

# Number System Constructions with Block Diagonal Bases

By

ATTILA KOVÁCS\*

## Abstract

This paper deals with number system constructions using block diagonal bases. We show how easy is creating new generalized number systems from the existing ones via homomorphic constructions. We prove that diagonal extensions can always be performed even if the basic blocks are not number systems. As a special case we consider simultaneous systems in the Gaussian ring. We present a searching method and verify by computer that except 43 cases the Gaussian integers are always able to serve as basic blocks for simultaneous number systems using dense digit sets.

## § 1. Introduction

Let  $\Lambda$  be a lattice in  $\mathbb{R}^n$ ,  $M : \Lambda \rightarrow \Lambda$  be a linear operator such that  $\det(M) \neq 0$ , and let  $D$  be a finite subset of  $\Lambda$  containing 0.

**Definition 1.1.** The triple  $(\Lambda, M, D)$  is called a *number system* (GNS) if every element  $x$  of  $\Lambda$  has a unique, finite representation of the form  $x = \sum_{i=0}^l M^i d_i$ , where  $d_i \in D$ ,  $l \in \mathbb{N}$  and  $d_l \neq 0$ .

In the definition  $l_1 = l + 1$  denotes the *length of the expansion*. Clearly, (applying a suitable basis transformation) we may assume that  $M$  is integral acting on  $\Lambda = \mathbb{Z}^n$ . If two elements of  $\Lambda$  are in the same coset of the factor group  $\Lambda/M\Lambda$  then they are said to be *congruent modulo  $M$* .

**Theorem 1.2** ([12]). *If  $(\Lambda, M, D)$  is a number system then (1)  $D$  must be a full residue system modulo  $M$ , (2)  $M$  must be expansive and (3)  $\det(I - M) \neq \pm 1$ .*

If a system fulfils these conditions then it is a *radix system* and the operator  $M$  is called a *radix base*.

Let  $\phi : \Lambda \rightarrow \Lambda$ ,  $x \mapsto M^{-1}(x - d)$  for the unique  $d \in D$  satisfying  $x \equiv d \pmod{M}$ . Since  $M^{-1}$  is contractive and  $D$  is finite there exists a norm  $\|\cdot\|$  on  $\mathbb{R}^n$  and a constant  $C \in \mathbb{R}$

---

Received 31 October, 2012, Revised 13 September, 2013, Accepted 26 October, 2013.

2010 Mathematics Subject Classification(s): 11A63

*Key Words:* number expansions, number systems

Supported by TÁMOP 4.2.1/B-09/1/KMR-2010-0003

\*Eötvös Loránd University Budapest, Hungary.

e-mail: attila.kovacs@compalg.inf.elte.hu

such that the orbit of every  $x \in \Lambda$  eventually enters the finite set  $\{x \in \Lambda : \|x\| < C\}$  for the repeated application of  $\phi$ . This means that the sequence  $x, \phi(x), \phi^2(x), \dots$  is eventually periodic for all  $x \in \Lambda$ . If a point  $p \in \Lambda$  is periodic then  $\|p\| \leq L = Kr/(1-r)$ , where  $r = \|M^{-1}\| = \sup_{\|x\| \leq 1} \|M^{-1}x\| < 1$  and  $K = \max_{d \in D} \|d\|$  (see [13]). There are various problems in the research of lattice-type number expansions.

- The *decision problem* for a given  $(\Lambda, M, D)$  asks if they form a GNS or not.
- The *classification problem* means finding all periods (witnesses).
- The *parametrization problem* means finding parametrized families of GNS.
- The *construction problem* aims at constructing a digit set  $D$  to a given  $M$  for which  $(\Lambda, M, D)$  is a GNS.

In this paper we concentrate on the construction problem regarding block diagonal bases. The second part of the paper deals with special block diagonal systems, the so-called simultaneous systems. To be more precise we investigate simultaneous systems in the ring of Gaussian integers.

## § 2. Block Diagonal Bases

### § 2.1. Basic Lemmas

Let the radix systems  $(\Lambda_i, M_i, D_i)$  be given ( $1 \leq i \leq k$ ). Let  $\Lambda = \otimes \Lambda_i$  the direct product of the lattices,  $M = \oplus_{i=1}^k M_i$  the direct sum of the bases and  $D_h = \{(d_1^T \| d_2^T \| \cdots \| d_k^T)^T : d_i \in D_i\}$  the *homomorphic digit set*. Here  $d^T$  is a row vector and  $\|$  means the concatenation operator.

**Lemma 2.1.** *Using the notations above the following statements hold:*

1. *The operation  $\oplus$  is associative.*
2.  $\text{charpoly}(\oplus_{i=1}^k M_i) = \prod_{i=1}^k \text{charpoly}(M_i)$ .
3.  $\det(\oplus_{i=1}^k M_i) = \prod_{i=1}^k \det(M_i)$ .
4.  $\rho((\oplus_{i=1}^k M_i)^{-1}) = \max(\rho(M_i^{-1}))$  where  $\rho$  denotes the spectral radius.
5.  $D_h$  is a full residue system modulo  $M$ .
6.  $\phi((x_1^T \| x_2^T \| \cdots \| x_k^T)^T) = (\phi_1(x_1)^T \| \phi_2(x_2)^T \| \cdots \| \phi_k(x_k)^T)^T$   
*This means the function  $\phi$  has a homomorphic property.*

*Proof.* Only the last two statements need some argumentation. Clearly, the set  $D_h$  has  $\prod_{i=1}^k \det(M_i)$  elements. If  $x, y \in D_h$ ,  $x \equiv y \pmod{M}$ ,  $x \neq y$ , then  $Mz = x - y$  for some  $z \in \Lambda$ , i.e.  $M_i z_i = x_i - y_i$  ( $1 \leq i \leq k$ ). But then  $x_i \equiv y_i \pmod{M_i}$  hold for all  $i$ , which is a contradiction. The homomorphic property of the function  $\phi$  is a direct consequence of the definition.  $\square$

**Lemma 2.2.**  $(\Lambda, M, D_h)$  is a number system if and only if  $(\Lambda_i, M_i, D_i)$  are number systems.

*Proof.* The correctness of the lemma follows immediately from the homomorphic property of the function  $\phi$ .  $\square$

*Remark.* Many new GNS can be created via the homomorphic construction.

**Example 2.3.** Different kinds of number systems may serve as basic blocks for constructing block diagonal systems:

- (1) Canonical number systems, where the operator  $M$  is the companion of some monic integer polynomial with constant term  $c_0 \geq 2$  using 1-canonical digit sets. These CNS-polynomials were extensively studied by S. Akiyama, H. Brunotte, W. Gilbert, I. Kátai, A. Pethő, J. Thuswaldner, and many many others (see the comprehensive papers [2, 3]).
- (2) GNS where  $\text{charpoly}(M) = c_0 + c_1x + \dots + c_{n-1}x^{n-1} + x^n$  has the strong dominant condition  $|c_0| > 2 \sum_{i=1}^n |c_i|$  with 1-symmetric digit sets [9].
- (3) GNS where  $\rho(M^{-1}) < 1/2$  with dense digit sets [9]. This spectral radius condition holds (for example) if  $M$  is strong diagonally-dominant, i.e., if the  $j$ -th row of  $M$  is  $[m_1, \dots, m_j, \dots, m_n]$  then  $\text{Disc}(0, 2) \cap \text{Disc}(m_j, \sum_{i \neq j} |m_i|) = \emptyset$  for all  $j$ . Here  $\text{Disc}(c, r)$  means the complex disc with radius  $r$  centered at  $c$ . Dense digit sets are important for example in public key cryptography operations [7, 8].
- (4) Some special family of GNS: Generalized Balanced Ternary [15].
- (5) Simultaneous number systems [10], etc.

## § 2.2. Diagonal Extensions

Consider the case when the basic blocks of  $(\Lambda, M, D)$  are not (all) number systems. Then is there any (non-homomorphic) digit set  $D'$  for which  $(\Lambda, M, D')$  is GNS? Sometimes this question can easily be answered, and sometimes not.

**Example 2.4.** Let us see some earlier results:

- (1) In dimension 1 there are parametrized families of GNS (see the results of D.W. Matula, A.M. Odlyzko, A. Pethő, B. Kovács).
- (2) In dimension 2 in the imaginary quadratic fields all base  $M$  can serve for a GNS with some digit set  $D$  [11].
- (3) The situation in the real quadratic fields are unknown, we have only partial results [6].

*Conjecture.* For every radix  $M$  in real quadratic fields there is a corresponding digit set  $D$  for which  $(\mathbb{Z}^2, M, D)$  is GNS.

It is known that there are some operators for which there does not exist any digit set for which they form a GNS [4]. The following theorem shows some construction mechanism for these cases.

**Theorem 2.5.** For every radix base  $M_1 : \mathbb{Z}^{n_1} \rightarrow \mathbb{Z}^{n_1}$  either

1. there is a digit set  $D_1$  for which  $(\mathbb{Z}^{n_1}, M_1, D_1)$  is GNS, or
2. there is a radix  $M_2 : \mathbb{Z}^{n_2} \rightarrow \mathbb{Z}^{n_2}$ , such that  $(\mathbb{Z}^{n_1+n_2}, M_1 \oplus M_2, D)$  is GNS for some digit set  $D$ .

*Proof.* The main part of the proof was inspired by the paper of S. Akiyama et al. [1]. Let  $f(x) \in \mathbb{Z}[x]$  be the characteristic polynomial of  $M_1$ . Clearly,  $f(x)$  is expanding and  $\deg(f) = n_1$ . First we prove that, for any real  $K > 1$ , there exists a monic polynomial

$$g(x) = g_0 + g_1x + \cdots + g_{m-1}x^{m-1} + x^m \in \mathbb{Z}[x]$$

such that (1)  $g(x)$  is expanding, (2)  $|g_0| > K \sum_{i=1}^m |g_i|$ , and (3)  $g(x)$  is a multiple of  $f(x)$ .

Without loss of generality we may assume that  $1 < |\alpha_1| \leq |\alpha_2| \leq \cdots \leq |\alpha_{n_1}|$  where  $f(\alpha_i) = 0$  for all  $1 \leq i \leq n_1$ . Let  $k$  be a positive integer and set

$$(2.1) \quad G_k(x) = \prod_{i=1}^{n_1} (x - \alpha_i^k) = G_0 + G_1x + \cdots + x^{n_1}.$$

Since  $M_1$  is integral and  $(-1)^{n_1} \det(M_1^k - \lambda I) = G_k(\lambda)$  therefore  $G_k(x) \in \mathbb{Z}[x]$  for all  $k \in \mathbb{N}^+$  ( $I$  denotes the identity matrix). Since

$$\lim_{k \rightarrow \infty} \frac{\alpha_{j_1}^k \cdots \alpha_{j_s}^k}{\alpha_1^k \cdots \alpha_{n_1}^k} = 0$$

for any proper subset  $\{j_1, \dots, j_s\} \subset \{1, \dots, n_1\}$  therefore

$$\lim_{k \rightarrow \infty} \frac{|G_{n_1-i}|}{|G_0|} = \lim_{k \rightarrow \infty} \frac{|\sum_{1 \leq j_1 < \cdots < j_i \leq n_1} \alpha_{j_1}^k \cdots \alpha_{j_i}^k|}{|\alpha_1^k \cdots \alpha_{n_1}^k|} = 0.$$

Hence for any real  $K > 1$  there exist a  $k \in \mathbb{N}^+$  such that

$$(2.2) \quad \frac{1}{K} > \frac{|G_1|}{|G_0|} + \frac{|G_2|}{|G_0|} + \cdots + \frac{|G_{n_1-1}|}{|G_0|} + \frac{1}{|G_0|}$$

which is equivalent to

$$|G_0| > K \sum_{i=1}^{n_1} |G_i|.$$

Finally, let

$$g(x) = G_k(x^k) = \prod_{i=1}^{n_1} (x^k - \alpha_i^k).$$

It is easy to check that the conditions (1)–(3) all hold. Since

$$\sum_{i=1}^{n_1} \frac{|\sum_{1 \leq j_1 < \cdots < j_i \leq n_1} \alpha_{j_1}^k \cdots \alpha_{j_i}^k|}{|\alpha_1^k \cdots \alpha_{n_1}^k|} \leq \prod_{i=1}^{n_1} (1 + |\alpha_i^{-k}|) \leq (1 + |\alpha_{n_1}^{-k}|)^{n_1}$$

therefore inequality (2.2) holds provided

$$\left(1 + |\alpha_{n_1}^{-k}|\right)^{n_1} < \frac{1}{K}$$

which is equivalent to

$$(2.3) \quad k > -\frac{\log(|K^{-1/n_1} - 1|)}{\log |\alpha_{n_1}|}.$$

Let  $K = 2$  in the previous computation and let  $M_2$  be the companion of  $g(x)/f(x) \in \mathbb{Z}[x]$  with degree  $n_2$ . Then for the characteristic polynomial  $p(x)$  of  $M_1 \oplus M_2$  the strong dominant condition  $|p_0| > 2 \sum_{i=1}^{n_1+n_2} |p_i|$  hold, hence  $(\mathbb{Z}^{n_1+n_2}, M_1 \oplus M_2, D)$  is GNS with the 1-symmetric digit set [9].  $\square$

*Remark.* (1) The previous construction does not necessarily produces the minimal appropriate  $M_2$ . The construction of such minimal  $M_2$  (i.e.,  $n_2$  is minimal) seems to be hard. (2) The estimation (2.3) is in most cases very crude.

**Example 2.6.** Let  $\Lambda_1 = \mathbb{Z}^4, M_1 = \begin{pmatrix} 1 & 1 & -1 & 0 \\ -1 & 0 & 1 & 1 \\ 1 & 0 & -1 & 1 \\ -1 & 0 & 0 & 0 \end{pmatrix}$ . It is known that there does not exist any digit set  $D_1$  for which  $(\Lambda_1, M_1, D_1)$  is GNS. The characteristic polynomial of  $M_1$  is  $f_1(x) = x^4 + x^2 + 2$ . The smallest index  $k$  for which the strong dominant condition in (2.1) holds is 5 (the estimation (2.3) would give 11) and then  $G_5(x) = x^4 + 11x^2 + 32$ . Hence  $g(x) = G_5(x^5) = x^{20} + 11x^{10} + 32$  and  $f_2(x) = g(x)/f_1(x) = x^{16} - x^{14} - x^{12} + 3x^{10} - x^8 + 6x^6 - 4x^4 - 8x^2 + 16$ . If  $M_2$  belongs to the integer similarity class of the companion of  $f_2(x)$  then  $(\mathbb{Z}^{20}, M_1 \oplus M_2, D)$  is GNS with the 1-symmetric digit set  $D = \{(j, 0, \dots, 0)^T : -16 \leq j \leq 15\}$ .

### § 3. Simultaneous Systems

#### § 3.1. Basic Notions

In this section we investigate a special block diagonal system. Let  $\Lambda = \mathbb{Z}^n$ ,  $M_i : \Lambda \rightarrow \Lambda$  ( $1 \leq i \leq k$ ) and consider the system

$$(\Lambda \otimes \Lambda \otimes \cdots \otimes \Lambda, M_1 \oplus M_2 \oplus \cdots \oplus M_k, D),$$

where  $d_j = (v^T \|v^T\| \cdots \|v^T\|)^T \in D$  ( $v \in \Lambda$ ). These systems are called *Simultaneous Systems*.

Kátai [10] investigated the case when  $N_1, N_2, \dots, N_k$  are mutual coprime integers (none of them is 0,  $\pm 1$ ) and  $D = \{\delta e\}$  where  $e = (1, 1, \dots, 1)^T$ ,  $\delta = 1, 2, \dots, |N_1 N_2 \cdots N_k| - 1$ . The proper work of  $\phi$  is based on Chinese Remaindering. Kátai showed that the system  $(\mathbb{Z}^2, N_1 \oplus N_2, D)$  is GNS if and only if  $N_1 < N_2 \leq -2$  and  $N_2 = N_1 + 1$ .

Ch. van de Woestijne [16] investigated special polynomial homomorphic systems with canonical digit sets.

**Example 3.1.** In order to have a better insight into the proper work of simultaneous systems let see the following example. Let

$$M = \begin{pmatrix} -6 & 0 \\ 0 & -7 \end{pmatrix},$$

$$D = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \dots, \begin{pmatrix} 41 \\ 41 \end{pmatrix} \right\}.$$

Then 2012 has the expansion  $(38, 19, 22, 18, 10, 1)$  simultaneously in bases  $-6$  and  $-7$ . To be more precise the orbit of the point  $(2012, 2012)^T$  is

$$\begin{pmatrix} 2012 \\ 2012 \end{pmatrix} \xrightarrow{38} \begin{pmatrix} -329 \\ -282 \end{pmatrix} \xrightarrow{19} \begin{pmatrix} 58 \\ 43 \end{pmatrix} \xrightarrow{22} \begin{pmatrix} -6 \\ -3 \end{pmatrix} \xrightarrow{18} \begin{pmatrix} 4 \\ 3 \end{pmatrix} \xrightarrow{10} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \xrightarrow{1} \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

where the digit  $a$  above means the vector  $(a, a)^T$ .

**Lemma 3.2.** *Let  $M_1, M_2, \dots, M_k$  be pairwise commute  $n \times n$  matrices. If  $(\Lambda \otimes \Lambda \otimes \dots \otimes \Lambda, M_1 \oplus M_2 \oplus \dots \oplus M_k, D)$  is a simultaneous GNS then  $\det(M_i - M_j) = \pm 1$  for all  $i \neq j$ .*

*Proof.* Let  $z_1, z_2 \in \Lambda$  be arbitrary vectors and let  $z_1 = d_0 + M_i d_1 + \dots + M_i^t d_t$ ,  $z_2 = d_0 + M_j d_1 + \dots + M_j^t d_t$ . Then

$$(3.1) \quad z_1 - z_2 = (M_i - M_j)d_1 + \dots + (M_i^t - M_j^t)d_t.$$

Since each term  $(M_i^s - M_j^s)d_s$  in (3.1) can be written in the form

$$(M_i - M_j)(M_i^{s-1} + M_i^{s-2}M_j + \dots + M_j^{s-1})d_s$$

therefore  $z_1 \equiv z_2 \pmod{(M_i - M_j)}$  which means that  $\det(M_i - M_j) = \pm 1$ .  $\square$

*Remark.* Let  $\mathbb{K}$  be a number field with degree  $n$  and let  $\mathcal{O}_{\mathbb{K}}$  be the ring of its integers. It is known that there is always a  $\mathbb{Z}$ -basis of  $\mathcal{O}_{\mathbb{K}}$ . Suppose that  $\alpha_1, \alpha_2, \dots, \alpha_k \in \mathcal{O}_{\mathbb{K}}$  and  $(\alpha_1, \alpha_2, \dots, \alpha_k; D)$  is a simultaneous number system (using the notation of Kátai). Then  $\alpha_i - \alpha_j$  must be equal to the units of  $\mathcal{O}_{\mathbb{K}}$  for all  $1 \leq i, j \leq n$ .

### § 3.2. Simultaneous systems in the Gaussian ring

G. Nagy [14] investigated the case when  $\Lambda$  is the ring of Gaussian integers. He proved that  $(\mathbb{Z}^2 \otimes \mathbb{Z}^2, M_1 \oplus M_2, D)$  can never be a GNS when  $D$  is  $\{1, 3\}$ -canonical, i.e.  $D = \{(i, 0, i, 0)^T : 0 \leq i \leq |\det(M_1 \oplus M_2)| - 1\}$ . He conjectured also all the periods in these systems.

In the following we call the operators

$$\begin{pmatrix} a-b & 0 & 0 \\ b & a & 0 & 0 \\ 0 & 0 & a+1 & -b \\ 0 & 0 & b & a+1 \end{pmatrix}, \quad \begin{pmatrix} a-b & 0 & 0 \\ b & a & 0 & 0 \\ 0 & 0 & a & -(b+1) \\ 0 & 0 & b+1 & a \end{pmatrix}$$

as type A and type B operators, respectively  $(a, b \in \mathbb{Z})$ . We denote them shortly by  $M_A(a, b)$  and  $M_B(a, b)$ .

**Theorem 3.3.** *Let  $M_1 = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$  and  $M_2 \in \mathbb{Z}^{2 \times 2}$  such that  $\det(M_2 - M_1) = \pm 1$ . Then  $(\mathbb{Z}^2 \otimes \mathbb{Z}^2, M_1 \oplus M_2, D)$  is simultaneous GNS with the dense digit set except the 43 radix bases which can be seen in Figure 1.*

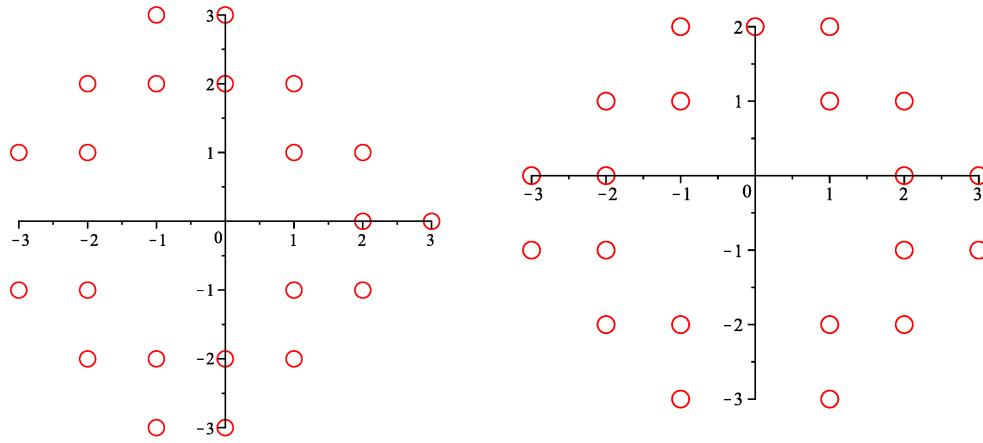


Figure 1. Radix bases for Simultaneous Number Systems in the ring of Gaussian integers with dense digit sets which are not number systems. A lattice point  $(a, b)$  in the picture denotes the  $M_A(a, b)$  (left picture) or the  $M_B(a, b)$  (right picture) operator, respectively. Altogether there are 43 exceptions. We note that  $M_A(i, j)$ ,  $-1 \leq i, j \leq 0$ ,  $M_A(-1, 1)$ ,  $M_A(0, 1)$ ,  $M_A(1, 0)$ ,  $M_A(-2, 0)$ , and  $M_B(i, j)$ ,  $-1 \leq i, j \leq 0$ ,  $M_B(0, 1)$ ,  $M_B(1, 0)$ ,  $M_B(1, -1)$ ,  $M_B(0, -2)$  are not radix bases.

*Proof.* The cases when  $\|M_1\|_2 > 4 + \frac{5}{2}\sqrt{2} + \frac{1}{2}\sqrt{98 + 72\sqrt{2}}$  ( $\approx 14.6$ ) has been proved by G. Nagy [14]. We deal with the remaining cases using a different construction.

Let  $M = M_A(a, b)$  or  $M_B(a, b)$ . Since  $r = \|M^{-1}\|_2 < 1$  always hold therefore in the following the norm  $\|\cdot\|$  means the 2-norm. We may assume that for the blocks  $\|M_1\| \leq \|M_2\|$ . Let  $S = \{(x, y, x, y)^T : x, y \in \mathbb{Z}\}$  be a linear subspace of  $\mathbb{Z}^4$ , and let  $D_1, D_2$  be full residue systems mod  $M_1$  and  $M_2$  respectively. First we show that there is a full residue system in  $S \pmod{M}$ . Let  $z = (z_1^T \| z_2^T)^T \in \mathbb{Z}^4$  arbitrary and consider the set  $D' = \{d_1 + M_1 d_2 : d_1 \in D_1, d_2 \in D_2\}$ . Then, applying Lemma 3.2 and Chinese Remaindering, the system of equations  $z_1 \equiv d \pmod{M_1}$ ,  $z_2 \equiv d \pmod{M_2}$  can be solved uniquely, where  $d \in D'$ .

Next, we can observe the integer similarity between  $\begin{pmatrix} a+1 & -b \\ b & a+1 \end{pmatrix}$  and  $\begin{pmatrix} a+1 & b \\ -b & a+1 \end{pmatrix}$ , furthermore between  $\begin{pmatrix} a & -(b+1) \\ b+1 & a \end{pmatrix}$  and  $\begin{pmatrix} a & b+1 \\ -b-1 & a \end{pmatrix}$ , hence it is enough to analyse the cases when  $b \geq 0$  and  $b \geq -1$ , respectively. Consider the dense digit set  $D$  in  $S$  modulo  $M$ , i.e., the set of elements with the smallest norm in each congruent set. We apply the following notations:

$$K = \max\{\|d\| : d \in D\}, K^* = \max\{\|d\| : d = (x, y)^T, (x, y, x, y)^T \in D\},$$

$$r = \|M^{-1}\|, r_i = \|M_i^{-1}\|, L = K \frac{r}{1-r}, L_i = K^* \frac{r_i}{1-r_i} \quad (i = 1, 2).$$

Let  $z = (z_1^T \| z_2^T)^T \in \mathbb{Z}^4$ ,  $\|z\| \leq L$ ,  $z \notin S$  be arbitrary. Then

$$\begin{aligned} \|\phi(z_1) - \phi(z_2)\| &= \\ \|M_1^{-1}(z_1 - d) - M_2^{-1}(z_2 - d)\| &= \\ \|M_1^{-1}(z_1 - d) - M_1^{-1}(z_2 - d) + M_1^{-1}(z_2 - d) - M_2^{-1}(z_2 - d)\| &\leq \\ \|M_1^{-1}(z_1 - d - (z_2 - d))\| + \|(M_1^{-1} - M_2^{-1})(z_2 - d)\| &\leq \\ \|M_1^{-1}\| \cdot \|(z_1 - d) - (z_2 - d)\| + \|M_1^{-1}M_2^{-1}\| \cdot \|z_2 - d\| &\leq \\ \|M_1^{-1}\| \cdot \|(z_1 - d) - (z_2 - d)\| + \|M_1^{-1}M_2^{-1}\| \cdot (L_2 + K^*) & \end{aligned}$$

where  $(d^T \|d^T)^T \in D$ . Clearly, if

$$\|M_1^{-1} \cdot M_2^{-1}\| \cdot (L_2 + K^*) < 1 - \|M_1^{-1}\|$$

then  $\|\phi(z_1) - \phi(z_2)\| < \|z_1 - z_2\|$ . Let

$$\kappa = \frac{\|M_1^{-1}\| \cdot \|M_2^{-1}\| \cdot (L_2 + K^*)}{1 - \|M_1^{-1}\|} = K^* \frac{r_1 r_2}{(1 - r_1)(1 - r_2)} = L_1 L_2 / K^*.$$

Since  $\|\pi\| \leq L$  holds for each periodic element  $\pi$  we proved the following lemma:

**Lemma 3.4.** *If (1)  $\kappa < 1$  and all the points in  $S \cap L \setminus \{\underline{0}\}$  are non-periodic or (2)  $\kappa \geq 1$  and all the points  $v = (x, y, z, w)^T$  ( $v \neq \underline{0}$ ) for which*

$$(3.2) \quad \|v\| \leq L, \quad \|(x, y)^T - (z, w)^T\| < \kappa$$

*are non-periodic then  $(\mathbb{Z}^2 \otimes \mathbb{Z}^2, M, D)$  is a simultaneous number system.*

Applying Lemma (3.4) we checked the possible candidates by computer, where  $\|M_1\| < 14.7$  ( $b \geq 0$  in type A and  $b \geq -1$  in type B operators). We got that except 43 cases all the examined systems are simultaneous number systems with dense digit sets. The exceptional cases can be seen in Figure 1. The proof of Theorem 3.3 is finished.  $\square$

**Example 3.5.** Let us examine the base  $M = M_A(2, 2)$ . Then  $\|M_1\| = 2.828$ ,  $\|M_2\| = 3.605$ , the dense digit set  $D$  in the subspace  $S$  has 104 elements,  $K^* = 10.198$ ,  $L_1 = 5.589$ ,  $L_2 = 3.906$ ,  $\kappa = 2.14$ . The number of elements satisfying (3.2) are 305, all of them runs to  $\underline{0} \in \mathbb{Z}^4$  for the repeated application of  $\phi$ , therefore the system is a number system.

*Remark.* For the computations we used the Maple programming language in a simple laptop. The total computing time was approximately 15 minutes.

Figure 1 shows the bases for which the dense digit sets are not appropriate for constituting simultaneous number systems. We plan to examine these cases applying a digit set construction algorithm or proving that such constructions are not possible at all.

The author is grateful to the reviewers for their helpful comments, which contributed to improve the quality of the paper.

## References

- [1] Akiyama, S., Drungilas, P., Jankauskas, J., Height reducing problem on algebraic integers, *Functiones at Approximatio, Commentarii Mathematici* **47**/1, (2012), 105–119.
- [2] Akiyama, S., Borbély, T., Brunotte, H., Pethő, A., Thuswaldner, J., Generalized radix representations and dynamical systems I, *Acta Mathematica Hungarica* **108**/3, (2005), 207–238.
- [3] Barat, G., Berthé, V., Liardet, P., Thuswaldner, J., Dynamical directions in numeration (Dynamique de la numération) *Annales de l'institut Fourier* **56**/7, (2006), 1987–2092.
- [4] Barbé, A., von Haeseler, F., Binary number systems for  $\mathbb{Z}^k$ , *J. Number Theory*, **117**/1, (2006), 14–30.



- [5] Burcsi, P., Kovács, A., Papp-Varga, Zs., Decision and classification algorithms for generalized number systems, *Annales Univ. Sci. Budapest. Sect. Comp.* **28**, (2008), 141–156.
- [6] Farkas, G., Kovács, A., Digital expansion in  $\mathbb{Q}(\sqrt{2})$ , *Annales Univ. Sci. Budapest. Sect. Comp.* **22**, (2003), 83–94.
- [7] Heuberger, C., Krenn, D., Optimality of the Width- $w$  Non-adjacent Form: General Characterisation and the Case of Imaginary Quadratic Bases, *arXiv:1110.0966*, 2011.
- [8] Heuberger, C., Krenn, D., Existence and Optimality of  $w$ -Non-adjacent Forms with an Algebraic Integer Base, *arXiv:1205.4414*, 2012.
- [9] Germán, L., Kovács, A., On number system constructions, *Acta Math., Hungar.*, **115**/(1-2), (2007), 155–167.
- [10] Indlekofer, K-H., Kátai, I., Racskó, P., Number systems and fractal geometry, *Probability Theory and Applications, Kluwer Academic Press*, (1993), 319–334.
- [11] Kátai, I., Number systems in imaginary quadratic fields, *Annales Univ. Sci. Budapest., Sect. Comp.*, **14**, (1994), 159–164.
- [12] Kovács, A., Number expansions in Lattices, *Math. Comput. Modelling*, **38**, (2003), 909–915.
- [13] Kovács, A., On computation of attractors for invertible expanding linear operators in  $\mathbb{Z}^k$ , *Publ. Math. Debrecen*, **56**/(1-2), (2000), 97–120.
- [14] Nagy, G., On the simultaneous number systems of Gaussian integers, *Annales Univ. Sci. Budapest., Sect. Comp.* **35** (2011), 223–238.
- [15] Vince, A., Replicating tessellations, *SIAM Journal of Discrete Math.*, **6**, (1993), 501–521.
- [16] van de Woestijne, C., Number systems and the Chinese Remainder Theorem, *arXiv:1106.4219*