From number systems to shift radix systems

Shigeki Akiyama* and Klaus Scheicher†

Abstract

Shift radix systems provide a unified notion to study two important types of number systems. In this paper, we briefly review the origin of this notion.

1. Introduction

Let \( r = (r_1, \ldots, r_d) \in \mathbb{R}^d \). Consider a mapping \( \tau_r : \mathbb{Z}^d \to \mathbb{Z}^d \), which maps each element \((z_1, \ldots, z_d)\) to \((z_2, \ldots, z_{d+1})\), provided that

\[
0 \leq r_1z_1 + r_2z_2 + \cdots + r_dz_d + z_{d+1} < 1.
\]

Obviously, \( \tau_r \) is defined by

\[
\tau_r((z_1, \ldots, z_d)) = (z_2, \ldots, z_d, -\lfloor r_1z_1 + \cdots + r_dz_d \rfloor).
\] (1.1)

We say that \( \tau_r \) has the finiteness property if for every \( z \in \mathbb{Z}^d \) there exists a \( k \), such that \( \tau_r^k(z) = 0 \).

This concept unifies notions for two important number systems, namely canonical number systems and \( \beta \)-expansions. For these number systems, the finiteness property means that all numbers of a certain set admit finite expansions. This property also plays an important role for constructing tilings giving the Markoff partitions of dynamical systems associated to these number systems.

If \( \tau_r \) has the finiteness property, then \((\mathbb{Z}, \tau_r)\) is called a shift radix system (for short SRS) (cf. [2, 3]). It turned out to be a hard problem to characterize all

*The first author was supported by the Japanese Ministry of Education, Culture, Sports, Science and Technology, Grant-in Aid for fundamental research 14540015, 2002–2005.
†The second author was supported by the FWF projects 8305 and 8308.
r ∈ Rd which give rise to a SRS and currently, a complete solution seems to be out of range. However, in the last years, several partial results have been established.

For an introduction to SRS, we do not aim to give an exact account. For detailed information, we refer to original papers. Emphasis will be put on results of Gilbert and Hollander who developed the essential structure of the SRS algorithm.

2. Canonical number systems

As an example, we consider Knuth’s number system. He proposed a way to express Gaussian integers by digits from $A = \{0, 1\}$ with base $\alpha = -1 + \sqrt{-1}$:

\[
\begin{align*}
1 &= \alpha^0 = (1)_\alpha \\
2 &= \alpha^3 + \alpha^2 = (1100)_\alpha \\
3 &= \alpha^3 + \alpha^2 + 1 = (1101)_\alpha \\
4 &= \alpha^8 + \alpha^7 + \alpha^6 + \alpha^4 = (111010000)_\alpha \\
5 &= \alpha^8 + \alpha^7 + \alpha^6 + \alpha^4 + 1 = (111010001)_\alpha
\end{align*}
\]

How do we find such expressions? This is done by so called residual algorithm. Take for example the expansion of 3 in base $\alpha$: As $A$ forms a complete system of representatives modulo $\alpha$, and $3 \equiv 1 \pmod{\alpha}$, the lowest digit is 1. We subtract 1 and then divide by $\alpha$. Then we restart this process from $(3-1)/\alpha = -1 - \sqrt{-1}$. Iterating this, we generate the expansion in base $\alpha$. After four steps, we terminate this process since we run into the trivial cycle $0 \rightarrow 0$ which generates infinitely many leading zeros.

Generally, we may start with an algebraic integer $\alpha$ of degree $d$ and a complete residue system $\mathcal{A}$ modulo $\alpha$ in $\mathbb{Z}[\alpha]$. If all algebraic conjugates of $\alpha$ have modulus greater than 1, then the residual algorithm can be viewed as a contractive map on $\mathbb{Z}[\alpha]$, which is isomorphic to $\mathbb{Z}^d$ as an additive group. This means that each orbit must be eventually periodic. However, it is not trivial that this process must terminate in finitely many steps. In fact, it is possible that the residual algorithm runs into a non trivial cycle. For e.g., let $\alpha' = 1 + \sqrt{-1}$ and $\mathcal{A} = \{0, 1\}$. If we try to expand $\sqrt{-1}$, we find that $\sqrt{-1} \equiv 1 \pmod{\alpha'}$ and $(\sqrt{-1} - 1)/\alpha' = \sqrt{-1}$. Thus,

$$\sqrt{-1} = (\cdots 111)_\alpha'.$$

For Knuth’s number system, it is proved that the process terminates for every starting value. This is exactly the above mentioned finiteness property. In this case, the pair $(\alpha, \mathcal{A})$ is called a canonical number system (CNS for short).
Before explaining Gilbert’s idea, we summarize known results on the characterization of CNS. A first systematic treatment was given in Kátai-Szabó [18], where all CNS bases for Gaussian integers have been characterized. This result was generalized to quadratic integers in Kátai-Kovács [16, 17] and independently in Gilbert [13]. Körmendi [19] dealt with a special class of cubic integers and recently Brunotte [8, 9] characterized all CNS whose bases are roots of trinomials. In the general case Kovács [20] proved that an algebraic integer \( \alpha \) gives rise to a CNS if its minimal polynomial
\[
P(x) = x^n + b_{n-1}x^{n-1} + \ldots + b_1x + b_0
\]
satisfies
\[
1 \leq b_{n-1} \leq b_{n-2} \leq \ldots \leq b_1 \leq b_0, \quad b_0 \geq 2.
\]
However, this characterization is far from complete. Examples not contained in this class are given in Kovács-Pethő [21], where also an algorithm is established to decide whether a given \( \alpha \) is a CNS base or not. Akiyama-Pethő [4] developed a much faster algorithm than the one in [21]. Akiyama-Rao [5] and Scheicher-Thuswaldner [26] studied CNS under a so called Dominant Condition
\[
|b_1| + \ldots + |b_n| < b_0.
\]
In particular, all CNS up to degree five with this additional property have been characterized. Finally, we mention that Brunotte [8, 9] provided the fastest known algorithm to determine if an arbitrary polynomial gives a CNS or not.

3. Gilbert’s Clearing Algorithm

In [13], W. J. Gilbert introduced his Clearing Algorithm which is one of the origins of the SRS setting. We explain his idea by using Knuth’s number system.

Let \( \alpha = -1 + \sqrt{-1} \). Then \( \mathbb{Z}[\alpha] = \mathbb{Z}[\sqrt{-1}] \). As \( \alpha \) satisfies \( x^2 + 2x + 2 = 0 \), we have an isomorphism \( \mathbb{Z}[\alpha] \cong \mathbb{Z}[x]/(x^2 + 2x + 2) \). The residual algorithm is interpreted by division algorithm on \( \mathbb{Z}[x] \). A polynomial \( Q(x) = \sum_i q_ix^i \in \mathbb{Z}[x] \) will be called cleared if \( q_i \in \{0, 1\} \). For a given \( A(x) \in \mathbb{Z}[x] \), we wish to find \( B(x) \) and \( Q(x) \) with

\[
A(x) = (x^2 + 2x + 2)B(x) + Q(x),
\]
such that \( Q(x) = \sum_i q_ix^i \) is cleared. If this holds, then \( Q(\alpha) = \sum_i q_i\alpha^i \) is the desired expression.

This process is visualized for \( A(x) = 5 \) in the Table 1. The first line contains coefficients of \( A(x) = 5 \). The last line gives coefficients of the cleared polynomial \( Q(x) \) and each intermediate horizontal line contains a multiple of \( x^2 + 2x + 2 \).
Now we come to the main point. We only keep track of a sequence

\[-2, 2, -1, 0, 1, -1, 1\]

appeared in the upper diagonal of the matrix in Table 1. This is nothing but the sequence of coefficients of \(B(x)\). Denote this sequence by \(z_1, z_2, z_3, \ldots\). The key step is to switch to this sequence instead of observing the output reminders

\[1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1\]

Then \(z_i\) are determined by the inequality

\[0 \leq z_i + 2z_{i+1} + 2z_{i+2} < 2.\]

Dividing by 2, we get

\[0 \leq \frac{1}{2}z_i + z_{i+1} + z_{i+2} < 1.\]

Thus \(r = \left(\frac{1}{2}, 1\right)\). If \(r\) gives a SRS, then Knuth’s number system has the expected finiteness property. A straightforward generalization yields

**Theorem 3.1** The polynomial \(P(x) = x^d + b_{d-1}x^{d-1} + \cdots + b_1x + b_0\) gives a canonical number system if and only if \(\left(\frac{1}{b_0}, \frac{b_{d-1}}{b_0}, \ldots, \frac{b_1}{b_0}\right)\) gives a \(d\)-dimensional SRS.

The clearing algorithm was reformulated by a suitable base change of \(\mathbb{Z}[\alpha]\) into a SRS. An important idea, the set of witnesses, was invented independently by Brunotte [8, 9] and Scheicher-Thuswaldner [25, 26] under this base change. This method gives the easiest and fastest algorithm to determine whether \(\alpha\) gives a CNS or not. Consult [2] to see how this idea works in SRS framework.
4. $\beta$-expansions

A second type of number system, so called $\beta$-expansions, are related to SRS as well. Given $\beta > 1$, we wish to express a positive real number $x$ in a form

$$x = x_m \beta^m + x_{m+1} \beta^{m-1} + \ldots$$  \hspace{1cm} (4.1)

with $x_i \in \mathcal{A} = [0, \beta) \cap \mathbb{Z}$. A sum of form (4.1) is called a $\beta$-representation of $x$. A special $\beta$-representation, which is called the $\beta$-expansion can be obtained as follows. Find the largest integer $m$ such that $\beta^m \leq x < \beta^{m+1}$. Compute $x - x_m \beta^m$ with

$$x_m = \max\{a \in \mathcal{A} : x - a \beta^m \geq 0\}.$$  \hspace{1cm} (4.2)

Iterating this process will lead to an expansion of form (4.1). This setting is also a natural generalization of the decimal expansions.

Since $x_m$ is the largest possible digit such that $\beta^m \leq x_m \beta^m < \beta^{m+1}$, this algorithm is called greedy algorithm. In general, there exist infinitely many $\beta$-representations apart from the $\beta$-expansion. For example, so called lazy expansions (cf. [10]) are defined by taking

$$x_m = \min\{a \in \mathcal{A} : x - a \beta^m < \beta^m\}$$

in place of (4.2). For $x \in [0, 1)$, the greedy algorithm is equivalent to the following setting: Define the $\beta$-transformation $T : x \rightarrow \beta x - \lfloor \beta x \rfloor$. By iterating this map and considering its trajectory

$$x \xrightarrow{T(x)} x_1 \xrightarrow{T^2(x)} x_2 \xrightarrow{T^3(x)} \ldots$$

with $x_j = \lfloor \beta T^{j-1} x \rfloor$, we obtain

$$x = \frac{x_1}{\beta} + \frac{x_2}{\beta^2} + \frac{x_3}{\beta^3} + \ldots.$$  

We say that $d_\beta(x)$ is finite when $x_i = 0$ for all sufficiently large $i$. This is the case when there in an integer $i \geq 0$ such that $T^i(x) = 0$. For an arbitrary $x \geq 1$, there is a maximal integer $m$ such that $\beta^{-m} x \in [0, 1)$ with $d_\beta(\beta^{-m} x) = x_m x_{m+1} \cdots$. By shifting, we obtain

$$d_\beta(x) = x_m x_{m+1} \cdots x_1 x_0 . x_1 x_2 \cdots .$$

Formally, by applying $T$, one can expand 1 and obtains $d_\beta(1) = c_1 c_2 \ldots$. In contrast to CNS, in $\beta$-expansions some subwords of $\mathcal{A}^*$ never appear. For example, a subword $w = c_1 (c_2 + 1)$ can not appear even if $c_1 (c_2 + 1) \in \mathcal{A}^2$. This is because $w$ is too large and we should have already removed it earlier by the
greedy algorithm. Thus, a word of $A^*$ appears as a subword of a $\beta$-expansion if and only if all its suffices are less than $d_\beta(1)$ in natural lexicographic order (cf. [22, 15]). For e.g., take a real root $\beta \approx 3.104$ of $x^3 - 3x^2 - 1$ with $A = \{0, 1, 2, 3\}$. Since $d_\beta(1) = .301$, we see that six words $\{33, 32, 31, 303, 302, 301\}$ are forbidden. In other words, the letter 3 must be followed by two 0’s in a $\beta$-expansion.

$\beta$-expansions were introduced by Rényi [23], who proved that the $\beta$-transformation is ergodic. An invariant measure has been computed independently by Gelfond and Parry [12, 22]. As a non-trivial example for a dynamical system where the invariant measure is explicitly known, its arithmetic, diophantine and ergodic properties have been extensively studied. Let

$$
\text{Per}(\beta) = \{x \in \mathbb{R}_+ : d_\beta(x) \text{ is eventually periodic}\} \quad \text{and} \quad \text{Fin}(\beta) = \{x \in \mathbb{R}_+ : d_\beta(x) \text{ is finite}\}.
$$

Recall that a Pisot number is an algebraic integer $\beta > 1$ for which all algebraic conjugates $\gamma \neq \beta$ satisfy $|\gamma| < 1$.

If $\beta$ is a Pisot number, then $\text{Per}(\beta) = \mathbb{Q}(\beta) \cap \mathbb{R}_+$ (cf. Bertrand and Schmidt [7, 27]), which is a generalization of the fact that decimal expansions of rational numbers are eventually periodic.

We say that a number $\beta > 1$ has the finiteness property or property (F), if

$$
\text{Fin}(\beta) = \mathbb{Z}[\beta^{-1}] \cap \mathbb{R}_+.
$$

The inclusion $\text{Fin}(\beta) \subset \mathbb{Z}[\beta^{-1}] \cap \mathbb{R}_+$ is trivial. Obviously a rational number with a denominator $10^n$ has a finite decimal expansion. Therefore we are just expecting to have finite expansions for all reasonable candidates. The notion of the property (F) was introduced in [11]. If $\beta$ has property (F) then $\beta$ is a Pisot number (cf. [11]). Even a weaker condition $\mathbb{Z}_+ \subset \text{Fin}(\beta)$ implies that $\beta$ is a Pisot number (cf. [1]). On the other hand, there exist Pisot numbers which do not have property (F).

In [2] it is proved, that the problem of characterizing bases $\beta$ with property (F) and the problem of characterizing CNS are both special cases of the SRS finiteness problem. Before this, the following partial results have been established: Let $x^d - a_{d-1}x^{d-1} - \ldots - a_0$ be the minimal polynomial of $\beta$. Frougny and Solomyak [11] proved that

$$
a_{d-1} \geq a_{d-2} \geq \cdots \geq a_0 > 0
$$

is a sufficient condition for (F). Hollander proved that

$$
a_{d-1} \geq a_{d-2} + \cdots + a_0, \quad a_i \geq 0,
$$
is also sufficient. Akiyama [1] classified all cubic Pisot units with (F). Akiyama-Rao-Steiner [6] includes further progress. However, the problem of characterizing all cubic Pisot numbers with property (F) is still open.

5. Hollander’s Carry Sequence

The second originator of SRS is M. Hollander who was a student of B. Solomyak. As his thesis [14] did not yet appear in publication, we emphasize that the idea of SRS is basically due to him. Start from a relation:

\[ \beta^d = a_{d-1}\beta^{d-1} + a_{d-2}\beta^{d-2} + \cdots + a_0 \]

which is not necessarily irreducible. Let

\[ r_1 = \frac{a_0}{\beta} \]
\[ r_2 = \frac{a_1}{\beta} + \frac{a_0}{\beta^2} \]
\[ \vdots \]
\[ r_d = \frac{a_{d-1}}{\beta} + \frac{a_{d-2}}{\beta^2} + \cdots + \frac{a_0}{\beta^d} . \]

Then \( r_d = 1 \) and \( \{r_1, \ldots, r_d\} \) generates \( \mathbb{Z}[\beta] \) as a \( \mathbb{Z} \)-module and gives a basis if the relation is irreducible. Therefore, each \( \gamma \in \mathbb{Z}[\beta] \) has a representation \( \gamma = \sum_{i=1}^{d} z_i r_i \) with \( z_i \in \mathbb{Z} \). Let \( \gamma \in \mathbb{Z}[\beta] \cap [0,1) \), i.e.,

\[ 0 \leq z_1 r_1 + z_2 r_2 + \ldots + z_d r_d < 1. \]

Then the \( \beta \)-transform of \( \gamma \) can be written as

\[ T(\gamma) = \sum_{i=1}^{d} z_{i+1} r_i \]

with \( z_{d+1} \) satisfying

\[ 0 \leq z_2 r_1 + z_3 r_2 + \ldots + z_{d+1} r_d < 1. \]

Note that \( z_{d+1} \) is uniquely determined by this inequality, i.e.

\[ z_{d+1} = -\lfloor z_2 r_1 + z_3 r_2 + \ldots + z_d r_{d-1} \rfloor . \]

Hollander called this sequence \( z_1, z_2 \ldots \) a Carry Sequence. We clearly have

**Theorem 5.1** \( \beta \) has property (F) if and only if \( (r_1, r_2, \ldots, r_{d-1}) \) gives a \( (d-1) \)-dimensional SRS.
Let us come back to the example \( \beta^3 = 3\beta^2 + 0\beta + 1 \) with \( \beta \approx 3.104 \). In Table 2, we expand \( 5\beta^{-2} + 5\beta^{-3} \approx 0.2010 \). The reader will see that Hollander’s idea is similar to Gilbert’s clearing algorithm. In this case, we keep track of a sequence \(-2, -1, 1, 1\) in the upper diagonal in Table 2. For example, by considering the second line to 4-th, the sequence \(-2, -1, 1\) appears because

\[
(-2)r_1 - r_2 + r_3 = -2 \left( \frac{1}{\beta} \right) - \left( \frac{0}{\beta} + \frac{1}{\beta^2} \right) + \left( \frac{3}{\beta} + \frac{0}{\beta^2} + \frac{1}{\beta^3} \right) \in [0, 1)
\]

gives the fractional part, the image by \( T \). From the third to 5-th, we have

\[
(-1)r_1 + r_2 + r_3 = - \left( \frac{1}{\beta} \right) + \left( \frac{0}{\beta} + \frac{1}{\beta^2} \right) + \left( \frac{3}{\beta} + \frac{0}{\beta^2} + \frac{1}{\beta^3} \right) \in [0, 1).
\]

The key idea of Gilbert and Hollander is simply summarized:

*Observe quotients instead of reminders.*

Since the algorithms of CNS and \( \beta \)-expansions seemingly have not much to do with each other, it is surprising that both systems could be unified to the SRS setting.

6. Recent developments

For \( r = (r_1, \ldots, r_d) \in \mathbb{R}^d \), let \( \varrho(r) \) be the maximum absolute value of all roots of the polynomial \( x^d + r_d x^{d-1} + \ldots + r_1 \). Let

\[
\mathcal{D}_d^0 = \{ r \in \mathbb{R}^d \mid \forall a \in \mathbb{Z}^d \exists k > 0 : \tau_r^k(a) = 0 \}
\]

\[
\mathcal{D}_d = \{ r \in \mathbb{R}^d \mid \forall a \in \mathbb{Z}^d \text{ the sequence } \{ \tau_r^k(a) \}_{k \geq 0} \text{ is ultimately periodic} \}
\]

\[
\mathcal{E}_d = \{ r \in \mathbb{R}^d \mid \varrho(r) < 1 \}.
\]

Thus, \( \mathcal{D}_d^0 \) is the set of all vectors \( r \in \mathbb{R}^d \), such that \((\mathbb{Z}, \tau_r)\) is a SRS. Note that \( \mathcal{E}_d \) is a bounded subset of \( \mathbb{R}^d \) which can be explicitly described by certain polynomial inequalities. Furthermore, \( \mathcal{E}_d \subset \mathcal{D}_d \subset \overline{\mathcal{E}_d} \) holds (see [2]).
Let \( H \) be a compact subset of \( E_d \). In [2], an algorithm to determine \( D_0^d \cap H \) was derived. The set \( D_0^d \cap H \) can be constructed efficiently from \( H \) by cutting out finitely many convex polyhedra. However this algorithm does not work if \( H \) intersects \( \partial(E_d) \). The closer \( H \) is to \( \partial(E_d) \), the harder becomes the computation. We have \( \mathcal{E}_2 = \{(x, y) \in \mathbb{R}^2 : x < 1, |y| < x + 1\} \). Figure 1 shows an approximation of \( D_0^2 \). In [2, 3], several parts of the shaded (resp. white) areas are proved to be in (resp. not in) \( D_0^2 \). For example,

\[
\mathcal{S} := \{(r_1, r_2) \in \mathbb{R}^2 \mid -r_1 \leq r_2 < r_1 + 1, \quad 0 \leq r_1 \leq \frac{2}{3}\} \subset D_0^2,
\]

which contains the point \((1/2, 1)\) for Knuth’s number system. Furthermore the point \((r_1, r_2) \approx (0.322, 0.104)\) for \( x^3 - 3x^2 - 1 \) belongs to \( \mathcal{S} \) which means that the root \( \beta \approx 3.104 \) has property (F).

The characterization of \( D_0^2 \) is a hard problem. The main difficulties occur near the line \( L = \{(1, y) : -1 \leq y \leq 2\} \).

A symmetric version of SRS can be defined by shifting by 1/2:

\[
-\frac{1}{2} \leq r_1z_1 + r_2z_2 + \cdots + r_dz_d + z_{d+1} < \frac{1}{2}.
\]

This change gives rise to other number systems. They are symmetric canonical number systems and symmetric \( \beta \)-expansions. Imagine a ternary expression using digits \{-1, 0, 1\} instead of \{0, 1, 2\}. Symmetric \( \beta \)-expansions of real numbers are generated by a transformation \( \tau'_\beta : x \rightarrow \beta x - \lfloor \beta x + \frac{1}{2}\rfloor \) on \([-\frac{1}{2}, \frac{1}{2})\). Let

\[
\mathcal{D}_0^d = \{r \in \mathbb{R}^d \mid \forall a \in \mathbb{Z}^d \exists k > 0 : \tau'_{\beta^k}(a) = 0\}.
\]

In [24], \( \mathcal{D}_0^2 \) was completely characterized in this case since the regions near \( \partial(E_2) \) were already cut out! A picture of \( \mathcal{D}_0^2 \) is given in Figure 2. The outcome of this slight shift should be compared with Figure 1.

References


Figure 1: The sets $D_2^0$ and $E_2$.

Figure 2: The sets $D_2^0$ and $E_2$. 


Shigeki Akiyama
Department of Mathematics
Faculty of Science
Niigata University
Ikarashi 2-8050
Niigata 950-2181, Japan.
akiyama@math.sc.niigata-u.ac.jp

Klaus Scheicher,
Johann Radon Institute for Computational and Applied Mathematics,
Altenbergerstraße 69,
A-4040 Linz, Austria.
klaus.scheicher@oeaw.ac.at