Mathematica Slovaca

Jean-Paul Allouche; Klaus Scheicher; Robert Franz Tichy

Regular maps in generalized number systems

Mathematica Slovaca, Vol. 50 (2000), No. 1, 41--58

Persistent URL: http://dml.cz/dmlcz/133301

Math. Slovaca, **50** (2000), No. 1, 41–58

Mathematica Slovaca

REGULAR MAPS IN GENERALIZED NUMBER SYSTEMS

JEAN-PAUL ALLOUCHE* — KLAUS SCHEICHER** — ROBERT F. TICHY**

(Communicated by Stanislav Jakubec)

ABSTRACT. This paper extends some results of Allouche and Shallit for q-regular sequences to numeration systems in algebraic number fields and to linear numeration systems. We also construct automata that perform addition and multiplication by a fixed number.

1. Introduction

A sequence is called q*-automatic* if its nth term can be generated by a finite state machine from the q-ary digits of n. The concept of automatic sequences was introduced in 1969 and 1972 by Cobham [8], [9]. In 1979 Christol [6] (see also Christol, Kamae, Mendès France and Rauzy [7]) discovered a nice arithmetic property of automatic sequences:

A sequence with values in a finite field of characteristic p is p-automatic if and only if the corresponding power series is algebraic over the field of rational functions over this finite field.

A brief survey on this subject is given in [2], see also [10]. Some generalizations of this concept were studied in [27], [23], [24], [3], see also the survey [1]. An automatic sequence has to take its values in a finite set. To relax this condition, Allouche and Shallit [5] introduced the notion of q*-regular sequences.* To give a hint of what q-regularity is, let us consider the following example. If $S(n)$ is the sum of the binary digits of n, then the sequence

$$n \longrightarrow S(n) \mod 2$$

is 2-automatic (this is the well-known Prouhet-Thue-Morse sequence), whereas the sequence

$$n \longrightarrow S(n)$$

1991 Mathematics Subject Classification: Primary 11B85, 11K31.
Key words: q-automatic sequence, q-regular map, numeration system.

is 2-regular.

Shallit [27] generalized the concept of q-automaticity to number systems with respect to linear recurring base sequences. The purpose of this paper is to generalize q-regularity to number systems in algebraic number fields as well as to number systems with respect to linear recurring bases.

2. Canonical number systems in algebraic fields

Let $\mathbb{Q}$ be the field of rational numbers. Let $\mathbb{K} = \mathbb{Q}(\alpha)$ be the simple extension field generated by the algebraic number α, and let $\mathbb{Z}_{\mathbb{K}}$ be the ring of algebraic integers in $\mathbb{K}$. For $\beta \in \mathbb{K}$ the symbol $N(\beta)$ denotes the norm of β and $\mathcal{N} = \{0, 1, \dots, |N(\beta)| - 1\}$. We say that $\{\beta, \mathcal{N}\}$ is a *canonical number system* (*CNS*) in $\mathbb{Z}_{\mathbb{K}}$ for some $\beta \in \mathbb{Z}_{\mathbb{K}}$, if every $\gamma \in \mathbb{Z}_{\mathbb{K}} \setminus \{0\}$ can be uniquely represented as

$$\gamma = a_0 + a_1\beta + \dots + a_h\beta^h, \qquad a_i \in \mathcal{N}, \ i = 0, 1, \dots, h, \quad a_h \neq 0.$$

This concept is a natural generalization of the base number systems in $\mathbb{Z}$. For an extensive literature we refer to Knuth [19]. The canonical number systems in the ring of integers of quadratic number fields were characterized by Kátai, Szabó [17] and Kátai, Kovács [15], [16]. Kovács [20] gave a necessary and sufficient condition for the existence of CNS in $\mathbb{Z}_{\mathbb{K}}$.

THEOREM 2.1 (KOVÁCS). *Let $\mathbb{K} = \mathbb{Q}(\alpha)$ be an extension of degree n, $n \geq 3$. There is a CNS in $\mathbb{Z}_{\mathbb{K}}$ if and only if there exists $\beta \in \mathbb{Z}_{\mathbb{K}}$ such that $\{1, \beta, \dots, \beta^{n-1}\}$ is an integral base of $\mathbb{Z}_{\mathbb{K}}$.*

Kovács and Pethő [21] characterized all those integral domains that have number systems.

Scheicher [25], [26] recently gave a new proof of the above theorem generalizing a result of Thuswaldner [28]. The main tool of his proof is the following:

LEMMA 2.1. *Let $\beta \in \mathbb{Z}_{\mathbb{K}}$, and let $\{1, \beta, \dots, \beta^{n-1}\}$ be an integral base of $\mathbb{Z}_{\mathbb{K}}$. Let β be a zero of the polynomial $x^n + b_{n-1}x^{n-1} + \dots + b_0$ with*

$$b_i \in \mathbb{Z}, \quad b_0 \geq 2, \quad \text{and} \quad b_0 \geq b_1 \geq \dots \geq b_{n-1} \geq 1,$$

and let $\mathcal{D} = \{0, 1, \dots, b_0 - 1\}$. Then $\{\beta, \mathcal{D}\}$ is a CNS in $\mathbb{Z}_{\mathbb{K}}$. Furthermore there exists a finite automaton with at most $2^{n+1} - 1$ states that is able to add 1 to every $\gamma \in \mathbb{Z}_{\mathbb{K}}$. Each state q_j can be interpreted as an additional carry. Such a *carry* q_j *has the form*

$$\begin{aligned} q_j = \ & (b_{i_1} \quad - b_{i_2} \quad + b_{i_3} \quad - \dots) \\ & + (b_{i_1+1} - b_{i_2+1} + b_{i_3+1} - \dots)\beta \\ & + (b_{i_1+2} - b_{i_2+2} + b_{i_3+2} - \dots)\beta^2 \\ & \vdots \end{aligned} \tag{1}$$

where $\{i_1, i_2, \dots, i_k\}$ *is a nonempty subset of* $\{0, \dots, n\}$.

3. The set of β-regular functions

Let $\mathbb{K} = \mathbb{Q}(\alpha)$ be an extension of degree n, and let $\{\beta, \mathcal{N}\}$ be a CNS in $\mathbb{Z}_{\mathbb{K}}$. Let $\boldsymbol{E}$ be a commutative Noetherian ring, and let $\boldsymbol{R}$ be a subring of $\boldsymbol{E}$.

DEFINITION 3.1. Let $s\colon \mathbb{Z}_{\mathbb{K}} \to \boldsymbol{E}$.

- The function s is called β*-automatic*, if $s(x)$ is a finite state function of the base-β expansion of x (see also [3]).
- The β*-kernel* of s is the set of functions

  $$K_\beta(s) = \left\{ s(\beta^k x + l) : \ k \geq 0, \ l \in \mathbb{Z}_{\mathbb{K},k} \right\}$$

  where

  $$\mathbb{Z}_{\mathbb{K},k} = \left\{ \sum_{j=0}^{k-1} d_j \beta^j : \ 0 \leq d_j \leq |N(\beta)| - 1 \right\}.$$

- The function s is called β*-regular*, if there exists a finite number of functions $s_1, \dots, s_r$ with values in $\boldsymbol{E}$, such that each function in the β-kernel is an $\boldsymbol{R}$-linear combination of the s_i's.
- Let

  $$x \in \mathbb{Z}_{\mathbb{K}}, \quad x = \sum_{j=0}^{k-1} d_j \beta^j, \quad d_j \in \mathcal{N},$$

  then the *shift-function* σ is given by

  $$\sigma(x) = \frac{x - d_0}{\beta} = \sum_{j=0}^{k-2} d_{j+1} \beta^j.$$

- There is a natural total ordering of the elements of each $\mathbb{Z}_{\mathbb{K},t}$; namely the lexicographic order (from most significant to least significant digit) induced by the order on digits. We define $\phi(x)$ the *index-function* of x by

$$\phi\left(\sum_{j=0}^{h} d_j\beta^j\right) = \sum_{j=0}^{h} d_j|N(\beta)|^j \qquad \text{and} \qquad \phi(0) = 0\,.$$

THEOREM 3.1. *The following statements are equivalent:*

(a) *The function $s\colon \mathbb{Z}_{\mathbb{K}} \to \boldsymbol{E}$ is β-regular.*

(b) *There exists a finite number of functions $s_1,\dots,s_r$ with values in $\boldsymbol{E}$ such that the $\boldsymbol{R}$-module generated by $K_\beta(s)$ is included in the $\boldsymbol{R}$-module generated by $s_1,\dots,s_r$. We write $\langle K_\beta(s)\rangle \subset \langle s_1,\dots,s_r\rangle$.*

(c) *There exists a finite number of functions $s_1,\dots,s_r$ with values in $\boldsymbol{E}$ such that $\langle K_\beta(s)\rangle = \langle s_1,\dots,s_r\rangle$.*

(d) *The $\boldsymbol{R}$-module generated by $K_\beta(s)$ is generated by a finite number of functions $s(\beta^{f_i}x + k_i)$, $k_i \in \mathbb{Z}_{\mathbb{K},f_i}$.*

(e) *There exists a positive integer E such that, for all $e_j > E$, each function $s(\beta^{e_j}x + r_j)$ with $r_j \in \mathbb{Z}_{\mathbb{K},e_j}$ can be expressed as an $\boldsymbol{R}$-linear combination*

$$s(\beta^{e_j}x + r_j) = \sum_i c_{ij}s(\beta^{f_{ij}}x + k_{ij})\,,$$

where $f_{ij} \le E$ and $k_{ij} \in \mathbb{Z}_{\mathbb{K},f_{ij}}$.

(f) *There exist an integer r and r functions $s = s_1,\dots,s_r$, such that for $1 \le i \le r$ the $|N(\beta)|$ functions $s_i(\beta x + a)$, $x \in \mathbb{Z}_{\mathbb{K}}$, $a \in \mathbb{Z}_{\mathbb{K},1}$ are $\boldsymbol{R}$-linear combinations of the s_i.*

(g) *There exist an integer r and r functions $s = s_1,\dots,s_r$, and $|N(\beta)|$ matrices $B_0,\dots,B_{|N(\beta)|-1}$ in $\boldsymbol{R}^{r\times r}$, such that, if*

$$V(x) = \begin{pmatrix} s_1(x) \\ \vdots \\ s_r(x) \end{pmatrix},$$

then

$$V(\beta x + k) = B_k V(x) \qquad \text{for} \quad k \in \mathbb{Z}_{\mathbb{K},1}\,.$$

Proof.

(a) $\Longrightarrow$ (b). This is trivial.

(b) $\Longrightarrow$ (c). It suffices to remember that, if $\boldsymbol{R}$ is a Noetherian ring, then any $\boldsymbol{R}$-submodule of an $\boldsymbol{R}$-module of finite type has finite type.

(c) $\Longrightarrow$ (d). There exist $s_1,\dots,s_r$ such that $\langle K_\beta(s)\rangle = \langle s_1,\dots,s_r\rangle$. Each s_i is a linear combination of elements of $K_\beta(s)$, and there are only finitely many s_i, so $\langle K_\beta(s)\rangle$ is generated by only finitely many members of $K_\beta(s)$.

(d) $\Longrightarrow$ (e). Let $\langle K_\beta(s)\rangle = \langle s(\beta^{f_i}x + b_i),\ i \le i'\rangle$. Let $E = \max\limits_{1\le i\le i'} f_i$. Then for all $e_j > E$, we can write

$$s(\beta^{e_j}x + a_j) = \sum_i c_{ij} s(\beta^{f_{ij}}x + b_{ij}),$$

where $f_{ij} \le E$ and $b_{ij} \in \mathbb{Z}_{\mathbb{K},f_{ij}}$.

(e) $\Longrightarrow$ (f). Take as the r functions the functions $s_i(x) = s(\beta^{f_i}x + b_i)$ with $0 \le f_i \le E$ and $b_i \in \mathbb{Z}_{\mathbb{K},f_i}$. Then

$$s_i(\beta x + a) = s(\beta^{f_i}(\beta x + a) + b_i) = s(\beta^{f_i+1}x + a\beta^{f_i} + b_i),$$

which, if $f_i + 1 \le E$, is an element of $K_\beta(s)$, and if $f_i + 1 > E$ is a linear combination of elements of $K_\beta(s)$.

(f) $\Longrightarrow$ (g). Follows trivially.

(g) $\Longrightarrow$ (a). We need to see that $s(\beta^e x + a)$ is a linear combination of the s_i. Express a in base β as

$$\sum_{0\le i<e} a_i\beta^i,$$

then it is easy to see that

$$V(\beta^e x + a) = B_{a_0}B_{a_1}\cdots B_{a_{e-1}}V(x),$$

and this expresses $s(\beta^e x + a)$ as a linear combination of the s_i. $\square$

THEOREM 3.2. *The function $s\colon \mathbb{Z}_{\mathbb{K}} \to \boldsymbol{E}$ is β-automatic if and only if it is β-regular and takes only finitely many values.*

Proof. If a function is β-automatic, it takes only a finite number of values. As $K_\beta(s)$ is finite, it clearly generates a finitely generated module.

Suppose now that $s(x)$ is β-regular and takes only a finite number of values. Theorem 3.1(g) implies that there exist functions $s = s_1, \dots, s_d$ in $K_\beta(s)$, and matrices $B_0, \dots, B_{|N(\beta)|-1}$ such that $V(x) = (s_1(x), \dots, s_d(x))^T$ satisfies

$$V(\beta x + k) = B_k V(x)$$

for all $k \in \mathbb{Z}_{\mathbb{K},1}$ and $x \in \mathbb{Z}_{\mathbb{K}}$. We will study functions $s(\beta^j x + r)$ with $r \in \mathbb{Z}_{\mathbb{K},j}$. Let $r = \sum_{k=0}^{j-1} d_k\beta^k$. Then

$$V(\beta^j x + r) = B_{d_0}\cdots B_{d_{j-1}}V(x).$$

Let Θ be the set of all values of V. This set is finite since $s_i(\mathbb{Z}_{\mathbb{K}}) \subset s(\mathbb{Z}_{\mathbb{K}})$ and $s(\mathbb{Z}_{\mathbb{K}})$ is finite. Thus the B_k's are functions from the finite set Θ into itself. Since there are only finitely many maps from a finite set into itself, the set of maps $x \mapsto V(\beta^j x + r)$, $j \ge 0$, $r \in \mathbb{Z}_{\mathbb{K},j}$, is finite. Hence $K_\beta(s)$ is finite. $\square$

THEOREM 3.3. *Let $s(x)$ and $t(x)$ be β-regular functions. Let α be a constant. Then $(s+t)(x) = s(x) + t(x)$, $(s \cdot t)(x) = s(x) \cdot t(x)$ and $(\alpha \cdot s)(x)$, $x \in \mathbb{Z}_{\mathbb{K}}$ are β-regular.*

Proof. Let $K_\beta(s) = \langle s_1, \ldots, s_r \rangle$, $\langle K_\beta(t) \rangle = \langle t_1, \ldots, t_{r'} \rangle$. Then $\langle K_\beta(s+t) \rangle$ is generated by the $r + r'$ functions $\{s_1, \ldots, s_r, t_1, \ldots, t_{r'}\}$. And $\langle K_\beta(s \cdot t) \rangle$ is generated by the $r \cdot r'$ functions $\{s_i \cdot t_j\}$, $0 \le i \le r$, $0 \le j \le r'$. Finally $\langle K_\beta(\alpha s) \rangle$ is generated by the r functions $\{\alpha s_1, \ldots, \alpha s_r\}$. □

THEOREM 3.4. *Let $u, v \in \mathbb{Z}_{\mathbb{K}}$, $u \neq 0$ such that the digits of $uz + v$ can be computed by a finite automaton from the digits of z, for all $z \in \mathbb{Z}_{\mathbb{K}}$. If $s(x)$, $x \in \mathbb{Z}_{\mathbb{K}}$, is a β-regular function, then the function $s(ux + v)$ is also β-regular.*

Proof. Define $t(x) = s(ux + v)$. There exist functions $s_1, \ldots, s_r$ such that $\langle K_\beta(s) \rangle \subset \langle s_1, \ldots, s_r \rangle$. Take now an element of the β-kernel of $t(x)$, say $t(\beta^k x + l)$, $l \in \mathbb{Z}_{\mathbb{K},k}$. Consider the base-$\beta$ expansion of $ul + v$ and write it as $ul + v = \beta^k a + b$. This expansion can be computed by a finite automaton from the digits of l. But

$$\begin{aligned} t(\beta^k x + l) &= s\big(u(\beta^k x + l) + v\big) \\ &= s\big(\beta^k(ux + a) + b\big). \end{aligned}$$

Since $l \in \mathbb{Z}_{\mathbb{K},k}$ and $a = \sigma^k(ul + v)$ there exists only a finite number of possible values of a. (The automaton has a finite number of states.) Hence $t(\beta^k x + l)$ is the value at the point $ux + a$ of an element of $K_\beta(s)$. □

Remark 3.1. The second author has written a computer program that constructs such automata.

THEOREM 3.5. *Let f be an integer ≥ 1. Then $s(x)$ is β-regular if and only if it is β^f-regular.*

Proof. Since $K_{\beta^f}(s) \subset K_\beta(s)$ the function is β^f-regular if it is β-regular. Assume now that $s(x)$ is β^f-regular. We will show that there exists a B such that for all $b > B$ and $c \in \mathbb{Z}_{\mathbb{K},b}$ each function $s(\beta^b x + c)$ can be expressed as a linear combination

$$s(\beta^b x + c) = \sum_i d_i s(\beta^{b_i} x + c_i)$$

with $b_i < B$ and $c_i \in \mathbb{Z}_{\mathbb{K},b_i}$. The result will then follow from Theorem 3.1(e). Let us write $b = fr + u$ with $0 \le u < f$, and $c = q\beta^{fr} + t$ with $t \in \mathbb{Z}_{\ ,f}$. From 3.1(e), there exists an E such that for all $r > E$ we can write

$$s\big((\beta^f)^r y + t\big) = \sum_i d_i s\big((\beta^f)^{r_i} y + t_i\big),$$

where $r_i < E$ and $t_i \in \mathbb{Z}_{\mathbb{K},fr_i}$.

Now put $y = \beta^u x + q$. We find

$$\begin{aligned} s\big((\beta^f)^r y + t\big) &= s(\beta^b x + c) \\ &= \sum_i d_i s\big(\beta^{fr_i+u} x + q\beta^{fr_i} + t_i\big) \\ &= \sum_i d_i s(\beta^{b_i} x + c_i)\,, \end{aligned}$$

where $b_i = fr_i + u$ and $c_i = q\beta^{fr_i} + t_i$. Note that $b_i < fE + f$ and $q \in \mathbb{Z}_{\mathbb{K},u}$. So

$$c_i = q\beta^{fr_i} + t_i \in \mathbb{Z}_{\mathbb{K},u+fr_i} = \mathbb{Z}_{\mathbb{K},b_i}\,.$$

Thus we may take $B = f(E+1)$. Hence $s(x)$ is β-regular. □

THEOREM 3.6. *Consider the ring of Gaussian integers $\mathbb{Z}_{\mathbb{K}} = \{x + yI : x, y \in \mathbb{Z}\}$, where $I^2 = -1$. Let $\beta = -a + I$, with $a \in \mathbb{N} \setminus \{0\}$. If $s(x)$ is a β-regular function, then there exists a constant c such that $|s(x)| = O\big(|x|^c\big)$.*

Proof. Let

$$x = \sum_{j=0}^{k-1} d_j \beta^j\,.$$

Then, by [14; Proposition 2.6], we have

$$\begin{aligned} 2\log_{a^2+1}|x| - 2\log_{a^2+1}\frac{a\sqrt{a^2+4}}{a^2+2} - 4 &\le k-1 \\ \le 2\log_{a^2+1}|x| - \log_{a^2+1}\left(1 - \frac{a\sqrt{a^2+4}}{a^2+2}\right) + 4\,. \end{aligned}$$

Thus

$$k \le b + 2\log_{a^2+1}|x|\,.$$

Theorem 3.1(g) gives

$$V(x) = B_{d_0} B_{d_1} \cdots B_{d_{k-1}} V(0)\,.$$

Let $|\cdot|$ be a vector-norm, let $\|\cdot\|$ be a matrix-norm, compatible with $|\cdot|$ (hence $|Mv| \le \|M\||v|$). Thus we see

$$|s(x)| \le |V(x)| \le \|B_{d_0}\|\|B_{d_1}\| \cdots \|B_{d_{k-1}}\||V(0)|\,.$$

Now let $c = \max\limits_{0 \le i \le k-1} \|B_i\|$, and $d = \|V(0)\|$. Then

$$|s(x)| \le c^{b + 2\log_{a^2+1}|x|} d \le d'|x|^{c'}\,.$$

□

EXAMPLE 3.1. We give here some examples of β-regular functions.

(a) Polynomials in x are β-regular functions since 1 and x are β-regular functions.

(b) The index-function $\phi(x)$ is β-regular since, for $j \in \mathbb{Z}_{\mathbb{K},k}$, we have $\phi(\beta^k x + j) = |N(\beta)|^k \phi(x) + \phi(j)1$.

(c) Suppose

$$x = \sum_{j \geq 0} d_j \beta^j$$

for $d_j \in \{0, \dots, |N(\beta)| - 1\}$.

In this expansion let h be the least index j such that $d_j \neq 0$. Then β^h is called the *β-residue* of x. We will construct an array $A(\beta) = \big(a(i,j)\big)_{i,j \geq 0}$ in the following way.

The first row of $A(\beta)$ contains the elements β^j, $j \geq 0$, i.e., $a(1,j) = \beta^{j-1}$. Column 1 contains the elements of $\mathbb{Z}_{\mathbb{K}}$ with β-residue 1.

Generally column j contains the elements with β-residue β^{j-1}.

If, for example $N(\beta) = 2$, then the lexicographic ordering of the elements of $\mathbb{Z}_{\mathbb{K}}$ is

$$(1), (01), (11), (001), (101), \dots .$$

Then we have

$$A(\beta) = \begin{bmatrix} (1) & (01) & (001) & \dots \\ (11) & (011) & (0011) & \dots \\ (101) & (0101) & (00101) & \dots \\ \dots & \dots & \dots & \dots \end{bmatrix}.$$

Thus every element of $\mathbb{Z}_{\mathbb{K}}$ occurs exactly once in $A(\beta)$.

DEFINITION 3.2. (see [18]) The *paraphrase-function* $p_\beta \colon \mathbb{Z}_{\mathbb{K}} \to \mathbb{N}$ is defined as follows

$$p_\beta(x) = \text{the index of the row of } A(\beta) \text{ in which } x \text{ occurs.}$$

Thus, if $x = a(i,j)$ then $p_\beta(x) = i$.

Remark 3.2. We get the paraphrase by ordering the elements of $\mathbb{Z}_{\mathbb{K}}$ lexicographically, beginning with the least significant digit.

THEOREM 3.7. *The paraphrase $p_\beta(x)$ is β-regular.*

Proof. If $\beta^e x + f = a(m,n)$ then $p_\beta(\beta^e x + f) = m$. Now f can be written as $f = \beta^{n-1} z$ for $0 \leq n-1 < e$. Thus $\beta^e x + f = \beta^e x + \beta^{n-1} z = \beta^{n-1}\big(\beta^{e-n+1} x + z\big)$ and

$$p_\beta(\beta^e x + f) = p_\beta\big(\beta^{e-n+1} x + z\big) \cdot$$

(If $\beta^e x + f = a(m,n)$, then $\beta^{e-n+1}x + z = a(m,1)$.) A simple consideration gives that

$$p_\beta(x) = \phi(x) - \left\lfloor \frac{\phi(x)}{|N(\beta)|} \right\rfloor \tag{2}$$

for all x that occur in the first column of $A(\beta)$. Hence

$$\begin{aligned} p_\beta(\beta^{e-n+1}x + z) &= \phi(\beta^{e-n+1}x + z) - \left\lfloor \frac{\phi(\beta^{e-n+1}x + z)}{|N(\beta)|} \right\rfloor \\ &= |N(\beta)|^{e-n+1}\phi(x) + \phi(z) - \left\lfloor \frac{|N(\beta)|^{e-n+1}\phi(x) + \phi(z)}{|N(\beta)|} \right\rfloor \\ &= |N(\beta)|^{e-n}\big(|N(\beta)| - 1\big) \cdot \phi(x) + \left(\phi(z) - \left\lfloor \frac{\phi(z)}{|N(\beta)|} \right\rfloor\right) \cdot 1 . \end{aligned}$$

Since $\phi(x)$ and 1 are β-regular $p_\beta(x)$ is β-regular. □

(d) The trace $\mathrm{Tr}(x)$ is β-regular. Since $\beta^n + b_{n-1}\beta^{n-1} + \dots + b_0 = 0$, there exist $a_{ki} \in \mathbb{Z}$ such that

$$\beta^k = \sum_{i=0}^{n-1} a_{ki}\beta^i .$$

Thus

$$\mathrm{Tr}(\beta^k x + l) = \sum_{i=0}^{n-1} a_{ki}\,\mathrm{Tr}(\beta^i x) + \mathrm{Tr}(l) .$$

THEOREM 3.8. *Let $\boldsymbol{R}$ be a Noetherian ring without zero divisors, and let $a \in \boldsymbol{R}$. Then, the function $s(x) = a^{\phi(x)}$ is β-regular if and only if $a = 0$ or a is a root of unity.*

Proof. One direction is trivial: Let $a^k = 1$, $k \in \mathbb{N} \setminus \{0\}$. Since $\phi(x)$ is regular, $\phi(x) \mod k$ is automatic. Thus $a^{\phi(x)} = a^{\phi(x) \bmod k}$ is automatic. Thus $a^{\phi(x)}$ is regular.

Assume now that $a^\phi(x)$ is β-regular. Then, there exist $r < \infty$ and λ_j with $0 \le j < r$, such that

$$\forall x \in \mathbb{Z}_{\mathbb{K}} \qquad \sum_{0 \le j < r} \lambda_j \big(a^{|N(\beta)|^{f_i}}\big)^{\phi(x)} = 0 .$$

We use the following formula for the Vandermonde determinant:

$$\begin{pmatrix} 1 & \xi_0 & \xi_0^2 & \dots & \xi_0^m \\ 1 & \xi_1 & \xi_1^2 & \dots & \xi_1^m \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \xi_m & \xi_m^2 & \dots & \xi_m^m \end{pmatrix} = \prod_{i>j} (\xi_i - \xi_j) .$$

From this, we can see that the functions $\xi_j^{\phi(x)}$ are linearly independent if and only if the numbers $\xi_1, \xi_2, \ldots, \xi_m$ are distinct.

Hence the numbers $a^{|N(\beta)|^{f_i}}$ are not all distinct and we must have

$$a^{|N(\beta)|^{f_i}} = a^{|N(\beta)|^{f_j}}$$

for some i, j with $i \neq j$. Since $\mathbb{Z}_{\mathbb{K}}$ does not have any zero-divisor, then, either $a = 0$ or a is a root of unity. □

4. The pattern transformation

The following construction of a kind of Fourier-transformation of a function $A\colon \mathbb{Z}_{\mathbb{K}} \to \mathbb{Z}$ is analogous to the pattern transformation of [22] (see also [4]).

Let $\{\beta, \mathcal{N}\}$ be a CNS on $\mathbb{Z}_{\mathbb{K}}$. If $\phi(x)$ is the index-function with respect to $\{\beta, \mathcal{N}\}$, then ϕ is a bijection from $\mathbb{Z}_{\mathbb{K}}$ to $\mathbb{N}$. Thus, there exists an isomorphism between the group $M = \big(\{A : \ \mathbb{Z}_{\mathbb{K}} \to \mathbb{Z}\}, +\big)$ and the group $(\mathbb{Z}^{\mathbb{N}}, +)$ of all integer sequences under termwise addition.

Let $A \in M$ and let

$$\nu(A) = \min\{n \geq 0 : \ A\big(\phi^{-1}(n)\big) \neq 0\}.$$

Then M becomes a metric group with distance function

$$\delta(A, B) = 2^{-\nu(A-B)}.$$

Let P be a *pattern*, i.e., a finite sequence of digits from $\mathcal{D}$.

We will denote the set of all patterns by $\mathcal{P}$. Thus $\mathcal{P} = \mathcal{D}^*$. Let $e_P(Q)$ be the pattern-function which counts the number of occurrences of the pattern P in the word Q. We assume that the pattern Q has as many leading zeros at the left hand side as the pattern P has. Furthermore let $a_P(Q) = (-1)^{e_P(Q)}$.

Let $\pi : \mathbf{Z}_{\mathbb{K}} \to \mathcal{P}$, $\pi(x) = (d_{L-1} d_{L-2} \ldots d_0)$, be the β-expansion of x. Then we can prove the following.

THEOREM 4.1. *Let $\{\beta, \mathcal{N}\}$ be a CNS in $\mathbf{Z}_{\mathbb{K}}$. Let $A\colon \mathbf{Z}_{\mathbb{K}} \to \mathbb{Z}$. Then there exists a function $\hat{A}\colon \mathbf{Z}_{\mathbb{K}} \to \mathbb{Z}$, such that*

$$A(x) = A(0) + \sum_{P \in \mathcal{P}} \hat{A}\big(\pi^{-1}(P)\big) e_P\big(\pi(x)\big).$$

The set $\big\{e_P\big(\pi(x)\big)\big\}$ is dense in M.

Proof. By subtracting $A(0)$ from $A(x)$, we can assume that $A(0) = 0$. Find $\min\{n : \ A\big(\phi^{-1}(n)\big) \neq 0\} =: n_1$ and let $y_1 = \phi^{-1}(n_1)$. Then

$$A(x) = A(y_1) e_{\pi(y_1)}\big(\pi(x)\big) \qquad \text{for all} \quad x \text{ with } \phi(x) \leq n_1.$$

Thus
$$\delta\Big(A(x), A(y_1)e_{\pi(y_1)}(\pi(x))\Big) \le 2^{-(n_1+1)}.$$
Define $\hat{A}(\pi^{-1}(y_1)) = A(y_1)$ and $\hat{A}(\pi^{-1}(y)) = 0$ for $\phi(y) < n_1$.

We can repeat this procedure with $A(x) - A(y_1)e_{\pi(y_1)}(\pi(x))$ instead of $A(x)$ to find an y_2, such that
$$A(x) - A(y_1)e_{\pi(y_1)}(\pi(x)) - \Big[A(y_2) - A(y_1)e_{\pi(y_1)}(\pi(y_2))\Big]e_{\pi(y_2)}(\pi(x)) = A(x)$$
for all x with $\phi(x) \le \phi(y_2) = n_2$. By induction, we can find a sequence $n_1 < n_2 < \dots$ such that
$$A(x) - \sum_{y:\,\phi(y)\le n_j} \hat{A}(\pi^{-1}(y))e_{\pi(y)}(\pi(x)) = 0$$
for all x with $\phi(x) \le n_j$. In other words
$$\delta\Bigg(A(x), \sum_{y:\,\phi(y)\le n_j} \hat{A}(\pi^{-1}(y))e_{\pi(y)}(\pi(x))\Bigg) \le 2^{-(n_j+1)}.$$
Since $n_j \to \infty$ as $j \to \infty$ we obtain the claimed formula.

The uniqueness of the *pattern-transform* $\hat{A}(\pi^{-1}(y))$ easily follows from
$$e_{\pi(x)}(\pi(x)) = 1 \qquad \text{and}$$
$$e_{\pi(x)}(\pi(y)) = 0 \qquad \text{for} \quad \phi(y) < \phi(x).$$
□

THEOREM 4.2. *The function $e_P(\pi(x))$ is β-regular for any pattern P.*

Proof. Let us introduce the following notation: if $w = w_1w_2\dots w_k$ is any string and $j \le k$, then
$$\mathrm{take}(j, w) = w_1 \dots w_j.$$

CLAIM. *Each element of the β-kernel can be written as a linear combination of the functions $e_P(\pi(\beta^f x + a))$, with $0 \le f < |P|$, and $a \in \mathbf{Z}_{\mathbb{K},f}$, and the constant function 1.*

Proof. Consider an element of the β-kernel $e_P(\pi(\beta^f x+a))$, with $a \in \mathbf{Z}_{\mathbb{K},f}$. Then if $f \le |P| - 1$, this function already is in the above list.

Consider now $f \ge |P|$. Then $\pi(\beta^f x + a)$ can be written as $\pi(x)\pi(a)$. Then
$$e_P(\pi(\beta^f x + a)) = e_P(\pi(\beta^{|P|-1}x + c)) + e_P(\pi(a)),$$
where $c = \phi^{-1}(\mathrm{take}(|P|, \pi(a)))$.

Now the first term on the right is in the list above, and the second term is a constant multiple of the constant function 1. Hence $e_P(\pi(\beta^f x + a))$ is a $\mathbb{Z}$-linear combination of elements in the list. □

Remark. The function $e_P(\pi(ax + b))$ is β-regular for $a, b \in \mathbf{Z}_{\mathbb{K}}$.

5. Linear recurring bases

5.1 The $(u;b)$ numeration.

The notion of numeration systems based on linear recurrent sequences was introduced by Fraenkel in [11]. We will follow here the notations of Shallit in [27]. Let $(u_n)_n$ be a linear recurrent sequence over $\mathbb{Z}$ satisfying the following properties:

(i) $u_0 = 1$;
(ii) $(u_n)_n$ is strictly increasing;
(iii) there exist $K \geq 1$, $M \geq 1$ and K coefficients in $\mathbb{N}$, $1 \leq b_1 = 1$, $b_2, \ldots, b_K \leq M$ such that, for all $n \geq M$, one has

$$u_n = \sum_{1 \leq i \leq K} u_{n-b_i} .$$

The $M + K$ integers $(u;b) = (u_0, u_1, \ldots, u_{M-1}; b_1, b_2, \ldots, b_K)$ suffice to characterize the sequence $(u_n)_n$. Note that some of the b_i's can be equal, actually allowing positive integers as coefficients.

Now any integer N is represented in base $(u;b)$ as follows:

- if $N < u_{M-1}$, then use any algorithm (for instance the greedy one) to express N as a sum of u_i's for $0 \leq i < M - 1$,
- otherwise, by induction, let j be the unique integer such that $u_{j-1} \leq N \leq u_j$, then there exists a unique $k \in [1, K]$ such that:

$$\sum_{1 \leq i \leq k-1} u_{j-b_i} \leq N < \sum_{1 \leq i \leq k} u_{j-b_i} ,$$

  then the representation of N is $\sum\limits_{1 \leq i \leq k-1} u_{j-b_i}$ plus the representation of $N - \sum\limits_{1 \leq i \leq k-1} u_{j-b_i}$.

Still following Shallit we note that this algorithm eventually writes $N \geq 0$ as $N = \sum\limits_{i \geq 0} n_i u_i$, where only finitely many n_i's are different from zero and that the digits n_i satisfy $n_i \leq K$ for $i \geq M$ and $n_i \leq T = K + \max\limits_{1 \leq i \leq M-1} \frac{u_i - 1}{u_{i-1}}$, for $0 \leq i \leq M - 1$.

As Shallit notes in [27], this representation generalizes many numeration systems in $\mathbb{N}$ and has two important properties: the set of all possible representations is regular and the total ordering on $\mathbb{N}$ defined by lexicographical comparison (starting with the most significant digit) coincides with the ordinary order. Shallit also notes that if the b_i's are increasing and the number of occurrences of any integer among the b_i's is decreasing, then the above representation coincides with the one given by the greedy algorithm.

5.2 The set of $(u;b)$-regular sequences.

Let $(u_n)_n$ be a sequence of integers satisfying (i), (ii), (iii) and let V be the set of all $(u;b)$-representations. Shallit [27] proved that V is a regular set. Let $T = K + \max_{1\le i\le M-1} \frac{u_i-1}{u_{i-1}}$ and $\Sigma = \{0,1,\dots,T-1\}$. For each word $s \in \Sigma^*$ let $W_s = \{x \in \Sigma^* \mid sx \in V\}$. Since V is regular, there is only a finite number of different sets W_s. It is easy to prove that W_s is either empty or is an infinite set. For each s with $W_s \neq \emptyset$, let $i_s(n)$ be the sequence such that $\{i_s(n) : n \ge 0\} = W_s$. (The elements of W_s are sorted in increasing order. For the empty word ε, we have $i_\varepsilon(n) = 0$.)

Definition 5.1. Similarly to the last section we give the following definitions, where i_s has been defined above.

- Let $(A(n))_n$ be any sequence. The subsequence of $(A(n))_n$ defined by $n \mapsto A(i_s(n))$ is called the *subsequence* of $(A(n))_n$ with least significant digits equal to s.
- The set of all these subsequences when s belongs to Σ^* is called the $(u;b)$*-kernel* of the sequence $(A(n))_n$ and is denoted by $K_{(u;b)}(A)$.
- Let $A(n)$ be a sequence with values in $\boldsymbol{R}$. We say that $(A(n))_n$ is $(u;b)$*-regular* if the $\boldsymbol{R}$-module generated by $K_{(u;b)}(A)$ is a finitely generated $\boldsymbol{R}$-module.
- Let $B(n)$ be a sequence with values in $\boldsymbol{R}$. We say that $(B(n))_n$ is $(u;b)$*-automatic* if $B(n)$ is a finite state function of the $(u;b)$-representation of n.
- Let
$$n = \sum_{j=0}^{k-1} n_j u_j .$$
Then
$$|n| = k$$
is called the *length of the digit representation* of n.

Theorem 5.1. *The following statements are equivalent:*

(a) *The sequence $(S(n))_n$ is $(u;b)$-regular.*

b) *The $\boldsymbol{R}$-module generated by $K_{(u;b)}(S)$ is generated by a finite number of sequences $S(i_{k_j}(n))$.*

(*There exists a positive integer E, such that for all $e_j > E$, each sequence $S(i_{r_j}(n))$ with $|r_j| = e_j$ can be expressed as an $\boldsymbol{R}$-linear combination*
$$S(i_{r_j}(n)) = \sum_l S(i_{k_{lj}}(n)) ,$$

where $|k_{lj}| \le E$.

(d) *There exist an integer* r, *and* r *sequences* $S = S_1, \dots, S_r$, *such that for* $1 \le i \le r$ *the sequences* $S_i\big(i_a(n)\big)$ *are* $\boldsymbol{R}$*-linear combinations of the* S_i*'s if the digit representation of* a *has one digit.*

(e) *There exists an integer* r, *and* r *sequences* $S = S_1, \dots, S_r$, *and matrices* $B_0, \dots, B_q$ *in* $\boldsymbol{R}^{r\times r}$, *such that if*

$$V(n) = \begin{pmatrix} S_1(n) \\ \vdots \\ S_r(n) \end{pmatrix}$$

one has

$$V\big(i_a(n)\big) = B_a V(n)$$

if the digit representation of a *has one digit.*

Proof. We will only prove the direction (e) $\Longrightarrow$ (a): we need to see that $S\big(i_a(n)\big)$ is a linear combination of the S_i's. Express a in base $(u;b)$ as

$$a = \sum_{0 \le i < e} a_i u_i \,,$$

then it is easy to see that

$$V\big(i_a(n)\big) = B_{a_0} B_{a_1} \cdots B_{a_{e-1}} V(n)\,,$$

and this expresses $S\big(i_a(n)\big)$ as a linear combination of the S_i's. □

THEOREM 5.2. *A sequence is* $(u;b)$*-automatic if and only if it is* $(u;b)$*-regular and takes only finitely many values.*

Proof. See Theorem 3.2. □

THEOREM 5.3. *If* $S(n)$ *is a* $(u;b)$*-regular sequence, then there exists a constant* c *such that* $|S(n)| = O(n^c)$.

Proof. Let

$$n = \sum_{i=0}^{j-1} n_i u_i \,.$$

Since u_j is generated by a linear recurring formula, there exists a $\lambda > 1$ such that

$$\lambda^{j-1} \le u_{j-1} \le n < u_j$$

if $|n| = j$. Thus

$$j \le 1 + \frac{\ln n}{\ln \lambda}\,.$$

Theorem 5.1(e) gives

$$V(n) = B_{n_0} B_{n_1} \cdots B_{n_{j-1}} V(0)\,.$$

See now Theorem 3.6. □

6. Computational results.

z_j		0			1		
c_j		d_j	c_{j+1}		d_j	c_{j+1}	
0	0	0	0	0	0	−2	−1
−2	−1	0	1	1	0	−1	0
1	1	1	1	0	1	−1	−1
1	0	1	0	0	1	−2	−1
−1	−1	1	1	1	1	−1	0
−1	0	1	2	1	1	0	0
2	1	0	−1	−1	0	−3	−2
−3	−2	1	2	2	1	0	1
2	2	0	0	−1	0	−2	−2
0	−1	0	−1	0	0	−3	−1
−3	−1	1	3	2	1	1	1
3	2	1	0	−1	1	−2	−2
−2	−2	0	0	1	0	−2	0
0	1	0	1	0	0	−1	−1
−2	0	0	2	1	0	0	0

FIGURE 1. The transducer for multiplication by 2 for $\beta = -1 + \mathrm{i}$.

The second author has written a computer program that constructs finite automata for addition and multiplication by a fixed number in integral domains. It searches for all possible states of the automaton and stores them in a tree. The state of the automaton corresponds to the carry in the actual step. If u and v are fixed algebraic numbers, the automaton will compute the digits of $uz + v$ from the digits of z. If $u = 1$ and $v = 1$ the automaton is just the odometer.

The automaton uses the following algorithm for multiplication by a fixed number: let

$$z = \sum_{j=0}^{n-1} z_j \beta^j .$$

Let c_j be the carry and d_j be the output at the j'th step.

(1) Let $c_0 = v$ be the initial carry.
(2) For $j = 0, 1, \dots$ do
d_j and c_{j+1} uniquely follow from $uz_j + c_j = d_j + \beta c_{j+1}$.

(v can be considered as initial carry when calculating $uz + v$. In case of pure multiplication we have $v = 0$.)

EXAMPLE 6.1. Let $m_\beta(x) = x^2 + 2x + 2$. Thus $\beta = -1 \pm i$ and $N(\beta) = 2$. The automaton which multiplies a number by 2 is given in Figure 1.

Remark 6.1. Multiplication cannot be generally performed by a finite automaton for linear recurring bases. Take for example the Fibonacci-base $u_0 = 1$, $u_1 = 2$, $u_n = u_{n-1} + u_{n-2}$. This base satisfies the identity

$$2 \sum_{k=0}^{m} u_{3k} = u_{3m+2} - 1 .$$

The $(u; b)$-representation of $u_{3m+2} - 1$ is either $(010 \dots 101)$ or $(101 \dots 101)$. This is dependent of m being even or odd. Thus the automaton has to store the whole $(u; b)$-representation to compute the least significant digit of the product. This cannot be done by a finite automaton.

This counterexample was given by G. Barat, during his visit in Graz in 1996. For related general results, see [12], [13].

Acknowledgments

Part of this work was done when JPA visited Graz in 1995. JPA wants to thank heartily his colleagues for their very warm hospitality, and J. Shallit for many interesting conversations on these topics. The authors thank the referee for its precise and useful comments.

REFERENCES

[1] ALLOUCHE, J.-P.: *q-regular sequences and other generalizations of q-automatic sequences.* In: Lecture Notes in Comput. Sci. 583, Springer, New York, 1992, pp. 15 23.

[2] ALLOUCHE, J.-P.: *Finite automata and arithmetic.* In: Séminaire Lotharingien de Combinatoire B30c, 1993, pp. 1 23.

[3] ALLOUCHE, J.-P. — CATELAND, E. — GILBERT, W. J. — PEITGEN, H.-O. — SHALLIT, J.—SKORDEV, G.: *Automatic maps in exotic numeration systems*, Theory Comput. Syst. (Formerly: Math. Systems Theory) **30** (1997), 285–331.

[4] ALLOUCHE, J.-P.—MORTON, P.—SHALLIT, J.: *Pattern spectra, substring enumeration, and automatic sequences*, Theoret. Comput. Sci. **94** (1992), 161–174.

[5] ALLOUCHE, J.-P.—SHALLIT, J.: *The ring of k-regular sequences*, Theoret. Comput. Sci. **98** (1992), 163–187.

[6] CHRISTOL, G.: *Ensembles presque-périodiques k-reconnaissables*, Theoret. Comput. Sci. **9** (1979), 141–145.

[7] CHRISTOL, G.—KAMAE, T.—MENDÈS FRANCE, M.—RAUZY, G.: *Suites algébriques, automates et substitutions*, Bull. Soc. Math. France **108** (1980), 401–419.

[8] COBHAM, A.: *On the base-dependence of sets of numbers recognizable by finite automata*, Math. Systems Theory **3** (1969), 186–192.

[9] COBHAM, A.: *Uniform tag sequences*, Math. Systems Theory **6** (1972), 164–192.

[10] DEKKING, F. M.—MENDÈS FRANCE, M.— VAN DER POORTEN, A. J.: *Folds!* Math. Intelligencer **4** (1982), 130–138, 173–181, 190–195.

[11] FRAENKEL, A. S.: *Systems of numeration*, Amer. Math. Monthly **92** (1985), 105–114.

[12] FROUGNY, C.: *Confluent linear numeration systems*, Theoret. Comput. Sci. **106** (1992), 183 219.

[13] FROUGNY, C.—SOLOMYAK, B.: *On representation of integers in linear numeration systems.* In: Ergodic Theory of $\mathbb{Z}^d$ actions. Proceedings of the Warwick Symposium, Warwick, UK, 1993–94 (M. Pollicott et al., eds.), London Math. Soc. Lecture Note Ser. 228, Cambridge University Press, Cambridge, 1996, pp. 345–368.

[14] GRABNER, P. G.—KIRSCHENHOFER, P.—PRODINGER, H.: *The sum of digits function for complex bases*, J. London Math. Soc. **57** (1998), 20–40.

[15] KÁTAI, I.—KOVÁCS, B.: *Kanonische Zahlensysteme in der Theorie der quadratischen algebraischen Zahlen*, Acta Sci. Math. (Szeged) **42** (1980), 99–107.

[16] KÁTAI, I.—KOVÁCS, B.: *Canonical number systems in imaginary quadratic fields*, Acta Math. Acad. Sci. Hungar. **37** (1981), 159–164.

[17] KÁTAI, I.—SZABO, J.: *Canonical number systems for complex integers*, Acta Sci. Math. (Szeged) **37** (1975), 255–260.

[18] KIMBERLING, C.: *Numeration systems and fractal sequences*, Acta Arith. **73** (1995), 103–117.

[19] KNUTH, D. E.: *The Art of Computer Programming, Vol. 2. Seminumerical Algorithms* (2nd ed.), Addison Wesley, Reading, 1981.

[20] KOVÁCS, B.: *CNS rings.* In: Topics in Classical Number Theory, Vol. II (G. Halász, ed.), Colloq. Math. Soc. János Bolyai 34, North-Holland, Amsterdam, 1984, pp. 961–971.

[21] KOVÁCS, B.—PETHŐ, A.: *Number systems in integral domains, especially in orders of algebraic number fields*, Acta Sci. Math. (Szeged) **55** (1991), 287–299.

[22] MORTON, P.—MOURANT, W.: *Paper folding, digit patterns and groups of arithmetic fractals*, Proc. London Math. Soc. **59** (1989), 253–293.

[23] SALON, O.: *Suites automatiques à multi-indices et algébricité*, C. R. Acad. Sci. Paris Sér. I Math. **305** (1987), 501–504.

[24] SALON, O.: *Propriétés arithmétiques des automates multidimensionnels.* Thèse, Université Bordeaux I, Bordeaux, 1989.

[25] SCHEICHER, K.: *Kanonische Ziffernsysteme und Automaten.* In: Grazer Math. Ber. 333, Karl-Franzens-Univ. Graz, Graz, 1997, pp. 1–17.

[26] SCHEICHER, K.: *Zifferndarstellungen, lineare Rekursionen und Automaten.* PhD Thesis, TU Graz, Graz, 1997.

[27] SHALLIT, J.: *A generalization of automatic sequences*, Theoret. Comput. Sci. **61** (1988), 1–16.

[28] THUSWALDNER, J.: *Elementary properties of canonical number systems in quadratic fields.* In: Applications of Fibonacci Numbers, Vol. 7 (Graz 1996), Kluwer Acad. Publ., Dordrecht, 1998, pp. 405–414.

Received January 12, 1998
Revised July 6, 1998

* *CNRS, LRI, Bâtiment 490*
F-91405 Orsay Cedex
FRANCE
E-mail: allouche@lri.fr

** *Mathematical Institute*
TU Graz
Steyrergasse 30
A-8010 Graz
AUSTRIA
E-mail: scheicher@weyl.math.tu-graz.ac.at
tichy@weyl.math.tu-graz.ac.at