Acta Mathematica Academiae Paedagogicae Nyíregyháziensis
22 (2006), 19–25
www.emis.de/journals
ISSN 1786-0091

BASIC PROPERTIES OF SHIFT RADIX SYSTEMS

SHIGEKI AKIYAMA, TIBOR BORBÉLY, HORST BRUNOTTE, ATTILA PETHŐ AND JÖRG M. THUSWALDNER

Abstract. Certain dynamical systems on the set of integer vectors $\mathbb{Z}^d$ are introduced and their basic properties are described. Applications to β-expansions and canonical number systems reveal unexpected relations between different radix representation concepts.

1. Introduction

Let $\mathbf{r} = (r_1, \ldots, r_d) \in \mathbb{R}^d$ $(d \geq 1)$. We are interested in the mapping $\tau_{\mathbf{r}} : \mathbb{Z}^d \to \mathbb{Z}^d$ defined by[1]

$$\tau_{\mathbf{r}}(\mathbf{a}) = (a_2, \ldots, a_d, -\lfloor r_1 a_1 + \cdots + r_d a_d \rfloor)$$

for $\mathbf{a} = (a_1, \ldots, a_d) \in \mathbb{Z}^d$. The mapping $\tau_{\mathbf{r}}$ is called a *shift radix system* (*SRS* for short) if for all $\mathbf{a} \in \mathbb{Z}^d$ we can find some $n \in \mathbb{N}$ with $\tau_{\mathbf{r}}^n(\mathbf{a}) = (0, \ldots, 0)$. In this note we give a short summary of basic properties and applications of SRS and mention some open problems. For more detailed background information and proofs the reader is referred to the original papers [1, 3].

Throughout we shall use the following sets which are closely connected to the orbits of $\tau_{\mathbf{r}}$:

$$\mathcal{D}_d^0 := \left\{ \mathbf{r} \in \mathbb{R}^d \,|\, \tau_{\mathbf{r}} \text{ is a SRS} \right\} \quad \text{and}$$
$$\mathcal{D}_d := \left\{ \mathbf{r} \in \mathbb{R}^d \,|\, \text{for all } \mathbf{a} \in \mathbb{Z}^d \text{ the sequence } (\tau_{\mathbf{r}}^n(\mathbf{a}))_{n \in \mathbb{N}} \text{ is ultimately periodic} \right\}.$$

Some subsets of these sets will be given later (see Sections 2 and 3), here we restrict to a few preliminary examples.

Examples. (i) $\mathcal{D}_1 = [-1, 1]$, $\mathcal{D}_1^0 = [0, 1)$ (see [1]).
(ii) $D \setminus \{(1, y) \in \mathbb{R}^2 \mid 0 < |y| < 1 \text{ or } 1 < |y| < 2\} \subseteq \mathcal{D}_2 \subseteq D$ where

$$D = \{(x, y) \in \mathbb{R}^2 \mid |x| \leq 1, |y| \leq 1 + x, \, (x, y) \neq (1, -2), (1, 2)\}$$
$$\setminus \{(x, -x - 1) \in \mathbb{R}^2 \mid 0 < x < 1\} \text{ (see [3]).}$$

2000 *Mathematics Subject Classification.* 11A63.
Key words and phrases. Beta expansion, canonical number system, dynamical system, Pisot number, radix representation.
The first author was supported by the Japan Society for the Promotion of Science, Grants in Aid for fundamental research 14540015, 2002–2005.
The fourth author was supported partially by the Hungarian National Foundation for Scientific Research Grant Nos. T42985 and T38225.
The fifth author was supported by project S8310 of the Austrian Science Foundation.

[1] $\lfloor \ldots \rfloor$ denotes the floor function.

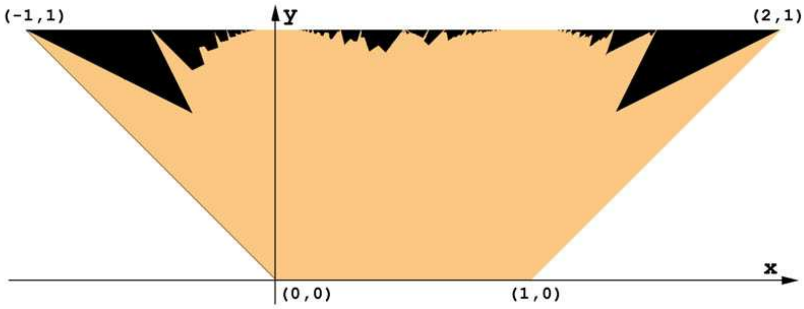

FIGURE 1. An approximation of $\mathcal{D}_2^0$.

(iii) Set

$$E_1 = \left\{ (x,y) \in \mathbb{R}^2 \;\middle|\; x < 1,\ y < 2x,\ \frac{2x}{3} + 1 \leq y \right\},$$

$$E_2 = \left\{ (x,y) \in \mathbb{R}^2 \;\middle|\; x < 1,\ \frac{x}{2} + 1 < y < 2x,\ y < \frac{2x}{3} + 1 \right\},$$

$$E_3 = \left\{ (x,y) \in \mathbb{R}^2 \;\middle|\; x < 1, -2x + 1 \leq y < -\frac{1}{2}x \right\}, \text{ and}$$

$$L = \left\{ (x,y) \in \mathbb{R}^2 \middle| 0 \leq x \leq \frac{5}{6},\ y < x + 1,\ y \geq -x \right\}.$$

Then $\mathcal{D}_2^0 \cap L = L \setminus (E_1 \cup E_2 \cup E_3)$ (see [3]).

In Figure 1 the gray points sketch an approximation of $\mathcal{D}_2^0$; note that the coordinate system is changed to be easier comparable to Figure 2 in Section 2.2.

2. Applications of shift radix systems

The main applications of SRS which have been dealt with so far are related to radix representations.

2.1 Shift radix systems and β-expansions. The so-called β-expansions have first been studied by A. RÉNYI [18] and W. PARRY [15] and have subsequently been intensively studied.

Let $\beta > 1$ be a non-integral real number. Then each $\gamma \in [0, \infty)$ can be represented uniquely by

$$\gamma = a_m \beta^m + a_{m-1}\beta^{m-1} + \cdots \tag{1}$$

with $a_i \in \{0, 1, \ldots, \lfloor \beta \rfloor\}$ such that

$$0 \leq \gamma - \sum_{i=n}^{m} a_i \beta^i < \beta^n \tag{2}$$

holds for all $n \leq m$. Since by condition (2) the digits a_i are selected as large as possible, the representation in (1) is called the *greedy expansion* of γ with respect to β.

Apart from the SRS notion the following theorem is basically due to M. HOLLANDER [7].

Theorem 1 (M. HOLLANDER)**.** *Let $d > 1$ and $\beta > 1$ be a real algebraic integer with minimal polynomial $X^d - b_1 X^{d-1} - \cdots - b_{d-1}X - b_d \in \mathbb{Z}[X]$. Define $r_2, \ldots, r_d \in \mathbb{R}$ by*

$$X^d - b_1 X^{d-1} - \cdots - b_{d-1}X - b_d = (X - \beta)(X^{d-1} + r_2 X^{d-2} + \cdots + r_d),$$

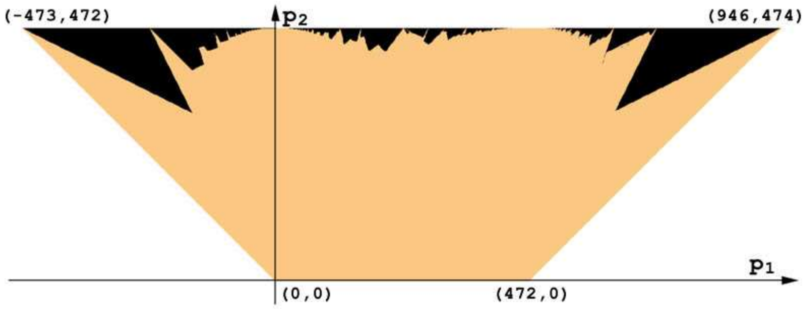

FIGURE 2. CNS polynomials $X^3 + p_2X^2 + p_1X + 474$.

hence $r_j = b_j\beta^{-1}+b_{j+1}\beta^{-2}+\cdots+b_d\beta^{j-d-1}$ $(2 \le j \le d)$. *Then* $(r_d, \ldots, r_2) \in \mathcal{D}_{d-1}^0$ *if and only if* $\mathbb{Z}[\frac{1}{\beta}] \cap [0,\infty)$ *coincides with the set of positive real numbers having finite greedy expansion with respect to* β.

Proof. See [1]. □

A. BERTRAND [4] and K. SCHMIDT [19] proved that if β is a Pisot number then the β-expansion of every element of $\mathbb{Q}(\beta)\cap[0,\infty)$ is ultimately periodic. The above mentioned finiteness property can only hold for Pisot numbers β (see [5], Lemma 1).

We remark that the characterization of Pisot numbers with the above mentioned finiteness property is not even known for degree $d = 3$.

2.1. **Shift radix systems and canonical number systems.** An example of a canonical number system was first studied by D. E. KNUTH [11, 12]. His notion was extended by W. J. GILBERT, I. KÁTAI, B. KOVÁCS and J. SZABÓ ([6, 8, 9, 10]) to quadratic number fields and by B. KOVÁCS [13] to arbitrary number fields as straightforward generalizations of the well-known radix representation of ordinary integers.

This concept was further generalized by the fourth author [17] by defining CNS polynomials: A monic integral polynomial $P(X)$ is called a *CNS polynomial* if every coset of $\mathbb{Z}[X]/P(X)\mathbb{Z}[X]$ contains an element of the form

$$a_0 + a_1x + \cdots + a_lx^l$$

with $a_0, \ldots, a_l \in \{0, 1, \ldots, |P(0)| - 1\}$ where x denotes the image of X under the canonical epimorphism from $\mathbb{Z}[X]$ to $\mathbb{Z}[X]/P(X)\mathbb{Z}[X]$.

Theorem 2. *Let* $p_0, \ldots, p_{d-1} \in \mathbb{Z}$ *with* $p_0 > 1$. *Then* $\left(\frac{1}{p_0}, \frac{p_{d-1}}{p_0}, \ldots, \frac{p_1}{p_0}\right) \in \mathcal{D}_d^0$ *if and only if* $X^d + p_{d-1}X^{d-1} + \cdots + p_0$ *is a CNS polynomial.*

Proof. See [1]. □

As an illustration the grey points in Figure 2 represent all cubic CNS polynomials with constant term equal to 474.

The complete description of CNS polynomials of degree $d > 2$ is still open.

3. BASIC PROPERTIES OF SHIFT RADIX SYSTEMS

For $\mathbf{r} = (r_1, \ldots, r_d) \in \mathbb{R}^d$ the mapping $\tau_{\mathbf{r}}$ differs from a linear mapping by a certain additive term. Although being small this term is the reason for the difficulties in controlling the iterates of $\tau_{\mathbf{r}}$: More precisely, we have for $\mathbf{a} \in \mathbb{Z}^d$

$$\tau_{\mathbf{r}}^n(\mathbf{a}) = R(\mathbf{r})^n\mathbf{a} + \sum_{i=1}^{n} R(\mathbf{r})^{n-i}\mathbf{v}_i$$

for all $n \in \mathbb{N}$ with the matrix

$$R(\mathbf{r}) := \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ -r_1 & -r_2 & \cdots & \cdots & -r_d \end{pmatrix}$$

and vectors $\mathbf{v}_i \in \mathbb{R}^d$ with $\| \mathbf{v}_i \|_\infty < 1$ (see [1]).

Theorem 3. (i) *The characteristic polynomial of $R(\mathbf{r})$ is given by*

$$X^d + r_d X^{d-1} + \cdots + r_2 X + r_1.$$

(ii) *If $\mathbf{r} \in \mathcal{D}_d$ then the spectral radius of $R(\mathbf{r})$ is less than or equal to 1.*

(iii) *If the spectral radius of $R(\mathbf{r})$ is less than 1 then $\mathbf{r} \in \mathcal{D}_d$.*

(iv) *Let $\mathbf{r} \in \mathbb{R}^d$ with spectral radius of $R(\mathbf{r})$ less than 1. Then there exists an effectively computable constant $c_\mathbf{r} \in \mathbb{R}$ with the property: $\mathbf{r} \in \mathcal{D}_d^0$ if for each $\mathbf{a} \in \mathbb{Z}^d$ with $\| \mathbf{a} \|_\infty \le c_\mathbf{r}$ the orbit of $\mathbf{a}$ under the iterates of $\tau_\mathbf{r}$ falls into the zero cycle.*

Proof. For (i), (ii), (iii) see [1] (note that the analogue of (ii) for canonical number systems is well known, see e. g. [6]). The proof of (iv) is analogous to that of Theorem 1 in [16]. □

By statement (iii) $\mathcal{D}_d$ contains the bounded set

$$\mathcal{E}_d = \big\{(r_1, \ldots, r_d) \in \mathbb{R}^d \,|\, \text{all roots of } X^d + r_d X^{d-1} + \cdots + r_1 \text{ lie inside the open unit circle}\big\}$$

which can be described by polynomial inequalities (for more information see the Schur-Cohn criterion (e. g. [14], Theorem 2.4.4)), and the closure of this set contains $\mathcal{D}_d$ by statement (ii).

Statement (iv) shows in particular that one can algorithmically decide whether or not a given $\mathbf{r}$ belongs to $\mathcal{D}_d^0$ (for a different algorithm and computational issues see [1]).

The next theorem exhibits a large subset of $\mathcal{D}_d^0$.

Theorem 4. *If $0 \le r_1 \le r_2 \le \cdots \le r_d < 1$ then $\mathbf{r} \in \mathcal{D}_d^0$.*

Proof. See [3]. □

Theorem 5. *For each $d \in \mathbb{N}$ the sets $\mathcal{D}_d$ and $\mathcal{D}_d^0$ are Lebesgue measurable. Further $\lambda(\mathcal{D}_d) = \lambda(\mathcal{E}_d)$ where λ denotes the d-dimensional Lebesgue measure.*

Proof. See [1]. □

The geometrical structure of $\mathcal{D}_d^0$ is quite complicated. For each $\mathbf{r} \in \mathcal{D}_d \setminus \mathcal{D}_d^0$ one can pick a point in $\mathbb{Z}^d$ which gives rise to a periodic orbit under the iterates of $\tau_\mathbf{r}$. On the other hand, given a point $\mathbf{a} \in \mathbb{Z}^d$ one may consider the collection of all $\mathbf{r} \in \mathbb{R}^d$ such that the sequences $(\tau_\mathbf{r}^n(\mathbf{a}))_{n\in\mathbb{N}}$ are periodic: More precisely, let

$$(a_{1+j}, \ldots, a_{d+j}) \qquad (0 \le j \le L-1)$$

with $a_{L+1} = a_1, \ldots, a_{L+d} = a_d$ be vectors of $\mathbb{Z}^d$. We ask for which $\mathbf{r} = (r_1, \ldots, r_d) \in \mathbb{R}^d$ we have $\tau_\mathbf{r}^L(\mathbf{a}) = \mathbf{a}$. By the definition of $\tau_\mathbf{r}$ this is the case if and only if the inequalities

$$0 \le r_1 a_{1+j} + \cdots + r_d a_{d+j} + a_{d+j+1} < 1 \quad (0 \le j \le L-1)$$

hold simultaneously. Hence, these points $\mathbf{r}$ form a (possibly degenerate) polyhedron in $\mathbb{R}^d$. As we saw in Example (i) we get $\mathcal{D}_1^0$ by simply taking away a single point

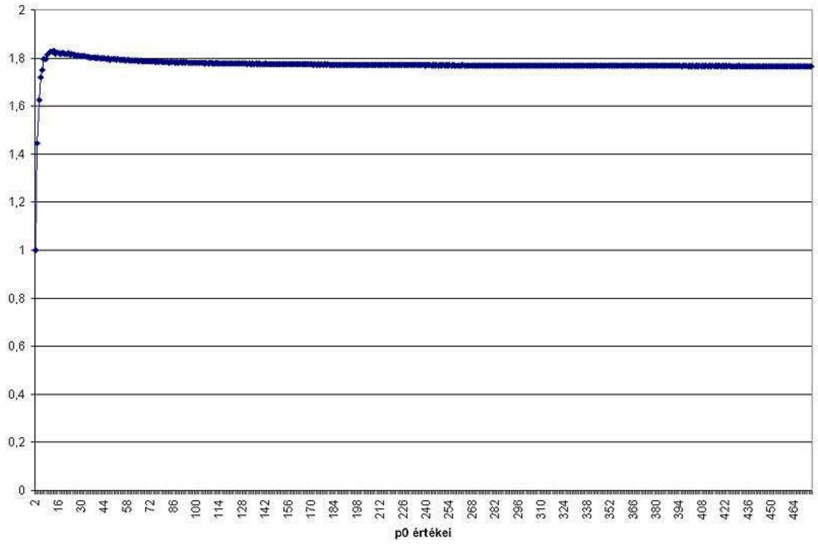

FIGURE 3. The behavior of $N^0(3, M)/M^2$ for $2 \le M \le 464$.

and a line segment from $\mathcal{D}_1$. However, it turns out that for $d > 1$ infinitely many polyhedra have to be removed from $\mathcal{D}_d$ in order to arrive at $\mathcal{D}_d^0$.

Theorem 6. *Let $d \ge 2$. Then $\mathcal{D}_d^0$ emerges from $\mathcal{D}_d$ by cutting out countably many polyhedra.*

Proof. See [1]. □

4. Some open problems

By what has been said above, the investigation of SRS leaves several questions open (see [1] and [3]). Here we only mention three problems.

1. We conjecture that $\mathcal{D}_2$ coincides with the set D defined in Example (ii). The truth of this conjecture would imply that $\mathcal{D}_2$ is convex. Results concerning this conjecture, including that the point $(1, \frac{1+\sqrt{5}}{2})$ belongs to $\mathcal{D}_2$ can be found in [2].

2. We conjecture that if $\mathbf{r} \in \mathcal{D}_d^0$ then the spectral radius of $R(\mathbf{r})$ is less than 1. This is clear for $d = 1$ (see Example (i) in Section 1), and for $d = 2$ it is proved in [3].

3. The following conjecture seems to be even more challenging: Let M be a positive integer and

$$N^0(d, M) = |\{(p_1, \dots, p_{d-1}) \in \mathbb{Z}^{d-1} \mid M + p_1 X + \cdots + p_{d-1} X^{d-1} + X^d \text{ is a CNS polynomial}\}|.$$

Then

$$\lim_{M \to \infty} \frac{N^0(d+1, M)}{M^d}$$

exists and is equal to the Lebesgue measure of $\mathcal{D}_d^0$. On Figure 3 we displayed[2] $N^0(3, M)/M^2$ for $2 \le M \le 464$. It seems that the quotient stabilizes after the first few values, which support the truth of the conjecture. An analogous conjecture has been formulated for the set $\mathcal{D}_d$ as well.

[2]We thank Andrea Huszti for preparing the Figure.

References

[1] S. Akiyama, T. Borbély, H. Brunotte, A. Pethő, and J. M. Thuswaldner. Generalized radix representations and dynamical systems. I. *Acta Math. Hungar.*, 108(3):207–238, 2005.

[2] S. Akiyama, A. Brunotte, A. Pethő, and W. Steiner. Remarks on a conjecture on certain integer sequences. To appear in Periodica Math. Hung.

[3] S. Akiyama, A. Brunotte, A. Pethő, and J. M. Thuswaldner. Generalized radix representations and dynamical systems ii. *Acta Arith.*, 121(1):21–61, 2006.

[4] A. Bertrand. Développements en base de Pisot et répartition modulo 1. *C. R. Acad. Sci. Paris Sér. A-B*, 285(6):A419–A421, 1977.

[5] C. Frougny and B. Solomyak. Finite beta-expansions. *Ergodic Theory Dynam. Systems*, 12(4):713–723, 1992.

[6] W. J. Gilbert. Radix representations of quadratic fields. *J. Math. Anal. Appl.*, 83(1):264–274, 1981.

[7] M. Hollander. *Linear Numerational Systems, Finite Beta Expansions, and Discrete Spectrum of Substitution Dynamical Systems.* PhD thesis, Washington University, Seattle, 1996.

[8] I. Kátai and B. Kovács. Kanonische Zahlensysteme in der Theorie der quadratischen algebraischen Zahlen. *Acta Sci. Math. (Szeged)*, 42(1-2):99–107, 1980.

[9] I. Kátai and B. Kovács. Canonical number systems in imaginary quadratic fields. *Acta Math. Acad. Sci. Hungar.*, 37(1-3):159–164, 1981.

[10] I. Kátai and J. Szabó. Canonical number systems for complex integers. *Acta Sci. Math. (Szeged)*, 37(3-4):255–260, 1975.

[11] D. E. Knuth. An imaginary number system. *Comm. ACM*, 3:245–247, 1960.

[12] D. E. Knuth. *The art of computer programming. Vol. 2 Seminumerical algorithms.* Addison-Wesley Publishing Co., third edition, 1998.

[13] B. Kovács. Canonical number systems in algebraic number fields. *Acta Math. Acad. Sci. Hungar.*, 37(4):405–407, 1981.

[14] M. Mignotte and D. Ştefănescu. *Polynomials.* Springer Series in Discrete Mathematics and Theoretical Computer Science. Springer-Verlag Singapore, Singapore, 1999. An algorithmic approach.

[15] W. Parry. On the β-expansions of real numbers. *Acta Math. Acad. Sci. Hungar.*, 11:401–416, 1960.

[16] A. Pethő. Notes on CNS polynomials and integral interpolation. to appear.

[17] A. Pethö. On a polynomial transformation and its application to the construction of a public key cryptosystem. In *Computational number theory (Debrecen, 1989)*, pages 31–43. de Gruyter, Berlin, 1991.

[18] A. Rényi. Representations for real numbers and their ergodic properties. *Acta Math. Acad. Sci. Hungar*, 8:477–493, 1957.

[19] K. Schmidt. On periodic expansions of Pisot numbers and Salem numbers. *Bull. London Math. Soc.*, 12(4):269–278, 1980.

Received July 3, 2005.

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

Tibor Borbély,
National Instruments Europe Kft,
H - 4031 Debrecen, Hatar u. 1/A,
Hungary
E-mail address: tibor.borbely@ni.com

Horst Brunotte,
Haus-Endt-Strasse 88, D-40593 Düsseldorf,
Germany
E-mail address: brunoth@web.de

Attila Pethő,
Department of Computer Science,
University of Debrecen,
P.O. Box 12, H-4010 Debrecen,
Hungary

Jörg M. Thuswaldner,
Chair of Mathematics and Statistics,
Leoben University,
Franz-Josef-Strasse 18, A-8700 Leoben,
Austria
E-mail address: joerg.thuswaldner@unileoben.ac.at