BASIC PROPERTIES OF SHIFT RADIX SYSTEMS

Shigeki Akiyama[1]
Department of Mathematics, Faculty of Science, Niigata University, Ikarashi 2-8050, Niigata 950-2181, JAPAN
akiyama@math.sc.niigata-u.ac.jp

Tibor Borbély
National Instruments Europe Kft, H - 4031 Debrecen, Hatar u. 1/A, HUNGARY
tibor.borbely@ni.com

Horst Brunotte
Haus-Endt-Straße 88, D-40593 Düsseldorf, GERMANY
brunoth@web.de

Attila Pethő[2]
Department of Computer Science, University of Debrecen, P.O. Box 12, H-4010 Debrecen, HUNGARY
pethoe@inf.unideb.hu

Jörg M. Thuswaldner[3]
Chair of Mathematics and Statistics, Leoben University, Franz-Josef-Straße 18, A-8700 Leoben, AUSTRIA
joerg.thuswaldner@unileoben.ac.at

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.

Key words: beta expansion, canonical number system, dynamical system, Pisot number, radix representation.

2000 Mathematics Subject Classification: 11A63

---

[1]The first author was supported by the Japan Society for the Promotion of Science, Grants in Aid for fundamental research 14540015, 2002–2005.

[2]The fourth author was supported partially by the Hungarian National Foundation for Scientific Research Grant Nos. T42985 and T38225.

[3]The fifth author was supported by project S8310 of the Austrian Science Foundation.

1. Introduction

Let $\mathbf{r} = (r_1, \dots, r_d) \in \mathbb{R}^d\,(d \geq 1)$. We are interested in the mapping $\tau_{\mathbf{r}} \;:\; \mathbb{Z}^d \to \mathbb{Z}^d$ defined by[4]

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

for $\mathbf{a} = (a_1, \dots, a_d) \in \mathbb{Z}^d$. 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 $\tau_{\mathbf{r}}^n(\mathbf{a}) = (0, \dots, 0)$. 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, 2].

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

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

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

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

(iii) Set

$$\begin{aligned}
E_1 &= \left\{(x, y) \in \mathbb{R}^2 \;\middle|\; x < 1,\ y < 2x,\ \frac{2x}{3} + 1 \leq y\right\}, \\
E_2 &= \left\{(x, y) \in \mathbb{R}^2 \;\middle|\; x < 1,\ \frac{x}{2} + 1 < y < 2x,\ y < \frac{2x}{3} + 1\right\}, \\
E_3 &= \left\{(x, y) \in \mathbb{R}^2 \;\middle|\; x < 1, -2x + 1 \leq y < -\frac{1}{2}x\right\}, \text{ and} \\
L &= \left\{(x, y) \in \mathbb{R}^2 \;\middle|\; 0 \leq x \leq \frac{5}{6},\ y < x + 1,\ y \geq -x\right\}.
\end{aligned}$$

Then

$$\mathcal{D}_2^0 \cap L = L \setminus (E_1 \cup E_2 \cup E_3) \text{ (see [2]).}$$

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.

[4] $\lfloor \dots \rfloor$ denotes the floor function.

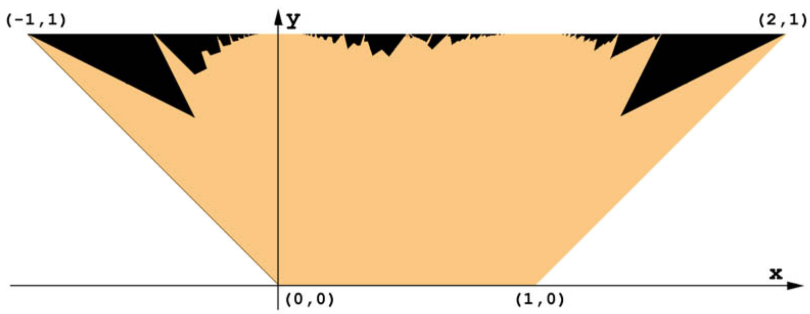

Figure 1: An approximation of $\mathcal{D}_2^0$.

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 [17] and W. Parry [14] 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 [6].

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

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

$$\text{hence } r_j \quad = \quad b_j \beta^{-1} + b_{j+1}\beta^{-2} + \cdots + b_d \beta^{j-d-1} \quad (2 \leq j \leq d).$$

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]. $\square$

A. Bertrand [3] and K. Schmidt [18] 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 [4], Lemma 1).

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

2.2 Shift radix systems and canonical number systems

An example of a canonical number system was first studied by D. E. Knuth [10, 11]. His notion was extended by W. J. Gilbert, I. Kátai, B. Kovács and J. Szabó ([5, 7, 8, 9]) to quadratic number fields and by B. Kovács [12] 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 [15] 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

$$a_0 + a_1 x + \cdots + a_l x^l$$

with $a_0, ..., a_l \in \{0, 1, \ldots, |P(0)| - 1\}$ 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]. $\square$

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

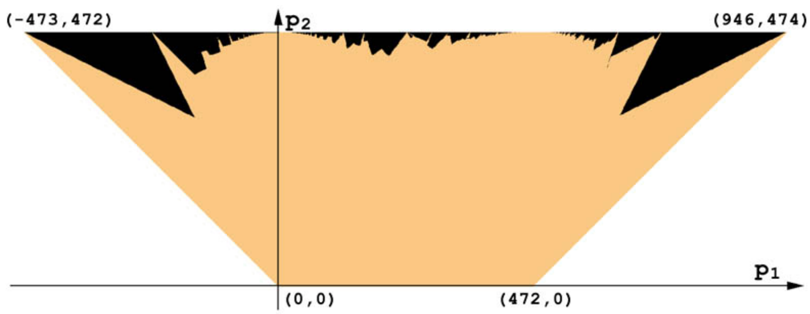

Figure 2: CNS polynomials $X^3 + p_2X^2 + p_1X + 474$.

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

$$X^d + r_dX^{d-1} + \cdots + r_2X + r_1.$$

(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 $\| \mathbf{a} \|_\infty \leq c_{\mathbf{r}}$ 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. [5]). The proof of (iv) is analogous to that of Theorem 1 in [16]. $\square$

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

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

which can be described by polynomial inequalities (for more information see the Schur-Cohn criterion (e. g. [13], 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 [2]. $\square$

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]. $\square$

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

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

with $a_{L+1} = a_1, \dots, a_{L+d} = a_d$ be vectors of $\mathbb{Z}^d$. We ask for which $\mathbf{r} = (r_1, \dots, r_d) \in \mathbb{R}^d$ 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 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]. $\square$

3. Some open problems

By what has been said above, the investigation of SRS leaves several questions open (see [1] and [2]). Here we only mention three problems.

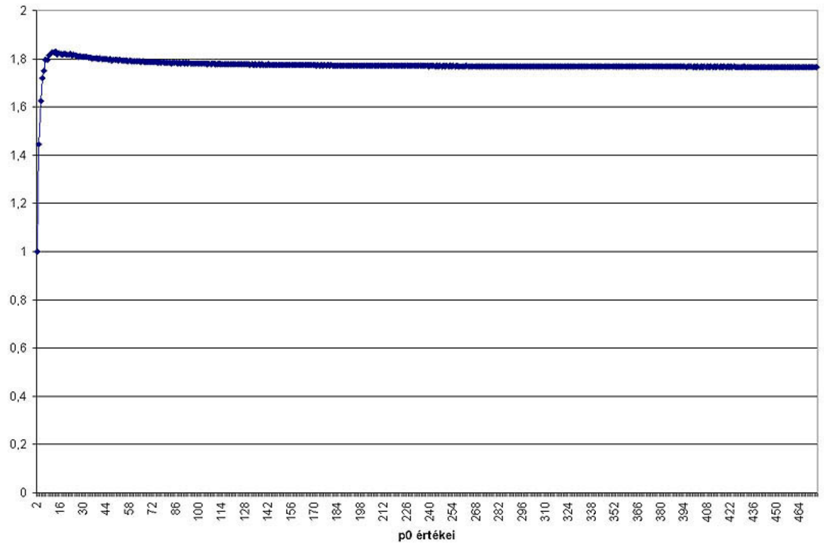

Figure 3: The behavior of $N^0(3, M)/M^2$ for $2 \leq M \leq 464$.

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. We thank W. Steiner [19] for the information that the point $(1, \frac{1+\sqrt{5}}{2})$ belongs to $\mathcal{D}_2$.

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 [2].

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

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

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 $N^0(3, M)/M^2$ for $2 \leq M \leq 464$. 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.

References

[1] S. Akiyama, T. Borbély, H. Brunotte, A. Pethő and J. M. Thuswald-

NER, Generalized radix representations and dynamical systems I, to appear in Acta Math. Hungar., **108 (3)** (2005), 207 – 238.

[2] S. Akiyama, H. Brunotte, A. Pethő and J. M. Thuswaldner, Generalized radix representations and dynamical systems II, to appear in Periodica Math. Hungar.

[3] A. Bertrand, *Développement en base de Pisot et répartition modulo* 1, C. R. Acad. Sci. Paris Sér. A-B, **285** (1977), 419 – 421.

[4] C. Frougny and B. Solomyak, *Finite beta-expansions*, Ergod. Th. and Dynam. Sys. **12** (1992), 713 – 723.

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

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

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

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

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

[10] D. E. Knuth, *An imaginary number system*, Comm. ACM, **3** (1960), 245 – 247.

[11] D. E. Knuth, *The Art of Computer Programming, Vol. 2 Semi-numerical Algorithms*, Addison Wesley (1998) London 3rd edition.

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

[13] M. Mignotte, D. Ştefănescu, *Polynomials*, Springer, Berlin Heidelberg New York (1999)

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

[15] A. Pethő, *On a polynomial transformation and its application to the construction of a public key cryptosystem, Computational Number Theory*, Proc., Walter de Gruyter Publ. Comp. Eds.: A. Pethő, M. Pohst, H. G. Zimmer and H. C. Williams, 1991, pp 31 – 43.

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

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

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

[19] W. Steiner, *private communication* (28/09/2004).