Algebraic aspects of B-regular series

Philippe Dumas

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Algebraic Aspects of B-regular Series

Philippe DUMAS

N° 1931
Juin 1993

PROGRAMME 2

Calcul symbolique,
programmation
et génie logiciel

Algebraic Aspects of B-regular Series

Philippe Dumas

Abstract

This paper concerns power series of an arithmetic nature that arise in the analysis of divide-and-conquer algorithms. Two key notions are studied: that of B-regular sequence and that of Mahlerian sequence with their associated power series. Firstly we emphasize the link between rational series over the alphabet $\{x_0, x_1, \ldots, x_{B-1}\}$ and B-regular series. Secondly we extend the theorem of Christol, Kamae, Mendès France and Rauzy about automatic sequences and algebraic series to B-regular sequences and Mahlerian series. We develop here a constructive theory of B-regular and Mahlerian series. The examples show the ubiquitous character of B-regular series in the study of arithmetic functions related to number representation systems and divide-and-conquer algorithms.

Aspects algébriques des séries B-régulières

Philippe Dumas

Résumé

Cet article porte sur des suites de nature arithmétique qui apparaissent dans les algorithmes du type *diviser pour régner*. Les notions de série génératrice B-régulière et de série mahlérienne sont les deux concepts de base. Nous insistons d'abord sur le lien entre les séries rationnelles sur l'alphabet $\{x_0, x_1, \ldots, x_{B-1}\}$ et les séries B-régulières. Ensuite nous étendons le théorème de Christol, Kamae, Mendès France et Rauzy, qui porte sur les suites automatiques et les séries algébriques, en un théorème sur les suites B-régulières et les séries mahlériennes. Les exemples montrent le caractère omniprésent des séries B-régulières dans les suites liées à la numération de position et les algorithmes du type *diviser pour régner*.

To appear in *Proceedings of ICALP'93* (Lectures notes in Computer Sciences; Editors: A. Lingas, S. Carlsson, and R. Karlsson).

Algebraic Aspects of B-regular Series

Ph. Dumas

Algorithms Project,
INRIA Rocquencourt BP 105,
78153 Le Chesnay Cedex, France

Abstract. This paper concerns power series of an arithmetic nature that arise in the analysis of divide-and-conquer algorithms. Two key notions are studied: that of B-regular sequence and that of Mahlerian sequence with their associated power series. Firstly we emphasize the link between rational series over the alphabet $\{x_0, x_1, \ldots, x_{B-1}\}$ and B-regular series. Secondly we extend the theorem of Christol, Kamae, Mendès France and Rauzy about automatic sequences and algebraic series to B-regular sequences and Mahlerian series. We develop here a constructive theory of B-regular and Mahlerian series. The examples show the ubiquitous character of B-regular series in the study of arithmetic functions related to number representation systems and divide-and-conquer algorithms.

The interest of 2-regular sequences comes from their presence in many problems which touch upon the binary representation of integers or divide-and-conquer algorithms, like sum-of-digits function, number of odd binomial coefficients, Josephus problem, mergesort, Euclidean matching or comparison networks. This explains why we study B-regular sequences that formalize the sequences which are solutions of certain difference equations of the divide-and-conquer type. In other words we want to show that B-regular series (i.e. generating functions of B-regular sequences) are as important in computer science as rational functions are common in mathematics.

Many properties of B-regular sequences like closure properties or growth properties have been established by Allouche and Shallit. In particular they showed that there is a link between B-regular sequences and rational series in the sense of formal language theory. The transition from one to another uses the B-ary representation of integers. There is already a long tradition about recognizable sets and automatic sequences.

The link provides us with the well known machinery of rational series and the first part of the paper is devoted to the illustration of its use. For example we introduce the Hankel matrix of a regular series. This is the practical way to find the rank of a regular series, to exhibit minimal recurrence relations or to build up linear representations.

In the second part we compare B-regular series and Mahlerian series. Our goal is to extend the theorem of Christol, Kamae, Mendès France and Rauzy [6], which asserts that q-automatic series with coefficients in the finite field $\mathbb{F}_q$ are exactly algebraic series. To that purpose we introduce a more general notion of Mahlerian series. We prove in particular that B-regular series are Mahlerian series.

The reciprocal is more intricate but most useful. Indeed the theorem of Christol *et alii* is not adequate for theoretical computer science where the sequences have elements that are integer rather than elements of a finite fields. We give a partial answer to this problem, that permits to cover numerous cases of application.

In all the examples we have aimed at making the computations effective.

It is worth noting that we concentrate here on one facet of B-regular sequences, their algebraic closure properties. A complementary point of vue is the study of asymptotic behaviour of these sequences. One will find numerous examples in [9, 10].

1 Rational Series and B-regular Series

The properties of B-regular series come mainly from the properties of rational series in non commutative indeterminates and we build up a catalog where each notion about B-regular series is a translation of the corresponding notion about rational series. In view of the richness of the subject we limit ourselves to the essentials.

Let us begin with an example which gives the flavour of 2-regular series.

Example 1. Let us assume that we want to go from 0 to an integer n by leaps whose lengths are power of 2 and directions are forward or backward. The shortest path has a length w_n which may be defined by the conditions $w_0 = 0$, $w_n = 1$ if $n = 2^k$ and $w_n = 1 + \min(w_{n-2^k}, w_{2^{k+1}-n})$ if $2^k < n < 2^{k+1}$. For example we find $w_{14} = 2$ because $14 = 16 - 2$.

Another way to obtain this sequence (w_n) is to consider the two square matrices

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

and the row and column matrices

$$\lambda = (\,0 \;\; 1 \;\; 1 \;\; 2\,), \quad \gamma = (\,1 \;\; 0 \;\; 0 \;\; 0\,)^T.$$

If the binary expansion of the integer n is $\epsilon_\ell \cdots \epsilon_1 \epsilon_0$, we have $w_n = \lambda A_{\epsilon_\ell} \cdots A_{\epsilon_1} A_{\epsilon_0} \gamma$. As an illustration

$$w_{14} = \lambda A_1 A_1 A_1 A_0 \gamma = 2.$$

This computation is akin to the definition of recognizable series and indeed B-regular series are merely a translation, as we shall see.

Let the alphabet $\mathcal{X}_\mathrm{B}$ be formed of the digits 0, 1, ..., B − 1 used to write the integers in B-ary notation. To avoid confusion between figures and scalars, which lie in a ring $\mathbb{A}$, we represent figures by the indeterminates x_0, x_1, ..., $x_{\mathrm{B}-1}$. We obtain B-regular series by translation of rational series [2].

Definition 1. A formal power series $f(z) \in \mathbb{A}[[z]]$ is a B-regular series if there exists a rational series $S \in \mathbb{A}^{\mathrm{rat}}\langle\langle \mathcal{X}_\mathrm{B} \rangle\rangle$ in non-commutating indeterminates, whose support is included in the language $\mathcal{N}$ of integers B-ary expansions,

$$S = \sum_{u \in \mathcal{N}} (S, u)\, u \;,$$

such that

$$f(z) = \sum_{n \geq 0} (S, \tilde{n})\, z^n \ ,$$

where $\tilde{n}$ is the B-ary expansion of n.

Linear Representations. In the study of recognizable series, the linear representations come from the use of the division operators that trim a word of its leftmost letter. Classically the divisions are on the left but we favour the right operations, which correspond to the least significant digits. If the alphabet is $\mathcal{X}$ and w is a word, the right division w^{-1} acts on the series S according to the formula

$$Sw^{-1} = \sum_{u \in \mathcal{X}^*} (S, uw)\, u \ .$$

The division operators give us the section operators S_r, $0 \leq r < \mathrm{B}$, acting on $f(z) = \sum_n f_n z^n$ by the formula

$$S_r f(z) = \sum_{n \geq 0} f_{\mathrm{B}n+r}\, z^n \ .$$

Theorem 2 (Stability theorem). *A formal series is* B*-regular if and only if there exists an* $\mathbb{A}$*-module of finite type which is left stable by the section operators and contains the series.*

We obtain a linear representation of a B-regular series by expressing the section operators with respect to a generating family of that module. Moreover the linear representation permits us to exhibit a rational expression of the series S associated with the B-regular series: if $\Xi = \sum_{0 \leq r < \mathrm{B}} x_r A_r$ and $\Xi_+ = \sum_{0 < r < \mathrm{B}} x_r A_r$, we have $S = \lambda(I + \Xi_+ \Xi^*)\gamma$. This formula is only a translation of the fact that $\mathcal{N} = \varepsilon + \mathcal{X}_+ \mathcal{X}^*$, where ε is the empty word, $\mathcal{X} = \mathcal{X}_{\mathrm{B}}$ and $\mathcal{X}_+ = \{x_1, \ldots, x_{\mathrm{B}-1}\}$.

Example 2. The complexity of mergesort in the worst case satisfies the divide-and-conquer recurrence

$$T_n = T_{\lfloor n/2 \rfloor} + T_{\lceil n/2 \rceil} + n - 1 \ ,$$

with the initial conditions $T_0 = T_1 = 0$. The generating series $T(z)$ is 2-regular because the $\mathbb{Z}$-module generated by $T(z)$, $T(z)/z$, $2z/(1-z)^2$, $z(1+z)/(1-z)^2$ and $(1+z)/(1-z)^2$ is left stable by the two section operators S_0 and S_1. With respect to this basis, the matrices of S_0 and S_1 are

$$A_0 = \begin{pmatrix} 2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & 3 \end{pmatrix}.$$

We take

$$\lambda = (\, 0 \ 0 \ 0 \ 0 \ 0 \ 1 \,), \quad \gamma = (\, 1 \ 0 \ 0 \ 0 \ 0 \ 0 \,)^T,$$

because the components of λ are the values at 0 of the series of the basis and γ gives the coordinates of $T(z)$.

Building a linear representation from the section operators gives the relation $\lambda A_0 = \lambda$ because the constant term of a series $g(z)$ is the constant term of $S_0 g(z)$ too. We call such a representation a standard linear representation. We have seen that every B-regular series $f(z)$ hides a rational series $S = \lambda(I + \Xi_+ \Xi^*)\gamma$, but for a standard representation it is simpler to introduce the rational series $R = \lambda\, \Xi^* \gamma$. Both series coincide on language $\mathcal{N} = \varepsilon + \mathcal{X}_+ \mathcal{X}^*$, but the first one extends $f(z)$ by 0 whereas the second one uses the rule $(R, x_0 w) = (R, w)$. Clearly each one determines the other and they have the same rank. By definition this is the rank of the series $f(z)$.

Recurrences. The B-regular series satisfy linear recurrences and the best way to find them is to use their Hankel matrices [5]. For the sake of simplicity, we assume the ring is a field $\mathbb{K}$.

The Hankel matrix of a series $f(z)$ is an infinite matrix whose rows are indexed by the integers and columns are indexed by the words in $\mathcal{X}_{\mathrm{B}}^*$. The columns of the matrix are simply the sequences (f_n), $(f_{\mathrm{B}n})$, $(f_{\mathrm{B}n+1})$, $\ldots$, $(f_{\mathrm{B}n+\mathrm{B}-1})$, $(f_{\mathrm{B}^2 n})$, $\ldots$, if we arrange the words according to their length and lexicographic order.

Definition 3. The Hankel matrix of $f(z) \in \mathbb{K}[[z]]$ is an infinite matrix of type $\mathbb{N} \times \mathcal{X}^*$. The coefficient $H_{n,w}$ of that matrix is $f_{\mathrm{B}^k n + r}$ if w has length k and r is the value of w for radix B.

Clearly a series is B-regular if and only if its Hankel matrix has finite rank. Moreover searching for relations between the columns of the matrix gives us recurrence relations.

Example 3. The van der Corput's sequence associates to an integer n with binary expansion $\epsilon_\ell \ldots \epsilon_0$ the rational number $v_n = \epsilon_0/2 + \epsilon_1/4 + \cdots + \epsilon_\ell/2^{\ell+1}$. It is 2-regular with rank 2 for it satisfies the recurrence

$$v_{2n} = v_n/2, \quad v_{2n+1} = 1/2 + v_n/2 \quad (n \geq 0) \ .$$

Its Hankel matrix begins with

$$\begin{pmatrix}
0 & 0 & 1/2 & 0 & 1/2 & 1/4 & 3/4 \\
1/2 & 1/4 & 3/4 & 1/8 & 5/8 & 3/8 & 7/8 \\
1/4 & 1/8 & 5/8 & 1/16 & 9/16 & 5/16 & 13/16 \\
3/4 & 3/8 & 7/8 & 3/16 & 11/16 & 7/16 & 15/16 \\
1/8 & 1/16 & 9/16 & 1/32 & 17/32 & 9/32 & 25/32 \\
5/8 & 5/16 & 13/16 & 5/32 & 21/32 & 13/32 & 29/32 \\
3/8 & 3/16 & 11/16 & 3/32 & 19/32 & 11/32 & 27/32 \\
7/8 & 7/16 & 15/16 & 7/32 & 23/32 & 15/32 & 31/32
\end{pmatrix} .$$

The two colums with indices ε and x_1 (the first and the third) are independents. Expressing the columns with indices x_0, $x_0 x_1$ and $x_1 x_1$ according to these, we obtain the relations

$$\begin{cases}
v_{2n} &= v_n/2 \ , \\
v_{4n+1} &= -v_n/4 + v_{2n+1} \ , \\
v_{4n+3} &= -v_n/2 + 3\, v_{2n+1}/2 \ ,
\end{cases}$$

which are easy to verify in this case. What we want to emphasize is the shape of these relations and a picture will be clearer than a long comment (see Figure 1).

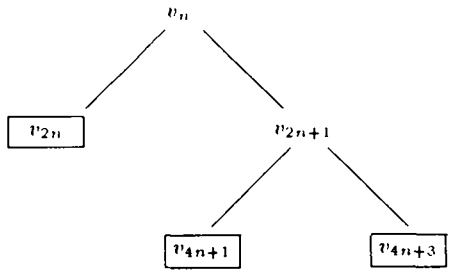

Fig. 1. The leaves of the tree give the shape of the recurrence relations.

This example epitomises the existence of a basis composed with sections $S_w f(z)$, such that the w are the addresses of the internal nodes of a B-ary tree. Furthermore to the leaves of the tree there correspond the recurrence relations; all the recurrences which express linear dependence between the sections are deduced from these [12].

Condensation. If $f(z)$ is B-regular and S is the associated rational series with support in $\mathcal{N} = \varepsilon + \mathcal{N}_+\mathcal{N}^*$, the commutative image [13, p. 147] is a rational series. We call it the condensate of $f(z)$ because it is simply

$$Kf(t) = f_0 + \sum_{l \geq 1} \left(\sum_{\mathrm{B}^{l-1} \leq n < \mathrm{B}^l} f_n \right) t^l \ .$$

The condensation is useful for regular series just as density is for a regular language.

Example 4. The Taylor series of the logarithm is not B-regular for all B. The condensate of the series

$$\frac{1}{z} \ln \frac{1}{1-z} = \sum_{n \geq 0} \frac{z^n}{n+1}$$

is

$$F(t) = 1 + \sum_{l \geq 1} (H_{\mathrm{B}^l} - H_{\mathrm{B}^{l-1}}) t^l \ ,$$

with H_n the n-th harmonic number. Using the equality

$$H_{\mathrm{B}^l} - H_{\mathrm{B}^{l-1}} \underset{l \to +\infty}{=} \ln \mathrm{B} + o(1)$$

and the transcendence of $\ln \mathrm{B}$, we see that $F(t)$ is not rational, hence the conclusion.

Closure. The closure properties of rational series show immediately that the set of B-regular series is a module left stable by Hadamard product. Besides, the Cauchy product of two B-regular series is B-regular (assuming that the ring is Noetherian) and a rational function is B-regular if and only if its poles are roots of unity (here we suppose the ring is a field). These properties have been established directly by Allouche and Shallit [2], using computation on sequences.

For the sake of simplicity we assume that we use a field in the next theorem.

Theorem 4 (Closure theorem). *A rational function is* B*-regular if and only if its poles are roots of unity. The set of* B*-regular series is closed under*

— *linear combination,*
— *Hadamard product (term by term product),*
— *Cauchy product (function product),*
— *derivation.*

Example 5. Greene and Knuth [11, pp. 25–28] consider the sequence $f(n)$ defined by

$$f(n) = 1 + \min_i \left\{ \frac{i-1}{n} f(i-1) + \frac{n-i}{n} f(n-i) \right\} .$$

which is relative to the search of an integer between 1 and n. The sequence $g(n) = nf(n)$ has second order difference given by

$$\Delta^2 g(n) = \begin{cases} 2 & \text{if } n \text{ is a power of 2} \\ 1 & \text{if } n \text{ is even but not a power of 2} \\ -1 & \text{if } n \text{ odd.} \end{cases}$$

Hence the generating series $g(z)$ is given by

$$g(z) = \frac{1}{(1-z)^2} \left(\frac{1}{1+z} + \sum_{k \geq 0} z^{2^k} \right)$$

and $g(z)$ is 2-regular as sum and product of 2-regular series.

Clearly the subject is not exhausted (we did not speak of Fatou lemma, of properties of coefficients, of decidability questions, *etc*).

2 Mahlerian Series and B-regular Series

As we want to extend the theorem of Christol *et alii* about automatic sequences, we recall at first the subject. Next we establish a general criterion and finally we apply the criterion to four cases:

1. a common case which is very useful because almost all divide-and-conquer recurrences are concerned,
2. the finite field case where we get back the theorem of Christol *et alii*,
3. the modular case, which provides examples where the ring is not an integral domain,
4. the algebraically closed field case, which completes the first case because it permits us to treat more complicated examples.

Let us recall the definition of a B-automatic sequence with values in a set $\mathcal{A}$. First a B-machine is a finite set of states, $\mathcal{S}$, with a distinguished initial state, i, and equipped with transitions $s \mapsto \epsilon.s$ $(0 \leq \epsilon < \mathrm{B})$ from $\mathcal{S}$ into itself. Next we adjoin to this B-machine an application π from $\mathcal{S}$ into $\mathcal{A}$ and so we have a B-automaton. Finally for each integer n, we write its B-ary expansion $\epsilon_\ell \cdots \epsilon_0$ and we compute the state $s = \epsilon_\ell . \cdots . \epsilon_1 . \epsilon_0 . i$ by going through the automaton from the state i according to the digits of n. The value of the sequence for n is $\pi(s)$.

Clearly the B-automatic sequences with values in a ring are B-regular sequences. The matrices of the transitions, the initial state and the output application provide a linear representation. Conversely a B-regular sequence which takes only a finite number of values is B-automatic.

The theorem under consideration is the next one and has given rise to an extended literature [1, 7].

Theorem 5 (Christol, Kamae, Mendès France, Rauzy). *The generating series of q-automatic sequences with values in the finite field $\mathbb{F}_q$ are exactly the series algebraic over the field $\mathbb{F}_q(z)$ of rational functions.*

This theorem is based on the equality $f(z^q) = f(z)^q$ for a formal series with coefficients in $\mathbb{F}_q$ and this is the reason why algebraic series are in question. In fact the equations which come naturally in light in this situation are Mahlerian equations.

Definition 6. A Mahlerian equation is a functional equation of the form

$$c_0(z)\,f(z) + c_1(z)\,f(z^{\mathrm{B}}) + \cdots + c_N(z)\,f(z^{\mathrm{B}^N}) = b(z)\ ,$$

where $c_0(z)$, ..., $c_N(z)$ are polynomials. A Mahlerian series is a power series which satisfies a non trivial homogeneous Mahlerian equation.

Our purpose is to extend the theorem to regular series and to separate the radix B and the characteristic m of the ring we use. We show first that every B-regular series is B-mahlerian, at least when the ring is a field. Next we give some criteria which focus on the coefficient $c_0(z)$ and ensure that a solution of the equation is B-regular.

Minimal Equation. Let us assume that the ring is a field $\mathbb{K}$. In this case one can develop an arithmetic for the ring of operators $\mathbb{K}[z, M]$, where M refer to the Mahler operator $f(z) \mapsto f(z^{\mathrm{B}})$. Precisely there is a Euclidean left division, which causes the left ideals to be principal and every Mahlerian series posesses a minimal homogeneous equation [8].

The proof given by Allouche [1] to etablish that a q-automatic series over $\mathbb{F}_q$ is algebraic remains adequate to show that a B-regular series is B-mahlerian. Moreover it often gives a minimal equation for the series if one uses carefully a linear representation of the series. The idea is just to express $f(z)$, $f(z^{\mathrm{B}})$, *etc* in the basis corresponding to the representation and it leads to an effective method of computation.

Example 6. The series $o(z) = \prod_{k\geq 0} \left(1 + 2\,z^{2^k}\right)$ gives the number of odd coefficients in a row of Pascal's triangle [2, ex. 14] [14, seq. 109] [15]. Consequently the complementary series $e(z) = \dfrac{1}{(1-z)^2} - o(z)$ gives the number of even coefficients in a row. This series is 2-regular with rank 3 and a representation is

$$A_0 = \begin{pmatrix} 0 & -2 & -4 \\ 1 & 3 & 4 \\ 0 & 0 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & -2 \\ 0 & 1 & 3 \end{pmatrix}, \quad \lambda = (\,0\ 0\ 1\,)\ , \quad \gamma = (\,1\ 0\ 0\,)^T.$$

The algorithm gives the equation

$$z^2e(z) - (3z^2 - z + 1)(z^2 + z + 1)e(z^2)$$
$$+ (3 + 4z^2 + 11z^4 + 2z^8 + 6z^6)e(z^4) - 2(2z^4 + 1)(1 + z^4)^2 e(z^8) = 0 .$$

In fact the minimal equation, which is the lcm of the minimal equations for $1/(1-z)^2$ and $o(z)$, is

$$z^2e(z) - [(1 + z^2)^2 + z^2(1 + 2z)]e(z^2) + (1 + z^2)^2(1 + 2z^2)e(z^4) = 0 .$$

Another proof, most in the spirit of this paper, consists in introducing the B-rational operators

$$F = \sum_{k \geq 0} c_k(z) M^k \in \mathbb{K}[[z, M]] ,$$

which are the images of the rational series S with support in $\mathcal{N} = \varepsilon + \mathcal{X}_+\mathcal{X}^*$ by the anti-morphism which associates to the letter x_r the operator $z^r M$. They are the natural intermediate between the rational series and the B-regular series, since every B-regular series is the value of a rational operator at the series 1. Using the closure properties of rational series and the arithmetic of operators, it is not difficult to prove that every B-rational operator satisfies an equality $QF = P$ where Q and P are two members of $\mathbb{K}[z, M]$ with the constraint $Q \neq 0$ and $\omega_M(Q) = 0$ (Q is a polynomial with respect to z and M and $\omega_M(Q)$ is the valuation of Q according to M). Now if $f(z)$ is a B-regular series it is written $f(z) = F.1$ where F is a rational operator; taking for Q a denominator of F, we have $Qf(z) = P.1$ hence a Mahlerian equation where the second member is a polynomial; it is not difficult to render it homogeneous.

General Criterion. For the rest of the paper we study the converse of the preceding property and we give first a general criterion to ensure that the solutions of a Mahlerian equation are B-regular.

Let us consider a Mahlerian equation

$$c_0(z)f(z) + c_1(z)f(z^{\mathrm{B}}) + \cdots + c_N(z)f(z^{\mathrm{B}^N}) = b(z)$$

where $b(z)$ is a B-regular series. We assume that the ring $\mathbb{A}$ is Noetherian and the coefficient of lowest degree in $c_0(z)$ is inversible in $\mathbb{A}$: we have $c_0(z) = Cz^\gamma g(z)$ with C inversible, γ a non negative integer and $g(0) = 1$. These constraints are normally fulfilled but we need to add the main condition: the set of the sections

$$S_{r_K} \cdots S_{r_1} \left(\frac{1}{g(z^{\mathrm{B}^{K-1}}) \cdots g(z^{\mathrm{B}})g(z)} \right) = S_{r_K} \frac{1}{g} \left(S_{r_{K-1}} \frac{1}{g} \left(\cdots S_{r_1} \left(\frac{1}{g} \right) \right) \right) ,$$

where $K \geq 0$, $0 \leq r_k < \mathrm{B}$ for $k = 1, \cdots, K$, is contained in a module of finite type. With these hypotheses a solution $f(z)$ of the equation is B-regular.

As we impose a condition only on coefficient c_0 and nothing on $c_1, \ldots, c_N$, there is no hope to find a necessary and sufficient condition. Nevertheless the hypothesis about the set of sections which appears in the criterion is exactly the condition which ensures that the Mahlerian infinite product

$$f(z) = \prod_{k \geq 0} \frac{1}{g(z^{\mathrm{B}^k})}$$

is B-regular.

Common Case. If $g(z) = 1$, the main condition vanishes and we have an easy criterion to recognize a B-regular series. The case contains almost all the divide-and-conquer recurrences and in view of its importance, we extend the result to study vector of series instead of series. This permits us to treat sequences which admits a definition by case according to the residue modulo a power of B, say B^{k+1}, which expresses $\mathrm{B}^{k+1}n + r$ according to the $\mathrm{B}^l n + s$ with $0 \leq l \leq k$. The next assertion uses a natural extension of B-regularity to vector of series.

Theorem 7 (Common case). *We consider a vector of series*

$$F(z) = (\ f_1(z)\ \ \ldots\ \ f_d(z)\ )^T$$

and we assume the following hypothesis:
— *the ring is Noetherian,*
— *the vector of series satisfies an equation*

$$z^\gamma F(z) + \sum_{k=1}^{N} C_k(z) F(z^{\mathrm{B}^k}) = B(z)$$

where $\gamma \geq 0$, $C_1(z), \ldots, C_N(z)$ are some square matrices of polynomials and $B(z)$ is a column matrix whose components are B*-regular series.*

With these conditions, the components of $F(z)$ are B*-regular series.*

Example 7. Supowit and Reingold [16] encountered the sequence (C_n) defined by the recurrence

$$\begin{cases} C_{4n} &= a(C_{2n+1} + C_{2n-1}) + b \\ C_{4n+1} &= a(C_{2n+1} + C_{2n}) \\ C_{4n+2} &= a(C_{2n+1} + C_{2n+1}) + b \\ C_{4n+3} &= a(C_{2n+2} + C_{2n+1}) \end{cases}$$

for $n \geq 1$ and the initial conditions $C_0 = C_1 = 0$, $C_2 = b$, $C_3 = ab$, with $a = 1/\sqrt{2}$ and $b = \sqrt{3}$. The number b is only a scale factor and with a division by b we may suppose $b = 1$.

We call $f(z)$ the generating series of (C_n) and we refer to the section $S_w f(z)$ as $f_w(z)$. The recurrence gives us the system

$$\begin{cases} f_{00}(z) &= a(1+z)f_1(z) + 1/(1-z) \\ f_{01}(z) &= af_1(z) + af_0(z) \\ f_{10}(z) &= 2af_1(z) + 1/(1-z) \\ f_{11}(z) &= af_0(z)/z + af_1(z)\ . \end{cases}$$

If we express $f_0(z)$ and $f_1(z)$ with respect to $f_{00}(z)$, $f_{01}(z)$, $f_{10}(z)$ and $f_{11}(z)$ as $f_\epsilon(z) = f_{0\epsilon}(z^2) + z f_{1\epsilon}(z^2)$, we obtain an equation

$$F(z) = a\, C_1(z) F(z^2) + B(z)$$

in which the unknown is the vector $F(z) = (\ f_{00}(z)\ \ f_{01}(z)\ \ f_{10}(z)\ \ f_{11}(z)\ )^T$ and the coefficients are given by

$$C_1(z) = \begin{pmatrix} 0 & 1+z & 0 & z(1+z) \\ 1 & 1 & z & z \\ 0 & 2 & 0 & 2z \\ 1/z & 1 & 1 & z \end{pmatrix}, \quad B(z) = \begin{pmatrix} 1/(1-z) \\ 0 \\ 1/(1-z) \\ 0 \end{pmatrix}.$$

In accordance with our result, we may assert that $F(z)$ and hence $f(z)$ is 2-regular.

Finite Fields and Rings. Let $p(z) \in \mathbb{A}[z]$ be a polynomial such that $p(0) = 1$. We say that T is the period of $p(z)$ if the sequence of coefficients of the formal power series $1/p(z)$ is periodic with period T. The study of the period [4] of

$$g(z^{\mathrm{B}^{K-1}}) \cdots g(z^{\mathrm{B}})g(z)$$

provide us with cases in which we can guarantee that the main condition is satisfied.

Theorem 8 (Finite field). *Let a formal series $f(z)$ have coefficients in the field $\mathbb{F}_q$ with characteristic p and satisfy a Mahlerian equation whose right-hand side is* B*-automatic*

$$c_0(z)\,f(z) + c_1(z)\,f(z^{\mathrm{B}}) + \cdots + c_N(z)\,f(z^{\mathrm{B}^N}) = b(z) \ .$$

We assume that $c_0(z) = C\,z^\gamma g(z)$ with $\gamma \geq 0$, $g(0) = 1$. If p divides B *or if the period T of $g(z)$ and the radix* B *have a common prime divisor, other than the characteristic p, then $f(z)$ is* B*-automatic.*

It is worth noting that $g(z)$ does not matter in the first condition about B. This case extends directly the theorem of Christol, Kamae, Mendès France and Rauzy.

Example 8. The polynomial $g(z) = 1 + z^2 + z^3$, which lies in $\mathbb{F}_2[z]$, is 7-periodic. Hence a formal series $f(z) \in \mathbb{F}_4[[z]]$ which satisfies a Mahlerian equation of the shape

$$z^{1993}(1 + z^2 + z^3)f(z) + c_1(z)f(z^{21}) + c_2(z)f(z^{441}) = 0$$

is 21-regular. (Here $p = 2$, $q = 4$, $T = 7$ and $\mathrm{B} = 21$.)

Starting from these results for the fields $\mathbb{F}_p$, it is not difficult to attain the quotient rings $\mathbb{Z}/(p^a)$. In fact if $g(z)$ has period t modulo p^a, it has period pt modulo p^{a+1}. Next the chinese remainder theorem permits us to consider rings $\mathbb{Z}/(m)$.

Theorem 9 (Modular case). *Let $f(z) \in \mathbb{Z}/(m)[[z]]$ be a formal series which satisfies*

$$c_0(z)f(z) + c_1(z)f(z^{\mathrm{B}}) + \cdots + c_N(z)f(z^{\mathrm{B}^N}) = b(z)$$

with right-hand side $b(z)$ B*-automatic, $c_0(z) = C\,z^\gamma g(z)$, C invertible, $\gamma \geq 0$ and $g(0) = 1$. We assume that for every prime divisor p of m, one of the next two conditions is satisfied: i) p divides* B*, or ii) there exists a prime number p' which is different from p and divides both the radix* B *and the period $T(g,p)$ of $g(z)$ reduced modulo p. Then $f(z)$ is* B*-automatic.*

Example 9. Let us consider the integer sequence (u_n) defined by the initial conditions $u_0 = 0$, $u_1 = 1$ and the recurrence relation

$$u_n = u_{n-1} + u_{n-2} + u_{\lfloor n/2 \rfloor} \ .$$

Clearly u_n is greater than the Fibonacci number F_{n-1} and the generating series

$$u(z) = z + 2\,z^2 + 4\,z^3 + 8\,z^4 + 14\,z^5 + 26\,z^6 + 44\,z^7 + 78\,z^8 + \cdots$$

is not 2-regular because its coefficients grow too rapidly. Nevertheless it is 2-regular when we reduce it modulo every integer. It suffices to look at the primary numbers p^a. If $p = 2$ the result is immediatly obtained for p equals B. Otherwise it suffices to remark that the period of $1 - z - z^2$ modulo an odd prime is even, because the Mahlerian equation which is to be considered is

$$(1 - z - z^2)u(z) - (1 + z)u(z^2) = z \ .$$

Example 10. A B-ary partition is an integer partition in which the parts are power of B. As an illustration there are nine 3-partitions of 16, namely 1^{16}, $1^{13}3$, $1^{10}3^2$, $1^7 3^3$, $1^4 3^4$, 13^5, $1^7 9$, $1^4 3\,9$, $13^2 9$ (we use the classical notation: $13^2 9$ refers to $1 + 3 + 3 + 9$). The generating function of the number of B-ary partition is [3, p. 161]

$$p(z) = \prod_{k=0}^{+\infty} \frac{1}{1 - z^{\mathrm{B}^k}}$$

and it satisfies the Mahlerian equation

$$(1 - z)p(z) = p(z^{\mathrm{B}}) \ .$$

Because the period of $g(z) = 1 - z$ is 1 modulo every integer, we cannot use the second condition of our theorem, but the first one shows that $p(z)$ is B-regular if we reduce it modulo m and every prime divisor of m divides B. As an example the number of binary partition reduced modulo 8 may be defined by the 2-automaton

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

$$\lambda = (\,1\ 1\ 0\ 4\ 2\ 0\ 6\,), \quad \gamma = (\,1\ 0\ 0\ 0\ 0\ 0\ 0\,)^T .$$

Algebraically Closed Field. Finally we apply our criterion to algebraically closed fields. Here the trick to obtain the main condition is to impose that

$$S_{r_K} \cdots S_{r_1} \left(\frac{1}{g(z^{\mathrm{B}^{K-1}}) \cdots g(z^{\mathrm{B}}) g(z)} \right)$$

have poles in a finite set with bounded multiplicities. This guarantees that they lie in a vector space of finite dimension. We obtain the following theorem.

Theorem 10 (Algebraically closed field). *Let $f(z)$ be a formal series with coefficients in an algebraically closed field. We assume that $f(z)$ satisfies a Mahlerian equation*

$$c_0(z)f(z) + c_1(z)f(z^{\mathrm{B}}) + \cdots + c_N(z)f(z^{\mathrm{B}^N}) = b(z)$$

in which $b(z)$ is B-regular, $c_0(z) = C\,z^\gamma g(z)$ with $C \neq 0$, $\gamma \geq 0$ and $g(0) = 1$. If all the roots of $g(z)$ are roots of unity with an order (in the sense of group theory) which is not prime relative to B, *then $f(z)$ is* B*-regular.*

Example 11. Let us consider the integer sequence (u_n) defined by $u_0 = 0$, $u_1 = 1$ and the recurrence

$$u_n = u_{n-1} - u_{n-2} + u_{\lfloor n/3 \rfloor} \quad (n \geq 2) \ .$$

Its generating function $u(z)$ is the solution of

$$(1 - z + z^2)u(z) - u(z^3) = z \ .$$

The roots of $1 - z + z^2$ are the primitive 6-th roots of unity, hence $u(z)$ is 3-regular. Besides its rank is 3. Moreover it is 3-automatic according to the equality

$$u(z) = (1 + z) \sum_{k,l \geq 0} (-1)^l z^{3^k(3l+1)} \ .$$

Acknowledgement. This work was (partially) supported by the ESPRIT Basic Research Action Nr. 7141 (ALCOM II).

References

1. J.-P. Allouche. Automates finis en théorie des nombres. *Expositiones Mathematicae*, 5:239–266, 1987.
2. J.-P. Allouche and J. Shallit. The ring of k-regular sequences. *Theoretical Computer Science*, 98:163–197, 1992.
3. G. E. Andrews. *The Theory of Partitions*, volume 2 of *Encyclopedia of Mathematics and its Applications*. Addison–Wesley, 1976.
4. E. R. Berlekamp. *Algebraic Coding Theory*. Mc Graw-Hill, revised 1984 edition, 1968.
5. J. Berstel and Ch. Reutenauer. *Rational series and their languages*, volume 12 of *EATCS monographs on theoretical computer science*. Springer, 1988.
6. G. Christol, T. Kamae, M. Mendès France, and G. Rauzy. Suites algébriques, automates et substitutions. *Bulletin de la Société Mathématique de France*, 108:401–419, 1980.
7. M. Dekking, M. Mendès France, and A. Van der Poorten. Folds! *Mathematical Intelligencer*, 4:130–138, 173–181, 190–195, 1982.
8. Philippe Dumas. *Récurrences Mahlériennes, suites automatiques, et études asymptotiques*. Doctorat de mathématiques, Université de Bordeaux I, 1993.
9. Philippe Flajolet and Mordecai Golin. Exact asymptotics of divide-and-conquer recurrences. Proceedings of ICALP'93, Lund., July 1993. This volume.
10. Philippe Flajolet, Peter Grabner, Peter Kirschenhofer, Helmut Prodinger, and Robert Tichy. Mellin transforms and asymptotics: Digital sums, July 1991. 23 pages. INRIA Research Report. Accepted for publication in *Theoretical Computer Science*.
11. D. H. Greene and D. E. Knuth. *Mathematics for the analysis of algorithms*. Birkhauser, Boston, 1981.
12. Ch. Reutenauer. Séries rationnelles et algèbres syntactiques. Master's thesis, Université Pierre et Marie Curie (Paris VI), 1980.
13. A. Salomaa and M. Soittola. *Automata-Theoretic Aspects of Formal Power Series*. Springer, Berlin, 1978.
14. N. J. A. Sloane. *A Handbook of Integer Sequences*. Academic Press, 1973.
15. Kenneth B. Stolarsky. Power and exponential sums of digital sums related to binomial coefficients. *SIAM Journal on Applied Mathematics*, 32(4):717–730, 1977.
16. K. J. Supowit and E. M. Reingold. Divide and conquer heuristics for minimum weighted Euclidean matching. *SIAM Journal on Computing*, 12(1):118–143, February 1983.

Unité de Recherche INRIA Rocquencourt
Domaine de Voluceau - Rocquencourt - B.P. 105 - 78153 LE CHESNAY Cedex (France)

Unité de Recherche INRIA Lorraine Technopôle de Nancy-Brabois - Campus Scientifique
615, rue du Jardin Botanique - B.P. 101 - 54602 VILLERS LES NANCY Cedex (France)
Unité de Recherche INRIA Rennes IRISA, Campus Universitaire de Beaulieu 35042 RENNES Cedex (France)
Unité de Recherche INRIA Rhône-Alpes 46, avenue Félix Viallet - 38031 GRENOBLE Cedex (France)
Unité de Recherche INRIA Sophia Antipolis 2004, route des Lucioles - B.P. 93 - 06902 SOPHIA ANTIPOLIS Cedex (France)

EDITEUR
INRIA - Domaine de Voluceau - Rocquencourt - B.P. 105 - 78153 LE CHESNAY Cedex (France)

ISSN 0249 - 6399
RR.1931