On number system constructions

László Germán* and Attila Kovács†

Abstract

In this paper we investigate various number system constructions. After summarizing the earlier results we prove that for a given lattice Λ and expansive matrix $M : \Lambda \to \Lambda$ if $\rho(M^{-1}) < 1/2$ then there always exists a suitable digit set D for which (Λ, M, D) is a number system. Here ρ means the spectral radius of M^{-1}. We shall prove further that if the polynomial $f(x) = c_0 + c_1 x + \cdots + c_k x^k \in \mathbb{Z}[x]$, $c_k = 1$ satisfies the condition $|c_0| > 2\sum_{i=1}^{k} |c_i|$ then there is a suitable digit set D for which $(\mathbb{Z}^k, M, D)$ is a number system, where M is the companion matrix of $f(x)$.

1 Statements and earlier results

A *lattice* in $\mathbb{R}^k$ is the set of all integer combinations of k linearly independent vectors. It can be viewed either as a set of points in the k-dimensional Euclidean space, as a $\mathbb{Z}$-module, or as a finitely generated free Abelian group. Let Λ be a lattice, $M : \Lambda \to \Lambda$ be a group endomorphism such that $\det(M) \neq 0$ and let D be a finite subset of Λ containing 0.

Definition The triple (Λ, M, D) is called a *number system* (or having the unique representation property) if every element x of Λ has a unique, finite representation of the form $x = \sum_{i=0}^{l} M^i d_i$, where $d_i \in D$ and $l \in \mathbb{N}$. The operator M is called the *base* or *radix*, D is the *digit set*.

Both Λ and $M\Lambda$ are Abelian groups under addition, the order of the factor group $\Lambda/M\Lambda$ is $t = |\det(M)|$. If two elements are in the same coset

*The research was supported by the Number Theory Research Group of the Hungarian Academy of Sciences

†The research was supported by OTKA-T043657 and Bolyai Stipendium

of this group then we say that they are congruent modulo M. In [21] the following theorem was stated:

Theorem 1 If (Λ, M, D) is a number system then
a) D must be a full residue system modulo M,
b) M must be expansive,
c) $\det(I - M) \neq \pm 1$.

In this paper we always assume that these conditions hold, in which case we call (Λ, M, D) a *radix system*. Every number system is a radix system, but the converse is not true.

The radix system (Λ, M, D) can be used to represent all the lattice points in Λ even if it is not a number system. Clearly, for each $\gamma \in \Lambda$ there exists a unique $d_j \in D$ such that $\gamma - d_j \in M\Lambda$. Let $\gamma_1 = M^{-1}(\gamma - d_j)$ and let us define the function $\Phi : \Lambda \to \Lambda$ by $\Phi(\gamma) = \gamma_1$. Let Φ^l denote the l-fold iterate of Φ, $\Phi^0(\gamma) = \gamma_0$. The sequence of integer vectors $\Phi^j(z_0) = z_j$ $(j = 0, 1, 2, \ldots)$ is called the *orbit* of z_0 generated by Φ. Since the spectral radius $\rho(M^{-1}) < 1$ therefore there exists a norm on $\mathbb{R}^k$ such that for the corresponding operator norm

$$\|M^{-1}\| = \sup_{\|x\| \leq 1} \|M^{-1}x\|$$

the inequality $\|M^{-1}\| < 1$ holds. The algorithmic construction of an appropriate vector norm was presented in [19]. Throughout this work $\|\,.\,\|$ denotes this vector and the induced operator norm. Let furthermore $K = \max_{d \in D} \|d\|$, $r = \|M^{-1}\|$, $L = Kr/(1 - r)$. I t is easy to see, that if $\|z\| \leq L$ then $\|\Phi(z)\| \leq L$, if $\|z\| > L$ then $\|\Phi(z)\| < \|z\|$. Since the inequality $\|x\| \leq L$ holds only for finitely many lattice points therefore the path $z, \Phi(z), \Phi^2(z), \ldots$ is ultimately periodic for all $z \in \Lambda$. The vector $\pi \in \Lambda$ is called *periodic* if there exist a $j \in \mathbb{N}$ such that $\Phi^j(\pi) = \pi$. Let $\mathcal{P}$ denote the set of all periodic elements. The function Φ defines a *discrete dynamic* on Λ in the following way: let $\mathcal{G}(\mathcal{P})$ be the directed graph defined on the set $\mathcal{P}$ by drawing an edge from $\pi \in \mathcal{P}$ to $\Phi(\pi)$. Then $\mathcal{G}(\mathcal{P})$ is a disjoint union of directed cycles, where loops are allowed. We say that $\mathcal{G}(\mathcal{P})$ is the *attractor set* of Λ generated by Φ. Observe that (Λ, M, D) is a number system if and only if $\mathcal{G}(\mathcal{P}) = \{0 \to 0\}$.

There are three types of problems in the mainstream of the number system research: decision, classification and construction. Decision means that for a given radix system (Λ, M, D) decide whether it is a number system. It has theoretic and algorithmic aspects, we refer only to [6, 14, 19, 21, 8, 34].

Classification means that for a given radix system (Λ, M, D) characterize the number, location and structure of the periodic elements. Some results in dimension two can be found in [9, 22, 23, 33]. In this paper we focus on construction problems: for a given lattice Λ and operator M satisfying criteria b) and c) in Theorem 1 is there any suitable digit set D for which (Λ, M, D) is a number system? If yes, how many and how to construct them? For a given radix system (Λ, M, D) some results are available:

Theorem 2 (Vince [34]) For a given $k \times k$ operator M if all its singular values are greater then $3\sqrt{k}$ then there exists a digit set D for which (Λ, M, D) is a number system. In dimensions one and two the bound $3\sqrt{k}$ can be improved to 2.

The digit set is $D = \Lambda \cap MV$, where V is the Voronoi domain of the cubic lattice (the closure of V is the unit cube centered at the origin).

Theorem 3 (A. Kovács [21]) For a given $k \times k$ operator M if

$$\|M^{-1}\|_2 \leq 1/(1+\sqrt{k}),$$

then there exists a digit set D for which (Λ, M, D) is a number system. Here $\|.\|_2$ is the operator norm induced by the Euclidean vector norm.

We note that if $\|M^{-1}\|_2 \leq 1/(1+\sqrt{k})$ then $\|M\|_2 \geq 1+\sqrt{k}$ but the converse is not necessary true. The digit set is by selecting a complete residue system around the origin keeping the norm of the elements minimal. Observe that the digit set D is not necessary unique. In this paper we shall prove the following:

Theorem 4 For a given matrix M if $\rho(M^{-1}) < 1/2$ then there exists a digit set D for which (Λ, M, D) is a number system.

Matrix transformations $M_1 : \Lambda \to \Lambda$ and $M_2 : \Gamma \to \Gamma$ of lattices Λ and Γ are *equivalent* (or similar) if there exists an invertible matrix Q such that $M_2 Q = Q M_1$ and $\Gamma = Q\Lambda$. It is easy to see that the equivalence preserves the number system property, i.e, if M_1 and M_2 are equivalent via the matrix Q and (Λ, M, D) is a number system then $(Q\Lambda, M_2, QD)$ is a number system as well. Hence, there is no loss of generality in assuming that M is an integral matrix acting on the lattice $\mathbb{Z}^k$. Searching for number systems in $\mathbb{Z}^k$ has a natural computational advantage, since the minimal and characteristic polynomial of M are also integral. Moreover, equivalence means a simple basis transformation, therefore there exist equivalent matrices in several canonical forms. The Frobenius normal form of a square $k \times k$

matrix M has the structure $F = \mathrm{diag}(C_1, \ldots, C_r)$, where C_i's are companion matrices associated with polynomials $p_1, \ldots, p_r$, where p_i is a factor of the characteristic polynomial of M with the property $p_i \mid p_{i+1}$ $(i = 1, \ldots, r-1)$. The Frobenius normal form defined in this way is unique and every matrix can be transformed by an equivalence transformation to its Frobenius normal form. We note that transforming M to its Frobenius canonical form there is no need to extend the field of its coefficients.

If the minimal polynomial is identical to the characteristic polynomial, the Frobenius normal form is the companion matrix of the characteristic polynomial. This case is extremely important due to the following construction. Consider a polynomial $f(x) = c_0 + c_1 x + \cdots + c_n x^k \in \mathbb{Z}[x]$, $c_k = 1$. Let (f) be the ideal generated by f, let Λ_f be the quotient ring $\mathbb{Z}[x]/(f)$ and let $\alpha = x + (f)$. Then, Λ_f can be realized as a free Abelian group or as a $\mathbb{Z}$-module with basis $(1, \alpha, \alpha^2, \ldots, \alpha^{k-1})$ and Λ_f is isomorphic to $\mathbb{Z}^k$. Hence, the companion matrix of $f(x)$ serves as the radix and acts on the cubic lattice $\mathbb{Z}^k$. Addition and multiplication of lattice points is just addition and multiplication in the ring Λ_f. We remark that using *canonical* digit sets the decision problem in this structure are in the forefront of the research [1, 3, 4, 7, 25, 30]. A set of integer vectors is called j-canonical with respect to the matrix M if all the elements have the form νe_j, where e_j denotes the j-th unit vector, $\nu = 0, 1, \ldots, |\det(M)| - 1$ (see [19]). 1-canonical complete residue systems are called canonical digit sets with respect to M.

In the special case when $f(x)$ is irreducible over $\mathbb{Z}$ then Λ_f is isomorphic to $\mathbb{Z}[\alpha]$, where α is any root of $f(x)$ in an appropriate extension field of the rationals. This case has been extensively studied, we refer only to [6, 11, 15, 16, 17, 18]

Let us denote the k-dimensional general linear group over $\mathbb{Z}$ by $GL(k, \mathbb{Z})$ and its subgroup, for which the determinant of the elements are ± 1 by $SL(k, \mathbb{Z})$. Let $A, B \in GL(k, \mathbb{Z})$. We say that A and B are *integrally similar* (or $\mathbb{Z}$-similar) if there exist a $T \in SL(k, \mathbb{Z})$ such that $AT = TB$. Clearly, if A and B are integrally similar then they are similar, but the converse is not true.

Example 1 The matrices

$$\begin{pmatrix} 0 & 1 \\ -6 & -1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} -2 & -4 \\ 2 & 1 \end{pmatrix}$$

have the same characteristic polynomial $x^2 + x + 6$, they are similar, but they are not $\mathbb{Z}$-similar.

Let $S(k, A, \mathbb{Q})$ and $S(k, A, \mathbb{Z})$ be the set of all $k \times k$ integer matrices which are similar to A over $\mathbb{Q}$ and over $\mathbb{Z}$, respectively (in other words the elements of the similarity matrices have rational and rational integral elements, respectively). Then $S(k, A, \mathbb{Q})$ is the union of integral similarity classes. Moreover, it is the union of finitely many integral similarity classes if and only if A is diagonalizable over $\mathbb{C}$ (see e.g. in [26]). This is the case if, for example, the minimal polynomial of A is irreducible over $\mathbb{Z}$.

Theorem 5 (Latimer–MacDuffee–Taussky [28, 32]) Let $f(x) \in \mathbb{Z}[x]$ be an irreducible monic polynomial of degree k. Then there is a bijection between the integral similarity classes of $k \times k$ integer matrices with characteristic polynomial $f(x)$ and the ideal classes in $\mathbb{Z}[\theta]$, where $f(\theta) = 0$, $\theta \in \mathbb{C}$.

It is also known that if A is an integer $k \times k$ matrix then every matrix $B \in S(k, A, \mathbb{Q})$ is integrally similar to A if and only if the minimal polynomial $m(x)$ of A has the form $p_1(x)p_2(x)\cdots p_r(x)$ (some $r \geq 1$) of distinct monic irreducible polynomials $p_1(x), \ldots, p_r(x)$ such that i) the ideal class number of $\mathbb{Q}(\theta_i)$ is 1 for $i = 1, 2, \ldots, r$, where θ_i is a root of the equation $p_i(x) = 0$, and ii) the resultant $\mathrm{res}(p_i, p_j) = \pm 1$ for all i, j with $1 \leq i \neq j \leq r$.

Summarizing the above reasoning, if for a given $k \times k$ integer matrix M we are able to find a suitable digit set D for which $(\mathbb{Z}^k, M, D)$ is a number system then we have a construction for all operators in $S(k, M, \mathbb{Z})$. If M is diagonizable over $\mathbb{C}$ then there are finitely many integral similarity classes and if the characteristic polynomial of M is irreducible then Theorem 5 shows also their cardinality.

In the same way, the concept of $\mathbb{Z}$-similarity plays an important role if one wants to show that for a given operator M there does not exist any appropriate digit set D for which $(\mathbb{Z}^k, M, D)$ is a number system.

Theorem 6 (Barbé, von Haeseler [5]) Let M be an expanding operator in $\mathbb{Z}^k$ with $|\det(M)| = 2$. There is a digit set D for which $(\mathbb{Z}^k, M, D)$ is a number system if and only if M is $\mathbb{Z}$-similar to the companion matrix C_M of the characteristic polynomial of M and $(\mathbb{Z}^k, C_M, \{0, e_1\})$ is a number system.

Since there exist irreducible, expansive polynomials $f(x)$ for which $f(0) = 2$ and the number of the ideal classes in $\mathbb{Z}[\theta]$ is greater than one ($f(\theta) = 0$), therefore there exist integral similarity classes in which the digit set construction is not possible. Such polynomials are $x^4 + x^2 + 2, x^6 - x^4 - x^2 + 2, x^6 + x^3 + x^2 - x + 2, x^6 + x^4 + 2, x^6 + x^5 + x^4 + 2x^3 + x^2 + x + 2$. Lagarias and Wang reports [27] that there does not exist any other polynomials having

the above property with degree less than or equal to 6.

Example 2 The matrix

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

is expansive, its characteristic polynomial is $f(x) = x^4 + x^2 + 2$, $D = \{0, e_1\}$ is a complete residue system modulo the companion matrix C_M of $f(x)$ and $(\mathbb{Z}^4, C_M, D)$ is a number system [20], but it is not possible to give any digit set D', for which $(\mathbb{Z}^4, M, D')$ would be a number system, since M is not $\mathbb{Z}$-similar to C_M. We note that for the matrix M the sets $\{0, e_2\}$ and $\{0, e_3\}$ are complete residue systems modulo M but $\{0, e_1\}$ is not.

The strength of Theorem 4 is that satisfying the condition $\rho(M^{-1}) < 1/2$ the digit set construction is always possible independently of the dimension and the basis of the space. To be more precise, if $(\mathbb{Z}^k, M, D)$ is a number system having $\rho(M^{-1}) < 1/2$ and $T \in S(k, M, \mathbb{Q})$ then $\rho(T^{-1}) < 1/2$ and $(\mathbb{Z}^k, T, D)$ is a number system as well since M and T have the same spectrum. If we restrict our attention to one $\mathbb{Z}$-similarity class we have the following result:

Theorem 7 (B. Kovács [24] and Pethő [29]) Let the polynomial $c_0 + c_1 x + \cdots + c_k x^k \in \mathbb{Z}[x]$, $(c_k = 1)$ be given and let us denote its companion matrix by M. If the conditions b) and c) in Theorem 1 hold, furthermore if

$$2 \leq c_0 \geq c_1 \geq \cdots \geq c_{k-1} \geq 1$$

then $(\mathbb{Z}^k, M, D)$ is a number system with the canonical digit set D.

We shall prove the following theorem.

Theorem 8 Let the polynomial $f(x) = c_0 + c_1 x + \cdots + c_k x^k \in \mathbb{Z}[x]$, $(c_k = 1)$ be given and let us denote its companion matrix by M. If the condition

$$|c_0| > 2 \sum_{i=1}^{k} |c_i| \tag{1}$$

holds then there exists a suitable digit set D for which $(\mathbb{Z}^k, M, D)$ is a number system.

First observe that (1) – which is called the weak dominant condition – implies the fulfillment of condition b) in Theorem 1. Otherwise for the $|\lambda| \leq 1$ root of $f(x)$ we have $|c_0| = |\sum_{i=1}^{k} c_i \lambda^i| \leq \sum_{i=1}^{k} |c_i| < |c_0|/2$, which is a contradiction. On the other hand the weak dominant condition implies that $\sum_{i=0}^{k} c_i \neq \pm 1$ which means exactly the condition c) in Theorem 1. Taking extra conditions the weak dominant condition can be made stronger:

Theorem 9 (Akiyama, Rao [2]) Let the polynomial $f(x) = c_0 + c_1 x + \cdots + c_k x^k \in \mathbb{Z}[x]$, $c_k = 1$ be given and let us denote its companion matrix by M. If the conditions

$$\begin{aligned} &a) \qquad |c_0| > \textstyle\sum_{i=1}^{k} |c_i|, \\ &b) \qquad \textstyle\sum_{i=1}^{k} c_i \geq 0, \\ &c) \quad c_i \geq 0, \ i = 2, 3, \ldots, k-1 \end{aligned} \tag{2}$$

hold then $(\mathbb{Z}^k, M, D)$ is a number system with the canonical digit set D. The strong dominant condition (2) can be replaced by $|c_0| \geq \sum_{i=1}^{k} |c_i|$ if either $p_1 < 0$ or $p_i > 0$ for all $i = 1, 2, \ldots, k-1$.

What is the situation in algebraic number fields? Let ϑ be a fixed algebraic number of degree k, its conjugates $\vartheta^{(1)} = \vartheta, \vartheta^{(2)}, \ldots, \vartheta^{(k)}$. Let $\Lambda^{(j)}$ be the set of integers in $\mathbb{Q}(\vartheta^{(j)})$, $\Lambda^{(1)} = \Lambda$. Let us fix an integer basis $\omega_1, \ldots, \omega_k$ in $\mathbb{Q}(\vartheta)$. Let furhermore $\Delta_j = |\omega_1^{(j)}| + \cdots + |\omega_k^{(j)}|$ where $\omega_k^{(j)}$ is the conjugate of ω_k belonging to $\mathbb{Q}(\vartheta^{(j)})$.

Theorem 10 (Kátai [12]) Assume that $\alpha \in \Lambda$ satisfies the conditions $|\alpha^{(j)}| > \max(2, 2\Delta_j)$, $(j = 1, \ldots, k)$. Then there exists a suitable digit set D for which (Λ, α, D) is a number system.

Let $K_j(D) = \max\{|\zeta^{(j)}| : \zeta \in D\}$. H. Brunotte made the observation (personal communication with I. Kátai) that if D is a complete residue system (mod α) such that $|\alpha^{(j)}| > \max\{2, 2\sqrt{K_j(D)}\}$ $(j = 1, \ldots, k)$ then there exists a complete residue system $\overline{D}$ such that $(\Lambda, \alpha, \overline{D})$ is a number system, and $K_j(\overline{D}) \leq K_j(D)$ $(j = 1, \ldots, k)$.

Theorem 11 (Kátai [13]) Let Λ be the set of algebraic integers in an imaginary quadratic field and let $\alpha \in \Lambda$. Then there exists a suitable digit set D by which (Λ, α, D) is a number system if and only if $|\alpha| > 1$, $|1-\alpha| > 1$ hold.

In other words Kátai was able to prove that in imaginary quadratic fields for the number system construction the conditions in Theorem 1 are also sufficient. His digit set construction based on the conjugates of the basic

lattice. He studied the construction of G. Steidl, who investigated the same for the ring of Gaussian integers [31].

In real quadratic fields the situation is more complicated. The following result is available [10]:

Theorem 12 (Farkas, A. Kovács) Let Λ be the set of algebraic integers in the real quadratic field $\mathbb{Q}(\sqrt{2})$ and let $0 \neq \alpha \in \Lambda$. If $\alpha, 1 \pm \alpha$ are not units and $|\alpha|, |\overline{\alpha}| > \sqrt{2}$ then there exists a suitable digit set D by which (Λ, α, D) is a number system.

The digit set construction is similar to Kátai's construction but it contains some improvement. This improvement is based on the observation that using Kátai's digit set construction the structure of the periodic elements is simple.

2 Proof of Theorem 4

Let the radix system (Λ, M, D) be given. Since $\rho(M^{-1}) < 1/2$ therefore there exists a vector norm for which the corresponding operator norm $\|M^{-1}\| < 1/2$ holds. Let furthermore

$$D = \{d_i \in \mathrm{coset}_i(M) | \text{ any } f \in \Lambda, f \equiv d_i \text{ implies } \|d_i\| \leq \|f\|, i = 1, \ldots, t\},$$

where $t = |\det(M)|$. Indirectly, let us suppose that there are periodic elements in (Λ, M, D) different from zero. Let $\pi \in \mathcal{P}$ such that for all $\pi' \in \mathcal{P}$ the inequality $\|\pi\| \geq \|\pi'\|$ holds. Consider the expansion of $\pi_0 = \pi_n = \pi$ by

$$\pi_i = d_i + M\pi_{i+1} \quad (i = 0, \ldots, n-1),$$

where n is the length of the expansion, $d_i \in D$, $d_i \equiv \pi_i \pmod{M}$. Clearly, by the construction of the digit set D

$$\|d_i\| \leq \|\pi_i\| \leq \|\pi\| \tag{3}$$

hold for all $i = 0, \ldots, n-1$. Let furthermore $A = M^{-1}$. Then,

$$A^n\pi = A^n d_0 + A^{n-1}d_1 + \cdots + Ad_{n-1} + \pi,$$

hence

$$(A^n - I)\pi = \sum_{k=1}^{n} A^k d_{n-k}. \tag{4}$$

Observe that the matrix $(A^n - I)$ is nonsingular for any positive integer n, othervise 1 would be an eigenvalue of A^n, so A would have an eigenvalue of modulus 1. Recall that the operator norm satisfies the following properties:

a) $\|B^m\| \leq \|B\|^m$ for any positive integer m and square matrix B.
b) If $\|B\| < 1$ then $(I - B)^{-1}$ exists,
c) $\|(I - B)^{-1}\| \leq 1/(1 - \|B\|)$ and
d) $I + B + B^2 + \cdots + B^m = (I - B)^{-1}(I - B^{m+1})$.

In virtue of (3) and (4) and the properties above we have that

$$\begin{aligned} \|\pi\| &\leq \|A\|\|\pi\| \, \frac{1 - \|A\|^n}{1 - \|A\|} \, \|(A^n - I)^{-1}\| \\ &\leq \|A\|\|\pi\| \, \frac{1 - \|A\|^n}{1 - \|A\|} \, \frac{1}{1 - \|A^n\|} \\ &\leq \|\pi\| \, \frac{\|A\|}{1 - \|A\|} \, < \|\pi\|, \end{aligned}$$

which is a contradiction.

S. Akiyama kindly pointed out that the necessary condition $\rho(M^{-1})$ can only be replaced to $\|M\| > 2$ if the condition number $\mathrm{cond}(M) = \|M\| \cdot \|M^{-1}\| = 1$. In algebraic number fields using the notations of Theorem 10 we have the following corollary:

Corollary Let Λ be the set of algebraic integers in $\mathbb{Q}(\sigma)$, where σ is an algebraic number of degree k. If $\alpha \in \Lambda$ satisfies the conditions $|\alpha^{(j)}| > 2$ $(j = 1, \ldots, k)$ then there exists a digit set D for which (Λ, α, D) is a number system.

3 Proof of Theorem 8

Let the polynomial $f(x) = c_0 + c_1 x + \cdots + c_k x^k \in \mathbb{Z}[x]$, $c_k = 1$ be given and let its companion matrix

$$M = \begin{pmatrix} 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & 0 & \cdots & -c_2 \\ & & \ddots & 0 & \\ 0 & 0 & \cdots & 1 & -c_{k-1} \end{pmatrix}.$$

Suppose that the condition (1) holds. We prove that there exists a suitable digit set D for which $(\mathbb{Z}^k, M, D)$ is a number system.

Let the matrix $Q \in SL(k, \mathbb{Z})$ be as follows:

$$Q = \begin{pmatrix} c_k & c_{k-1} & \cdots & c_2 & c_1 \\ 0 & c_k & c_{k-1} & \cdots & c_2 \\ 0 & 0 & c_k & \cdots & c_3 \\ & & & \ddots & \\ 0 & 0 & 0 & \cdots & c_k \end{pmatrix}.$$

Clearly, the matrix

$$M_1 = \begin{pmatrix} -c_{k-1} & -c_{k-2} & \cdots & -c_1 & -c_0 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ & & \ddots & & \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

is integrally similar to M via the matrix Q. Hence, it is enough to find a digit set D_1 for which $(\mathbb{Z}^k, M_1, D_1)$ is a number system. Why do we use this basis? Because the function Φ, which describes the dynamic of the lattice points, becomes very simple. To be more precise, since

$$M_1^{-1} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ & & & \ddots & 0 \\ 0 & 0 & 0 & \cdots & 1 \\ -1/c_0 & -c_{k-1}/c_0 & -c_{k-2}/c_0 & \cdots & -c_1/c_0 \end{pmatrix}$$

therefore the function Φ acts as a kind of a left shift map: if $y = [y_1, y_2, \ldots, y_k]^T \in \mathbb{Z}^k$, $d = [d_1, d_2, \ldots, d_k]^T \in D_1$, $y \equiv d \pmod{M_1}$ and $z = [z_1, z_2, \ldots, z_k]^T = [y_1 - d_1, y_2 - d_2, \ldots, y_k - d_k]^T$ then $\Phi(z) = [z_2, z_3, \ldots, z_k, z_{k+1}]^T$, where

$$z_{k+1} = -\frac{1}{c_0} \sum_{j=1}^{k} z_{k-j+1} c_j. \tag{5}$$

Clearly, if the digit set has a special (e.g. canonical) form, then the function Φ is even simpler. This basis was first suggested by H. Brunotte examining

number systems with canonical digit sets, and later extensively used by S. Akiyama, H. Rao, A. Pethő, and J.M. Thuswaldner.

Let us consider the symmetric digit set

$$D_1 = \{\nu e_1 \mid \nu = -\lfloor (|c_0|-1)/2 \rfloor, \ldots, \lfloor |c_0|/2 \rfloor\}. \tag{6}$$

Then, by (5) and (6) for any $[z_i, z_{i+1}, \ldots, z_{i+k-1}]^T \in \mathbb{Z}^k$ we have that

$$z_i c_k + z_{i+1} c_{k-1} + \cdots + z_{i+k-1} c_1 + z_{i+k} c_0 \in D_1, \tag{7}$$

where z_{i+k} is defined by (5). Let us suppose that $(\mathbb{Z}^k, M_1, D_1)$ is not a number system. Then there is a period different from $0 \to 0$. Let $\eta = \max\{\ z_i \mid [z_j, z_{j+1}, \ldots, z_{j+k-1}]^T \in \mathcal{P}, j \le i \le j+k-1\}$. It follows from the structure of the digit set that $\eta > 0$. Let us choose an i in (7) such that $z_{i+k} = \eta$.

Let c_0 be even. By using (7) if $\operatorname{sgn}(c_0) > 0$ then

$$c_0\big(\eta - \frac{1}{2}\big) \le \eta\big(\sum_{j=1}^{k} |c_i|\big),$$

if $\operatorname{sgn}(c_0) < 0$ then

$$-\big(\frac{|c_0|}{2} - 1 - \eta|c_0|\big) = |c_0|\big(\eta - \frac{1}{2}\big) + 1 \le \eta\big(\sum_{j=1}^{k} |c_i|\big).$$

Let c_0 be odd. Again, using (7) if $\operatorname{sgn}(c_0) > 0$ then

$$-\frac{c_0 - 1}{2} + c_0\eta = c_0\big(\eta - \frac{1}{2}\big) + \frac{1}{2} \le \eta\big(\sum_{j=1}^{k} |c_i|\big),$$

if $\operatorname{sgn}(c_0) < 0$ then

$$-\big(\frac{|c_0| - 1}{2} - \eta|c_0|\big) = |c_0|\big(\eta - \frac{1}{2}\big) + \frac{1}{2} \le \eta\big(\sum_{j=1}^{k} |c_i|\big).$$

Thus, in any case, we have

$$|c_0|\big(\eta - \frac{1}{2}\big) \le \eta\big(\sum_{j=1}^{k} |c_i|\big). \tag{8}$$

Reordering inequality (8) we got that

$$\eta\big(|c_0| - \sum_{j=1}^{k} |c_j|\big) \leq \frac{|c_0|}{2} \ ,$$

by which

$$\eta \leq \frac{|c_0|}{2(|c_0| - \sum_{j=1}^{k} |c_j|)} \ .$$

Hence, if $|c_0| > 2\sum_{j=1}^{k} |c_j|$ then $\eta < 1$ which is a contradiction. The proof is finished.

4 Summary

This paper contains some new results regarding general number system constructions. To have a better view we summarized also the earlier results. Comparing our theorems with each other one can see that in some cases, e.g. when for the characteristic polynomial of the radix M the inequality $c_0 > 2^k \sum_{i=1}^{k} |c_i|$ holds, our both constructions are applicable. On the other hand, for the case $f(x) = x^3 - 2x^2 - 7x + 15$ only Theorem 4, while for the cases $f(x) = x^k - \sum_{i=1}^{k-1} x^i + 2k + 1$, $k = 3, 4, \ldots$ only Theorem 8 can be applied. But we must stress the difference. While Theorem 4 works for all operators M for which $\|M^{-1}\| < 1/2$, Theorem 8 works only for one integral similarity class.

Furthermore, Example 2 shows that the conditions in Theorem 1 are not sufficient for the number system constructions. Regarding one $\mathbb{Z}$-similarity class in dimension two – via the characteristic polynomial of M – we believe that the necessary conditions in Theorem 1 are also sufficient. This points out the direction of our further research.

The authors are grateful to Professor I. Kátai, who kindly presented the results of his personal communication with H. Brunotte, and to S. Akiyama, who found a bad argumentation at the proof of Theorem 4 in the original manuscript.

References

[1] Akiyama, S., Pethő, A., *On canonical number systems*, Theor. Comp. Sci., **270**, (2002), 921–933.

[2] Akiyama S., Rao, H., *New criteria for canonical number systems*, Acta Arithm. **111**, (2004), 5–25.

[3] Akiyama, S., Brunotte, H., Pethő, A., *Cubic CNS polynomials, notes on a conjecture of W.J. Gilbert*, J. Math. Anal. and Appl. **281**, (2003), 402–415.

[4] Akiyama, S., Borbély, T., Brunotte, H., Pethő, A., *On a generalization of the radix representation – a survey*, High Primes and Misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, Fields Inst. Commun. **41**, (2004), 19–27.

[5] Barbé, A., von Haeseler, F., *Binary number systems for* $\mathbb{Z}^k$., Internal report 04-90 ESAT-SISTA, K. U. Leuven, (2004), to appear in J. of Number Theory.

[6] Brunotte, H., *On trinomial bases of radix representation of algebraic integers*, Acta Sci. Math. (Szeged), **67**, (2001), 407–413.

[7] Brunotte, H., *Characterization of CNS trinomials*, Acta Sci. Math. (Szeged) **68**, (2002), 673–679.

[8] Burcsi, P., Kovács, A., *An algorithm checking a necessary condition of number system constructions*, Annales Univ. Sci. Budapest, Sect. Comp. **40**, to appear.

[9] Farkas, G., *Location and number of periodic elements in* $\mathbb{Q}(\sqrt{2})$, Annales Univ. Sci. Budapest, Sect. Comp. **20**, (2001), 133–146.

[10] Farkas, G., Kovács, A., *Digital expansion in* $\mathbb{Q}(\sqrt(2))$, Annales Univ. Sci. Budapest, Sect. Comp. **22**, (2003), 83–94.

[11] Gilbert, W. J., *Radix representation of quadratic fields*, J. Math. Anal. Appl. **83**, (1991), 264–274.

[12] Kátai, I., *Construction of number systems in algebraic number fields*, Annales Univ. Sci. Budapest, Sect. Comp. **18**, (1999), 103–107.

[13] Kátai, I., *Number systems in imaginary quadratic fields*, Annales Univ. Sci. Budapest, Sect. Comp. **18**, (1994), 91–103.

[14] Kátai, I., *Generalized number systems in Euclidean spaces*, Math. and Comp. Modelling **38**/7-9, (2003), 883–892.

[15] Kátai, I., Kovács, B., *Kanonische Zahlensysteme bei reelen quadratischen algebraischen Zahlen*, Acta Sci. Math. **42**, (1980), 99–107.

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

[17] Kátai, I., Környei, I., *On number systems in algebraic number fields*, Publ. Math. Debrecen, **41**/(3-4), (1992), 289–294.

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

[19] Kovács, A., *On computation of attractors for invertible expanding linear operators in* $\mathbb{Z}^k$, Publ. Math. Debrecen **56**/(1-2), (2000), 97–120.

[20] Kovács, A., *Generalized binary number systems*, Annales Univ. Sci. Budapest, Sect. Comp. **20**, (2001), 195–206.

[21] Kovács, A., *Number expansion in lattices*, Math. and Comp. Modelling, **38**, (2003), 909–915.

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

[23] Kovács, A., *Canonical expansions of integers in imaginary quadratic fields*, Acta Math. Hungar. **93**/4, (2001), 347–357.

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

[25] Körmendi, S., *Canonical number systems in* $\mathbb{Q}(\sqrt[3]{2})$, Acta Sci. Math. (Szeged) **50**, (1986), 351–357.

[26] Laffey, T.J., *Lectures on integer matrices*, hermite.cii.fc.ul.pt/meetings/im_1997/lectures.pdf, 1–38.

[27] Lagarias, J.C., Wang, Y., *Corrigendum/addendum: "Haar bases for* $L^2(\mathbb{R}^n)$ *and algebraic number theory" [J. Number Theory, 57/1 1996.]* J. of Number Theory, **76**/2, (1999), 330–336.

[28] Latimer, C.G., MacDuffee, C.C., *A correspondence between classes of ideals and classes of matrices*, Annals Math., **34**, (1933), 313–316.

[29] Pethő, A., *On a polynomial transformation and its application to the construction of a public key cryptosystem*, Computational Number Theory, Proc., Walter de Gruyter Publ. Co. (1991), 31–44.

[30] Scheicher, K., Thuswaldner, J.M., *On the characterization of canonical number systems*, Osaka J. Math. **41**, (2004), 327–351.

[31] Steidl, G., *On symmetric representation of Gaussian integers*, BIT, **29**, (1989), 563–571.

[32] Taussky, O., *On matrix classes corresponding to an ideal and its inverse*, Illinois J. Math., **1**, (1957), 108–113.

[33] Thuswaldner, J.M., *Attractors for invertible expanding linear operators and number systems in* $\mathbb{Z}^2$, Publ. Math. Debrecen, **58**/3, (2001), 423–440.

[34] Vince, A., *Replicating tessellations*, SIAM J. Discrete Math., **6**, 191–215, (1995).

László Germán and Attila Kovács
Department of Computer Algebra
Eötvös Loránd University
1117 Budapest
Pázmány P. sétány I/C.
Hungary
{german,attila}@compalg.inf.elte.hu