Digit systems with rational base matrix over lattices

J. Jankauskas, J. Thuswaldner

Vilnius university, Montanuniversität Leoben

Lise Meitner Project M2259

February 1 2022

Sources

- J. J. & J .M. Thuswaldner, *Characterization of rational matrices that admit digit systems with the finiteness property*, Linear Algebra and its Applications, **557** (2018), 350–358. arXiv: `https://arxiv.org/abs/1801.01839`
- J. J. & J .M. Thuswaldner, *Rational matrix digit systems*, Linear and Multilinear Algebra (to appear), `https://arxiv.org/abs/2107.14168`
- L. Rossi, W. Steiner, J. M. Thuswaldner, *Rational self-affine tiles associated to standard and nonstandard digit systems* `https://arxiv.org/abs/2110.09112`

Classical (integer base) number systems

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

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

  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: $62 = 2 + 10 \cdot 6 = 14 + 3 \cdot 16 = 3E_{16}$, o $2021 = 5615_7$.
- 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 $(3, \{-1, 0, 1\})$.



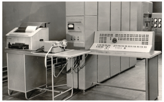


Figure: `Setun` computer

  - For optical computer, ternary is perfect (polarization!)

N.S. in algebraic number rings, I

- Number systems with complex bases α in place of *a*:
  - 1960: D. Knuth $(2i, \{0, 1, 2, 3\})$.
  - 1965: D. Penney $(-1 + i, \{0, 1\})$.
- 1975, 1980–1990: Kátai, Szabó, Kovács, Indlekofer, Gilbert ir kt. defined and studied number systems in orders of algebraic number fields.
- A number $\alpha \in \mathbb{C}$ is an algebraic integer, if it is a root of the monic polynomial with integer coefficients:

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

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 α:

  $$\mathbb{Z}[\alpha] = \{b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^n, b_j \in \mathbb{Z}, 0 \leqslant j < n\}.$$

  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 α.
- 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 sturctures 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:

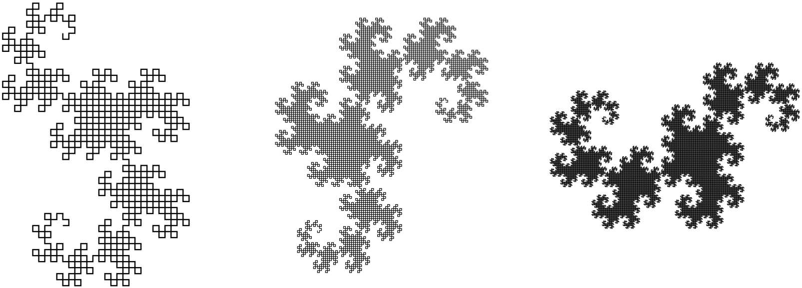


Figure: Elements of $\mathbb{Z}[i]$ with representations in n.s. $(-1+i, \{0,1\})$ of fixed length. Source: https://bentrubewriter.com

- 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

- A. Vince, *Replicating tessellations*, SIAM J. Discrete Math. **6** (3) (1993).
- **Base**: $A \in M_n(\mathbb{Z})$ – $n \times n$ integer matrix.
- **Digit set**: $\mathcal{D} = \{\mathbf{d}_1, \ldots, \mathbf{d}_k\} \subset \mathbb{Z}^n$
- **Digit system:** the pair $(A, \mathcal{D})$ with the set of possible radix expansions of finite length:

$$\mathcal{D}[A] = \left\{\boldsymbol{\epsilon}_0 + A\boldsymbol{\epsilon}_1 + \cdots + A^{l-1}\boldsymbol{\epsilon}_{l-1}, \boldsymbol{\epsilon}_j \in \mathcal{D}\right\}.$$

- **Finiteness**: $\forall \mathbf{z} \in \mathbb{Z}^n$, $\mathbf{z} = \overline{\boldsymbol{\epsilon}_{l-1}\boldsymbol{\epsilon}_{l-2}\ldots\boldsymbol{\epsilon}_0}, \boldsymbol{\epsilon}_j \in \mathcal{D}$.

$$\mathcal{D}[A] = \mathbb{Z}^n.$$

- **Uniqueness**: $\overline{\boldsymbol{\epsilon}_{l-1}\boldsymbol{\epsilon}_{l-2}\ldots\boldsymbol{\epsilon}_0} = \overline{\boldsymbol{\delta}_{k-1}\boldsymbol{\delta}_{k-2}\ldots\boldsymbol{\delta}_0} \iff$

$$k = l, \boldsymbol{\delta}_j = \mathbf{e}_j.$$

- **Standard d.s.**: both (F) and (U) holds (some authors also require $\mathbf{0}_n \in \mathcal{D}$).

Facts about D.S. $(A, \mathcal{D})$ in lattices $\mathbb{Z}^d$.

- **Necessary conditions** for standard d. s.
  - A must be **expanding**: $\forall$ eigenvalue $|\lambda| > 1$;
  - $\det(I_d - A) \neq \pm 1$;
  - $\mathcal{D} = \mathbb{Z}^n / A\mathbb{Z}^n = \mathcal{D}$, and $\#\mathcal{D} = |\det A|$.
- If A is expanding, there always $\exists$ some finite set $\mathcal{D} \in \mathbb{Z}^n$, s.t. $(A, \mathcal{D})$ has property (F). **Note**: such a D.S. will be, in general, not standard.
- The mapping $\Phi : \mathbb{Z}^n \mapsto \mathbb{Z}^n$

$$\Phi(\mathbf{x}) = A^{-1}(\mathbf{x} - \mathbf{d}(\mathbf{x})),$$

with the digit function

$$\mathbf{d} : \mathbb{Z}^n \mapsto \mathcal{D}, \mathbf{d}(\mathbf{x}) \equiv \mathbf{x} \pmod{A\mathbb{Z}^n}.$$

has finite attractor set in $\mathbb{Z}^n$.

Example of standard D.S. in $\mathbb{Z}^2$

.

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

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

- $(A, \mathcal{D})$ generalize n.s. $(\alpha, \mathcal{E})$ in orders (take A to be companion matrix of α with $\mathcal{D} = \{\varepsilon \mathbf{e}_1, \varepsilon \in \mathcal{E}\}$
- $\mathbb{Z}^n$ is not a ring (this means no digit wise multiplication $(A, \mathcal{D})$, unless specially defined for appropriate A and $\mathcal{D}$).

Generalizing finiteness result for $(A, \mathcal{D})$.

- 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 $\mathcal{D} \subset \mathbb{Z}^n[A]$ that makes $(A, \mathcal{D})$ a digit system in $\mathbb{Z}^n[A]$ with finiteness property iff A has no eigenvalue λ with $|\lambda| < 1$. The digit set $\mathcal{D}$ 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 λ not a root of unity, infinite orbits $\{A^{-n}\mathbf{x}, \mathbf{x} \in \mathbb{R}^n\}$ show up.
- When A contains Jordan blocks $J(\lambda)$ of order $\geqslant 2$, $|\lambda| = 1$, **unbounded orbits** show up, i.e.

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

- When $A \notin M_n(\mathbb{Z})$, 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!

Auxiliary lattice

- Define the auxiliary lattice and its simplified residue set by

$$\mathcal{L} = \mathbb{Z}^n \cap A\mathbb{Z}^n, \qquad \mathcal{R} = \mathbb{Z}^n/\mathcal{L}.$$

- $\mathcal{R}$ 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:

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

where $\varphi_D(x)$ is the char. polynomial of $D = \mathrm{SNF}(B)$ and $cont(\varphi_D(qx))$ denotes the g.c.d. of its coefficients.

Restricted and extended remainder division

- Restricted division (preserves $\mathbb{Z}^n$):

$$\mathbf{d}_r : \mathbb{Z}^n \mapsto \mathcal{R}, \qquad \mathbf{d}_r(\mathbf{x}) \equiv \mathbf{x} \pmod{\mathcal{L}}.$$

$$\Phi_r : \mathbb{Z}^n \mapsto \mathbb{Z}^n, \qquad \Phi_r(\mathbf{x}) = A^{-1}(\mathbf{x} - \mathbf{d}_r(\mathbf{x}))$$

- *Extended division* $\Psi : \mathbb{Z}^d[A] \mapsto \mathbb{Z}^d[A]$

$$\Psi(\mathbf{z}_0 + \cdots + A^n \mathbf{z}_n) = \mathbf{d}_r(\mathbf{z}_0) + A(\mathbf{z}_1 + \Phi_r(\mathbf{z}_1)) + \cdots + A^n \mathbf{z}_n.$$

- If matrix A is expanding, then Φ and Ψ have finite attractors, and this can be used to produce the digit systems in $\mathbb{Z}^d[A]$ that have propety (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

$$(\pm 1), \qquad \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix}$$

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

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

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 $\mathbf{r} \in \mathcal{R}$, the interior of the convex hull of

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

contains the origin $\mathbf{0}_n$.
- **Division function** $\Phi_r : \mathbb{Z}^n \mapsto \mathbb{Z}^n$ by

$$\Phi_r(\mathbf{x}) := A^{-1}(\mathbf{x} - \mathbf{d}_r(\mathbf{x})).$$

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

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

New results

Theorem 3 (J.J. & J. Thuswaldner)

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

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

Example I (beginning)

- The 2×2 matrix

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

- This is a rotation by the angle

$$\theta = 53.1301\ldots^\circ$$

that **is not a rational multiple of** 2π.

- Since A is orthogonal, $||\mathbf{x}||_{A^{-1}} = ||\mathbf{x}||_{\text{Euclidean}}$, $Q = \mathbf{1}_2$.

Example I: 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 $\mathcal{R}$:

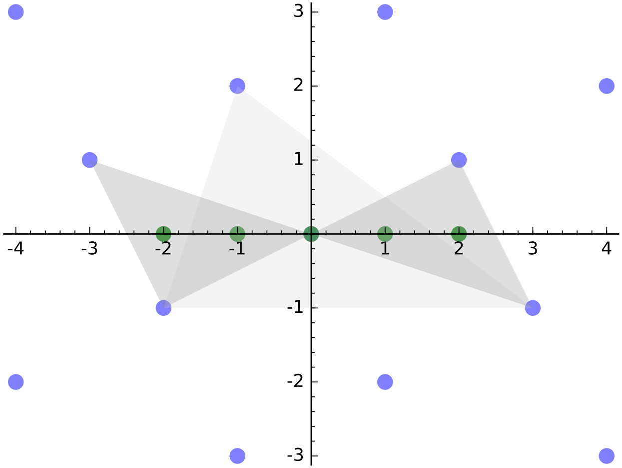


Figure: Lattice $\mathcal{L} = \mathbb{Z}^2 \cap A\mathbb{Z}^2$ (blue), residue set $\mathcal{R} = \mathbb{Z}^2/\mathcal{L}$ (green). Triangles (grey and light grey) with vertices in $\mathcal{L}$ that enclose $\mathcal{R}$ with vertices $\mathcal{T}_1, -\mathcal{T}_1, \mathcal{T}_2 \subset \mathcal{L}$.

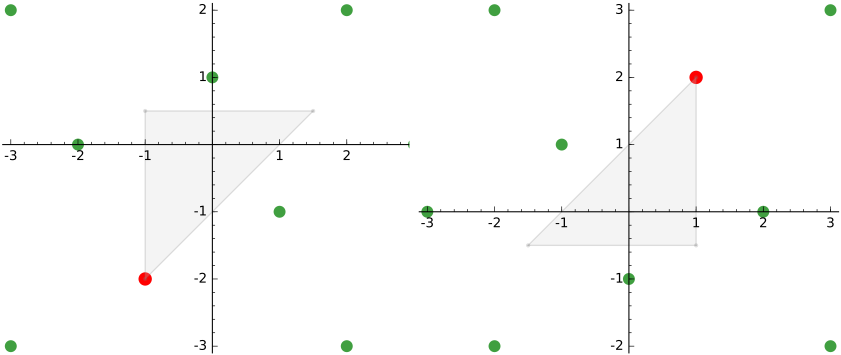
Example I: convex digit set $\mathcal{D}$ (pre-periodic)

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

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

has **good enclosure**.

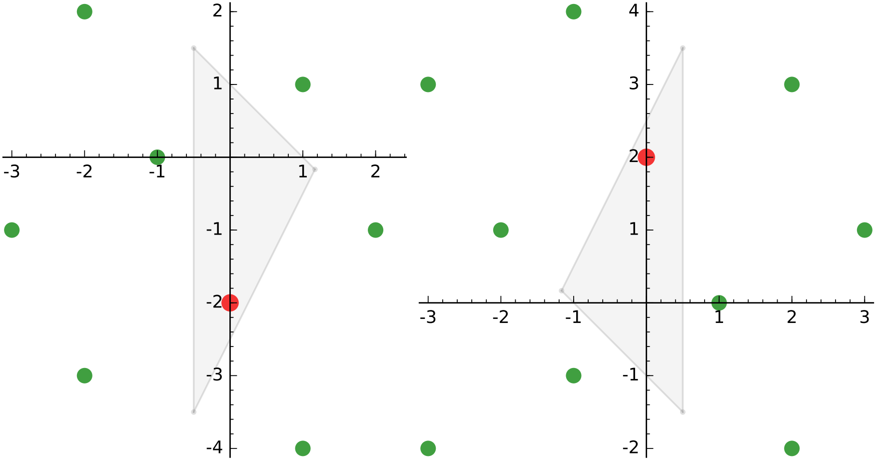
Example I continued: attractor set in $\mathbb{Z}^2$



(a) $\mathbf{r} = (-2, 0)^T$ (b) $\mathbf{r} = (2, 0)^T$

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

Example I continued: attractor set in $\mathbb{Z}^2$

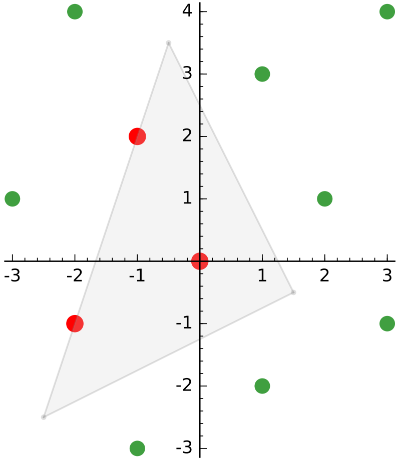


(a) $\mathbf{r} = (-1, 0)^T$

(b) $\mathbf{r} = (1, 0)^T$

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

Example I continued: attractor set in $\mathbb{Z}^2$



(a) $\mathbf{r} = (0,0)^T$

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

Example I continued: optimizing the final digit set

- $\Phi_r(0,0) = \Phi_r(0,2) = (1,2)$,
  $\Phi_r(0,-2) = \Phi_r(-2,-1) = (-1,-2)$,
  $\Phi_r(-1,2) = (2,-1)$, $\Phi_r(2,-1) = (0,0)$,
  $\Phi_r(1,2) = (1,2)$, $\Phi_r(-1,-2) = (-1,-2)$.
- $\forall \mathbf{x} \in \mathbb{Z}^n$, $\Phi_r^k(\mathbf{x})$ always visits

$$\mathcal{P} = \{(1,2), (-1,-2)\}.$$

- **Final digit set**

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

Example (end)

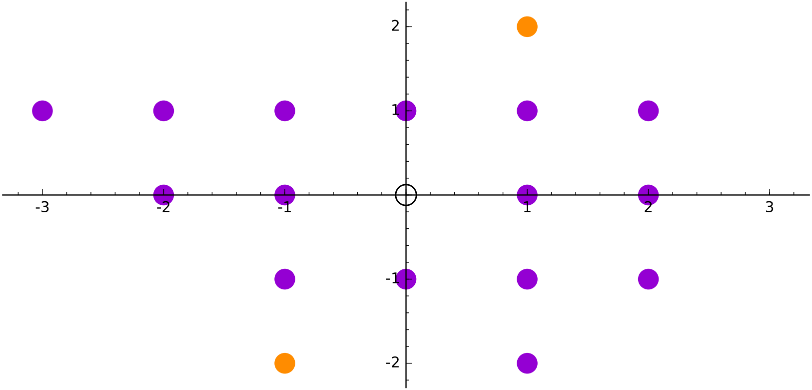


Figure: Final digit set $\mathcal{D}$: Pre-periodic digits (violet) and periodic digits (orange); Note that $\mathbf{0}_2 \notin \mathcal{D}$ and $\#\mathcal{D} = 17$.

Th. 3: Idea of proof

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

Th. 3: Heart of proof

Lemma 4

The set $\{\mathbf{y} \in \mathbb{R}^n : M\mathbf{y} \leqslant \mathbf{b}\}$ *where* $M \in M_n(\mathbb{R})$ *and* $\mathbf{b} \in \mathbb{R}^n_{\geqslant 0}$ *is compact iff* $\mathbf{0}_m$ *is an interior point of the* $Conv(rows(M))$*.*

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 $C \in \mathbb{Z}^{n\times m}$.

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

- For two d.s. $(A, \mathcal{D}_A)$ and $(B, \mathcal{D}_B)$ one defines:

$$\begin{aligned}
\mathbf{d}_{\mathrm{r},A} &: \mathbb{Z}^m \to \mathcal{D}_A, & \mathbf{d}_{\mathrm{r},A}(\mathbf{x}) &\equiv \mathbf{x} \pmod{\mathbb{Z}^d \cap A\mathbb{Z}^d}, & (1)\\
\Phi_{\mathrm{r},A} &: \mathbb{Z}^m \to \mathbb{Z}^m, & \Phi_{\mathrm{r},A}(\mathbf{x}) &= A^{-1}(\mathbf{x} - \mathbf{d}_{\mathrm{r},A}(\mathbf{x})), & (2)\\
\mathbf{d}_{\mathrm{r},B} &: \mathbb{Z}^n \mapsto \mathcal{D}_B, & \mathbf{d}_{\mathrm{r},B}(\mathbf{y}) &\equiv \mathbf{y} \pmod{\mathbb{Z}^d \cap B\mathbb{Z}^d}, & (3)\\
\Phi_{\mathrm{r},B} &: \mathbb{Z}^n \mapsto \mathbb{Z}^n, & \Phi_{\mathrm{r},B}(\mathbf{y}) &= B^{-1}(\mathbf{y} - \mathbf{d}_{\mathrm{r},B}(\mathbf{y})), & (4)
\end{aligned}$$

for every $\mathbf{x} \in \mathbb{Z}^m$, $\mathbf{y} \in \mathbb{Z}^n$. These mappings perform ‘remainder division’ in $\mathbb{Z}^m$ and $\mathbb{Z}^n$, respectively.

Semi-direct (twisted) sums of d.s., II

- New d.s. $(M, \mathcal{D}_A \oplus \mathcal{D}_B)$ in $\mathbb{Z}^m \oplus \mathbb{Z}^n = \mathbb{Z}^{m+n}$:

$$\mathbf{d}_{r,M} = \mathbf{d}_{r,A} \oplus_c \mathbf{d}_{r,B}, \qquad \mathbf{d}_{r,M}(\mathbf{z}) \equiv \mathbf{z} \pmod{\mathbb{Z}^{m+n} \cap M\mathbb{Z}^{m+n}}$$

$$\mathbf{d}_{\mathrm{r},M}(\mathbf{z}) := \begin{pmatrix} \mathbf{d}_{\mathrm{r},A}(\mathbf{x}) \\ \mathbf{d}_{\mathrm{r},B}\left(\mathbf{y} - C \cdot \Phi_{\mathrm{r},A}(\mathbf{x})\right) \end{pmatrix},$$

- '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:

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

Lemma 5

Suppose that $\mathbf{0}_m \in \mathcal{D}_A$, $\mathbf{0}_n \in \mathcal{D}_B$, and the attractors of the linear mappings $\Phi_{\mathrm{r},A}$, $\Phi_{\mathrm{r},B}$ in $\mathbb{Z}^m$ and $\mathbb{Z}^n$ are $\{\mathbf{0}_m\}$, $\{\mathbf{0}_n\}$, respectively. Then the attractor of $\Phi_{\mathrm{r},M} = \Phi_{\mathrm{r},A} \oplus_c \Phi_{\mathrm{r},B}$ is $\{\mathbf{0}_{m+n}\} \subset \mathbb{Z}^{m+n}$. 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).

Example II - Twisted d.s.: beginning

- The companion matrix of $x^2 + x/2 + 1$

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

- A is generalized rotation:

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

- A^{-1}-invariant norm $||\mathbf{x}||_{A^{-1}} = ||T^{-1}\mathbf{x}||_2$.

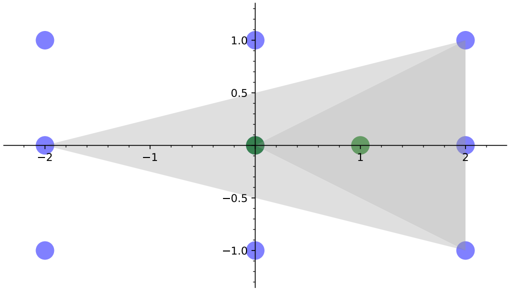
Example II - Twisted d.s.: beginning

- Auxiliary lattice:

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

- Residue group:

$$\mathcal{R} = \mathbb{Z}^2/\mathcal{L} = \{(0,0),(1,0)\}$$



Example II: the digit set

- Pre-periodic digit set:

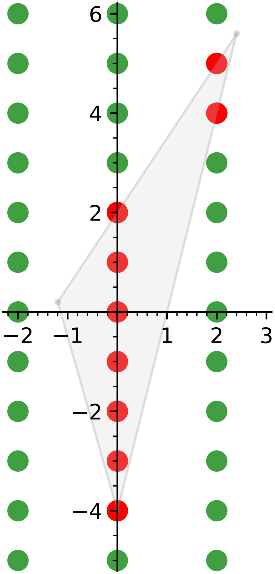
$$\mathcal{D}' = \{(2,0),(-2,-1),(-2,1),(1,0),(-1,-1),(-1,1)\}\,.$$

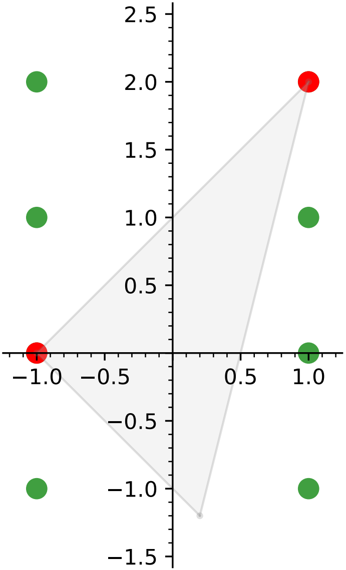
- Attractor points:

$$(0,-4),(0,-3),(0,-2),(0,-1),(0,0),$$

$$(0,1),(0,2),(2,4),(2,5),(-1,0),(1,2)$$

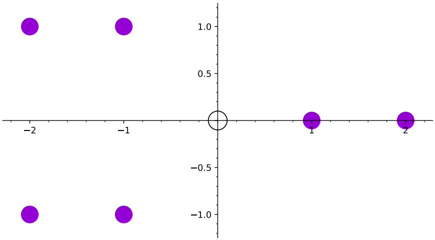
Example II: attractor points





Example II: twisted d.s.

- $(A, \mathcal{D}')$:



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

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

Example II continued: twisted d.s.

- Twisted d.s. $(M, \mathcal{D} \oplus \mathcal{D})$ has 49 digits:
- Pvz.

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

- We can optimize $\mathcal{D} \oplus \mathcal{D}$ down to 18 digits:

$$\mathcal{D}'' = (\mathcal{D}' \oplus \mathcal{R}) \bigcup (\{(0,0)\} \oplus \mathcal{D}')$$

Open problems

Problem 1

Let $A \in M_n(\mathbb{Q})$. Does there exist an algorithm to check whether a given vector $\mathbf{u} \in \mathbb{Q}^n$ 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 λ with $|\lambda| \geq 1$, and at least one eigenvalue is of absolute value $|\lambda| = 1$. Is it true that a digit system $(A, \mathcal{D})$ 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 $(A, \mathcal{D})$ in $\mathbb{Z}^n[A]$ has the finiteness property. What is **the smallest possible** *size $\#\mathcal{D}$ of the digit set?*

The End

Thank you!