GNS such as  $G = (\ell!)_{\ell \in \mathbb{N}}$ .)

### 5.3.2 Ergodicity of greedy numeration systems

Let  $G$  be a GNS. We denote the successor function on  $L_G$  by  $\text{Succ}_G$  (rather than  $\text{Succ}_{L_G}$ ). The definition of the compactification of  $L_G$ , which we denote by  $\mathcal{K}_G$  (rather than  $\mathcal{K}_{L_G}$ ), takes a simpler form since  $0^* L_G$  is closed under right-factor:

$$\mathcal{K}_G = \overline{0^* L_G} = \left\{ s \in {}^\omega A \mid \forall j \in \mathbb{N} \quad s_{[j,0]} \in 0^* L_G \right\} .$$

The same closure property by right-factor yields the definition of an odometer.

**Theorem 5.9** ([3, 19]). *Let  $G$  be a GNS. For every  $s$  in  $\mathcal{K}_G$ ,  $\lim_{j \rightarrow \infty} \text{Succ}_G(s_{[j,0]})$  exists and defines the odometer  $\tau_G: \mathcal{K}_G \rightarrow \mathcal{K}_G$ :*

$$\forall s \in \mathcal{K}_G \quad \tau_G(s) = \lim_{j \rightarrow \infty} \text{Succ}_G(s_{[j,0]}) .$$

The carry propagation at  $s$  in  $\mathcal{K}_G$  is defined by  $\text{cp}_G(s) = \Delta(s, \tau_G(s))$  as announced above, and is denoted by  $\text{cp}_G(s)$  (rather than  $\text{cp}_{L_G}(s)$ ). The carry propagation of  $L_G$ , which we denote by  $\text{CP}_G$  (rather than  $\text{CP}_{L_G}$ ) is then defined, when it exists, by (cf. (30)):

$$\text{CP}_G = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{i=0}^{N-1} \text{cp}_G(\tau_G^i(0)) .$$

**Remark 5.10.** The language  $L_G$  is not necessarily a regular language. But when it is, then

- (i) the basis  $G$  is a linear recurrent sequence, a result due to Shallit [33];
- (ii) the odometer  $\tau_G$  is continuous if and only if  $\text{Succ}_G$  is realizable by a finite right sequential transducer [16]. We come back to this result and the definition of finite right sequential transducers in the hopefully forthcoming sequel of this work [8].

The odometer  $\tau_G$  may be continuous or not, as shown in Examples 5.40 and 5.41 below. Resorting to the Ergodic Theorem requires some further hypothesis as well as some technical developments.

**Definition 5.11.** A GNS  $G$  is said to be exponential if it is equivalent to a sequence which is homothetic to a geometric progression, that is, if there exist two real constants  $\alpha > 1$  and  $C > 0$  such that  $G_\ell \sim C\alpha^\ell$  when  $\ell$  tends to infinity.

Exponential GNS are of interest to us because of the following result.

**Theorem 5.12** ([4], Theorem 8). *If  $G$  is an exponential GNS, then the dynamical system  $(\mathcal{K}_G, \tau_G)$  is uniquely ergodic.*

If  $G$  is an exponential GNS, the unique  $\tau_G$ -invariant measure on  $\mathcal{K}_G$  is denoted by  $\mu_G$ . Since  $\tau_G$  is not necessarily continuous, and even though the system  $(\mathcal{K}_G, \tau_G)$  is uniquely ergodic, we only have the first part of Ergodic Theorem 5.1 at hand. The following definitions and results, again borrowed from [3], are used in the proof of Theorem 5.17 we are aiming at and which amounts indeed to the proof that 0 is contained in the set of  $\mu_G$ -almost all points for which (29) holds.

We first have an evaluation of the measure of the cylinders generated by the maximal words, that holds without the assumption of exponentiality.

**Proposition 5.13** ([3], Eq. 4.8). *Let  $G$  be a GNS and  $\mu$  a  $\tau_G$ -invariant measure. Then, for every  $\ell$  in  $\mathbb{N}$ , we have:*

$$\mu([g_\ell]) \leq 1/G_\ell .$$



**Notation.** For every  $i$  in  $\mathbb{N}$ , we denote by  $\delta_i$  the *Dirac measure* at point  $\langle i \rangle_G = \tau_G^i(0)$  of  $\mathcal{K}_G$  and, for every  $N$  in  $\mathbb{N}$ , by  $\nu_N$  the mean of these measures on the ‘first’  $N$  points of  $\mathcal{K}_G$ :

$$\nu_N = \frac{1}{N} \sum_{i=0}^{N-1} \delta_i .$$

We write  $\chi_S$  for the *characteristic function* of a subset  $S$  of  $\mathcal{K}_G$ . We thus have, for any  $w \in L_G$ :

$$\nu_N([w]) = \frac{1}{N} \sum_{i=0}^{N-1} \chi_{[w]}(\tau_G^i(0)) .$$

The main result of [3] we rely on is the expression of  $\mu_G$  in terms of the  $\nu_N$ .

**Theorem 5.14** ([3], Theorem 2). *Let  $G$  be a GNS and  $(\mathcal{K}_G, \tau_G)$  the associated dynamical system. If  $(\mathcal{K}_G, \tau_G)$  is uniquely ergodic with measure  $\mu_G$ , then for every  $w$  in  $L_G$ , we have:*

$$\lim_{N \rightarrow \infty} \nu_N([w]) = \mu_G([w]) .$$

**Remark 5.15.** The determined reader who refers himself to [3] will hardly recognize Theorem 5.14 there. Indeed, Theorem 2 in [3] is much more general and says, roughly, that *any invariant measure* on  $\mathcal{K}_G$  is a *cluster point of sequences* of convex combinations of the  $\nu_N$ ’s. If  $\mathcal{K}_G$  is uniquely ergodic, then  $\mu_G$  is the only possible cluster point, and, on the other hand, the limit of the sequence of the  $\nu_N$ ’s is a cluster point.

**Remark 5.16.** One may say that Theorem 5.14, or the convergence of the  $\nu_N$ ’s toward  $\mu_G$ , expresses the property that 0 is a *generic point* of the system  $(\mathcal{K}_G, \tau_G)$  in the sense that the measure of any cylinder  $[w]$  is obtained as the limit of the *statistics* induced by the orbit of 0 under  $\tau_G$ , or, to put it in a way that is more congruent with the Ergodic Theorem, we have:

$$\forall w \in A_G^* \quad \int_{\mathcal{K}_G} \chi_{[w]} d\mu_G = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{i=0}^{N-1} \chi_{[w]}(\tau_G^i(0)) ,$$

This *does not imply* that

$$\forall f \in L^1(\mu_G) \quad \int_{\mathcal{K}_G} f d\mu_G = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{i=0}^{N-1} f(\tau_G^i(0)) . \quad (32)$$

It suffices to take  $f = \chi_{\Omega(0)}$  the characteristic function of the orbit of 0: the left-hand side is 0 since the domain of  $\Omega(0)$  is denumerable and the mean of the sum in the right-hand side is uniformly equal to 1, hence has limit 1.

In order to prove Theorem 5.17 below, we have to prove that the function  $\text{cp}_G$  is somehow *regular enough* to guarantee (32). Equation (32) holds

for any *Riemann-integrable* function  $f$ . On the other hand,  $\chi_{\Omega(0)}$  is typical of a function that is Lebesgue-integrable but not Riemann-integrable. The function  $\text{cp}_G$  is not Riemann-integrable either, since it is *unbounded*. It should be treated as an *improper integral*.

### 5.3.3 Carry propagation in greedy numeration systems

We are now in a position to give an ergodic proof of the existence of the carry propagation for a family of greedy numeration systems.

**Theorem 5.17.** *Let  $G$  be a GNS that meets the following two conditions:*

- (i)  $(\mathcal{K}_G, \tau_G)$  is uniquely ergodic;
- (ii)  $\sum_{k=0}^{+\infty} \frac{k}{G^k}$  is bounded.

*Then, the carry propagation  $\text{CP}_G = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{i=0}^{N-1} \text{cp}_G(\tau^i(0))$  exists.*

As a consequence of Theorem 5.12, and since condition (ii) is obviously satisfied by an exponential GNS, we have:

**Corollary 5.18.** *If  $G$  is an exponential GNS, then  $\text{CP}_G$  exists.*

Before proving Theorem 5.17 at Sec. 5.3.4, we establish that  $\text{cp}_G$  is an integrable function (Proposition 5.20). To that end and for the sake of further developments, we first define subsets of  $\mathcal{K}_G$  according to the values taken by  $\text{cp}_G$ :

$$\forall k \in \mathbb{N} \quad D_k = \left\{ s \in \mathcal{K}_G \mid \text{cp}_G(s) = k + 1 \right\} .$$

The subsets  $D_k$  are Boolean combinations of cylinders. Indeed,  $\text{cp}_G(s) = k + 1$  if and only if:

- (a)  $g_k$  is a right-factor of  $s$ ;
- (b) no  $g_m$ ,  $m \geq k + 1$ , is a right-factor of  $s$ .

(Remember that for every integer  $\ell$ ,  $g_\ell$  is the maximal word of  $L_G$  of length  $\ell$  and  $g_\ell = \langle G_\ell - 1 \rangle_G$ .) If  $g_k$  is not a right-factor of  $g_m$ , then  $[g_k] \cap [g_m] = \emptyset$ , hence we can write:

$$\forall k \in \mathbb{N} \quad D_k = [g_k] \setminus \bigcup_{m \geq k+1} [g_m] , \tag{33}$$

and the  $D_k$  are measurable.

One can be more precise and give an expression of the  $D_k$  that is unambiguous and that will be used in actual computations. Consider the (strict) ordering relation ‘being a right-factor’ (on  $A_G^*$ ):  $h_1 >_{\text{rf}} h_2$  if  $h_2$  is a right-factor of  $h_1$  (and  $h_1 \neq h_2$ ). Let

$$\forall k \in \mathbb{N} \quad T(k) = \{ g_m \in \text{Max} | \text{g}(L_G) \mid g_m >_{\text{rf}} g_k \}$$

and

$$T'(k) = \min T(k) = \{g_m \in T(k) \mid \text{there exists no } g_n \text{ in } T(k) \text{ } g_m >_{\text{rf}} g_n\} .$$

For the ease of writing, we define:

$$I(k) = \{m \in \mathbb{N} \mid g_m \in T'(k)\} ,$$

and we have

$$D_k = [g_k] \setminus \biguplus_{m \in I(k)} [g_m] , \quad (34)$$

where  $\biguplus$  is the *disjoint* union. Finally, let us give some more notation.

- For every  $k$  in  $\mathbb{N}$ , let  $M_k = \sum_{j=k+1}^{\infty} \frac{j+1}{G_j}$ . By hypothesis,  $\lim_{k \rightarrow \infty} M_k = 0$ .
- We write  $F_k = \bigcup_{j=0}^{j=k} D_j$ .
- We denote by  $f_k$  the function that is equal to  $\text{cp}_G$  on  $F_k$  and to 0 everywhere else.

For every  $k$  in  $\mathbb{N}$ , the function  $f_k$  is a *step function*, that is, a linear combination of characteristic functions of measurable sets, in this case, of the characteristic functions of the  $D_j$ ,  $0 \leq j \leq k$  and of the one of  $\mathcal{K}_G \setminus F_k$ . As a direct consequence of Theorem 5.14, we then have:

**Proposition 5.19.**

$$\forall k \in \mathbb{N} \quad \int_{\mathcal{K}_G} f_k d\mu_G = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{i=0}^{N-1} f_k(\tau^i(0)) .$$

From the definition of the  $D_k$ 's, we now derive that  $\text{cp}_G$  is an integrable function:

**Proposition 5.20.** *Under the conditions of Theorem 5.17,  $\text{cp}_G$  is in  $L^1(\mu_G)$ , that is,  $\int_{\mathcal{K}_G} \text{cp}_G d\mu_G$  exists.*

*Proof.* Since all terms are positive, we have:

$$\int_{\mathcal{K}_G} \text{cp}_G d\mu_G = \lim_{k \rightarrow \infty} \sum_{j=0}^k (j+1) \mu_G(D_j) . \quad (35)$$

From (34) and Proposition 5.13, follows

$$\forall k \in \mathbb{N} \quad \sum_{j=k+1}^{\infty} (j+1) \mu_G(D_j) \leq \sum_{j=k+1}^{\infty} (j+1) \mu_G([g_j]) \leq \sum_{j=k+1}^{\infty} \frac{j+1}{G_j} = M_k .$$

Since  $\int_{\mathcal{K}_G} f_k d\mu_G = \sum_{j=0}^k (j+1) \mu_G(D_j)$  we have:

$$\int_{\mathcal{K}_G} f_k d\mu_G \leq \int_{\mathcal{K}_G} \text{cp}_G d\mu_G \leq \int_{\mathcal{K}_G} f_k d\mu_G + M_k , \quad (36)$$

which shows not only that  $\int_{\mathcal{K}_G} \text{cp}_G d\mu_G$  exists but also that

$$\lim_{k \rightarrow \infty} \int_{\mathcal{K}_G} f_k d\mu_G = \int_{\mathcal{K}_G} \text{cp}_G d\mu_G . \quad \square$$

Of course, we have:

$$\forall k \in \mathbb{N}, \forall N \in \mathbb{N} \quad \frac{1}{N} \sum_{i=0}^{N-1} f_k(\tau^i(0)) \leq \frac{1}{N} \sum_{i=0}^{N-1} \text{cp}_G(\tau^i(0)) , \quad (37)$$

but it is not enough that the left-hand side has a limit for the right-hand side to have also one. We need to find a bounding interval as in (36) in order to insure that the quantity  $\frac{1}{N} \sum_{i=0}^{N-1} \text{cp}_G(\tau^i(0))$  converges when  $N$  tends to infinity. And this is what is done in the next subsection.

### 5.3.4 Proof of Theorem 5.17

We begin with some more notation. First, for every integer  $N$  in  $\mathbb{N}$ , we write  $\partial_G(N)$  for the *degree*, or *height*, with respect to the basis (or scale)  $G$ , that is, the integer  $k = \partial_G(N)$  is such that  $G_k \leq N < G_{k+1}$ . In particular,  $|\langle N \rangle_G| = \partial_G(N) + 1$ .

Second, for every integer  $n$  in  $\mathbb{N}$ , and for every  $k \geq |\langle n \rangle_G| = \ell$ , we write  $\langle n \rangle_{G,k}$  for  $\langle n \rangle_{G,k} = 0^{k-\ell} \langle n \rangle_G$ , that is,  $\langle n \rangle_{G,k}$  is the *unique* word in  $A_G^k \cap 0^* \langle n \rangle_G$ . Finally, in the same way as we write  $\text{cp}_G(n)$  for  $\text{cp}_G(\tau^n(0))$ , we write  $f_k(n)$  for  $f_k(\tau^n(0))$ . The greedy algorithm (Definition 5.8) may then equivalently be rewritten as follows.

**Lemma 5.21.** *The  $G$ -expansions of integers, that is, the greedy algorithm for the basis  $G$ , is described by the following recurrence formula:*

- (i)  $\langle 0 \rangle_G = \varepsilon$ ;
- (ii)  $\forall N \in \mathbb{N}$ , if  $k = \partial_G(N)$ , then  $\langle N \rangle_G = d \langle r \rangle_{G,k}$   
with  $d = N \div G_k$  and  $r = N \% G_k$ .

### Corollary 5.22.

Let  $N$  in  $\mathbb{N}$  and  $k = \partial_G(N)$ . If  $N < G_{k+1} - 1$ , then:  $\text{cp}_G(N) = \text{cp}_G(N \% G_k)$ .

*Proof.* Let  $\langle N \rangle_G = dw$ ; then  $\langle N \% G_k \rangle_G = w$  with  $|w| = k$ . There are two possibilities: either  $\text{cp}_G(N) = k + 1$  or  $\text{cp}_G(N) \leq k$ . Indeed, the possibility

that  $N + 1 = G_{k+1}$  and  $\text{cp}_G(N) = k + 2$  is ruled out by the hypothesis  $N < G_{k+1} - 1$ .

If  $\text{cp}_G(N) = k + 1$ , then  $\langle N + 1 \rangle_G = (d+1)0^k$  and then  $\langle N \% G_k + 1 \rangle_G = 10^k$  and  $\text{cp}_G(N \% G_k) = k + 1$ .

If  $\text{cp}_G(N) \leq k$ , then  $\langle N + 1 \rangle_G = dw'$  and then  $\langle N \% G_k + 1 \rangle_G = w'$  and  $\text{cp}_G(N \% G_k) = \text{cp}_G(N)$  again.  $\square$

The first step toward Theorem 5.17 is the description of the relationship between the functions  $f_{k-1}$  and  $f_k$  for all numbers less than  $G_{k+1}$ , as expressed by the following.

**Proposition 5.23.** *For every  $k$  in  $\mathbb{N}$ , we have:*

$$\forall N \in \mathbb{N}, 0 < N < G_{k+1} \quad \sum_{i=0}^{N-1} f_k(i) = \sum_{i=0}^{N-1} f_{k-1}(i) + \left\lfloor \frac{N}{G_k} \right\rfloor (k+1) . \quad (38)$$

*Proof.* Let  $k$  in  $\mathbb{N}$  and  $d_k$  be the largest digit that appears at index  $k$  (remember that the rightmost index is 0), that is:

$$d_k G_k < G_{k+1} \leq (d_k + 1) G_k .$$

(An integer base is the case where the equality on the right holds for the same digit for every  $k$ .) Let us consider the integers in the interval  $[0, G_{k+1}[$  and the functions  $f_{k-1}$  and  $f_k$ :

$$\begin{array}{ll} \text{If } 0 \leq n < G_k - 1 & \text{then } \text{cp}_G(n) \leq k \quad \text{and } f_{k-1}(n) = f_k(n) \\ n = G_k - 1 & \text{then } \text{cp}_G(n) = k + 1 \quad \text{and } f_{k-1}(n) = 0, f_k(n) = k + 1 \\ G_k - 1 \leq n < 2G_k - 1 & \text{then } \text{cp}_G(n) \leq k \quad \text{and } f_{k-1}(n) = f_k(n) \\ n = 2G_k - 1 & \text{then } \text{cp}_G(n) = k + 1 \quad \text{and } f_{k-1}(n) = 0, f_k(n) = k + 1 \\ & \dots\dots\dots \end{array}$$

$$d_k G_k - 1 \leq n < G_{k+1} - 1 \quad \text{then } \text{cp}_G(n) \leq k \quad \text{and } f_{k-1}(n) = f_k(n)$$

Taking advantage that all summations go to  $N - 1$ , these  $2d_k + 1$  lines of equalities imply (38).  $\square$

The aim is to obtain an equation of the same kind as (38) but which holds for all  $N$  in  $\mathbb{N}$ . Corollary 5.22 leads to the definition of  $(H, L)$ -extensions, Proposition 5.23 gives us a hint for the elementary arithmetic Lemma 5.25 that will pave the way to the solution (Proposition 5.26).

**Definition 5.24.** *Let  $H$  and  $L$  in  $\mathbb{N}$ , with  $H < L$ . Let  $\alpha: [0, H[ \rightarrow \mathbb{N}$  be a function. Let  $\alpha': [0, L[ \rightarrow \mathbb{N}$  be the function defined by*

$$\forall m \in [0, L[ \quad \alpha'(m) = \alpha(m \% H) . \quad (39)$$

*We call  $\alpha'$  the  $(H, L)$ -extension of  $\alpha$ .*

The graph of the  $(H, L)$ -extension of  $\alpha$  consists then of the repetition of the graph of  $\alpha$  translated by the quantities  $H, 2H, \text{etc.}$ , along the  $x$ -axis, until  $kH$ , where  $kH < L \leq (k+1)H$ , the last piece being cut off at the abscissa  $L$ .

**Lemma 5.25.** *Let  $H$  in  $\mathbb{N}$  and  $\alpha, \beta: [0, H[ \rightarrow \mathbb{N}$  be two functions with the property that there exists a  $K$  in  $\mathbb{N}$  (presumably  $K < H$ ) and a constant  $C$  in  $\mathbb{N}$  such that*

$$\forall n \in ]0, H] \quad \sum_{i=0}^{n-1} \beta(i) \leq \sum_{i=0}^{n-1} \alpha(i) + C \left\lfloor \frac{n}{K} \right\rfloor . \quad (40)$$

*Let  $L$  in  $\mathbb{N}$  ( $L > H$ ), and  $\alpha', \beta': [0, L[ \rightarrow \mathbb{N}$  be the  $(H, L)$ -extensions of  $\alpha$  and  $\beta$  respectively. Then we have:*

$$\forall m \in ]0, L] \quad \sum_{j=0}^{m-1} \beta'(j) \leq \sum_{j=0}^{m-1} \alpha'(j) + C \left\lfloor \frac{m}{K} \right\rfloor . \quad (41)$$

*Proof.* From (40) follows in particular

$$\sum_{i=0}^{H-1} \beta(i) \leq \sum_{i=0}^{H-1} \alpha(i) + C \left\lfloor \frac{H}{K} \right\rfloor .$$

For  $m$  in  $\mathbb{N}$ , let us write  $d = m \div H$  and  $n = m \% H$  (hence  $m = dH + n$ ). Then, using the definition of  $(H, L)$ -extension, one writes

$$\sum_{j=0}^{m-1} \beta'(j) = d \left( \sum_{i=0}^{H-1} \beta(i) \right) + \sum_{i=0}^{n-1} \beta(i) ,$$

with the convention that  $\sum_{i=0}^{i=-1} \beta(i) = 0$ . We then have:

$$\begin{aligned} \sum_{j=0}^{m-1} \beta'(j) &\leq d \left( \sum_{i=0}^{H-1} \alpha(i) + C \left\lfloor \frac{H}{K} \right\rfloor \right) + \sum_{i=0}^{n-1} \alpha(i) + C \left\lfloor \frac{n}{K} \right\rfloor \\ &\leq \sum_{j=0}^{m-1} \alpha'(j) + C \left( d \left\lfloor \frac{H}{K} \right\rfloor + \left\lfloor \frac{n}{K} \right\rfloor \right) \\ &\leq \sum_{j=0}^{m-1} \alpha'(j) + C \left\lfloor \frac{m}{K} \right\rfloor , \end{aligned}$$

from the obvious inequality  $d \left\lfloor \frac{H}{K} \right\rfloor + \left\lfloor \frac{n}{K} \right\rfloor \leq \left\lfloor \frac{dH + n}{K} \right\rfloor$ . □

The key statement for the proof of Theorem 5.17 reads as follows.

**Proposition 5.26.** *Let  $k$  be a fixed integer greater than 1. Then, for every  $N$  in  $\mathbb{N}$ :*

$$\sum_{i=0}^{N-1} f_k(i) \leq \sum_{i=0}^{N-1} f_{k-1}(i) + \left\lfloor \frac{N}{G_k} \right\rfloor (k+1) . \quad (42)$$

*Proof.* Let us establish by induction that for every  $h$ ,  $h \geq k$ , we have:

$$\forall N \in ]0, G_{h+1}[ \quad \sum_{i=0}^{N-1} f_k(i) \leq \sum_{i=0}^{N-1} f_{k-1}(i) + \left\lfloor \frac{N}{G_k} \right\rfloor (k+1) . \quad (43)$$

Proposition 5.23 asserts that indeed *equality* holds in (42) for all  $N$  in  $]0, G_{k+1}[$ . If  $N = G_{k+1}$ , the summations in (42) go up to  $n = G_{k+1} - 1$ , and then  $\text{cp}_G(n) = k+2$  and  $f_{k-1}(n) = f_k(n) = 0$ . Hence the equality still holds, but for the case where  $G_{k+1} = (d_k + 1)G_k$  (and then  $\left\lfloor \frac{N}{G_k} \right\rfloor = d_{k+1}$ ) in which case the *inequality* holds and (43) is established for  $h = k$ .

Let us call  $\alpha$  and  $\beta$  the restrictions to  $]0, G_{h+1}[$  of  $f_{k-1}$  and  $f_k$  respectively. Let  $L = G_{h+2} - 1$ ; from Corollary 5.22 follows that the  $(G_{h+1}, L)$ -expansions of  $\alpha$  and  $\beta$  are the restrictions to  $]0, G_{h+2} - 1[$  of  $f_{k-1}$  and  $f_k$  respectively.

From Lemma 5.25 we deduce that the inequality (42) holds for every  $N$  in  $]0, G_{h+2} - 1[$ .

Since  $\text{cp}_G(G_{h+2} - 1) = h + 3$ , then  $f_{k-1}(G_{h+2} - 1) = f_k(G_{h+2} - 1) = 0$  and (42) also holds for  $N = G_{h+2}$ , which completes the induction step.  $\square$

*Proof of Theorem 5.17.* Let  $k$  be a fixed integer. For every  $N$  in  $\mathbb{N}$ , there exists an  $h = \sup_{n \in [0, N]} \text{cp}_G(n) - 1$  such that  $\text{cp}_G(n) = f_h(n)$  for all  $n$  in  $]0, N[$ . (Note that we cannot exchange the quantifiers and state: ‘there exists an  $h$  such that for every  $N$  etc.’) We then have

$$\frac{1}{N} \sum_{i=0}^{N-1} f_h(\tau^i(0)) = \frac{1}{N} \sum_{i=0}^{N-1} \text{cp}_G(\tau^i(0)) .$$

From (37) and Proposition 5.26 follows

$$\begin{aligned} \frac{1}{N} \sum_{i=0}^{N-1} f_k(\tau^i(0)) &\leq \frac{1}{N} \sum_{i=0}^{N-1} \text{cp}_G(\tau^i(0)) \\ &\leq \frac{1}{N} \sum_{i=0}^{N-1} f_k(\tau^i(0)) + \sum_{j=k+1}^{j=h} \frac{1}{N} \left\lfloor \frac{N}{G_j} \right\rfloor (k+1) . \end{aligned}$$

Two obvious majorizations give

$$\frac{1}{N} \sum_{i=0}^{N-1} f_k(\tau^i(0)) \leq \frac{1}{N} \sum_{i=0}^{N-1} \text{cp}_G(\tau^i(0)) \leq \frac{1}{N} \sum_{i=0}^{N-1} f_k(\tau^i(0)) + M_{k+1} ,$$

which yields, when  $N$  tends to infinity, and taking Proposition 5.19 into account:

$$\forall k \in \mathbb{N} \quad \int_{\mathcal{K}_G} f_k d\mu_G \leq \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{i=0}^{N-1} \text{cp}_G(\tau^i(0)) \leq \int_{\mathcal{K}_G} f_k d\mu_G + M_{k+1} .$$

If we make now  $k$  tend to infinity we get both that the limit

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{i=0}^{N-1} \text{cp}_G(\tau^i(0)) \text{ exists, and that this limit is } \int_{\mathcal{K}_G} \text{cp}_G d\mu_G . \quad \square$$

In the case where the language  $L_G$  of the exponential greedy numeration system  $G$  is PCE, we can use the results of Sec. 3 and give the value of the carry propagation. Since  $G_\ell \sim C \alpha^\ell$  implies that the local growth rate of  $L_G$  is equal to  $\alpha$ , we have, by Corollary 3.16:

**Theorem 5.27.** *If  $G$  is an exponential GNS with  $G_\ell \sim C \alpha^\ell$  and if  $L_G$  is PCE, then  $\text{CP}_G$  exists and*

$$\text{CP}_G = \frac{\alpha}{\alpha - 1} .$$

The next section deals with a family of greedy numeration systems which have PCE languages, namely  $\beta$ -numeration systems.

**Remark 5.28.** It is somewhat unsatisfactory to have to put an hypothesis on  $L_G$  directly. It would be more natural to have a condition on the basis  $G$  itself which would insure that  $L_G$  be PCE.

A necessary condition for  $L_G$  to be PCE is that the sequence  $\left[ \frac{G_{n+1}}{G_n} \right]$  be *non-increasing*. But it is not a sufficient condition, as shown by the sequence  $G = 1, 2, 3, 5, 9, 14, 23, \dots$  : the representation of 8 is 1100 but neither 110 nor 11 are in  $L_G$ .

**Remark 5.29.** The above computations also open the way for the computation of  $\text{CP}_G$  that would be independent from the PCE hypothesis. From (34) and (35) follows:

$$\int_{\mathcal{K}_G} \text{cp}_G d\mu_G = \sum_{k \geq 0} (k+1) \mu_G(D_k) = \sum_{k \geq 0} (k+1) \left( \mu_G([g_k]) - \sum_{m \in I(k)} \mu_G([g_m]) \right) . \quad (44)$$

Instead of using the measure of  $D_k$  for every  $k$ , it is more efficient to compute the sum in (44) ‘layer by layer’ so to speak. If we invert the relation  $I$ , that is, if we write  $J(m) = \{k \mid m \in I(k)\}$ ,  $J(m)$  is a singleton for every  $m$  since  $g_{J(m)}$  is the *longest* right-factor of  $g_m$  in  $\text{Maxlg}(L_G)$ . The contribution to the sum of the ‘layer’  $[g_k]$  will be  $(k+1) - (J(k)+1) = k - J(k)$ . Since  $g_0 = \varepsilon$  and  $\mu_G([\varepsilon]) = 1$ , we then have:

$$\int_{\mathcal{K}_G} \text{cp}_G d\mu_G = 1 + \sum_{k \geq 1} (k - J(k)) \mu_G([g_k]) . \quad (45)$$

In [3], a machinery has been developed for computing the measure of the cylinders  $[g_k]$  which then would allow one to obtain the value of the carry propagation without the PCE hypothesis and the results of Sec. 3. Some examples of the usage of (45) are given below.

## 5.4 Beta-numeration

Let  $\beta > 1$  be a real number. The definition of a GNS associated with  $\beta$  — due to Bertrand–Mathis [11] — goes in three steps: the definition of the  $\beta$ -*expansion*



of real numbers, the one of *quasi-greedy*  $\beta$ -expansion of 1, and finally the one of the basis  $G_\beta$ .

For any real number  $x$ , let us denote by  $\{x\}$  the *fractional part* of  $x$ , that is,  $\{x\} = x - \lfloor x \rfloor$ . In [30], Rényi proposed the following greedy algorithm for any  $x \in [0, 1]$ : let  $r_0 = x$  and, for every  $i \geq 1$ , let  $x_i = \lfloor \beta r_{i-1} \rfloor$  and  $r_i = \{\beta r_{i-1}\}$ . Then,

$$x = \sum_{i=1}^{+\infty} x_i \beta^{-i} \quad \text{with} \quad \forall i \geq 1 \quad x_i \in A_\beta = \{0, \dots, \lceil \beta \rceil - 1\} . \quad (46)$$

The sequence  $d_\beta(x) = (x_i)_{i \geq 1}$  is called the  $\beta$ -*expansion* of  $x$ . Seen as a *right* infinite word of  $A_\beta^\omega$ , it is the *greatest* in the lexicographic ordering of  $A_\beta^\omega$  for which (46) holds. When the expansion ends in infinitely many 0's, it is said to be *finite* (and the 0's are omitted). If  $x$  is greater than 1, the same algorithm is used for  $x\beta^{-k}$  such that  $x\beta^{-k} \in [0, 1]$  and then the radix point is placed after the  $k$ -th digit; we thus obtain the  $\beta$ -expansion of  $x$  for any  $x$  in  $\mathbb{R}_+$ .

Let  $d_\beta(1) = (t_n)_{n \geq 1}$  be the  $\beta$ -expansion of 1. We define the *infinite word*  $d_\beta^*(1)$ , called the *quasi-greedy expansion* of 1, in the following way. If  $d_\beta(1)$  is infinite, then  $d_\beta^*(1) = d_\beta(1)$ . If  $d_\beta(1)$  is finite, of the form  $d_\beta(1) = t_1 \cdots t_m$ ,  $t_m \neq 0$ , then  $d_\beta^*(1) = (t_1 \cdots t_{m-1} (t_m - 1))^\omega$ . It is easy to see that  $d_\beta^*(1)$  is a  $\beta$ -representation of 1, that is, it satisfies (46) for  $x = 1$ .

**Definition 5.30** ([11]). *Let  $\beta > 1$  be a real number and  $d_\beta^*(1) = (d_i)_{i \geq 1}$  the quasi-greedy expansion of 1. The canonical greedy numeration system associated with  $\beta$  is defined by the basis  $G_\beta = (G_\ell)_{\ell \in \mathbb{N}}$  inductively defined by:*

$$G_0 = 1 \quad \text{and} \quad \forall \ell \geq 1 \quad G_\ell = d_1 G_{\ell-1} + d_2 G_{\ell-2} + \cdots + d_\ell G_0 + 1 .$$

The canonical GNS associated with  $\beta$  is exponential as asserted by the following.

**Proposition 5.31** ([11]). *Let  $\beta > 1$  be a real number and  $G_\beta = (G_\ell)_{\ell \in \mathbb{N}}$  the canonical GNS associated with  $\beta$ . There exists a real constant  $K > 0$  such that  $G_\ell \sim K \beta^\ell$ .*

It is easy to verify that  $A_\beta = A_{G_\beta}$ , but, of course, the  $G_\beta$ -representation of an integer  $n$  is not the same as the  $\beta$ -expansion of  $n$ . With a slight abuse, we nevertheless write  $L_\beta$  (rather than  $L_{G_\beta}$ ) for the representation language of  $G_\beta$ . The language  $L_\beta$  is characterized by the following.

**Proposition 5.32** ([26]). *Let  $\beta > 1$  be a real number and  $d_\beta^*(1) = (d_i)_{i \geq 1}$  the quasi-greedy expansion of 1. A word  $w = w_k \cdots w_0$  is in  $L_\beta$  if and only if for every  $i$ ,  $0 \leq i \leq k$ ,  $w_i \cdots w_0 \preceq d_1 \cdots d_{i+1}$ .*

A comprehensive survey on  $\beta$ - and  $G_\beta$ -numeration systems can be found in [17]. We now study the carry propagation in these numeration systems.

We write  $\text{CP}_\beta$  rather than  $\text{CP}_{L_\beta}$ . The last two propositions and the results of Sec. 5.3.4 immediately imply the following.

**Corollary 5.33.**

*Let  $\beta > 1$  be a real number. Then, the language  $L_\beta$  is a PCE language.*

*Proof.* (i)  $L_\beta$  is prefix-closed since, by definition of the lexicographic order, we have  $d_1 \cdots d_{j+1} \preceq d_1 \cdots d_{i+1}$  for every  $j \leq i$ .

(ii)  $L_\beta$  is extendable since if  $w$  is in  $L_\beta$ , then  $w0$  is in  $L_\beta$  as well since we have  $d_1 \cdots d_{i+1}0 \preceq d_1 \cdots d_{i+1}d_{i+2}$ .  $\square$

**Corollary 5.34.** *Let  $\beta > 1$  be a real number. Then, the carry propagation of the language  $L_\beta$  exists and is equal to:*

$$\text{CP}_\beta = \frac{\beta}{\beta - 1} .$$

The value of the carry propagation can also be computed directly from (45) according to the self-overlapping properties of the quasi-greedy expansion of 1  $d_\beta^*(1) = (d_i)_{i \geq 1}$ . We develop below two examples borrowed from [3].

**Example 5.35.** This first example is the case where the quasi-greedy expansion of 1 is such that no left factor  $d_1 \cdots d_m$  of  $d_\beta^*(1)$  has a right-factor of the form  $d_1 \cdots d_k$ ,  $k < m$  — this is the case for instance when  $d_1 > d_j$  for every  $j \geq 2$ . This implies in particular, with the notation of Remark 5.29, that  $J(k) = 0$  for all  $k \geq 1$ . In [3, Example 5], the measure of cylinders is computed for this case and expressed by the following:

$$\forall k \geq 1 \quad \mu_\beta([d_1 \cdots d_k]) = (\beta - 1)\beta^{-k-1} . \quad (47)$$

Since the derivation of the series expansion of

$$\frac{1}{\beta - 1} = \sum_{k \geq 1} \frac{1}{\beta^k} \quad \text{yields} \quad \frac{1}{(\beta - 1)^2} = \sum_{k \geq 1} \frac{k}{\beta^{k+1}} ,$$

Equations (47) and (45) together gives:

$$\text{CP}_\beta = 1 + \sum_{k \geq 1} k \mu_\beta([d_1 \cdots d_k]) = 1 + (\beta - 1) \sum_{k \geq 1} \frac{k}{\beta^{k+1}} = \frac{\beta}{\beta - 1} .$$

**Example 5.36. The Tribonacci numeration system.** Let  $\psi$  be the zero greater than 1 of the polynomial  $X^3 - X^2 - X - 1$ . Then  $d_\psi(1) = 111$  and  $d_\psi^*(1) = (110)^\omega$  ( $\psi$  is what is called below a *simple Parry number*). It follows that in this case,  $J(1) = 0$ ,  $J(2) = 1$  and  $J(k) = k - 3$  for all  $k \geq 3$ .

In [3, Example 2], the measure of cylinders is computed for this case and given by the following:

$$\mu_\psi([d_1]) = 1 - \psi^{-1} \quad \text{and} \quad \forall k \geq 2 \quad \mu_\psi([d_1 \cdots d_k]) = \psi^{-k-1} .$$

Equation (45) then becomes:

$$\begin{aligned}
\text{CP}_\psi &= 1 + \mu_\psi([d_1]) + \mu_\psi([d_1 d_2]) + 3 \sum_{k \geq 3} \mu_\psi([d_1 \cdots d_k]) \\
&= 1 + \left(1 - \frac{1}{\psi}\right) + \frac{1}{\psi^3} + 3 \sum_{k \geq 3} \frac{1}{\psi^{k+1}} = 2 - \frac{1}{\psi} + \frac{1}{\psi^3} + \frac{3}{\psi^3(\psi - 1)} \\
&= \frac{2\psi^4 - 3\psi^3 + \psi^2 + \psi + 2}{\psi^3(\psi - 1)} = \frac{\psi^4 + (\psi - 2)(\psi^3 - \psi^2 - \psi - 1)}{\psi^3(\psi - 1)} = \frac{\psi}{\psi - 1}
\end{aligned}$$

since  $\psi^3 - \psi^2 - \psi - 1 = 0$ .

It may seem frustrating that these computations of  $\text{CP}_G$  are conducted precisely in cases where the result is already known but, on the other hand, it is interesting to consider these cases where *two completely different computation methods* may be conducted (and luckily give the same result). Along the same line, we finally say a word on numeration systems which are relevant to both methods of Sec. 4 and that of Sec. 5. The latter put into light, of course, the continuity, or non-continuity, of the odometer. We begin with some more definitions and results.

**Definition 5.37** ([17]). *A real number  $\beta$  greater than 1 is called a Parry number if the  $\beta$ -expansion of 1 is finite or infinite eventually periodic. If the  $\beta$ -expansion of 1 is finite, then  $\beta$  is called a simple Parry number.*

**Proposition 5.38.** *Let  $\beta$  be a Parry number.*

- (i) [18] *The language  $L_\beta$  is rational.*
- (ii) [18] *The automaton  $\mathcal{A}_\beta$  which recognizes the language  $0^* L_\beta$  is strongly connected.*
- (iii) [23, Proposition 7.2.21]  *$\beta$  is the dominant root of the characteristic polynomial of the adjacency matrix of  $\mathcal{A}_\beta$ .*
- (iv) [19] *The odometer  $\tau_\beta$  is continuous if and only if  $\beta$  is a simple Parry number.*

It follows from (i)–(iii) that if  $\beta$  is a Parry number, then  $L_\beta$  and all its quotients are (rational, PCE, and) DEV languages with  $\beta$  as local growth rate and Theorem 4.1 yields an algebraic proof of the following particular case of Corollary 5.34.

**Corollary 5.39.** *If  $\beta$  is a Parry number, then  $\text{CP}_\beta$  exists and  $\text{CP}_\beta = \frac{\beta}{\beta - 1}$ .*

If  $\beta$  is a simple Parry number, it follows from (iv) that, conversely, the Ergodic Theorem directly implies the existence of the carry propagation of  $L_\beta$  (via Proposition 5.6).

**Example 5.40** (Example 2.5 continued). The Fibonacci numeration system is the canonical GNS associated with the golden mean  $\varphi$ . Since  $d_\varphi(1) = 11$ ,  $\varphi$  is a simple Parry number. The set of greedy expansions of the natural integers is  $L_\varphi = 1\{0, 1\}^* \setminus \{0, 1\}^* 11\{0, 1\}^* \cup \{\varepsilon\}$ . The automaton below recognizes  $0^* L_\varphi$ .

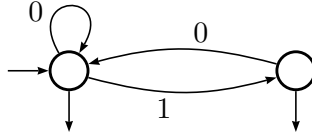
The compactification of  ${}^\omega 0 L_\varphi$  is

$$\mathcal{K}_\varphi = \mathcal{K}_{L_\varphi} = \left\{ s = (\cdots s_2 s_1 s_0) \in {}^\omega \{0, 1\} \mid \forall j \quad s_{[j, 0]} = s_j \cdots s_0 \prec (10)^\omega \right\} .$$

For instance:  $\tau_\varphi({}^\omega(01) 0(01)^n) = {}^\omega(01) 010^{2n-1}$ . On the other hand,

$$\tau_\varphi({}^\omega(01)) = \lim_{n \rightarrow \infty} \text{Succ}_\varphi((01)^n) = \lim_{n \rightarrow \infty} 10^{2n-1} = {}^\omega 0 .$$

This illustrates the fact that the odometer  $\tau_\varphi$  is continuous.



**Example 5.41** (Example 2.6 continued). The Fina numeration system is the canonical GNS associated with  $\theta = \frac{3+\sqrt{5}}{2}$ . Since  $d_\theta^*(1) = 21^\omega$ ,  $\theta$  is a Parry number which is not simple. We have:

$$\tau_\theta({}^\omega 1) = \lim_{n \rightarrow \infty} \text{Succ}_\theta(1^n) = \lim_{n \rightarrow \infty} 1^{n-1} 2 = {}^\omega 1 2 .$$

On the other hand, let us consider the sequence  $(w^{(n)})_n = ({}^\omega 0 2 1^n)_n$ . We have:  $\lim_{n \rightarrow \infty} (w^{(n)})_n = {}^\omega 1$ , and, for each  $n$ ,  $\tau_\theta(w^{(n)}) = {}^\omega 1 0^{n+1}$ , which tends to  ${}^\omega 0$ , thus the odometer  $\tau_\theta$  is not continuous.

## References

- [1] S. Akiyama, Ch. Frougny, J. Sakarovitch, Powers of rationals modulo 1 and rational base number systems, *Israel J. Math.* **168** (2008) 53–91.
- [2] A. Avizienis, Signed-digit number representations for fast parallel arithmetic, *IRE Trans. Electron. Comput.* **10** (1961) 389–400.
- [3] G. Barat, P. Grabner, Combinatorial and probabilistic properties of systems of numeration, *Ergod. Th. & Dynam. Sys.* **36** (2016) 422–457.
- [4] G. Barat, T. Downarowicz, P. Liardet, Dynamiques associées à une échelle de numération, *Acta Arith.* **103** (2002) 41–78.
- [5] E. Barcucci, R. Pinzani, M. Poneti, Exhaustive generation of some regular languages by using numeration systems, *Proc. Words 2005* (S. Brlek, Ch. Reutenauer, Eds.), *Monographies du LaCIM* **36**, UQaM (2005) 119–127.

- [6] J. Berstel, Ch. Reutenauer, *Noncommutative Rational Series with Applications*, Cambridge University Press (2011).
- [7] V. Berthé, Ch. Frougny, M. Rigo, J. Sakarovitch, On the cost and complexity of the successor function, *Proc. Words 2007* (P. Arnoux, N. Bédaride, and J. Cassaigne, Eds.), Tech. Rep., Institut de mathématiques de Luminy (Marseille) (2007) 43–56.
- [8] V. Berthé, Ch. Frougny, M. Rigo, J. Sakarovitch, The concrete complexity of the successor function. In preparation.
- [9] V. Berthé, M. Rigo, Abstract Numeration Systems and Tilings, *Proc. MFCS 2005*, Lect. Notes in Comput. Sci. **3618**, Springer (2005) 131–143.
- [10] V. Berthé, M. Rigo, Odometers on regular languages, *Theory Comput. Syst.* **40** (2007) 1–31.
- [11] A. Bertrand-Mathis, Comment écrire les nombres entiers dans une base qui n'est pas entière, *Acta Math. Acad. Sci. Hungar.* **54** (1989) 237–241.
- [12] N. Bourbaki, *Fonctions d'une variable réelle*, Éléments de mathématique, Springer (2007).
- [13] A. W. Burks, H. H. Goldstine, J. von Neumann, Preliminary discussion of the logical design of an electronic computing instrument, in *Collected Works of John von Neumann* (A. H. Taub, Ed.), Vol. 5, 34–79, Macmillan, 1963.
- [14] C.Y. Chow, J.E. Robertson, Logical design of a redundant binary adder, *Proc. 4th IEEE Symposium on Computer Arithmetic* (1978) 109–115.
- [15] A. S. Fraenkel, Systems of numeration, *Amer. Math. Monthly* **92** (1985) 105–114.
- [16] Ch. Frougny, On the sequentiality of the successor function, *Inform. and Comput.* **139** (1997) 17–38.
- [17] Ch. Frougny, J. Sakarovitch, Number representation and finite automata, Chapter 2 in *Combinatorics, Automata and Number Theory* (V. Berthé, M. Rigo, Eds), Cambridge University Press, 2010.
- [18] Ch. Frougny, B. Solomyak, On the representation of integers in linear numeration systems, in Ergodic theory of  $Z_d$  actions (Warwick, 1993–1994), 345–368, *London Math. Soc. Lecture Note Ser.* **228**, Cambridge University Press, 1996.
- [19] P. J. Grabner, P. Liardet, and R. F. Tichy, Odometers and systems of numeration, *Acta Arith.* **70** (1995) 103–123.

- [20] D. E. Knuth, The average time for carry propagation, *Nederl. Akad. Wetensch. Indag. Math.* **40** (1978) 238–242.
- [21] P. Lecomte, M. Rigo, Numeration systems on a regular language, *Theory Comput. Syst.* **34** (2001) 27–44.
- [22] P. Lecomte, M. Rigo, Abstract numeration systems, Chapter 3 in *Combinatorics, Automata and Number Theory* (V. Berthé, M. Rigo, Eds), Cambridge University Press, 2010.
- [23] M. Lothaire, *Algebraic Combinatorics on Words*, Cambridge University Press, 2002.
- [24] V. Marsault, J. Sakarovitch, The signature of rational languages, *Theoret. Computer Sci.* **658** (2017) 216–234.
- [25] V. Marsault, J. Sakarovitch, Trees and languages with periodic signature, *Indagationes Mathematicae* **28** (2017) 221–246.
- [26] W. Parry, On the  $\beta$ -expansions of real numbers, *Acta Math. Acad. Sci. Hungar.* **11** (1960) 401–416.
- [27] K. Petersen, *Ergodic Theory*, Cambridge University Press, 1983.
- [28] N. Pippenger, Analysis of carry propagation in addition: an elementary approach, *J. Algorithms* **42** (2002) 317–333.
- [29] N. Pytheas Fogg, *Substitutions in Dynamics, Arithmetics and Combinatorics* (V. Berthé, S. Ferenczi, C. Mauduit, A. Siegel, Eds.), Lect. Notes in Math. **1794**, Springer, 2005.
- [30] A. Rényi, Representations for real numbers and their ergodic properties, *Acta Math. Acad. Sci. Hungar.* **8** (1957) 477–493.
- [31] M. Rigo, *Formal Languages, Automata and Numeration Systems*, vol.1, ISTE-Wiley, 2014.
- [32] J. Sakarovitch, *Éléments de théorie des automates*, Vuibert, 2003. English corrected edition: *Elements of Automata Theory*, Cambridge University Press, 2009.
- [33] J. Shallit, Numeration systems, linear recurrences, and regular sets, *Inform. and Comput.* **113** (1994) 331–347.
- [34] A. M. Shur, Combinatorial Complexity of Regular Languages, *Proc. CSR 2008*, Lect. Notes in Comput. Sci. **5010**, Springer (2008) 289–301.