



# Mean asymptotic behaviour of radix-rational sequences and dilation equations (Extended version)

Philippe Dumas

## ► To cite this version:

Philippe Dumas. Mean asymptotic behaviour of radix-rational sequences and dilation equations (Extended version). 2008. inria-00294520v2

**HAL Id: inria-00294520**

**<https://hal.inria.fr/inria-00294520v2>**

Submitted on 21 Aug 2008

**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.

**MEAN ASYMPTOTIC BEHAVIOUR OF RADIX-RATIONAL  
SEQUENCES AND DILATION EQUATIONS  
(EXTENDED VERSION)**

PHILIPPE DUMAS

ABSTRACT. The generating series of a radix-rational sequence is a rational formal power series from formal language theory viewed through a fixed radix numeration system. For each radix-rational sequence with complex values we provide an asymptotic expansion for the sequence of its Cesàro means. The precision of the asymptotic expansion depends on the joint spectral radius of the linear representation of the sequence; the coefficients are obtained through some dilation equations. The proofs are based on elementary linear algebra.

CONTENTS

1. Introduction	2
2. Radix-rational series and dilation equations	4
2.1. Radix-rational series	4
2.2. Notations and hypotheses	5
2.3. Self-similarity	8
2.4. Wavelets and refinement schemes	10
3. Basic limit theorem	12
3.1. Uniform convergence	12
3.2. Basic theorem	13
3.3. Hölder property	14
4. Asymptotic expansion	16
4.1. Jordan vector	17
4.2. Noise	20
4.3. General case	22
5. Radix-rational sequences and periodic functions	26
5.1. Asymptotic expansion	26
5.2. Substitutions and automata	38
5.3. Linear representation insensitive to the leftmost zeroes	41
5.4. Periodicity versus pseudo-periodicity	42
References	44

---

*Date:* August 21, 2008.

*Key words and phrases.* radix-rational sequence, radix-rational series, rational formal power series, dilation equation, self-similarity, numeration system, asymptotic analysis, divide-and-conquer strategy.

## 1. INTRODUCTION

Radix-rational sequences come to light in various domains of knowledge and almost every example has been first studied for itself and by elementary methods. As a result there does not exist a general theorem about their asymptotic behaviour. Flajolet (Flajolet and Golin, 1994; Flajolet et al., 1994) has developed a method based on the analytic theory of numbers. The used frame of divide-and-conquer recurrences is wider than ours and permits to deal with many examples, but even if the underlying idea has a geometric evidence the application remains delicate.

Yet these sequences are a mere generalization of classical rational sequences, that is sequences which satisfy a linear homogeneous recurrence with constant coefficients. In the same manner they satisfy a linear homogeneous recurrence with constant coefficients but where the shift  $n \mapsto n+1$  is replaced by the pair of scaling transformations  $n \mapsto 2n$  and  $n \mapsto 2n+1$  (or more generally  $n \mapsto Bn+r$ ,  $0 \leq r < B$ , if the used radix is  $B \geq 2$ ). The first example which comes in mind (Trollope, 1968; Delange, 1975) is the binary sum-of-digits function, that is the number  $s_2(n)$  of 1's in the binary expansion of an integer  $n$ . (Drmotá and Gajdosik (1998) give an extended bibliography.) The sequence satisfies  $s_2(0) = 0$ ,  $s_2(2n) = s_2(n)$ ,  $s_2(2n+1) = s_2(n) + 1$ . It may seem to the reader that such a sequence is of limited interest, but it appears in many problems like the study of the maximum of a determinant of a  $n \times n$  matrix with entries  $\pm 1$  (Clements and Lindström, 1965) or in a merging process occurring in graph theory (McIlroy, 1974). This example have been greatly generalized with the number of occurrences of some pattern in the binary code (Boyd et al., 1989), or in the Gray code: Flajolet and Ramshaw (1980) study the average case of Batcher's odd-even merge by using the sum-of-digits function of the Gray code. Among the sequences directly related to a numeration system the Thue-Morse sequence which writes  $u(n) = (-1)^{s_2(n)}$  is certainly the one which has caused the greatest number of publications (Allouche and Shallit, 1999). There exist variants with some subsequences (Newman, 1969; Coquet, 1983) or with binary patterns (Boyd et al., 1989) other than the simple pattern 1: the Rudin-Shapiro sequence associated to the pattern 11 was initially designed to minimize the  $L^\infty$  norm of a sequence of trigonometric polynomials with coefficients  $\pm 1$  (Rudin, 1959; Shapiro, 1951). The study of the complexity of algorithms is another source of radix-rational sequences. The cost  $c_n$  of computing the  $n$ -th power of a matrix by binary powering satisfies  $c_0 = 0$ ,  $c_{2n} = c_n + 1$ ,  $c_{2n+1} = c_n + 2$ . The idea of binary powering has been re-employed by Morain and Olivos (1990) in the context of computations on an elliptic curve where the subtraction has the same cost than addition. Supowit and Reingold (1983) have used the divide-and-conquer strategy to provide heuristics for the problem of Euclidean matching and this leads them to a 4-rational sequence in the worst case. The theory of numbers is another domain which provides examples like the number of odd binomial coefficients in row  $n$  of Pascal's triangle (Stolarsky, 1977) or the number of integers which are a sum of three squares in the first  $n$  integers (Osbaldestin and Shiu, 1989).

It is the merit of Allouche and Shallit (1992, 2003) to have put all these scattered examples in a common framework. A sequence  $(u_n)$  is rational with respect to the radix  $B$  if all the sequences obtained from it by applying the scaling transforms  $n \mapsto Bn+r$ ,  $0 \leq r < B$ , remain in a finite dimensional vector space  $V$ . This leads to the idea of a linear representation with matrices of size  $d$  if  $V$  is  $d$ -dimensional. For the examples above the dimension  $d$  is usually small, say from 1 to 4, but there

exist examples where  $d$  is larger, like in the work of (Cassaigne, 1993) which uses  $d = 30$ . In such cases a general method of study is necessary.

Our aim is to provide asymptotic expansions for radix-rational sequences. Because the sequences under consideration may have a chaotic behaviour, we cannot expect an asymptotic expansion in a usual asymptotic scale for all these sequences. We provide only an asymptotic expansion in the mean, that is for the Cesàro mean

$$\frac{1}{N} \sum_{n=0}^N u_n$$

if we study the sequence  $(u_n)$ . The way we will follow is based on elementary linear algebra. This is natural because radix-rational sequences are defined by linear recurrences and after all the mean asymptotic behaviour of a radix-rational sequence originates in the asymptotic expansion of a classical rational sequence, as we shall prove. Eventually we obtain a general theorem, valid for all radix-rational sequences. Evidently the asymptotic expansions which result from this theorem are not significantly different from those of our predecessors. Roughly speaking, they have the form

$$\sum_{\alpha > \alpha_*, \ell \geq 0} N^\alpha \log_B^\ell(N) \sum_{\omega} \omega^{\lfloor \log_B N \rfloor} \Psi_{\alpha, \ell, \omega}(\log_B N) + O(N^{\alpha_*}),$$

where the  $\omega$ 's are some complex numbers of modulus 1 and the  $\Psi$ 's are 1-periodic functions. The true difference lies in the fact that the theorem has a precise framework.

The organization of the paper is as follows. In Section 2 we present the definition of a radix-rational series and a linear representation  $L$ ,  $(A_r)_{0 \leq r < B}$ ,  $C$  of such a series. We expose the link with the idea of a rational formal power series in non-commutative variables from the formal language theory. Such a series is the main object of study and a radix-rational series is only a metamorphosis of a formal power series through the interpretation of integers as their radix expansions in a given base. We address the problem of the asymptotic behaviour for  $K$  large of a vector-valued running sum

$$\mathbf{S}_K(x) = \sum_{\substack{|w|=K \\ (0.w)_B \leq x}} A_w C,$$

which depends on the length  $K$  of words and on a real number  $x \in [0, 1]$  through the interpretation of words as  $B$ -ary expansions of real numbers from  $[0, 1)$ . We give technical notations and hypotheses useful for this study. Particularly we recall the idea of joint spectral radius for a family of matrices, because the joint spectral radius  $\lambda_*$  of a linear representation governs the precision of the asymptotic expansion we will obtain. Next we divide the running sum  $\mathbf{S}_K(x)$  by its dominant behaviour. This gives a vector-valued function  $\mathbf{F}_K(x)$  and in the limit a functional equation appears. Surprisingly we have a dilation equation and such equations have been deeply studied because they are useful in the theory of wavelets and in the theory of refinement schemes.

Section 3 is the basic part of the paper. Theorem A shows that the sequence  $(\mathbf{F}_K)$  converges uniformly towards the unique solution  $\mathbf{F}$  of the dilation equation. Moreover in the special case where  $C$  is an eigenvector of a certain matrix  $Q$  relative to an eigenvalue with modulus  $\rho$  the speed of convergence is essentially  $O((\lambda_*/\rho)^K)$ .

In Section 4 we elaborate on this point by considering generalized eigenvectors. The main result is Theorem B which gives an asymptotic expansion for  $\mathbf{S}_K(x)$  from the linear representation. The technical hypotheses used as we work out the theorem reflect in the error term of the expansion which is essentially  $O(\lambda_*^K)$ . This asymptotic expansion has coefficients which are solutions of some dilation equations.

Section 5 translates Theorem B for rational formal power series into Theorem C for radix-rational sequences. So we obtain an asymptotic expansion for the running sums of a given radix-rational sequence (or for its Cesàro mean, it is the same). The solutions of the dilation equations become functions which are practically periodic with respect to the logarithm of the index. The theorem even though it is general may give an obvious formula. A typical example is the Thue-Morse sequence for which we conclude that it is  $O(1)$ . This flaw is quite normal because the running sum of the Thue-Morse sequence is almost the sequence itself. We illustrate the result with the study of the periodic function which appears in the asymptotic expansion for the Rudin-Shapiro sequence and specifically of its symmetries. We compare our work and the work of Dumont where a similar result appears. At the end we emphasize the fact that in full generality the coefficients of the asymptotic expansion are not periodic functions but only pseudo-periodic functions.

To summarize, this paper gives a theorem, which is new and general, about the asymptotic behaviour of radix-rational sequences. Moreover it shows a link with the well developed domain of dilation equations.

## 2. RADIX-RATIONAL SERIES AND DILATION EQUATIONS

**2.1. Radix-rational series.** For an integer  $n$  whose binary expansion is the word  $n_{K-1} \dots n_0$ , with figures  $n_{K-1}, \dots, n_0$  in the set  $\mathcal{B} = \{0, 1\}$ , the number of ones is

$$s_2(n) = \sum_{k \geq 0} n_k$$

and the generating function is

$$S_2(z) = \sum_{n \geq 0} s_2(n) z^n.$$

It is easy to verify the following relationships

$$\forall n \in \mathbb{N}_{\geq 0}, \quad s_2(2n) = s_2(n), \quad s_2(2n+1) = s_2(n) + 1.$$

The constant sequence  $e = 1$  satisfies obviously

$$\forall n \in \mathbb{N}_{\geq 0}, \quad e(2n) = e(n), \quad e(2n+1) = e(n).$$

It appears that the sequences  $s_2$  and  $e$  generate a  $\mathbb{Z}_{\geq 0}$ -module which is left stable by the following linear right action of the monoid of words  $\mathcal{B}^*$ : the image of a sequence  $u$  under the action of a figure  $r \in \{0, 1\}$  is the sequence  $u.r = (u(2n+r))$ . The example leads to the following definition. We consider a radix  $B \geq 2$  and the associated alphabet  $\mathcal{B} = \{0, \dots, B-1\}$ . For a semi-ring  $\mathbb{K}$ , the monoid  $\mathcal{B}^*$ , equipped with the concatenation, operates on the  $\mathbb{K}$ -module of all sequences with values in  $\mathbb{K}$  by the map  $(u(n))_{n \geq 0} \mapsto (u(Bn+r))_{n \geq 0}$  for each figure  $r$  in  $\mathcal{B}$ .

**Definition 1.** A generating function  $U(z) = \sum_{n \geq 0} u_n z^n$  whose coefficients take their values in a semi-ring  $\mathbb{K}$  is *B-rational* (or *B-recognizable*, or *B-regular*) if the  $\mathbb{K}$ -module generated by the sequence under the right action of the monoid of

words  $\mathcal{B}^*$  is of finite type. It is radix-rational (or radix-recognizable, or radix-regular) if it is  $B$ -rational for some radix  $B$ . The sequence of coefficients  $(u_n)$  is termed in the same manner.

Allouche and Shallit (1992) named such sequences of coefficients "k-regular sequences" ( $k$  is the radix). The adjective "regular" is reminiscent of "regular language" for a computer scientist but it is meaningless for a mathematician. The expression "recognizable sequence" has the same flaw, even if the preceding definition would be more satisfying with recognizable in place of rational for a computer scientist. To the contrary "radix-rational sequence" make sense for both computer scientist and mathematician and we adopt this terminology. The name *radix-rational series* has the merit to remind that these series are a generalization of classical rational functions. These one admit a representation with only one square matrix, while  $B$ -rational series admits a representation with  $B$  square matrices, as we shall see just below.

Radix-recognizable series are a metamorphosis of recognizable formal series. Indeed, let  $e^1, \dots, e^d$  be a family of sequences which generates a module left stable under the action of  $\mathcal{B}^*$  and containing the sequence of coefficients  $u$  of a radix-rational series  $U(z)$ . Such a family will be called a generating family for the sequence  $u$  in the sequel. Each of the sequences  $e^{j.r}$ ,  $0 \leq r < B$ ,  $1 \leq j \leq d$ , writes as a linear combination  $e^{j.r} = \sum_i a_{r,i,j} e^i$ , not necessarily in a unique manner. The sequence  $u$  writes  $u = \sum_i c_i e^i$ , again not necessarily in a unique manner.

**Definition 2.** The row vector  $L = (e^j(0))$ , the matrices  $A_r = (a_{r,i,j})$ ,  $0 \leq r < B$ , and the column vector  $C = (c_i)$ , all together, is a linear representation of the series  $U(z)$  or of the sequence  $u$ .

Besides the linear representation defines a recognizable series over  $\mathcal{B}^*$  with coefficients in  $\mathbb{K}$  in the sense of formal language theory. A formal series, usually written

$$S = \sum_{w \in \mathcal{B}^*} (S, w) w,$$

is an application from  $\mathcal{B}^*$  into  $\mathbb{K}$ , which associates to a word  $w$  the coefficient  $(S, w)$  (Berstel and Reutenauer, 1988; Sakarovitch, 2005). Here we consider the formal series  $S$  defined by

$$(S, w) = LA_{w_1} \cdots A_{w_K} C$$

for a word  $w = w_1 \dots w_K$ . The sequence  $u$  is obtained by restricting the formal series to the radix  $B$  expansions of integers.

**2.2. Notations and hypotheses.** The data is a linear representation  $L$ ,  $A = (A_x)_{x \in \mathcal{X}}$ ,  $C$  of dimension  $d$  with a finite alphabet  $\mathcal{X}$  of cardinality greater or equal to 2. The coefficients of the matrices are taken from the field of complex numbers in the most general case. Up to a permutation,  $\mathcal{X}$  may be taken equal to  $\{0, 1, \dots, B-1\}$  for some integer  $B \geq 2$ . The linear representation defines first a rational formal series  $S$  and second a radix-rational series  $U$ , by restriction to the radix  $B$  expansions of the integers. To abbreviate, we write  $A_w = A_{w_1} \cdots A_{w_K}$  for  $w = w_1 \dots w_K$ , hence the writing  $(S, w) = LA_w C$ . We denote by  $u$  the sequence of coefficients of  $U$ , which means that we have  $u(n) = (S, w)$  for the integer  $n = (n_{K-1} \dots n_0)_B$  whose radix  $B$  expansion is the word  $w = n_{K-1} \dots n_0$ .

For such a given  $\mathbb{C}$ -rational formal series  $S$  we consider the running sum over words  $w$  of length  $K$  submitted to the condition that the real number with radix  $B$  expansion  $(0.w)_B$  is not greater than  $x$  in  $[0, 1]$

$$\mathbf{S}_K(x) = \sum_{\substack{|w|=K \\ (0.w)_B \leq x}} A_w C$$

for all nonnegative integer  $K$  and we want to estimate its asymptotic behaviour when  $K$  tends towards  $+\infty$ . With  $Q = A_0 + A_1 + \dots + A_{B-1}$ , it writes

$$(1) \quad \mathbf{S}_K(x) = \sum_{r_1 < x_1} A_{r_1} Q^{K-1} C + \sum_{r_2 < x_2} A_{x_1} A_{r_2} Q^{K-2} C + \sum_{r_3 < x_3} A_{x_1} A_{x_2} A_{r_3} Q^{K-3} C \\ + \dots + \sum_{r_K \leq x_K} A_{x_1} A_{x_2} \dots A_{r_K} C$$

if  $x$  admits the radix  $B$  expansion  $x = (0.x_1 x_2 \dots)_B$ . The formula renders evident the following lemma.

**Lemma 1.** *With  $Q = A_0 + A_1 + \dots + A_{B-1}$ , the sequence of running sums  $(\mathbf{S}_K)$  satisfies the recursion*

$$\mathbf{S}_{K+1}(x) = \sum_{r_1 < x_1} A_{r_1} Q^K C + A_{x_1} \mathbf{S}_K(Bx - x_1),$$

where  $x_1$  is the first figure in the radix  $B$  expansion of  $x$  in  $[0, 1]$ , with  $\mathbf{S}_0(x) = C$ .

The matrix  $Q$  is the essential component which governs the mean asymptotic behaviour of  $S$  first, and of the sequence  $u$  next. Lemma 1 leads us to consider the powers  $Q^K$  of the matrix  $Q$ . More precisely, we look at the dominant term (from the asymptotic point of view) in the vector  $Q^K C$  and we will use the following hypothesis (named (ADT) for asymptotic dominant term).

**Hypothesis (ADT)** The sequence  $(Q^K C)$  admits the asymptotic expansion

$$(2) \quad Q^K C \underset{K \rightarrow +\infty}{=} R(K)V + O(R'(K))$$

with

$$(3) \quad \frac{R(K+1)}{R(K)} \underset{K \rightarrow +\infty}{=} \rho \omega \left( 1 + O\left(\frac{1}{K}\right) \right), \quad \rho > 0, \quad |\omega| = 1, \\ \text{and} \quad R'(K) \underset{K \rightarrow +\infty}{=} R(K)O\left(\frac{1}{K}\right).$$

Necessarily the vector  $V$  is an eigenvector of  $Q$  for the eigenvalue  $\rho\omega$ .

In Section 4, we will expand the vector  $C$  over a Jordan basis, and this leads us to consider the following hypothesis (named (GEV) for generalized eigenvector). This hypothesis leads to a more particular but more precise expression of  $Q^K C$  than Hypothesis (ADT) does.

**Hypothesis (GEV)** The family  $(V^{(j)})_{0 \leq j < \nu}$  is full rank and satisfies  $QV^{(0)} = \rho\omega V^{(0)}$  and  $QV^{(j)} = \rho\omega V^{(j)} + V^{(j-1)}$  for  $j > 0$ , with  $\rho \geq 0$  and  $|\omega| = 1$ .

At occasion, we will say that  $\nu$  is the height of the generalized eigenvector  $V^{(\nu-1)}$ .

Formula (1) use products of square matrices  $A_r$ ,  $0 \leq r < B$ . A possible property to bound these products is the following (named (RSR) for rough spectral radius).

**Hypothesis (RSR)** There exists an induced norm  $\|\cdot\|$ , and a constant  $\lambda$  with  $0 < \lambda < \rho$  such that all matrices  $A_r$ ,  $0 \leq r < B$ , satisfy  $\|A_r\| \leq \lambda$ .

We will tacitly use a norm on  $\mathbb{C}^d$  and the induced norms on square matrices in order to guarantee the previous hypothesis. As a consequence we have  $\|A_{r_1} \cdots A_{r_K}\| \leq \lambda^K$  for every integer  $K$ .

Hypothesis (RSR) will prove to be useful, but it is not sufficiently well designed. So we refine it as follows. We consider all the products  $A_w$  for words  $w$  of a given length  $T$  and their norms. With the notation

$$\lambda_T = \max_{|w|=T} \|A_w\|^{1/T},$$

the joint spectral radius of the set  $A_r$ ,  $0 \leq r < B$ , is the number (Rota and Strang, 1960; Blondel, 2008)

$$\lambda_* = \lim_{T \rightarrow +\infty} \lambda_T.$$

It is known that the joint spectral radius is not greater than any of the numbers  $\lambda_T$ . Moreover  $\lambda_*$  is independent of the used induced norm. The following hypothesis (named (JSR) for joint spectral radius) is made to replace Hypothesis (RSR).

**Hypothesis (JSR)** The joint spectral radius  $\lambda_*$  of the family of matrices  $(A_r)_{0 \leq r < B}$  is smaller than the number  $\rho$ , that is  $\lambda_* < \rho$ .

It is known that  $\lambda_*$  is difficult to compute (Tsitsiklis and Blondel, 1997). For our purpose it is sufficient to find an induced norm and a  $T$  such that  $\lambda_T < \rho$ . To the sake of clarity we will use a superior index to show the used norm if necessary, like  $\lambda_T^{(1)}$  if we use the absolute maximum column norm induced by the norm of index 1 of  $\mathbb{C}^d$ . In the sequel, we will say that  $\lambda_*$  is attained if there exists an induced norm and an integer  $T$  such that  $\lambda_* = \lambda_T$ .

Besides, the joint spectral radius depends on the linear representation. To each representation is associated a finite dimensional vector subspace of the space of formal series left stable by the operators  $S \mapsto S.r^{-1} = \sum_w (S, wr)$ . The representation is reduced if the subspace is as small as possible (Berstel and Reutenauer, 1988). Evidently the smaller is the subspace the smaller is the joint spectral radius and all reduced representations provide the same  $\lambda_*$  because they are isomorphic. Hence it is better to always use a reduced representation and the joint spectral radius associated to a reduced representation depends only on the formal series; it is intrinsic. But it may be easier to compute the joint spectral radius for a non reduced representation, at the risk of obtaining a too large value.

**Example 1 [Rudin-Shapiro sequence].** The Rudin-Shapiro sequence may be defined as  $u(n) = (-1)^{e_{2;11}(n)}$  where  $e_{2;11}(n)$  is the number of (possibly overlapping) occurrences of the pattern 11 in the binary expansion of the integer  $n$  (Brillhart and Carlitz, 1970). This sequence was defined independently by Shapiro (1951) and Rudin (1959) to solve a problem of optimality about the  $L^\infty$  norm of trigonometric polynomials with coefficients  $\pm 1$ . It is 2-rational: it admits the generating family  $(u(n), u(2n+1))$  and the reduced linear representation

$$L = \begin{pmatrix} 1 & 1 \end{pmatrix}, \quad A_0 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0 & 0 \\ 1 & -1 \end{pmatrix}, \quad C = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

The matrix

$$Q = A_0 + A_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$



has two eigenvalues  $\pm\sqrt{2}$  which have the same absolute value. The vector  $Q^K C$  has expression

$$Q^K C = \frac{2^{K/2}}{4} \begin{pmatrix} (2 + 2^{1/2}) + (-1)^K (2 - 2^{1/2}) \\ 2^{1/2}(1 + (-1)^K) \end{pmatrix}$$

and Hypothesis (ADT) is not satisfied. The sequence is 4-rational too with representation (Allouche and Shallit, 2003), relative to the generating family  $(u(n), u(4n + 2))$ ,

$$L = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad A_0^{(2)} = A_0^2 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \quad A_1^{(2)} = A_0 A_1 = \begin{pmatrix} 1 & -1 \\ 0 & 0 \end{pmatrix}, \\ A_2^{(2)} = A_1 A_0 = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, \quad A_3^{(2)} = A_1^2 = \begin{pmatrix} 0 & 0 \\ -1 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

The matrix  $Q^{(2)} = A_0^2 + A_0 A_1 + A_1 A_0 + A_1^2 = (A_0 + A_1)^2 = Q^2$  has a dominant eigenvalue  $\rho = 2$  and it is evident that Hypothesis (ADT) is satisfied for this linear representation. Because  $A_0$  and  $A_1$  maps each vector of the canonical basis onto a vector of the canonical basis or its negative, we have  $\lambda_T = 1$  for every  $T \geq 1$  if we use a norm which gives the same value for both vectors of the canonical basis. Hence Hypothesis (RSR) is satisfied for the radix 4 representation above and Hypothesis (JSR) too because  $\lambda_* = 1$ .

**2.3. Self-similarity.** For any positive integer  $K$ , let us introduce the function  $\mathbf{F}_K$  from  $[0, 1]$  into  $\mathbb{C}^d$  defined by

$$\mathbf{F}_K(x) = \frac{1}{R(K)} \mathbf{S}_K(x).$$

Lemma 1 translates into the equation

$$(4) \quad \mathbf{F}_{K+1}(x) = \frac{1}{R(K+1)} \sum_{r_1 < x_1} A_{r_1} Q^K C + \frac{R(K)}{R(K+1)} A_{x_1} \mathbf{F}_K(Bx - x_1).$$

We may consider the operator  $\mathcal{L}_K$  of the space of continuous functions from  $[0, 1]$  into  $\mathbb{C}^d$  defined by

$$\mathcal{L}_K \Phi(x) = \frac{1}{R(K+1)} \sum_{r_1 < x_1} A_{r_1} Q^K C + \frac{R(K)}{R(K+1)} A_{x_1} \Phi(Bx - x_1).$$

(In all the paper  $x_1$  is the first digit of  $x \in [0, 1]$ .) Equation (4) rewrites

$$\mathbf{F}_{K+1}(x) = \mathcal{L}_K \mathbf{F}_K(x).$$

According to Hypothesis (ADT), the sequence of operators  $\mathcal{L}_K$  converges weakly towards the operator  $\mathcal{L}$  defined by

$$(5) \quad \mathcal{L}\Phi(x) = \frac{1}{\rho\omega} \sum_{r_1 < x_1} A_{r_1} V + \frac{1}{\rho\omega} A_{x_1} \Phi(Bx - x_1)$$

and we will first study the equation  $\mathcal{L}\Phi = \Phi$ .

In the sequel, the following system of equations, whose unknown is a function from the segment  $[0, 1]$  into the space  $\mathbb{C}^d$ ,

- $\Phi(0) = 0, \Phi(1) = V,$
- for every figure  $r$  of the radix  $B$  system and for  $x$  in  $[r/B, (r+1)/B),$

$$(6) \quad \Phi(x) = \frac{1}{\rho\omega} \sum_{r_1 < r} A_{r_1} V + \frac{1}{\rho\omega} A_r \Phi(Bx - r)$$

will be named *the basic dilation equation*.

**Proposition 1.** *Let  $L, (A_r)_{0 \leq r < B}, C$  be a linear representation of dimension  $d$  for the radix  $B$ . Under Hypotheses (ADT) and (RSR) the problem*

- $\Phi$  is a continuous function from the segment  $[0, 1]$  into the space  $\mathbb{C}^d,$

–  $\Phi$  is a solution of the basic dilation equation,  
has a unique solution  $\mathbf{F}$ .

Before we go further we have to do a simple remark. If we multiply the square matrices  $A_r$ ,  $0 \leq r < B$ , by a nonzero scalar  $\alpha$ , the eigenvalue  $\rho\omega$  is multiplied by  $\alpha$ , the running sum  $\mathbf{S}_K(x)$  and the dominant asymptotic behaviour  $R(K)$  are multiplied by  $\alpha^K$ . It follows that  $\mathbf{F}_K$  and the operator  $\mathcal{L}_K$  are unchanged. In the same manner the operator  $\mathcal{L}$  is not modified and the solution of the fixed point problem described in the previous proposition remains the same. This permits us to consider that the modulus 1 number  $\omega$  is equal to 1 in order to prove the assertions. Even we may assume that  $\rho\omega$  is equal to 1 but we prefer to keep in mind the modulus  $\rho$  of the eigenvalue  $\rho\omega$ . (Nevertheless see the next subsection.)

*Proof.* According to the previous remark, we may assume  $\omega = 1$  by multiplying all the square matrices  $A_r$ ,  $0 \leq r < B$ , by the conjugate number  $\bar{\omega}$ .

The space of continuous functions from  $[0, 1]$  into the space  $\mathbb{C}^d$ , equipped with the norm of the maximum  $\|\Phi\|_\infty = \max_x \|\Phi(x)\|$ , is a complete normed space. (Recall that Hypothesis (RSR) assumes that we have chosen a norm on  $\mathbb{C}^d$ .) The continuous functions  $\Phi$  which satisfy  $\Phi(0) = 0$  and  $\Phi(1) = V$  are the elements of a closed, hence complete, subspace  $\mathcal{C}$  of this complete space. The equation of the problem appears as a fixed point equation  $\Phi = \mathcal{L}\Phi$ . It is sufficient to see that the subspace  $\mathcal{C}$  is left invariant by  $\mathcal{L}$  and that  $\mathcal{L}$  is a contraction to prove the assertion.

We must verify that for a continuous  $\Phi$  in  $\mathcal{C}$  the function  $\Psi = \mathcal{L}\Phi$  is a member of  $\mathcal{C}$ . According to the piecewise definition of  $\Psi$ , we have to consider the left and right limits of  $\Psi$  at the points  $r/B$  for  $0 \leq r \leq B$ . The definition of  $\Psi$  and the continuity of  $\Phi$  give immediately

$$\begin{aligned} \Psi(0) &= \frac{1}{\rho} A_0 \Phi(0) = 0, \\ \Psi(1-0) &= \frac{1}{\rho} \sum_{0 \leq s < B'} A_s V + \frac{1}{\rho} A_{B'} V = \frac{1}{\rho} QV = V, \quad \Psi(1) = V, \end{aligned}$$

and for  $0 < r < B$

$$\begin{aligned} \Psi\left(\frac{r}{B} + 0\right) &= \Psi\left(\frac{r}{B}\right) = \frac{1}{\rho} \sum_{0 \leq s < r} A_s V, \\ \Psi\left(\frac{r}{B} - 0\right) &= \frac{1}{\rho} \sum_{0 \leq s < r-1} A_s V + \frac{1}{\rho} A_s \Phi(1) = \frac{1}{\rho} \sum_{0 \leq s < r} A_s V. \end{aligned}$$

The constraints are satisfied and the subspace  $\mathcal{C}$  is stable.

If we have two functions  $\Phi_1$  and  $\Phi_2$  in  $\mathcal{C}$ , let  $\Psi_1$  and  $\Psi_2$  be their images by  $\mathcal{L}$ . From  $\Psi_1(x) - \Psi_2(x) = (1/\rho)A_r(\Phi_1(Bx - r) - \Phi_2(Bx - r))$  follows the inequality  $\|\Psi_1 - \Psi_2\| \leq (\lambda/\rho)\|\Phi_1 - \Phi_2\|$  because the norm of each matrix  $A_r$  is bounded by  $\lambda$ . As a consequence of Hypothesis (RSR) the operator  $\mathcal{L}$  is a contraction.  $\square$

In fact Hypotheses (ADT) and (RSR) are not necessary to conclude that the solution of the basic dilation equation is unique. A drop of regularity is sufficient.

**Lemma 2.** *The basic dilation equation may have only one solution under the sole hypothesis  $\rho > 0$ ,  $|\omega| = 1$  if we ask for a function continuous on the right.*

*Proof.* For a  $B$ -adic number, that is a number  $x$  whose radix  $B$  expansion is finite, the dilation equation gives the value  $F(x)$  because the recursion formula provided by the dilation equation terminates on the basic case  $x = 0$ . But the set of  $B$ -adic numbers is dense in  $[0, 1]$  and the function is assumed to be right continuous at every point. Hence it is completely determined.  $\square$

**Example 2 [Regular self-similar functions].** Often the functional equations like (6) are presented as leading necessarily to chaotic functions, but some very regular functions may satisfy such a self-similarity property. As an example consider the sequence with takes value 1 on all the multiple of 3 and 0 for the others integers. It is rational in the classical sense and its generating function is rational with poles which are all roots of the unity. As a consequence (Allouche and Shallit, 2003, Th. 16.4.3, p. 446) the sequence is rational with respect to every radix. Here is a binary linear representation (Sakarovitch, 2005, p. 6),

$$L = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}, \quad A_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

The system satisfied by  $\mathbf{F}$  is

$$\begin{cases} F_1(x) = \frac{1}{2}F_1(2x), \\ F_2(x) = \frac{1}{2}F_3(2x), \\ F_3(x) = \frac{1}{2}F_2(2x), \end{cases} \quad \text{for } 0 \leq x < \frac{1}{2}; \quad \begin{cases} F_1(x) = \frac{1}{2} + \frac{1}{2}F_2(2x-1), \\ F_2(x) = \frac{1}{2} + \frac{1}{2}F_1(2x-1), \\ F_3(x) = \frac{1}{2} + \frac{1}{2}F_3(2x-1). \end{cases} \quad \text{for } 0 \leq x < 1.$$

We find immediately the solution  $\mathbf{F}(x) = \begin{pmatrix} x & x & x \end{pmatrix}^{\text{tr}}$ .

Dinsenbacher and Hardin (1999) have studied the distributional solutions with a bounded support of a dilation equation. The idea is to use an antiderivative of sufficiently high order  $n$ . This makes contracting the operator behind the equation.

**2.4. Wavelets and refinement schemes.** The basic dilation equation enters into the domain of what is called a *two-scale difference equation*, namely

$$\varphi(x) = \sum_{n \in \mathbb{Z}} c_n \varphi(2x - n).$$

(For the sake of simplicity, we limit ourselves to radix  $B = 2$  in this subsection.) These equations have been heavily studied because they appear in the theory of wavelets to define a *scale function* and in the theory of refinement schemes of computer graphics to define a *refinement function*. Daubechies and Lagarias (1991) provide an expository of their occurrences and a bibliography. See also (Heil and Colella, 1996).

For compactly supported wavelets the previous sum is finite and the equation may be rewritten in a way which looks like our dilation equation. We follow (Daubechies and Lagarias, 1992, p.1036) or (Daubechies, 1992, p. 235). The equation

$$\varphi(x) = \sum_{n=0}^N c_n \varphi(2x - n)$$

is translated into an equation

$$\Phi(x) = \begin{cases} T_0 \Phi(2x) & \text{if } 0 \leq x \leq 1/2, \\ T_1 \Phi(2x-1) & \text{if } 1/2 \leq x \leq 1, \end{cases}$$

with a vector-valued unknown function

$$\Phi(x) = \begin{pmatrix} \varphi(x) & \varphi(x+1) & \varphi(x+2) & \dots & \varphi(x+N-1) \end{pmatrix}^{\text{tr}}$$

and square matrices  $T_0 = (c_{2i-j-1})_{1 \leq i, j \leq N}$ ,  $T_1 = (c_{2i-j})_{1 \leq i, j \leq N}$  (it is assumed  $c_n = 0$  for  $n$  outside  $[0, N]$ ). Scalars  $c_n$  are constrained by  $\sum_m c_{2m} = \sum_n c_{2n+1} = 1$  and the number 1 is an eigenvalue for both  $T_0$  and  $T_1$ , and for  $M = (c_{2i-j})_{1 \leq i, j \leq N-1}$ . We consider a right eigenvector  $W = (w_i)_{1 \leq i \leq N-1}$  for  $M$  (an additional condition imposes that 1 is a simple eigenvalue, so there is essentially only one possibility for  $W$ ). We extend  $W$  by  $w_0 = 0$ ,  $w_N = 0$  and define  $V = (v_i)_{1 \leq i \leq N}$  by  $v_i = w_{i-1}$  for  $1 \leq i \leq N$ , so that  $W$  is an eigenvector for  $T_0$  and  $V$  is an eigenvector for  $T_1$  relative to the eigenvalue 1. Boundary conditions are added to the equation, namely  $\Phi(0) = W$ ,  $\Phi(1) = V$ , which guarantee the well definition of the equation and the continuity of the solution  $\varphi$  (under some conditions on the  $c_n$ 's).

Besides our dilation equation writes

$$\mathbf{F}(x) = \begin{cases} T_0 \mathbf{F}(2x) & \text{if } 0 \leq x \leq 1/2, \\ T_0 V + T_1 \mathbf{F}(2x - 1) & \text{if } 1/2 \leq x \leq 1, \end{cases}$$

where matrices  $T_0$  and  $T_1$  are defined by

$$T_0 = \frac{1}{\rho\omega} A_0, \quad T_1 = \frac{1}{\rho\omega} A_1,$$

and  $V$  is an eigenvector for  $T_0 + T_1$  relative to the eigenvalue 1. Here the boundary conditions are  $\mathbf{F}(0) = 0$  and  $\mathbf{F}(1) = V$ .

Evidently both equations are very akin. The two-scale difference equation for the scale function of wavelets is homogeneous while our dilation equation is not, but their linear parts are the same. Inhomogeneous dilation equations have been studied (Strang and Zhou, 1998), because they are useful in the construction of wavelets on a finite interval and of multiwavelets. Nevertheless this contrast is an illusion: if we extend the function  $\mathbf{F}$  as a continuous function over the whole real line by making it constant on  $(-\infty, 0]$  with value 0 and constant on  $[1, +\infty)$  with value  $V$ , the dilation equation rewrites

$$\mathbf{F}(x) = T_0 \mathbf{F}(2x) + T_1 \mathbf{F}(2x - 1)$$

for  $x$  real. The writing of the dilation equation by cases is more concrete, but the homogeneous version above is more compact and more practical for proofs. So we will made use of the following convention (named (HEC) for homogeneous equation convention) at occasion.

**Convention** (HEC) The solution of a basic dilation equation is extended to the whole real line as a continuous function constant on the left of 0 and on the right of 1.

The eigenvalue 1 appears in both cases. The boundary conditions are not of the same form and the matrices  $T_0$  and  $T_1$  for the wavelets have a very special structure, while the matrices  $A_0$  and  $A_1$  of a linear representation are not constrained in our study. As a result, even if the computations are not exactly the same, the ideas which work for wavelets work too for rational series. For example, the basic idea of the *cascade algorithm* (Daubechies, 1992, § 6.5, p. 206) or of the refinement schemes (Dyn and Levin, 2002), which computes the value of a scale function for dyadic numbers, applies here. We have yet used it in Lemma 2, and evidently to draw the pictures in the paper. In the same manner, the key point for the existence and uniqueness of the solution of these two-scale difference equations is the occurrence of a contracting operator (Daubechies and Lagarias, 1991, Sec. 4). The same idea have appeared before in (Hutchinson, 1981) which describes a construction of

self-similar parameterized curves (and the construction of the sequence  $(\mathbf{G}_K)$  in the proof of Lemma 3 below is of the type described in its § 3.5).

### 3. BASIC LIMIT THEOREM

**3.1. Uniform convergence.** We are now in position to prove a first result about the asymptotic behaviour of the running sums  $\mathbf{S}_K$ .

**Proposition 2.** *Under Hypotheses (ADT) and (RSR), the sequence  $(\mathbf{F}_K)$  converges uniformly towards the function  $\mathbf{F}$  defined in Proposition 1.*

*Proof.* To obtain a uniform convergence, we take care that all the big oh with respect to  $K$  are uniform with respect to  $x$ . Also we may assume  $\omega = 1$  as in the proof of Proposition 1.

We first note that the sequence  $(\mathbf{F}_K(x))$  is uniformly bounded. Actually let  $\varepsilon > 0$  chosen such that

$$k = \frac{\lambda}{\rho} \frac{1}{1 - \varepsilon} < 1.$$

There exists a  $K_0$  such that for  $K \geq K_0$  we have the inequality

$$\left| \frac{1}{\rho} \frac{R(K+1)}{R(K)} - 1 \right| < \varepsilon.$$

The triangular inequality applied to the right member of Formula (4) provides an inequality

$$\|\mathbf{F}_{K+1}\|_\infty \leq k(\gamma + \|\mathbf{F}_K\|_\infty),$$

where  $\gamma$  is a constant. By induction we obtain

$$\|\mathbf{F}_K\|_\infty \leq \frac{k\gamma}{1-k} + \|\mathbf{F}_{K_0}\|_\infty$$

for  $K \geq K_0$ . Hence the sequence  $(\|\mathbf{F}_K\|_\infty)$  is bounded.

Formula (4) and Formula (6) (applied to  $\mathbf{F}(x)$ ) provide

$$(7) \quad \mathbf{F}_{K+1}(x) - \mathbf{F}(x) = \sum_{r_1 < x_1} A_{r_1} \left( \frac{1}{R(K+1)} Q^K C - \frac{1}{\rho} V \right) + A_{x_1} \left( \frac{R(K)}{R(K+1)} \mathbf{F}_K(Bx - x_1) - \frac{1}{\rho} \mathbf{F}(Bx - x_1) \right).$$

The writing  $Q^K C = R(K)V + R(K)O(1/K)$  gives

$$\begin{aligned} \mathbf{F}_{K+1}(x) - \mathbf{F}(x) &= \sum_{r_1 < x_1} A_{r_1} O\left(\frac{1}{K}\right) + A_{x_1} \mathbf{F}_K(Bx - x_1) O\left(\frac{1}{K}\right) \\ &\quad + \frac{1}{\rho} A_{x_1} (\mathbf{F}_K(Bx - x_1) - \mathbf{F}(Bx - x_1)) \end{aligned}$$

and next, with the uniformly bounded character of  $(\mathbf{F}_K(x))$ ,

$$\|\mathbf{F}_{K+1} - \mathbf{F}\|_\infty \leq O\left(\frac{1}{K}\right) + \frac{\lambda}{\rho} \|\mathbf{F}_K - \mathbf{F}\|_\infty.$$

By induction, we find  $\|\mathbf{F}_K - \mathbf{F}\|_\infty = O(1/K)$ . If the constant implied in the big oh of the last but one formula is  $\gamma$ , we may take  $2\gamma/(1 - \lambda/\rho)$  for the constant in the big oh of the last formula.  $\square$

We may be more precise about the speed of convergence, but we content ourselves with a particular case (which will prove to be basic).

**Corollary 1.** *Under Hypotheses (ADT), (RSR), if  $C$  is an eigenvector associated to the eigenvalue  $\rho\omega$ , the speed of convergence is  $\|\mathbf{F}_K - \mathbf{F}\|_\infty = O((\lambda/\rho)^K)$ .*

*Proof.* We do not assume here  $|\omega| = 1$  hence  $\rho$  must be replaced by  $\rho\omega$ . By substituting  $Q^K C = R(K)V + O(R'(K))$  into Formula (7), we obtain

$$(8) \quad \|\mathbf{F}_{K+1} - \mathbf{F}\|_\infty \leq O\left(\frac{R(K)}{R(K+1)} - \frac{1}{\rho\omega}\right) + O\left(\frac{R'(K)}{R(K+1)}\right) + \frac{\lambda}{\rho} \|\mathbf{F}_K - \mathbf{F}\|_\infty.$$

But if  $C$  is an eigenvector, we have  $R(K+1)/R(K) = \rho\omega$  and  $R'(K) = 0$  and Formula (8) becomes  $\|\mathbf{F}_{K+1} - \mathbf{F}\|_\infty \leq (\lambda/\rho) \|\mathbf{F}_K - \mathbf{F}\|_\infty$ , hence the conclusion.  $\square$

**3.2. Basic theorem.** Let us assume that we group the letters into pairs, which means that we consider only words of even length. We obtain a new formal series  $S_2$ . It is rational and admits a linear representation whose square matrices are the  $B^2$  products  $A_r A_s$  with  $0 \leq r, s < B$ . The associated matrix  $Q$  becomes  $Q_2 = Q^2$ . (See Ex. 1.) The sequence of running sums  $(\mathbf{S}_K)$  is changed into its subsequence  $(\mathbf{S}_{2K})$  and it is the same thing for the sequence  $(\mathbf{F}_K)$ . In the same manner we may group the letters by  $T$  for a given  $T$ . This leads us to consider the subsequence  $(\mathbf{F}_{KT})$  and the power  $Q^T$ .

In order that Proposition 2 applies to a power of matrix  $Q$ , we have to consider all products  $A_w$  for words  $w$  of a given length and their norms. Hypothesis (RSR) will be satisfied for some power  $Q^T$  if we impose Hypothesis (JSR). If  $\varepsilon > 0$  is chosen such that  $\lambda_*(1 + \varepsilon) < \rho$  and  $T$  is sufficiently large, we thus have  $\|A_w\| \leq (\lambda_T)^T \leq \lambda_*^T (1 + \varepsilon)^T < \rho^T$  for all words  $w$  of length  $T$ . Hence the subsequence  $(\mathbf{F}_{KT})$  is convergent. We will show that not only this subsequence is convergent but the sequence  $(\mathbf{F}_K)$  is convergent.

**Theorem A.** *Under Hypotheses (ADT) and (JSR), the sequence  $(\mathbf{F}_K)$  converges uniformly towards the unique continuous solution  $\mathbf{F}$  of the basic dilation equation (6).*

*Proof.* As we have explained just before the wording of the theorem, the sequence  $(\mathbf{F}_{KT})$  converges uniformly to a function  $\mathbf{F}^0$  for some  $T$ . Let us consider the sequence  $(\mathbf{F}_{KT+1})$ . According to Lemma 1, we have

$$\frac{1}{R(KT+1)} \mathbf{S}_{KT+1}(x) = \frac{1}{R(KT+1)} \sum_{r_1 < x_1} A_{r_1} Q^{KT} C + \frac{1}{R(KT+1)} \mathbf{S}_{KT}(Bx - x_1),$$

hence

$$\begin{aligned} \mathbf{F}_{KT+1}(x) &= \frac{1}{R(KT+1)} \sum_{r_1 < x_1} A_{r_1} (R(KT)V + O(R'(KT))) \\ &\quad + \frac{R(KT)}{R(KT+1)} \mathbf{F}_{KT}(Bx - x_1). \end{aligned}$$

Because  $(\mathbf{F}_{KT})$  converges uniformly towards  $\mathbf{F}^0$ , we see that  $(\mathbf{F}_{KT+1})$  converges uniformly towards  $\mathbf{F}^1 = \mathcal{L}\mathbf{F}^0$ . Repeating the argument, we conclude that each subsequence  $(\mathbf{F}_{KT+s})$  converges uniformly towards  $\mathbf{F}^s = \mathcal{L}^s \mathbf{F}^0$  for  $s \geq 1$ . But each of these functions satisfies  $\mathbf{F}^s = \mathcal{L}^T \mathbf{F}^s$ , because  $\mathbf{F}^0$  is a fixed point of  $\mathcal{L}^T$ . Since

the unique solution of this equation is  $\mathbf{F}^0$ , all these functions are equal. Henceforth the sequence  $(\mathbf{F}_K)$  is uniformly convergent towards  $\mathbf{F}^0$ . Because of the equality  $\mathbf{F}^0 = \mathbf{F}^1$  the function  $\mathbf{F}^0$  is the unique solution of the equation  $\Phi = \mathcal{L}\Phi$ . (The uniqueness of the solution for the last equation is guaranteed by Lemma 2.)  $\square$

The following case will prove to be useful in Section 4, where it will be extended.

**Corollary 2.** *Under Hypotheses (ADT) and (JSR), if  $C$  is an eigenvector associated to the eigenvalue  $\rho\omega$ , the speed of convergence is  $\|\mathbf{F}_K - \mathbf{F}\|_\infty = O((\lambda/\rho)^K)$  for every  $\lambda > \lambda_*$ . If  $\lambda_*$  is attained we may replace  $\lambda$  by  $\lambda_*$ .*

*Proof.* Corollary 1 gives the speed of convergence for the subsequence  $(\mathbf{F}_{KT})$  and we obtain  $\|\mathbf{F}_{KT} - \mathbf{F}\|_\infty = O(r_T^K)$  with  $r_T = \lambda_T^T/\rho^T$  because we use the power  $Q^T$  in place of  $Q$ . This gives  $\|\mathbf{F}_{KT+s} - \mathbf{F}\|_\infty = O(r_T^K)$  for  $0 \leq s < T$  because the operator  $\mathcal{L}$  is continuous and because there is a finite number of subsequences to consider. We obtain  $\|\mathbf{F}_K - \mathbf{F}\|_\infty = O(r_T^{K/T})$  and the formula above because  $T$  was chosen such that  $\lambda_T \leq \lambda_*(1 + \varepsilon)$  for an arbitrary  $\varepsilon > 0$ . In case  $\lambda_*$  is attained the positive number  $\varepsilon$  is useless.  $\square$

**Example 3 [Worst mergesort sequence].** Mergesort is a comparison based sorting algorithm which uses the recursive divide-and-conquer strategy. The list to be sorted is split into two lists of almost equal size; both are sorted by mergesort (there is nothing to do for a list with only one item); both sorted lists are merged. Taking into account the number of comparisons, the cost of mergesort for a list of  $n$  items is

$$u_n = u_{\lfloor n/2 \rfloor} + u_{\lceil n/2 \rceil} + m_n, \quad u_1 = 0,$$

where  $m_n$  is the cost of merging two sorted lists with  $\lfloor n/2 \rfloor$  and  $\lceil n/2 \rceil$  elements (Flajolet and Golin, 1994). The cost of mergesort in the worst case (that is  $m_n = n - 1$ ) writes  $u_n = \sum_{k=1}^n \lceil \log_2 k \rceil$  and the sequence  $(v_n)$  defined by  $v_0 = 0$  and  $v_n = \lceil \log_2 n \rceil$  for  $n \geq 1$  is a 2-rational sequence which admits the representation, relative to the basis  $(v(n), v(2n), v(2n+1), v(4n+2))$ ,

$$L = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}^{\text{tr}}, \quad A_0 = \begin{pmatrix} 0 & -1 & -1 & -1 \\ 1 & 2 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & -1 & -1 \\ 1 & 0 & -1 & -2 \\ 0 & 1 & 2 & 3 \end{pmatrix}, \quad C = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

The matrix  $Q = A_0 + A_1$  has two eigenvalues, namely 2 and 1, which are double. A computation, based on the Jordan reduced form of  $Q$ , gives

$$Q^K C = 2^K K \begin{pmatrix} 0 \\ 0 \\ -1 \\ 1 \end{pmatrix} + 2^K \begin{pmatrix} 0 \\ 0 \\ 2 \\ -1 \end{pmatrix} + K \begin{pmatrix} -1 \\ 1 \\ 1 \\ -1 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ -2 \\ 1 \end{pmatrix}$$

and Hypothesis (ADT) works with

$$\rho = 2, \quad \omega = 1, \quad R(K) = 2^K K, \quad V = (0 \ 0 \ -1 \ 1)^{\text{tr}}, \quad R'(K) = 2^K.$$

With the absolute maximum column norm, we find that the maximal norm of the matrices  $A_w$  with  $w$  of length 4 is 9. This gives  $\lambda_4^{(1)} \simeq 1.73$  and Hypothesis (JSR) is satisfied. As a consequence  $(\mathbf{F}_K)$  converges uniformly towards  $\mathbf{F}$  which is nothing but

$$\mathbf{F}(x) = (0 \ 0 \ -x \ x)^{\text{tr}}.$$

**3.3. Hölder property.** Let us recall that a function  $f$  from the real line into a normed space is Hölder with exponent  $\alpha$  if it satisfies  $\|f(y) - f(x)\| \leq c|y - x|^\alpha$  for some constant  $c$ . Under the hypotheses of Theorem A the function  $\mathbf{F}$  is not only continuous but Hölder. Such a result is classical in the study of dilation

equations and the proof below is a replay of point (7) in the proof of Th. 2.2 from (Daubechies and Lagarias, 1992). See also (Rioul, 1992).

**Lemma 3.** *Under Hypotheses (ADT) and (RSR) the function  $\mathbf{F}$  is Hölder with exponent  $\log_B(\rho/\lambda)$ .*

The inequality  $\lambda < \rho$  is assumed, but we have also  $\rho \leq \|Q\| \leq B\lambda$  by triangular inequality. This gives bounds  $0 < \log_B(\rho/\lambda) \leq 1$  for the exponent, as expected.

*Proof.* Let us introduce the sequence  $\mathbf{G}_K$  defined by  $\mathbf{G}_0(x) = xV$  and  $\mathbf{G}_{K+1} = \mathcal{L}\mathbf{G}_K$ , where  $\mathcal{L}$  is the operator defined by Eq. (5) and used in the basic dilation equation (6). The function  $\mathbf{G}_0$  is linear and thanks to the properties of the operator  $\mathcal{L}$ , all the functions  $\mathbf{G}_K$  are piecewise linear and continuous. More precisely  $\mathbf{G}_K$  is linear in each of the interval  $[k/B^K, (k+1)/B^K]$ ,  $0 \leq k < B^K$ .

Let  $s$  and  $t$  be two real numbers which are situated in one of these intervals  $[k/B^K, (k+1)/B^K]$ ,  $0 \leq k < B^K$ , and satisfy  $1/B^{K+1} \leq |t-s| < 1/B^K$ . Their radix  $B$  expansions have the same first  $K$  figures, but the  $(K+1)$ th figures are different. We may write  $s = (0.u_1 \dots u_K s_1 \dots)_B$ ,  $t = (0.u_1 \dots u_K t_1 \dots)_B$  and  $s' = (0.s_1 \dots)_B$ ,  $t' = (0.t_1 \dots)_B$ . According to the definition of  $\mathcal{L}$ , we have

$$\mathbf{G}_K(t) - \mathbf{G}_K(s) = \frac{1}{(\rho\omega)^K} A_{u_1} \dots A_{u_K} (t' - s')V.$$

Consequently we obtain

$$\|\mathbf{G}_K(t) - \mathbf{G}_K(s)\| \leq \left(\frac{\lambda}{\rho}\right)^K \|V\| \leq B \|V\| \left(\frac{B\lambda}{\rho}\right)^K |t-s|,$$

using the hypothesis  $1/B^{K+1} \leq |t-s|$ . Because  $\mathbf{G}_K$  is piecewise linear this inequality is valid for all pairs  $(s, t)$  taken from  $[0, 1]$ . Let us insist on that point. The function  $\Delta : (s, t) \mapsto \|\mathbf{G}_K(t) - \mathbf{G}_K(s)\| / |t-s|$  is defined on the square  $[0, 1]^2$  minus its diagonal. It gives the mean speed of the parameterized curve  $\mathbf{G}_K$  on the interval whose ends are  $s$  and  $t$ . According to the previous computation the quantity  $B \|V\| (B\lambda/\rho)^K$  is an upper bound for the mean speed  $\Delta$  on each square  $[k/B^K, (k+1)/B^K]^2$  (minus their diagonals),  $0 \leq k < B^K$ , because  $\mathbf{G}_K$  is piecewise linear and  $\Delta$  is constant on such a square. Again because  $\mathbf{G}_K$  is piecewise linear these particular squares give the larger value of  $\Delta$ . Henceforth the previous upper bound is valid on the entire square  $[0, 1]^2$  (minus its diagonal).

Let  $x$  and  $y$  be two real numbers from  $[0, 1]$  which satisfy  $1/B^{\nu+1} < |y-x| \leq 1/B^\nu$  for some integer  $\nu$ . The sequence  $(\mathbf{G}_K)$  converges uniformly towards  $\mathbf{F}$  and we may guarantee  $\|\mathbf{G}_\nu - \mathbf{F}\|_\infty \leq \gamma(\lambda/\rho)^\nu$  for some constant  $\gamma$  because the operator  $\mathcal{L}$  is a contraction with ratio  $\lambda/\rho$ . Using the triangular inequality we obtain

$$\|\mathbf{F}(y) - \mathbf{F}(x)\| \leq 2\gamma \left(\frac{\lambda}{\rho}\right)^\nu + B \|V\| \left(\frac{B\lambda}{\rho}\right)^\nu |y-x| \leq (2\gamma + B \|V\|) \left(\frac{\lambda}{\rho}\right)^\nu,$$

the last inequality coming from the hypothesis  $|y-x| \leq 1/B^\nu$ . But the inequality  $1/B^\nu < B|y-x|$  provides an inequality of the desired form with the help of the formula  $\lambda/\rho = (1/B)^{\log_B(\rho/\lambda)}$ .  $\square$

**Proposition 3.** *Under Hypotheses (ADT) and (JSR) the function  $\mathbf{F}$  is Hölder with exponent  $\log_B(\rho/\lambda)$  for every  $\lambda > \lambda_*$ . Moreover  $\lambda = \lambda_*$  may be used if  $\lambda_*$  is attained.*



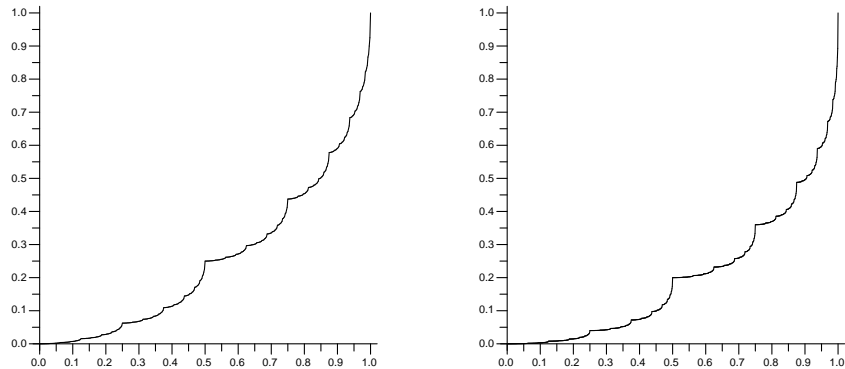


FIGURE 1. Limit probability distributions which come from a Bernoulli process described in Ex. 4.

*Proof.* If  $\lambda > \lambda_*$  there is a  $T$  such that  $\lambda \geq \lambda_T$  and we may assume  $\lambda = \lambda_T$  for the proof because the smaller is  $\lambda$ , the stronger is the constraint imposed by the Hölder property (the exponent  $\log_B(\rho/\lambda)$  is a decreasing function of  $\lambda$ ). We replace the radix  $B$  by  $B^T$ . This changes  $\rho$  into  $\rho^T$  and  $\lambda$  into  $\lambda^T$ , but  $\log_{B^T}(\rho^T/\lambda^T) = \log_B(\rho/\lambda)$  remains the same and the previous lemma gives the conclusion.  $\square$

**Example 4 [Billingsley's distribution function].** Billingsley (1995, Ex. 31.1, p. 407) studied the random variable  $X = \sum_{n \geq 0} X_n/2^n$  where  $X_n$  is the result of a coin tossing with probabilities  $p_0$  and  $p_1$  for  $X_n = 0$  and  $X_n = 1$  respectively. This defines a rational series with dimension 1, radix 2 and a linear representation

$$L = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad A_0 = \begin{pmatrix} p_0 \\ 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} p_1 \\ 1 \end{pmatrix}, \quad C = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

with  $0 < p_0, p_1 < 1$ ,  $p_0 + p_1 = 1$ . We have  $Q = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ ,  $\rho = 1$ ,  $V = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ ,  $R(K) = 1$ ,  $R'(K) = 0$ ,  $\lambda_* = \max(p_0, p_1)$ . The distribution function  $F$  is the limit function of Theorem A and it is Hölder with exponent  $\log_2(1/\lambda_*)$ . We illustrate the example (Fig. 1, left-hand side) with  $p_0 = 1/4$ ,  $p_1 = 3/4$  as in (Billingsley, 1995, p. 408) and the exponent is  $\log_2(4/3) \simeq 0.415$ , and (Fig. 1, right-hand side) with  $p_0 = 1/5$ ,  $p_1 = 4/5$  and the exponent is  $\log_2(4/5) \simeq 0.322$ . Following the same way as in (Dumas et al., 2007, § 4.3), it is possible to show that, assuming  $p_0 \leq p_1$ , at every dyadic point the best Hölder exponent is  $\log_2(1/p_0)$  on the right-hand side and  $\log_2(1/\lambda_*)$  on the left-hand side. Except in the case  $p_0 = p_1 = 1/2$ , this gives  $\log_2(1/p_0) > 1$  and this explains the horizontal tangents on the right-hand side that we see on the pictures. But we will not elaborate upon this point because the argument is very simple and assumes a linear representation with nonnegative coefficients while (Daubechies and Lagarias, 1992) has provided a general approach to this subject.

#### 4. ASYMPTOTIC EXPANSION

To a linear representation  $L$ ,  $(A_r)_{0 \leq r < B}$ ,  $C$ , we associate a vector-valued sequence of running sums

$$\mathbf{S}_K(x) = \sum_{\substack{|w|=K \\ (0.w)_B \leq x}} A_w C.$$

We want to derive an asymptotic expansion for the sequence  $(\mathbf{S}_K)$  and as a by-product an asymptotic expansion for the sequence  $(S_K) = (L\mathbf{S}_K)$ . Theorem A and

its corollaries provide a one term expansion

$$\mathbf{S}_K(x) \underset{K \rightarrow +\infty}{=} R(K)\mathbf{F}(x) + o(R(K)).$$

In order to obtain a more precise expansion, we generalize the result of Corollary 2, which deals with eigenvectors of  $Q$ . We find a basis which reduces the matrix  $Q = \sum_{0 \leq r < B} A_r$  to its Jordan normal form and we decompose the column vector  $C$  on this basis. The sequence  $(\mathbf{S}_K)$  appears as a sum of sequences associated to the vectors of the basis. We have to discuss according to the eigenvalue of  $Q$  relative to each vector. If the modulus of an eigenvalue is larger than  $\lambda_*$  we have to consider a generalized eigenvector or a Jordan vector and this will be made in the next section. After that it remains only to consider the case where the modulus is less or equal to the joint spectral radius  $\lambda_*$ . This case produces a noise which will enter in the error term of the asymptotic expansion.

**4.1. Jordan vector.** We use a family of linearly independent vectors  $(V^{(j)})_{0 \leq j < \nu}$  which satisfies  $QV^{(j)} = \rho\omega V^{(j)} + V^{(j-1)}$  for  $j > 0$  and  $QV^{(0)} = \rho\omega V^{(0)}$ , with  $\rho > \lambda_*$  and  $|\omega| = 1$ , that is we assume Hypothesis (GEV) with Hypothesis (JSR). As a consequence  $Q$  induces on the vector space generated by  $V^{(0)}, V^{(1)}, \dots, V^{(\nu-1)}$  the usual Jordan block of size  $\nu$ ,

$$(9) \quad J_{\rho\omega} = \begin{pmatrix} \rho\omega & 1 & & & \\ & \rho\omega & 1 & & \\ & & \ddots & \ddots & \\ & & & & 1 \\ & & & & \rho\omega \end{pmatrix}.$$

This gives immediately

$$(10) \quad Q^K V^{(\nu-1)} = \binom{K}{\nu-1} (\rho\omega)^{K-\nu+1} V^{(0)} + \binom{K}{\nu-2} (\rho\omega)^{K-\nu+2} V^{(1)} + \dots \\ + \binom{K}{1} (\rho\omega)^{K-1} V^{(\nu-2)} + (\rho\omega)^K V^{(\nu-1)}.$$

We claim that the running sum associated to the vector  $V^{(\nu-1)}$

$$\mathbf{S}_K(x) = \sum_{\substack{|w|=K \\ (0.w)_B \leq x}} A_w V^{(\nu-1)}$$

admits an asymptotic expansion of the form

$$\mathbf{S}_K(x) \underset{K \rightarrow +\infty}{=} \binom{K}{\nu-1} (\rho\omega)^{K-\nu+1} \mathbf{F}^{(0)}(x) + \binom{K}{\nu-2} (\rho\omega)^{K-\nu+2} \mathbf{F}^{(1)}(x) + \dots \\ + \binom{K}{1} (\rho\omega)^{K-1} \mathbf{F}^{(\nu-2)}(x) + (\rho\omega)^K \mathbf{F}^{(\nu-1)}(x) + \text{error}_K(x),$$

where the  $\mathbf{F}^{(j)}$ 's are continuous functions from  $[0, 1]$  into  $\mathbb{C}^d$  and the error term is  $O(\lambda^K)$  for every  $\lambda > \lambda_*$ .

The polynomial function  $K \mapsto (\rho\omega)^{-K} Q^K V^{(\nu-1)}$  has a unique writing on the basis  $\binom{K}{j}$ ,  $0 \leq j < \nu$ , and we have necessarily  $\mathbf{F}^{(j)}(1) = V^{(j)}$  for  $0 \leq j < \nu$ . In

the same manner the uniqueness of asymptotic expansions shows that the family  $(\mathbf{F}^{(j)})_{0 \leq j < \nu}$  must satisfy the system of dilation equations,

$$(11) \quad \left\{ \begin{array}{l} \rho\omega\mathbf{F}^{(0)}(x) = \sum_{r_1 < x_1} A_{r_1} V^{(0)} + A_{x_1} \mathbf{F}^{(0)}(Bx - x_1), \\ \mathbf{F}^{(0)}(x) + \rho\omega\mathbf{F}^{(1)}(x) = \sum_{r_1 < x_1} A_{r_1} V^{(1)} + A_{x_1} \mathbf{F}^{(1)}(Bx - x_1), \\ \vdots \\ \mathbf{F}^{(\nu-2)}(x) + \rho\omega\mathbf{F}^{(\nu-1)}(x) = \sum_{r_1 < x_1} A_{r_1} V^{(\nu-1)} + A_{x_1} \mathbf{F}^{(\nu-1)}(Bx - x_1). \end{array} \right.$$

We obtain these formulæ by substituting the asymptotic expansion into the functional equation of Lemma 1. Evidently the first equation of the system is nothing but the basic dilation equation (6). To obtain the proposition we have in mind, we will follow the same path as in Sections 3.1–3.3. For the sake of clarity we cut the proof into lemmas.

**Lemma 4.** *Under Hypotheses (JSR) and (GEV), System (11) has a unique solution  $(\mathbf{F}^{(j)})_{0 \leq j < \nu}$  in the space  $\Pi_{0 \leq j < \nu} \mathcal{C}^{(j)}$  where  $\mathcal{C}^{(j)}$  is the space of continuous functions from  $[0, 1]$  into  $\mathbb{C}^d$  which satisfy  $\mathbf{F}^{(j)}(0) = 0$ ,  $\mathbf{F}^{(j)}(1) = V^{(j)}$  for  $0 \leq j < \nu$ .*

*Proof.* It is possible to consider one equation at a time, but it is more enlightening to deal globally with the system. Let us introduce the matrix  $\mathbb{F}(x)$  of type  $d \times [0, \nu]$  whose columns are the column vectors  $\mathbf{F}^{(0)}(x)$ ,  $\mathbf{F}^{(1)}(x)$ ,  $\dots$ ,  $\mathbf{F}^{(\nu-1)}(x)$ . The system writes

$$(12) \quad \mathbb{F}(x)J_{\rho\omega} = \sum_{r < x_1} A_r V + A_{x_1} \mathbb{F}(Bx - x_1),$$

where  $V$  is the matrix whose columns are the column vectors  $V^{(0)}$ ,  $V^{(1)}$ ,  $\dots$ ,  $V^{(\nu-1)}$ , and  $J_{\rho\omega}$  is the Jordan block defined by Eq. (9). Because of the positivity of  $\rho$ , the matrix  $J_{\rho\omega}$  is invertible and the system turns out to be a fixed point equation  $\mathbb{F} = \mathcal{L}\mathbb{F}$ , namely

$$\mathbb{F}(x) = \sum_{r < x_1} A_r V J_{\rho\omega}^{-1} + A_{x_1} \mathbb{F}(Bx - x_1) J_{\rho\omega}^{-1}$$

for some operator  $\mathcal{L}$ . Let  $\mu$  lie between  $\lambda_*$  and  $\rho$ , that is  $\lambda_* < \mu < \rho$ . Because the spectral radius of  $J_{\rho\omega}^{-1}$  is  $1/\rho$ , there exists an induced norm which provides  $1/\rho \leq \|J_{\rho\omega}^{-1}\| < 1/\mu$ . Next there exists an integer  $T$  which gives  $\lambda_* \leq \lambda_T < \mu$ . We consider for a while that the radix is  $B^T$ . From  $\|A_{x_1}\| \|J_{\rho\omega}^{-1}\| < \mu \times 1/\mu = 1$ , we see that the right-hand side of the previous equation turns out to be the image of  $\mathbb{F}$  by a contracting operator. We conclude as in the proof of Proposition 1 that the equation  $\mathbb{F} = \mathcal{L}^T \mathbb{F}$  has a unique continuous solution  $\mathbb{F}^{(0)}$  from  $[0, 1]$  into the space of matrices  $M_{d \times [0, \nu]}(\mathbb{C})$  which satisfies the constraints  $\mathbb{F}^{(0)}(0) = 0$ ,  $\mathbb{F}^{(0)}(1) = V$ . Next we prove that  $\mathbb{F}^{(0)}$  is the unique solution of the problem, in the same way we have finished the proof of Theorem A.  $\square$

**Lemma 5.** *Let  $\mathbf{A}_K$  be the function from  $[0, 1]$  into  $\mathbb{C}^d$  defined by*

$$\begin{aligned} \mathbf{A}_K(x) = & \binom{K}{\nu-1} (\rho\omega)^{K-\nu+1} \mathbf{F}^{(0)}(x) + \binom{K}{\nu-2} (\rho\omega)^{K-\nu+2} \mathbf{F}^{(1)}(x) + \dots \\ & + \binom{K}{1} (\rho\omega)^{K-1} \mathbf{F}^{(\nu-2)}(x) + (\rho\omega)^K \mathbf{F}^{(\nu-1)}(x) \end{aligned}$$

for each nonnegative integer  $K$ , where  $\mathbf{F}^{(0)}, \dots, \mathbf{F}^{(\nu-1)}$  are the functions whose existence and uniqueness are asserted by Lemma 4. Under Hypotheses (JSR) and (GEV), the running sum  $\mathbf{S}_K$  associated to  $V^{(\nu-1)}$  writes  $\mathbf{S}_K(x) = \mathbf{A}_K(x) + O(\lambda^K)$  for every  $\lambda > \lambda_*$  and the big oh is uniform with respect to  $x$  in  $[0, 1]$ . Moreover if  $\lambda_*$  is attained we may replace  $\lambda$  by  $\lambda_*$ .

*Proof.* With  $\text{error}_K(x) = \mathbf{S}_K(x) - \mathbf{A}_K(x)$  it is not difficult to obtain, by substitution, the recursion

$$\text{error}_{K+1}(x) = A_{x_1} \text{error}_K(Bx - x_1).$$

More precisely, we use the recursion of Lemma 1, System (11), and the fundamental formula of binomial coefficients. For  $\lambda > \lambda_*$  we choose an integer  $T$  such that  $\lambda_* \leq \lambda_T < \lambda$ . We readily obtain  $\|\text{error}_{KT}\|_\infty = O(\lambda_T^{KT})$ . Next the recursion shows that we have  $\|\text{error}_{KT+s}\|_\infty = O(\lambda_T^{KT+s})$  for  $0 \leq s < T$ , hence the result. If  $\lambda_*$  is some  $\lambda_T$ , it is useless to consider a  $\lambda > \lambda_*$ .  $\square$

As in Lemma 3, we show that the functions  $\mathbf{F}^{(j)}$ 's are somewhat regular.

**Lemma 6.** *Under Hypotheses (JSR) and (GEV), each of the functions  $\mathbf{F}^{(j)}$ ,  $0 \leq j < \nu$ , defined in Lemma 4 is Hölder with exponent  $\log_B(\rho/\lambda)$  for every  $\lambda > \lambda_*$ . If  $\lambda_*$  is attained, they are Hölder with exponent  $\log_B(\rho/\lambda_*)$ .*

*Proof.* We define a sequence of parameterized curves in the space of matrices of type  $d \times [0, \nu)$ . The first one is  $\Gamma_0 = 0$  and the others are defined by the recursion  $\Gamma_{K+1} = \mathcal{L}\Gamma_K$ , where  $\mathcal{L}$  is the operator we used in the proof of Lemma 4, namely

$$\Gamma_{K+1}(x) = \sum_{r < x_1} A_r V J_{\rho\omega}^{-1} + A_{x_1} \Gamma_K(Bx - x_1) J_{\rho\omega}^{-1}.$$

Each  $\Gamma_K$  is piecewise linear.

We choose an induced norm and a  $T$  such that  $\lambda_* \leq \lambda_T < \rho$ , and we consider that we use the radix  $B^T$ . As in the proof of Proposition 3 we observe that the sequence  $(\Gamma_{KT})$  converges uniformly towards the solution  $\mathbb{F} = (\mathbf{F}^{(j)})_{0 \leq j < \nu}$  described in Lemma 4. This permits us to show that  $\mathbb{F}$  is Hölder with exponent  $\log_B(\rho/\lambda_T)$ . The argument remains the same: the maximal speed of a piecewise linear function is the greatest uniform speed on each piece and to compute a uniform speed it is sufficient to test two distinct points of the interval under consideration.  $\square$

We summarize the obtained result.

**Proposition 4.** *Under Hypotheses (JSR) and (GEV), System (11) has a unique solution  $(\mathbf{F}^{(j)})_{0 \leq j < \nu}$  in the space of continuous functions from  $[0, 1]$  into  $\mathbb{C}^{d \times [0, \nu)}$  such that  $\mathbf{F}^{(j)}(0) = 0$ ,  $\mathbf{F}^{(j)}(1) = V^{(j)}$  for  $0 \leq j < \nu$ . Each of the functions  $\mathbf{F}^{(j)}$ ,  $0 \leq j < \nu$ , is Hölder with exponent  $\log_B(\rho/\lambda)$  for every  $\lambda > \lambda_*$ . The running sum*

$\mathbf{S}_K$  associated to  $V^{(\nu-1)}$  admits the asymptotic expansion

$$\begin{aligned} \mathbf{S}_K(x) &= \binom{K}{\nu-1} (\rho\omega)^{K-\nu+1} \mathbf{F}^{(0)}(x) + \binom{K}{\nu-2} (\rho\omega)^{K-\nu+2} \mathbf{F}^{(1)}(x) + \dots \\ &\quad + \binom{K}{1} (\rho\omega)^{K-1} \mathbf{F}^{(\nu-2)}(x) + (\rho\omega)^K \mathbf{F}^{(\nu-1)}(x) + O(\lambda^K) \end{aligned}$$

for every  $\lambda > \lambda_*$  and the big oh is uniform with respect to  $x$  in  $[0, 1]$ . Moreover if  $\lambda_*$  is attained, the functions  $\mathbf{F}^{(j)}$ 's,  $0 \leq j < \nu$ , are Hölder with exponent  $\log_B(\rho/\lambda_*)$ , and we may replace  $\lambda$  by  $\lambda_*$  in the asymptotic expansion.

Despite of its technical aspect, the obtained result is very simple: each term of the expansion of  $Q^K V^{(\nu-1)}$  is shaken by a somewhat regular vector-valued function which goes from 0 to the vector which appears at the same place in the expansion.

**4.2. Noise.** So far we did not take into account the case  $\rho \leq \lambda_*$ . Some experiments lead us to expect a chaotic behaviour for the running sums and we content ourselves with exhibiting a natural bound.

First we consider an eigenvector  $V$  of  $Q$  associated to an eigenvalue  $\rho\omega$ , with  $\rho \geq 0$  and  $|\omega| = 1$ . Note that this time the modulus  $\rho$  may be 0.

**Lemma 7.** *Let  $V$  be an eigenvector for  $Q$  with eigenvalue of modulus  $\rho \geq 0$  which satisfies  $\rho \leq \lambda_*$ . The sequence of running sums associated to  $V$  satisfies  $\|\mathbf{S}_K\|_\infty = O(\lambda^K)$  for every  $\lambda > \lambda_*$ . If  $\lambda_*$  is attained, we may replace  $O(\lambda^K)$  by  $O(\lambda_*^K)$  in case  $\rho < \lambda_*$  and by  $O(K\lambda_*^K)$  in case  $\rho = \lambda_*$ .*

*Proof.* The functional equation satisfied by the running sum associated to the eigenvector  $V$  is

$$\mathbf{S}_{K+1}(x) = \sum_{r_1 < x_1} A_{r_1} Q^K V + A_{x_1} \mathbf{S}_K(Bx - x_1),$$

that is

$$\mathbf{S}_{K+1}(x) = (\rho\omega)^K \sum_{r_1 < x_1} A_{r_1} V + A_{x_1} \mathbf{S}_K(Bx - x_1).$$

Let us assume first that we have a  $\lambda$  such that  $\rho \leq \lambda$  and  $\|A_r\| \leq \lambda$  for  $0 \leq r < B$  and for some induced norm, that is let us assume in a certain sense the converse of Hypothesis (RSR). We obtain

$$\|\mathbf{S}_{K+1}(x)\| \leq \rho^K \sum_{r_1 < x_1} \lambda \|V\| + \lambda \|\mathbf{S}_K(Bx - x_1)\|,$$

hence

$$\|\mathbf{S}_{K+1}\|_\infty \leq \rho^K B \lambda \|V\| + \lambda \|\mathbf{S}_K\|_\infty.$$

With  $\|\mathbf{S}_K\|_\infty = \lambda^K u_K$ , we have  $u_{K+1} \leq (\rho/\lambda)^K B \|V\| + u_K$ . In case  $\rho < \lambda$ , we have  $u_K \leq u_0 + B \|V\| / (1 - \rho/\lambda)$  and we conclude  $\|\mathbf{S}_K\|_\infty = O(\lambda^K)$ . In case  $\rho = \lambda$ , we have  $u_K \leq u_0 + KB \|V\|$  and we conclude  $\|\mathbf{S}_K\|_\infty = O(K\lambda^K)$ .

Second we consider the general case, which divides into two sub-cases. Let us assume that the joint spectral radius is smaller than all  $\lambda_T$ , for every induced norm. For any  $\lambda > \lambda_*$ , we may find, for a given induced norm, a  $T$  such that  $\lambda_* < \lambda_T \leq \lambda$ . We apply the previous argument to the sequence  $(\mathbf{S}_{KT})$ . This gives  $\|\mathbf{S}_{KT}\|_\infty = O(\lambda_T^{KT})$  because we have  $\rho \leq \lambda_* < \lambda_T$ . Next, Lemma 1 gives  $\|\mathbf{S}_{KT+s}\|_\infty = O(\lambda_T^{KT+s})$  for  $0 \leq s < T$ , because there is a finite number of  $s$

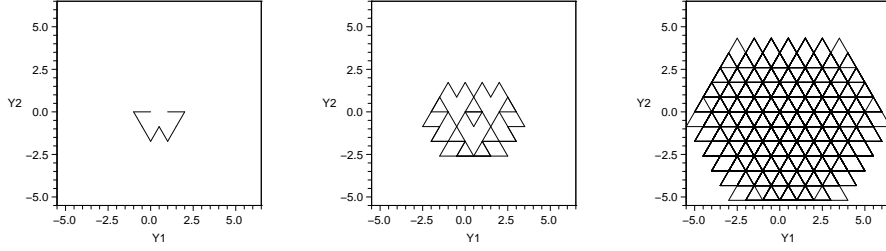


FIGURE 2. The image of the parameterized curve  $\mathbf{S}_K$  from Ex. 5 grows linearly with  $K$ . Here we see  $\mathbf{S}_3$ ,  $\mathbf{S}_6$ , and  $\mathbf{S}_{12}$ .

between 0 and  $T$ . In this way, we obtain  $\|\mathbf{S}_K\|_\infty = O(\lambda_T^K)$ , and we conclude  $\|\mathbf{S}_K\|_\infty = O(\lambda^K)$  for every  $\lambda > \lambda_*$ .

Let us assume that  $\lambda_*$  is some  $\lambda_T$  for some induced norm. In case  $0 \leq \rho < \lambda_* = \lambda_T$  the same reasoning as above, with  $\lambda_*$  in place of  $\lambda$ , gives  $\|\mathbf{S}_K\|_\infty = O(\lambda_*^K)$ . In case  $\rho = \lambda_*$  we find  $\|\mathbf{S}_{KT}\|_\infty = O(K\lambda_*^{KT})$ . As above and again because there is a finite number of integers between 0 and  $T$ , we obtain  $\|\mathbf{S}_K\|_\infty = O(K\lambda_*^K)$ .  $\square$

The next example shows that the upper bound we have found in case  $\rho = \lambda_*$  has the right order of growth.

**Example 5 [Triangular tiling].** For a real  $\vartheta$ , we consider the rotation matrix

$$R_\vartheta = \begin{pmatrix} \cos \vartheta & -\sin \vartheta \\ \sin \vartheta & \cos \vartheta \end{pmatrix}.$$

In the following we use  $V_0 = E_1$  the first vector of the canonical basis and  $V_\vartheta = R_\vartheta V_0$ . The example is based on the linear representation

$$L = \begin{pmatrix} 1 & 0 \end{pmatrix}, \quad A_0 = R_{-\vartheta}, \quad A_1 = R_\vartheta, \quad C = V_0.$$

Because we use orthogonal matrices, the joint spectral radius is  $\lambda_* = 1$ . We specialize the case to  $\vartheta = \pi/3$ , so that we have  $\rho = \lambda_*$ .

We consider the words  $u = 11$ ,  $v = 01$ , and the rational numbers  $x_{2K+2}$  and  $y_{2K}$  whose binary expansions are  $(0.uv^K)_2$  and  $(0.v^K)_2$  respectively. According to the functional equation satisfied by  $(\mathbf{S}_K)$ , we have

$$\begin{aligned} \mathbf{S}_{2K+2}(x_{2K+2}) &= R_{-\pi/3}V_0 + R_{\pi/3}(R_{-\pi/3}V_0 + R_{\pi/3}\mathbf{S}_{2K}(y_{2K})) \\ &= V_{-\pi/3} + V_0 + R_{2\pi/3}\mathbf{S}_{2K}(y_{2K}), \end{aligned}$$

$$\mathbf{S}_{2K}(y_{2K}) = R_{-\pi/3}(R_{-\pi/3}V_0 + R_{\pi/3}\mathbf{S}_{2K-2}(y_{2K-2})) = V_{-2\pi/3} + \mathbf{S}_{2K-2}(y_{2K-2}).$$

With  $\mathbf{S}_0(\varepsilon) = V_0$  ( $\varepsilon$  is the empty word), we obtain by induction  $\mathbf{S}_{2K}(y_{2K}) = KV_{-2\pi/3} + V_0$  and

$$\mathbf{S}_{2K+2}(x_{2K+2}) = (K+1)V_0 + V_{-\pi/3} + V_{2\pi/3} = (K+1)V_0.$$

Hence the  $O(K\lambda_*^K)$  we have found in Lemma 7 is satisfying.

The orbit of the parameterized curve  $\mathbf{S}_K$  is illustrated in Fig. 2. In this example the recurrences which define the sequence  $(\mathbf{S}_K)$  and the sequence  $(\mathbf{F}_K)$  are exactly the same. Moreover computing the values  $\mathbf{S}_K(x)$  for a rational  $x$  whose binary expansion has length at most  $K$  is almost the same as computing the values  $\mathbf{F}(x)$  for a hypothetical solution of the basic dilation equation. This is not really true because  $A_0V_0$  is not  $V_0$ , and the less significant bits with value 0 must be taken into account. (Look at Fig. 2. From the first to the second picture a half-turn has been applied to the little pattern of the leftmost picture, because  $A_0^3 = -I_2$ .) But  $A_0^6 = I_2$  and if we use radix  $2^6 = 64$  in place of 2 this problem disappears. The computation we have made shows that the basic dilation equation has no solution: if  $\mathbf{F}$  was a solution, it would satisfy  $\mathbf{F}(y) = V_{-2\pi/3} + \mathbf{F}(y)$  for  $y = 1/3 = (0.010101\dots)_2$ .

We generalize slightly the previous lemma into the following assertion.

**Proposition 5.** *Under Hypothesis (GEV) with  $0 \leq \rho \leq \lambda_*$ , the sequence of running sums  $(\mathbf{S}_K)$  associated to  $V^{(\nu-1)}$  satisfies  $\|\mathbf{S}_K\|_\infty = O(\lambda^K)$  for every  $\lambda > \lambda_*$ . Moreover if  $\lambda_*$  is attained, we may replace  $O(\lambda^K)$  by  $O(\lambda_*^K)$  in case  $\rho < \lambda_*$  and by  $O(\lambda_*^K K^\nu)$  otherwise.*

*Proof.* The generalized eigenvector  $V^{(\nu-1)}$  satisfies  $Q^K V^{(\nu-1)} = O(\rho^K K^{\nu-1})$ . As above we conclude  $\|\mathbf{S}_K\|_\infty = O(\lambda^K)$  for every  $\lambda > \lambda_*$ . We may refine the computation in case  $\lambda_*$  is some  $\lambda_T$ : in that case, if  $\rho < \lambda_*$  we have  $\|\mathbf{S}_K\|_\infty = O(\lambda_*^K)$ , and if  $\rho = \lambda_*$  we obtain  $\|\mathbf{S}_K\|_\infty = O(\lambda_*^K K^\nu)$ .  $\square$

**Example 6 [Powers of 2 characteristic sequence].** The sequence  $(u(n))$  which takes value 1 on the powers of 2 and 0 on the others integers admits the generating family  $(u(n), u(2n+1))$  and the linear representation

$$L = \begin{pmatrix} 0 & 1 \end{pmatrix}, \quad A_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Matrix  $Q = A_0 + A_1$  has 1 as a unique eigenvalue and the plane  $\mathbb{R}^2$  is the characteristic subspace  $\text{Ker}(Q - I_2)^2$ . Hypothesis (ADT) is satisfied with

$$\rho = 1, \quad R(K) = K, \quad V = \begin{pmatrix} 0 & 1 \end{pmatrix}^{\text{tr}}.$$

The joint spectral radius is  $\lambda_* = 1$  (consider  $A_0$ ). The fixed point equation is

$$\begin{cases} F_1(x) = F_1(2x), \\ F_2(x) = F_2(2x), \end{cases} \quad \text{for } 0 \leq x < \frac{1}{2}; \quad \begin{cases} F_1(x) = 0, \\ F_2(x) = 1 + F_1(2x-1), \end{cases} \quad \text{for } \frac{1}{2} \leq x < 1.$$

It admits the only solution (consider  $F_1$  and first the interval  $[1/2, 1[$ , next the interval  $[1/4, 1/2[$ , and so on)

$$\mathbf{F}(x) = \begin{cases} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^{\text{tr}} & \text{if } 0 < x \leq 1, \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}^{\text{tr}} & \text{if } x = 0. \end{cases}$$

(We do not forget the conditions  $\mathbf{F}(0) = 0$ ,  $\mathbf{F}(1) = V$ .) The sequence  $(\mathbf{F}_K)$  satisfies

$$\mathbf{F}_K(x) = \begin{cases} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}^{\text{tr}} & \text{if } 0 \leq x < 1/2^K, \\ \begin{pmatrix} 1/K & k/K \end{pmatrix}^{\text{tr}} & \text{if } 2^{k-1}/2^K \leq x < 2^k/2^K \text{ for } 1 \leq k \leq K, \\ \begin{pmatrix} 1/K & 1 \end{pmatrix}^{\text{tr}} & \text{if } x = 1. \end{cases}$$

It turns out that  $(\mathbf{F}_K)$  converges simply towards  $\mathbf{F}$ . This implies that we have  $\mathbf{S}_K(x) = K\mathbf{F}(x) + O(1)$  and  $\|\mathbf{S}_K\|_\infty \sim K$ .

Previous Examples 5 and 6 show that under the condition  $\rho = \lambda_*$  the sequence of running sums  $(\mathbf{S}_K)$  can or cannot define a limit function  $\mathbf{F}$  according to the case.

**4.3. General case.** The general case is obtained by expanding the vector  $C$  over a Jordan basis for  $Q$ . Let us recall that the height of a generalized eigenvector is the dimension of the subspace it spans under the action of  $Q$ . Gathering Prop. 4 and 5, we arrive at the following assertion.

**Theorem B.** *Let  $L, (A_r)_{0 \leq r < B}, C$  be a linear representation of a rational formal power series. The sequence of running sums*

$$\mathbf{S}_K(x) = \sum_{\substack{|w|=K \\ (0.w)_B \leq x}} A_w C$$

*admits an asymptotic expansion with error term  $O(\lambda^K)$  for every  $\lambda > \lambda_*$ , where  $\lambda_*$  is the joint spectral radius of the family  $(A_r)_{0 \leq r < B}$ . The used asymptotic scale is the family of sequences  $\rho^K \binom{K}{\ell}$ ,  $\rho > 0$ ,  $\ell \in \mathbb{N}_{\geq 0}$ . The error term is uniform with respect to  $x \in [0, 1]$ .*

*If  $C$  is a generalized eigenvector  $V$  for  $Q$  of height  $\nu$  associated to an eigenvalue  $\rho\omega$  of modulus  $\rho > \lambda_*$  and if  $(V^{(j)})_{0 \leq j < \nu}$  is the associated family of vectors*

such that  $V^{(\nu-1)} = V$ ,  $QV^{(j)} = \rho\omega V^{(j)} + V^{(j-1)}$  for  $j > 0$  and  $QV^{(0)} = \rho\omega V^{(0)}$ , from the expansion

$$Q^K V = \binom{K}{\nu-1} (\rho\omega)^{K-\nu+1} V^{(0)} + \binom{K}{\nu-2} (\rho\omega)^{K-\nu+2} V^{(1)} + \dots \\ + \binom{K}{1} (\rho\omega)^{K-1} V^{(\nu-2)} + (\rho\omega)^K V^{(\nu-1)}.$$

is deduced the asymptotic expansion

$$\sum_{\substack{|w|=K \\ (0.w)_B \leq x}} A_w V \underset{K \rightarrow +\infty}{=} \binom{K}{\nu-1} (\rho\omega)^{K-\nu+1} \mathbf{F}^{(0)}(x) + \binom{K}{\nu-2} (\rho\omega)^{K-\nu+2} \mathbf{F}^{(1)}(x) \\ + \dots + \binom{K}{1} (\rho\omega)^{K-1} \mathbf{F}^{(\nu-2)}(x) + (\rho\omega)^K \mathbf{F}^{(\nu-1)}(x) + O(\lambda^K)$$

where the family  $(\mathbf{F}^{(j)})_{0 \leq j < \nu}$  is the unique solution to the system of dilation equations

$$\left\{ \begin{array}{l} \rho\omega \mathbf{F}^{(0)}(x) = \sum_{r_1 < x_1} A_{r_1} V^{(0)} + A_{x_1} \mathbf{F}^{(0)}(Bx - x_1), \\ \mathbf{F}^{(0)}(x) + \rho\omega \mathbf{F}^{(1)}(x) = \sum_{r_1 < x_1} A_{r_1} V^{(1)} + A_{x_1} \mathbf{F}^{(1)}(Bx - x_1), \\ \vdots \\ \mathbf{F}^{(\nu-2)}(x) + \rho\omega \mathbf{F}^{(\nu-1)}(x) = \sum_{r_1 < x_1} A_{r_1} V^{(\nu-1)} + A_{x_1} \mathbf{F}^{(\nu-1)}(Bx - x_1). \end{array} \right.$$

Moreover if the joint spectral radius  $\lambda_*$  is attained, the error term may be improved in the following way. Let  $\mathcal{V}$  be a Jordan basis for  $Q$ . Let  $m$  be the maximal height of the generalized eigenvectors  $V$  from  $\mathcal{V}$  associated to an eigenvalue of modulus  $\lambda_*$  such that the vector  $C$  has a nonzero component over  $V$ , with  $m = 0$  if there does not exist such generalized eigenvector. The error term may be taken as  $O(\lambda_*^K K^m)$ .

The asymptotic expansion is concretely obtained by the algorithm of page 24 named **LRtoAE1** (for linear representation to asymptotic expansion). Clearly this gives an asymptotic expansion for the number-valued sum  $S_K(x) = \mathbf{L}S_K(x)$  too. It is noteworthy that two important hypotheses are made in the algorithm. First it is assumed that the joint spectral radius  $\lambda_*$  is known and even more it is assumed that we know if the joint spectral radius is attained. This is not an obstacle to the use of the algorithm. If we have at our disposal an upper bound  $\lambda_+ > \lambda_*$ , we may replace  $\lambda_*$  by  $\lambda_+$ , obtaining of course a less precise expansion. Second it is assumed that we can solve dilation equations according to Lemma 4. This is evidently wrong in full generality, but the solution is mathematically well defined and may be computed exactly over a dense subset by the cascade algorithm.

**Example 7 [Lipmaa–Wallen’s formal power series].** For a nonnegative integer  $K$ , the ring  $\mathbb{Z}/2^K\mathbb{Z}$  may be equipped with two additions. The first one is the quotient addition  $+$  which comes from the addition of the ring of integers  $\mathbb{Z}$ . The second one uses the identification of the set  $\mathbb{Z}/2^K\mathbb{Z}$  with the set  $(\mathbb{Z}/2\mathbb{Z})^K$  through the correspondence which maps a  $K$ -tuple of bits  $(\varepsilon_k)_{0 \leq k < K}$  onto the integer  $\varepsilon_0 + 2\varepsilon_1 + \dots + 2^{K-1}\varepsilon_{K-1}$ . It is the bitwise addition  $\oplus$ , or exclusive-or. The cryptanalysts Lipmaa and Wallen have studied the propagation of differences (in the sense of  $+$ ) through  $\oplus$  and more precisely the additive differential probability  $\text{adp}$  which maps a triple  $(\alpha, \beta, \gamma) \in (\mathbb{Z}/2^K\mathbb{Z})^3$  onto the probability that the difference  $((x + \alpha) \oplus (y + \beta)) - x \oplus y$



**Algorithm 1: LRtoAE1**

**Input** : A linear representation  $L$ ,  $(A_r)_{0 \leq r < B}$ ,  $C$ , and its joint spectral radius  $\lambda_*$ .

**Output**: An asymptotic expansion of the running sum  $\mathbf{S}_K(x)$  associated to the vector  $C$  when  $K$  goes to infinity at the precision  $O^-(\lambda_*^K)$  if  $\lambda_*$  is attained and  $O(\lambda^K)$  for a  $\lambda$  slightly greater than  $\lambda_*$  if not, with respect to the scale  $\rho^K \binom{K}{\ell}$ ,  $\rho > 0$ ,  $\ell \in \mathbb{N}_{\geq 0}$ .

```

1  $Q := \sum_{0 \leq r < B} A_r$ ;
2 if  $\lambda_*$  is attained then
3    $\lambda := \lambda_*$ 
4 else
5    $\lambda :=$  any number between  $\lambda_*$  and the infimum of the modulus of
   eigenvalues of  $Q$  greater than  $\lambda_*$ 
6 end
7 compute a Jordan basis  $\mathcal{V}$  for the matrix  $Q$ ;
8 expand the column vector  $C$  of the linear representation over the Jordan
   basis, as  $C = \sum_{V \in \mathcal{V}} \gamma_V V$ ;
9  $\mathcal{V}_> :=$  the set of generalized eigenvectors in  $\mathcal{V}$  such that  $\gamma_V \neq 0$  and the
   associated eigenvalue  $\rho\omega$  has a modulus  $\rho > \lambda$ ;
10 for each vector  $V$  in  $\mathcal{V}_>$  do
11    $\rho\omega :=$  the eigenvalue associated to  $V$ ;
12    $\nu :=$  the height of  $V$ ;
13   an asymptotic expansion
       
$$\mathbf{A}_{V;K}(x) := \binom{K}{\nu-1} (\rho\omega)^{K-\nu+1} \mathbf{F}^{(0)}(x) + \binom{K}{\nu-2} (\rho\omega)^{K-\nu+2} \mathbf{F}^{(1)}(x) +$$

       
$$\dots + \binom{K}{1} (\rho\omega)^{K-1} \mathbf{F}^{(\nu-2)}(x) + (\rho\omega)^K \mathbf{F}^{(\nu-1)}(x)$$

       is deduced from Proposition 4
14 end
15  $\mathbf{A}_K(x) := \sum_{V \in \mathcal{V}_>} \gamma_V \mathbf{A}_{V;K}(x)$ ;
16 error term $_K(x) := O(\lambda^K)$ ;
17 if  $\lambda_*$  is attained then
18    $\mathcal{V}_= :=$  the set of generalized eigenvectors in  $\mathcal{V}$  such that  $\gamma_V \neq 0$  and the
   associated eigenvalue  $\rho\omega$  has a modulus  $\rho = \lambda_*$ ;
19    $m := 0$ ;
20   for each  $V$  in  $\mathcal{V}_=$  do
21      $\nu :=$  the height of  $V$ ;
22      $m := \max(m, \nu)$ 
23   end
24   error term $_K(x) := O(\lambda_*^K K^m)$ 
25 end
26 return

```

$$\mathbf{S}_K(x) \underset{K \rightarrow +\infty}{=} \mathbf{A}_K(x) + \text{error term}_K(x)$$

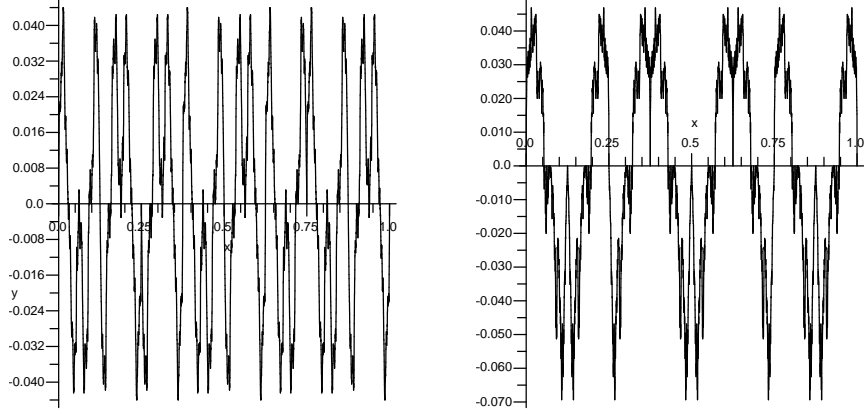


FIGURE 3. Refinement functions which originate from cryptanalysis (Ex. 7).

has value  $\gamma$  for  $x, y$  taken from  $\mathbb{Z}/2^K\mathbb{Z}$  with equiprobability. By coding every triple  $(\alpha, \beta, \gamma)$  as a word  $w$  over the alphabet  $\mathbb{Z}/8\mathbb{Z}$  (with  $w_k = 4\alpha_k + 2\beta_k + \gamma_k$  for  $0 \leq k < K$ ), Lipmaa et al. (2004) show that  $\text{adp}$  turns out to be a rational series. With  $(E_j)_{1 \leq j \leq 8}$  the canonical basis of  $\mathbb{Q}^8$ , it admits the 8-dimensional linear representation

$$L = \sum_{0 \leq r < 8} E_i^{\text{tr}}, \quad (A_r)_{0 \leq r < 8}, \quad C = E_1$$

where  $A_0$  is defined as

$$A_0 = \frac{1}{4} \begin{pmatrix} 4 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

and the other matrices  $A_r$  with  $r \neq 0$  are obtained from  $A_0$  by permuting row  $i$  with row  $i \oplus r$  and column  $j$  with column  $j \oplus r$ . Using the maximum absolute column sum norm, we find  $\lambda_* \leq 1$  and because 1 is an eigenvalue for all matrices  $A_r$ ,  $0 \leq r < 8$ , we have  $\lambda_* = 1$ .

The matrix

$$Q = A_0 + A_1 + \dots + A_7 = \frac{1}{4} \begin{pmatrix} 7 & 2 & 2 & 1 & 2 & 1 & 1 & 0 \\ 2 & 7 & 1 & 2 & 1 & 2 & 0 & 1 \\ 2 & 1 & 7 & 2 & 1 & 0 & 2 & 1 \\ 1 & 2 & 2 & 7 & 0 & 1 & 1 & 2 \\ 2 & 1 & 1 & 0 & 7 & 2 & 2 & 1 \\ 1 & 2 & 0 & 1 & 2 & 7 & 1 & 2 \\ 1 & 0 & 2 & 1 & 2 & 1 & 7 & 2 \\ 0 & 1 & 1 & 2 & 1 & 2 & 2 & 7 \end{pmatrix}$$

is diagonalizable, with eigenvalues 4, 2, 1, and eigenspaces respectively of dimension 1, 3, 4. The vector  $C = E_1$  decomposes as  $C = V_4 + V_2 + V_1$ , where

$$V_4 = \frac{1}{8} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \quad V_2 = \frac{1}{8} \begin{pmatrix} 3 \\ 1 \\ 1 \\ -1 \\ 1 \\ -1 \\ -1 \\ -3 \end{pmatrix}, \quad V_1 = \frac{1}{4} \begin{pmatrix} 2 \\ -1 \\ -1 \\ 0 \\ -1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

are respectively eigenvectors for the eigenvalues 4, 2, 1. According to Theorem B, we obtain the following asymptotic expansion (with  $F_\rho = LF_\rho$  for  $\rho = 4, 2$ )

$$\sum_{\substack{|w|=K \\ (0.w)_8 \leq x}} \text{adp}(w) \underset{K \rightarrow +\infty}{=} 4^K F_4(x) + 2^K F_2(x) + O(K),$$

where the functions  $\mathbf{F}_4$  and  $\mathbf{F}_2$  are determined by the dilation equation (as usual  $x_1$  is the first octal digits after the octal point of  $x \in [0, 1)$ )

$$\mathbf{F}_\rho(x) = \frac{1}{\rho} \sum_{r < x_1} A_r V_\rho + \frac{1}{\rho} A_{x_1} \mathbf{F}_\rho(8x - x_1), \quad \text{with } \mathbf{F}_\rho(0) = 0 \text{ and } \mathbf{F}_\rho(1) = V_\rho$$

for  $\rho = 4, 2$ . Functions  $\mathbf{F}_4$  and  $\mathbf{F}_2$  are respectively Hölder with exponent  $\log_8 4 = 2/3$  and  $\log_8 2 = 1/3$ . Function  $F_4 = LF_4$  is very near the identity and the graph of  $x \mapsto F_4(x) - x$  is drawn on the left of Fig. 3. On the right is the graph of  $F_2 = LF_2$ . Both functions have an amplitude of order about 0.05. The obtained result improves (Dumas et al., 2007) which gives only an error term  $O(2^K)$ .

## 5. RADIX-RATIONAL SEQUENCES AND PERIODIC FUNCTIONS

It is usual that sequences rational with respect to a radix introduce periodic functions in logarithmic scale. These periodic functions appear either by subtle elementary arguments, like explicit expression of the sequence with fractional part of a logarithm in base  $B$ , or by sophisticated argument which express partial sums by contour integral of a meromorphic function whose poles are regularly spaced on a vertical line. With the approach used in this paper, the introduction of periodic functions is natural. Nevertheless these functions are generally only pseudo-periodic functions and we will see why they are periodic in the previous works on the subject.

**5.1. Asymptotic expansion.** To a rational series  $S$  defined by a linear representation  $L, A_0, \dots, A_{B-1}, C$  is associated a sequence  $u$  defined in the following way: we write the integer  $n$  with respect to the radix  $B$ ,  $n = (w)_B$ , and the value of the sequence for  $n$  is the value of the rational series for the word  $w$ , that is  $u(n) = (S, w)$ . We want to evaluate the partial sums  $\sum_{0 \leq n \leq N} u(n)$  of the sequence for  $N$  large. With  $t \in [0, 1)$  and  $K$  integer, we may write  $N = B^{K+t}$ , that is  $K$  is the integer part of  $\log_B N$  and  $t$  is its fractional part. The partial sum up to  $N$  is the sum of the partial sum up to  $B^K - 1$  and a complementary term. The first appears as the sum of  $(S, w)$  over all words  $w$  of length not greater than  $K$  minus the sum over all the previous words which begin with a 0. The complementary term appears as the running sum associated to  $S$  we have studied, but without the

words of length  $K + 1$  which begin by a 0. This remark gives the following formula

$$\sum_{n \leq B^{K+t}} u(n) = \sum_{0 \leq k \leq K} \left( \sum_{|w|=k} LA_w C - \sum_{|w'|=k-1} LA_0 A_{w'} C \right) + \left( \sum_{\substack{|w|=K+1 \\ (w)_B \leq B^{K+1} B^{t-1}}} LA_w C - \sum_{|w'|=K} LA_0 A_{w'} C \right)$$

that is

$$(13) \quad \sum_{n \leq B^{K+t}} u(n) = L(I_d - A_0) \sum_{0 \leq k \leq K} Q^k C + \sum_{\substack{|w|=K+1 \\ (w)_B \leq B^{K+1} B^{t-1}}} LA_w C.$$

Just as we have considered the sums  $\mathbf{S}_K(x)$ , we introduce the vector-valued sums

$$(14) \quad \mathbf{\Sigma}_N = \sum_{(w)_B \leq N} A_w C,$$

that is

$$(15) \quad \mathbf{\Sigma}_N = (I_d - A_0) \sum_{0 \leq k \leq K} Q^k C + \sum_{\substack{|w|=K+1 \\ (w)_B \leq B^{K+1} B^{t-1}}} A_w C$$

with  $N = B^{K+t}$ ,  $0 \leq t < 1$ . As in the previous section, we decompose the column vector  $C$  over a Jordan basis for the matrix  $Q$ . Hence we consider for the rest of the section a family of linearly independent vectors  $(V^{(j)})_{0 \leq j < \nu}$  which satisfies  $QV^{(j)} = \rho\omega V^{(j)} + V^{(j-1)}$  for  $j > 0$  and  $QV^{(0)} = \rho\omega V^{(0)}$ , with  $\rho > \lambda_*$  and  $|\omega| = 1$ . In other words, we assume Hypotheses (GEV) and (JSR). We want to determine an asymptotic expansion for the running sums  $\mathbf{\Sigma}_N$  associated to  $V = V^{(\nu-1)}$ .

Formula (15) expresses the running sums of the sequence as the sum of two terms. For the first term in the right member of Formula (15), we use formulæ like Eq. (10) and the following elementary summation formula

$$(16) \quad \sum_{k=\ell}^K \binom{k}{\ell} \alpha^{k-\ell} = \begin{cases} \binom{K}{\ell+1} + \binom{K}{\ell} & \text{if } \alpha = 1, \\ \binom{K}{\ell} \frac{\alpha^{K-\ell+1}}{\alpha-1} + \sum_{j=1}^{\ell} (-1)^j \binom{K}{\ell-j} \frac{\alpha^{K-\ell+j}}{(\alpha-1)^{j+1}} + (-1)^{\ell+1} \frac{1}{(\alpha-1)^{\ell+1}} & \text{if } \alpha \neq 1. \end{cases}$$

As a consequence, the first term of Formula (15) has an asymptotic expansion in the asymptotic scale  $\rho^K \binom{K}{\ell}$ ,  $\rho > 0$ ,  $\ell \in \mathbb{N}_{\geq 0}$ .

**Lemma 8.** *Under Hypothesis (GEV) with  $C = V^{(\nu-1)}$  the first term in the right member of Formula (15) has the following expansion*

$$(17) \quad (\mathbf{I}_d - A_0) \sum_{k=0}^K Q^k V^{(\nu-1)} = \binom{K}{\nu-1} \frac{(\rho\omega)^{K-\nu+2}}{\rho\omega-1} (\mathbf{I}_d - A_0) V^{(0)} \\ + \sum_{\ell=0}^{\nu-2} \binom{K}{\ell} (\rho\omega)^{K-\ell} \left[ \frac{\rho\omega}{\rho\omega-1} (\mathbf{I}_d - A_0) V^{(\nu-\ell-1)} \right. \\ \left. + \sum_{j=\ell+1}^{\nu-1} \frac{(-1)^{j-\ell}}{(\rho\omega-1)^{j-\ell+1}} (\mathbf{I}_d - A_0) V^{(\nu-j-1)} \right] \\ + \sum_{\ell=0}^{\nu-1} (-1)^{\ell+1} \frac{1}{(\rho\omega-1)^{\ell+1}} (\mathbf{I}_d - A_0) V^{(\nu-\ell-1)}$$

in case  $\rho\omega \neq 1$  and

$$(18) \quad (\mathbf{I}_d - A_0) \sum_{k=0}^K Q^k V^{(\nu-1)} = \binom{K}{\nu} (\mathbf{I}_d - A_0) V^{(0)} \\ + \sum_{\ell=1}^{\nu-1} \binom{K}{\ell} (\mathbf{I}_d - A_0) \left[ V^{(\nu-\ell)} + V^{(\nu-\ell-1)} \right] + (\mathbf{I}_d - A_0) V^{(\nu-1)}$$

in case  $\rho\omega = 1$ .

The previous expansion is not an asymptotic expansion but it may easily be converted into such an expansion in the scale  $\rho^K \binom{K}{\ell}$ ,  $\rho > 0$ ,  $\ell \in \mathbb{N}_{\geq 0}$ , with  $K = \lfloor \log_B N \rfloor$ . The error term depends on the relative places of  $\lambda_*$ ,  $\rho$ , and 1. We will return on this point in a while.

The second term in the right member of Formula (15) is nothing but  $\mathbf{S}_{K+1}(B^{t-1})$ . Proposition 4 translates into the following result.

**Lemma 9.** *Under Hypotheses (GEV) and (JSR), the second term in the right member of Formula (15) for the running sum associated to  $V^{(\nu-1)}$  admits the following asymptotic expansion with respect to the scale  $\rho^K \binom{K}{\ell}$ ,  $\rho > 0$ ,  $\ell \in \mathbb{N}_{\geq 0}$ , with  $K = \lfloor \log_B N \rfloor$ , where the functions  $\mathbf{F}^{(\ell)}$ 's are defined in Lemma 4,*

$$(19) \quad \sum_{\substack{|w|=K+1 \\ (w)_B \leq B^{K+1} B^{t-1}}} A_w V^{(\nu-1)} \underset{N \rightarrow +\infty}{=} \binom{K}{\nu-1} (\rho\omega)^{K-\nu+2} \mathbf{F}^{(0)}(B^{t-1}) \\ + \sum_{\ell=0}^{\nu-2} \binom{K}{\ell} (\rho\omega)^{K-\ell} \left[ \rho\omega \mathbf{F}^{(\nu-\ell-1)}(B^{t-1}) + \mathbf{F}^{(\nu-\ell-2)}(B^{t-1}) \right] + O(\lambda^K).$$

for every  $\lambda > \lambda_*$  and the big oh is uniform with respect to  $t$  in  $[0, 1]$ . Moreover if  $\lambda_*$  is attained we may replace  $\lambda$  by  $\lambda_*$  in the asymptotic expansion.

*Proof.* Proposition 4 and the fundamental formula of binomial coefficients provide the expansion of  $\mathbf{S}_{K+1}(B^{t-1})$  by a mere substitution.  $\square$

Gathering the results of the previous discussion, we arrive at the following qualitative theorem.

**Theorem C.** *Let  $L$ ,  $(A_r)_{0 \leq r < B}$ ,  $C$  be a linear representation of a radix-rational sequence  $(u_n)$ . The vector-valued running sum  $\Sigma_N$  defined by Equation (14) admits an asymptotic expansion with error term  $O(N^{\log_B \lambda})$  for every  $\lambda > \lambda_*$ , where  $\lambda_*$  is the joint spectral radius of the family  $(A_r)_{0 \leq r < B}$ . If  $\lambda_*$  is attained the error term may be replaced by  $O(N^{\log_B \lambda_*})$ , where the soft big oh hides a power of  $\log N$ . The used asymptotic scale is the family of sequences  $N^\alpha(\lfloor \log_B N \rfloor)$ ,  $\alpha \in \mathbb{R}$ ,  $\ell \in \mathbb{N}_{\geq 0}$ .*

Theorem C translates concretely into Algorithm LRtoAE2 of pages 30, 31. It is a simple variation on Algorithm LRtoAE1, but is a little more complicated because it takes into account the relative positions of the parameter  $\lambda$ , which governs the error term, and of the number 1. The right member of Eq. (19) causes no problem because it is readily seen as an asymptotic expansion in the scale  $N^\alpha(\lfloor \log_B N \rfloor)$ . The right member of Eq. (17) and (18) is more annoying. In case  $\lambda > 1$ , we take into account only the eigenvalues with modulus  $\rho > 1$  and the case  $\rho\omega = 1$  of Lemma 8 cannot happen. For the case  $\rho > 1$ , we consider in the right member of Eq. (17) only the quantity

$$X = \binom{K}{\nu-1} \frac{(\rho\omega)^{K-\nu+2}}{\rho\omega-1} (\mathbf{I}_d - A_0) V^{(0)} + \sum_{\ell=0}^{\nu-2} \binom{K}{\ell} (\rho\omega)^{K-\ell} \left[ \frac{\rho\omega}{\rho\omega-1} (\mathbf{I}_d - A_0) V^{(\nu-\ell-1)} + \sum_{j=\ell+1}^{\nu-1} \frac{(-1)^{j-\ell}}{(\rho\omega-1)^{j-\ell+1}} (\mathbf{I}_d - A_0) V^{(\nu-j-1)} \right]$$

because the quantity

$$Y = \sum_{\ell=0}^{\nu-1} (-1)^{\ell+1} \frac{1}{(\rho\omega-1)^{\ell+1}} (\mathbf{I}_d - A_0) V^{(\nu-\ell-1)}$$

is  $O(1)$  and negligible in that case. (See lines 13–14 and 20–21 of Algorithm LRtoAE2.) In case  $\lambda < 1$ , all terms must be taken into account but we have to distinguish between the cases  $\rho\omega \neq 1$  and  $\rho\omega = 1$ . (See lines 13–16, 17–18, and 22–23.) Lastly in case  $\lambda = 1$ , the case  $\rho\omega = 1$  does not appear because it is assumed  $\rho > \lambda$ , but it may have an effect on the error term if  $\lambda_*$  is attained. (See lines 2–3 and 29–36.) The case  $\rho\omega \neq 1$  provide the term  $X$ . (See lines 13–14 and 20–21.) The term  $Y$ , which is  $O(1)$ , comes automatically into the error term, which is  $O(\lambda^K)$  that is  $O(1)$ .

The asymptotic expansion has essentially the form

$$\Sigma_N \underset{N \rightarrow +\infty}{=} \sum_{\rho > \lambda_*, \ell \geq 0} N^{\log_B \rho} \binom{\lfloor \log_B N \rfloor}{\ell} \sum_{\omega} \omega^{\lfloor \log_B N \rfloor} \Phi_{\rho, \ell, \omega}(\log_B N) + O(N^{\log_B \lambda_*}),$$

where  $\rho$  is the modulus of any eigenvalue of  $Q$ ,  $\omega$  is a complex number with modulus 1, and  $\ell$  is an integer related to the maximal size of the Jordan blocks associated to  $\rho\omega$ . As regards  $\Phi$ , we change the status of the variable  $t$ . It was only an abbreviation for  $\{\log_B N\}$ . Now we see it as a real variable and we substitute to it the logarithm base  $B$  of  $N$  to obtain the expression of the expansion. As a consequence the functions  $\Phi$  appear as 1-periodic functions.

**Algorithm 2:** LRtoAE2 (beginning)

**Input** : A linear representation  $L$ ,  $(A_r)_{0 \leq r < B}$ ,  $C$ , and its joint spectral radius  $\lambda_*$ .

**Output:** An asymptotic expansion of the running sum  $\Sigma_N$  associated to the vector  $C$  when  $N$  goes to infinity at the precision  $O(N^{\log_B \lambda_*})$  if  $\lambda_*$  is attained and  $O(N^{\log_B \lambda})$  for a  $\lambda$  slightly greater than  $\lambda_*$  if not, with respect to the scale  $N^\alpha (\lceil \log_B N \rceil)^\ell$ ,  $\alpha \in \mathbb{R}$ ,  $\ell \in \mathbb{N}_{\geq 0}$ .

```

1  $Q := \sum_{0 \leq r < B} A_r$ ;
2 if  $\lambda_*$  is attained then
3   |  $\lambda := \lambda_*$ 
4 else
5   |  $\lambda :=$  any number between  $\lambda_*$  and the infimum of the modulus of
   | eigenvalues of  $Q$  greater than  $\lambda_*$ 
6 end
7 compute a Jordan basis  $\mathcal{V}$  for the matrix  $Q$ ;
8 expand the column vector  $C$  of the linear representation over the Jordan
  basis, as  $C = \sum_{V \in \mathcal{V}} \gamma_V V$ ;
9  $\mathcal{V}_> :=$  the set of generalized eigenvectors in  $\mathcal{V}$  such that  $\gamma_V \neq 0$  and the
  associated eigenvalue  $\rho\omega$  has a modulus  $\rho > \lambda$ ;
10 for each vector  $V$  in  $\mathcal{V}_>$  do
11   |  $\rho\omega :=$  the eigenvalue associated to  $V$ ;
12   |  $\nu :=$  the height of  $V$ ;
13   if  $\rho\omega \neq 1$  then
14     | using Eq. (17)
15     | 
$$X := \binom{K}{\nu-1} \frac{(\rho\omega)^{K-\nu+2}}{\rho\omega-1} (\mathbf{I}_d - A_0) V^{(0)} +$$

16     | 
$$\sum_{\ell=0}^{\nu-2} \binom{K}{\ell} (\rho\omega)^{K-\ell} \left[ \frac{\rho\omega}{\rho\omega-1} (\mathbf{I}_d - A_0) V^{(\nu-\ell-1)} + \sum_{j=\ell+1}^{\nu-1} \frac{(-1)^{j-\ell}}{(\rho\omega-1)^{j-\ell+1}} (\mathbf{I}_d - A_0) V^{(\nu-j-1)} \right];$$

17     | 
$$Y := \sum_{\ell=0}^{\nu-1} (-1)^{\ell+1} \frac{1}{(\rho\omega-1)^{\ell+1}} (\mathbf{I}_d - A_0) V^{(\nu-\ell-1)};$$

18     | 
$$Z := X + Y$$

19   else
20     | using Eq. (18)
21     | 
$$Z := \binom{K}{\nu} (\mathbf{I}_d - A_0) V^{(0)} + \sum_{\ell=1}^{\nu-1} \binom{K}{\ell} (\mathbf{I}_d - A_0) [V^{(\nu-\ell)} + V^{(\nu-\ell-1)}] + (\mathbf{I}_d - A_0) V^{(\nu-1)}$$

22   end
23   if  $\lambda \geq 1$  then
24     |  $\mathbf{A}_{V;N} := X$ 
25   else
26     |  $\mathbf{A}_{V;N} := Z$ 
27   end
28   according to Eq. (19), a second term is added
29   | 
$$\mathbf{A}_{V;N} := \mathbf{A}_{V;N} + \binom{K}{\nu-1} (\rho\omega)^{K-\nu+2} \mathbf{F}^{(0)}(B^{t-1})$$

30   | 
$$+ \sum_{\ell=0}^{\nu-2} \binom{K}{\ell} (\rho\omega)^{K-\ell} [\rho\omega \mathbf{F}^{(\nu-\ell-1)}(B^{t-1}) + \mathbf{F}^{(\nu-\ell-2)}(B^{t-1})]$$

31 end
32  $\mathbf{A}_N := \sum_{V \in \mathcal{V}_>} \gamma_V \mathbf{A}_{V;N}$ ;

```

**Algorithm 2:** LRtoAE2 (end)

---

```

28 error termN := O(NlogB λ);
29 if λ* is attained then
30   |  V= := the set of generalized eigenvectors in V such that γV ≠ 0 and the
31   |  associated eigenvalue ρω has a modulus ρ = λ*;
32   |  m := 0;
33   |  for each V in V= do
34   |  |  ν := the height of V;
35   |  |  m := max(m, ν)
36   |  end
37   error termN := O(NlogB λ* logBm N)
38 end
39 return

```

---

$$\Sigma_N \underset{N \rightarrow +\infty}{=} \mathbf{A}_N + \text{error term}_N$$


---

The asymptotic expansion has variable coefficients (Bourbaki, 1976, Chapter V). The coefficients are taken from the vector space generated by sequences which write  $(\omega^{\lfloor \log_B N \rfloor} \Phi(\log_B N))$  with  $|\omega| = 1$  and  $\Phi$  a 1-periodic function.

**Example 8 [Discrepancy of the van der Corput sequence].** B ejian and Faure (1977, 1978) show that the discrepancy of the van der Corput sequence satisfies the following recursion

$$D(1) = 1, \quad D(2n) = D(n), \quad D(2n+1) = \frac{1}{2}(D(n) + D(n+1) + 1)$$

and we add  $D(0) = 0$ . Let us recall first that the (binary) van der Corput sequence is defined as follows: for an integer  $n$ , we write its binary expansion  $(n_{K-1} \dots n_1 n_0)_2$ ; we reverse it and we place it after the binary dot. The real number  $(0.n_0 n_1 \dots n_{K-1})_2$  is the value  $x_n$  of the van der Corput sequence for the integer  $n$ . Second the discrepancy of the sequence  $(x_n)$  is

$$D(n) = \sup_{0 \leq \alpha < \beta \leq 1} \left| \frac{\nu(n, \alpha, \beta)}{n} - (\beta - \alpha) \right|,$$

where  $\nu(n, \alpha, \beta)$  is the number of terms  $x_k$ ,  $1 \leq k \leq n$ , which fall in the interval  $[\alpha, \beta)$ . It measures the deviation from the uniform distribution for the sequence  $(x_n)$  (Niederreiter, 1992). We want to evaluate more precisely the mean value of the sequence  $(D(n))$  given by (B ejian and Faure, 1978, Th. 3)

$$\frac{1}{N} \sum_{n=1}^N D(n) \underset{N \rightarrow +\infty}{=} \frac{1}{4} \log_2 N + O(1).$$

The sequence  $(D(n))$  is 2-rational and admits the following linear representation

$$L = \begin{pmatrix} 0 & 1 & 1 \end{pmatrix}, \quad A_0 = \begin{pmatrix} 1 & 1/2 & 0 \\ 0 & 1/2 & 0 \\ 0 & 1/2 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 1/2 & 0 & 0 \\ 1/2 & 1 & 0 \\ 1/2 & 0 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

with respect to the generating family  $(D(n), D(n+1), 1)$ . Numerical computations lead us to think that the joint spectral radius of the representation is  $\lambda_* = 1$ . To prove this result we use the Lie algebra  $\mathfrak{g}$  generated by  $A_0$  and  $A_1$  (with the usual bracket product  $[A, B] = AB - BA$ ). The derived series of a Lie algebra  $\mathfrak{g}$  is the filtration  $\mathfrak{g} = D^0 \mathfrak{g} \supset D^1 \mathfrak{g} \supset \dots \supset D^k \mathfrak{g} \supset \dots$  defined inductively by  $D^1 \mathfrak{g} = [\mathfrak{g}, \mathfrak{g}]$ ,  $D^k \mathfrak{g} = [D^{k-1} \mathfrak{g}, D^{k-1} \mathfrak{g}]$ . The Lie algebra  $\mathfrak{g}$  is defined to be solvable if  $D^k \mathfrak{g} = \{0\}$  for some nonnegative integer  $k$ . According to Lie's theorem, if  $\mathfrak{g}$  is a solvable Lie algebra over the algebraically closed field of complex numbers there exists a change of basis matrix which makes triangular all matrices of any representation of  $\mathfrak{g}$  (Goze and Khakimdjano, 2000). As a consequence if  $\mathcal{A}$  is a finite set of real matrices which generates a solvable Lie algebra, the joint spectral radius of  $\mathcal{A}$  is the maximum of the spectral radii  $\rho(A)$  for  $A$  in  $\mathcal{A}$ . Moreover the



joint spectral radius is attained with a Euclidean norm which writes  $x \mapsto (x^{\text{tr}} P x)^{1/2}$  where  $P$  is a symmetric definite positive matrix (Blondel et al., 2005).

To apply this result it remains to compute the derived series of  $\mathfrak{g}$ . We use  $B_0 = 2A_0$  and  $B_1 = 2A_1$  to avoid denominators. Let  $\mathfrak{g}$  be the Lie algebra generated by  $B_0$  and  $B_1$ . We find at the same time a basis of this algebra and its multiplication table, namely

$[\cdot, \cdot]$	$B_0$	$B_1$	$B_2$	$B_3$
$B_0$	0	$-B_2$	$-B_3$	$-B_2$
$B_1$	$B_2$	0	$B_4$	$-B_2$
$B_2$	$B_3$	$-B_4$	0	$B_5$
$B_3$	$B_2$	$B_2$	$-B_5$	0

with

$$B_2 = [B_1, B_0] = \begin{pmatrix} -1 & 1 & 0 \\ 1 & 1 & 0 \\ -1 & 1 & 0 \end{pmatrix}, \quad B_3 = [B_2, B_0] = \begin{pmatrix} -1 & -1 & 0 \\ 1 & 1 & 0 \\ -1 & -3 & 0 \end{pmatrix}$$

and  $B_4 = 2B_0 - 2B_1 + B_3$ ,  $B_5 = -2B_0 + 2B_1 - 2B_3$ . Hence  $\mathfrak{g}$  admits the basis  $(B_0, B_1, B_2, B_3)$  and  $D^1\mathfrak{g}$  admits the basis  $(B_2, B_3, B_4)$ . Next we find that  $D^2\mathfrak{g}$  has dimension 1 and is generated by  $B_3 + B_4 = 2B_0 - 2B_1 + 2B_3$ . As a consequence  $D^3\mathfrak{g} = \{0\}$  and  $\mathfrak{g}$  is solvable. Further the joint spectral radius is  $\lambda_* = 1$  and it is attained. Because 1 is a simple eigenvalue of  $Q = A_0 + A_1$ , the error term of the asymptotic expansion for the running sum is  $O(\log N)$ .

Using the basis  $(V_1, V_2^0, V_2^1)$  with

$$V_1 = \begin{pmatrix} 1/2 \\ -1/2 \\ 0 \end{pmatrix}, \quad V_2^0 = \begin{pmatrix} 0 \\ 0 \\ 1/2 \end{pmatrix}, \quad V_2^1 = \begin{pmatrix} 1/2 \\ 1/2 \\ 0 \end{pmatrix},$$

the matrix  $Q$  takes the Jordan form

$$J = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}.$$

The vector  $C$  expands as  $C = V_1 + V_2^1$ , and because  $V_1$  is related to the eigenvalue 1 it may be neglected. We find

$$\mathbf{S}_K(x) = \frac{1}{2} 2^K K \mathbf{F}^0(x) + 2^K \mathbf{F}^1(x)$$

where  $\mathbf{F}^0$  and  $\mathbf{F}^1$  are solutions of the dilation equations

$$\mathbf{F}^0(x) = \frac{1}{2} A_0 \mathbf{F}^0(2x), \quad \text{for } 0 \leq x < 1/2,$$

$$\mathbf{F}^0(x) = \frac{1}{2} A_0 V_2^0 + \frac{1}{2} \mathbf{F}^0(2x - 1), \quad \text{for } 1/2 \leq x < 1;$$

$$\mathbf{F}^1(x) = -\frac{1}{2} \mathbf{F}^0(x) + \frac{1}{2} A_0 \mathbf{F}^0(2x), \quad \text{for } 0 \leq x < 1/2,$$

$$\mathbf{F}^1(x) = -\frac{1}{2} \mathbf{F}^0(x) + \frac{1}{2} A_0 V_2^1 + \frac{1}{2} \mathbf{F}^1(2x - 1), \quad \text{for } 1/2 \leq x < 1$$

with the boundary conditions  $\mathbf{F}^0(0) = 0$ ,  $\mathbf{F}^0(1) = V_2^0$ ,  $\mathbf{F}^1(0) = 0$ ,  $\mathbf{F}^1(1) = V_2^1$ . It is readily seen that  $\mathbf{F}^0(x) = xV_2^0$ , but  $\mathbf{F}^1$  is not explicit. Eventually we arrive at the formula

$$\frac{1}{N} \sum_{n=1}^N D(n) \underset{N \rightarrow +\infty}{=} \frac{1}{4} \log_2 N + \frac{1}{4} \left( 1 - \{t\} + 2^{3-\{t\}} \left( F_2^1(2^{\{t\}-1}) + F_3^1(2^{\{t\}-1}) \right) \right) + O\left(\frac{\log N}{N}\right).$$

Figure 4 show the empirical periodic function and the comparison between the empirical and theoretical periodic functions.

The coefficients of the asymptotic expansion of the running sum  $\Sigma_N$  inherit the properties of the coefficients of the asymptotic expansion of  $\mathbf{S}_K(x)$ . To see this we need to be more precise about the way we obtain the asymptotic expansion. Anew we use the same formalism as in Section 4.1.

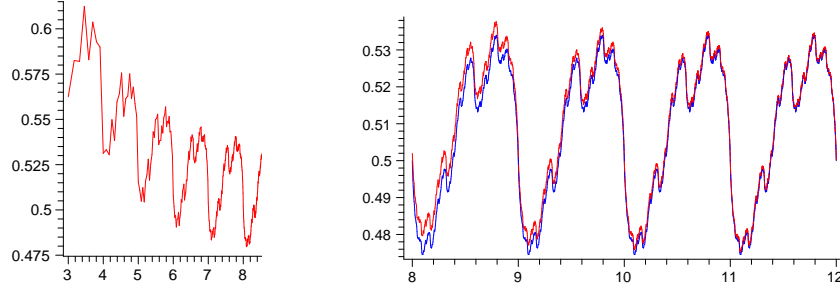


FIGURE 4. On the left the empirical (red) periodic function of Ex. 8 (mean discrepancy of the van der Corput sequence), and on the right the comparison between it and the theoretical (blue) periodic function computed by the cascade algorithm.

**Corollary 3.** *Under Hypotheses (GEV) and (JSR) the asymptotic expansion of the running sum  $\Sigma_N$  associated with  $V^{(\nu-1)}$  has coefficients which are Hölder with exponent  $\log_B(\rho/\lambda)$  for  $\lambda > \lambda_*$  and  $\lambda$  may be replaced by  $\lambda_*$  if  $\lambda_*$  is attained.*

*Proof.* The only point which is to be verified is the continuity at integers, because up to this property the Hölderian character is evident (the coefficients are expressed as combinations of solutions of dilation equations and functions which are smooth except perhaps to integers). As we have seen the expansion of  $\Sigma_N$  comes from both terms in the right member of Formula (15). The first is  $(I_d - A_0) \sum_{0 \leq k \leq K} Q^k V^{(\nu-1)}$  and we do not want to expand it here, because the asymptotic expansion varies with the relative position of  $\rho$ ,  $\lambda_*$ , and 1. Moreover this is not necessary since it depends on  $t$  only through  $K$ . The expansion of the second term is given by Formula (19). We note that this expression is merely the last column of the matrix  $\mathbb{F}(B^{t-1})J_{\rho\omega}^{K+1}$  with the notations used in the proof of Lemma 4. Hence we are considering the matrix

$$\mathbb{A}(t) = (I_d - A_0) \sum_{0 \leq k \leq K} Q^k V + \mathbb{F}(B^{t-1})J_{\rho\omega}^{K+1},$$

where  $V$  is the matrix whose columns are the column vectors  $V^{(0)}, V^{(1)}, \dots, V^{(\nu-1)}$  as in the proof of Lemma 4. The last column of the matrix  $\mathbb{A}(t)$  is the regular part of the expansion of  $\Sigma_N$  (that is without the error term), and we want to verify that  $t \mapsto \mathbb{A}(t)$  is a continuous function at integers. Let  $K_0$  be an integer. When  $t$  tends towards  $K_0$  from above, we have  $K = \lfloor t \rfloor = K_0$  and

$$\lim_{t \gtrsim K_0} \mathbb{A}(t) = (I_d - A_0) \sum_{0 \leq k \leq K_0} Q^k V + \mathbb{F}(1/B)J_{\rho\omega}^{K_0+1},$$

but according to the dilation equation (12),  $\mathbb{F}(1/B) = A_0 V J_{\rho\omega}^{-1}$  and we find

$$\lim_{t \gtrsim K_0} \mathbb{A}(t) = (I_d - A_0) \sum_{0 \leq k \leq K_0} Q^k V + A_0 V J_{\rho\omega}^{K_0}.$$

On the other side when  $t$  tends towards  $K_0$  from below, we have  $K = \lfloor t \rfloor = K_0 - 1$  and

$$\lim_{t \lesssim K_0} \mathbb{A}(t) = (I_d - A_0) \sum_{0 \leq k \leq K_0-1} Q^k V + \mathbb{F}(1)J_{\rho\omega}^{K_0} = (I_d - A_0) \sum_{0 \leq k \leq K_0-1} Q^k V + V J_{\rho\omega}^{K_0}.$$

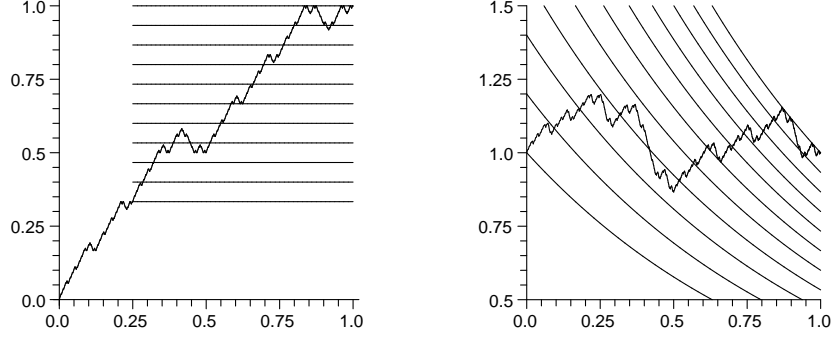


FIGURE 5. The change from the function  $F(x)$  (left) to the periodic function  $\Phi(t)$  (right) illustrated for the Coquet sequence.

The difference is

$$\lim_{t \gtrsim K_0} \mathbb{A}(t) - \lim_{t \lesssim K_0} \mathbb{A}(t) = (\mathbb{I}_d - A_0)Q^{K_0}V + (A_0 - \mathbb{I}_d)VJ_{\rho\omega}^{K_0}$$

but Hypothesis (GEV) writes  $QV = VJ_{\rho\omega}$  and we conclude that the difference is the null matrix.  $\square$

Theorem C deserves some comments. Functions which roughly write  $\Phi(t) = \omega^K \rho^{1-t} F(B^{t-1})$  have not the self-similar character of the solution  $F(x)$  of a dilation equation, because we have cut the piece of the function between 0 and  $1/B$ . Moreover it is possible to use a more ordinary scale by expanding  $\binom{\lfloor \log_B N \rfloor}{\ell} = \binom{-t + \log_B N}{\ell}$  as a polynomial in  $\log_B N$  with coefficients in  $t = \{\log_B N\}$ . But doing this we hide completely the structure of the asymptotic expansion and the dilation equations which are behind it. This is certainly the reason why these equations have not been perceived before, even if the word “fractal” is frequently employed.

**Example 9 [Coquet sequence].** The Coquet sequence (Coquet, 1983) is defined as  $u(n) = (-1)^{s_2(3n)}$ . (We recall that  $s_2(n)$  is the sum of the bits in the binary expansion of  $n$ .) It is 4-rational and it admits (with  $(u(n), u(4n+2), u(4n+3))$  as a generating family) the linear representation

$$A_0 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

$$L = (1 \ 1 \ 1), \quad A_2 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & -1 & 1 \end{pmatrix}.$$

The matrix

$$Q = A_0 + A_1 + A_2 + A_3 = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & -1 \\ 1 & -1 & 2 \end{pmatrix}$$

has as eigenvalue 3, which is double, and 0, which is simple. The joint spectral radius of the family  $(A_r)_{0 \leq r < 4}$  is  $\lambda_* = 1$ , because with the maximum sum column norm we find  $\lambda_1^{(1)} = 1$  and 1 is an eigenvalue of each matrix  $A_r$ ,  $0 \leq r < 4$ . The column vector  $C$  decomposes as  $C = V_3 + V_0$ , with

$$V_3 = \begin{pmatrix} 2/3 \\ 1/3 \\ 1/3 \end{pmatrix}, \quad V_0 = \begin{pmatrix} 1/3 \\ -1/3 \\ -1/3 \end{pmatrix}$$

and  $V_\rho$  is an eigenvector for  $\rho = 3, 0$ .

Theorem C applies and we obtain (Coquet, 1983; Flajolet et al., 1994)

$$\sum_{n \leq N} (-1)^{s_2(3n)} =_{N \rightarrow +\infty} N^{\log_4 3} 3^{1-\{t\}} F(4^{\{t\}-1}) + O(1),$$

with  $t = \log_4 N$ . The function  $F$  is the sum  $F = F_1 + F_2 + F_3$ , where  $\mathbf{F} = (F_1, F_2, F_3)$  is the unique solution of the dilation equation, written with Convention (HEC),

$$\begin{cases} F_1(x) = \frac{1}{3}F_1(4x) + \frac{1}{3}F_2(4x) + \frac{1}{3}F_3(4x) + \frac{1}{3}F_1(4x-1), \\ F_2(x) = \frac{1}{3}F_2(4x-1) - \frac{1}{3}F_3(4x-1) + \frac{1}{3}F_1(4x-2) + \frac{1}{3}F_2(4x-2), \\ F_3(x) = \frac{1}{3}F_3(4x-2) + \frac{1}{3}F_1(4x-3) - \frac{1}{3}F_2(4x-3) + \frac{1}{3}F_3(4x-3), \end{cases}$$

with the conditions  $F_1(0) = F_2(0) = F_3(0) = 0$ ,  $F_1(1) = 2/3$ ,  $F_2(1) = F_3(1) = 1/3$ . The function  $F(x)$  and the periodic function  $\Phi(t) = 3^{1-\{t\}}F(4^{\{t\}-1})$  are illustrated in Fig. 5 respectively on the left and on the right. The positive character of  $\Phi$  proves a subtle phenomenon (Newman, 1969): the number of ones in the binary expansion of the integers which are multiple of 3 is more often even than odd. Both functions are Hölder with exponent  $\log_4 3 \simeq 0.795$ . In the translation from  $F$  to  $\Phi$ , the first quarter of  $F$  is lost and  $\Phi$  has not the auto-similar character of  $F$ .

As we have seen if the previous sections, it may be interesting to change the radix. Going from radix  $B$  to radix  $B^T$ , we change the matrix  $Q$  into its power  $Q^T$ . Frequently the eigenvalues of  $Q$  have arguments which are commensurable with  $\pi$  and a suitable choice of  $T$  gives a matrix  $Q$  whose all eigenvalues are real nonnegative. This trick is often used implicitly. For example the Coquet sequence is viewed as a 4-rational sequence (as we have made in the previous example) in (Coquet, 1983; Dumont and Thomas, 1989; Allouche and Shallit, 2003) (but this is not the case in (Flajolet et al., 1994)). However it may be of interest to use two radices at a time. Even if both dilation equations define as well the function under consideration, it may be practically simpler to study the solution for one radix in terms of solutions for the other radix. The next example illustrates this point.

**Example 10 [Rudin-Shapiro sequence continued].** As an application of Theorem C, we obtain the asymptotic expansion for the Rudin-Shapiro sequence defined in Ex. 1 (Brillhart et al., 1983)

$$\sum_{n \leq N} u_n =_{N \rightarrow +\infty} \sqrt{N}\Phi(\log_4 N) + O(1)$$

where  $\Phi$  is the 1-periodic function defined by  $\Phi(t) = 2^{1-\{t\}}F(4^{\{t\}-1})$  and  $F$  is defined through a dilation equation for radix 4. Functions  $F$  and  $\Phi$  are illustrated in Fig. 6. Let us denote  $\pi_k$  the part of the graph of  $F$  which corresponds to the interval  $[k/8, (k+1)/8]$  for  $0 \leq k < 8$ . It is evident that the parts of odd index on one side and the part of even index on the other side reproduce the same pattern (with a piece upside down) and we want to prove these facts.

Besides of radix 4, we will use radix 2. The matrix  $Q$  for radix 2 (see Ex. 1) has two eigenvalues  $\pm\sqrt{2}$  and associated eigenvectors  $V_\pm = (2 \pm \sqrt{2}, \pm\sqrt{2})/4$ . The vector  $C$  of the representation writes  $C = V_+ + V_-$  and we have to consider two vector-valued functions  $\mathbf{F}_\pm$ . Their components are  $F_{\pm,1}$  and  $F_{\pm,2}$ . The function under study is  $F = F_{+,1} + F_{+,2} + F_{-,1} + F_{-,2}$ .

To abbreviate the computations and with the hope to make them clearer, we introduce the following formalism. The group of affine transforms of the real line acts on the vector space of functions from the real line into itself. More precisely the group acts on the right by substitution: for an affine transform  $a$  and a function  $f$ , the image  $f \circ a$  is simply the composed map  $f \circ a$ . As affine transforms it is natural in the actual context to consider  $d_0 : x \mapsto 2x$  and  $d_1 : x \mapsto 2x - 1$ . We will use  $t_{1/2} : x \mapsto x + 1/2$  too. With these notations the dilation equation for  $\mathbf{F}_\pm$  writes (We use Convention (HEC) to write the dilation equations, that is we consider that functions are adequately extended to the whole real line.)

$$(20) \quad F_{\pm,1} = \pm \frac{1}{\sqrt{2}}F_{\pm,1} \circ d_0 \pm \frac{1}{\sqrt{2}}F_{\pm,2} \circ d_0, \quad F_{\pm,2} = \pm \frac{1}{\sqrt{2}}F_{+,1} \circ d_1 \mp \frac{1}{\sqrt{2}}F_{\pm,2} \circ d_1,$$

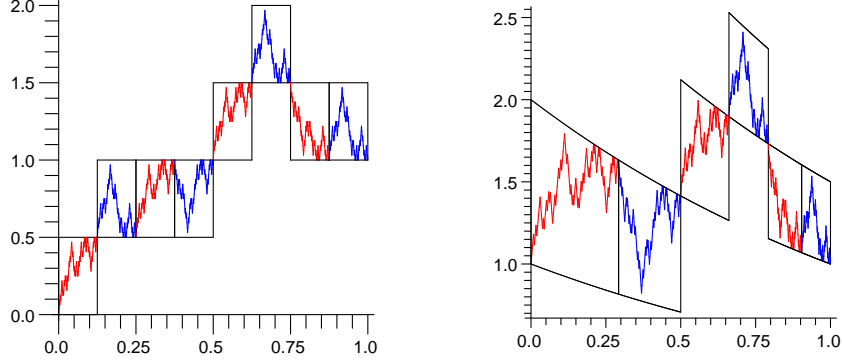


FIGURE 6. The solution of the dilation equation (left-hand side) and the periodic function (right-hand side) associated to the Rudin-Shapiro sequence show some symmetries.

with the conditions  $\mathbf{F}_{\pm}(0) = 0$  and  $\mathbf{F}_{\pm}(1) = V_{\pm}$ . We will collect some simple facts in order to achieve our goal. It results from the dilation equations that  $F_{\pm,2}$  is 0 on the left of  $1/2$ , while  $F_{\pm,1}$  is constant on the right of  $1/2$ . The action of  $t_{1/2}$  on both members of the second equation above with the equality  $d_1 \circ t_{1/2} = d_0$  provides

$$F_{+,2}.t_{1/2} = \frac{1}{\sqrt{2}}F_{+,1}.d_0 - \frac{1}{\sqrt{2}}F_{+,2}.d_0.$$

A subtraction and an addition give respectively

$$(21) \quad F_{+,1} - F_{+,2}.t_{1/2} = \sqrt{2}F_{+,2}.d_0, \quad F_{+,1} + F_{+,2}.t_{1/2} = \sqrt{2}F_{+,1}.d_0.$$

From these preliminaries follow the following formulæ

$$(22) \quad \begin{aligned} F\left(x + \frac{1}{2}\right) - F(x) &= 1, & \text{for } 0 \leq x \leq \frac{1}{4}, & & F\left(x + \frac{1}{2}\right) + F(x) &= 2, & \text{for } \frac{1}{4} \leq x \leq \frac{1}{2}, \\ F\left(x + \frac{1}{4}\right) - F(x) &= \frac{1}{2}, & \text{for } 0 \leq x \leq \frac{1}{8}, & & F\left(x + \frac{1}{4}\right) + F(x) &= \frac{3}{2}, & \text{for } \frac{1}{8} \leq x \leq \frac{1}{4}. \end{aligned}$$

We prove only the third one; the other proof are of the same type. For  $0 \leq x \leq 1/8$ , the number  $x + 1/4$  lies in  $[1/4, 3/8]$  and both numbers are in  $[0, 1/2]$ . The dilation equations (20) give

$$F_{\pm,1}(x) = \pm \frac{1}{\sqrt{2}}F_{\pm,1}(2x) \pm \frac{1}{\sqrt{2}}F_{\pm,2}(2x), \quad F_{\pm,2}(x) = 0,$$

and

$$F_{\pm,1}\left(x + \frac{1}{4}\right) = \pm \frac{1}{\sqrt{2}}F_{\pm,1}\left(2x + \frac{1}{2}\right) \pm \frac{1}{\sqrt{2}}F_{\pm,2}\left(2x + \frac{1}{2}\right), \quad F_{\pm,2}\left(x + \frac{1}{4}\right) = 0.$$

Since  $F$  is  $F_{+,1} + F_{+,2} + F_{-,1} + F_{-,2}$ , we obtain

$$\begin{aligned} F\left(x + \frac{1}{4}\right) - F(x) &= \frac{1}{\sqrt{2}}\left[F_{+,1}\left(2x + \frac{1}{2}\right) + F_{+,2}\left(2x + \frac{1}{2}\right)\right. \\ &\quad \left. - F_{-,1}\left(2x + \frac{1}{2}\right) - F_{-,2}\left(2x + \frac{1}{2}\right) - F_{+,1}(2x) - F_{+,2}(2x) + F_{-,1}(2x) + F_{-,2}(2x)\right]. \end{aligned}$$

However  $2x$  is in  $[0, 1/4]$  and  $2x + 1/2$  is in  $[1/2, 3/4]$ . The functions  $F_{\pm,1}$  are constant on the right of  $1/2$ , while the functions  $F_{\pm,2}$  are constant on the left of  $1/2$ . Making explicit these constant values, we obtain

$$F\left(x + \frac{1}{4}\right) - F(x) = \frac{1}{\sqrt{2}}\left[\frac{1}{2}\sqrt{2} - F_{+,1}(2x) + F_{-,1}(2x) + F_{+,2}\left(2x + \frac{1}{2}\right) - F_{-,2}\left(2x + \frac{1}{2}\right)\right].$$

Besides Formula (21) gives

$$F_{\pm,1}(2x) = F_{\pm,2}\left(2x + \frac{1}{2}\right)$$

because  $x$  is in  $[0, 1/8]$ . The expected formula is proved.

The previous computations ask some questions. We have established formulæ which write

$$\sum_{f,a} \lambda_{f,a} f.a = c,$$

where  $f$  runs through the four functions  $F_{+,1}, F_{+,2}, F_{-,1}, F_{-,2}$ ;  $a$  runs through the set of affine transforms of the real line; the family  $(\lambda_{f,a})$  has a finite support;  $c$  is some constant. Is it possible to design a method in order to find such relationships? For example, how to obtain mechanically the formula

$$\frac{4}{2 + \sqrt{2}} F_{\pm,1}(x) - \frac{4}{\sqrt{2}} F_{\mp,2}(1-x) = 1?$$

Does exist a regular process which gives formulæ of the type

$$\sum_a \lambda_a F.a = C?$$

Evidently we want a minimal generating set for such formulæ.

From the four formulæ (22) above we deduce that all pieces of the graph of  $F$  are obtained from  $\pi_0$  and  $\pi_1$  by some translations or glide reflections. The symmetries of  $F$  are translated to  $\Phi$ , but they lose their graphical evidence. The pieces  $\pi_0$  and  $\pi_1$  disappear and the pieces  $\pi_k$ ,  $2 \leq k < 8$  become the pieces  $\pi'_k$  associated to the interval  $[\log_4(k/2), \log_4((k+1)/2)]$ . The links between the pieces become more intricate. For example the pieces  $\pi'_2$  and  $\pi'_3$  on one side and  $\pi'_6$  and  $\pi'_7$  on the other side are linked by the formula  $2^s \Phi(s) + 2^t \Phi(t) = 4$  under the condition that both numbers  $s \in [0, 1/2]$  and  $t \in [\log_4 3, 1]$  are related by  $4^t - 4^s = 2$ .

**Example 11 [Rescaling].** In the study of radix-rational sequences, it is an attractive idea at first sight to multiply all the matrices  $A_0, \dots, A_{B-1}$  of a linear representation by a scalar in order to control the order of growth of the sequence. But after a while the idea seems to be silly, because it introduces a weighting according to the length of the radix  $B$  expansions of the integers. The previous theorem shows clearly the effect of such a rescaling. It appears that the modification does not change at all the functions  $F(x)$  defined by a dilation equation, and changes very simply the periodic functions  $\Phi(t)$ .

Let us consider the sequence  $u(n) = n$ . It admits the representation

$$L = \begin{pmatrix} 0 & 1 \end{pmatrix}, \quad A_0 = \begin{pmatrix} B & 0 \\ 0 & 1 \end{pmatrix}, \quad A_r = \begin{pmatrix} B & 0 \\ r & 1 \end{pmatrix} \text{ for } r > 0, \quad C = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

for radix  $B$ . There is a dominant eigenvalue  $\rho = B^2$ , with associated functions  $F(x) = x^2$  and  $\Phi(t) = 1/2$ . We obtain the obvious asymptotic expansion

$$\sum_{n \leq N} n \underset{N \rightarrow +\infty}{=} \frac{1}{2} N^2 + O(N).$$

Now consider the sequence  $u(n) = n/B^{\lambda_B(n)}$ , where  $\lambda_B(n)$  is the length of the radix  $B$  expansion of  $n$ . With  $B = 2$  it begins with 0, 0.1, 0.10, 0.11, 0.100, 0.101, 0.110, 0.111, 0.1000, ... It admits the representation

$$L = \begin{pmatrix} 0 & 1 \end{pmatrix}, \quad A_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1/B \end{pmatrix}, \quad A_r = \begin{pmatrix} 1 & 0 \\ r/B & 1/B \end{pmatrix} \text{ for } r > 0, \quad C = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

and again we have  $F(x) = x^2$ , but  $\rho = B$ . We obtain the less obvious asymptotic expansion

$$\sum_{n \leq N} \frac{n}{B^{\lambda_B(n)}} \underset{N \rightarrow +\infty}{=} \frac{1}{2} N \Phi(\log_B N) + O(1)$$

with

$$\Phi(t) = \frac{B^{-t} + B^{t-1}}{2} = \frac{1}{B^{1/2}} \cosh\left(\left(t - \frac{1}{2}\right) \ln B\right), \quad \text{for } 0 \leq t < 1.$$

The convergence towards this function is illustrated in Fig. 7 where a (piece of) catenary appears in an evident way.

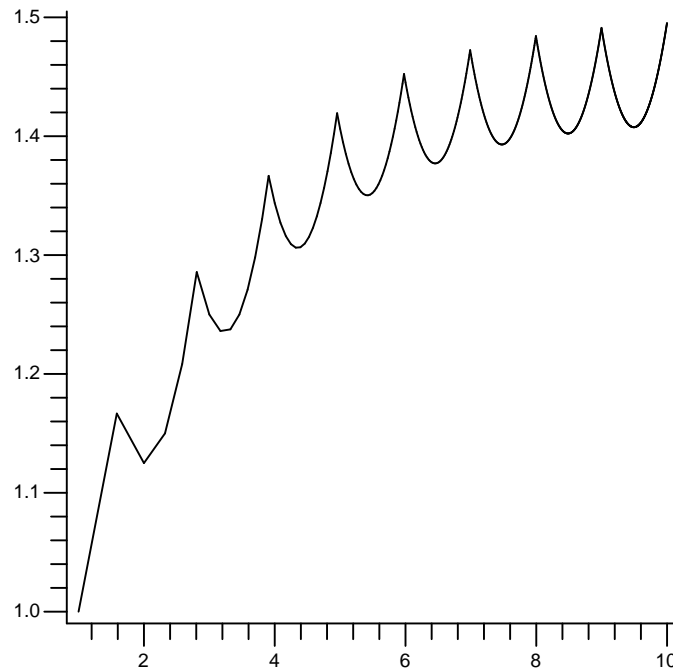


FIGURE 7. The empirical periodic function for sequence  $u(n) = n/2^{\lambda_2(n)}$  (where  $\lambda_2(n) = 1 + \lfloor \log_2 n \rfloor$  is the length of the binary expansion of  $n$ ) as a function of  $\log_2 n$ . A catenary appears.

**5.2. Substitutions and automata.** In the very beginning of the introduction we have written that nobody has asserted a general theorem about the asymptotic expansion of radix-rational sequences. This is not quite the truth because Allouche and Shallit (2003, Sec. 3.5) provide a theorem. But their statement suffers from a severe restriction because they assume for example the hypothesis  $A_w = O(K)$  for  $|w| = K$ , that is  $\lambda_* \leq 1$ , and some other technical hypotheses. It is noteworthy that the result they give has no error term and for this it appears as a direct generalization of (Delange, 1975).

Other works which deserve attention are related to the name of Dumont (Dumont and Thomas, 1989; Dumont, 1990; Dumont et al., 1999). There is a link between these works and the present one, but it needs some explanations to be emphasized. We consider a finite alphabet  $\mathcal{X}$ . A substitution  $\sigma$  on  $\mathcal{X}$  is a map which associates to each letter a non empty word. It extends as a morphism of  $\mathcal{X}^*$  by concatenation. If  $a$  is a letter which turns out to be a strict prefix of the word  $\sigma(a)$ , the sequence  $(\sigma^k(a))$ , obtained by iteration of  $\sigma$  from  $a$ , converges to an infinite word  $\omega = (\omega_n)_{n \geq 0}$ , which is named a fixed point of  $\sigma$  (Fogg, 2002).

We may associate to the substitution  $\sigma$  and to the letter  $a$  an automaton  $\mathcal{A}_\sigma$ . The state of the automaton are the letters of the alphabet. There is a unique initial state which is the letter  $a$ . All states are final states. The transitions are labeled by nonnegative integers and obtained in the following way. For a letter  $x$ , the non empty word  $\sigma(x)$  has length  $\ell \geq 1$  and writes  $\sigma(x) = \sigma_0(x)\sigma_1(x) \dots \sigma_{\ell-1}(x)$ .

There is a transition from state  $x$  to state  $\sigma_r(x)$  labeled by  $r$ . Conversely the automaton determines the substitution and the fixed point of the substitution which begins by  $a$ . If  $B$  is the maximal length of the words  $\sigma(x)$  for  $x$  a letter, all labels are bounded above by  $B - 1$ . To the automaton is associated the language  $\mathcal{L}$  it recognizes, that is the set of words over the alphabet  $\{0, 1, \dots, B - 1\}$  which translate a sequence of transitions from the initial state to a final state. This language is regular because it is recognized by the automaton. The simplest case is the case where the substitution is of constant length, which means that all words  $\sigma(x)$ ,  $x \in \mathcal{X}$ , have the same length  $B \geq 2$ . In such a case the language  $\mathcal{L}$  is merely the free monoid  $\{0, 1, \dots, B - 1\}^*$ .

The automaton may be enriched by an output function  $f$  which associates to each state, that is letter, a value. The output function extends to words and the image of the fixed point  $\omega$  is an infinite sequence of values. Dumont and Thomas (1989) study the asymptotic behaviour of the running sum

$$S^f(N) = \sum_{0 \leq n < N} f(\omega_n)$$

where  $f$  is real-valued, under some hypotheses which we will describe later.

To merge the framework of (Dumont and Thomas, 1989) and ours it suffices to consider a linear version of the automaton. For a given commutative field  $\mathbb{K}$ , we consider the space  $\mathbb{K}^{\mathcal{X}}$ , whose canonical base is  $(e_x)_{x \in \mathcal{X}}$ . To each integer  $r$  between 0 and  $B - 1$  we associate a  $d \times d$  matrix  $A_r$ , where  $d$  is the size of the alphabet, defined by  $A_r e_x = e_y$  if there is a transition labeled  $r$  from state  $x$  to state  $y$  in the automaton, and  $A_r e_x = 0$  otherwise. The matrix  $Q = A_0 + \dots + A_{B-1}$  is the incidence matrix of the substitution; its entries  $Q_{x,y}$  is the number of occurrences of the letter  $y$  in the word  $\sigma(x)$ . We insert in the description the column vector  $C = e_a$  and the row vector  $L = (f(x))_{x \in \mathcal{A}}$  and we have a linear representation. For a word  $w = w_0 \dots w_{K-1}$  taken from the language  $\mathcal{L}$  of the automaton, it is equivalent to follow from the initial state  $a$  the transitions labeled  $w_0, \dots, w_{K-1}$  and to compute the value  $f(z)$  of the state  $z$  where ends the path, or to compute the matrix product  $LA_{w_{K-1}} \dots A_{w_0} C$ . We are not far to the definition of a radix-rational sequence, but the idea of a numeration system is yet lacking.

The lengths of the iterates  $\sigma^n(a)$  are the elements of an increasing sequence  $\mathcal{B} = (B_n)_{n \geq 0}$  which begins with  $B_0 = 1$ . This sequence defines a numeration system: a nonnegative integer  $n$  admits an expansion  $(a_{K-1} \dots a_0)_{\mathcal{B}}$  in the system  $\mathcal{B}$  if it writes  $n = a_0 B_0 + a_1 B_1 + \dots + a_{K-1} B_{K-1}$ . There is always at least one expansion named the normal  $\mathcal{B}$ -representation, which is obtained by a greedy algorithm. The language  $\mathcal{S}$  associated to the system of numeration is the set of all normal  $\mathcal{B}$ -representations of nonnegative integers. (The representation of 0 is the empty word.) Generally speaking, the language  $\mathcal{L}$  is not regular and is distinct from the language  $\mathcal{S}$ , but in the simple case where the substitution is of constant length  $B$ , both languages  $\mathcal{L}$  and  $\mathcal{S}$  are equal. As a consequence the sequence  $(f(\omega_n))$  is  $B$ -rational. It is even  $B$ -automatic: for an nonnegative integer  $n$  we write its radix  $B$  expansion and we use this word to follow a path which begins with  $a$  in the automaton; the end of the path is  $\omega_n$  and the value associated to  $n$  is  $f(\omega_n)$ . It is proved that a  $B$ -automatic sequence is a  $B$ -rational sequence which takes a finite number of values.

Nevertheless the previous system of numeration is not suitable in case of a substitution which is not of constant length. The prefix-suffix automaton  $\mathcal{A}'_{\sigma}$  (Mossé,



1996; Canterini and Siegel, 2001) is the right automaton. Its states are the letters of  $\mathcal{X}$ . There is a transition labeled  $(p, x, s) \in \mathcal{X}^* \times \mathcal{X} \times \mathcal{X}^*$  from  $x$  to  $y$  if  $\sigma(y) = pxs$  (hence the name of the automaton). All states are initial and  $a$  is the only final states. Clearly  $\mathcal{A}'_\sigma$  is a sophisticated version of  $\mathcal{A}$  (the transitions are reversed but this is of no importance), which is equivalent in case of a substitution of constant length. Dumont and Thomas (1989) use a version of this automaton which takes into account only the prefixes. The language  $\mathcal{L}'$  recognized by  $\mathcal{A}'_\sigma$  may be defined by a set of prohibited patterns: a pair of labels  $((p, x, s), (p', y, s'))$  such that  $\sigma(y) \neq p's'$  does not occur in a word of  $\mathcal{L}'$ . For every subword  $\omega^N = (\omega_n)_{0 \leq n < N}$  there exists a unique path  $((p_k, x_k, s_k))_{0 \leq k < K}$  of length  $K$ , determined by  $B_K \leq N < B_{K+1}$ , which ends at  $a$ . In other terms there exists a unique word  $((p_k, x_k, s_k))_{0 \leq k < K}$  from  $\mathcal{L}'$  of length  $K$  such that  $x_{K-1} = a$ . It defines a cutting of  $\omega^N = (\omega_n)_{0 \leq n < N}$  which writes  $\omega^N = \sigma^{K-1}(p_{K-1})\sigma^{K-2}(p_{K-2}) \dots \sigma^0(p_0)$ . Moreover the prefixes  $p_k$  lie in the finite set of strict prefixes of the words  $\sigma(x)$  with  $x$  a letter. Such a result demands hypotheses (Mossé, 1992): the substitution is primitive, which means that there exists a  $k$  such that for every pair of letters  $x$  and  $y$  the letter  $x$  occurs in  $\sigma^k(y)$ ; the fixed point  $\omega$  is not a periodic sequence. Taking into account the lengths of the words, we obtain  $N = |\sigma^{K-1}(p_{K-1})| + |\sigma^{K-2}(p_{K-2})| + \dots + |\sigma^0(p_0)|$ . This is the expansion of the integer  $N$  according to the numeration system associated with the substitution  $\sigma$  and  $a$ . (Note that there does not exist a general definition of what is a numeration system.) The proof of the existence of the expansion is anew a greedy algorithm (Dumont and Thomas, 1989, Lemma 1.3):  $p_{K-1}$  is the longest prefix of  $\omega$  such that  $\sigma^{K-1}(p_{K-1})$  is a prefix of  $\omega^N$ .

The asymptotic study of the sequence  $(S^f(N))_{N \geq 0}$  is based on the following remarks. The function  $f$  is defined on the letters of the alphabet  $\mathcal{X}$  and extends additively to the word of  $\mathcal{X}^*$ . Particularly we have  $S^f(N) = f(\omega^N)$ . Let  $L$  the row vector whose entries are the values of  $f$  on the letters of the alphabet; let  $C_w$  the column whose entries are the number of occurrences of each letter in the word  $w$ . A consequence of these definition is the formula  $f(w) = LC_w$ . Let  $Q$  be the incidence matrix of the substitution  $\sigma$ . We see immediately the recursion  $C_{\sigma(w)} = QC_w$ . As a consequence we have two analogous formulæ

$$S^f(N) = f(\omega^N) = L \sum_{k=0}^{K-1} Q^k C_{p_k}, \quad N = U \sum_{k=0}^{K-1} Q^k C_{p_k},$$

where  $U$  is the row vector whose all entries are equal to 1. Both formulæ render plausible the following result (Dumont and Thomas, 1989, Th. 2.6),

$$S^f(N) \underset{N \rightarrow +\infty}{=} LAN + \log_\theta^\alpha NN^\beta G(N) + o(\log_\theta^\alpha NN^\beta).$$

It is proved under the following hypotheses and through the following assertions. Because  $Q$  is a primitive nonnegative matrix, its spectral radius  $\theta$  is a dominant eigenvalue. The column vector  $\Lambda$  is its positive eigenvector, normalized by  $U\Lambda = 1$ . The existence of a sub-dominant eigenvalue  $\theta'$  is assumed. It dominates all others eigenvalues apart  $\theta$ , that is  $\theta > \theta' > |\theta''|$  for all eigenvalues  $\theta''$  except  $\theta$  and  $\theta'$ . Moreover it is assumed  $\theta' > 1$ . The integer  $\alpha$  is defined such that  $\alpha + 1$  is the multiplicity of  $\theta'$  as root of the minimal polynomial of  $Q$  and the real number  $\beta$  is defined by  $\beta = \log_\theta \theta'$ . The function  $G$  is defined as the limit

$$\forall x > 0, \quad G(x) = x^{-\beta} \lim_{k \rightarrow +\infty} \frac{S^f(\lfloor \theta^k x \rfloor) - L\Lambda \lfloor \theta^k x \rfloor}{k^\alpha \theta'^k}.$$

It satisfies  $G(\theta x) = G(x)$  for  $x$  positive and is Hölder of exponent  $\beta$ .

To summarize Dumont and Thomas (1989) study the mean asymptotic behaviour of real-valued sequences defined by substitutions and for substitutions with constant length this reduces to automatic sequences. We study complex-valued sequences associated to complex rational formal power series and for series which takes only a finite number of values this reduces to automatic sequences.

**5.3. Linear representation insensitive to the leftmost zeroes.** In the use of Formula (13), we may introduce a simplifying hypothesis which turns out to be non restrictive. To a rational formal series we associate a radix-rational series through a numeration system. But the knowledge of a radix-rational sequence does not determine a unique rational formal series, because the expansions of the integers does not use the words which begin with a zero. A first idea which comes in mind to complete the definition of the formal series is to decide that words which begin with zero give a null value. But there is another way to extend a radix-rational sequence into a formal series and it is more natural after all. Let us say that a linear representation of a radix-rational series is *insensitive to the leftmost zeroes* if it satisfies  $LA_0 = L$ . For such a representation the formal power series is completely determined by the radix-rational series, because the adding of some zeroes on the left of the expansion of an integer does not change the value associated to this word.

**Lemma 10.** *Every radix-rational sequence has a (reduced) linear insensitive to the leftmost zeroes representation, that is a representation such that  $LA_0 = L$ .*

This point is described in (Dumas, 1993, sec. 4.2) (where an insensitive to the leftmost zeroes representation is termed standard), but we give a proof because it explains how most of the linear representations in this paper are obtained.

*Proof.* For the sake of simplicity, let us assume that the radix is  $B = 2$ . The hypothesis is that all subsequences  $(u_{2^k n+r})$ ,  $k \geq 0$ ,  $0 \leq r < 2^k$ , of the radix-rational sequence  $(u_n)$  generate a finite dimensional vector space  $U$ . Let  $d$  be the dimension of that vector space. (For the null sequence, we have  $d = 0$ . We exclude this case.) We consider the subsequences  $(u_n)$ ,  $(u_{2n})$ ,  $(u_{2n+1})$ ,  $(u_{4n})$ ,  $(u_{4n+1})$ ,  $(u_{4n+2})$ ,  $\dots$  in that order and the dimension  $d_j$  of the vector space generated by the  $j$  first subsequences (with  $d_{-1} = 0$ ). We select the subsequences  $v^1, v^2, \dots, v^d$  such that the dimension increases by 1 when they encountered in the previous list. The family  $(v^\ell)_{1 \leq \ell \leq d}$  is a basis of  $U$ . The sequence  $(u_n)$  expresses as a linear combination of  $v^1, v^2, \dots, v^d$  (the sequence  $(u_n)$  is nothing but  $v^1$ ), and this gives the column vector  $C$  of the linear representation we are building. Next we consider the action of 0 and 1 over the sequences  $v^\ell$  defined by  $(0.v^\ell)_n = v_{2n}^\ell$  and  $(1.v^\ell)_n = v_{2n+1}^\ell$  and we express the images in the basis  $(v^\ell)_{1 \leq \ell \leq d}$ . This gives the square matrices  $A_0$  and  $A_1$  of the representation. At last the row vector  $L$  is the vector of initial values  $v_0^\ell$ . In that way, we have a linear representation of the sequence  $(u_n)$ . This may be readily verified by considering the sequence of row vectors  $\Lambda_n = (v_n^1, v_n^2, \dots, v_n^d)$  which satisfies  $u_n = \Lambda_n C$ ,  $\Lambda_{2n} = \Lambda_n A_0$ ,  $\Lambda_{2n+1} = \Lambda_n A_1$ ,  $L = \Lambda_0$ . (Note that Allouche and Shallit (2003) use a column vector for  $\Lambda_n$ , hence the transposed matrices for  $A_0, A_1$ .) Moreover the equation  $(0.v^\ell)_0 = v_0^\ell$ , that is  $\Lambda_0 A_0 = \Lambda_0$ , renders evident the formula  $LA_0 = L$ . The proof would be more enlightening by considering a binary tree and a prefix part of the monoid of words, but we will not insist on this point.  $\square$

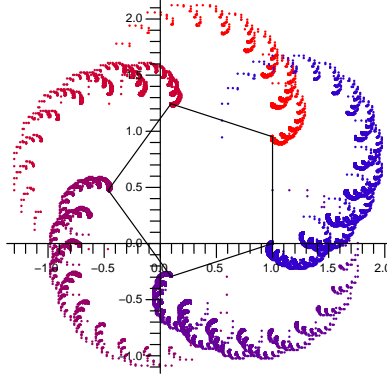


FIGURE 8. The empirical rosette of Ex. 12 with  $\vartheta = 2\pi/5$ . For each frond of the rosette, the index  $N$  goes from  $2^K$  to  $2^{K+1} - 1$ . Here  $K$  goes from 11 to 15 and the color from red to blue. The vertices of the pentagon are the points  $\Gamma(K)$  with  $K$  integer.

We do not have used this hypothesis of insensitivity in the proofs because it is unsuitable for the vector-valued version we have elaborated, but most of the examples we have given have this property and this saves us to compute the first term of Formula (13).

**5.4. Periodicity versus pseudo-periodicity.** The occurrence of periodic functions in logarithmic scale is common in the asymptotic study of radix-rational sequences (Coquet, 1983; Delange, 1975; Dumont et al., 1999; Flajolet and Golin, 1994; Flajolet et al., 1994; Osbaldestin and Shiu, 1989). Nevertheless the rising of periodic functions, if true in practical examples, is wrong in full generality. The reason is the following: in common examples the eigenvalues of the matrix  $Q$  have arguments which are commensurable with  $\pi$ . As we have already explained, a change of radix permits to consider that the useful eigenvalues are all positive numbers. As a consequence functions  $\Phi$  are periodic, because they depend only on the fractional part of the variable  $t$ . But in the general case they write something like  $\Phi(t) = \omega^{\lfloor t \rfloor} \rho^{1-\{t\}} F(B^{\{t\}-1})$  and if  $\omega$  does not write  $\omega = e^{i\vartheta}$  with  $\vartheta/\pi$  a rational number, the function  $\Phi$  is not periodic but only pseudo-periodic. Below we exemplify this phenomenon.

**Example 12 [Rosettes].** Let us consider the linear representation for radix  $B = 2$  and dimension 2,

$$A_0 = \begin{pmatrix} \cos \vartheta & 0 \\ 0 & \cos \vartheta \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0 & -\sin \vartheta \\ \sin \vartheta & 0 \end{pmatrix},$$

where  $\vartheta$  is a real number restricted by the condition  $\vartheta \not\equiv 0 \pmod{\pi/2}$  to avoid degeneracy. We do not define the row vector  $L$ , because we are interested in the vector-valued sequence

$$\Sigma_N = \sum_{0 \leq n \leq N} A_w C$$

( $w$  is the binary expansion of the integer  $n$ ). With regard to the column vector  $C$ , we note that both matrices  $A_0$  and  $A_1$  write  $A_0 = \cos \vartheta I_2$ ,  $A_1 = \sin \vartheta R_{\pi/2}$  (notation of Ex. 5:  $R_\varphi$  is the rotation matrix with angle  $\varphi$ ). As a consequence they commute with all rotation matrices and

if  $C$  is changed into  $R_\varphi C$ , then  $\Sigma_N$  is changed into  $R_\varphi \Sigma_N$ . Evidently we have a similar formula with dilations and so we may take as vector  $C$  the first vector  $E_1$  of the canonical basis.

The joint spectral radius is  $\lambda_* = \max(|\cos \vartheta|, |\sin \vartheta|)$ , because  $\|A_0\|_1 = |\cos \vartheta|$ ,  $\|A_1\|_1 = |\sin \vartheta|$  and  $A_0^2$  and  $A_1^2$  admit respectively the eigenvalues  $\cos^2 \vartheta$  and  $-\sin^2 \vartheta$ . The matrix  $Q = A_0 + A_1$  is the rotation matrix  $R_\vartheta$  and its eigenvalues are  $\rho\omega_\pm$  with  $\rho = 1$  and  $\omega_\pm = e^{\pm i\vartheta}$ . We take as eigenvectors respectively for  $\omega_+$  and  $\omega_-$  the vectors  $V_+ = \begin{pmatrix} 1 & -i \end{pmatrix}^{\text{tr}}$ ,  $V_- = \begin{pmatrix} 1 & i \end{pmatrix}^{\text{tr}}$ . The vector  $C$  expands as  $C = (V_+ + V_-)/2$ . We have  $\lambda_* < \rho$  and Theorem C applies. The asymptotic expansion for the sum  $\Sigma_{+,N}$  associated with  $V_+$  writes

$$\Sigma_{+,N} = (I_2 - A_0) \sum_{k=0}^K Q^k V_+ + e^{i(K+1)\vartheta} \mathbf{F}_+(2^{\{t\}-1}) + O(\lambda_*^K),$$

where  $\mathbf{F}_\pm$  is defined by the dilation equation

$$\begin{cases} F_{\pm,1}(x) = \cos \vartheta e^{\mp i\vartheta} F_{\pm,1}(2x), & \text{for } 0 \leq x < \frac{1}{2}; \\ F_{\pm,2}(x) = \cos \vartheta e^{\mp i\vartheta} F_{\pm,2}(2x), & \\ \begin{cases} F_{\pm,1}(x) = \cos \vartheta e^{\mp i\vartheta} - \sin \vartheta e^{\mp i\vartheta} F_{\pm,2}(2x-1), \\ F_{\pm,2}(x) = \mp i \cos \vartheta e^{\mp i\vartheta} + \sin \vartheta e^{\mp i\vartheta} F_{\pm,1}(2x-1), \end{cases} & \text{for } \frac{1}{2} \leq x < 1, \end{cases} \end{cases}$$

with the boundary conditions  $\mathbf{F}_\pm(0) = 0$ ,  $\mathbf{F}_\pm(1) = V_\pm$ . Both vector-valued functions  $\mathbf{F}_\pm$  are conjugate. Emphasizing their real and imaginary parts  $\mathbf{U}$  and  $\pm \mathbf{V}$  and carrying on with the computation we obtain for the sum  $\Sigma_N$  associated with  $C = E_1$  the asymptotic expansion

$$\Sigma_N \underset{N \rightarrow +\infty}{=} \Gamma(t) + O(\lambda_*^K),$$

with  $\Gamma : t \mapsto \Omega + \mathbf{A}(t) + \mathbf{B}(t)$ ,

$$\Omega = \sin \frac{\vartheta}{2} \begin{pmatrix} \sin \vartheta/2 \\ \cos \vartheta/2 \end{pmatrix}, \quad \mathbf{A}(t) = \sin \frac{\vartheta}{2} \begin{pmatrix} \cos((K+1/2)\vartheta - \pi/2) \\ \sin((K+1/2)\vartheta - \pi/2) \end{pmatrix},$$

$$\mathbf{B}(t) = \cos((K+1)\vartheta) \mathbf{U}(2^{\{t\}-1}) - \sin((K+1)\vartheta) \mathbf{V}(2^{\{t\}-1}).$$

Obviously an increasing of  $t$  (and consequently of  $K$ ) by 1 rotates the vector  $\mathbf{A}(t)$  by  $\vartheta$ . The change for  $\mathbf{B}$  is less obvious. From the real point of view, the dilation equation for  $\mathbf{F}_+$  rewrites

$$\Phi(x) = T_0 \Phi(2x) \quad \text{for } 0 \leq x < \frac{1}{2}, \quad \Phi(x) = T_0 W + T_1 \Phi(2x-1) \quad \text{for } \frac{1}{2} \leq x < 1,$$

where  $\Phi$  is the 4-dimensional vector-valued function  $\Phi = \begin{pmatrix} \mathbf{U} & \mathbf{V} \end{pmatrix}^{\text{tr}}$ . The matrices  $T_0$  and  $T_1$  have the following expressions

$$T_0 = \begin{pmatrix} \cos^2 \vartheta & 0 & \cos \vartheta \sin \vartheta & 0 \\ 0 & \cos^2 \vartheta & 0 & \cos \vartheta \sin \vartheta \\ -\cos \vartheta \sin \vartheta & 0 & \cos^2 \vartheta & 0 \\ 0 & -\cos \vartheta \sin \vartheta & 0 & \cos^2 \vartheta \end{pmatrix} = \cos \vartheta R_{-\vartheta} \otimes I_2,$$

$$T_1 = \begin{pmatrix} 0 & -\cos \vartheta \sin \vartheta & 0 & -\sin^2 \vartheta \\ \cos \vartheta \sin \vartheta & 0 & \sin^2 \vartheta & 0 \\ 0 & \sin^2 \vartheta & 0 & -\cos \vartheta \sin \vartheta \\ -\sin^2 \vartheta & 0 & \cos \vartheta \sin \vartheta & 0 \end{pmatrix} = \sin \vartheta R_{-\vartheta} \otimes R_{\pi/2}.$$

The boundary conditions are  $\Phi(0) = 0$  and  $\Phi(1) = W$  with  $W = \begin{pmatrix} 1 & 0 & 0 & -1 \end{pmatrix}^{\text{tr}}$ . Let  $P$  be the matrix

$$P = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}.$$

We verify  $P^{-1}T_0P = T_0$ ,  $P^{-1}T_1P = T_1$ ,  $PW = W$ . As a result  $P\Phi$  is a solution of the dilation equation. But the dilation equation has a unique solution and we conclude that  $\Phi$  satisfies  $P\Phi = \Phi$ . This means  $-\mathbf{V} = R_{\pi/2}\mathbf{U}$ . This shows the formula  $\mathbf{B}(t+1) = R_\vartheta \mathbf{B}(t)$ . Eventually we see that  $\Gamma(t+1)$  is the image of  $\Gamma(t)$  by the rotation of angle  $\vartheta$  about  $\Omega$ .

Let us assume that  $\vartheta$  is commensurable with  $\pi$ , and let us write  $\vartheta/\pi = p/q$  where  $p/q$  is in lowest terms. We see immediately that the arc  $\Gamma$  is  $2q$ -periodic, and even  $2^{1-\kappa}q$ -periodic if  $\kappa$  is the dyadic valuation of  $p$ . This phenomenon is illustrated by Fig. 8. Besides it is easy to verify  $\Gamma(t + 2^{-\kappa}q) + \Gamma(t) = 2\Omega$ .

To the contrary when the ratio  $\vartheta/\pi$  is irrational, the rotation  $R_\vartheta$  leaves invariant the image of the arc  $\Gamma$  but its order is infinite. The non-periodic character of the arc  $\Gamma$  is evident when we consider its value at integers,

$$\Gamma(K) = \Omega + \cos \frac{\vartheta}{2} \begin{pmatrix} \cos(K - 1/2)\vartheta \\ \sin(K - 1/2)\vartheta \end{pmatrix}.$$

Hence we see that the functions  $\Phi$  are not necessarily periodic, even if they are frequently periodic in concrete examples.

**Acknowledgment.** I am most grateful towards FRÉDÉRIC CHYZAK (ALGORITHMS PROJECT, INRIA) for his ever patient ear during my effort to understand radix-rational sequences.

#### REFERENCES

- Jean-Paul Allouche and Jeffrey Shallit. The ring of  $k$ -regular sequences. *Theoret. Comput. Sci.*, 98(2):163–197, 1992. ISSN 0304-3975.
- Jean-Paul Allouche and Jeffrey Shallit. The ubiquitous Prouhet-Thue-Morse sequence. In *Sequences and their applications (Singapore, 1998)*, Springer Ser. Discrete Math. Theor. Comput. Sci., pages 1–16. Springer, London, 1999.
- Jean-Paul Allouche and Jeffrey Shallit. *Automatic sequences*. Cambridge University Press, Cambridge, 2003. ISBN 0-521-82332-3. Theory, applications, generalizations.
- Robert Bézian and Henri Faure. Discrépance de la suite de van der Corput. *C. R. Acad. Sci. Paris Sér. A-B*, 285(5):A313–A316, 1977.
- Robert Bézian and Henri Faure. Discrépance de la suite de Van der Corput. In *Séminaire Delange-Pisot-Poitou, 19e année: 1977/78, Théorie des nombres, Fasc. 1*, pages Exp. No. 13, 14. Secrétariat Math., Paris, 1978.
- Jean Berstel and Christophe Reutenauer. *Rational series and their languages*, volume 12 of *EATCS Monographs on Theoretical Computer Science*. Springer-Verlag, Berlin, 1988. ISBN 3-540-18626-3.
- Patrick Billingsley. *Probability and measure*. Wiley Series in Probability and Mathematical Statistics: Probability and Mathematical Statistics. John Wiley & Sons Inc., New York, third edition, 1995. ISBN 0-471-00710-2.
- Vincent D. Blondel. Special issue on the joint spectral radius: Theory, methods and applications. *Linear Algebra and its Applications*, 428(10):2259–2404, 2008. Edited by Vincent D. Blondel, Michael Karow, Vladimir Protassov and Fabian R. Wirth.
- Vincent D. Blondel, Yurii Nesterov, and Jacques Theys. On the accuracy of the ellipsoid norm approximation of the joint spectral radius. *Linear Algebra Appl.*, 394:91–107, 2005. ISSN 0024-3795.
- Nicolas Bourbaki. *Éléments de mathématique Fonctions d'une variable réelle Théorie élémentaire*. Hermann, 1976.
- David W. Boyd, Janice Cook, and Patrick Morton. On sequences of  $\pm 1$ 's defined by binary patterns. *Dissertationes Math. (Rozprawy Mat.)*, 283:64, 1989. ISSN 0012-3862.
- John Brillhart and Leonard Carlitz. Note on the Shapiro polynomials. *Proc. Amer. Math. Soc.*, 25:114–118, 1970. ISSN 0002-9939.
- John Brillhart, Paul Erdős, and Patrick Morton. On sums of Rudin-Shapiro coefficients. II. *Pacific J. Math.*, 107(1):39–69, 1983. ISSN 0030-8730.
- Vincent Canterini and Anne Siegel. Automate des préfixes-suffixes associé à une substitution primitive. *J. Théor. Nombres Bordeaux*, 13(2):353–369, 2001. ISSN 1246-7405.
- Julien Cassaigne. Counting overlap-free binary words. In *STACS 93 (Würzburg, 1993)*, volume 665 of *Lecture Notes in Comput. Sci.*, pages 216–225. Springer, Berlin, 1993.
- George F. Clements and Bernt Lindström. A sequence of  $(\pm 1)$ -determinants with large values. *Proc. Amer. Math. Soc.*, 16:548–550, 1965. ISSN 0002-9939.
- Jean Coquet. A summation formula related to the binary digits. *Invent. Math.*, 73(1):107–115, 1983. ISSN 0020-9910.
- Ingrid Daubechies. *Ten lectures on wavelets*, volume 61 of *CBMS-NSF Regional Conference Series in Applied Mathematics*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1992. ISBN 0-89871-274-2.

- Ingrid Daubechies and Jeffrey C. Lagarias. Two-scale difference equations. I. Existence and global regularity of solutions. *SIAM J. Math. Anal.*, 22(5):1388–1410, 1991. ISSN 0036-1410.
- Ingrid Daubechies and Jeffrey C. Lagarias. Two-scale difference equations. II. Local regularity, infinite products of matrices and fractals. *SIAM J. Math. Anal.*, 23(4):1031–1079, 1992. ISSN 0036-1410.
- Hubert Delange. Sur la fonction sommatoire de la fonction “somme des chiffres”. *Enseignement Math. (2)*, 21(1):31–47, 1975.
- Thomas B. Dinsbacher and Douglas P. Hardin. Multivariate nonhomogeneous refinement equations. *J. Fourier Anal. Appl.*, 5(6):589–597, 1999. ISSN 1069-5869.
- Michael Drmota and Johannes Gajdosik. The distribution of the sum-of-digits function. *J. Théor. Nombres Bordeaux*, 10(1):17–32, 1998. ISSN 1246-7405.
- Philippe Dumas. Algebraic aspects of B-regular series. In A. Lingas, R. Karlsson, and S. Carlsson, editors, *Automata, Languages and Programming*, Lecture Notes in Computer Science 700, pages 457–468. EATCS, Springer Verlag, 1993. ISBN 3-540-56939-1. Proceedings of the 20th International Colloquium ICALP 93, Lund, Sweden.
- Philippe Dumas, Helger Lipmaa, and Johan Wallén. Asymptotic behaviour of a non-commutative rational series with a nonnegative linear representation. *Discrete Mathematics & Theoretical Computer Science*, 9(1):247–274, 2007. ISSN 1365-8050. URL <http://www.dmtcs.org/dmtcs-ojs/index.php/dmtcs/article/view/478/1836>.
- Jean-Marie Dumont. Summation formulae for substitutions on a finite alphabet. In *Number theory and physics (Les Houches, 1989)*, volume 47 of *Springer Proc. Phys.*, pages 185–194. Springer, Berlin, 1990.
- Jean-Marie Dumont, Nikita Sidorov, and Alain Thomas. Number of representations related to a linear recurrent basis. *Acta Arith.*, 88(4):371–396, 1999. ISSN 0065-1036.
- Jean-Marie Dumont and Alain Thomas. Systemes de numeration et fonctions fractales relatifs aux substitutions. *Theoret. Comput. Sci.*, 65(2):153–169, 1989. ISSN 0304-3975.
- Nira Dyn and David Levin. Subdivision schemes in geometric modelling. *Acta Numer.*, 11:73–144, 2002. ISSN 0962-4929.
- Philippe Flajolet and Mordecai Golin. Mellin transforms and asymptotics. The mergesort recurrence. *Acta Inform.*, 31(7):673–696, 1994. ISSN 0001-5903.
- Philippe Flajolet, Peter Grabner, Peter Kirschenhofer, Helmut Prodinger, and Robert F. Tichy. Mellin transforms and asymptotics: digital sums. *Theoret. Comput. Sci.*, 123(2):291–314, 1994. ISSN 0304-3975.
- Philippe Flajolet and Lyle Ramshaw. A note on Gray code and odd-even merge. *SIAM J. Comput.*, 9(1):142–158, 1980. ISSN 0097-5397.
- N. Pytheas Fogg. *Substitutions in dynamics, arithmetics and combinatorics*, volume 1794 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2002. ISBN 3-540-44141-7. Edited by V. Berthé, S. Ferenczi, C. Mauduit and A. Siegel.
- Michel Goze and Yusupdjani Khakimdjanov. Nilpotent and solvable Lie algebras. In M. Hazewinkel, editor, *Handbook of algebra*, volume 2, pages 615–663. North-Holland, Amsterdam, 2000. ISBN 0-444-50396-X.
- Christopher Heil and David Colella. Matrix refinement equations: existence and uniqueness. *J. Fourier Anal. Appl.*, 2(4):363–377, 1996. ISSN 1069-5869.
- John E. Hutchinson. Fractals and Self Similarity. *Indiana University Mathematics Journal*, 30(5):713–747, 1981.
- Helger Lipmaa, Johan Wallén, and Philippe Dumas. On the additive differential probability of exclusive-or. In Bimal Roy and Willi Meier, editors, *Fast Software Encryption 2004*, volume 3017 of *Lecture Notes in Computer Science*, pages 317–331. Springer-Verlag, 2004.
- M. Douglas McIlroy. The number of 1’s in binary integers: bounds and extremal properties. *SIAM J. Computing*, 3:255–261, 1974.
- François Morain and Jorge Olivos. Speeding up the computations on an elliptic curve using addition-subtraction chains. *RAIRO Inform. Théor. Appl.*, 24(6):531–543, 1990. ISSN 0988-3754.
- Brigitte Mossé. Puissances de mots et reconnaissabilité des points fixes d’une substitution. *Theoret. Comput. Sci.*, 99(2):327–334, 1992. ISSN 0304-3975.
- Brigitte Mossé. Reconnaissabilité des substitutions et complexité des suites automatiques. *Bull. Soc. Math. France*, 124(2):329–346, 1996. ISSN 0037-9484.

- Donald J. Newman. On the number of binary digits in a multiple of three. *Proc. Amer. Math. Soc.*, 21:719–721, 1969. ISSN 0002-9939.
- Harald Niederreiter. *Random number generation and quasi-Monte Carlo methods*, volume 63 of *CBMS-NSF Regional Conference Series in Applied Mathematics*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1992. ISBN 0-89871-295-5.
- Andrew H. Osbaldestin and Peter Shiu. A correlated digital sum problem associated with sums of three squares. *Bull. London Math. Soc.*, 21(4):369–374, 1989. ISSN 0024-6093.
- Olivier Rioul. Simple regularity criteria for subdivision schemes. *SIAM J. Math. Anal.*, 23(6):1544–1576, 1992. ISSN 0036-1410.
- Gian-Carlo Rota and Gilbert Strang. A note on the joint spectral radius. *Nederl. Akad. Wetensch. Proc. Ser. A 63 = Indag. Math.*, 22:379–381, 1960.
- Walter Rudin. Some theorems on Fourier coefficients. *Proc. Amer. Math. Soc.*, 10:855–859, 1959. ISSN 0002-9939.
- Jacques Sakarovitch. *Elements of Automata Theory*. Cambridge University Press, 2005. ISBN 0-521-84425-8.
- Harold S. Shapiro. Extremal problems for polynomials and power series. Master’s thesis, Massachusetts Institute of Technology, 1951.
- Kenneth B. Stolarsky. Power and exponential sums of digital sums related to binomial coefficient parity. *SIAM J. Appl. Math.*, 32(4):717–730, 1977. ISSN 1095-712X.
- Gilbert Strang and Ding-Xuan Zhou. Inhomogeneous refinement equations. *J. Fourier Anal. Appl.*, 4(6):733–747, 1998. ISSN 1069-5869.
- Kenneth J. Supowit and Edward M. Reingold. Divide and conquer heuristics for minimum weighted Euclidean matching. *SIAM J. Comput.*, 12(1):118–143, 1983. ISSN 0097-5397.
- J. R. Trollope. An explicit expression for binary digital sums. *Math. Mag.*, 41:21–25, 1968. ISSN 0011-801x.
- John N. Tsitsiklis and Vincent D. Blondel. The Lyapunov exponent and joint spectral radius of pairs of matrices are hard—when not impossible—to compute and to approximate. *Math. Control Signals Systems*, 10(1):31–40, 1997. ISSN 0932-4194.

ALGORITHMS PROJECT, INRIA ROCQUENCOURT, 78153 LE CHESNAY CEDEX, FRANCE  
*E-mail address:* [Philippe.Dumas@inria.fr](mailto:Philippe.Dumas@inria.fr)