Jean-Paul Allouche; Klaus Scheicher; Robert Franz Tichy
Regular maps in generalized number systems


Persistent URL: [http://dml.cz/dmlcz/133301](http://dml.cz/dmlcz/133301)

Terms of use:

© Mathematical Institute of the Slovak Academy of Sciences, 2000

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these Terms of use.

This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* [http://project.dml.cz](http://project.dml.cz)
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 \( n \)th 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

\[ n \rightarrow S(n) \mod 2 \]

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

\[ n \rightarrow S(n) \]

is 2-regular (this is the well-known Prouhet-Thue-Morse sequence).
JEAN-PAUL ALLOUCHE — KLAUS SCHEICHER — ROBERT F. TICHY

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

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

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 Katai, Szabo [17] and Katai, Kovacs [15], [16]. Kovacs [20] gave a necessary and sufficient condition for the existence of CNS in $\mathbb{Z}_K$.

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

Kovacs and Pethö [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 $\beta \in \mathbb{Z}_K$, and let $\{1, \beta, \ldots, \beta^{n-1}\}$ be an integral base of $\mathbb{Z}_K$. Let $\beta$ be a zero of the polynomial $x^n + b_{n-1}x^{n-1} + \cdots + b_0$ with

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

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

$$q_j = (b_{i_1} - b_{i_2} + b_{i_3} - \ldots)$$
$$+ (b_{i_1+1} - b_{i_2+1} + b_{i_3+1} - \ldots)\beta$$
$$+ (b_{i_1+2} - b_{i_2+2} + b_{i_3+2} - \ldots)\beta^2$$
$$\vdots$$

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

3. The set of $\beta$-regular functions

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

**Definition 3.1.** Let $s: \mathbb{Z}_K \to E$.

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

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

where

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

- The function $s$ is called $\beta$-regular, if there exists a finite number of functions $s_1, \ldots, s_r$ with values in $E$, such that each function in the $\beta$-kernel is an $R$-linear combination of the $s_i$’s.
- Let

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

then the shift-function $\sigma$ 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 $\mathbb{Z}_{K, t}$; 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

$$\phi \left( \sum_{j=0}^{h} d_j \beta^j \right) = \sum_{j=0}^{h} d_j |N(\beta)|^j$$

and $\phi(0) = 0$.

**Theorem 3.1.** The following statements are equivalent:

(a) The function $s: \mathbb{Z}_K \to E$ is $\beta$-regular.

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

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

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

(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 $R$-linear combination

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

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

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

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

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

then

$$V(\beta x + k) = B_k V(x) \quad \text{for} \quad k \in \mathbb{Z}_{\mathbb{K}, 1}.$$
(d) \implies (e). Let \( (K_\beta(s)) = \{s(\beta^i x + b_i), i \leq i' \} \). Let \( E = \max_{1 \leq i \leq i'} f_i \). Then for all \( e_j \geq E \), we can write
\[
s(\beta^e x + a_j) = \sum_i c_{ij} s(\beta^{f_i} x + b_{ij}),
\]
where \( f_{ij} \leq E \) and \( b_{ij} \in \mathbb{Z}_{\mathbb{K}, f_i} \).

(e) \implies (f). Take as the \( r \) functions the functions \( s_i(x) = s(\beta^{f_i} x + b_i) \) with \( 0 \leq f_i \leq E \) and \( b_i \in \mathbb{Z}_{\mathbb{K}, f_i} \). Then
\[
s_i(\beta^e x + a) = s(\beta^{f_i} (\beta^e x + a) + b_i) = s(\beta^{f_i+e} x + a\beta^{f_i} + b_i),
\]
which, if \( f_i + e \leq E \), is an element of \( K_\beta(s) \), and if \( f_i + e > E \) is a linear combination of elements of \( K_\beta(s) \).

(f) \implies (g). Follows trivially.

(g) \implies (a). We need to see that \( s(\beta^e x + a) \) is a linear combination of the \( s_i \). Express \( a \) in base \( \beta \) as
\[
\sum_{0 \leq i < e} a_i \beta^i,
\]
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 \( s_i \).

**Theorem 3.2.** The function \( s: \mathbb{Z}_\mathbb{K} \to \mathbb{E} \) is \( \beta \)-automatic if and only if it is \( \beta \)-regular and takes only finitely many values.

**Proof.** If a function is \( \beta \)-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 \( \beta \)-regular and takes only a finite number of values. Theorem 3.1(g) implies that there exist functions \( s = s_1, \ldots, s_d \) in \( K_\beta(s) \), and matrices \( B_0, \ldots, B_{|N(\beta)|-1} \) such that \( V(x) = (s_1(x), \ldots, s_d(x))^T \) 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 \( r = \sum_{k=0}^j d_k \beta^k \). Then
\[
V(\beta^j x + r) = B_{d_0} \cdots B_{d_{j-1}} V(x).
\]
Let \( \Theta \) 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 \( \Theta \) into itself. Since there are only finitely many maps from a finite set into itself, the set of maps \( x \mapsto V(\beta^j x + r), j \geq 0, r \in \mathbb{Z}_{\mathbb{K}, j} \), is finite. Hence \( K_\beta(s) \) is finite. \( \square \)
**THEOREM 3.3.** Let $s(x)$ and $t(x)$ be $\beta$-regular functions. Let $\alpha$ be a constant. Then $(s + t)(x) = s(x) + t(x)$, $(s \cdot t)(x) = s(x) \cdot t(x)$ and $(\alpha \cdot s)(x)$, $x \in \mathbb{Z}_K$ are $\beta$-regular.

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

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

**Proof.** Define $t(x) = s(ux + v)$. There exist functions $s_1, \ldots, s_r$ such that $K_\beta(s) \subset \langle s_1, \ldots, s_r \rangle$. Take now an element of the $\beta$-kernel of $t(x)$, say $t(\beta^k x + l)$, $l \in \mathbb{Z}_K$. 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

$$t(\beta^k x + l) = s(u(\beta^k x + l) + v) = s(\beta^k (ux + a) + b).$$

Since $l \in \mathbb{Z}_K$ 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 $\geq 1$. Then $s(x)$ is $\beta$-regular if and only if it is $\beta^f$-regular.

**Proof.** Since $K_{\beta^f}(s) \subset K_\beta(s)$ the function is $\beta^f$-regular if it is $\beta$-regular. Assume now that $s(x)$ is $\beta^f$-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

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

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

$$s((\beta^f)^r y + t) = \sum_i d_i s((\beta^f)^r y + t_i),$$
where \( r_i < E \) and \( t_i \in \mathbb{Z}_{f r_i} \).

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

\[
s((\beta^t)^r y + t) = s(\beta^b x + c)
= \sum_i d_i s(\beta^b x + c_i)
\]

where \( b_i = f r_i + u \) and \( c_i = q \beta^b x + t_i \). Note that \( b_i < E + f \) and \( q \in \mathbb{Z}_{f u} \).

So

\[
c_i = q \beta^b x + t_i \in \mathbb{Z}_{f r_i + f} = \mathbb{Z}_{f b_i}.
\]

Thus we may take \( B = f(E + 1) \). Hence \( s(x) \) is \( \beta \)-regular.

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

**Proof.** Let

\[
x = \sum_{j=0}^{k-1} d_j \beta^j.
\]

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

\[
2 \log_{a^2 + 1} |x| - 2 \log_{a^2 + 1} \frac{a \sqrt{a^2 + 4}}{a^2 + 2} - 4 \leq k - 1
\]

\[
\leq 2 \log_{a^2 + 1} |x| - \log_{a^2 + 1} \left(1 - \frac{a \sqrt{a^2 + 4}}{a^2 + 2}\right) + 4.
\]

Thus

\[
k \leq b + 2 \log_{a^2 + 1} |x|.
\]

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 \( |Mv| \leq ||M|||v| \)). Thus we see

\[
|s(x)| \leq |V(x)| \leq ||B_{d_0}|| ||B_{d_1}|| \cdots ||B_{d_{k-1}}|| |V(0)|.
\]

Now let \( c = \max_{0 \leq i \leq k-1} ||B_i|| \), and \( d = ||V(0)|| \). Then

\[
|s(x)| \leq c^{b+2 \log_{a^2 + 1} |x|} d \leq d' |x|^c.
\]

\[\square\]
Example 3.1. We give here some examples of $\beta$-regular functions.

(a) Polynomials in $x$ are $\beta$-regular functions since $1$ and $x$ are $\beta$-regular functions.

(b) The index-function $\phi(x)$ is $\beta$-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 $d_j \in \{0, \ldots, |N(\beta)| - 1\}$.

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

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

Generally column $j$ contains the elements with $\beta$-residue $\beta^{j-1}$.

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

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

Then we have

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

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

Definition 3.2. (see [18]) The paraphrase-function $p_\beta: \mathbb{Z}_K \to \mathbb{N}$ 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 $\mathbb{Z}_K$ lexicographically, beginning with the least significant digit.

Theorem 3.7. The paraphrase $p_\beta(x)$ is $\beta$-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 $\beta^e x + f = \beta^e x + \beta^{n-1} z = \beta^{n-1} (\beta^{e-n+1} x + z)$ and

$$p_\beta(\beta^e x + f) = p_\beta(\beta^{e-n+1} x + z) .$$
REGULAR MAPS IN GENERALIZED NUMBER SYSTEMS

(If \( \beta^e x + f = a(m, n) \), then \( \beta^{e-n+1} x + z = a(m, 1) \).) A simple consideration gives that
\[
p_\beta(x) = \phi(x) - \left\lfloor \frac{\phi(x)}{|N(\beta)|} \right\rfloor
\]
for all \( x \) that occur in the first column of \( A(\beta) \). Hence
\[
p_\beta(\beta^{e-n+1} x + z) = \phi(\beta^{e-n+1} x + z) - \left\lfloor \frac{|N(\beta)|^{e-n+1} \phi(x) + \phi(z)}{|N(\beta)|} \right\rfloor
= |N(\beta)|^{e-n} (|N(\beta)| - 1) \cdot \phi(x) + \left( \phi(z) - \left\lfloor \frac{\phi(z)}{|N(\beta)|} \right\rfloor \right) \cdot 1.
\]
Since \( \phi(x) \) and 1 are \( \beta \)-regular \( p_\beta(x) \) is \( \beta \)-regular.

(d) The trace \( \text{Tr}(x) \) is \( \beta \)-regular. Since \( \beta^n + b_{n-1}\beta^{n-1} + \cdots + b_0 = 0 \), there exist \( a_{ki} \in \mathbb{Z} \) such that
\[
\beta^k = \sum_{i=0}^{n-1} a_{ki} \beta^i.
\]
Thus
\[
\text{Tr}(\beta^k x + l) = \sum_{i=0}^{n-1} a_{ki} \text{Tr}(\beta^i x) + \text{Tr}(l).
\]

**Theorem 3.8.** Let \( R \) be a Noetherian ring without zero divisors, and let \( a \in R \). Then, the function \( s(x) = a^{\phi(x)} \) is \( \beta \)-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 \( a^{\phi(x)} = a^{\phi(x) \mod k} \) is automatic. Thus \( a^{\phi(x)} \) is regular.

Assume now that \( a^{\phi(x)} \) is \( \beta \)-regular. Then, there exist \( r < \infty \) and \( \lambda_j \) with \( 0 \leq j < r \), such that
\[
\forall x \in \mathbb{Z}_K \sum_{0 \leq j < r} \lambda_j (a^{|N(\beta)|^f_i})^{\phi(x)} = 0.
\]
We use the following formula for the Vandermonde determinant:
\[
\begin{pmatrix}
1 & \xi_0 & \xi_0^2 & \cdots & \xi_0^m \\
1 & \xi_1 & \xi_1^2 & \cdots & \xi_1^m \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
1 & \xi_m & \xi_m^2 & \cdots & \xi_m^m
\end{pmatrix} = \prod_{i>j}(\xi_i - \xi_j).
\]

49
From this, we can see that the functions \( \xi^\phi(x) \) are linearly independent if and only if the numbers \( \xi_1, \xi_2, \ldots, \xi_m \) are distinct.

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

\[
a_{|N(\beta)|^i} = a_{|N(\beta)|^j}
\]

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

\[\square\]

4. The pattern transformation

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

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

Let \( A \in M \) and let

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

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 \( D \).

We will denote the set of all patterns by \( \mathcal{P} \). Thus \( \mathcal{P} = D^* \). 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 \( \pi : \mathbb{Z}_K \to \mathcal{P} \), \( \pi(x) = (d_{L-1}d_{L-2}\ldots d_0) \), be the \( \beta \)-expansion of \( x \). Then we can prove the following.

**Theorem 4.1.** Let \( \{\beta, N\} \) be a CNS in \( \mathbb{Z}_K \). Let \( A : \mathbb{Z}_K \to \mathbb{Z} \). Then there exists a function \( \hat{A} : \mathbb{Z}_K \to \mathbb{Z} \), such that

\[
A(x) = A(0) + \sum_{P \in \mathcal{P}} \hat{A}(\pi^{-1}(P))e_p(\pi(x)).
\]

The set \( \{e_p(\pi(x))\} \) is dense in \( M \).

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

\[
A(x) = A(y_1)e_{\pi(y_1)}(\pi(x)) \quad \text{for all } x \text{ with } \phi(x) \leq n_1.
\]
Thus
\[ \delta\left(A(x), A(y_1)e_{\pi(y_1)}(\pi(x))\right) \leq 2^{-(n_1+1)}.\]

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
\[ A(x) - A(y_1)e_{\pi(y_1)}(\pi(x)) - \left[ A(y_2) - A(y_1)e_{\pi(y_1)}(\pi(y_2)) \right] e_{\pi(y_2)}(\pi(x)) = A(x) \]
for all \( x \) with \( \phi(x) \leq \phi(y_2) = n_2 \). By induction, we can find a sequence \( n_1 < n_2 < \ldots \) such that
\[ A(x) - \sum_{y : \phi(y) \leq n_j} \hat{A}(\pi^{-1}(y)) e_{\pi(y)}(\pi(x)) = 0 \]
for all \( x \) with \( \phi(x) \leq n_j \). In other words
\[ \delta\left(A(x), \sum_{y : \phi(y) \leq n_j} \hat{A}(\pi^{-1}(y)) e_{\pi(y)}(\pi(x))\right) \leq 2^{-(n_j+1)} .\]

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
\[
e_{\pi(x)}(\pi(x)) = 1 \quad \text{and} \quad e_{\pi(x)}(\pi(y)) = 0 \quad \text{for} \quad \phi(y) < \phi(x).
\]

\[ \square \]

**Theorem 4.2.** The function \( e_P(\pi(x)) \) is \( \beta \)-regular for any pattern \( P \).

**Proof.** Let us introduce the following notation: if \( w = w_1w_2\ldots w_k \) is any string and \( j \leq k \), then
\[ \text{take}(j, w) = w_1\ldots w_j. \]

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

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

Consider now \( f \geq |P| \). 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 \( c = \phi^{-1}(\text{take}([|P|, \pi(a)])) \).

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. \( \square \)

**Remark.** The function \( e_P(\pi(ax + b)) \) is \( \beta \)-regular for \( a, b \in \mathbb{Z}_{\mathbb{K}} \).
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 \(u_{j-1} \leq N < u_j\), 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 \(\sum_{1 \leq i \leq k-1} u_{j-b_i}\) plus the representation of \(N - \sum_{1 \leq i \leq k-1} u_{j-b_i}\).

Still following Shallit we note that this algorithm eventually writes \(N \geq 0\) as \(N = \sum_{i \geq 0} n_i u_i\), 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 \(n_i \leq T = K + \max_{1 \leq i \leq M-1} \frac{u_{i-1}-1}{u_i-1}\), 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 \(T = K + \max \{n-1 \mid 1 \leq i \leq M-1\}\) and \(\Sigma = \{0, 1, \ldots, T-1\}\). 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 \(\{i_s(n) : n \geq 0\} = W_s\). (The elements of \(W_s\) are sorted in increasing order. For the empty word \(\varepsilon\), 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 \(\Sigma^*\) 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 \(R\). We say that \((A(n))_n\) is \((u; b)\)-regular if the \(R\)-module generated by \(K_{(u; b)}(A)\) is a finitely generated \(R\)-module.
- Let \(B(n)\) be a sequence with values in \(R\). 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 \(R\)-module generated by \(K_{(u; b)}(S)\) is generated by a finite number of sequences \(S(i_{k, j}(n))\).

(c) 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 \(R\)-linear combination

\[
    S(i_{r, j}(n)) = \sum_l S(i_{k_l j}(n)),
\]

53
where \( |k_{ij}| \leq E \).

(d) There exist an integer \( r \), and \( r \) sequences \( S = S_1, \ldots, S_r \), such that for \( 1 \leq i \leq r \) the sequences \( S_i(i_a(n)) \) are \( \mathbb{R} \)-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 \( S = S_1, \ldots, S_r \), and matrices \( B_0, \ldots, B_q \) in \( \mathbb{R}^{r \times r} \), such that if

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

one has

\[
V(i_a(n)) = B_a V(n)
\]

if the digit representation of \( a \) has one digit.

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

\[
a = \sum_{0 \leq i < e} a_i u_i,
\]

then it is easy to see that

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

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

\[\square\]

**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. \[\square\]

**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

\[
\lambda^{j-1} \leq u_{j-1} \leq n < u_j
\]

if \( |n| = j \). Thus

\[
j \leq 1 + \frac{\ln n}{\ln \lambda}.
\]

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. \[\square\]
6. Computational results.

<table>
<thead>
<tr>
<th>(z_j)</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>(c_j)</td>
<td>(d_j)</td>
<td>(c_{j+1})</td>
</tr>
<tr>
<td>0 0</td>
<td>0 0</td>
<td>0</td>
</tr>
<tr>
<td>-2 -1</td>
<td>0 1</td>
<td>1</td>
</tr>
<tr>
<td>1 1</td>
<td>1 0</td>
<td>1</td>
</tr>
<tr>
<td>1 0</td>
<td>1 0</td>
<td>1</td>
</tr>
<tr>
<td>-1 -1</td>
<td>1 1</td>
<td>1</td>
</tr>
<tr>
<td>-1 0</td>
<td>1 2</td>
<td>1</td>
</tr>
<tr>
<td>2 1</td>
<td>0 -1 -1</td>
<td>0</td>
</tr>
<tr>
<td>-3 -2</td>
<td>1 2 2</td>
<td>1</td>
</tr>
<tr>
<td>2 2</td>
<td>0 0 -1</td>
<td>0</td>
</tr>
<tr>
<td>0 -1</td>
<td>0 -1 0</td>
<td>0</td>
</tr>
<tr>
<td>-3 -1</td>
<td>1 3 2</td>
<td>1</td>
</tr>
<tr>
<td>3 2</td>
<td>1 0 -1</td>
<td>1</td>
</tr>
<tr>
<td>-2 -2</td>
<td>0 0 1</td>
<td>0</td>
</tr>
<tr>
<td>0 1</td>
<td>0 1 0</td>
<td>0</td>
</tr>
<tr>
<td>-2 0</td>
<td>0 2 1</td>
<td>0</td>
</tr>
</tbody>
</table>

Figure 1. The transducer for multiplication by 2 for \(\beta = -1 + i\).

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
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 $j = 0, 1, \ldots$ 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 $(010 \ldots 101)$ or $(101 \ldots 101)$. 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**


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