Publ. Math. Debrecen
58 / 3 (2001), 423–440

Attractors for invertible expanding linear operators and number systems in $\mathbb{Z}^2$

By JÖRG M. THUSWALDNER (Leoben)

Abstract. Let M be a 2×2 matrix whose eigenvalues have all modulus greater than 1, and let $\mathcal{N}$ be a complete residue system of vectors $\bmod M(\mathbb{Z}^2)$. Define a mapping $\Phi(z) = M^{-1}(z - \delta)$, for $\delta \in \mathcal{N}$, such that $\Phi(z)$ has integer coordinates. Then the iterates $\Phi^k(z)$ give rise to a dynamical system, whose attractor $\mathcal{P}$ is a bounded set. In this paper we determine $\mathcal{P}$ explicitely for a certain class of matrices. For the special case $\mathcal{P} = \{0\}$, the pair $(M, \mathcal{N})$ can be regarded as a number system in $\mathbb{Z}^2$. These number systems have strong connections to number systems in number fields. So we are able to give an easy proof for the characterization of the bases of canonical number systems in quadratic fields with help of our results. This characterization was first given in a series of papers by Kátai, Kovács and Szabó.

1. Introduction

Let $M \in \mathbb{Z}^{n \times n}$ be an invertible matrix with integer entries, whose eigenvalues have all modulus greater than one. Then $M\mathbb{Z}^n$ is a sublattice of $\mathbb{Z}^n$ with index $\beta := \det M$. Let $\mathcal{N}$ be a complete residue system of elements of $\mathbb{Z}^n$ modulo $M\mathbb{Z}^n$. Now define the mapping

$$\Phi(z) := M^{-1}(z - \delta),$$

where δ is the unique element of $\mathcal{N}$ with $\delta \equiv z \pmod{M}$. If $\Phi^l(z)$ denotes the l-th iterate of Φ then for each $z \in \mathbb{Z}^n$ we call $\Phi^j(z)$, $(j \geq 0)$ the orbit of z generated by Φ. It is easy to see (cf. [4], [8]), that there exists a

Mathematics Subject Classification: 11A63, 68Q68.
Key words and phrases: radix representations, automata, dynamical systems.
The author was supported by project number 34oeu24 of the Stiftung Aktion Österreich-Ungarn.

constant C with the following property: Let $\|\cdot\|$ denote any norm in $\mathbb{R}^n$. Then for each $z \in \mathbb{Z}^n$ there exists an integer j_0 such that for each $j \geq j_0$ we have $\|\Phi^j(z)\| \leq C$. Since there exist only finitely many elements of $\mathbb{Z}^n$ with $\|z\| \leq C$, we conclude, that the sequence

$$\Phi^0(z),\ \Phi^1(z), \dots \tag{1}$$

is ultimately periodic for each $z \in \mathbb{Z}^n$.

Let us call an element $p \in \mathbb{Z}^n$ *periodic*, if for some positive integer ω we have $\Phi^\omega(p) = p$, and denote the set of all periodic elements by $\mathcal{P}$. Since the sequence $\{\|\Phi^j(z)\|\}_{j\geq 0}$ is ultimately $\leq C$ we conclude, that $\mathcal{P}$ has only finitely many elements. It is clear, that (1) ends in a cycle of periodic points for each z. Thus $\mathcal{P}$ is the *attractor* of the dynamical system generated by Φ.

The aim of the present paper is the determination of $\mathcal{P}$ for certain matrices M. For some cases a similar problem has been investigated in Kovács [9]. Furthermore, properties of the attractor $\mathcal{P}$ have been studied in several papers. For instance, I. Kátai [4] studied periodic points of so called *just touching covering systems* and recently A. Kovács [8] obtained some general results for $\mathcal{P}$. In the following paragraph we want to restate some easy observations that can be found also in these papers.

First of all, it is immediate from the definition of Φ and $\mathcal{P}$, that each $z \in \mathbb{Z}^n$ admits a unique representation of the shape

$$z = \sum_{\ell=0}^{L} M^\ell a_\ell + M^{L+1} p \tag{2}$$

with $p \in \mathcal{P}$, $a_\ell \in \mathcal{N}$ and L as small as possible. We call this representation the *M-adic* representation of z. Since p is a periodic point, there exists a positive integer ω, such that $p = \sum_{k=0}^{N\omega-1} M^k b_{k \bmod \omega} + M^{N\omega} p$, with $b_0, \dots, b_{\omega-1} \in \mathcal{N}$ and $N \in \mathbb{N}$ arbitrary large. So we can rewrite (2) in the form

$$z = \sum_{\ell=0}^{L} M^\ell a_\ell + M^{L+1} \sum_{k=0}^{N\omega-1} M^k b_{k \bmod \omega} + M^{L+1+N\omega} p$$

for any $N \in \mathbb{N}$. Denoting the infinite repetition of a string $b_{\omega-1} \dots b_0$ by $(b_{\omega-1} \dots b_0)^\infty$ we identify z with the infinite digit string

$$z = ((b_{\omega-1} \dots b_0)^\infty a_L \dots a_0)_M.$$

Thus for $\mathcal{P} = \{0\}$ each z has a unique M-adic representation of the form

$$z = \sum_{\ell=0}^{L} M^{\ell} a_{\ell} \tag{3}$$

with $a_\ell \in \mathcal{N}$ and $a_L \neq 0$ for $L \neq 0$. In this case we call the pair $(M, \mathcal{N})$ a *number system* in $\mathbb{Z}^n$.

In this paper we will explicitely compute the attractor $\mathcal{P}$ for each invertible matrix $M \in \mathbb{Z}^{2\times 2}$ with the corresponding set $\mathcal{N}_0 = \{(0,0)^T, (1,0)^T, \ldots, (|\beta|-1,0)^T\}$ (v^T denotes the transposition of a vector v). Of course, this makes sense only for matrices M, for which $\mathcal{N}_0$ forms a complete residue system modulo M, since otherwise the mapping Φ were not defined correctly. It is easy to see, that this is the case exactly for those matrices M that satisfy

$$M = \begin{pmatrix} a & b \\ \varepsilon & d \end{pmatrix} \quad \text{with } \varepsilon = \pm 1.$$

In the remaining part of this paper we will always tacitly assume, that M has this form. If a matrix M forms a number system with respect to the set $\mathcal{N}_0$ we call $(M, \mathcal{N}_0)$ a *canonical number system*. Thus we get the characterization of all canonical number systems in $\mathbb{Z}^2$ as a corollary to our result. This gives the solution of the two-dimensional case of Problems 1 and 6 of KOVÁCS [8].

2. Statement of results

In this section we give our main results. The first result gives a characterization of the set of periodic points of a pair $(M, \mathcal{N}_0)$, the second one characterizes the matrices M, that give rise to a canonical number system.

Theorem 2.1. *Let $M := \left(\begin{smallmatrix} a & b \\ \varepsilon & d \end{smallmatrix}\right)$ with $\varepsilon \in \{-1, 1\}$ be a matrix with characteristic polynomial $p(x) = x^2 + \alpha x + \beta$ and $\mathcal{N}_0 = \{(0,0)^T, (1,0)^T, \ldots, (|\beta|-1,0)^T\}$. Let $\Phi(z) = M^{-1}(z-\delta)$, where δ is the unique element of $\mathcal{N}_0$ with $\delta \equiv z \pmod{M}$, and let $\mathcal{P}$ be the attractor of the dynamical system generated by Φ. Then $\mathcal{P}$ has the following shape:*

- *For $0 \leq \alpha \leq \beta \geq 2$ we have $\mathcal{P} = \{0\}$ and $\Phi(0) = 0$.*

- *For $0 < -\alpha \le \beta \ge 2$ let $\gamma := \beta + \alpha + 1$ and let K be the integer defined by $K\gamma \le \beta - 1 < (K+1)\gamma$. Then*

$$\mathcal{P} = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1-d \\ \varepsilon \end{pmatrix}, \dots, \begin{pmatrix} K(1-d) \\ K\varepsilon \end{pmatrix} \right\}$$

  and $\Phi(p) = p$ for each $p \in \mathcal{P}$.

- *For $0 \le -\alpha < -\beta \ge 2$ we have*

$$\mathcal{P} = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \end{pmatrix}, \begin{pmatrix} d \\ -\varepsilon \end{pmatrix} \right\}.$$

  Furthermore, $\Phi(0) = 0$, $\Phi((-1,0)^T) = (d, -\varepsilon)^T$ and $\Phi((d,-\varepsilon)^T) = (-1,0)^T$.

- *For $0 < \alpha < -\beta \ge 2$ let $\gamma := -\beta - \alpha - 1$ and define K by $K\gamma \le -\beta - 1 < (K+1)\gamma$. Then*

$$\mathcal{P} = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} d-1 \\ -\varepsilon \end{pmatrix}, \dots, \begin{pmatrix} K(d-1) \\ -K\varepsilon \end{pmatrix} \right\}$$

  and $\Phi(p) = p$ for each $p \in \mathcal{P}$.

In the remaining cases $|\beta| = 1$ or $2 \le \beta < |\alpha|$ or $2 \le -\beta \le |\alpha|$ the corresponding matrix M has at least one eigenvalue with modulus less than or equal to 1.

Corollary 2.1. *Let M, $\mathcal{N}_0$, α and β be defined as in Theorem 2.1. Then $(M, \mathcal{N}_0)$ is a canonical number system if and only if $-1 \le \alpha \le \beta \ge 2$.*

This corollary is an immediate consequence of Theorem 2.1.

The main tool for the proof of Theorem 2.1 will be a so-called *transducer automaton* (cf. for instance [1], [12] for its definition) that performs the addition of $(1,0)^T$ on the M-adic representations. For the construction of this automaton, we will need the identity

$$M^2 + \alpha M + \beta I = 0 \tag{4}$$

which directs the possible carries occurring by the addition of $(1,0)^T$ in M-adic representations. Similar "counting automata" where studied in Grabner–Kirschenhofer–Prodinger [2]. Thuswaldner [13] mentioned that they are useful for the characterization of bases of number systems in number fields.

3. The case $0 \le \alpha \le \beta$

In this section we will prove, that a matrix M satisfying $0 \le \alpha \le \beta$ has always $\mathcal{P} = \{0\}$. Thus in this case M is the base of a canonical number system in $\mathbb{Z}^2$. For convenience, we will identify the digit $(\nu, 0)^T$ with ν. This will cause no confusions and allows an easier notation.

The plan of our proof is the following: Obviously $(0,0)^T$ has the finite representation 0. Let $z \in \mathbb{Z}^2$ have a finite M-adic representation of the shape (2) with $p = 0$. We shall prove that then $z+(\pm 1, 0)^T$ and $z+(0, \pm 1)^T$ have again finite M-adic representations. This implies by induction, that any $z \in \mathbb{Z}^2$ has a representation of the form (2) with $p = 0$. Thus $\mathcal{P} = \{0\}$.

As mentioned in the previous section, so-called counting automata are an appropriate tool to perform the addition of 1 on the M-adic representations. Adopting the notations of [2], let σ be a digit string. Let $(\sigma)_M$ denote the vector, whose M-adic representation has digit string σ. Let furthermore σ^P, σ^{-P}, σ^Q, σ^{-Q}, σ^R and σ^{-R} be the string defined respectively by

$$\begin{aligned} (\sigma^{\pm P})_M &= (\sigma)_M \pm (1,0)^T, \\ (\sigma^{\pm Q})_M &= (\sigma)_M \pm M(1,0)^T \pm (\alpha - 1, 0)^T, \\ (\sigma^{\pm R})_M &= (\sigma)_M \mp M(1,0)^T \mp (\alpha, 0)^T. \end{aligned} \tag{5}$$

Using (4) we obtain the following rules for these operations (remember the convention for writing the digits; a bar over a term indicates, that this term represents one digit).

$$(\sigma\nu)^P = \begin{cases} \sigma\overline{\nu+1}, & \nu \in \{0, \dots, \beta-2\} \\ \sigma^R 0, & \nu = \beta - 1, \end{cases}$$

$$(\sigma\nu)^{-P} = \begin{cases} \sigma^{-R}\overline{\beta-1}, & \nu = 0 \\ \sigma\overline{\nu-1}, & \nu \in \{1, \dots, \beta-1\}, \end{cases}$$

$$(\sigma\nu)^Q = \begin{cases} \sigma^P\overline{\nu+\alpha-1}, & \nu \in \{0, \dots, \beta-\alpha\} \\ \sigma^{-Q}\overline{\nu-\beta+\alpha-1}, & \nu \in \{\beta-\alpha+1, \dots, \beta-1\}, \end{cases}$$

$$(\sigma\nu)^{-Q} = \begin{cases} \sigma^Q\overline{\nu+\beta-\alpha+1}, & \nu \in \{0, \dots, \alpha-2\} \\ \sigma^{-P}\overline{\nu-\alpha+1}, & \nu \in \{\alpha-1, \dots, \beta-1\}, \end{cases}$$

$$(\sigma\nu)^R = \begin{cases} \sigma^Q\overline{\nu+\beta-\alpha}, & \nu \in \{0,\dots,\alpha-1\} \\ \sigma^{-P}\overline{\nu-\alpha}, & \nu \in \{\alpha,\dots,\beta-1\}, \end{cases}$$

$$(\sigma\nu)^{-R} = \begin{cases} \sigma^P\overline{\nu+\alpha}, & \nu \in \{0,\dots,\beta-\alpha-1\} \\ \sigma^{-Q}\overline{\nu-\beta+\alpha}, & \nu \in \{\beta-\alpha,\dots,\beta-1\}. \end{cases}$$

We want to prove only the first rule, all the others can be established by similar reasoning. Let $\sigma = \dots\sigma_3\sigma_2\sigma_1$ with $\sigma_j \in \mathcal{N}_0$ $(j \geq 1)$ be the digit string of an M-adic representation and define L as in Section 1. We want to get a recurrence for the digit string of the M-adic representation of $((\sigma\nu)^P)_M = (\sigma\nu)_M + (1,0)^T$. We first add the digit string of the representation $(1,0)^T = (1)_M$ to $\sigma\nu$. Digitwise addition yields the digit string $\sigma\overline{\nu+1}$. If $\nu \in \{0,\dots,\beta-2\}$ then $\nu+1 \in \mathcal{N}_0$ and we arrive at $(\sigma\nu)^P = \sigma\overline{\nu+1}$.

If $\nu = \beta-1$, $\nu+1 = \beta \notin \mathcal{N}_0$. In this case the addition of $(1,0)^T$ produces a carry. By (4) this carry is described by $(\beta,0)^T = -M^2(1,0)^T - M(\alpha,0)^T$. Thus, using (5) we derive

$$\begin{aligned} \big((\sigma\overline{\beta-1})^P\big)_M &= M^{L+1}p + \sum_{j=1}^{L} M^j\sigma_j + (\beta,0)^T \\ &= M^{L+1}p + \sum_{j=1}^{L} M^j\sigma_j - M^2(1,0)^T - M(\alpha,0)^T \\ &= M\big((\sigma)_M - M(1,0)^T - (\alpha,0)^T\big) \\ &= M(\sigma^R)_M = (\sigma^R 0)_M \end{aligned}$$

and we are ready.

Since these rules are rather hard to survey, we visualize them with help of the transducer automaton depicted in Figure 1.

Remark 3.1. Note that for $\alpha = \beta$ or $\alpha = 0$ the automaton becomes simpler. Anyway, the following considerations apply also to these cases.

If we want to add 1, i.e. perform the operation P, we start at state P. Starting at one of the other states, will add the quantities related to it according to (5). The automaton reads the digits from right to left. The notation $j \mid k$ means, that the automaton reads j and writes out k, moving along the according edge. The states indicated by "•" in Figure 1 are called

Figure 1.

accepting states. If the automaton reaches one of the two accepting states, it copies all the remaining digits of the input string to the output string.

Now suppose, we want to add $(1,0)^T$ to the representation of a given element $z \in \mathbb{Z}^2$ with finite M-adic representation. To z there corresponds a string σ having only finitely many nonzero digits. Starting at P, we run through the automaton according to the digits of z until we have processed all its nonzero digits. If we find ourselves in one of the accepting states at this point, we are ready, since the remaining zero digits are just copied to the output string. Thus in this case the output string also has only finitely many nonzero digits. In other words, $z + 1$ has a finite M-adic

representation. Suppose now, that we find ourselves in one of the other states. Since the remaining digits of z are all equal to zero, we look at the walks of the automaton that are labelled only with zeros. Since each of these walks leads to one of the accepting states after at most three vertices, we conclude that the representation for $z+1$ is finite also in this case (in fact, the representation (3) of $z+1$ is at most three digits longer than the representation of z).

Since the same arguments apply to the addition of $(-1,0)^T$, we have proved that the addition of $(\pm 1,0)^T$ transforms finite representations to finite representations. Now note, that $-R$ performs the addition of $(-d,\varepsilon)$. In order to perform the addition of $(0,\varepsilon)^T$ we have to add $-R$ and then d times P. Since the addition of $-R$ as well as each addition of P transforms finite M-adic representations to finite M-adic representations, we conclude, that this is also true for the addition of $(0,\varepsilon)^T$. The same can be shown for the addition of $(0,-\varepsilon)^T$. Because zero has a finite representation and any $z\in\mathbb{Z}^2$ can be reached by a finite number of additions of $(\pm 1,0)$ and $(0,\pm 1)$, each $z\in\mathbb{Z}^2$ has a finite M-adic representation. Thus

$$\mathcal{P}=\{0\}$$

for the case treated in this section. Furthermore, it is obvious that $\Phi(0)=0$.

4. The case $0 < -\alpha \leq \beta$

The automaton in the last section had the advantage, that it transformed finite representations to finite representations for any starting state. We saw, that this property has the consequence, that each $z\in\mathbb{Z}^2$ is representable by means of a finite M-adic representation. Thus the related matrices M gave rise to canonical number systems in $\mathbb{Z}^2$. The key observation was, that each walk, labelled only with zeros, leads to one of the accepting states after at most three steps. In the case we want to consider now, things get a little bit more complicated. Because α is no longer an element of $\mathcal{N}_0$, the automaton gets a different shape. Let $\sigma^{\pm P}$ and $\sigma^{\pm R}$ be defined in the same way as in (5) and set

$$\left(\sigma^{\pm S}\right)_M=(\sigma)_M\mp M(1,0)^T\mp(\alpha+1,0)^T.$$

Figure 2.

Again using (4) one gets the counting automaton shown in Figure 2. Note that for $\beta = -\alpha$ the automaton becomes simpler. Anyway, the following considerations apply also to this case.

Since $\pm P$ and $\pm R$ occur again as states of the automaton it is possible to perform the addition of $(\pm 1, 0)$ and $(0, \pm 1)$ with it. Thus the M-adic representation of any $z \in \mathbb{Z}^2$ emerges from the representation 0 after finitely many applications of the automaton. We now characterize the possible periodicities in the representations of z. For abbrevation we set $\gamma := \beta + \alpha + 1$ and define the integer K by

$$K\gamma \leq \beta - 1 < (K+1)\gamma. \tag{6}$$

Let $0 \le l \le K$ and suppose, that z has the M-adic representation

$$z = ((\overline{l\gamma})^\infty a_L \dots a_0)_M.$$

If we put z into the automaton with an arbitrary starting state the following things can happen:

- The walk directed by the representation of z ends up in the accepting state. Then the output string is of the form $(\overline{l\gamma})^\infty a'_L \dots a'_0$.
- The walk ends up in the cycle at S (this is possible only for $l > 0$). Then the output string is of the form $(\overline{(l-1)\gamma})^\infty a'_L \dots a'_0$.
- The walk ends up in the cycle at $-S$ (this is possible only for $l < K$). Then the output string is of the form $(\overline{(l+1)\gamma})^\infty a'_L \dots a'_0$.

Note, that if we apply the automaton to any number z with periodicity $(\overline{l\gamma})^\infty$, the walk directed by z ends up in the accepting state or in one of the cycles at S and $-S$. Thus the other cycles occurring in the automaton do not play any role. This ensures, that the only possible periodicities are $(\overline{l\gamma})^\infty$ for $0 \le l \le K$. Hence, each z has a representation of the shape

$$z = \sum_{\ell=0}^{L} M^\ell a_\ell + M^{L+1} p_l$$

for some $l \in \{0, 1, \dots, K\}$ and

$$p_l = ((\overline{l\gamma})^\infty)_M \quad (0 \le l \le K).$$

Putting 0 at the starting state $-S$ into the automaton and iterating this l times, we get $p_l = M(l,0)^T + (l(\alpha+1),0)^T$ $(0 \le l \le K)$. Thus we have shown that

$$\mathcal{P} = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1-d \\ \varepsilon \end{pmatrix}, \dots, \begin{pmatrix} K(1-d) \\ K\varepsilon \end{pmatrix} \right\}$$

with K as in (6) in this case. Since the period length of p_l is 1 we have $\Phi(p_l) = p_l$ for $0 \le l \le K$.

5. The case $0 \le -\alpha < -\beta$

Again we can attach an automaton to this case. Let $\sigma^{\pm P}$, $\sigma^{\pm Q}$ and $\sigma^{\pm R}$ be as before. Obtaining the rules between the additions of the related

Figure 3.

quantities results in the automaton depicted in Figure 3. Note, that the automaton gets simpler for $\alpha = 0$. Nevertheless, the following considerations are true also in this case.

The same considerations as in the previous sections show, that the M-adic representation of each $z \in \mathbb{Z}^2$ can be obtained by applying the automaton to the representation of 0 with appropriate starting states. Thus we get any informations about the possible periodicities from the automaton. Suppose first, that

$$z = \left((0)^\infty a_L \dots a_0\right)_M. \tag{7}$$

Putting z in the automaton with arbitrary starting state, the following things can happen:

- The walk directed by the digits of z ends up in one of the accepting states. Then the output string has the form $(0)^\infty a'_L \dots a'_0$.
- The walk ends up in the cycle $-P \to R \to -P$. Then the resulting output string has the form

$$\left(\overline{(-\beta-1)}\,\overline{(-\alpha)}\right)^\infty a'_L \dots a'_0$$

or

$$\left(\overline{(-\alpha)}\,\overline{(-\beta-1)}\right)^\infty a''_L \dots a''_0.$$

Now, suppose that z has a representation of the form

$$\left(\overline{(-\beta-1)}\,\overline{(-\alpha)}\right)^\infty a'_L \dots a'_0. \tag{8}$$

Then we find the following possibilities:

- The walk directed by z ends up in the accepting state. Then the output string is of the same shape as the one in (8).
- The walk ends up in the cycle $P \to -R \to P$. Then the output string has the shape $(0)^\infty a'_L \dots a'_0$.

  If z has a representation of the shape

$$\left(\overline{(-\alpha)}\,\overline{(-\beta-1)}\right)^\infty a'_L \dots a'_0$$

the possible output strings can be determined in a similar way. Summing up we arrive at

$$\mathcal{P} = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \end{pmatrix}, \begin{pmatrix} d \\ -\varepsilon \end{pmatrix} \right\}$$

in this case. The behaviour of Φ on $\mathcal{P}$ follows easily from the shape of the occurring periodicities.

6. The case $0 < \alpha < -\beta$

As in the foregoing sections we attach an automaton to this case. It is depicted in Figure 4.

Figure 4.

In this case, things are similar to the case $0 < -\alpha \leq \beta$. Let $\gamma = -\beta - \alpha - 1$ and define K by

$$K\gamma \leq -\beta - 1 < (K+1)\gamma.$$

Again, the cycles at S and $-S$ transform a periodic element $(\overline{l\gamma})^\infty$ to $(\overline{(l+1)\gamma})^\infty$ and $(\overline{(l-1)\gamma})^\infty$, respectively. Note, that the cycles $P \to -R \to P$ and $-P \to R \to -P$ do not play a role in this case, since a representation with periodicity $(\overline{l\gamma})^\infty$ $(0 \leq l \leq K)$ can not end up in one of these cycles. Thus $(\overline{l\gamma})^\infty$ $(1 \leq l \leq K)$ are the only periodicities that

can occur and we arrive at

$$\mathcal{P} = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} d-1 \\ -\varepsilon \end{pmatrix}, \dots, \begin{pmatrix} K(d-1) \\ -K\varepsilon \end{pmatrix} \right\}.$$

Again it is easy to see that $\Phi(p) = p$ for each $p \in \mathcal{P}$.

7. The remaining cases

In this section we will deal with the cases

(i) $2 \le \beta < |\alpha|$,

(ii) $2 \le -\beta \le |\alpha|$.

The case $|\beta| = 1$ is trivial. It will turn out, that in these cases the corresponding matrix M has at least one eigenvalue, whose modulus is less than or equal to 1.

Let M be a matrix having eigenvalues, whose moduli are all greater than 1. In the introduction we remarked, that in this case the orbit of any $z \in \mathbb{Z}^2$ generated by Φ ends up in a set $\mathcal{P} \subset \{\|z\| \le C\}$ (C an absolute constant depending only on M). We will show, that such a constant C does not exist in the cases treated in this section. This will lead to the desired conclusion.

First we deal with Case (i). We will show, that to each N there exists a number z_N, whose orbit is contained in $K_N := \{x \in \mathbb{Z}^2 \mid \|x\| \ge N\}$. To this matter consider

$$\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} -\sigma_1 r_0 d + \sigma_2 s_0 \\ \sigma_1 r_0 \end{pmatrix} \quad (0 \le s_0 \le r_0), \tag{9}$$

for $\sigma_1, \sigma_2 \in \{-1, 1\}$. Applying Φ to this vector, we arrive at a vector $(x_1, y_1)^T$ with (note that $\alpha = -a - d$ and $\beta = ad \mp \varepsilon$)

$$x_1 = -dy_1 + \sigma_1 r_0$$

$$y_1 = \frac{x_0 - ay_0 - \delta}{-\beta} = \frac{\sigma_1 r_0 \alpha + \sigma_2 s_0 - \delta}{-\beta},$$

where $(\delta, 0)^T \in \mathcal{N}_0$ is selected suitably, according to the definition of Φ. Now set $\sigma_3 := \sigma_1 \operatorname{sign} \alpha$. Then we get

$$|y_1| = \left| \frac{|r_0|\,|\alpha| + \sigma_3(\sigma_2 s_0 - \delta)}{|\beta|} \right| \ge \left| \frac{|r_0|\,|\beta| + r_0 + \sigma_3(\sigma_2 s_0 - \delta)}{|\beta|} \right| \ge r_0.$$

These inequalities hold because, by the definition of Φ and by $s_0 \le r_0$ we have $|\sigma_3(\sigma_2 s_0 - \delta)| \le r_0$. Thus there are $\sigma_1', \sigma_2' \in \{-1, 1\}$ such that $y_1 = \sigma_1' r_1$ with $r_1 \ge r_0$ and $x_1 = -\sigma_1' d r_1 + \sigma_2' s_1$ with $s_1 := r_0$. Hence, we arrive at

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \begin{pmatrix} -\sigma_1' r_1 d + \sigma_2' s_1 \\ \sigma_1' r_1 \end{pmatrix} \qquad (0 \le s_1 \le r_1 \ge r_0). \tag{10}$$

Iterating this procedure, we conclude, that $r_0 = |y_0| \le |y_1| \le |y_2| \le \cdots$. Since r_0 can be selected arbitrary, we found elements of $\mathbb{Z}^2$, whose orbits are contained in K_N for each N. Thus in this case the related matrix M has at least one eigenvalue of modulus less than or equal to 1.

Case (ii) can be treated in a similar way. Let (x_0, y_0) be defined in the same way as in (9), but assume that $\sigma_2 := \sigma_1 \operatorname{sign} \alpha$. Defining x_1 and y_1 in the same way as in Case (i) we derive

$$\begin{aligned} r_1 := |y_1| &\ge \Big| \frac{r_0|\alpha| + s_0 - \sigma_1(\operatorname{sign}\alpha)\delta)}{|\beta|} \Big| \\ &\ge \Big| \frac{r_0|\beta| + s_0 - \sigma_1(\operatorname{sign}\alpha)\delta)}{|\beta|} \Big| \ge r_0 = |y_0| \end{aligned}$$

and $\operatorname{sign} y_1 = \sigma_1(\operatorname{sign}\alpha) =: \sigma_1'$. Setting $\sigma_2' := (\operatorname{sign}\alpha)\sigma_1'$ and $s_1 := r_0$ yields (10) and the existence of eigenvalues of modulus ≤ 1 now follows in the same way as in Case (i).

8. Connections to number systems in quadratic number fields

In this section we want to discuss certain connections between canonical number systems in $\mathbb{Z}^2$, and canonical number systems in number fields. Let n be a squarefree number and consider the quadratic number field $\mathbb{Q}(\sqrt{n})$. Let μ be an element of its ring of integers $\mathcal{O}$ and set $\mathcal{M}_0 := \{0, 1, \ldots, |N(\mu)| - 1\}$, where $N(\mu)$ denotes the norm of μ over $\mathbb{Q}$. The pair $(\mu, \mathcal{M}_0)$ is called a canonical number system in $\mathbb{Q}(\sqrt{n})$, if each $z \in \mathcal{O}$ has a unique representation of the shape

$$z = c_0 + c_1\mu + \cdots + c_H\mu^H$$

with $c_j \in \mathcal{M}$ $(0 \le j \le H)$ and $c_H \ne 0$ for $H \ne 0$. These number systems have been studied, for instance, in [7], [5], [6], [11]. In particular, in the first

three of these papers the bases of canonical number systems in quadratic fields where characterized. In this section we will give a short proof of these characterizations using Corollary 2.1.

It is easy to see, that μ can be a basis of a canonical number system only if $\{1, \mu\}$ is an integral basis of $\mathcal{O}$ (cf. KOVÁCS [10, Lemma 1]). Let now μ be such that $\{1, \mu\}$ forms an integral basis of $\mathcal{O}$, and let $m(x) = x^2 + \alpha x + \beta$ be the minimal polynomial of μ. We now want to characterize the numbers $\mu \in \mathcal{O}$ that give rise to a canonical number system $(\mu, \mathcal{M}_0)$. To this matter we define the mapping $\Psi : \mathbb{Q}(\sqrt{n}) \to \mathbb{R}^2$, $\xi_0 + \xi_1\mu \mapsto (\xi_0, \xi_1)$. Since μ is an integral basis, we have $\Psi(\mathcal{O}) = \mathbb{Z}^2$. Furthermore, $\Psi(\mu x) = M\Psi(x)$, with

$$M = \begin{pmatrix} 0 & -\beta \\ 1 & -\alpha \end{pmatrix}.$$

Since $\Psi(\mathcal{M}_0) = \mathcal{N}_0$, it is easy to see that μ is the basis of a canonical number system $(\mu, \mathcal{M}_0)$ if and only if M is the basis of the canonical number system $(M, \mathcal{N}_0)$. According to the different shape of the integral bases of quadratic number fields we have to distinguish two cases (cf. HARDY–WRIGHT [3]). Namely, $\{1, \mu\}$ is an integral basis of $\mathcal{O}$ iff

$$\mu = \mu_1 = r \pm \sqrt{n} \qquad \text{for } n \equiv 2, 3 \pmod 4,$$

$$\mu = \mu_2 = \frac{1}{2}(s \pm \sqrt{n}) \quad \text{for } n \equiv 1 \pmod 4 \text{ and } s \equiv 1 \pmod 2.$$

Since these numbers have the minimal polynomials $m_1(x) = x^2 - 2rx + (r^2 - n)$ and $m_2(x) = x^2 - sx + \frac{1}{4}(s^2 - n)$, respectively, the corresponding matrices are

$$M_1 = \begin{pmatrix} 0 & n - r^2 \\ 1 & 2r \end{pmatrix} \quad \text{and} \quad M_2 = \begin{pmatrix} 0 & \frac{1}{4}(n - s^2) \\ 1 & s \end{pmatrix}.$$

But by Corollary 2.1 these matrices give rise to a canonical number system in $\mathbb{Z}^2$ if and only if

$$-1 \le -2r \le r^2 - n \ge 2 \quad \text{and} \quad -1 \le s \le \frac{1}{4}(s^2 - n),$$

respectively. We have reproved the following result:

Theorem 8.1. *Let $\mathbb{Q}(\sqrt{n})$, with n squarefree and not equal to 1, be a quadratic number field. μ is the basis of the canonical number system $(\mu, \mathcal{M}_0)$ if and only if one of the following conditions holds.*

- *$n > 0$ and $n \equiv 2, 3 \pmod 4$ (cf. [5]):*

$$\mu = r \pm \sqrt{n} \quad \text{with} \quad 6 \leq -2r \leq r^2 - n \geq 2.$$

- *$n > 0$ and $n \equiv 1 \pmod 4$ (cf. [5]):*

$$\mu = \frac{1}{2}(s \pm \sqrt{n}) \quad \text{with} \quad 5 \leq -s \leq \frac{1}{4}(s^2 - n) \geq 2 \quad (s \equiv 1 \pmod 2).$$

- *$n = -1$ (cf. [7]):*

$$\mu = r \pm i \quad \text{with} \quad 2 \leq -2r \leq r^2 + 1 \geq 2.$$

- *$n < -1$ and $n \equiv 2, 3 \pmod 4$ (cf. [6]):*

$$\mu = r \pm \sqrt{n} \quad \text{with} \quad 0 \leq -2r \leq r^2 - n \geq 2.$$

- *$n < -1$ and $n \equiv 1 \pmod 4$ (cf. [6]):*

$$\mu = \frac{1}{2}(s \pm \sqrt{n}) \quad \text{with} \quad -1 \leq -s \leq \frac{1}{4}(s^2 - n) \geq 2 \quad (s \equiv 1 \pmod 2).$$

Remark 2.1. In the case $n > 0$ and $n \equiv 2, 3 \pmod 4$ of the above theorem Corollary 2.1 yields only $-1 \leq -2r \leq r^2 - n \geq 2$. But together with the conditions posed upon n these inequalities imply $3 \leq -r$. Thus in this case $-1 \leq -2r$ can be replaced by $6 \leq -2r$. In the remaining cases the lower bounds for $-2r$ and $-s$ can be established in the same way.

References

[1] S. Eilenberg, Automata, Languages and Machines, *Academic Press*, *New York*, 1974.

[2] P. J. Grabner, P. Krischenhofer and H. Prodinger, The sum-of-digits-function for complex bases, *J. London Math. Soc.* **57** (1) (1998), 20–40.

[3] G. H. Hardy and E. M. Wright, An introduction to the Theory of Numbers, 2nd edition, *Clarendon Press*, *Oxford*, 1960.

[4] I. Kátai, Number systems and fractal geometry, *Pécs, Hungary*, 1995, 1–39.

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

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

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

[8] A. Kovács, On computation of attractors for invertible expanding linear operators in Z^n, *(preprint)*.

[9] A. Kovács, On expansions of Gaussian with non-negative digits, *Math. Pannonica* **10** (2) (1999), 177–191.

[10] B. Kovács, Canonical numbers systems in algebraic numbers fields, *Acta Math. Hungar.* **37** (1981), 405–407.

[11] B. Kovács and A. Pethő, Number systems in integral domains, especially in orders of algebraic number fields, *Acta Sci. Math. (Szeged)* **55** (1991), 286–299.

[12] W. Kuich and A. Salomaa, Semirings, Automata, Languages, *Springer*, *Berlin*, 1986.

[13] J. M. Tuswaldner, Elementary properties of the sum of digits function in quadratic number fields, Applications of Fibonacci Numbers (G.E. Bergum et al., eds.), volume 7, *Kluwer Academic Publisher*, 1998.

JÖRG M. THUSWALDNER
INSTITUT FÜR MATHEMATIK UND ANGEWANDTE GEOMETRIE
ABTEILUNG FÜR MATHEMATIK UND STATISTIK
MONTANUNIVERSITÄT LEOBEN
FRANZ–JOSEF–STRASSE 18
A–8700 LEOBEN
AUSTRIA

(Received June 30, 1999; revised May 2, 2000)