Rational matrix digit systems

Jonas Jankauskas & Jörg M. Thuswaldner

Published online: 07 May 2022.

Submit your article to this journal ⇗

Article views: 326

View related articles ⇗

View Crossmark data ⇗

Taylor & Francis
Taylor & Francis Group

RESEARCH ARTICLE

OPEN ACCESS Check for updates

Rational matrix digit systems

Jonas Jankauskas [a,b] and Jörg M. Thuswaldner [b]

[a]Faculty of Mathematics and Informatics, Institute of Mathematics, Vilnius University, Vilnius, LT, Lithuania;
[b]Mathematik und Statistik, Montanuniversität Leoben, Leoben, Austria

ABSTRACT
Let A be a $d \times d$ matrix with rational entries which has no eigenvalue $\lambda \in \mathbb{C}$ of absolute value $|\lambda| < 1$ and let $\mathbb{Z}^d[A]$ be the smallest nontrivial A-invariant $\mathbb{Z}$-module. We lay down a theoretical framework for the construction of *digit systems* $(A, \mathcal{D})$, where $\mathcal{D} \subset \mathbb{Z}^d[A]$ finite, that admit finite expansions of the form

$$\mathbf{x} = \mathbf{d}_0 + A\mathbf{d}_1 + \cdots + A^{\ell-1}\mathbf{d}_{\ell-1} \quad (\ell \in \mathbb{N}, \ \mathbf{d}_0, \dots, \mathbf{d}_{\ell-1} \in \mathcal{D})$$

for every element $\mathbf{x} \in \mathbb{Z}^d[A]$. We put special emphasis on the explicit computation of *small digit sets* $\mathcal{D}$ that admit this property for a given matrix A, using techniques from matrix theory, convex geometry, and the Smith Normal Form. Moreover, we provide a new proof of general results on this *finiteness property* and recover analogous finiteness results for digit systems in number fields a unified way.

1. Introduction and main results

Let $A \in \mathbb{Q}^{d \times d}$ be an invertible matrix with rational entries. It is easy to see that the smallest nontrivial A-invariant $\mathbb{Z}$-module containing $\mathbb{Z}^d$ is given by the set $\mathbb{Z}^d[A]$ of vectors $\mathbf{x} \in \mathbb{Q}^d$ that can be written as

$$\mathbf{x} = \mathbf{x}_0 + A\mathbf{x}_1 + \cdots + A^{k-1}\mathbf{x}_{k-1}, \tag{1}$$

where $k \in \mathbb{N}$ and $\mathbf{x}_0, \dots, \mathbf{x}_{k-1} \in \mathbb{Z}^d$, i.e.

$$\mathbb{Z}^d[A] := \bigcup_{k=1}^{\infty} \left(\mathbb{Z}^d + A\mathbb{Z}^d + \cdots + A^{k-1}\mathbb{Z}^d \right).$$

Thus $\mathbb{Z}^d[A]$ is the set of all vectors that can be expanded in terms of positive powers of A with integer vectors as coefficients. Motivated by the existing vast theory and many practical applications of number systems, it is natural to ask the following question. Is there a

---

finite set $\mathcal{D} \subset \mathbb{Z}^d[A]$, such that every vector $\mathbf{x} \in \mathbb{Z}^d[A]$ has an expansion of the form

$$\mathbf{x} = \mathbf{d}_0 + A\mathbf{d}_1 + \cdots + A^{\ell-1}\mathbf{d}_{\ell-1}, \tag{2}$$

where $\ell \in \mathbb{N}$ and $\mathbf{d}_0, \ldots, \mathbf{d}_{\ell-1} \in \mathcal{D}$. To put this in another way: can one find a finite digit set $\mathcal{D} \subset \mathbb{Z}^d[A]$ such that

$$\mathbb{Z}^d[A] = \mathcal{D}[A], \tag{3}$$

where

$$\mathcal{D}[A] := \bigcup_{\ell=1}^{\infty} \left(\mathcal{D} + A\mathcal{D} + \cdots + A^{\ell-1}\mathcal{D} \right). \tag{4}$$

A lot of work related to this problem has been done in the context of number systems in number fields (cf. [1–4]), polynomial rings (see [5–9] and the survey [10]), lattices (see e.g. [11,12]), and rational bases (cf. [13]). Moreover, it is intimately related to the study of self-affine tiles (see [14–16]) and the so-called *height reducing property* (cf. [17–20]). As we will see below, the problem of the existence of such a set $\mathcal{D}$ can be restated in terms of a so-called *finiteness* property of general *digit systems*. It is the aim of the present paper to construct sets $\mathcal{D}$ that satisfy (3). Here we strive for very general theory on the one side while paying attention to algorithmic issues on the other side.

The pair $(A, \mathcal{D})$ is called *a matrix digit system* or simply *a digit system*. The matrix A is then called *the base* of this digit system and the elements of $\mathcal{D}$ are called its *digits*. We say that $(A, \mathcal{D})$ has *the finiteness property* in $\mathbb{Z}^d[A]$ (or Property (F) for short), if every vector $\mathbf{x} \in \mathbb{Z}^d[A]$ has a finite expansion of the form (2), i.e. if (3) holds. It is easily seen that the requirement that $\mathcal{D}$ contains a complete system of residue class representatives of $\mathbb{Z}^d[A]/A\mathbb{Z}^d[A]$ is a necessary, but in general not sufficient, condition for $(A, \mathcal{D})$ to have the finiteness property. One also says that $(A, \mathcal{D})$ possesses *the uniqueness property*, or Property (U), if two different finite radix expressions in (4) always yield different vectors of $\mathbb{Z}^d[A]$. For the number systems that already possess Property (F), a necessary and sufficient condition to have Property (U) is $|\mathcal{D}| = |\mathbb{Z}^d[A]/A\mathbb{Z}^d[A]|$.

Digit systems that possess both properties (F) and (U) are called *standard*. Frequently, one additional requirement is imposed on standard digit systems: the zero vector $\mathbf{0}_d$ must belong to $\mathcal{D}$ (which enables natural positional arithmetics). Standard digit systems in $\mathbb{Z}^d$ in integer matrix bases have been studied extensively in the literature.

Clearly, matrix digit systems are modeled after the usual number systems in $\mathbb{Z}$ (see [21] for the negative case). Concerning rational matrices, in dimension $d = 1$ one recovers the base $A = \frac{p}{q} \in \mathbb{Q}$, with $p \in \mathbb{Z}, q \in \mathbb{N}, \gcd(p, q) = 1$. In this case, $\mathbb{Z}[\frac{p}{q}] = \mathbb{Z}[\frac{1}{q}]$ is the set of all rational fractions with denominators that divide some power of q, and the submodule $\frac{p}{q}\mathbb{Z}[\frac{p}{q}] = p\mathbb{Z}[\frac{1}{q}]$ represents fractions with numerators divisible by p; so that $\mathcal{D}\{0, 1, \ldots, p - 1\}$ is a complete set of coset representatives of $\mathbb{Z}[\frac{p}{q}]$ modulo $\frac{p}{q}\mathbb{Z}^d[\frac{p}{q}]$. The pair $(\frac{p}{q}, \mathcal{D})$ then is a rational matrix number system in $\mathbb{Z}[\frac{1}{q}]$. Such systems have been studied in [13].

If $A \in \mathbb{Z}^{d \times d}$ is an integer matrix, the module $\mathbb{Z}^d[A]$ reduces to the lattice $\mathbb{Z}^d$. Digit systems in lattices with expanding base matrices were introduced by Vince [12,22,23] and studied extensively in connection with fractal tilings. Indeed, a tiling theory for the standard digit systems with expanding integral base matrices was worked out by Gröchenig and

Haas [24], and Lagarias and Wang [15,25,26]. A corresponding theory for tilings produced by rational algebraic number base systems was developed by Steiner and Thuswaldner [16].

When trying to study the finiteness property of digit systems $(A, \mathcal{D})$ for large classes of base matrices A and digits sets $\mathcal{D}$, new challenges of geometrical and arithmetical nature arise. First, if A is allowed to have eigenvalues $\lambda \in \mathbb{C}$ of absolute value $|\lambda| = 1$, then A^{-1} is no longer a contracting linear mapping. If such λ are not roots of unity, then there exist points $\mathbf{x} \in \mathbb{R}^n$ with infinite, non-periodic orbits $(A^{-n}\mathbf{x})_{n=1}^{\infty}$. Even worse, if A has a Jordan block of order ≥ 2 corresponding to the eigenvalue λ on the complex unit circle in its Jordan decomposition, then $A^{-n}\mathbf{x}$ can diverge to ∞, as it is easily seen from the simple 2×2 example $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ by taking $\mathbf{x} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. These situations require careful control of vectors in certain directions when multiplication by A^{-1} is performed. Aside from the issues of geometric nature, arithmetics in $\mathbb{Z}^d[A]$ is also more difficult when A has rational entries: even the computation of the residue class group for the expansions in base A is no longer trivial and causes significant problems.

As a result of the aforementioned challenges, properties (F) and (U) no longer go well together: we typically need *more* than $[\mathbb{Z}^d[A] : A\mathbb{Z}^d[A]]$ digits to address all possible issues. In this situation, one is forced to make a choice, which property, (F) or (U), must be sacrificed to reinforce another. We make the choice in favour of Property (F): it is often important to have multiple digital expressions for every $\mathbf{x} \in \mathbb{Z}^d[A]$, rather than leave some $\mathbf{x}$ with no such expression whatsoever while trying to preserve (U).

The aim of the present paper is to 'build up' digit sets with Property (F) in an explicit and algorithmic way. We reveal the dynamical systems underlying the digit systems $(A, \mathcal{D})$ and interpret the finiteness property in terms of their attractors. The properties of these dynamical systems are investigated in Section 2. After that, we decompose a given rational matrix A into 'generalized Jordan blocks', called *the hypercompanion matrices*, build digits systems for each such block separately, and then patch them together (see Section 4). In these building blocks, *generalized rotation matrices* play a crucial role in order to treat the eigenvalues of modulus 1. These matrices and their digit sets are thoroughly studied in Section 3. The decomposition of A has the advantage that we get much better hold on the size and structure of the digit sets than in previous papers (like [18,20]). This can be used to give new proofs of the main results of [18,20] which can easily be turned in algorithms in order to construct convenient digit sets for any given matrix A (see Section 5). The algorithmic nature of our approach is exploited in the discussion of various examples. In particular, in Section 6 we use the Smith Normal Form in order to get results on the size of certain residue class rings that are relevant for the construction of digit sets with finiteness property. In Section 7 these results are combined with our general theory in order to construct examples of small digit sets for matrices with particularly interesting properties.

Summing up, in the present paper we lay down a comprehensive (and much simplified) theory for the finiteness property in digit systems with rational matrix bases. Our construction of the digit sets is based on the theory of matrices, convex geometry and Smith Normal Form representations of lattice bases; these proofs are independent from the previous constructions of [18,20], that were based on digit systems in number fields. In fact, we show that our finiteness result on matrix-base digit systems implies the according result on digit systems in number fields, thereby demonstrating that these two finiteness results are of the same strength.

2. Arithmetics of matrix digit systems

In this section, we discuss discrete dynamical systems associated that represent 'the remainder division' in the module $\mathbb{Z}^d[A]$. If these dynamical systems have finite attractors, this enables us to construct a digit system $(A, \mathcal{D})$ with Property (F). We also consider certain restrictions of these dynamical mappings to the integer lattice $\mathbb{Z}^d$ and their subsequent extensions to the whole module $\mathbb{Z}^d[A]$ which appear to be very useful in the practical computations.

2.1. Classical remainder division

Let $A \in \mathbb{Q}^{d \times d}$ be given and let $\mathcal{D} \subset \mathbb{Z}^d[A]$ be a digit set. We take a closer look at the arithmetics of $\mathbb{Z}^d[A]$. Associated with the digit system $(A, \mathcal{D})$ is the procedure of division with remainder in $\mathbb{Z}^d[A]$. As usual, a mapping $\mathbf{d} : \mathbb{Z}^d[A] \to \mathcal{D}$ is called *a digit function* if $\mathbf{d}(\mathbf{x}) \equiv \mathbf{x} \pmod{A\mathbb{Z}^d[A]}$, i.e. if $\mathbf{d}(\mathbf{x}) - \mathbf{x} \in A\mathbb{Z}^d[A]$. Thus, using $\mathbf{d}$ we can define the dynamical system

$$\Phi : \mathbb{Z}^d[A] \to \mathbb{Z}^d[A], \quad \Phi(\mathbf{x}) := A^{-1}(\mathbf{x} - \mathbf{d}(\mathbf{x})). \tag{5}$$

As we allow $A \in \mathbb{Q}^{d \times d}$ to have non-integral coefficients, our first step is to show that division with remainder works essentially in the same way, as in the classical case. In this context, the following definition is of importance.

Definition 2.1 (Attractor of Φ): A set $\mathcal{A} \subset \mathbb{Z}^d[A]$ with the properties that:

  (i) $\Phi(\mathcal{A}) \subset \mathcal{A}$,
 (ii) for every $\mathbf{x} \in \mathbb{Z}^d[A]$, there exists $n = n(\mathbf{x}) \in \mathbb{N}$, such that $\Phi^n(\mathbf{x}) \in \mathcal{A}$
(iii) no proper subset of $\mathcal{A}$ satisfies properties $(i - ii)$

is called *an attractor* of Φ and will be denoted $\mathcal{A}_\Phi$.

   It should be noted that multiple variants of Definition 2.1 are used in the literature (cf. [27, Section 1.13]). In general, the attractor might not exist, or be infinite. However, if the attractor $\mathcal{A}_\Phi$ exits, Definition 2.1 implies it is unique. If the attractor $\mathcal{A}_\Phi$ of Φ is finite, then one can construct a digit system $(A, \mathcal{D})$ that satisfies Property (F).

Proposition 2.2: *Suppose that the attractor $\mathcal{A}_\Phi$ of the quotient function Φ is a finite set. Then, for every $\mathbf{x} \in \mathbb{Z}^d[A]$, the orbit $(\Phi^n(\mathbf{x}))_{n=1}^\infty$ is eventually periodic, with only a finite number of possible periods. In particular, the digit system $(A, \mathcal{D} \cup \mathcal{A}_\Phi)$ has the finiteness property.*

Proof of Proposition 2.2: By Definition 2.1, for each $\mathbf{x} \in \mathbb{Z}^d[A]$, there is $n_0(\mathbf{x}) \in \mathbb{N}$, such that $\mathbf{x} = \boldsymbol{\varepsilon}_0 + A\boldsymbol{\varepsilon}_1 + \cdots + A^{n-1}\boldsymbol{\varepsilon}_{n-1} + A^n \Phi^n(\mathbf{x})$, with $\boldsymbol{\varepsilon}_1, \ldots, \boldsymbol{\varepsilon}_{n-1} \in \mathcal{D}$ and $\Phi^n(\mathbf{x}) \in \mathcal{A}_\Phi$ holds for each $n \geq n_0(\mathbf{x})$. Thus $\mathbb{Z}^d[A] = (\mathcal{D} \cup \mathcal{A}_\Phi)[A]$ and, hence, $(A, \mathcal{D} \cup \mathcal{A}_\Phi)$ has the finiteness property. As the value of $\Phi^{n+1}(\mathbf{x})$ depends only on $\Phi^n(\mathbf{x})$, the statement on the ultimate periodicity and periods follows from the finiteness of $\mathcal{A}_\Phi$. ∎

Suppose that $(A, \mathcal{D})$ is a digit system. Then we can use the dynamical system Φ in order to generate expansions of $x \in \mathbb{Z}^d[A]$. Indeed, by the definition of Φ there are uniquely defined elements $\mathbf{d}_0, \mathbf{d}_1, \ldots \in \mathcal{D}$ satisfying

$$\mathbf{x} = \boldsymbol{\varepsilon}_0 + A\boldsymbol{\varepsilon}_1 + \cdots + A^{n-1}\boldsymbol{\varepsilon}_{n-1} + A^n \Phi^n(\mathbf{x}) \quad (n \in \mathbb{N}).$$

If the attractor of Φ is $\{\mathbf{0}_d\}$ this implies that for each $\mathbf{x} \in \mathbb{Z}^d[A]$ there is $n \in \mathbb{N}$ such that

$$\mathbf{x} = \boldsymbol{\varepsilon}_0 + A\boldsymbol{\varepsilon}_1 + \cdots + A^{n-1}\boldsymbol{\varepsilon}_{n-1}. \tag{6}$$

In this case we say that (6) is *a finite expansion of* $\mathbf{x}$ *generated by* Φ.

For number systems in $\mathbb{Z}^d$ with integer matrices as base it is well-known that the attractor of a number system $(A, \mathcal{D})$ with an expanding matrix $A \in \mathbb{Z}^{d \times d}$ and a digit set $\mathcal{D} \subset \mathbb{Z}^d$ is a finite set (see e.g. [12, Section 5]). Our next goal is to show that the same result holds in our more general context. Let $A \in \mathbb{Q}^{d \times d}$ be an invertible rational matrix. As the entries of the vectors in $\mathbb{Z}^d[A]$ may have arbitrarily large denominators, $\mathbb{Z}^d[A]$, in general, does not possess any finite $\mathbb{Z}$-basis. This entails that our proofs become a bit more complicated than in the integer case. In particular we will frequently need the following sequence of rational lattices. Starting with the lattice $\mathbb{Z}^d$ and repeatedly multiplying its vectors by A, $k = 1, 2, \ldots$ times, one defines

$$\mathbb{Z}_k^d[A] := \mathbb{Z}^d + A\mathbb{Z}^d + \cdots + A^{k-1}\mathbb{Z}^d.$$

Since $\mathbb{Z}_k^d[A] \subset \mathbb{Z}_{k+1}^d[A]$, these rational lattices form a nested chain.

We need two preparatory lemmas.

Lemma 2.3: *If $A \in \mathbb{Q}^{d \times d}$ is invertible, then $\mathbb{Z}^d[A]/A\mathbb{Z}^d[A]$ is a finite Abelian group. Moreover, there exists $k := k_A \in \mathbb{N}$, such that*

$$\mathbb{Z}^d \cap A\mathbb{Z}^d[A] = \mathbb{Z}^d \cap A\mathbb{Z}_k^d[A], \quad and \quad \mathbb{Z}^d[A]/A\mathbb{Z}^d[A] = \mathbb{Z}^d / \left(\mathbb{Z}^d \cap A\mathbb{Z}_k^d[A] \right). \tag{7}$$

In particular, representatives for $\mathbb{Z}^d[A]/A\mathbb{Z}^d[A]$ can be chosen from $\mathbb{Z}^d$.

Proof of Lemma 2.3: As $\mathbb{Z}^d[A] = \mathbb{Z}^d + A\mathbb{Z}^d[A]$, the Second Isomorphism Theorem for modules yields

$$\mathbb{Z}^d[A]/A\mathbb{Z}^d[A] = \left(\mathbb{Z}^d + A\mathbb{Z}^d[A] \right)/A\mathbb{Z}^d[A] \simeq \mathbb{Z}^d / \left(\mathbb{Z}^d \cap A\mathbb{Z}^d[A] \right). \tag{8}$$

Since A is invertible, $\mathbb{Z}^d \cap A\mathbb{Z}^d[A]$ is a d-dimensional additive subgroup of $\mathbb{Z}^d$. Hence, it is a lattice and has a finite index in $\mathbb{Z}^d$. Therefore, $\mathbb{Z}^d[A]/A\mathbb{Z}^d[A]$ is a finite Abelian group. Now, consider the nested chain of lattices

$$\mathbb{Z}^d \cap A\mathbb{Z}_1^d[A] \subset \cdots \subset \mathbb{Z}^d \cap A\mathbb{Z}_j^d[A] \subset \mathbb{Z}^d \cap A\mathbb{Z}_{j+1}^d[A] \subset \cdots \subset \mathbb{Z}^d \cap A\mathbb{Z}^d[A] \subset \mathbb{Z}^d.$$

Since the index $\mathbb{Z}^d \cap A\mathbb{Z}_j^d[A]$ in $\mathbb{Z}^d$ cannot decrease indefinitely, the chain must eventually stabilize, hence, there is a constant $k = k_A$ such that $\mathbb{Z}^d \cap A\mathbb{Z}_{j+1}^d[A] = \mathbb{Z}^d \cap A\mathbb{Z}_j^d[A]$ holds for $j \geq k$. This yields the first identity in (7). Thus in order to establish the second identity it is sufficient to prove equality (instead of isomorphy) in (8). From

$\mathbb{Z}^d[A] = \mathbb{Z}^d + A\mathbb{Z}^d[A]$ and $\mathbb{Z}^d = \mathcal{R} + \mathbb{Z}^d \cap A\mathbb{Z}^d[A]$, where $\mathcal{R}$ is a complete set of coset representatives of $\mathbb{Z}^d/(\mathbb{Z}^d \cap A\mathbb{Z}^d[A])$, it follows that $\mathbb{Z}^d[A] = \mathcal{R} + A\mathbb{Z}^d[A]$. Thus, $\mathcal{R}$ contains all coset representatives of $\mathbb{Z}^d[A]/A\mathbb{Z}^d[A]$. $|\mathcal{R}| = |\mathbb{Z}^d[A]/A\mathbb{Z}^d[A]|$ by (8), these representatives also must be different modulo $A\mathbb{Z}^d[A]$. Therefore, the isomorphism '$\simeq$' symbol in (8) can indeed be replaced with '$=$'. ∎

Lemma 2.4: *There exists $l := l(A, \mathcal{D}) \in \mathbb{N}$, such that, for every $\mathbf{x} \in \mathbb{Z}^d[A]$ and sufficiently large $n \geq n_{\mathbf{x}}$, $\Phi^n(\mathbf{x}) \in \mathbb{Z}_l^d[A]$.*

Proof of Lemma 2.4: According to Lemma 2.3, there exists $k = k_A$, such that $\mathbb{Z}^d \cap A\mathbb{Z}^d[A] = \mathbb{Z}^d \cap A\mathbb{Z}_k^d[A]$. Choose the smallest integer $l \geq k_A$, such that $\mathcal{D} \subset \mathbb{Z}_l^d[A]$. Assume that $\mathbf{x} = \mathbf{x}_0 + A\mathbf{x}_1 + \cdots + A^{m-1}\mathbf{x}_{m-1} \in \mathbb{Z}_m^d[A]$, with $\mathbf{x}_0, \ldots, \mathbf{x}_{m-1} \in \mathbb{Z}^d$. Because $\mathbf{d}(\mathbf{x}) \in \mathcal{D}$ there are $\boldsymbol{\varepsilon}_0, \ldots, \boldsymbol{\varepsilon}_{l-1} \in \mathbb{Z}^d$ such that $\mathbf{d}(\mathbf{x}) = \boldsymbol{\varepsilon}_0 + A\boldsymbol{\varepsilon}_1 + \cdots + A^{l-1}\boldsymbol{\varepsilon}_{l-1}$. Therefore we have $\mathbf{x} - \mathbf{d}(\mathbf{x}) \in (\mathbf{x}_0 - \boldsymbol{\varepsilon}_0 + A\mathbb{Z}_i^d[A]) \cap A\mathbb{Z}^d[A]$, with $i = \max\{l-1, m-1\}$ from which we conclude that $\mathbf{x}_0 - \boldsymbol{\varepsilon}_0 \in \mathbb{Z}^d \cap A\mathbb{Z}^d[A] = \mathbb{Z}^d \cap A\mathbb{Z}_k^d[A] \subset A\mathbb{Z}_l^d[A]$. This implies that $\Phi(\mathbf{x}) \in \mathbb{Z}_j^d[A]$, where $j = \max\{l, m-1\}$. By iteration, eventually $\Phi^n(\mathbf{x}) \in \mathbb{Z}_l^d[A]$. ∎

We are now in a position to prove that expanding matrices lead to finite attractors.

Proposition 2.5: *If $A \in \mathbb{Q}^{d \times d}$ is expanding and $\mathcal{D}$ is a digit set, then the quotient function Φ of $(A, \mathcal{D})$ has a finite attractor $\mathcal{A}_\Phi \subset \mathbb{Z}^d[A]$. Consequently, the digit system $(A, \mathcal{D} \cup \mathcal{A}_\Phi)$ has the finiteness property in $\mathbb{Z}^d[A]$.*

Proof of Proposition 2.5: By Lemma 2.4, there exists $l \in \mathbb{N}$, such that $\Phi^n(\mathbf{x}) \in \mathbb{Z}_l^d[A]$ for every $n \geq n_1(\mathbf{x})$. From $\mathbf{x} = \boldsymbol{\varepsilon}_0 + A\boldsymbol{\varepsilon}_1 + \cdots + A^{n-1}\boldsymbol{\varepsilon}_{n-1} + A^n\Phi^n(\mathbf{x}), \boldsymbol{\varepsilon}_0, \ldots, \boldsymbol{\varepsilon}_{n-1} \in \mathcal{D}$, one deduces $\Phi^n(\mathbf{x}) = A^{-n}\mathbf{x} - A^{-1}\boldsymbol{\varepsilon}_{n-1} - A^{-2}\boldsymbol{\varepsilon}_{n-2} - \cdots - A^{-n}\boldsymbol{\varepsilon}_0$. Since A is expanding, the operator norm series $\sum_{n=0}^\infty \left\| A^{-n} \right\|_\infty < C_A < \infty$. It means $\|\Phi^n(\mathbf{x})\| \leq C_A \max\{\|\boldsymbol{\varepsilon}\| : \boldsymbol{\varepsilon} \in \mathcal{D}\}$. As $\mathbb{Z}_l^d[A]$ is a lattice, $\mathbb{Z}_l^d[A] \cap B(\mathbf{0}_d, r)$ must be finite. Therefore, Φ has a finite attractor $\mathcal{A}_\Phi \subset \mathbb{Z}_l^d[A] \cap B(\mathbf{0}_d, r)$. It remains to apply Proposition 2.2. ∎

2.2. Auxiliary lattice and division with remainder with respect to it

Let $(A, \mathcal{D})$ be a digit system. A necessary condition for $(A, \mathcal{D})$ to have the finiteness property is the fact that $\mathcal{D}$ contains a complete set of residue class representatives of the group $\mathbb{Z}^d[A]/A\mathbb{Z}^d[A]$. Thus it is desirable to shed some light on this group. While in the case of an integer matrix A we have $|\det A| = |\mathbb{Z}^d[A]/A\mathbb{Z}^d[A]|$, for a rational matrix A the group $\mathbb{Z}^d[A]/A\mathbb{Z}^d[A]$ and its size is not so easy to. In order to get information on $\mathbb{Z}^d[A]/A\mathbb{Z}^d[A]$, one must obtain the base matrix $L \in \mathbb{Q}^{d \times d}$ for the rational lattice $A\mathbb{Z}_k^d[A] = L\mathbb{Z}^d$ with $k = k_A$ described in Lemma 2.3. Unfortunately, no satisfactory representation theory for the nested lattices $\mathbb{Z}_k^d[A]$ in $\mathbb{Z}^d[A]$ is yet available for the determination of the required index $k = k_A$ in Lemma 2.3 where the nested chain of lattices stabilizes. Another drawback is that, in general, $\mathbb{Z}^d$ is not be preserved when doing division with remainders modulo $A\mathbb{Z}^d[A]$. In order to deal with these issues, in this subsection, we introduce an auxiliary lattice and a division with the remainder with respect to this lattice, that eventually can be

used for the computation of digital expansions in $\mathbb{Z}^d[A]$. Indeed, it turns out that complete sets of residue classes are easy to deal with in this auxiliary lattice. Moreover, they contain complete sets of residue classes of $\mathbb{Z}^d[A]/A\mathbb{Z}^d[A]$.

Definition 2.6: The lattice $\mathbb{Z}^d \cap A\mathbb{Z}^d$ will be referred as *the auxiliary lattice* of the matrix $A \in \mathbb{Q}^{d \times d}$.

If A is invertible, $\mathbb{Z}^d \cap A\mathbb{Z}^d$ is a full-rank sublattice of $\mathbb{Z}^d$, hence, in this case $\mathbb{Z}^d/(\mathbb{Z}^d \cap A\mathbb{Z}^d)$ is a finite group. Furthermore, we have the following result.

Lemma 2.7: Let $A \in \mathbb{Q}^{d \times d}$ be given. Then $\mathbb{Z}^d[A]/A\mathbb{Z}^d[A]$ is isomorphic to a subgroup of $\mathbb{Z}^d/(\mathbb{Z}^d \cap A\mathbb{Z}^d)$.

Proof of Lemma 2.7: By applying the 3rd Isomorphism theorem to nested modules $\mathbb{Z}^d \cap A\mathbb{Z}^d \subset \mathbb{Z}^d \cap A\mathbb{Z}^d[A] \subset \mathbb{Z}^d$, we obtain

$$\frac{\mathbb{Z}^d/\left(\mathbb{Z}^d \cap A\mathbb{Z}^d\right)}{\left(\mathbb{Z}^d \cap A\mathbb{Z}^d[A]\right)/\left(\mathbb{Z}^d \cap A\mathbb{Z}^d\right)} \simeq \frac{\mathbb{Z}^d}{\mathbb{Z}^d \cap A\mathbb{Z}^d[A]} \simeq \mathbb{Z}^d[A]/A\mathbb{Z}^d[A],$$

where the last isomorphism comes from Lemma 2.3. ∎

An advantage in using the auxiliary lattice $\mathbb{Z}^d \cap A\mathbb{Z}^d$ for arithmetics comes from the fact that its base matrix can be computed directly from the base matrix A using its Smith Normal Form, see Section 6. We will now develop a special kind of division with the remainder based on this auxiliary lattice and its residue group. The first step of this construction is to restrict our division to $\mathbb{Z}^d$ according to the following definition.

Definition 2.8: Let $\mathcal{D} \subset \mathbb{Z}^d$ be a finite digit set that contains a complete set of coset representatives of $\mathbb{Z}^d/(\mathbb{Z}^d \cap A\mathbb{Z}^d)$. *A restricted digit function* is a mapping $\mathbf{d}_r : \mathbb{Z}^d \to \mathcal{D}$ with the homomorphism property $\mathbf{d}_r(\mathbf{x}) \equiv \mathbf{x} \pmod{\mathbb{Z}^d \cap A\mathbb{Z}^d}$. To this restricted setting we associate the dynamical system $\Phi_r : \mathbb{Z}^d \to \mathbb{Z}^d$ given by $\Phi_r(\mathbf{x}) := A^{-1}(\mathbf{x} - \mathbf{d}_r(\mathbf{x}))$.

The attractor $\mathcal{A}_{\Phi_r} \subset \mathbb{Z}^d$ of the dynamical system Φ_r is defined analogously to the attractor of Φ.

In the second step of our construction we extend this restricted division procedure to the full module $\mathbb{Z}^d[A]$. For any $\mathbf{x} \in \mathbb{Z}^d[A]$, there always exists a smallest $k \in \mathbb{N}$, such that $\mathbf{x} \in \mathbb{Z}_k^d[A]$. That is, there exists a shortest expansion of the form

$$\mathbf{x} = \mathbf{x}_0 + A\mathbf{x}_1 + \cdots + A^{k-1}\mathbf{x}_{k-1}, \tag{9}$$

with $\mathbf{x}_0, \ldots, \mathbf{x}_{k-1} \in \mathbb{Z}^d$. In general, such expressions (even the shortest ones) are not unique: for instance, one can modify $\mathbf{x}_0$ by adding any element $\mathbf{v} \in \mathbb{Z}^d \cap A\mathbb{Z}^d$ to it, and then subtracting $A^{-1}\mathbf{v}$ from $\mathbf{x}_1$. However, we re-impose the uniqueness by introducing arbitrary (lexicographic) order $\mathcal{O}$ on k-tuples of vectors from $\mathbb{Z}^d$, for $k \in \mathbb{N}$, and then always picking the expansion (9) whose set of vectors $(\mathbf{x}_0, \ldots, \mathbf{x}_{k-1})$ is the smallest w.r.t. this order. Note that the definition of such an order is always possible, since the set of of all such representations (9) is set-isomorphic to the countable set $\bigcup_{k=1}^{\infty} \mathbb{Z}^{d \times k}$. This order enables us to

define a dynamical system $\Psi : \mathbb{Z}^d[A] \to \mathbb{Z}^d[A]$. Indeed, let (9) be the minimal expansion of $\mathbf{x} \in \mathbb{Z}^d[A]$ w.r.t. the order $\mathcal{O}$. Then Ψ is given by

$$\Psi(\mathbf{x}) := A^{-1}(\mathbf{x} - \mathbf{d}_r(\mathbf{x}_0)) = (\Phi_r(\mathbf{x}_0) + \mathbf{x}_1) + A\mathbf{x}_2 + \cdots + A^{k-2}\mathbf{x}_{k-1}. \qquad (10)$$

(We note that the expression on the right-hand side of (10) is not necessarily the shortest possible expansion of $\Psi(\mathbf{x})$.)

The attractor $\mathcal{A}_\Psi$ of the dynamical systems Ψ, respectively, is defined analogously to the attractor of Φ.

Let $A \in \mathbb{Q}^{d \times d}$ be given. The following lemma shows that it suffices to look at the dynamical system Φ_r acting on $\mathbb{Z}^d$ in order to construct a digit system in the larger space $\mathbb{Z}^d[A]$ that enjoys the finiteness property.

Lemma 2.9: *Let $A \in \mathbb{Q}^{d \times d}$ and let $\mathcal{D} \subset \mathbb{Z}^d$ be a finite set that contains a complete set of coset representatives of $\mathbb{Z}^d/(\mathbb{Z}^d \cap A\mathbb{Z}^d)$. If Φ_r in $\mathbb{Z}^d$ has a finite attractor $\mathcal{A}_{\Phi_r}$, then $\mathcal{A}_{\Phi_r} = \mathcal{A}_\Psi$. In particular, if Φ_r is ultimately zero in $\mathbb{Z}^d$, then Ψ is ultimately zero in $\mathbb{Z}^d[A]$ and the digit system $(A, \mathcal{D}_r \cup \mathcal{A}_{\Phi_r})$ has the finiteness property.*

Proof of Lemma 2.9: As Ψ maps $\mathbb{Z}^d_j[A]$ to $\mathbb{Z}^d_{j-1}[A]$, for every $\mathbf{x} \in \mathbb{Z}^d[A]$, there exists $k = k(\mathbf{x})$, such that $\Psi^k(\mathbf{x}) \in \mathbb{Z}^d$. Thus, by the definition of Ψ in (10) we gain $\Psi^{n+k}(\mathbf{x}) = \Phi^n_r(\Psi^k(\mathbf{x}))$ for each $n \geq 0$. Thus, one eventually ends up with an expansion of an integral vector $\Psi^k(\mathbf{x}) \in \mathbb{Z}^d$. This proves that $\mathcal{A}_{\Phi_r} = \mathcal{A}_\Psi$. The remaining assertions immediately follow from this identity. ∎

By using $\mathbb{Z}^d$, Φ_r, $\mathcal{D}_r$, and $\mathbb{Z}^d \cap A\mathbb{Z}^d$ in place of $\mathbb{Z}^d[A]$, Φ, $\mathcal{D}$, and $A\mathbb{Z}^d[A]$ in the proof of Proposition 2.5 we obtain immediately that, for every expanding matrix $A \in \mathbb{Q}^{d \times d}$, dynamical system Φ_r has a finite attractor $\mathcal{A}_{\Phi_r}$ in $\mathbb{Z}^d$. By Lemma 2.9, the same set $\mathcal{A}_{\Phi_r}$ then is a finite attractor of the extended remainder division Ψ in $\mathbb{Z}^d[A]$. In a similar way, one can replace Φ with Ψ in Proposition 2.5 and prove that the periodicity and finiteness properties of Ψ are completely analogous to those of Φ. Thus, in most cases Ψ can replace the classical remainder division Φ when performing arithmetics in $\mathbb{Z}^d[A]$.

In the same way as in (6) we define finite expansions of $\mathbb{Z}^d$ generated by Φ_r as well as finite expansions of $\mathbb{Z}^d[A]$ generated by Ψ. Using this terminology we get the following corollary.

Corollary 2.10: *If $A \in \mathbb{Q}^{d \times d}$ is expanding, then one can always find a digit set $\mathcal{D} \subset \mathbb{Z}^d$, such that the following assertions hold.*

(a) *every $\mathbf{x} \in \mathbb{Z}^d$ has a finite expansion in $\mathcal{D}[A]$ generated by Φ_r.*
(b) *every $\mathbf{x} \in \mathbb{Z}^d[A]$ has a finite expansion generated by Ψ. This implies that $(A, \mathcal{D})$ has the finiteness property.*

Thus, the dynamical system Ψ allows to do radix expansions in $\mathbb{Z}^d[A]$, while preserving $\mathbb{Z}^d$. This feature is extremely handy in constructing 'twisted sums' of digit systems in a way that avoids 'mixing' the arithmetics of $\mathbb{Z}^d[A]$ and $\mathbb{Z}^d[B]$, for different matrices $A \neq B$. We will come back to this in Section 4.

3. The finiteness property for generalized rotations

A matrix in $\mathbb{R}^{d \times d}$ that is similar to some orthogonal matrix in $\mathbb{R}^{d \times d}$ is called *a generalized rotation*. These matrices will be of importance when we have to deal with eigenvalues of modulus one in general matrices. In this section, we will show how to get small digit sets that ensure the finiteness property for the rational matrices that are generalized rotations.

3.1. Compactness criterion for solutions to a norm inequality

Equip the space $\mathbb{R}^d$ with the usual Euclidean norm $\|\cdot\|$ and let $\mathcal{S} = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_s\}$ be a finite subset of $\mathbb{R}^d$. Recall that *the cone* generated by vectors from $\mathcal{S}$ is defined as

$$\mathrm{Cone}\,(\mathcal{S}) = \left\{ t_1 \mathbf{v}_1 + t_2 \mathbf{v}_2 + \cdots + t_s \mathbf{v}_s : t_j \geq 0, 1 \leq j \leq s \right\}.$$

It will turn out that the condition $\mathrm{Cone}\,(\mathcal{S}) = \mathbb{R}^d$ will be an important property of certain collections of digits $\mathcal{S}$ for systems whose bases are generalized rotations. One can show that $\mathrm{Cone}\,(\mathcal{S}) = \mathbb{R}^d$ is equivalent to the fact that $\mathbf{0}_d$ is an inner point of *the convex hull* of $\mathcal{S}$, which is defined as

$$\mathrm{Conv}\,(\mathcal{S}) = \left\{ t_1 \mathbf{v}_1 + t_2 \mathbf{v}_2 + \cdots + t_s \mathbf{v}_s : t_j \geq 0, t_1 + \cdots + t_s \leq 1, 1 \leq j \leq s \right\}.$$

We will give two simple examples of sets that satisfy this property. These examples will be useful latter.

Example 3.1: Let $\mathbf{e}_1, \dots, \mathbf{e}_d$ be a standard basis of $\mathbb{R}^d$. Define the set $\mathcal{S} = \{\mathbf{v}_1, \dots, \mathbf{v}_{d+1}\}$ by

$$\mathbf{v}_j := \begin{cases} \mathbf{e}_j, & \text{for } 1 \leq j \leq d \\ -\mathbf{e}_1 - \cdots - \mathbf{e}_d, & \text{for } j = d+1. \end{cases}$$

Since $\{\mathbf{v}_j, 1 \leq j \leq d\}$ is the standard basis of $\mathbb{R}^d$, and

$$-\mathbf{v}_k = \sum_{\substack{j=1 \\ j \neq k}}^{d+1} \mathbf{v}_j,$$

one sees immediately that $\mathrm{Cone}\,(\mathcal{S}) = \mathbb{R}^d$.

Example 3.2: Let $\mathcal{S} \subset \mathbb{R}^d$ be finite, $\mathbf{v} \in \mathbb{R}^d$ arbitrary fixed vector and suppose that the matrix $M \in \mathbb{R}^{d \times d}$ is invertible. If $\mathrm{Cone}\,(\mathcal{S}) = \mathbb{R}^d$, then, for every sufficiently large $\lambda > 0$, $\mathrm{Cone}\,(\lambda M \mathcal{S} + \mathbf{v}) = \mathbb{R}^d$.

We need to restate previous definitions in terms of matrices. Recall that, for any two vectors $\mathbf{v}, \mathbf{w}$ with real entries and equal dimensions, one writes $\mathbf{v} \leq \mathbf{w}$ if every coordinate of $\mathbf{v}$ is less or equal than the corresponding coordinate of $\mathbf{w}$: $v_k \leq w_k$. In particular, $\mathbf{w} \geq \mathbf{0}_d$ means that all coordinates of $\mathbf{w}$ are non-negative. Let $M \in \mathbb{R}^{s \times d}$ be the matrix whose rows

consist of vectors from $\mathcal{S}$, that is $M^T := (\mathbf{v}_1 \, \mathbf{v}_2 \, \cdots \mathbf{v}_s)$. Then one can rewrite the definition of the cone as

$$\text{Cone}\,(\mathcal{S}) = \{M^T\mathbf{u} : \mathbf{u} \in \mathbb{R}^s, \mathbf{u} \geq \mathbf{0}_s\}.$$

Now we can prove an important criterion on the compactness of the set solutions to the matrix inequality in terms of the dual condition on M^T.

Lemma 3.3: *Let $M \in \mathbb{R}^{s \times d}$ be a real matrix with row vectors $\mathcal{S} = \{\mathbf{v}_1, \ldots, \mathbf{v}_s\} \in \mathbb{R}^d$ and fix a vector $\mathbf{b} \in \mathbb{R}^s$, with $\mathbf{b} \geq \mathbf{0}_s$. Then the subset $\mathcal{V} := \{\mathbf{x} \in \mathbb{R}^d : M\mathbf{x} \leq \mathbf{b}\}$ of $\mathbb{R}^d$ is compact if and only if $\text{Cone}\,(\mathcal{S}) = \mathbb{R}^d$ (equivalently $\mathbf{0}_d \in \text{Int}(\text{Conv}\,(\mathcal{S}))$).*

Proof of Lemma 3.3: '$\Leftarrow$': Suppose that $\text{Cone}\,(\mathcal{S}) = \mathbb{R}^d$. Obviously, $\mathcal{V}$ is closed in $\mathbb{R}^d$ and $\mathbf{0}_d \in \mathcal{V}$. Let $\mathbf{x} \in \mathcal{V}$ be arbitrary. Since $\text{Cone}\,(\mathcal{S}) = \mathbb{R}^d$, for each standard basis vector $\mathbf{e}_j \in \mathbb{R}^d$, $1 \leq j \leq d$, one can find vectors $\mathbf{y}_j \geq \mathbf{0}_s$, $\mathbf{z}_j \geq \mathbf{0}_s$ in $\mathbb{R}^s$, such that $\mathbf{y}_j^T M = \mathbf{e}_j^T$, $\mathbf{z}_j^T M = -\mathbf{e}_j^T$. The left-multiplication on left and right sides of $M\mathbf{x} \leq \mathbf{b}$ by $\mathbf{y}_j$ and by $\mathbf{z}_j$, respectively, yields

$$x_j := \mathbf{e}_j^T\mathbf{x} = (\mathbf{y}_j^T M)\mathbf{x} \leq \mathbf{y}_j^T\mathbf{b}, \quad \text{and} \quad -x_j = \mathbf{e}_j^T(-\mathbf{x}) = (\mathbf{z}_j^T M)\mathbf{x} \leq \mathbf{z}_j^T\mathbf{b}.$$

As the coordinates x_j of $\mathbf{x}$ are bounded by $-\mathbf{z}_j^T\mathbf{b} \leq x_j \leq \mathbf{y}_j^T\mathbf{b}$, the set $\mathcal{V}$ must be compact.

'$\Rightarrow$': By contradiction, suppose that $\mathcal{V}$ is compact but $\mathcal{S}$ has no proper enclosure. Since $\text{Cone}\,(\mathcal{S}) \neq \mathbb{R}^d$, there exists $\mathbf{c} \in \mathbb{R}^d$, such that the linear problem $M^T\mathbf{y} = \mathbf{c}$ has no solution $\mathbf{y} \in \mathbb{R}^s$ with $\mathbf{y} \geq \mathbf{0}_s$. Then, by *Farkas lemma* (named after [28], in modern form, stated in [29, Lemma 1 on p. 318]), the dual linear problem $M\mathbf{x} \geq \mathbf{0}_s$ has a non-zero solution $\mathbf{x} = \mathbf{n} \in \mathbb{R}^d$, such that $\mathbf{n}^T\mathbf{c} < 0$, (geometrically, a hyper-plane with the normal vector $\mathbf{n} \in \mathbb{R}^d$ through the origin separates $\mathbf{c}$ from $\text{Cone}\,(\mathcal{S})$). Since $\mathbf{b} \geq \mathbf{0}_s$, this means one can find arbitrarily large solutions to the system $M\mathbf{x} \leq \mathbf{b}$ by taking $\mathbf{x} = -\lambda\mathbf{n} \in \mathcal{V}$ and arbitrarily large $\lambda > 0$. This contradicts the compactness of $\mathcal{V}$. ∎

An easy consequence of Lemma 3.3 is the following:

Remark 3.4: If the set of solutions $\mathcal{V} := \{\mathbf{x} \in \mathbb{R}^d : M\mathbf{x} \leq \mathbf{b}\}$ is compact, then the set $\mathcal{S} = \text{Columns}(M^T) \subset \mathbb{R}^d$ contains at least $s \geq d + 1$ vectors, and some d of these are linearly independent among each other.

Lemma 3.3 is the main ingredient of the following result, which will have very important application later.

Corollary 3.5: *Suppose that $\mathcal{S} \subset \mathbb{R}^d$ is finite. Then the set of vectors $\mathbf{x} \in \mathbb{R}^d$ which, for every $\mathbf{v} \in \mathcal{S}$, satisfy*

$$\|\mathbf{x} - \mathbf{v}\| \geq \|\mathbf{x}\|$$

is compact if and only if $\text{Cone}\,(\mathcal{S}) = \mathbb{R}^d$.

Proof of Corollary 3.5: The inequality is equivalent to $\|\mathbf{x}\|^2 - 2\mathbf{v}^T\mathbf{x} + \|\mathbf{v}\|^2 \geq \|\mathbf{x}\|^2$, or, $\mathbf{v}^T\mathbf{x} \leq \frac{1}{2}\|\mathbf{v}\|^2$, for each $\mathbf{v} \in \mathcal{S}$. Suppose that $\mathcal{S} = \{\mathbf{v}_1, \ldots, \mathbf{v}_s\}$ and let $M \in \mathbb{R}^{s \times d}$ be the matrix whose rows consist of vectors from $\mathcal{S}$, that is $M^T := (\mathbf{v}_1 \, \mathbf{v}_2 \, \cdots \mathbf{v}_s)$. One obtains a system of linear inequalities $M\mathbf{x} \leq \mathbf{b}$ where the non-negative vector $\mathbf{b} \in \mathbb{R}^s$ is defined by $b_j := 1/2 \|\mathbf{v}_j\|^2$. Now apply Lemma 3.3. ∎

3.2. Generalized rotation and its invariant norm

We now give the formal definition of the main objects of the present section.

Definition 3.6 (Generalized rotation): A real square matrix $M \in \mathbb{R}^{d \times d}$ is called *generalized rotation*, if M is similar to some orthogonal matrix R.

It is known that matrices $M \in \mathbb{R}^{d \times d}$ that are diagonalizable over $\mathbb{C}$, with all eigenvalues $\lambda \in \mathbb{C}$ of absolute value $|\lambda| = 1$ are general rotations; see, for instance [30, Chapter 9, Section 13, Equations (102)–(106)]. For a general rotation M there always exists an invertible real transformation $T \in \mathbb{R}^{d \times d}$, such that $M := TRT^{-1}$ takes a block-diagonal form with 1×1 blocks (± 1) or 2×2 blocks

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \quad \theta \in [0, 2\pi)$$

that correspond to eigenvalues $\lambda = e^{i\theta}$. Such R is a composition of mutually orthogonal rotations and is itself an orthogonal matrix, i.e. $R^T R = \mathbb{1}_d$. Details of such decomposition are outlined in [30, Chapter 9, Section 13]), equations (112)–(113) therein. Furthermore, orthogonal matrices R can be parametrized using Cayley formulas [30, Chapter 9, equations (123)–(126)] (cf. [31,32]). Explicit parametrization formulas in small dimensions $d = 3, 4$ are available [33–37].

If M is a general rotation, then there exist an M-invariant norm on $\mathbb{R}^d$. Indeed, let T be the aforementioned transformation that brings M to its rotational form R. Define $\|\mathbf{x}\|_M := \|T^{-1}\mathbf{x}\|$, where $\|\cdot\|$ is the usual Euclidean norm in $\mathbb{R}^d$. Then

$$\|M\mathbf{x}\|_M = \|T^{-1}M\mathbf{x}\| = \|(T^{-1}MT)T^{-1}\mathbf{x})\| = \|RT^{-1}\mathbf{x}\| = \|T^{-1}\mathbf{x}\| = \|\mathbf{x}\|_M,$$

since R is orthogonal, and $\|R\mathbf{y}\| = \|\mathbf{y}\|$ for any $\mathbf{y} \in \mathbb{R}^d$.

One important fact that we will need in the sequel: Corollary 3.5 of previous Section 3.1 still holds true if one replaces the Euclidean norm $\|\cdot\|$ by this new norm $\|\cdot\|_M$.

Corollary 3.7: *Let $\mathcal{S} \subset \mathbb{R}^d$ be a finite set and suppose that $M \in \mathbb{R}^{d \times d}$ is a generalized rotation. Then the set of vectors $\mathbf{x} \in \mathbb{R}^d$ which, for every $\mathbf{v} \in \mathcal{S}$, satisfy $\|\mathbf{x} - \mathbf{v}\|_M \geq \|\mathbf{x}\|_M$ in M-invariant norm $\|\cdot\|_M$ of $\mathbb{R}^d$ is compact if and only if $\mathrm{Cone}\,(\mathcal{S}) = \mathbb{R}^d$.*

Proof of Corollary 3.7: The M-invariant norm inequality reads $\|T^{-1}\mathbf{x} - T^{-1}\mathbf{v}\| \geq \|T^{-1}\mathbf{x}\|$ in Euclidean norm, where $T \in \mathbb{R}^{d \times d}$ is invertible. By continuity, T^{-1} and T both preserve the open inclusion of $\mathbf{0}_d$ between $\mathcal{S}$ and $T^{-1}\mathcal{S}$, as well as the compactness. Hence, Corollary 3.5 applies. ∎

3.3. Finiteness property for generalized rotations

In this section, we assume that $A \in \mathbb{Q}^{d \times d}$ is a generalized rotation, characterized in Definition 3.6 of Section 3.2. Generalized rotations serve as a fundamental building block to construct digit systems with the finiteness property for a general rational matrix with eigenvalues of absolute value $= 1$. For general rotation bases, we introduce digit sets with special geometric properties.

Definition 3.8 (Good enclosure): The digit set $\mathcal{D} \subset \mathbb{Z}^d[A]$ is said to have *a good enclosure*, if, for each coset representative $\mathbf{x} \in \mathbb{Z}^d[A]/A\mathbb{Z}^d[A]$, the subset

$$\mathcal{D}(\mathbf{x}) := \left\{ \mathbf{d} \in \mathcal{D} : \mathbf{d} \equiv \mathbf{x} \pmod{A\mathbb{Z}^d[A]} \right\}$$

satisfies Cone $(\mathcal{D}(\mathbf{x})) = \mathbb{R}^n$, or, equivalently: the origin $\mathbf{0}_d$ always lies in the interior of the convex hull of $\mathcal{D}(\mathbf{x})$ for any given residue class modulo $\pmod{A\mathbb{Z}^d[A]}$.

If A is general rotation, then A^{-1} is also general rotation. Pick an A^{-1}-invariant norm $\|\cdot\|_{A^{-1}}$ in $\mathbb{R}^d$, defined in Section 3.2. Enumerate the digits $\mathcal{D} = \{\mathbf{d}_1, \ldots, \mathbf{d}_k\}$ and define *the digit function* $\mathbf{d} : \mathbb{Z}^d[A] \to \mathcal{D}$ by

$$\mathbf{d}(\mathbf{x}) := \mathbf{d}_j \in \mathcal{D}, \quad \text{such that} \begin{cases} \mathbf{d}_j \equiv \mathbf{x} \pmod{A\mathbb{Z}^d[A]}, \\ \mathbf{d}_j \text{ minimizes } \|\mathbf{x} - \mathbf{d}_j\|_{A^{-1}} \text{ in } \mathcal{D}, \\ \text{the index } j \text{ is the smallest possible.} \end{cases} \tag{11}$$

The smallest index condition is to impose uniqueness in cases where the norm-minimum is achieved for several $\mathbf{d}_j \in \mathcal{D}(\mathbf{x})$. The quotient function $\Phi : \mathbb{Z}^d[A] \to \mathbb{Z}^d[A]$ used in the division with remainder for the digit sets with good enclosures is defined as in (5).

Now comes the most important result of this section.

Theorem 3.9: *Let $A \in \mathbb{Q}^{d \times d}$ be a generalized rotation. If $\mathcal{D}$ has a good enclosure, then the remainder division $\Phi : \mathbb{Z}^d[A] \to \mathbb{Z}^d[A]$ with the digit function from* (11) *has a finite attractor set $\mathcal{A}_\Phi \subset \mathbb{Z}^d[A]$. In particular, Φ is ultimately periodic mapping with a finite number of possible smallest periods.*

Proof of Theorem 3.9: First we show that the set $\mathcal{V} := \{\mathbf{x} \in \mathbb{Z}^d[A] : \|\Phi(\mathbf{x})\|_{A^{-1}} \geq \|\mathbf{x}\|_{A^{-1}}\}$ is bounded in $\mathbb{R}^d$. By A^{-1}-invariance, $\|\Phi(\mathbf{x})\|_{A^{-1}} = \|\mathbf{x} - \mathbf{d}(\mathbf{x})\|_{A^{-1}}$. For each $\mathbf{x} \in \mathcal{V}, \mathcal{D}(\mathbf{x}) \neq \varnothing$ by Definition 3.8 and $\|\mathbf{x} - \mathbf{d}_j\|_{A^{-1}} \geq \|\mathbf{x}\|_{A^{-1}}$ holds for each digit $\mathbf{d}_j \in \mathcal{D}(\mathbf{x})$ by (11). Since $\mathcal{D}(\mathbf{x})$ has good enclosure, by Corollary 3.7, the set of vectors $\mathbf{x} \in \mathbb{R}^d$ that satisfy the last stated norm inequality for each $\mathbf{d}_j \in \mathcal{D}(\mathbf{x})$ must be compact. Therefore $\mathcal{V}$ must be bounded, and we can define the critical radius $r := r(\mathcal{V}, \mathcal{D}) := \sup_{\mathbf{x} \in \mathcal{V}} \|\mathbf{x}\|_{A^{-1}} + \max_{\mathbf{d} \in \mathcal{D}} \|\mathbf{d}\|_{A^{-1}}$.

By Lemma 2.4, there exists $l \in \mathbb{N}$, such that the orbit $\{\mathbf{x}_n := \Phi^n(\mathbf{x})\}_{n=1}^\infty$ of every point $\mathbf{x} \in \mathbb{Z}^d[A]$ eventually reaches and then stays in the lattice $\mathbb{Z}_l^d[A]$. Since $\mathbb{Z}_l^d[A]$ is a lattice, one cannot have $\|\mathbf{x}_{n+1}\| < \|\mathbf{x}_n\|$ for every $n > n_0$. Therefore, $\|\mathbf{x}_{n+1}\| \geq \|\mathbf{x}_n\|$ occurs infinitely many times. For such n, one must have $\mathbf{x}_n \in \mathcal{V} \cap \mathbb{Z}_l^d[A]$. At the next step after such occurrence, we have

$$\|\mathbf{x}_{n+1}\|_{A^{-1}} = \|\Phi(\mathbf{x}_n)\|_{A^{-1}} = \|\mathbf{x}_n - \mathbf{d}(\mathbf{x}_n)\|_{A^{-1}} \leq \|\mathbf{x}_n\|_{A^{-1}} + \|\mathbf{d}(\mathbf{x}_n)\|_{A^{-1}} \leq r(\mathcal{V}, \mathcal{D}).$$

In subsequent iterations, we have either $\mathbf{x}_{j+1} \in \mathcal{V}$ again, or the $\|\mathbf{x}_{j+1}\|_{A^{-1}} < \|\mathbf{x}_j\|_{A^{-1}}$. Therefore, $\Phi^n(\mathbf{x})$ ultimately enters the ball $B_{A^{-1}}(\mathbf{0}, r)$ and then never leaves it. Since $\mathbb{Z}_l^d[A]$ is a lattice, $B_{A^{-1}}(0, r) \cap \mathbb{Z}_l^d[A]$ must be finite. Hence, Φ has a finite attractor set $\mathcal{A}_\Phi \subset B_{A^{-1}}(0, r) \cap \mathbb{Z}_l^d[A]$. The last statement of Theorem 3.9 follows from the fact that $\Phi^{n+1}(\mathbf{x})$ is uniquely determined by $\Phi^n(\mathbf{x})$. ∎

Corollary 3.10: *For every general rotation $A \in \mathbb{Q}^{d \times d}$, there exists a digit set $\mathcal{D} \subset \mathbb{Z}^d[A]$ of the size $\#\mathcal{D} = (d+1)[\mathbb{Z}^d[A] : A\mathbb{Z}^d[A]]$, such that the division mapping $\Phi : \mathbb{Z}^d[A] \to \mathbb{Z}^d[A]$ is ultimately periodic and has finite attractor. In particular, one can find such digit sets in $\mathbb{Z}^d$.*

Proof of Corollary 3.10: Let $\mathcal{R}$ be a complete set of residue class representatives of the residue class ring $\mathbb{Z}^d/(\mathbb{Z}^d \cap A\mathbb{Z}_k^d[A])$ and take $\mathcal{S} = \{\mathbf{e}_1, \ldots, \mathbf{e}_d, -\mathbf{e}_1 - \cdots - \mathbf{e}_d\}$ from Example 3.1 of Section 3.1. For every sufficiently large integer $s \in \mathbb{N}$, that is divisible by all denominators of the rational entries of the matrix A, the digit set $\mathcal{D} := sA\mathcal{S} + \mathcal{R} \subset \mathbb{Z}^d$ contains all residue classes (mod $A\mathbb{Z}^d[A]$) and satisfies the conditions of Theorem 3.9, as explained in Example 3.2 of Section 3.1. Now apply Theorem 3.9. ∎

Corollary 3.11: *For every generalized rotation $A \in \mathbb{Q}^{d \times d}$, there exist digit sets $\mathcal{D} \subset \mathbb{Z}^d[A]$ (and even $\mathcal{D} \subset \mathbb{Z}^d$), such that the digit system $(A, \mathcal{D})$ has the finiteness property in $\mathbb{Z}^d[A]$.*

Proof of Corollary 3.11: Consider the digit set $\mathcal{D}'$ used in Corollary 3.10 and apply the second part of Proposition 2.2 to $\mathcal{D} := \mathcal{D}' \cup \mathcal{A}_\Phi$. ∎

Remark 3.12: All results of Section 3 for generalized rotations $A \in \mathbb{Q}^{d \times d}$ remain true for Φ_r in $\mathbb{Z}^d$ with respect to auxiliary lattice $\mathbb{Z}^d \cap A\mathbb{Z}^d$, provided that one defines the good arithmetical enclosure property in $\mathbb{Z}^d$ (mod $\mathbb{Z}^d \cap A\mathbb{Z}^d$) instead of (mod $A\mathbb{Z}^d[A]$) in Definition 3.8 and Equation (11), and substitutes $\mathbb{Z}^d$ in place of $\mathbb{Z}^d[A]$ where appropriate.

4. Twisted digits systems for hypercompanion matrices

In the present section, we show how we can build up number systems with property (F) from simple building blocks. We develop a certain version of a direct sum that generalizes the notion of *simultaneous digit systems* previously considered by Kóvacs [38–40]; see also [8, Section 3] and [9] for related *products of number systems* in polynomial rings. This will enable us to construct digit sets with Property (F) for the hypercompanion block matrices.

First, let us recall the notations of 'the direct sum' of vectors and matrices. For two vectors $\mathbf{x} \in \mathbb{Q}^m$ and $\mathbf{y} \in \mathbb{Q}^n$, their direct sum is a block vector $\mathbf{x} \oplus \mathbf{y} := \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} \in \mathbb{Q}^{m+n}$. This notation extends to the sets of vectors $\mathcal{S} \subset \mathbb{Q}^m, \mathcal{T} \subset \mathbb{Q}^n$ by

$$\mathcal{S} \oplus \mathcal{T} := \{\mathbf{x} \oplus \mathbf{y} : \mathbf{x} \in \mathcal{S}, \mathbf{y} \in \mathcal{Y}\},$$

for instance, $\mathbb{Q}^m \oplus \mathbb{Q}^n = \mathbb{Q}^{m+n}$. Secondly, the direct sum of two matrices, say, $A \in \mathbb{Q}^{m \times m}$ and $B \in \mathbb{Q}^{n \times n}$ is defined as the block matrix

$$A \oplus B = \begin{pmatrix} A & O \\ O & B. \end{pmatrix}$$

4.1. Semi–direct (twisted) sums of digit systems

Let A, B be two invertible rational matrices of dimensions $m \times m, n \times n$, respectively, let O be the $m \times n$ zero-matrix, and C be an $n \times m$ integer matrix. By block multiplication,

we see that the partitioned matrices

$$M = \begin{pmatrix} A & O \\ C & B \end{pmatrix}, \quad M^{-1} = \begin{pmatrix} A^{-1} & O \\ -B^{-1}CA^{-1} & B^{-1} \end{pmatrix},$$

are inverse to each other. We will call the partioned matrix M *the sum of A and B, twisted by C* (a semi–direct sum, or a twisted sum for short). This will be abbreviated as $M := A \oplus_C B$.

Suppose that $\mathcal{D}_A \in \mathbb{Z}^m$ and $\mathcal{D}_B \in \mathbb{Z}^n$ are the digit sets satisfying $\mathbb{Z}^m/(\mathbb{Z}^m \cap A\mathbb{Z}^m) \subset \mathcal{D}_A$ and $\mathbb{Z}^n/(\mathbb{Z}^m \cap B\mathbb{Z}^m) \subset \mathcal{D}_B$. This containment can be strict: digit sets are allowed to be larger than residue sets.

Associated with $(A, \mathcal{D}_A)$ and $(B, \mathcal{D}_B)$ are the corresponding *restricted digit functions* together with the dynamical systems

$$d_{r,A} : \mathbb{Z}^m \to \mathcal{D}_A, \quad d_{r,A}(x) \equiv x \pmod{\mathbb{Z}^d \cap A\mathbb{Z}^d}, \tag{12}$$

$$\Phi_{r,A} : \mathbb{Z}^m \to \mathbb{Z}^m, \quad \Phi_{r,A}(x) = A^{-1}(x - d_{r,A}(x)), \tag{13}$$

$$d_{r,B} : \mathbb{Z}^n \mapsto \mathcal{D}_B, \quad d_{r,B}(y) \equiv y \pmod{\mathbb{Z}^d \cap B\mathbb{Z}^d}, \tag{14}$$

$$\Phi_{r,B} : \mathbb{Z}^n \mapsto \mathbb{Z}^n, \quad \Phi_{r,B}(y) = B^{-1}(y - d_{r,B}(y)), \tag{15}$$

for $x \in \mathbb{Z}^m$ and $y \in \mathbb{Z}^n$. They perform division with remainder in the lattices $\mathbb{Z}^m$ and $\mathbb{Z}^n$, respectively; see Definition 2.8 in Section 2.

We will build the corresponding digit set and restricted remainder division by M in $\mathbb{Z}^m \oplus \mathbb{Z}^n = \mathbb{Z}^{m+n}$ modulo the sublattice $\mathbb{Z}^{m+n} \cap M\mathbb{Z}^{m+n}$.

To account for the carry from the first component to the second, we first set up a modified digit function $\widetilde{d}_{r,B} : \mathbb{Z}^{m+n} \to \mathcal{D}_B$ and an associated dynamical system $\widetilde{\Phi}_{r,B} : \mathbb{Z}^{m+n} \mapsto \mathbb{Z}^n$ for the division with remainder $\pmod{\mathbb{Z}^n \cap B\mathbb{Z}^n}$ on the second component of $z = x \oplus y$ by

$$\widetilde{d}_{r,B}(z) := d_{r,B}\left(y - C \cdot \Phi_{r,A}(x)\right), \quad \widetilde{\Phi}_{r,B}(z) := B^{-1}\left(y - C \cdot \Phi_{r,A}(x) - \widetilde{d}_{r,B}(z)\right).$$

The function $\widetilde{d}_{r,B}(z)$ is well-defined, since C is integral and its dimensions $n \times m$ match with the dimensions $m \times 1$ of $\Phi_{r,A}(x)$. The function $\widetilde{\Phi}_{r,B}(z)$ is also well-defined, since $y - C \cdot \Phi_{r,A}(x) - \widetilde{d}_{r,B}(z) \equiv 0 \pmod{\mathbb{Z}^n \cap B\mathbb{Z}^n}$, so the multiplication by B^{-1} produces a vector in $\mathbb{Z}^n$.

We are now in the position to define *the twisted restricted division with remainder by M.* Let *the twisted digit function* $d_{r,M} : \mathbb{Z}^{m+n} \to \mathcal{D}_A \oplus \mathcal{D}_B$ be given by

$$d_{r,M}(z) := ((d_{r,A} \circ \pi_A)) \oplus \widetilde{d}_{r,B})(z) = \begin{pmatrix} d_{r,A}(x) \\ \widetilde{d}_{r,B}(z) \end{pmatrix} = \begin{pmatrix} d_{r,A}(x) \\ d_{r,B}\left(y - C \cdot \Phi_{r,A}(x)\right) \end{pmatrix}, \tag{16}$$

where $\pi_A : \mathbb{Z}^{m+n} \mapsto \mathbb{Z}^m$ is simply a projection of the first component $\pi_A \begin{pmatrix} x \\ y \end{pmatrix} = x$. It will be abbreviated as $d_{r,M} = d_{r,A} \oplus_C d_{r,B}$.

Then we define the associated dynamical system in the usual way by setting

$$\Phi_{r,M} : \mathbb{Z}^{m+n} \to \mathbb{Z}^{m+n}, \quad \Phi_{r,M}(\mathbf{z}) := M^{-1}(\mathbf{z} - \mathbf{d}_{r,M}(\mathbf{z})).$$

This construction will be abbreviated as $\Phi_{r,M} := \Phi_{r,A} \oplus_C \Phi_{r,B}$. One verifies easily that

$$
\begin{aligned}
\Phi_{r,M}(\mathbf{z}) &= \begin{pmatrix} A^{-1} & O \\ -B^{-1}CA^{-1} & B^{-1} \end{pmatrix} \begin{pmatrix} \mathbf{x} - \mathbf{d}_{r,A}(\mathbf{x}) \\ \mathbf{y} - \widetilde{\mathbf{d}}_{r,B}(\mathbf{z}) \end{pmatrix} \\
&= \begin{pmatrix} A^{-1}(\mathbf{x} - \mathbf{d}_{r,A}(\mathbf{x})) \\ B^{-1}\left(-CA^{-1}(\mathbf{x} - \mathbf{d}_{r,A}(\mathbf{x})) + \mathbf{y} - \widetilde{\mathbf{d}}_{r,B}(\mathbf{z})\right) \end{pmatrix} \\
&= \begin{pmatrix} \Phi_{r,A}(\mathbf{x}) \\ \widetilde{\Phi}_{r,B}(\mathbf{z}) \end{pmatrix} = \left((\Phi_{r,A} \circ \pi_A) \oplus \widetilde{\Phi}_{r,B}\right)(\mathbf{z}).
\end{aligned}
$$

Thus, $\Phi_{r,M}$ is defined correctly. Since $\mathbf{z} = \mathbf{d}_{r,M}(\mathbf{z}) + M\Phi_{r,M}(\mathbf{z})$, we obtain that $\mathbf{z} \equiv \mathbf{d}_{r,M}(\mathbf{z})$ (mod $\mathbb{Z}^{m+n} \cap M\mathbb{Z}^{m+n}$). This last congruence implies that the mapping $\mathbf{z} \mapsto \mathbf{d}_{r,M}(\mathbf{z})$ (mod $\mathbb{Z}^{m+n}/(\mathbb{Z}^{m+n} \cap M\mathbb{Z}^{m+n})$) is a homomorphism from $\mathbb{Z}^{m+n}$ to $\mathbb{Z}^{m+n}/(\mathbb{Z}^{m+n} \cap M\mathbb{Z}^{m+n})$. In particular, $\mathcal{D}_A \oplus \mathcal{D}_B$ must contain all the representatives of $\mathbb{Z}^{m+n}/(\mathbb{Z}^{m+n} \cap M\mathbb{Z}^{m+n})$. By (16), $\mathbf{d}_{r,M}(\mathbf{z})$ attain all possible values in $\mathcal{D}_A \oplus \mathcal{D}_B$ as $\mathbf{x}$ and $\mathbf{y}$ run through $\mathbb{Z}^m/(\mathbb{Z}^m \cap A\mathbb{Z}^m)$ and $\mathbb{Z}^n/(\mathbb{Z}^n \cap B\mathbb{Z}^m)$, respectively.

Lemma 4.1: *If $\mathbf{0}_m \in \mathcal{D}_A, \mathbf{0}_n \in \mathcal{D}_B$ and attractors of $\Phi_{r,A}$ and $\Phi_{r,B}$ consist only of the zero vectors in $\mathbb{Z}^m$ and $\mathbb{Z}^n$, respectively, then $\Phi_{r,M} = \Phi_{r,A} \oplus_C \Phi_{r,B}$ has attractor $\{\mathbf{0}_{m+n}\}$ in $\mathbb{Z}^{m+n}$. In this case, the digit system $(M, \mathcal{D}_A \oplus \mathcal{D}_B)$ in $\mathbb{Z}^{m+n}[M]$, where $M = A \oplus_C B$, has the finiteness property.*

Proof of Lemma 4.1: Notice that

$$\Phi_{r,M}^k(\mathbf{z}) = \begin{pmatrix} \Phi_{r,A}^k(\mathbf{x}) \\ \widetilde{\Phi}_{r,B}(\Phi_{r,M}^{k-1}(\mathbf{z})) \end{pmatrix} = \begin{pmatrix} \mathbf{0}_m \\ \widetilde{\Phi}_{r,B}(\Phi_{r,M}^{k-1}(\mathbf{z})) \end{pmatrix}$$

for $k \geq k_0 = k_0(\mathbf{x})$. When the first component $\mathbf{x}$ of $\mathbf{z}$ is $\mathbf{0}_m$, then $\Phi_{r,M}$ reduces to $\Phi_{r,B}$, i.e. $d_{r,M}(\mathbf{z}) = \mathbf{d}_{r,B}(\mathbf{y})$ and $\widetilde{\Phi}_{r,B}(\mathbf{z}) = \Phi_{r,B}(\mathbf{y})$. Thus,

$$\Phi_{r,M}^k(\mathbf{z}) = \begin{pmatrix} \mathbf{0}_m \\ \Phi_{r,B}^{k-k_0}(\pi_B \circ \Phi_{r,M}^{k_0}(\mathbf{z})) \end{pmatrix} = \begin{pmatrix} \mathbf{0}_m \\ \mathbf{0}_n \end{pmatrix}, \quad \text{for } k \geq k_0 + k_1, k_1 = k_1(\mathbf{z}).$$

Thus, $\Phi_{r,M}$ is ultimately zero in $\mathbb{Z}^{m+n}$. To show that $(M, \mathcal{D}_A \oplus \mathcal{D}_B)$ has the finiteness property in $\mathbb{Z}^{n+m}[M]$, apply Lemma 2.9 with Ψ_M (which is defined in terms of $\Phi_{r,M}$). ■

4.2. Hypercompanion bases

Equipped with the twisted sums of digit systems we can establish the finiteness result for generalized Jordan blocks matrices. Recall that *the companion matrix $C(f) \in \mathbb{Q}^{d \times d}$ of a*

monic polynomial

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$$

of degree $d := \deg f \geq 1$ is defined by

$$C(f) = \begin{pmatrix} 0 & 0 & \ldots & 0 & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 & -a_{d-2} \\ 0 & 0 & \ldots & 0 & 1 & -a_{d-1} \end{pmatrix}.$$

Following the notation in [41, Section 8.9, pp. 161–163], we define the *the hypercompanion matrix* $H_k := H_k(f)$ of $f(x)$ of order k. For $k = 1$, it is simply equal to $H_1 := C(f)$, while, for $k \geq 2$, it is defined by $k \times k$ block structure

$$H_k(f) := \begin{pmatrix} C(f) & O & \cdots & O & O \\ N & C(f) & \cdots & O & O \\ O & N & \ddots & O & O \\ \vdots & \vdots & \ddots & C(f) & O \\ O & O & \cdots & N & C(f) \end{pmatrix}. \tag{17}$$

Here, $N \in \mathbb{Z}^{d \times d}$ has 1 in its top–right corner and all other entries 0. Clearly, $H_k \in \mathbb{Q}^{kd \times kd}$. In our paper, we use the transposed form of [41], due to our choice of matrix-vector multiplication. An alternative form of hypercompanion matrices, where N^t would appear above the principal diagonal is used in Jacobson [42, p. 72]. In the literature, the hypercompanion matrices also appear under the names of *the (primary) rational canonical form* [43], or *the generalized Jordan block* [44]: in the special case $d = 1$, H_k is simply the classical Jordan block with a rational eigenvalue of multiplicity k.

Lemma 4.2: *Let $f \in \mathbb{Q}[x]$ of degree d be monic and irreducible over $\mathbb{Q}$, with the associated hypercompanion matrix $H_k = H_k(f) \in \mathbb{Q}^{n \times n}$ of order k and dimension dk. If all the zeros of $f(x)$ in $\mathbb{C}$ are of absolute value ≥ 1, then there exists a digit set $\mathcal{D}_{H_k}$, containing the zero vector, a restricted digit function $\mathbf{d}_{r,H_k} : \mathbb{Z}^{dk} \to \mathcal{D}_{H_k}$ with associated dynamical system $\Phi_{r,H_k} : \mathbb{Z}^{dk} \to \mathbb{Z}^{dk}$, such that Φ_{r,H_k} has attractor $\{\mathbf{0}_{dk}\}$.*

Proof of Lemma 4.2: Consider the case $k = 1$. Then $H = H_1(f)$ is the companion matrix of f. Since f is irreducible over $\mathbb{Q}$, there are two possibilities: either f has all roots of absolute value > 1, or all roots of absolute value $= 1$. In the first case, H^{-1} is a contraction, and we can take the digit set $\mathcal{D}'_H$ which is a complete set of coset representatives of the residue class ring $\mathbb{Z}^d/(\mathbb{Z}^d \cap H\mathbb{Z}^d)$ which leads to a finite attractor of Φ_{r,H_1}. In the second case, H is a generalized rotation, so according to the Remark 3.4, there exists a digit set $\mathcal{D}'_H$ that contains all coset representatives of $\mathbb{Z}^d/(\mathbb{Z}^d \cap H\mathbb{Z}^d)$ and that has a good enclosure. In both cases, the division mapping $\Phi_{r,H}(\mathbf{x}) = H^{-1}(\mathbf{x} - \mathbf{d}_{r,H}(\mathbf{x}))$, where $\mathbf{d}_{r,H} : \mathbb{Z}^d \to \mathcal{D}'_H$ satisfies $\mathbf{d}_{r,H}(\mathbf{x}) \equiv \mathbf{x} \pmod{\mathbb{Z}^d \cap H\mathbb{Z}^d}$ is ultimately periodic by Remark 2.10 and Remark 3.4. Now

take $\mathcal{D}_H$ to be the union of $\mathcal{D}'_H$, the zero digit $\mathbf{0}_d$ and the points from the attractor of $\Phi_{\mathrm{r},H}$ in $\mathbb{Z}^d$, and modify the digit function $\mathbf{d}_{\mathrm{r},H}$ so that it $\mathbf{d}_{\mathrm{r},H}(\mathbf{x}) = \mathbf{x}$ for $\mathbf{x} = \mathbf{0}_d$ or $\mathbf{x}$ in the attractor. Clearly, $\Phi_{\mathrm{r},H}$ has attractor $\{\mathbf{0}_d\}$. Hence, $(H, \mathcal{D}_H)$ now has Property (F) in $\mathbb{Z}^d[H]$.

Assume that the lemma is true for all hypercompanion matrices of order $\leq k$, and that we already have the digit sets $\mathcal{D}_{H_k}$ and functions $\mathbf{d}_{\mathrm{r},H_k}, \Phi_{\mathrm{r},H_k}$ with the required properties. Notice that, by denoting the $d \times d(k+1)$ block matrix $G = (O \ \dots \ O \ N)$ with integer entries, one can write H_{k+1} is a twisted sum $H_{k+1} = H_k \oplus_G H_1$. By Lemma 4.1, the dynamical system $\Phi_{\mathrm{r},H_{k+1}} := \Phi_{\mathrm{r},H_k} \oplus_G \Phi_{\mathrm{r},H_1}$ with the digit set $\mathcal{D}_{H_k} \oplus \mathcal{D}_{H_1}$ and the digit function $\mathbf{d}_{\mathrm{r},H_{k+1}} := \mathbf{d}_{\mathrm{r},H_k} \oplus_G \mathbf{d}_{\mathrm{r},H_1}$ has attractor $\{\mathbf{0}_{d(k+1)}\}$ and, hence, $(H_{k+1}, \mathcal{D}_{H_k} \oplus \mathcal{D}_{H_1})$ has the finiteness property in $\mathbb{Z}^{d(k+1)}[H_{k+1}]$. ∎

5. Applications to the general theory

In this section, we use our theory in order to give new proofs of some general characterization results of Property (F) established in [18] and [20]. The advantage of these proofs is the fact that they are more algorithmic and allow good control on the size of the digit sets.

In [20], we have proved the following result.

Theorem 5.1 (Jankauskas and Thuswaldner [20]): *Let A be an $d \times d$ matrix with rational entries. There is a digit set $\mathcal{D} \subset \mathbb{Z}^d[A]$ that makes $(A, \mathcal{D})$ a digit system in $\mathbb{Z}^d[A]$ with finiteness property if and only if A has no eigenvalue λ with $|\lambda| < 1$. The digit set $\mathcal{D}$ can even be chosen to be a subset of $\mathbb{Z}^d$.*

The proof Theorem 5.1 in [20] essentially builds on the following theorem.

Theorem 5.2 (Akiyama et al. [18]): *Let $\alpha \in \mathbb{C}$. Then, there is a finite subset F of $\mathbb{Z}$, such that $\mathbb{Z}[\alpha] = F[\alpha]$, if and only if α is an algebraic number whose conjugates, over $\mathbb{Q}$, are all of modulus one, or all of modulus greater than one.*

In order to prove Theorem 5.1 in [20], the main result of [18], Theorem 5.2, was translated into the polynomial ring setting and formulated in terms of a finiteness property for the representations of polynomials in the quotient ring $\mathbb{Z}[x]/(f)$, where $f = f(x) \in \mathbb{Z}[x]$. Then, it was shown that this finiteness property can be transferred from these intermediate polynomial rings to companion matrices of powers of irreducible factors of $f(x)$. The last step was to 'assemble' the finite representations together through the Frobenius normal form of A. While our approach in [20] resulted in a very concise proof of Theorem 5.1, the introduction of intermediate algebraic structures make the practical computation of the radix expansions extremely complicated. First key moment – the control on the orbit of $A^{-n}\mathbf{x}$ in the directions of eigenvectors with $|\lambda| = 1$ – is achieved through the embedding into a more complicated representation space $\mathbb{R}^d \times \prod_{\mathfrak{p}} \mathbb{Q}_{\mathfrak{p}}$ (an open subset of an adèle ring) in the proof of Theorem 5.2 in [18]. The second key moment – control over the behaviour of $A^{-n}\mathbf{x}$ in the directions that correspond to Jordan blocks of order $m \geq 2$ – is performed in [20] by convolving the finite representations in the intermediate rings $\mathbb{Z}[x]/(f^m)$. This obscures the dynamics of the radix expansion process. Another side effect is, that the introduction of the intermediate structures and the subsequent process of assembling the finite representations typically blows out the sizes of the digit sets. All factors combined, the proof of Theorem 5.1 in [20] does not translate in a straightforward

way into a practical algorithm and makes the computation of radix expansions in $(A, \mathcal{D})$ rather complicated. These drawbacks are no longer there in the proofs of these theorems we will now provide.

Proof of Theorem 5.1: We first prove the sufficiency: if all the eigenvalues of A are of absolute value ≥ 1, there exists $(A, \mathcal{D})$ with the finiteness property in $\mathbb{Z}^d[A]$.

By [41, Chapter 8, p. 162, Theorem 8.10] there exists an invertible matrix $T \in \mathbb{Q}^{d \times d}$, such that $B = T^{-1}AT$ takes a block diagonal form $B = \oplus_{j=1}^r H_j$, where each block $H_j = H_{k_j}(f_j) \in \mathbb{Q}^{d_j \times d_j}, 1 \leq j \leq r, 1 \leq d_j \leq d, d_1 + \cdots + d_r = d$, is a hypercompanion matrix of order k_j of a monic irreducible polynomial $f_j(x) \in \mathbb{Q}[x]$ that divides the characteristic polynomial $\Phi_r(x)$ of A. Since for any $t \in \mathbb{Z}, (tT)A(tT)^{-1} = TAT^{-1}$, we can assume that $T \in \mathbb{Z}^{d \times d}$. First, we will construct the digit system with the finiteness property for the module $\mathbb{Z}^d[B]$.

By assumption, $A \in \mathbb{Q}^{d \times d}$ has no eigenvalues $\lambda \in \mathbb{C}$ of absolute value $|\lambda| < 1$. By the irreducibly of f_j, all eigenvalues of H_j are of absolute value > 1, or all of them are of absolute value $= 1$. We consider two possibilities: a) every H_j either is expanding, or has order $k_j = 1$; b) some H_j of order $k_j \geq 2$ are not expanding, that is, have only unimodular eigenvalues.

Case (a) according to Proposition 2.5 (for expanding matrices H_j) and by Corollary 3.11 (for generalized rotation matrices H_j), there exists digit sets $\mathcal{D}_j \subset \mathbb{Z}^{d_j}[H_j]$ (and even $\mathcal{D}_j \subset \mathbb{Z}^{d_j}$), such that each digit system $(H_j, \mathcal{D}_j)$ has the finiteness property in $\mathbb{Z}^{d_j}[H_j]$; each such digit system is equipped with the dynamical system $\Phi_j : \mathbb{Z}^{d_j}[H_j] \to \mathbb{Z}^{d_j}[H_j]$, each of which has attractor $\{\mathbf{0}_{d_j}\}$ in $\mathbb{Z}^{d_j}[H_j]$. In order to compensate for the different lengths of radix expansions across all blocks, we need $\mathbf{0}_{d_j} \in \mathcal{D}_j$ (or simply adjoin the zero vectors to the digit sets). Then we take their cartesian product $\mathcal{D} := \oplus_{j=1}^r \mathcal{D}_j$. Since $B = \oplus_{j=1}^r H_j$, one readily verifies $\mathbb{Z}^d[B] = \oplus_{j=1}^r \mathbb{Z}^{d_j}[H_j]$. By the finiteness property of $(H_j, \mathcal{D}_j)$, for each $j, 1 \leq j \leq r, \mathbb{Z}^{d_j}[H_j] = \mathcal{D}_j[H_j]$. By collecting terms with equal powers of matrices H_j^n in the same vectors and using padding with zero vectors in each factor, if necessary, when exchanging $\oplus$ and the $\sum$ in radix expansions (see [20, (5),(6)]), one obtains

$$\mathbb{Z}^d[B] = \oplus_{j=1}^r \mathcal{D}_j[H_j] = (\oplus_{j=1}^r \mathcal{D}_j)[\oplus_{j=1}^r H_j] = \mathcal{D}[B]. \tag{18}$$

In other words, the digit system $(\oplus_{j=1}^r H_j, \oplus_{j=1}^r \mathcal{D}_j) = (B, \mathcal{D})$, and it has the finiteness property in $\mathbb{Z}^d[B]$. The dynamical system $\Phi = \oplus_{j=1}^r \Phi_j$ then performs the division with remainder by B in $\mathbb{Z}^d[B]$.

Case (b) is more subtle. By Corollary 2.10 and Lemma 4.2, for each (expanding or non-expanding) H_j of order $k_j \geq 2$ and dimension $d_j \times d_j$, there exists an integer digit set $\mathcal{D}_j \subset \mathbb{Z}^{d_j}$ containing $\mathbf{0}_{d_j}$, and a restricted dynamical system $\Phi_{\mathbf{r}, H_j} : \mathbb{Z}^{d_j} \to \mathbb{Z}^{d_j}$, that has attractor $\{\mathbf{0}_{d_j}\}$ in $\mathbb{Z}^{d_j}$. Then, one constructs the extended division function Ψ_j in $\mathbb{Z}^{d_j}[H_j]$, as in (10), that performs division with remainder by H_j in $\mathbb{Z}^{d_j}[H_j]$ with respect to $\mathcal{D}_j$. Then Ψ_j has attractor $\{\mathbf{0}_{d_j}\}$ in $\mathbb{Z}^{d_j}[H_j]$, and $\mathcal{D}_j[H_j] = \mathbb{Z}^{d_j}[H_j]$ by Lemma 2.9. From that point on, one takes the direct sum (18) over every $\mathcal{D}_j[H_j]$ as in case (a), only using the extended division Ψ_j in $\mathbb{Z}^{d_j}[H_j]$ in the place of Φ_j, whenever $k_j \geq 2$ and H_j is not expanding.

Thus, in both cases (a) or (b), one arrives to the situation $\mathbb{Z}^d[B] = \mathcal{D}[B]$, for some finite digit set $\mathcal{D} \subset \mathbb{Z}^d[A]$, which can be also be selected from $\mathbb{Z}^d$, if necessary. The last step is the

same as in the proof of [20, Theorem 2, p. 357], after conjugating with $T \in \mathbb{Z}^{d \times d}$, and using $TBT^{-1} = A$, one obtains $(T\mathbb{Z}^d)[A] = \mathcal{D}'[A]$, with $\mathcal{D}' = T\mathcal{D}$. As $T\mathbb{Z}^d \subset \mathbb{Z}^d$ is a sublattice, a set of residue class representatives $\mathcal{R}$ of $\mathbb{Z}^d/T\mathbb{Z}^d$ is finite, and $\mathbb{Z}^d = T\mathbb{Z}^d + \mathcal{R}$. This gives

$$\mathbb{Z}^d[A] = (T\mathbb{Z}^d + \mathcal{R})[A] = (T\mathbb{Z}^d)[A] + \mathcal{R}[A] = \mathcal{D}'[A] + \mathcal{R}[A] = \mathcal{D}''[A],$$

for the finite digit set $\mathcal{D}'' := \mathcal{D}' + \mathcal{R}$.

For the converse part of the Theorem 5.1, we proceed as in [22], [45], or [20]. Assume that $(A, \mathcal{D})$ has the finiteness property. Pick arbitrary $\mathbf{z} = \mathbf{d}_0 + A\mathbf{d}_1 + \cdots + A^k\mathbf{d}_k \in \mathcal{D}[A]$ and let $\mathbf{v} \in \mathbb{C}^d$ satisfy $\mathbf{v}^t A = \lambda \mathbf{v}^t$. If $|\lambda| < 1$, then $\mathbf{v}^t\mathbf{z} = \mathbf{v}^t\mathbf{d}_0 + \lambda\mathbf{v}^t\mathbf{d}_1 + \cdots \lambda^k\mathbf{v}^t\mathbf{d}_k$, As $\mathcal{D}$ is finite, pick $C > 0$, such that $\left|\mathbf{v}^t\mathbf{d}\right| < C$, for every $\mathbf{d} \in \mathcal{D}$. Then,

$$(\Re\mathbf{v})^t\mathbf{z} = \Re(\mathbf{v}^t\mathbf{z}) \leq \left|\mathbf{v}^t\mathbf{z}\right| < C(1 + |\lambda| + \cdots + |\lambda|^k) < C/(1 - |\lambda|).$$

In particular, this means that all integer vectors $\mathbb{Z}^d \subset \mathcal{D}[A]$ lie in a half-plane, as $\mathbb{Z}^d[A] = \mathcal{D}[A]$, but that is impossible. Therefore, every eigenvalue λ of A must be $|\lambda| \geq 1$. ∎

We now derive Theorem 5.2 from Theorem 5.1.

Proof of Theorem 5.2: Assume that no algebraic conjugate of α over $\mathbb{Q}$ is of absolute value < 1. Let $A = C(f) \in \mathbb{Q}^{d \times d}$ be the companion matrix of the minimal polynomial $f \in \mathbb{Z}[x]$ of α. As the eigenvalues of A are all ≥ 1 in absolute value then, according to Theorem 5.1, one can find a finite set $\mathcal{D} \subset \mathbb{Z}^d$, such that

$$\mathbb{Z}[A]\mathbf{e}_1 \subseteq \mathbb{Z}^d[A] = \mathcal{D}[A], \tag{19}$$

where $\mathbb{Z}[A]$ is the set of matrix polynomials in A with integer coefficients and the standard basis $\mathbf{e}_j \in \mathbb{Z}^d$, $1 \leq j \leq d$ satisfy $A\mathbf{e}_j = \mathbf{e}_{j+1}$, for $1 \leq j \leq d - 1$. Let $D \subset \mathbb{Z}^d$ denote the set of the integer coordinate vectors of the digits $\mathbf{d}_i = \sum_{j=1}^d d_{ij}\mathbf{e}_j \in \mathcal{D}$ w.r.t. the standard basis. Define the finite set $F := \underbrace{D + D + \cdots + D}_{d-\text{times}}$. Write $\mathbf{d}_i = \sum_{j=1}^d d_{ij}A^{j-1}\mathbf{e}_1$. For arbitrary $\mathbf{z} \in \mathcal{D}[A]$,

$$\mathbf{z} = \sum_{j=0}^k A^i\mathbf{d}_i = \sum_{i=0}^k A^i\left(\sum_{j=1}^d d_{ij}A^{j-1}\mathbf{e}_1\right) = \sum_{i=1}^{k+d} A^{i-1}\left(\sum_{j=1}^{\min\{d,i\}} d_{i-j,j}\mathbf{e}_1\right) = \sum_{j=1}^{k+d} f_iA^{i-1}\mathbf{e}_1,$$

where $f_i := \sum_{j=1}^{\min\{d,i\}} d_{i-j,j} \in F$. Hence, $\mathcal{D}[A] \subset F[A]\mathbf{e}_1$. In view of (19), $\mathbb{Z}[A]\mathbf{e}_1 \subseteq F[A]\mathbf{e}_1 \subseteq \mathbb{Z}[A]\mathbf{e}_1$, since $F \subset \mathbb{Z}$. Therefore, $\mathbb{Z}[A]\mathbf{e}_1 = F[A]\mathbf{e}_1$. Now pick the right eigenvector $\mathbf{v} \in \mathbb{C}^d$ of A, such that $\mathbf{v}^t\mathbf{e}_1 \neq 0$ (such $\mathbf{v}$ exists, because the companion matrix A of the minimal polynomial of $\alpha \neq 0$ is diagonalizable over $\mathbb{C}$ and invertible). Then $\mathbf{v}^t A = \alpha'\mathbf{v}$, where α' is algebraically conjugate to α over $\mathbb{Q}$. Since $\mathbf{v}^t\mathbb{Z}[A]\mathbf{e}_1 = \mathbb{Z}[\alpha']\mathbf{v}^t\mathbf{e}_1$, $\mathbf{v}^t F[A]\mathbf{e}_1 = F[\alpha']\mathbf{v}^t\mathbf{e}_1$, $\mathbf{v}^t\mathbf{e}_1 \neq 0$, we obtain $\mathbb{Z}[\alpha'] = F[\alpha']$. By applying the Galois automorphism $\alpha' \mapsto \alpha$, we find that $\mathbb{Z}[\alpha] = F[\alpha]$.

Conversely, assume that $\mathbb{Z}[\alpha] = F[\alpha]$ for some finite set $F \in \mathbb{C}$. Then, F is a subset of $\mathbb{Z}[\alpha]$ itself. Suppose that α has an algebraic conjugate over $\mathbb{Q}$ of absolute value < 1. We proceed in the same way as in the lattice digit system case. By taking Galois automorphism $\alpha \mapsto \alpha'$, we see that $\mathbb{Z}[\alpha'] = F'[\alpha']$, for some finite set $F' \subset \mathbb{Z}[\alpha']$. Therefore,

we can assume that α itself is of the absolute value < 1. Then, an arbitrary element of $\beta \in F[\alpha], \beta = f_0 + f_1\alpha + \cdots + f_n\alpha^n, f_j \in F$ is of absolute value at most

$$|\beta| \leq C(1 + |\alpha| + \cdots + |\alpha^n|) < C/(1 - |\alpha|),$$

where $C = \max_{f \in F} |f|$. This shows that $F[\alpha]$ is a bounded subset of $\mathbb{C}$, which is impossible, because it contains $\mathbb{Z}$, if $F[\alpha] = \mathbb{Z}[\alpha]$. ∎

6. Maximal integral sublattice of a rational lattice

For practical computations in Section 7, the auxiliary lattice of the form $\mathcal{L} = \mathbb{Z}^d \cap A\mathbb{Z}^d$ (that is, 'the integral part' of $A\mathbb{Z}^d$), where A is an invertible rational matrix, and the group of its coset representatives $\mathbb{Z}^d/\mathcal{L}$) play very important roles. In particular, $\mathbb{Z}^d/\mathcal{L}$ can be viewed as 'the approximation of the first order' to the group $A\mathbb{Z}^d[A]/\mathbb{Z}^d[A]$, hypothetically the smallest necessary subset of digits needed to represent elements of $\mathbb{Z}^d[A]$. Since it is desirable to control the size of a digit set we will need a formula for the basis matrix and the coset representatives of this auxiliary lattice $\mathcal{L}$ in $\mathbb{Z}^d$.

6.1. Review of lattices

We recall basic facts on lattices. An additive subgroup $\mathcal{L} \subset \mathbb{R}^d$ is called *a lattice*, if $\mathcal{L}$ is a uniformly discrete and relatively dense subset of $\mathbb{R}^d$. In this case, $\mathcal{L}$ is a free $\mathbb{Z}$- module of rank d and there exists a set $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_d\}$ of d linearly independent (over $\mathbb{R}$) vectors in $\mathbb{R}^d$ that generate $\mathcal{L}$ over $\mathbb{Z}$, so that $\mathcal{L} = \mathbb{Z}\mathbf{v}_1 + \mathbb{Z}\mathbf{v}_2 + \cdots + \mathbb{Z}\mathbf{v}_d$ ([46, Proposition 4.2 of Section 4]). This can be also written as $\mathcal{L} = L\mathbb{Z}^d$, where $L \in \mathbb{R}^{d \times d}$ denotes the basis matrix with columns $\mathbf{v}_1, \ldots, \mathbf{v}_d$. In particular, if $L \in \mathbb{Q}^{d \times d}$ or $L \in \mathbb{Z}^{d \times d}$, then $\mathcal{L}$ is called *rational*, or *integral* lattice, respectively. The matrix L is not unique and depends on the choice of the basis for $\mathcal{L}$. Two lattices $\mathcal{L} = L\mathbb{Z}^d$ and $\mathcal{M} = M\mathbb{Z}^d, L, M \in \mathbb{R}^d$, are nested $\mathcal{L} \subset \mathcal{M}$ if and only if L is left divisible by M in $\mathbb{Z}^{d \times d}$, i.e. if there exist an integer matrix $Q \in \mathbb{Z}^{d \times d}$, such that $L = MQ$. In particular, $\mathcal{L} = \mathcal{M}$ if and only if Q is *a unimodular* matrix, that is, $\det(Q) = \pm 1$; in that case $M = LQ^{-1}$. In particular, for any unimodular $Q \in \mathbb{Z}^{d \times d}$, one has $Q\mathbb{Z}^d = \mathbb{Z}^d$.

From the theory of the Smith Normal Form (SNF) [47,48], for an arbitrary invertible matrix $B \in \mathbb{Z}^{d \times d}$ there exist unimodular matrices $P, Q \in \mathbb{Z}^{d \times d}$, such that $B = PDQ^{-1}$, where $D = \mathrm{SNF}(B)$ is the unique diagonal matrix,

$$D = \begin{pmatrix} n_1 & 0 & \ldots & 0 \\ 0 & n_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & n_d \end{pmatrix}, \tag{20}$$

whose entries $n_1, \ldots, n_d$, called the *elementary divisors*, are positive integers satisfying the divisibility properties $n_1 \mid n_2, n_2 \mid n_3, \ldots, n_{d-1} \mid n_d$. The matrices P, Q, and D can be found by reducing the rows and columns of B through the integer division with remainder (which corresponds to invertible base transformations in $\mathbb{Z}^d$ and $\mathcal{L} = B\mathbb{Z}^d$). A few other facts on SNF that we will need further are summarized in Proposition 6.1.

Proposition 6.1: *Let* $\mathcal{L} = L\mathbb{Z}^d, L \in \mathbb{Z}^{d \times d}$ *be a lattice that has a* SNF *factorization* $L = PDQ^{-1}$. *Then* $\mathbb{Z}^d = L\mathbb{Z}^d + \mathcal{R}$, *where the* $\mathcal{R}$ *is the full set of coset representatives*

$$\mathcal{S} := \left\{ \sum_{i=1}^{d} j_i P \mathbf{e}_i, 0 \le j_i \le n_i - 1 \right\}. \tag{21}$$

Here, $\mathbf{e}_i, i = 1, \ldots, d$ *is the standard basis of* $\mathbb{Z}^d$ *and* n_i *are the elementary divisors from* $D = \mathrm{SNF}(L)$. *Consequently,* $[\mathbb{Z}^d : \mathcal{L}] = |\mathcal{R}| = n_1 \cdots n_d = |\det(D)| = |\det(L)|$.

Proof of Proposition 6.1: As D is diagonal, $\mathbb{Z}^d/D\mathbb{Z}^d \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_d}$ with the set of representatives $\mathcal{T} := \{\sum_{i=1}^{d} j_i \mathbf{e}_i, 0 \le j \le n_i - 1\}$. Hence, $\mathbb{Z}^d = D\mathbb{Z}^d + \mathcal{T}$. By the unimodularity of P and $Q, \mathbb{Z}^d = P\mathbb{Z}^d = PD\mathbb{Z}^d + P\mathcal{T} = PDQ^{-1}\mathbb{Z}^d + P\mathcal{T}$. Setting $\mathcal{S} := P\mathcal{T}$ we obtain $\mathbb{Z}^d = PDQ^{-1}\mathbb{Z}^d + P\mathcal{T} = L\mathbb{Z}^d + \mathcal{S}$. Notice that $P\mathbf{x} \in \mathbb{Z}^d$ belongs to $L\mathbb{Z}^d = PDQ^{-1}\mathbb{Z}^d = PD\mathbb{Z}^d$ if and only if $\mathbf{x} \in D\mathbb{Z}^d$, therefore $\mathbb{Z}^d/D\mathbb{Z}^d$ and $\mathbb{Z}^d/L\mathbb{Z}^d$ are isomorphic. The last statement follows. ■

6.2. A result on rational lattices

We turn our attention to rational lattices $\mathcal{L} = A\mathbb{Z}^d$, where $A \in \mathbb{Q}^{d \times d}$ is invertible. Let $q \in \mathbb{N}$ be a common denominator to the fractions that appear in the entries of A (not necessary the smallest one). Then $A = q^{-1}B$, where $B \in \mathbb{Z}^{d \times d}$. We are interested in the largest integral sub-lattice $\mathbb{Z}^d \cap \mathcal{L} = \mathbb{Z}^d \cap (q^{-1}B)\mathbb{Z}^d$.

Theorem 6.2: *Let* $B \in \mathbb{Z}^{d \times d}$ *have* SNF *factorization* $B = PDQ^{-1}$, *with elementary divisors* $n_1, \ldots, n_d$, *and let* $q \in \mathbb{N}$. *Then the matrices* $L = PN$ *and* $L' = LQ^{-1} = PNQ^{-1}$, *with*

$$N = \begin{pmatrix} n_1/\gcd(q, n_1) & 0 & \ldots & 0 \\ 0 & n_2/\gcd(q, n_2) & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & n_d/\gcd(q, n_d) \end{pmatrix}$$

where $n_1, n_2, \ldots, n_d$ *stands for the elementary divisors of* $D = \mathrm{SNF}(B)$, *are two possible basis matrices for the maximal integral sub-lattice* $\mathbb{Z}^d \cap \mathcal{L}$ *of the rational lattice* $\mathcal{L} := q^{-1}B\mathbb{Z}^d \subset \mathbb{Q}^d$. *The set*

$$\mathcal{S} = \left\{ \sum_{i=1}^{d} j_i P \mathbf{e}_i, 0 \le j_i < n_i/\gcd(n_i, q) \right\}$$

consists of all distinct coset representatives of $\mathbb{Z}^d/(\mathbb{Z}^d \cap \mathcal{L})$.

Proof of Theorem 6.2: Consider the scaled lattice $\mathcal{M} := q \cdot (\mathbb{Z}^d \cap \mathcal{L}) = q\mathbb{Z}^d \cap B\mathbb{Z}^d$. Then

$$\mathcal{M}' := P^{-1}\mathcal{M} = (qP^{-1})\mathbb{Z}^d \cap (P^{-1}B)\mathbb{Z}^d = (qP^{-1}\mathbb{Z}^d) \cap (P^{-1}B)\mathbb{Z}^d = q\mathbb{Z}^d \cap (P^{-1}B)\mathbb{Z}^d,$$

since $P^{-1}\mathbb{Z}^d = \mathbb{Z}^d$. Also, $(P^{-1}B)\mathbb{Z}^d = P^{-1}BQ\mathbb{Z}^d = D\mathbb{Z}^d$. Therefore, $\mathcal{M}' = q\mathbb{Z}^d \cap D\mathbb{Z}^d$. As $q\mathbb{Z}^d$ consists of vectors whose entries are divisible by q and $D\mathbb{Z}^d$ consists of vectors

whose ith entry is divisible by n_i by (20), $1 \leq i \leq d$, $q\mathbb{Z}^d \cap D\mathbb{Z}^d$ consists of vectors whose ith entry is divisible by $\mathrm{lcm}(q, n_i)$. In other words $\mathcal{M}' = C\mathbb{Z}^d$, where C is

$$C = \begin{pmatrix} \mathrm{lcm}(q, n_1) & 0 & \ldots & 0 \\ 0 & \mathrm{lcm}(q, n_2) & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \mathrm{lcm}(q, n_d) \end{pmatrix}.$$

Scaling back, $\mathbb{Z}^d \cap \mathcal{L} = q^{-1}\mathcal{M} = P(q^{-1}C)\mathbb{Z}^d = PN\mathbb{Z}^d = PNQ^{-1}\mathbb{Z}^d$. Therefore, one can take $L := PN$ or $L' = PNQ^{-1}$ to be the basis matrix of $\mathbb{Z}^d \cap \mathcal{L}$. Coset representatives are obtained from (21) in Proposition 6.1. ∎

In order to state the next result, recall that *the content* [49] of the polynomial $f(x) = a_d x^d + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ is defined by $c(f) := \gcd(|a_0|, |a_1|, \ldots, |a_n|)$. By the Gauss Lemma [49], for any two polynomials $f, g \in \mathbb{Z}[x]$, one has $\mathcal{C}(f \cdot g) = \mathcal{C}(f) \cdot \mathcal{C}(g)$.

Theorem 6.3: *Let $B \in \mathbb{Z}^{d \times d}$ be invertible and $q \in \mathbb{N}$. The index of the maximal integral sublattice $\mathbb{Z}^d \cap \mathcal{L}$ of $\mathcal{L} = q^{-1}B\mathbb{Z}^d$ in $\mathbb{Z}^d$ is*

$$[\mathbb{Z}^d : (\mathbb{Z}^d \cap \mathcal{L})] = \frac{|\det(B)|}{\mathcal{C}(\varphi_D(qx))},$$

where and $\varphi_D(x)$ is the characteristic polynomial of $D = \mathrm{SNF}(B)$.

Proof of Theorem 6.3: By Theorem 6.2,

$$[\mathbb{Z}^d : (\mathbb{Z}^d \cap \mathcal{L})] = \det N = \prod_{j=1}^{d} \frac{n_j}{\gcd(q, n_j)} = \frac{|\det(B)|}{\prod_{j=1}^{d} \gcd(q, n_j)}.$$

The content of $n_j - qx$ is exactly $\gcd(q, n_j)$. Since $\varphi_D(x) = \prod_{j=1}^{d}(n_j - x)$, one has $\prod_{j=1}^{d} \gcd(q, n_j) = \prod_{j=1}^{d} \mathcal{C}(n_j - qx) = \mathcal{C}(\varphi_D(qx))$. ∎

7. Numerical examples

We illustrate the main features of the theory of digit systems developed so far with examples.

7.1. Rotation digit system associated to smallest Pythagorean triple.

Consider the 2×2 matrix

$$A = \begin{pmatrix} 3/5 & -4/5 \\ 4/5 & 3/5 \end{pmatrix},$$

that corresponds to the Pythagorean triple $3^2 + 4^2 = 5^2$. This is a rotation by the angle $\theta = 53.1301023542\ldots^\circ$. We shall construct a small digit set $\mathcal{D}$, such that $(A, \mathcal{D})$ in $\mathbb{Z}^2[A]$ has the finiteness property.

First, we determine the basis for the auxiliary lattice $\mathcal{L} := \mathbb{Z}^2 \cap A\mathbb{Z}^2$. Let

$$B := 5A = \begin{pmatrix} 3 & -4 \\ 4 & 3 \end{pmatrix}.$$

Then, $\mathcal{L} = \mathbb{Z}^2 \cap A\mathbb{Z}^2 = \frac{1}{5}(5\mathbb{Z}^2 \cap B\mathbb{Z}^2)$. The SNF decomposition yields $B = PDQ^{-1}$ with

$$D = \begin{pmatrix} 1 & 0 \\ 0 & 25 \end{pmatrix}, \quad P = \begin{pmatrix} 7 & 1 \\ 1 & 0 \end{pmatrix}, \quad Q = \begin{pmatrix} 1 & 3 \\ -1 & -4 \end{pmatrix}.$$

with $\det P = \det Q = -1$. According to Theorem 6.2, $\mathcal{L} = L\mathbb{Z}^d$ with the basis matrix

$$L = PN = \begin{pmatrix} 7 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1/\gcd(5,1) & 0 \\ 0 & 25/\gcd(5,25) \end{pmatrix} = \begin{pmatrix} 7 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix} = \begin{pmatrix} 7 & 5 \\ 1 & 0 \end{pmatrix}.$$

One possible set of coset representatives of $\mathbb{Z}^2$ modulo $\mathcal{L}$ (equivalent to the one given in Theorem 6.2) is

$$\mathcal{S} = \mathbb{Z}^2/\mathcal{L} = \{0P\mathbf{e}_1 + 0P\mathbf{e}_2, 0P\mathbf{e}_1 + 1P\mathbf{e}_2, 0P\mathbf{e}_1 + 2P\mathbf{e}_2, 0P\mathbf{e}_1 + 3P\mathbf{e}_2, 0P\mathbf{e}_1 + 4P\mathbf{e}_2\} =$$
$$= \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 4 \\ 0 \end{pmatrix} \right\} =$$

After translating $\mathcal{S}$ by $-2\mathbf{e}_1$, we obtain an equivalent set of representatives with reduced coordinates:

$$\mathcal{R} := \mathcal{S} - 2\mathbf{e}_1 = U^{-1} = \left\{ \begin{pmatrix} -2 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \end{pmatrix} \right\} =$$
$$= \{-2\mathbf{e}_1, -\mathbf{e}_1, \mathbf{0}, \mathbf{e}_1, 2\mathbf{e}_1\}.$$

Next, we construct a *pre-periodic* digit set $\mathcal{D}'_r$ that has a good convex enclosure with respect to $\mathcal{R}$ as depicted as points in Figure 1.

Notice that the residues $\mathbf{e}_1$ and $2\mathbf{e}_1$ are the inner points of a triangle with vertices

$$\mathcal{T}_1 = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ -1 \end{pmatrix} \right\} \subset \mathcal{L}.$$

Likewise, $-\mathbf{e}_1, -2\mathbf{e}_1$ are the inner points of the triangle with vertices in $-\mathcal{T}_1$. The last residue $\mathbf{0}_2$ is an inner point of the triangle with vertices

$$\mathcal{T}_2 = \left\{ \begin{pmatrix} -2 \\ -1 \end{pmatrix}, \begin{pmatrix} -1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ -1 \end{pmatrix} \right\} \subset \mathcal{L}.$$
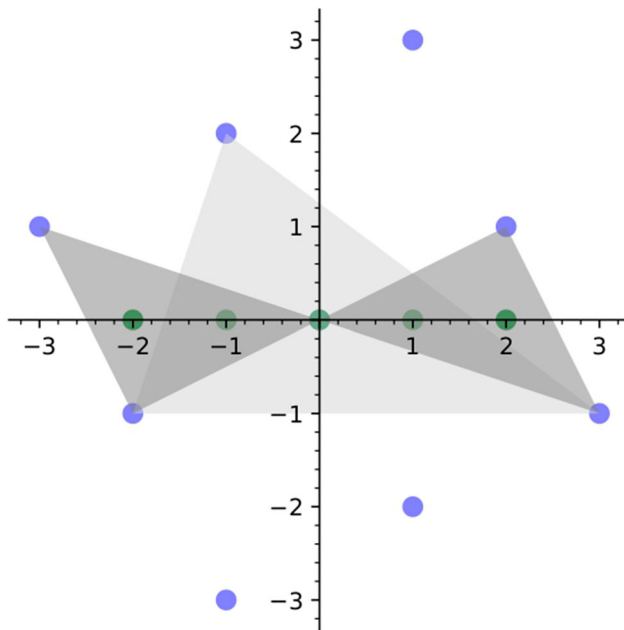
Figure 1. Points from $\mathcal{L} = \mathbb{Z}^2 \cap A\mathbb{Z}^2$ (blue) and from $\mathcal{R} = \mathbb{Z}^2/\mathcal{L}$ (green). Two dark grey triangles, namely, $\mathcal{T}_1$ and $-\mathcal{T}_1$ and one light grey triangle $\mathcal{T}_2$ with vertices in $\mathcal{L}$ enclose elements of $\mathcal{R}$.

Define the sets

$$\mathcal{D}(\mathbf{0}) := \mathbf{0} - \mathcal{T}_2 = \left\{ \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -2 \end{pmatrix}, \begin{pmatrix} -3 \\ 1 \end{pmatrix} \right\},$$

$$\mathcal{D}(\mathbf{e}_1) := \mathbf{e}_1 - \mathcal{T}_1 = \left\{ \begin{pmatrix} -1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -2 \\ 1 \end{pmatrix} \right\},$$

$$\mathcal{D}(-\mathbf{e}_1) := -\mathbf{e}_1 + \mathcal{T}_1 = \left\{ \begin{pmatrix} -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}.$$

$$\mathcal{D}(2\mathbf{e}_1) := 2\mathbf{e}_1 - \mathcal{T}_1 = \left\{ \begin{pmatrix} 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \end{pmatrix} \right\},$$

$$\mathcal{D}(-2\mathbf{e}_1) := -2\mathbf{e}_1 + \mathcal{T}_1 = \mathcal{T} \left\{ \begin{pmatrix} -2 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}.$$

As $\mathbf{0}_2$ is an inner point of these sets, their union

$$\mathcal{D}' = \bigcup_{\mathbf{x} \in \mathcal{R}} \mathcal{D}(\mathbf{x})$$

has good enclosure with respect to $\mathcal{R}$. By Theorem 3.9 and Remark 3.12, the division mapping $\Phi_r(\mathbf{x}) = A^{-1}(\mathbf{x} - \mathbf{d}_r(\mathbf{x}))$ with the digit $\mathbf{d}_r(\mathbf{x}) \in \mathcal{D}'$, restricted to $\mathbb{Z}^2$, has a finite attractor $\mathcal{A}_{\Phi_r}$ in $\mathbb{Z}^2$. To compute the set $\mathcal{A}_{\Phi_r}$, first notice that our matrix A is orthogonal (it is a rotation matrix): by taking the identity matrix $T = \mathbb{K}_2$ in the definition of A–invariant norm form on p.11, one obtains that the usual Euclidean norm $\|\ldots\|_2$ is A and

A^{-1}–invariant. To determine the attractor set $\mathcal{A}_{\Phi_r}$, one needs to find the repeller points $\mathbf{x} \in \mathbb{Z}^2$, such that $\|\Phi_r(\mathbf{x})\|_{A^{-1}} \geq \|\mathbf{x}\|_{A^{-1}}$ and then determine their orbits. In our case, we need to compute all the integral points in the feasible regions $\bigcup_{\mathbf{x} \in \mathcal{R}} \mathcal{V}(\mathbf{x})$, such that

$$\mathcal{V}(\mathbf{x}) := \{\mathbf{y} \in \mathbb{R}^n : \|\mathbf{x} - \mathbf{d}\| \geq \|\mathbf{x}\|, \forall \mathbf{d} \in \mathcal{D}'(\mathbf{x})\}.$$

By Corollary 3.7 the feasible regions $\mathcal{V}(\mathbf{x})$ are compact since $\mathcal{D}'$ has good enclosure with respect to $\mathcal{R}$. For each $\mathbf{x} \in \mathcal{R}$, we write down and solve the linear program that corresponds to $\mathcal{V}(\mathbf{x})$, as in the proof of Corollary 3.7. We use SAGE [50] Polyhedron and Mixed Integer Linear Programming (MILP) modules in a combination with PPL solver to explicitly solve for the feasible regions and enumerate the sets of contained integer points

$$\mathrm{Rep}_{\Phi_r}(\mathbf{x}) := \mathcal{V}(\mathbf{x}) \cap (\mathbf{x} + \mathcal{L}),$$

refer to Figure 2. Our calculations yield:

$$\mathrm{Rep}_{\Phi_r}(-2\mathbf{e}_1) = \left\{ \begin{pmatrix} -1 \\ -2 \end{pmatrix} \right\}, \quad \mathrm{Rep}_{\Phi_r}(2\mathbf{e}_1) = \left\{ \begin{pmatrix} 1 \\ 2 \end{pmatrix} \right\},$$

$$\mathrm{Rep}_{\Phi_r}(-\mathbf{e}_1) = \left\{ \begin{pmatrix} 0 \\ -2 \end{pmatrix} \right\}, \quad \mathrm{Rep}_{\Phi_r}(\mathbf{e}_1) = \left\{ \begin{pmatrix} 0 \\ 2 \end{pmatrix} \right\},$$

and

$$\mathrm{Rep}_{\Phi_r}(\mathbf{0}) = \left\{ \begin{pmatrix} -1 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -2 \\ -1 \end{pmatrix} \right\}.$$

The last step is to optimize the digit set by picking up the minimal possible number of representatives from the periods in orbits of points in $\mathrm{Rep}_{\Phi_r}(\mathbf{x})$. To find this minimal set, we compute the images

$$\Phi_r \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \Phi_r \begin{pmatrix} 0 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \quad \Phi_r \begin{pmatrix} 0 \\ -2 \end{pmatrix} = \Phi_r \begin{pmatrix} -2 \\ -1 \end{pmatrix} = \begin{pmatrix} -1 \\ -2 \end{pmatrix},$$

$$\Phi_r \begin{pmatrix} -1 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ -1 \end{pmatrix}, \quad \Phi_r \begin{pmatrix} 2 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

and,

$$\Phi_r \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \quad \Phi_r \begin{pmatrix} -1 \\ -2 \end{pmatrix} = \begin{pmatrix} -1 \\ -2 \end{pmatrix}.$$

Therefore, any orbit of a point $\mathbf{x} \in \mathbb{Z}^2$ eventually hits the set

$$\mathcal{P} = \left\{ \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} -1 \\ -2 \end{pmatrix} \right\}.$$

For the final digit set, we take

$$\mathcal{D} = \mathcal{D}' \cup \mathcal{P}.$$

It consists of 17 digits, all depicted in Figure 3. Any $\mathbb{Z}^2$ vector has a finite radix expansion in base A with digits $\mathcal{D}$. For instance, the radix expansion of $(6, -7)^t \in \mathbb{Z}^2$ is

$$\begin{pmatrix} 6 \\ -7 \end{pmatrix} = \begin{pmatrix} 1 \\ -2 \end{pmatrix} + A \begin{pmatrix} 1 \\ -1 \end{pmatrix} + A^2 \begin{pmatrix} -2 \\ 0 \end{pmatrix} + A^3 \begin{pmatrix} -1 \\ 1 \end{pmatrix} + A^4 \begin{pmatrix} 0 \\ 1 \end{pmatrix} + A^5 \begin{pmatrix} 1 \\ 2 \end{pmatrix} \in \mathcal{D}[A].$$
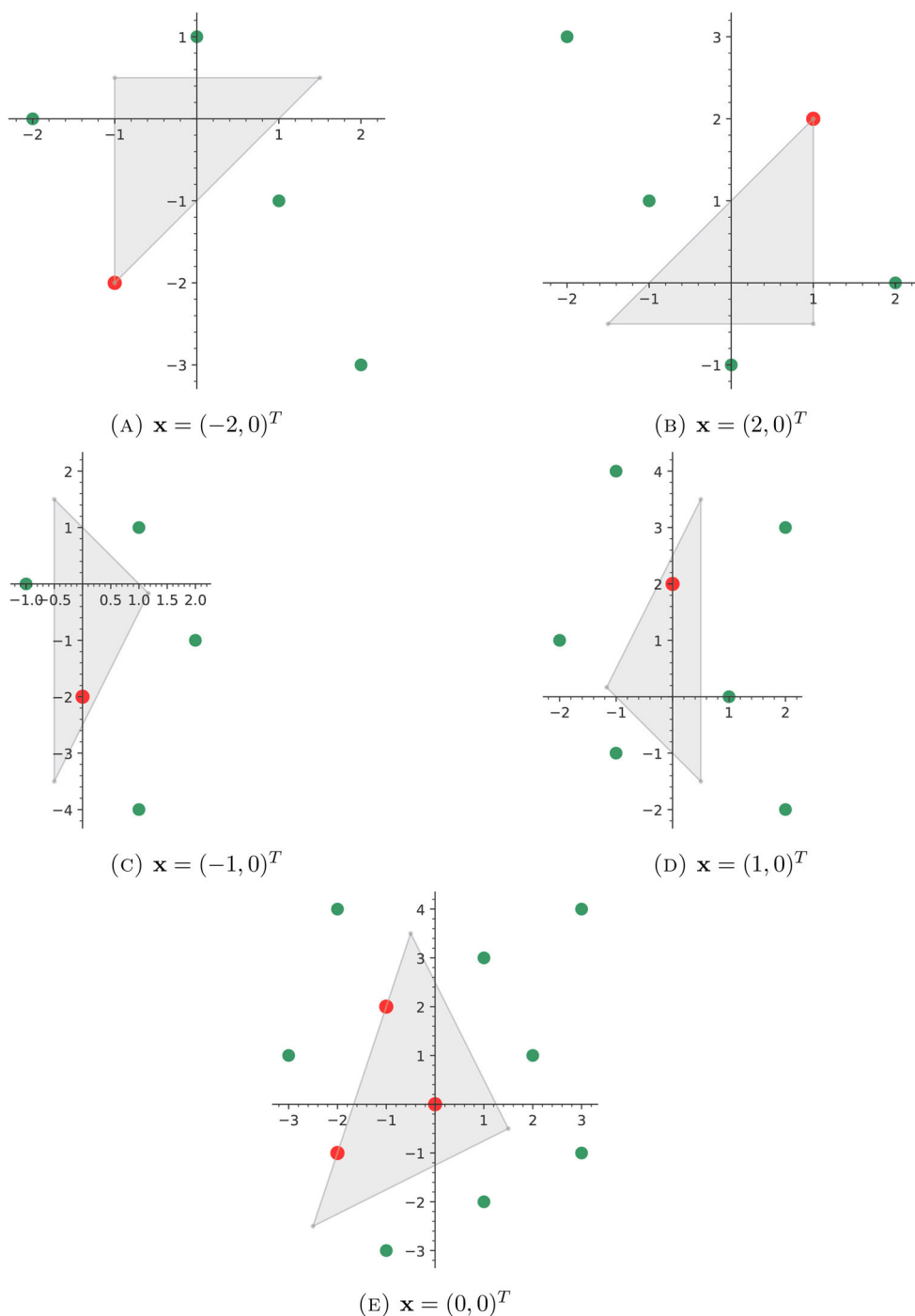
(A) $\mathbf{x} = (-2, 0)^T$

(B) $\mathbf{x} = (2, 0)^T$

(C) $\mathbf{x} = (-1, 0)^T$

(D) $\mathbf{x} = (1, 0)^T$

(E) $\mathbf{x} = (0, 0)^T$

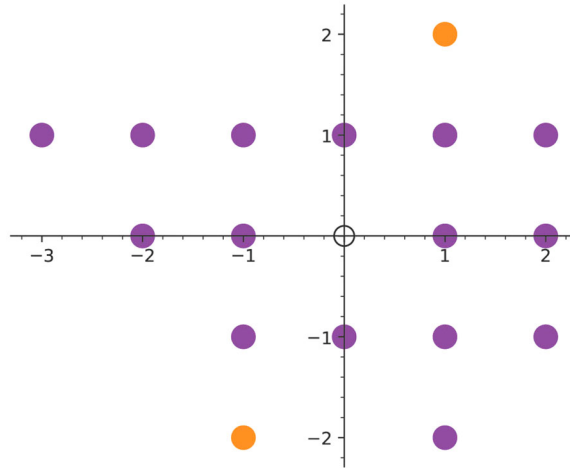**Figure 2.** Repeller points $\mathrm{Rep}_{\Phi_r}(\mathbf{x})$ (in red) inside the regions of repelling action of Φ_r (in grey), for each residue class $\mathbf{x} \in \mathbb{Z}^2/\mathcal{L}$. Green coloured are the remaining points from the same residue class $\mathbf{x} + \mathcal{L}$. (A) $\mathbf{x} = (-2, 0)^T$, (B) $\mathbf{x} = (2, 0)^T$, (C) $\mathbf{x} = (-1, 0)^T$, (D) $\mathbf{x} = (1, 0)^T$, (E) $\mathbf{x} = (0, 0)^T$.

Figure 3. The digit set $\mathcal{D}$: the initial digits $\mathcal{D}'$ (violet) and additional points from $\mathcal{A}_{\Phi_r}$ (orange) that represent periods; notice that $\mathbf{0}_2 \notin \mathcal{D}$.

It is remarkable that non-trivial rotational digit systems that possess the finiteness property in principle do not require zero digit $\mathbf{0}_d \in \mathcal{D}$. In the present example, the zero vector $\mathbf{0}_2$ is represented in $\mathcal{D}[A]$ as

$$\begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix} + A \begin{pmatrix} -2 \\ 1 \end{pmatrix}.$$

In some situations (like taking the twisted sums of the rotational digit systems), the artificial inclusion of $\mathbf{0}_d$ in $\mathcal{D}$ might be necessary, see Section 7.2.

The finite digital expansions of vectors from lattice from $\mathbb{Z}^2$ in the digit system $(A, \mathcal{D})$ yield the finite expansions of vectors from module $\mathbb{Z}^2[A]$. Let us illustrate the expansion process for the vector

$$v = \begin{pmatrix} -156/25 \\ -8/25 \end{pmatrix} = \begin{pmatrix} -3 \\ 0 \end{pmatrix} + A \cdot \begin{pmatrix} 0 \\ 2 \end{pmatrix} + A^2 \begin{pmatrix} -1 \\ 2 \end{pmatrix} \in \mathbb{Z}^2[A].$$

By applying the mappings $\mathbf{d}_r, \Phi_r$, one expresses $\begin{pmatrix} -3 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ 1 \end{pmatrix} + A \begin{pmatrix} -2 \\ 1 \end{pmatrix}$ and then carrying $\begin{pmatrix} -2 \\ 1 \end{pmatrix}$ forward and adding to $\begin{pmatrix} 0 \\ 2 \end{pmatrix}$ yields

$$v = \begin{pmatrix} -1 \\ 1 \end{pmatrix} + A \cdot \begin{pmatrix} -2 \\ 3 \end{pmatrix} + A^2 \begin{pmatrix} -1 \\ 2 \end{pmatrix}$$

Similarly, $\begin{pmatrix} -2 \\ 3 \end{pmatrix} = \begin{pmatrix} -1 \\ 1 \end{pmatrix} + A \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ gives

$$v = \begin{pmatrix} -1 \\ 1 \end{pmatrix} + A \cdot \begin{pmatrix} -1 \\ 1 \end{pmatrix} + A^2 \begin{pmatrix} 0 \\ 4 \end{pmatrix}$$

By replacing $\begin{pmatrix} 0 \\ 4 \end{pmatrix}$ in $\mathbb{Z}^2$ with its expansion in $\mathcal{D}[A]$, one finds

$$\begin{pmatrix} -156/25 \\ -8/25 \end{pmatrix} = \begin{pmatrix} -1 \\ 1 \end{pmatrix} + A \cdot \begin{pmatrix} -1 \\ 1 \end{pmatrix} + A^2 \begin{pmatrix} -1 \\ 1 \end{pmatrix} + A^3 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + A^4 \begin{pmatrix} 2 \\ -1 \end{pmatrix} \in \mathcal{D}[A].$$

It should be noted that, for this process to work, one must know at least one arbitrary (not necessarily the shortest one) representation of the form $\sum_{j=0}^{k-1} A^j \mathbf{z}_j, \mathbf{z}_j \in \mathbb{Z}^2[A]$ of the vector $v \in \mathbb{Z}^2[A]$ to perform the subsequent digital expansion.

7.2. Twisted sum of a rotational digit system with itself.

Consider the matrix

$$A = \begin{pmatrix} 0 & -1 \\ 1 & -1/2 \end{pmatrix},$$

that is a companion matrix to its characteristic polynomial $\varphi_A(x) = x^2 + x/2 + 1$. It is easy to see this is a generalized rotation: it is similar to a rotation matrix via the transformation

$$T = \begin{pmatrix} 4 & 0 \\ 1 & \sqrt{15} \end{pmatrix}, \quad T^{-1}AT = \begin{pmatrix} -1/4 & -\sqrt{15}/4 \\ \sqrt{15}/4 & -1/4 \end{pmatrix}.$$

The $\mathbb{R}^2$ norm $\|\mathbf{x}\|_{A^{-1}} = \left\| T^{-1}\mathbf{x} \right\|_{euclidean}$ is then A^{-1} invariant. Calculations similar to those in Section 7.1 yield the residue group with respect of the lattice

$$\mathcal{L} = \mathbb{Z}^2 \cap A\mathbb{Z}^2 = L\mathbb{Z}^2, \quad L = \begin{pmatrix} 2 & 2 \\ 1 & 0 \end{pmatrix}$$

is

$$\mathcal{R} = \mathbb{Z}^2/\mathcal{L} = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\}.$$

By enclosing these residue vectors inside the triangles with vertices

$$\mathcal{T}_1 := \left\{ \begin{pmatrix} -2 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ -1 \end{pmatrix} \right\}, \quad \mathcal{T}_2 := \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ -1 \end{pmatrix} \right\},$$

as depicted in Figure 4, one finds the pre–periodic digit set

$$\mathcal{D}\begin{pmatrix} 0 \\ 0 \end{pmatrix} := \begin{pmatrix} 0 \\ 0 \end{pmatrix} - \mathcal{T}_1, \quad \mathcal{D}\begin{pmatrix} 1 \\ 0 \end{pmatrix} := \begin{pmatrix} 1 \\ 0 \end{pmatrix} - \mathcal{T}_2,$$

$$\mathcal{D}' = \mathcal{D}\begin{pmatrix} 0 \\ 0 \end{pmatrix} \bigcup \mathcal{D}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \left\{ \begin{pmatrix} 2 \\ 0 \end{pmatrix}, \begin{pmatrix} -2 \\ -1 \end{pmatrix}, \begin{pmatrix} -2 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ -1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \end{pmatrix} \right\}.$$

Then $\Phi_{r,A}(\mathbf{x}) = A^{-1}(\mathbf{x} - \mathbf{d}_{r,A}(x))$ is ultimately periodic in $\mathbb{Z}^2$. The subsequent analysis of the repeller points, similar to the one in Section 7.1 carried out by solving corresponding
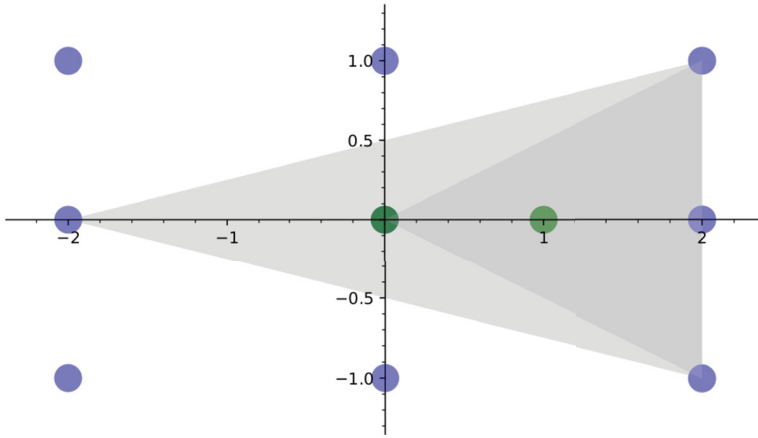
Figure 4. Points from $\mathcal{L} = \mathbb{Z}^2 \cap A\mathbb{Z}^2$ (blue) and from $\mathcal{R} = \mathbb{Z}^2/\mathcal{L}$ (green). Two triangles, namely, $\mathcal{T}_1$ (dark grey) and $\mathcal{T}_2$ (light grey) enclose $(0, 0)^T$ and $(0, 1)^T$, the elements of $\mathcal{R}$.

linear programs yields 11 integral repeller points

$$\mathrm{Rep}_{\Phi_{\mathrm{r},A}}$$

$$:= \left\{ \begin{pmatrix} 0 \\ -4 \end{pmatrix}, \begin{pmatrix} 0 \\ -3 \end{pmatrix}, \begin{pmatrix} 0 \\ -2 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 4 \end{pmatrix}, \begin{pmatrix} 2 \\ 5 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix} \right\},$$

as illustrated in Figure 5, (A) and (B). It turns out, the orbits of each repeller point already contains at least one digit of $\mathcal{D}'$ that is depicted in Figure 6. Therefore, the digit system $(A, \mathcal{D}')$ with 6 digits already has the finiteness property in $\mathbb{Z}^2[A]$.

Next we append the zero vector $\mathcal{D} = \mathcal{D}' \cup \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\}$. in order to construct the twisted sum of this digit system with itself. Consider the twisted sum $M = A \oplus_N A$, where

$$N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad M = A \oplus_N A = \begin{pmatrix} A & O_{2\times 2} \\ N & A \end{pmatrix} = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & -1/2 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1/2 \end{pmatrix}.$$

The matrix $M = H_2(\varphi_A)$ is an order–2 hypercompanion matrix to the polynomial $\varphi_A(x)$. Then the digit system $(M, \mathcal{D} \oplus \mathcal{D})$ has the finiteness property in $\mathbb{Z}^4$ by Lemma 4.1: the radix expansions in $\mathbb{Z}^4$ are done using the twisted mapping $\Phi_{\mathrm{r},M} = \Phi_{\mathrm{r},A} \oplus_N \Phi_{\mathrm{r},A}$ described in Section 4.1. For instance,

$$\begin{pmatrix} 1 \\ 2 \\ -3 \\ 4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ -1 \\ 1 \end{pmatrix} + M \begin{pmatrix} 2 \\ 0 \\ 2 \\ 0 \end{pmatrix} + M^2 \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + M^3 \begin{pmatrix} 0 \\ 0 \\ -2 \\ -1 \end{pmatrix} + M^4 \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

The finiteness property of $(M, \mathcal{D} \oplus \mathcal{D})$ extends to the whole module $\mathbb{Z}^4[M]$ through the mapping Ψ_M (10) by Corollary 2.10.
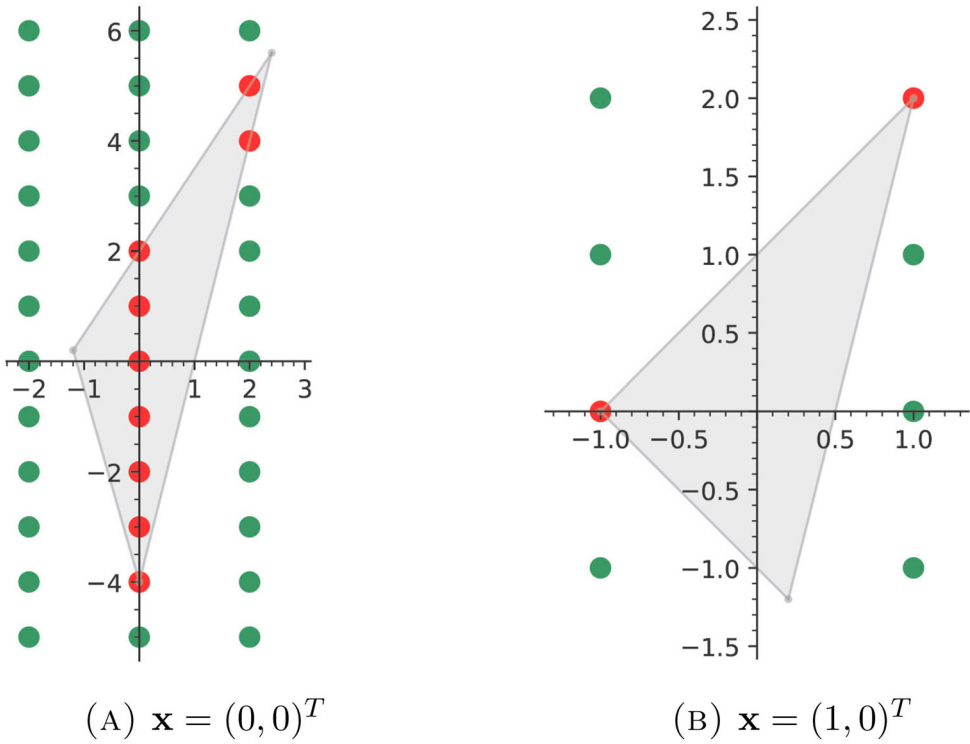
Figure 5. Repeller points $\mathrm{Rep}_{\Phi_{r,A}}(\mathbf{x})$ (in red) inside the regions of repelling action of $\Phi_{r,A}$ (in grey), for each residue class $\mathbf{x} \in \mathbb{Z}^2/\mathcal{L}$. Remaining points $\mathbf{x} + \mathcal{L}$ are coloured green. (A) $\mathbf{x} = (0,0)^T$, (B) $\mathbf{x} = (1,0)^T$.
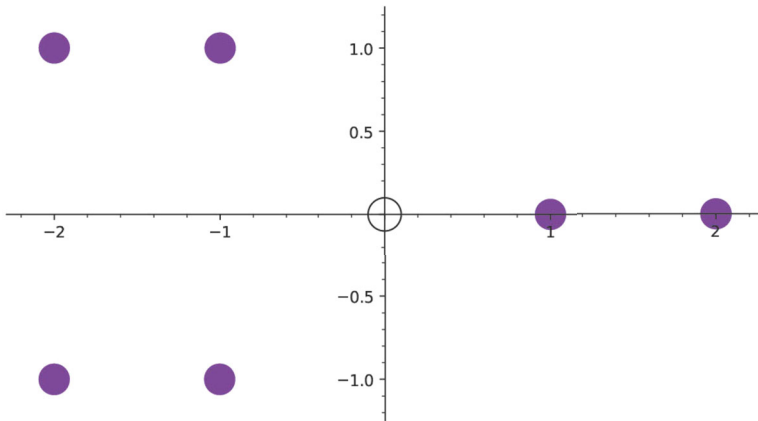

Figure 6. The digit set $\mathcal{D}'$ for which $(A, \mathcal{D}')$ has finiteness property in $\mathbb{Z}^2[A]$. Notice again that $\mathbf{0}_2 \notin \mathcal{D}'$.

The digit set $\mathcal{D} \oplus \mathcal{D}$ is not the smallest possible digit set for which the digit system that has M as its base matrix retains the finiteness property. It can be shown that it is possible to minimize the digit set size further in the following way. Use the digit set $\mathcal{D}_1 = \mathcal{D}' \oplus \mathcal{R}$

for vectors $\mathbf{x} \oplus \mathbf{y} \in \mathbb{Z}^4$ as long as $\mathbf{x} \neq \mathbf{0}_2$ and switch to the digit set $\mathcal{D}_2 = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\} \oplus \mathcal{D}'$ as soon as $\mathbf{x}$ becomes $= \mathbf{0}_2$ in the dynamical system $\Phi_{\mathrm{r},M}$. Such a digit system $(M, \mathcal{D}'')$ with the digit set $\mathcal{D}'' = \mathcal{D}_1 \cup \mathcal{D}_{r2}$ consists of 18 digits and has the finiteness porperty in $\mathbb{Z}^4[M]$. It's highly likely 18 is the minimal possible digit set size for which the finiteness property still holds in this particular base M.

The code for the examples provided in Section 7.1 and 7.2 is available to download online from [51].

8. Concluding remarks

We would like to conclude this paper by adding two open problems to the list of questions posed in [20] on the arithmetics of module $\mathbb{Z}^d[A]$.

Problem 8.1: *Let $\mathbf{x} \in \mathbb{Q}^d$ be such that every prime factor $p \in \mathbb{N}$ of the least common denominator of its coordinates divide the least common denominator of the entries in the matrix A. Is it true that such $\mathbf{x} \in \mathbb{Z}^d[A]$?*

Note that if there exists a prime number $p \in \mathbb{N}$, such that p divides the least common denominator of the coordinates of $\mathbf{x}$ and p does not divide the denominator of any entry of $A \in \mathbb{Q}^{d \times d}$ then it is clear that $\mathbf{x} \notin \mathbb{Z}^d[A]$.

Problem 8.2: *Let $A \in \mathbb{Q}^{d \times d}$ be non–degenerate. How to compute the stabilization index k_A in Lemma 2.3, namely, the smallest integer $k := k_A$, such that*

$$\mathbb{Z}^d \cap A\mathbb{Z}^d[A] = \mathbb{Z}^d \cap \mathbb{Z}_k^d[A] = \mathbb{Z}^d \cap \left(\mathbb{Z}^d + A\mathbb{Z}^d + \cdots + A^{k-1}\mathbb{Z}^d \right)?$$

We know how to find such k_A for certain classes of matrices A, but the general case seems to be tied deeply to the representations of lattices (i.e. discrete subgroups) in locally compact groups.

Let us conclude with one final remark. If $(A, \mathcal{D})$ is the classical standard digit system in $\mathbb{Z}^d$ for some expanding base matrix $A \in \mathbb{Z}^{d \times d}$ and some digit set $\mathcal{D} \subset \mathbb{Z}^d$, then the knowledge of the number of digits in the set $\mathcal{D}$ (which can be determined by observing the number of different symbols used in strings corresponding to radix expansions of random vectors) immediately yields the value of $|\det A|$. Thus, it determines the possible conjugacy classes of A in the group $\mathrm{GL}(d, \mathbb{Z})$. In contrast, for the rotational digit systems $(A, \mathcal{D})$, $A \in \mathbb{Q}^{d \times d}$ with Property (F), described in Section 3, the size of the digit set depends on the attractor set $\mathcal{A}_{\Phi_r}$, which in turn depends (in a complicated way) on the choice of the coset representatives and their convex enclosures. Therefore, the size of $\mathcal{D}$ alone does not reveal so much information about the base matrix A or its main characteristics, like the determinant or the dimension of A. It would be interesting to know if this could be useful in cryptography applications (in particular, for scrambling the messages and encoding data streams, cf. [7]).

Acknowledgements

Disclosure statement

Funding

ORCID

Jonas Jankauskas   http://orcid.org/0000-0001-9770-7632
Jörg M. Thuswaldner   http://orcid.org/0000-0001-5308-762X

References

[1] Kovács B, Pethő A. Canonical systems in the ring of integers. Publ Math Debr. 1983;30(1–2):39–45.

[2] Kovács B, Pethő A. Number systems in integral domains, especially in orders of algebraic number fields. Acta Sci Math (Szeged). 1991;55(3–4):287–299.

[3] Brunotte H. On trinomial bases of radix representations of algebraic integers. Acta Sci Math (Szeged). 2001;67(3–4):521–527.

[4] Evertse JH, Győry K, Pethő A, et al. Number systems over general orders. Acta Math Hungarica. 2019;159(1):187–205.

[5] Akiyama S, Pethő A. On canonical number systems. Theor Comput Sci. 2002;270(1–2):921–933.

[6] Akiyama S, Rao H. New criteria for canonical number systems. Acta Arith. 2004;111(1):5–25.

[7] Pethő A. On a polynomial transformation and its application to the construction of a public key cryptosystem. Computational Number Theory (Debrecen, 1989); 1991. p. 31–43.

[8] Scheicher K, Surer P, Thuswaldner JM, et al. Digit systems over commutative rings. Int J Number Theory. 2014;10(6):1459–1483.

[9] van de Woestijne CE. Number systems and the chinese remainder theorem; arXiv:1106.4219 [math.NT], 2011.

[10] Barat G, Berthé V, Liardet P, et al. Dynamical directions in numeration. Ann Inst Fourier (Grenoble). 2006;56(7):1987–2092. Numération, pavages, substitutions.

[11] Kovács A. Number expansions in lattices. Math Comput Model. 2003;38(7–9):909–915. Hungarian applied mathematics and computer applications.

[12] Vince A. Replicating tessellations. SIAM J Discrete Math. 1993;6(3):501–521.

[13] Akiyama S, Frougny C, Sakarovitch J. Powers of rationals modulo 1 and rational base number systems. Isr J Math. 2008;168(1):53–91.

[14] Kirat I, Lau KS, Rao H. Expanding polynomials and connectedness of self-affine tiles. Discrete Comput Geom. 2004;31(2):275–286.

[15] Lagarias JC, Wang Y. Integral self-affine tiles in $\mathbf{R}^n$. II. Lattice tilings. J Fourier Anal Appl. 1997;3(1):83–102.

[16] Steiner W, Thuswaldner JM. Rational self-affine tiles. Trans Am Math Soc. 2015;367(11):7863–7894.

[17] Akiyama S, Drungilas P, Jankauskas J. Height reducing problem on algebraic integers. Funct Approx Comment Math. 2012;47(part 1):105–119.

[18] Akiyama S, Thuswaldner JM, Zaïmi T. Comments on the height reducing property II. Indag Math (NS). 2015;26(1):28–39.

[19] Akiyama S, Zaïmi T. Comments on the height reducing property. Cent Eur J Math. 2013;11(9):1616–1627.

[20] Jankauskas J, Thuswaldner JM. Characterization of rational matrices that admit finite digit representations. Linear Algebra Appl. 2018;557:350–358.

[21] Grünwald V. Intorno all'aritmetica dei sistemi numerici a base negativa con particolare riguardo al sistema numerico a base negativo-decimale per lo studio delle sue analogie coll'aritmetica (decimale). Giornale di Matematiche di Battaglini. 1885;23:203–221. Errata, p. 367.

[22] Vince A. Radix representation and rep-tiling. In: Proceedings of the twenty-fourth southeastern international conference on combinatorics, graph theory, and computing (Boca Raton, FL, 1993); 1993. p. 199–212.

[23] Vince A. Rep-tiling Euclidean space. Aequationes Math. 1995;50(1–2):191–213.

[24] Gröchenig K, Haas A. Self-similar lattice tilings. J Fourier Anal Appl. 1994;1(2):131–170.

[25] Lagarias JC, Wang Y. Integral self-affine tiles in $\mathbf{R}^n$. I. Standard and nonstandard digit sets. J London Math Soc (2). 1996;54(1):161–179.

[26] Lagarias JC, Wang Y. Self-affine tiles in $\mathbf{R}^n$. Adv Math. 1996;121(1):21–49.

[27] Brin M, Stuck G. Introduction to dynamical systems. Cambridge: Cambridge University Press; 2015. Corrected paper back edition of the 2002 original [MR1963683].

[28] Farkas J. Theorie der einfachen Ungleichungen. J Reine Angew Math. 1902;124:1–27.

[29] Gale D, Kuhn HW, Tucker AW. Linear programming and the theory of games. Activity Analysis of Production and Allocation; 1951. p. 317–329. MR0046018.

[30] Gantmacher FR. The theory of matrices. Vols. 1, 2, New York: Chelsea Publishing Co; 1959. Translated by K. A. Hirsch.

[31] Reiersøl O. Rational orthogonal matrices. Am Math Mon. 1963;70(1):63–65.

[32] Liebeck H, Osborne A. The generation of all rational orthogonal matrices. Am Math Mon. 1991;98(2):131–133.

[33] Pall G. On the rational automorphs of $x_1^2 + x_2^2 + x_3^2$. Ann of Math (2). 1940;41(4):754–766.

[34] Sholander M. Rational orthogonal matrices. Am Math Mon. 1961;68:350. MR 124332.

[35] Cremona J. Letter to the editor. Am Math Mon. 1987;94(8):757–758.DOI:10.1080/00029890. 1987.12000713 .

[36] Du Val P. Homographies, quaternions and rotations. Oxford: Clarendon Press; 1964. (Oxford Mathematical Monographs).

[37] Mebius JE. A matrix-based proof of the quaternion representation theorem for four-dimensional rotations (unpublished electronic notes). (200502).

[38] Kovács A. Algorithmic construction of simultaneous number systems in the lattice of Gaussian integers. Ann Univ Sci Budapest Sect Comput. 2013;39:279–290.

[39] Kovács A. Simultaneous number systems in the lattice of Eisenstein integers. Ann Univ Sci Budapest Sect Comput. 2013;41:43–55.

[40] Kovács A. Number system constructions with block diagonal bases. Numeration and Substitution 2012; 2014. p. 205–213. MR3330567.

[41] Perlis S. Theory of matrices. New York: Dover Publications, Inc.; 1991. Reprint of the 1958 edition.

[42] Jacobson N. Lectures in abstract algebra. Vol. 2, Toronto-New York-London: D. Van Nostrand Co. Inc.; 1953. (Linear algebra).

[43] Hartwig RE. Roth's removal rule and the rational canonical form. Am Math Mon. 1996; 103(4):332–335.

[44] Bhattacharya PB, Jain SK, Nagpaul S. Basic abstract algebra. Cambridge, UK: Cambridge University Press; 2nd ed.; 1994.

[45] Gilbert WJ. Radix representations of quadratic fields. J Math Anal Appl. 1981;83(1):264–274.

[46] Neukirch J. Algebraic number theory. Berlin: Springer-Verlag; 1999. (Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]; Vol. 322). Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[47] Newman M. Integral matrices. New York-London: Academic Press; 1972. (Pure and Applied Mathematics, Vol. 45).

[48] Newman M. The Smith normal form. In: Proceedings of the fifth conference of the international linear Algebra society (Atlanta, GA, 1995); 1997. p. 367–381.

[49] Anderson DD. GCD domains, Gauss' lemma, and contents of polynomials. In: Chapman ST, Glaz S, editors. Non-Noetherian commutative ring theory; Boston (MA): Springer; p. 1–31. (Mathematics and its Applications, Vol. 520.) . DOI:10.1007/978-1-4757-3180-4_1.

[50] The Sage Developers. Sagemath, the Sage Mathematics Software System (Version 9.2.); 2021. Available from: https://www.sagemath.org.

[51] Jankauskas J. DigitSystems, a GitHub repository; 2021. Available from: git@github.com: jonas-jankauskas/DigitSystems.git.