Digit systems with rational base matrix over lattices

J. Jankauskas, J. Thuswaldner

Vilnius university, Montanuniversität Leoben

Lise Meitner Project M2259
February 1 2022
Sources


Classical (integer base) number systems

Let $\mathcal{D} = \{d_1, d_2, \ldots, d_k\} \subset \mathbb{Z}$ be finite; fix $a \in \mathbb{Z}$, $|a| \geq 2$. The finite sum

$$z = \varepsilon_k a^k + \varepsilon_{k-1} a^{k-1} + \cdots + \varepsilon_1 a + a_0 = \varepsilon_k \ldots \varepsilon_1 \varepsilon_0.$$

is called a (radix, or, digital) expansion of $z \in \mathbb{Z}$ in base $a$ and digits $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_k \in \mathcal{D}$.

Example: $62 = 2 + 10 \cdot 6 = 14 + 3 \cdot 16 = 3E_{16}$, 0 $2021 = 5615_{7}$.

The pair $(a, \mathcal{D})$ is called a (positional) number system in $S \subset \mathbb{Z}$, if each number $s \in S$ has a finite expansion.
Number systems for computers

With the advent of a digital computer, different digit systems were considered. The most simple – binary system \((2, \{0, 1\})\) was standardized by electronics industry.

- 1950 C. Shannon: *symmetric systems* (with *negative digits*).
- 1958 SSRS *Setun* computer, used balanced ternary \((3, \{-1, 0, 1\})\).

Figure: *Setun* computer

For optical computer, ternary is perfect (polarization!)
Number systems with complex bases $\alpha$ in place of $a$:

- 1960: D. Knuth $(2i, \{0, 1, 2, 3\})$.
- 1965: D. Penney $(-1 + i, \{0, 1\})$.


A number $\alpha \in \mathbb{C}$ is an algebraic integer, if it is a root of the monic polynomial with integer coefficients:

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$$

For instance, $\alpha = -1 + i$, $p(x) = x^2 + 2x + 2$. 
N.S. in algebraic number rings

- The order \( \mathbb{Z}[\alpha] \) is a simplest ring generated by 1 and \( \alpha \):
  \[
  \mathbb{Z}[\alpha] = \{ b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}, b_j \in \mathbb{Z}, 0 \leq j < n \}. 
  \]
  For instance, \( \mathbb{Z}[-1 + i] = \mathbb{Z}[i] \) - Gaussian integers.

- Let \( \mathcal{D} \subset \mathbb{Z}[\alpha] \) be finite digit set, (typically, \( \mathcal{D} \subset \mathbb{Z} \)). N.s. \((\alpha, \mathcal{D})\) is defined in the same way as in rational integer case: just replace \( a \) by \( \alpha \).

- In 1990-present: many different variants of n.s. in number fields and more abstract polynomial rings (canonical, symmetric n.s.) were considered by Akiyama, Kovács, Pető, Scheicher, Steiner, Surer, Thuswaldner, Woestijne, Zaïmi, and many many other authors.
Motivation

- Applications:
  - Representation of complicated algebraic structures in computer hardware (CPU) and software (computer algebra systems)
  - Faster/more reliable data transmission
  - Cryptography
Motivation II: beauty of mathematics

1970 D. Knuth ir C. Davis:

Figure: Elements of $\mathbb{Z}[i]$ with representations in n.s. $(-1 + i, \{0, 1\})$ of fixed length. Source: https://bentrubewriter.com

One can think of n.s. as the ways to write elements of locally compact groups (i.e., $p$-adic numbers $\mathbb{Z}_p$).
Digit systems \((A, \mathcal{D})\) in lattices


- **Base**: \(A \in M_n(\mathbb{Z}) - n \times n\) integer matrix.

- **Digit set**: \(\mathcal{D} = \{d_1, \ldots, d_k\} \subset \mathbb{Z}^n\)

- **Digit system**: the pair \((A, \mathcal{D})\) with the set of possible radix expansions of finite length:
  \[
  \mathcal{D}[A] = \{ \epsilon_0 + A\epsilon_1 + \cdots + A^{l-1}\epsilon_{l-1}, \epsilon_j \in \mathcal{D} \}.
  \]

- **Finiteness**: \(\forall z \in \mathbb{Z}^n, z = \overline{\epsilon_{l-1}\epsilon_{l-2}\cdots\epsilon_0}, \epsilon_j \in \mathcal{D}\).
  \[
  \mathcal{D}[A] = \mathbb{Z}^n.
  \]

- **Uniqueness**: \(\overline{\epsilon_{l-1}\epsilon_{l-2}\cdots\epsilon_0} = \overline{\delta_{k-1}\delta_{k-2}\cdots\delta_0} \iff k = l, \delta_j = e_j\).

- **Standard d.s.**: both (F) and (U) holds (some authors also require \(0_n \in \mathcal{D}\)).
Facts about D.S. \((A, D)\) in lattices \(\mathbb{Z}^d\).

- **Necessary conditions** for standard d. s.
  - \(A\) must be **expanding**: \(\forall\) eigenvalue \(|\lambda| > 1\);
  - \(\det (I_d - A) \neq \pm 1\);
  - \(D = \mathbb{Z}^n / A\mathbb{Z}^n = D\), and \(#D = |\det A|\).

- If \(A\) is expanding, there always \(\exists\) some finite set \(D \in \mathbb{Z}^n\), s.t. \((A, D)\) has property (F). **Note**: such a D.S. will be, in general, not standard.

- The mapping \(\Phi : \mathbb{Z}^n \mapsto \mathbb{Z}^n\)

\[
\Phi(x) = A^{-1}(x - d(x)),
\]

with the digit function

\[
d : \mathbb{Z}^n \mapsto D, d(x) \equiv x \pmod{A\mathbb{Z}^n}.
\]

has finite attractor set in \(\mathbb{Z}^n\).
Example of standard D.S. in $\mathbb{Z}^2$

- Standard d.s. in $\mathbb{Z}^2$:

\[
A = \begin{pmatrix} 0 & -2 \\ 1 & -2 \end{pmatrix}, \quad D = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\}.
\]

- $(A, D)$ generalize n.s. $(\alpha, \mathcal{E})$ in orders (take $A$ to be companion matrix of $\alpha$ with $D = \{\varepsilon e_1, \varepsilon \in \mathcal{E}\}$

- $\mathbb{Z}^n$ is not a ring (this means no digit wise multiplication $(A, D)$, unless specially defined for appropriate $A$ and $D$).
Generalizing finiteness result for \((A, D)\).

- We allow \(A \in M_n(\mathbb{Q})\), also with eigenvalues \(|\lambda| = 1\).
- Minimal \(A\)-invariant \(\mathbb{Z}\)-module that contains \(\mathbb{Z}^n\):

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

**Theorem 1 (J.J. & J.T.)**

Let \(A\) be an \(n \times n\) matrix with rational entries. There is a digit set \(D \subset \mathbb{Z}^n[A]\) that makes \((A, D)\) a digit system in \(\mathbb{Z}^n[A]\) with finiteness property iff \(A\) has no eigenvalue \(\lambda\) with \(|\lambda| < 1\). The digit set \(D\) can even be chosen to be a subset of \(\mathbb{Z}^n\).

**Note:** Thm. 1 is based on (and generalizes) an earlier result of Akiyama, Thuswaldner, Zaïmi from 2015.
Goals

- Earlier proofs were indirect (using n.s.)
- We are interested in pure-matrix proof of Property (F)
- We need linear algebra machinery for actual computations
Key difficulties

▫ When $|\lambda| = 1$, $A^{-1}$ not contractive; if $\lambda$ not a root of unity, infinite orbits $\{A^{-n}x, x \in \mathbb{R}^n\}$ show up.

▫ When $A$ contains Jordan blocks $J(\lambda)$ of order $\geq 2$, $|\lambda| = 1$, unbounded orbits show up, i.e.

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \quad A^{-n}x = \begin{pmatrix} x_1 - nx_2 \\ x_2 \end{pmatrix}$$

▫ When $A \not\in M_n(\mathbb{Z})$, usually $\mathbb{Z}^n[A] \subset \mathbb{R}^n$ no longer a lattice, for instance, $\mathbb{Z}[3/2]$.

▫ The residue group of $\mathbb{Z}^n[A]/A\mathbb{Z}^n[A]$ is now much more difficult to compute!
Define the auxiliary lattice and its simplified residue set by

\[ \mathcal{L} = \mathbb{Z}^n \cap A\mathbb{Z}^n, \quad \mathcal{R} = \mathbb{Z}^n / \mathcal{L}. \]

\[ \mathcal{R} \] is much simpler and contains \( \mathbb{Z}^d[A] / A\mathbb{Z}^d[A] \).

**Theorem 2 (J. T. & J. J.)**

Tegul \( B \in \mathbb{Z}^{n \times n} \) be non degenerate, and let \( A = q^{-1}B \), where \( q \in \mathbb{N} \). Then:

\[
\# \mathcal{R} = [\mathbb{Z}^n : \mathcal{L}] = \frac{|\det(B)|}{\text{cont}(\phi_D(qx))},
\]

where \( \varphi_D(x) \) is the char. polynomial of \( D = \text{SNF}(B) \) and \( \text{cont}(\varphi_D(qx)) \) denotes the g.c.d. of its coefficients.
Restricted and extended remainder division

- **Restricted division** (preserves \( \mathbb{Z}^n \)):
  \[
  d_r : \mathbb{Z}^n \mapsto \mathcal{R}, \quad d_r(x) \equiv x \pmod{\mathcal{L}}.
  \]
  \[
  \Phi_r : \mathbb{Z}^n \mapsto \mathbb{Z}^n, \quad \Phi_r(x) = A^{-1}(x - d_r(x)).
  \]

- **Extended division** \( \Psi : \mathbb{Z}^d[A] \mapsto \mathbb{Z}^d[A] \)
  \[
  \Psi(z_0 + \cdots + A^n z_n) = d_r(z_0) + A(z_1 + \Phi_r(z_1)) + \cdots + A^n z_n.
  \]

- If matrix \( A \) is expanding, then \( \Phi \) and \( \Psi \) have finite attractors, and this can be used to produce the digit systems in \( \mathbb{Z}^d[A] \) that have property (F) as in classical case.
D.S. with (F) for Rotation Matrices

- For practical computation of D.S. with (F), one needs effective version of 2015 result of Akiyama, Thuswaldner and Zaïmi.
- A real matrix $A \in M_n(\mathbb{Q})$ is called **general rotation**, if it is fully diagonalizable over $\mathbb{C}$ and all eigenvalues $\lambda \in \mathbb{C}$ of $A$ are of absolute value $|\lambda| = 1$.
- If $A$ is a general rotation, $\exists Q \in M_n(\mathbb{R})$, such that $Q^{-1}AQ$ takes block–diagonal form with blocks

  $$(\pm 1), \quad \left( \begin{array}{cc} \cos \phi & -\sin \phi \\ \sin \phi & \cos \phi \end{array} \right)$$

- $A^{-1}$–invariant norm on $\mathbb{R}^n$ is defined by

  $$\|x\|_{A^{-1}} = \left\| Q^{-1}x \right\|_{\text{Euclidean}}, \quad \left\| A^{-1}x \right\|_{A^{-1}} = \|x\|_{A^{-1}}.$$


Digit sets with *good* convex enclosure

A digit set $\mathcal{D} \subset \mathbb{Z}^n$ is said to have a **good enclosure** with respect to $\mathcal{R}$, when, for every $r \in \mathcal{R}$, the interior of the convex hull of

$$\mathcal{D}(r) := \{ d \in \mathcal{D} : d \equiv r \pmod{L} \}.$$ 

contains the origin $0_n$.

**Division function** $\Phi_r : \mathbb{Z}^n \mapsto \mathbb{Z}^n$ by

$$\Phi_r(x) := A^{-1}(x - d_r(x)).$$

with **reminder function** $r(x) : \mathbb{Z}_k[A] \mapsto \mathcal{D}$

$$d_r(x) = \begin{cases} 
  d_r(x) \equiv x \pmod{\mathcal{R}}; \\
  \text{minimizes } \|x - d_r(x)\|_{A^{-1}} \text{ in } \mathcal{D};
\end{cases}$$
New results

Theorem 3 (J.J. & J. Thuswaldner)
Let $A \in \mathbb{Q}^{n \times n}$ be generalized rotation and suppose that $D \subset \mathbb{Z}^n$ has a good convex enclosure with respect to $\mathcal{R} = \mathbb{Z}^n / \mathcal{L}$. Then the division mapping $\Phi_r : \mathbb{Z}^n \rightarrow \mathbb{Z}^n$ has finite attractor $A_{\Phi_r} \subset \mathbb{Z}^n$: $\Phi_r$ is ultimately periodic with a finite number of possible smallest periods all of which lie in $\mathbb{Z}^n$.

Consequence: The d.s. $(A, D')$ with a digits set $D' = D \cup A_{\Phi_r}$ has Property (F) in $\mathbb{Z}^d[A]$ (Hint: apply extended division $\Psi$ to elements of $\mathbb{Z}^d[A]$ – it has the same attractor as $\Phi_r$).
Example I (beginning)

- The 2 × 2 matrix

\[ A = \begin{pmatrix} 3/5 & -4/5 \\ 4/5 & 3/5 \end{pmatrix}, \quad (3/5)^2 + (4/5)^2 = 1. \]

- This is a rotation by the angle

\[ \theta = 53.1301 \ldots \degree \]

that is not a rational multiple of \( 2\pi \).

- Since \( A \) is orthogonal, \( \|x\|_{A^{-1}} = \|x\|_{\text{Euclidean}}, \quad Q = 1_2. \)
Example 1: residue set $\mathcal{R}$

- Auxiliary lattice $\mathcal{L} = \mathbb{Z}^2 \cap A\mathbb{Z}^2$ has the basis $\mathcal{L} = T\mathbb{Z}^2$:

  $$T := \begin{pmatrix} 7 & 5 \\ 1 & 0 \end{pmatrix}.$$ 

- The residue set

  $$\mathcal{R} := \mathbb{Z}^2 / L\mathbb{Z}^2 = \left\{ \begin{pmatrix} -2 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \end{pmatrix} \right\} = \{ -2\mathbf{e}_1, -\mathbf{e}_1, \mathbf{0}_2, \mathbf{e}_1, 2\mathbf{e}_1 \}.$$ 

- **Remark**: $\mathbb{Z}^2 / \mathcal{L}\mathbb{Z}^2$ is of prime order 5, $\mathcal{R}$ is actually a full residue group for $\mathbb{Z}^2[A] / A\mathbb{Z}^2[A]$. 
Example: convex enclosure of $R$:

Figure: Lattice $\mathcal{L} = \mathbb{Z}^2 \cap A\mathbb{Z}^2$ (blue), residue set $R = \mathbb{Z}^2 / \mathcal{L}$ (green). Triangles (grey and light grey) with vertices in $\mathcal{L}$ that enclose $R$ with vertices $T_1, -T_1, T_2 \subset \mathcal{L}$. 
Example I: convex digit set $\mathcal{D}$ (pre-periodic)

- $\mathcal{D}(0_2) := 0_2 - \mathcal{T}_2 = \{(2, 1), (1, -2), (-3, 1)\}$
- $\mathcal{D}(e_1) := e_1 - \mathcal{T}_1 = \{(-1, -1), (1, 0), (-2, 1)\}$
- $\mathcal{D}(-e_1) := -e_1 + \mathcal{T}_1 = \{(-1, 0), (2, -1), (1, 1)\}$
- $\mathcal{D}(2e_1) := 2e_1 - \mathcal{T}_1 = \{(0, -1), (2, 0), (-1, 1)\},$
- $\mathcal{D}(-2e_1) := -2e_1 + \mathcal{T}_1 = \mathcal{T} \{(−2, 0), (1, −1), (0, 1)\}$.
- **Pre-periodic** digit set is defined

$$\mathcal{D}' := \bigcup_{r \in \mathcal{R}} \mathcal{D}(r)$$

has good enclosure.
Example I continued: attractor set in $\mathbb{Z}^2$

Figure: Attractor points $\text{Attr}_{\Phi_r}(r)$ (red) for each residue class $r \in \mathbb{Z}^2/\mathcal{L}$. Green colored are points from $r + \mathcal{L}$.

(a) $r = (-2, 0)^T$

(b) $r = (2, 0)^T$
Example I continued: attractor set in $\mathbb{Z}^2$

Figure: Attractor points $\text{Attr}_{\Phi_r}(r)$ (red) for each $r \in \mathbb{Z}^2 / \mathcal{L}$. Green colored are points from $r + \mathcal{L}$.

(a) $r = (-1, 0)^T$

(b) $r = (1, 0)^T$
Example 1 continued: attractor set in $\mathbb{Z}^2$

\begin{figure}
\centering
\includegraphics[width=\textwidth]{attractor_set}
\caption{$r = (0, 0)^T$}
\end{figure}

**Figure:** Attractor points $\text{Attr}_{\Phi, r}(r)$ (red) for each $r \in \mathbb{Z}^2 / \mathcal{L}$. Green colored are points from $r + \mathcal{L}$. 
Example I continued: optimizing the final digit set

- \( \Phi_r(0, 0) = \Phi_r(0, 2) = (1, 2) \),
  \( \Phi_r(0, -2) = \Phi_r(-2, -1) = (-1, -2) \),
  \( \Phi_r(-1, 2) = (2, -1) \),
  \( \Phi_r(2, -1) = (0, 0) \),
  \( \Phi_r(1, 2) = (1, 2) \),
  \( \Phi_r(-1, -2) = (-1, -2) \).

- \( \forall x \in \mathbb{Z}^n, \Phi^k_r(x) \) always visits
  \[ \mathcal{P} = \{(1, 2), (-1, -2)\} \].

- Final digit set
  \[ \mathcal{D} = \mathcal{D}' \cup \mathcal{P}, \]
Figure: Final digit set $\mathcal{D}$: Pre-periodic digits (violet) and periodic digits (orange); Note that $0_2 \notin \mathcal{D}$ and $\#\mathcal{D} = 17.$
Th. 3: Idea of proof

- For any \( x \in \mathbb{Z}^n \), \( \exists k_0 : \Phi_r^k(x) \in \mathbb{Z}^n \) for \( k > k_0 \).
- \( \Phi_r(x) \) pulls/pushes/doesn’t move \( x \in \mathbb{Z}^n \) to/from \( 0_d \):
  - \( \| \Phi_r(x) \|_{A^{-1}} < \| x \|_{A^{-1}} \), \( \| \Phi_r(x) \|_{A^{-1}} \geq \| x \|_{A^{-1}} \)
  - \( \forall r \in D(x) : \| x - r \|_{A^{-1}} \geq \| x \|_{A^{-1}} \)
- Set \( y := Q^{-1}x \), \( v := Q^{-1}r \).
  - \( \| y - v \| \geq \| y \| \), \( \| y \|^2 - 2v^T y + \| v \|^2 \geq \| y \|^2 \)
  - It reduces to : \( v^T y \leq \| v \|^2 / 2 \)
- Inequalities \( \forall r \in D(x) : My \leq b \), \( M \in \mathbb{R}^{m \times n} \), \( b \in \mathbb{R}^m \).
Lemma 4

The set \( \{ y \in \mathbb{R}^n : My \leq b \} \) where \( M \in M_n(\mathbb{R}) \) and \( b \in \mathbb{R}^n_{\geq 0} \) is compact iff \( 0_m \) is an interior point of the \( \text{Conv(rows}(M)) \).
Semi-direct (twisted) sums of d.s., I

Let $A \in \mathbb{Q}^{m \times m}$, $B \in \mathbb{Q}^{n \times n}$ be non-degenerate, $O \in \mathbb{Q}^{m \times n}$ – zero matrix, and $C \in \mathbb{Z}^{n \times m}$.

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

For two d.s. $(A, D_A)$ and $(B, D_B)$ one defines:

$$d_{r,A} : \mathbb{Z}^m \rightarrow D_A, \quad d_{r,A}(x) \equiv x \pmod{\mathbb{Z}^d \cap A\mathbb{Z}^d}, \quad (1)$$
$$\Phi_{r,A} : \mathbb{Z}^m \rightarrow \mathbb{Z}^m, \quad \Phi_{r,A}(x) = A^{-1}(x - d_{r,A}(x)), \quad (2)$$
$$d_{r,B} : \mathbb{Z}^n \rightarrow D_B, \quad d_{r,B}(y) \equiv y \pmod{\mathbb{Z}^d \cap B\mathbb{Z}^d}, \quad (3)$$
$$\Phi_{r,B} : \mathbb{Z}^n \rightarrow \mathbb{Z}^n, \quad \Phi_{r,B}(y) = B^{-1}(y - d_{r,B}(y)), \quad (4)$$

for every $x \in \mathbb{Z}^m$, $y \in \mathbb{Z}^n$. These mappings perform ‘remainder division’ in $\mathbb{Z}^m$ and $\mathbb{Z}^n$, respectively.
New d.s. \((M, \mathcal{D}_A \oplus \mathcal{D}_B)\) in \(\mathbb{Z}^m \oplus \mathbb{Z}^n = \mathbb{Z}^{m+n}\):

\[d_{r,M} = d_{r,A} \oplus_c d_{r,B}, \quad d_{r,M}(z) \equiv z \pmod{\mathbb{Z}^{m+n} \cap M\mathbb{Z}^{m+n}}\]

\[d_{r,M}(z) := \begin{pmatrix} d_{r,A}(x) \\ d_{r,B}(y - C \cdot \Phi_{r,A}(x)) \end{pmatrix},\]

‘Twisted’ remainder division \(\Phi_{r,M} := \Phi_{r,A} \oplus_c \Phi_{r,B}\) in \(\mathbb{Z}^{m+n}\) performs ‘carry’ from 1st component to 2nd:

\[\Phi_{r,M} : \mathbb{Z}^{m+n} \to \mathbb{Z}^{m+n}, \quad \Phi_{r,M}(z) := M^{-1}(z - d_{r,M}(z)).\]

**Lemma 5**

Suppose that \(0_m \in \mathcal{D}_A, 0_n \in \mathcal{D}_B\), and the attractors of the linear mappings \(\Phi_{r,A}, \Phi_{r,B}\) in \(\mathbb{Z}^m\) and \(\mathbb{Z}^n\) are \(\{0_m\}, \{0_n\}\), respectively. Then the attractor of \(\Phi_{r,M} = \Phi_{r,A} \oplus_c \Phi_{r,B}\) is \(\{0_{m+n}\} \subset \mathbb{Z}^{m+n}\). In this case, \((M, \mathcal{D}_A \oplus \mathcal{D}_B)\) in \(\mathbb{Z}^{m+n}[M]\), where \(M = A \oplus_c B\) has Property \((F)\).
The companion matrix of $x^2 + x/2 + 1$

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

$A$ is generalized rotation:

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

$A^{-1}$-invariant norm $\|x\|_{A^{-1}} = \|T^{-1}x\|_2.$
Example II - Twisted d.s.: beginning

- Auxiliary lattice:

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

- Residue group:

\[ \mathcal{R} = \mathbb{Z}^2 / \mathcal{L} = \{(0, 0), (1, 0)\} \]
Example II: the digit set

- Pre-periodic digit set:

\[ D' = \{(2, 0), (-2, -1), (-2, 1), (1, 0), (-1, -1), (-1, 1)\} . \]

- Attractor points:

\[
(0, -4), (0, -3), (0, -2), (0, -1), (0, 0), \\
(0, 1), (0, 2), (2, 4), (2, 5), (-1, 0), (1, 2)
\]
Example II: attractor points
Example II: twisted d.s.

\[
(A, D'):
\]

![Graph](image)

- We take \( D = D' \cup \{(0, 0)\} \)

\[
M = A \oplus_N A = \begin{pmatrix} A & O_{2 \times 2} \\ N & A \end{pmatrix} = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & -1/2 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1/2 \end{pmatrix}.
\]
Example II continued: twisted d.s.

- Twisted d.s. \((M, D \oplus D)\) has 49 digits:

- Pvz.

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

- We can optimize \(D \oplus D\) down to 18 digits:

\[
D'' = (D' \oplus R) \bigcup ((0, 0) \oplus D')
\]
Open problems

Problem 1
Let $A \in M_n(\mathbb{Q})$. Does there exist an algorithm to check whether a given vector $u \in \mathbb{Q}^n$ belongs to $\mathbb{Z}^n[A]$ or not? (Maybe even a practical algorithm)?

Problem 2
Suppose a matrix $A \in M_n(\mathbb{Q})$ has eigenvalues $\lambda$ with $|\lambda| \geq 1$, and at least one eigenvalue is of absolute value $|\lambda| = 1$. Is it true that a digit system $(A, D)$ in $\mathbb{Z}^n[A]$ that has finiteness property does not admit unique representation property?

Problem 3
Suppose again that $A$ satisfies all the assumptions of P2, and that $(A, D)$ in $\mathbb{Z}^n[A]$ has the finiteness property. What is the smallest possible size $\#D$ of the digit set?
The End

Thank you!