



HAL
open science

Expanding toral endomorphisms are Bernoulli: towards explicit isomorphisms

Christophe Leuridan

► **To cite this version:**

Christophe Leuridan. Expanding toral endomorphisms are Bernoulli: towards explicit isomorphisms. 2024. hal-04556762v2

HAL Id: hal-04556762

<https://hal.science/hal-04556762v2>

Preprint submitted on 27 Aug 2024 (v2), last revised 29 Aug 2024 (v3)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Expanding toral endomorphisms are Bernoulli: towards explicit isomorphisms.

Christophe Leuridan

August 27, 2024

Abstract

Let $A \in \mathcal{M}_d(\mathbb{Z})$ be a $d \times d$ matrix with integer coefficients. The linear map $x \mapsto Ax$ from \mathbb{R}^d provides an endomorphism T_A of the torus $\mathbb{T}^d := \mathbb{R}^d/\mathbb{Z}^d$ which preserves the Haar measure. The endomorphism T_A is r -to-one, where $r := |\det A|$. When A is expanding (i.e. the modulus of each eigenvalue is > 1). Mihailescu [11] proved that T_A is isomorphic to the one-sided uniform Bernoulli shift on $\llbracket 0, r-1 \rrbracket^{\mathbb{Z}^+}$. This proof is not constructive.

Actually, in many situations, some explicit isomorphisms are known, at least by specialists of integral self-affine tiles. But the known conditions to have an explicit isomorphism are involved and not very tractable. In this work, we provide simple sufficient conditions and other examples of explicit isomorphisms which work in a lot of situations.

MSC Classification : 37A05,60J05.

Keywords : endomorphisms of the torus, Bernoulli shifts, constructive Markov chains.

1 Introduction

Fix a positive integer d . Let $A \in \mathcal{M}_d(\mathbb{Z})$ be a $d \times d$ matrix with integer coefficients such that $|\det A| = r \geq 2$. Since the linear map $x \mapsto Ax$ from \mathbb{R}^d to \mathbb{R}^d sends the group \mathbb{Z}^d onto the subgroup $A\mathbb{Z}^d$, one derives by taking quotients a continuous group endomorphism T_A of the compact additive group $\mathbb{R}^d/\mathbb{Z}^d$. For every $x \in \mathbb{R}^d$, $T_A(\bar{x}) = \overline{Ax}$, where $\bar{x} = x + \mathbb{Z}^d$ denotes the equivalence class of x in $\mathbb{R}^d/\mathbb{Z}^d$.

The endomorphism T_A thus defined preserves the Haar measure η on $\mathbb{R}^d/\mathbb{Z}^d$ and is r -to-one: given a uniform random variable X_0 with values in $\mathbb{R}^d/\mathbb{Z}^d$, the distribution of $T_A(X_0)$ is still uniform a random variable taking values on Q with law η , the distribution of $T_A(X_0)$ is still uniform and for (almost) every $y \in \mathbb{R}^d/\mathbb{Z}^d$, the conditional law $\mathcal{L}(X_0|T_A(X_0) = y)$ is uniform on the set $T_A^{-1}(\{y\})$, which has exactly r elements.

Is T_A isomorphic to S_r , where S_r denotes the uniform one-sided Bernoulli shift on $\llbracket 0, r-1 \rrbracket^{\mathbb{Z}^+}$? Katznelson [7] proved in 1971 that if no eigenvalues of A is a root of unity, then the natural extension of T_A and S_r are isomorphic. But this weaker property does not ensure that the endomorphism T_A itself is Bernoulli.

A positive partial answer was given much later (2012) by Mihailescu [11]: When A is *expanding*, i.e. when the modulus of every eigenvalue of A is strictly greater than 1, the endomorphism T_A is isomorphic to S_r . Mihailescu's proof is not constructive and

relies on a criterion introduced by Hoffman and Rudolph [5], which is called *tree very weak Bernoulli*.

From now on, we assume that A is expanding. Equivalently, A is invertible in $\mathcal{M}_d(\mathbb{Q})$ and $\rho(A^{-1}) < 1$, where ρ denotes the spectral radius: for every $M \in \mathcal{M}_d(\mathbb{R})$,

$$\rho(M) := \max\{|\alpha| : \alpha \text{ eigenvalue of } M\}.$$

Recall that for any operator norm $\|\cdot\|$ on the linear space $\mathcal{M}_d(\mathbb{R})$,

$$\rho(M) = \lim_{n \rightarrow +\infty} \|M^n\|^{1/n} = \inf_{n \geq 1} \|M^n\|^{1/n}.$$

Given any basis $\mathbf{u} = (u_1, \dots, u_d)$ of \mathbb{R}^d , we note $|\cdot|_{\mathbf{u}, \infty}$ the norm on \mathbb{R}^d defined by

$$|x|_{\mathbf{u}, \infty} := \max_{1 \leq i \leq d} |\xi_i| \text{ where } x = \sum_{i=1}^d \xi_i u_i.$$

For every $M \in \mathcal{M}(\mathbb{R}^d)$, denote by $\|M\|_{\mathbf{u}, \infty}$ the associated operator norm of M . One can check that $\rho(M)$ is the infimum of $\|M\|_{\mathbf{u}, \infty}$ over all basis \mathbf{u} of \mathbb{R}^d . Since $\|M\|_{\mathbf{u}, \infty}$ depends continuously on the vectors u_1, \dots, u_d , one may restrict ourselves to vectors with *rational* coordinates, or even with *integer* coordinates, by homogeneity.

Yet, the determinant of (u_1, \dots, u_d) may be different from ± 1 , so *we may not* assume that \mathbf{u} a \mathbb{Z} -basis of \mathbb{Z}^d (i.e. that $\mathbb{Z}u_1 \oplus \dots \oplus \mathbb{Z}u_d$ is the whole group \mathbb{Z}^d). This distinction is important in what follows.

Our purpose is to exhibit an explicit isomorphism. We will view two different approaches, which yield symmetrical results. The classical approach via radix expansions shows that T_A is a factor of S_r , and the factor map is m -to-one for some positive integer m . The new approach we introduce involves Markov chains and shows that S_r is a factor of T_A , and the factor map is s -to-one for some positive integer s .

Both approaches provide an explicit isomorphism when $\|A^{-1}\|_{\mathbf{u}, \infty} < 1$ for some \mathbb{Z} -basis \mathbf{u} of \mathbb{Z}^d . This condition is a bit stronger than Mihailescu's sufficient condition $\rho(A^{-1}) < 1$ for the existence of such isomorphisms. Since $(T_A)^n = T_{A^n}$ for all $n \geq 1$ and since $\rho(A^{-1}) < 1$ implies $\|A^{-n}\|_{\mathbf{u}, \infty} < 1$ for all large enough n , both methods provide explicit isomorphisms between $(T_A)^n$ and the Bernoulli shift S_{r^n} for all large enough n .

Note also that our problem is preserved by unimodular change of coordinates: if $U \in GL_d(\mathbb{Z})$ then the map $x \mapsto Ux$ provides an isomorphism transforming T_A the measure-preserving map T_A into the measure-preserving map $T_{UAU^{-1}}$.

1.1 The classical approach using radix expansions and self-affine tiles

A natural idea is to imitate the r -adic expansions of the real numbers. Indeed, proving that the measure-preserving map $T_r : x \mapsto rx - [rx]$ from $[0, 1[$ (endowed with the Lebesgue measure) is isomorphic to the uniform one-sided Bernoulli shift on $\llbracket 0, r-1 \rrbracket^\infty$ is quite simple. Indeed, if x is uniformly chosen on $[0, 1[$, then in its r -adic expansion, its digits in are i.i.d. and uniform on $\llbracket 0, r-1 \rrbracket$. Moreover, if the r -adic expansion of x is $0.\xi_1\xi_2\dots$ the r -adic expansion of $T_r(x)$ is $0.\xi_2\xi_3\dots$

Now, let us replace the base r and the set $\llbracket 0, r-1 \rrbracket$ of possible digits by the matrix A and by some fixed set \mathbb{D} of representatives of $\mathbb{Z}^d/A\mathbb{Z}^d$, containing 0. The theory of lattices shows that $A\mathbb{Z}^d$ is a subgroup of index r in \mathbb{Z}^d , so $|\mathbb{D}| = r$.

It is convenient to introduce Minkovski sums. Given two subsets B and C of \mathbb{R}^d , their Minkovski sum is $B + C := \{b + c : (b, c) \in B \times C\}$. When each point of $B + C$ has a unique decomposition $b + c$ with $(b, c) \in B \times C$, we say that the sum is direct, and we may use the notation $B \oplus C$. Minkovski sums and direct sums are commutative and associative.

The assumption that \mathbb{D} is a complete residue system modulo $A\mathbb{Z}^d$, i.e. a system of representatives of $\mathbb{Z}^d/A\mathbb{Z}^d$, is equivalent to the equality $\mathbb{Z}^d = \mathbb{D} \oplus A\mathbb{Z}^d$. There is a natural way to produce systems of representatives of $\mathbb{Z}^d/A\mathbb{Z}^d$ from a *fundamental domain* of $\mathbb{R}^d/\mathbb{Z}^d$, i.e. any Borel subset of \mathbb{R}^d containing exactly one element in each equivalence class of $\mathbb{R}^d/\mathbb{Z}^d$. Indeed, if D is fundamental domain of $\mathbb{R}^d/\mathbb{Z}^d$, then $\mathbb{R}^d = D \oplus \mathbb{Z}^d$, so $\mathbb{R}^d = A\mathbb{R}^d = AD \oplus A\mathbb{Z}^d$ and $\mathbb{Z}^d = (AD \cap \mathbb{Z}^d) \oplus A\mathbb{Z}^d$. As a result, $AD \cap \mathbb{Z}^d$ is a set of representatives of $\mathbb{Z}^d/A\mathbb{Z}^d$.

Given any complete residue system \mathbb{D} modulo $A\mathbb{Z}^d$, containing 0, we get by induction

$$\forall n \geq 1, \quad \mathbb{Z}^d = \mathbb{D} \oplus \dots \oplus A^{n-1}\mathbb{D} \oplus A^n\mathbb{Z}^d.$$

so the set $\mathbb{D}_n := \mathbb{D} \oplus A\mathbb{D} + \dots \oplus A^{n-1}\mathbb{D}$ is a system of representatives of $\mathbb{Z}^d/A^n\mathbb{Z}^d$. Furthermore, the sequence $(\mathbb{D}_n)_{n \geq 1}$ is increasing since we assumed that $0 \in \mathbb{D}$. A natural question is whether the increasing union

$$\mathbb{D}_\infty := \bigcup_{n \geq 1} \mathbb{D}_n.$$

is the whole lattice \mathbb{Z}^d or not. If yes, one checks that any vector of \mathbb{Z}^d has a unique expansion ‘in base A ’, and any vector of \mathbb{R}^d has at least a fractional expansion, not necessarily unique.

Such generalizations of r -adic expansions have been considered independently by several authors for applications in various domains: computer science, wavelets analysis,... Matula [10] considered expansions of relative integers and of real numbers in a given base $\beta \in \mathbb{Z} \setminus \{-1, 0, 1\}$. The system of digits \mathbb{D} is assumed to contain 0 and to exactly one representative in each equivalence class of $\mathbb{Z}/|\beta|\mathbb{Z}$. Knuth [8] fixed an integer $n \geq 2$ and considered expansions of complex numbers in base $\sqrt{-n}$ with digits in $\llbracket 0, n-1 \rrbracket$. Later, W. Penney [12] considered expansions of complex numbers in base $-1 + i$ with digits in $\{0, 1\}$. More generally, Duda [2] considered complex bases z which are solutions of some quadratic equation and have modulus > 1 . Duda also briefly considered possible generalisations in higher dimension, replacing the base by replace by some matrix with integer coefficients, of the form ρO , where $\rho > 1$ and O is an orthogonal matrix.

Expansions in which the base is replaced by any expansive matrix A with integer entries have been studied more recently. One important object of interest are the sets

$$K_{\mathbb{D}} := \left\{ \sum_{k=1}^{+\infty} A^{-k} v_k : (v_k)_{k \geq 1} \in \mathbb{D}^\infty \right\},$$

where \mathbb{D} is a set \mathbb{D} of representatives of $\mathbb{Z}^d/A\mathbb{Z}^d$. Here, we omit the index A because the expansive matrix A is assumed to be fixed.

Such sets have remarkable properties: $K_{\mathbb{D}}$ is compact and has positive (and finite) Lebesgue measure $\lambda(K_{\mathbb{D}})$. Moreover, $K_{\mathbb{D}}$ is the union of the $A^{-1}K_{\mathbb{D}} + A^{-1}v$ over all $v \in \mathbb{D}$, and this union is almost disjoint: whenever v and v' are distinct elements in \mathbb{D} , the intersection of $A^{-1}K_{\mathbb{D}} + A^{-1}v$ and $A^{-1}K_{\mathbb{D}} + A^{-1}v'$ is a null set (for the Lebesgue measure λ). That is why the compact set $K_{\mathbb{D}}$ is called a *self affine-tile*.

We now recall some facts stated in Hacon, Saldanha, Veerman in [4]. Up to null sets, the subsets $(K_{\mathbb{D}} + v)_{v \in \mathbb{D}}$ form a uniform partition of $AK_{\mathbb{D}}$. The map $T_{A, K_{\mathbb{D}}} : K_{\mathbb{D}} \rightarrow K_{\mathbb{D}}$ which sends each $x \in K_{\mathbb{D}}$ on the almost surely unique $y \in K_{\mathbb{D}}$ such that $Ax - y \in \mathbb{D}$ preserves the uniform measure $\mathcal{U}(K_{\mathbb{D}}) := \lambda(\cdot | K_{\mathbb{D}})$ on $K_{\mathbb{D}}$, and the map $\Phi : \mathbb{D}^{\infty} \rightarrow K_{\mathbb{D}}$ defined by

$$\Phi((v_k)_{k \geq 1}) := \sum_{k=1}^{+\infty} A^{-k} v_k$$

is an isomorphism transforming the uniform Bernoulli shift on \mathbb{D}^{∞} into the measure-preserving map $T_{A, K_{\mathbb{D}}}$.

Call $p_{\mathbb{T}^d}$ the canonical projection from \mathbb{R}^d onto $\mathbb{T}^d = \mathbb{R}^d / \mathbb{Z}^d$. Corollary 1.7 in [4] states that the restriction $p_{\mathbb{T}^d}|_{K_{\mathbb{D}}}$ is m -to-one (up to null sets) for some positive integer m , therefore this integer m equals the Lebesgue measure of $K_{\mathbb{D}}$. Therefore, $p_{\mathbb{T}^d}|_{K_{\mathbb{D}}}$ is a m -to-one factor map transforming $T_{A, K_{\mathbb{D}}}$ into T_A .

Hence, the endomorphism T_A is a factor of the uniform Bernoulli shift on \mathbb{D}^{∞} (or, equivalently, on $\llbracket 0, r-1 \rrbracket^{\mathbb{Z}^+}$) and the factor map is $\lambda(K_{\mathbb{D}})$ -to-one. In particular, $\lambda(K_{\mathbb{D}})$ is always a positive integer and $p_{\mathbb{T}^d}|_{K_{\mathbb{D}}}$ is an isomorphism if and only if the Lebesgue measure of $K_{\mathbb{D}}$ is 1.

Actually, the volume $\lambda(K_{\mathbb{D}})$ does depend on the choice of the set \mathbb{D} of representatives of $\mathbb{Z}^d / A\mathbb{Z}^d$. For example, when $d = 1$ and $A = 2$, the choice $\mathbb{D} = \{0, 1\}$ yields $K_{\mathbb{D}} = [0, 1]$, whereas the choice $\mathbb{D} = \{0, 3\}$ yields $K_{\mathbb{D}} = [0, 3]$.

The results given by Matula in [10] in the one-dimensional case can be adapted to our context and further pursued. This yields the theorem below.

Theorem 1. *Fix a norm $|\cdot|$ on \mathbb{R}^d such that the associated operator norm satisfies $\|A^{-1}\| < 1$. Set $M = \max\{|A^{-1}v| : v \in \mathbb{D}\}$. Then the statements below are equivalent:*

1. $\mathbb{D}_{\infty} = \mathbb{Z}^d$.
2. \mathbb{D}_{∞} contains all vectors $x \in \mathbb{Z}^d$ such that $|x| \leq M/(1 - \|A^{-1}\|)$.
3. $\forall n \geq 1, \mathbb{D}_n \cap (A^n - I_d)\mathbb{Z}^d = \{0\}$.

Moreover, if the equivalent properties above hold, then $\lambda(K_{\mathbb{D}}) = 1$.

The equivalence between items 1,2,3 is a simple adaptation of Matula's work. That they imply $\lambda(K_{\mathbb{D}}) = 1$ was not written in Matula's paper, but it follows easily from the fact that $AK_{\mathbb{D}}$ is the almost disjoint union of the sets $K_{\mathbb{D}} + v$ over all $v \in \mathbb{D}$.

Theorem 1 provides a sufficient (but not necessary) conditions on A and \mathbb{D} to have $\lambda(K_{\mathbb{D}}) = 1$. For example, in the one-dimensional case considered by Matula,

- If $A = r$ and $\mathbb{D} = \llbracket 0, r-1 \rrbracket$, then for every $n \geq 1$, $\mathbb{D}_n = \llbracket 0, r^n - 1 \rrbracket$. Therefore, $\mathbb{D}_n \cap (r^n - 1)\mathbb{Z} = \{0, r^n - 1\}$ and $\mathbb{D}_{\infty} = \mathbb{N}$. Yet, $K_{\mathbb{D}} = [0, 1]$ so $\lambda(K_{\mathbb{D}}) = 1$.
- If $A = -r$ and $\mathbb{D} = \llbracket 0, r-1 \rrbracket$, then $\mathbb{D}_{\infty} = \mathbb{Z}$ and $K_{\mathbb{D}} = [-r/(r+1), 1/(r+1)]$, so $\lambda(K_{\mathbb{D}}) = 1$.

To get a less simple example, take $d = 2$, $A = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}$ so $r = 5$. One may choose $\mathbb{D} = \{(0, 0), (0, 1), (0, -1), (1, 0), (-1, 0)\}$. The endomorphism of \mathbb{R}^2 canonically associated to A is a direct similitude with ratio $\sqrt{5}$. Thus theorem 1 applies with the canonical

Euclidean norm on \mathbb{R}^2 , and $M = \|A^{-1}\| = 1/\sqrt{5}$, so $M/(1 - \|A^{-1}\|) = 1/(\sqrt{5} - 1) < 1$. Since the only point $x \in \mathbb{Z}^2$ such that $|x| \leq 1/(\sqrt{5} - 1)$ is 0, statement 2 holds trivially, therefore statements 1 and 3 also hold and $\lambda(K_{\mathbb{D}}) = 1$.

Now, let us mention more recent works which study the quantity $\lambda(K_{\mathbb{D}})$.

In [3], Gabardo and Yu give an algorithm to compute this Lebesgue measure. In [9], Lagarias and Wang prove the existence of a lattice tiling with the tile $K_{\mathbb{D}}$: there exists some lattice $\Lambda \subset \mathbb{Z}^d$ such that $K_{\mathbb{D}} + \Lambda = \mathbb{R}^d$ and such that the translated sets $(K_{\mathbb{D}} + v)_{v \in \Lambda}$ do not overlap. Thus, the volume $\lambda(K_{\mathbb{D}})$ equals the index of Λ in \mathbb{Z}^d . Using this lattice tiling, Lagarias and Wang establish a highly non-trivial necessary and sufficient condition for $\lambda(K_{\mathbb{D}})$ to equal 1. This condition is involved and not very tractable, although it provides many simple corollaries.

Hence, many questions arise:

- Is it always possible to choose \mathbb{D} to have $\lambda(K_{\mathbb{D}})$ to equal 1 and how?
- Given $c \in \mathbb{R}^d$ and any \mathbb{Z} -basis (u_1, \dots, u_d) of \mathbb{Z}^d , one checks that the parallelotope $P = c + [0, 1[u_1 + \dots + [0, 1[u_d$ is a fundamental domain of $\mathbb{R}^d/\mathbb{Z}^d$, so $AP \cap \mathbb{Z}^d$ is system of representatives of $\mathbb{Z}^d/A\mathbb{Z}^d$. Does such a system of representatives always work?

The example above suggests that choosing a norm on \mathbb{R}^d such that the associated operator norm satisfies $\|A^{-1}\| < 1$ and choosing the vectors of \mathbb{D} having norms as small as possible could be a good strategy.

To answer these questions, we establish some remarkable consequences of Lagarias and Wang's condition in subsection 4.7. We provide counterexamples showing that the answer to both question is negative. Yet, we have a positive result when $d = 2$.

Theorem 2. *If $d = 2$, then it is always possible to choose the system \mathbb{D} of representatives so that $\lambda(K_{\mathbb{D}}) = 1$.*

And still when $d = 2$, the answer to the second question is positive provided an extra assumption of primitivity holds (see Corollary 39).

In subsection 4.5, we develop a variant of the approach followed by Hacon, Saldanha, Veerman and mentionned above. Given a bounded fundamental domain D_0 of $\mathbb{R}^d/\mathbb{Z}^d$, the sets $(D_n)_{n \geq 1}$ defined by

$$D_n = A^{-n}D_0 + A^{-n}\mathbb{D} + \dots + A^{-1}\mathbb{D}.$$

form a uniformly bounded sequence of fundamental domains. We show that the facts stated in Hacon, Saldanha, Veerman and recalled above still work if one replaces $K_{\mathbb{D}}$ with the set

$$L = \limsup_n D_n := \{x \in \mathbb{R}^d : x \in D_n \text{ for infinitely many } n \geq 0\}.$$

In particular, T_A is a factor of some explicit measure-preserving map on $(L, \mathcal{B}(L), \mathcal{U}(L))$, which is obviously isomorphic to the uniform Bernoulli shift on \mathbb{D}^∞ . Furthermore, the Lebesgue measure of L is a positive integer and the factor map $p_{\mathbb{T}^d}|_L$ is $\lambda(L)$ -to-one. When $\lambda(L)$ equals 1, we derive an explicit isomorphism between T_A and the uniform Bernoulli shift on \mathbb{D}^∞ .

Actually, the closure of $\limsup D_n$ is $K_{\mathbb{D}}$, and we have $\lambda(K_{\mathbb{D}}) \geq \lambda(L) \geq 1$. The interest of working with the smaller set $\limsup_n D_n$ instead of $K_{\mathbb{D}}$ is that it is easier to check that – under appropriate conditions – its Lebesgue measure is 1.

Theorem 3. *Assume that $\|A^{-1}\|_{\mathbf{u},\infty} < 1$ for some \mathbb{Z} -basis $\mathbf{u} = (u_1, \dots, u_d)$ of \mathbb{Z}^d . Let*

$$c := (1/2)A^{-1}(u_1 + \dots + u_d), \quad D_0 := c + \sum_{i=1}^d [-1/2, 1/2]u_i, \quad \mathbb{D} := AD_0 \cap \mathbb{Z}^d.$$

Consider the fundamental domains $(D_n)_{n \geq 1}$ defined by

$$D_n = A^{-n}D_0 + A^{-n}\mathbb{D} + \dots + A^{-1}\mathbb{D}.$$

Then $\lambda(\limsup_n D_n) = 1$.

The proof of Theorem 3 does not use the theorem of Lagarias and Wang. It relies on the study of the external boundary of the sets \mathbb{D}_n when \mathbb{Z}^d is endowed with some graph structure on \mathbb{Z}^d related to the set \mathbb{D} .

1.2 A new approach using bounded fundamental domains

An alternative approach relies on the study a stationary Markov chain on $\mathbb{R}^d/\mathbb{Z}^d$ whose evolution consists in choosing at random successive preimages by T_A . Since one cannot apply A^{-1} to elements of $\mathbb{R}^d/\mathbb{Z}^d$, it is convenient to fix a bounded fundamental domain D . The theory of lattices ensures that $\lambda(D) = 1$.

For every $x \in \mathbb{Z}^d$, call $p_D(x)$ the unique element of D in the coset $x + \mathbb{Z}^d$. We call *projection on D* the map $p_D : \mathbb{R}^d \rightarrow D$ thus defined. One checks that the discontinuity set of p_D is $\Delta_D := \partial D + \mathbb{Z}^d$. Moreover, if B is a Borel subset of \mathbb{R}^d , then

$$p_D(B) = \bigcup_{k \in \mathbb{Z}^d} (B - k) \cap D$$

is still a Borel subset.

Instead of T_A , we study the map $T_{A,D} : x \mapsto p_D(Ax)$ from D to D . One checks that $T_{A,D}$ preserves the uniform measure $\mathcal{U}_D := \lambda(\cdot|D)$ on D . Moreover, the dynamical system $(D, \mathcal{B}(D), \mathcal{U}_D, T_{A,D})$ is isomorphic to $(\mathbb{R}^d/\mathbb{Z}^d, \mathcal{B}(\mathbb{R}^d/\mathbb{Z}^d), \eta, T_A)$: indeed, if $p_{\mathbb{T}^d}$ denotes the canonical projection from \mathbb{R}^d to \mathbb{T}^d , the restriction $p_{\mathbb{T}^d}|_D$ is an isomorphism transforming $T_{A,D}$ into T . Hence, we will frequently omit the subscript D in $T_{A,D}$.

The simplest fundamental domain we will work with is the cube $Q = [0, 1]^d$. The projection on Q is given by the formula $p_Q(x) = x - \lfloor x \rfloor$, where we set

$$\lfloor x \rfloor := (\lfloor x_1 \rfloor, \dots, \lfloor x_d \rfloor) \text{ for every } x = (x_1, \dots, x_d) \in \mathbb{R}^d.$$

The discontinuity set of p_Q is the set Δ_Q of all vectors having at least a coordinate in \mathbb{Z} (in the canonical basis). We will also work with more general parallilipeds, namely with images of Q by affine maps in \mathbb{R}^d of the form $x \mapsto y_0 + Ux$ with $y_0 \in \mathbb{R}^d$ and $U \in \text{GL}_d(\mathbb{Z}) = \{M \in \mathcal{M}_d(\mathbb{Z}) : \det M = \pm 1\}$.

Now, fix a set \mathbb{D} of representatives of $\mathbb{Z}^d/A\mathbb{Z}^d$. For each $v \in \mathbb{D}$, call let $f_v : D \rightarrow D$ be the map given by $f_v(y) := p_D(A^{-1}y + A^{-1}v)$ and set $P_v := f_v(D)$. Note that the maps $(f_v)_{v \in \mathbb{D}}$ and the subsets $(P_v)_{v \in \mathbb{D}}$ thus defined do not depend on the choice of \mathbb{D} . Indeed,

if one replaces some vector $v \in \mathbb{D}$ by a vector v' belonging to the same class of $\mathbb{Z}^d/A\mathbb{Z}^d$, then for every $y \in \mathbb{R}^d$, $f_{v'}(y) = f_v(y)$ since $(A^{-1}y + A^{-1}v) - (A^{-1}y + A^{-1}v') \in \mathbb{Z}^d$.

The maps $(f_v)_{v \in \mathbb{D}}$ and the subsets $(P_v)_{v \in \mathbb{D}}$ have interesting properties.

Proposition 4. *Call $\Delta_D = \partial D + \mathbb{Z}^d$ the discontinuity set of p_D .*

- *For each $y \in D$, the vectors $(f_v(y))_{v \in \mathbb{D}}$ are pairwise distinct and are the preimages of y by T_A . Therefore, $\pi := (P_v)_{v \in \mathbb{D}}$ is a partition π of D . Moreover, for each $v \in \mathbb{D}$, the map f_v induces a bijection from D to P_v , whose inverse map is $T_A|_{P_v}$.*
- *For each $v \in \mathbb{D}$, the map $y \mapsto f_v(y) - A^{-1}y$ is constant on each subset $AD - v + Ak$ with $k \in \mathbb{Z}^d$ and takes only finitely many values on \mathbb{D} . Its discontinuity set is contained in $\Delta_v := A\Delta_D - v$.*
- *The sets P_0, \dots, P_{r-1} are Borel and with Lebesgue measure $1/r$ each.*
- *The partitions $(T_A^{-n}(\pi))_{n \geq 0}$ are independent.*

For every $x \in D$, call $\pi(x)$ the index of the only block of the partition π which contains x , namely $\pi(x) \in \mathbb{D}$ and $x \in P_{\pi(x)}$. By construction, the factor map $\Psi : x \mapsto (\pi(T_A^n(x)))_{n \geq 0}$ from D to $\mathbb{D}^{\mathbb{Z}^+}$ transforms T_A into the uniform Bernoulli shift S .

The partition π seems to be a good candidate for being an independent generator of T_A . Actually, assuming that D is bounded with ‘small’ boundary, we prove a slightly weaker statement. Here, we need a few notations.

Given a subset S of \mathbb{R}^d , the *upper box dimension* of S is defined by

$$\dim_{\text{upper box}} S = \limsup_{\varepsilon \rightarrow 0} \frac{\ln N_S(\varepsilon)}{|\ln \varepsilon|} = d - \liminf_{\varepsilon \rightarrow 0} \frac{|\ln \lambda(S_\varepsilon)|}{|\ln \varepsilon|},$$

where $N_S(\varepsilon)$ is the minimal number of open balls with radius ε required to cover S , and S_ε is the ε -neighbourhood of S , namely $S_\varepsilon = \{x \in \mathbb{R}^d : \text{dist}(x, S) < \varepsilon\}$.

Theorem 5. *Assume D is bounded and that $\dim_{\text{upper box}}(\partial D) < d$. Then the factor map $\Psi : x \mapsto (\pi(T_A^n(x)))_{n \geq 0}$ from D to $\mathbb{D}^{\mathbb{Z}^+}$ is s -to-one for some integer $s \geq 1$.*

The integer s measures the information missing in the partitions $(T_A^{-n}(\pi))_{n \geq 0}$. The partition π is a generator if and only if $s = 1$. The following example involving various parallelotopes shows that the integer s actually depends on the choice of the fundamental set D . Hence, this choice has a great importance, whereas the choice of the set \mathbb{D} plays no role in this approach.

Example 6. *Let*

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

One can choose $\mathbb{D} = \{0, e_1\}$, where (e_1, e_2) is the canonical basis of \mathbb{R}^2 .

1. *If $D = [0, 1]^2$, then $s = 2$.*
2. *If $D = [-1/2, 1/2]^2$, then $s = 8$.*
3. *If $D = [0, 1]e_1 + [0, 1]e_2$, then $s = 1$.*

We now introduce an additional assumption which ensures that π is an independent generator of T_A . Observe that for every fundamental domain D and every $v_0, v_{-1}, v_{-2}, \dots$ in \mathbb{D} , the sets $(f_{v_0} \circ \dots \circ f_{v_{-n+1}})(D)$ form a decreasing sequence. Here, we use negative indexes because we couple from the past.

Theorem 7. *Keep the assumptions of Theorem 5. Fix any norm $|\cdot|$ on \mathbb{R}^d , and denote the associated open balls by the letter B . Assume that $D = c + UQ$ for some $c \in \mathbb{Z}^d$ and $U \in GL_d(\mathbb{Z})$. Assume furthermore that there exists $x_0 \in D$ which is a continuity point of all functions of the form $f_{v_n} \circ \dots \circ f_{v_1}$ and some sequence $v_0, v_{-1}, v_{-2}, \dots$ of elements of \mathbb{D} such that for every $\delta > 0$,*

$$(f_{v_0} \circ \dots \circ f_{v_{-n+1}})(D) \subset B(x_0, \delta) \text{ for every large enough } n.$$

Then the factor map $\Psi : D \rightarrow \mathbb{D}^{\mathbb{Z}^+}$ is an isomorphism. Moreover, Ψ is continuous almost everywhere on D and Ψ^{-1} is continuous almost everywhere on $\{0, 1\}^{\mathbb{Z}^+}$.

Actually, we will see that Theorem 7 applies in a lot of situations.

Theorem 8. *Assume that $\|A^{-1}\|_{\mathbf{u}, \infty} < 1$ for some \mathbb{Z} -basis \mathbf{u} of \mathbb{Z}^d . Let $c \in \mathbb{R}^d$ and $D = c + P_{\mathbf{u}}$. Assume that $0 \in \mathbb{D}$.*

1. *If ($c = 0$ and r is odd), or if the real numbers $1, c_1, \dots, c_d$ are linearly independent over \mathbb{Q} , the point 0 is a continuity point of all functions of the form $f_{v_n} \circ \dots \circ f_{v_1}$.*
2. *If c is small enough, we have $A^{-1}D \subset D$, so the map f_0 coincides with $y \mapsto A^{-1}y$, and for every $\delta > 0$, $f_0^n(D) \subset B(0, \delta)$ for every large enough n .*
3. *If conditions 1 and 2 hold, then Theorem 7 applies, so the factor map $\Psi : D \rightarrow \mathbb{D}^{\mathbb{Z}^+}$ is an isomorphism.*

The proof of Theorem 5 relies on the study of a stationary Markov chain on $\mathbb{R}^d/\mathbb{Z}^d$ whose evolution is given as follows: at each time, the new position is chosen at random among the r successive preimages by T_A of the previous position.

1.3 Plan of the paper

Section 2 is devoted to useful preliminary results. Among them, we establish a general result on Markov chains, Theorem 13. Considering a Markov chain $(X_n)_{n \in \mathbb{Z}}$ and governed by a recursion relation of the form $X_{n+1} = f_{V_{n+1}}(X_n)$, this theorem compares the natural filtration of $((X_n, V_n))_{n \in \mathbb{Z}}$ with the smaller natural filtration of $(V_n)_{n \in \mathbb{Z}}$.

In section 3, we prove Theorems 5, 7, 8 and Example 6.

2 Proof of preliminary facts

2.1 Exactness of T_A

We begin with a simple lemma.

Lemma 9. *The subgroup $\bigcup_{n \geq 0} A^{-n}\mathbb{Z}^d$ is dense in \mathbb{R}^d .*

Proof. Let us endow \mathbb{R}^d with the norm $|\cdot|_{\mathbf{e},\infty}$, where \mathbf{e} is the canonical basis of \mathbb{R}^d , and $\mathcal{M}_d(\mathbb{R})$ with the associated operator norm. For every $x \in \mathbb{R}^d$ and $n \geq 0$,

$$|x - A^{-n}[A^n x]|_{\mathbf{e},\infty} = |A^{-n}(A^n x - [A^n x])|_{\mathbf{e},\infty} \leq \|A^{-n}\|.$$

Since $\|A^{-n}\|^{1/n} \rightarrow \rho(A^{-1}) < 1$ as $n \rightarrow +\infty$, we derive $A^{-n}[A^n x] \rightarrow x$ as $n \rightarrow +\infty$. \square

Proposition 10. *When $\rho(A^{-1}) < 1$, the transformation T_A is exact.*

Proof. Let B be in $\bigcap_{n \geq 0} T_A^{-n} \mathcal{B}(D)$. Call $f = \mathbf{1}_B \circ p_D$ be \mathbb{Z}^d -periodic extension of $\mathbf{1}_B$.

Fix $n \geq 1$ and $v \in A^{-n} \mathbb{Z}^d$. Let us check that v is a period of f . Since $B \in T_A^{-n} \mathcal{B}(D)$, there exists $C \in \mathcal{B}(D)$ such that $B = T_A^{-n} \mathcal{B}(C)$. For every $x \in \mathbb{R}^d$,

$$f(x + v) = \mathbf{1}_B(p_D(x + v)) = \mathbf{1}_C(T_A^n(p_D(x + v))).$$

Since $A \mathbb{Z}^d \subset \mathbb{Z}^d$ and $A^n v \in \mathbb{Z}^d$, we have

$$T_A^n(p_D(x + v)) \equiv A^n(p_D(x + v)) \equiv A^n(x + v) \equiv A^n x \equiv A^n(p_D x) \equiv T_A^n(p_D x) \pmod{\mathbb{Z}^d},$$

so $T_A^n(p_D(x + v)) = T_A^n(p_D x)$ since both sides of the equality belong to D . Thus

$$f(x + v) = \mathbf{1}_C(T_A^n(p_D(x + v))) = \mathbf{1}_C(T_A^n(p_D(x))) = f(x),$$

which shows that v is a period of f .

Hence, the set of all periods of f contains $\bigcup_{n \geq 0} A^{-n} \mathbb{Z}^d$, which it is dense in \mathbb{R}^d . Therefore, the continuous map $v \mapsto f(\cdot + v)|_D$ from \mathbb{R}^d to $L^1(D)$ is constant. Thus f is constant almost everywhere, namely $\lambda(B) \in \{0, 1\}$. \square

2.2 Study of the maps $(f_v)_{v \in \mathbb{D}}$

In this section, we establish useful properties of the maps $(f_v)_{v \in \mathbb{D}}$.

Let us prove Proposition 4.

Proof. Let x and y in D . Since $T_A(x) = p_D(Ax)$, $A^{-1} \mathbb{Z}^d = A^{-1} \mathbb{D} \oplus \mathbb{Z}^d$ and $f_v(y) = p_D(A^{-1}y + A^{-1}v)$ for every $v \in \mathbb{D}$, we have

$$\begin{aligned} T_A(x) = y &\iff Ax \in y + \mathbb{Z}^d \\ &\iff x \in A^{-1}y + A^{-1} \mathbb{Z}^d \\ &\iff \exists v \in \mathbb{D} : x \in A^{-1}y + A^{-1}v + \mathbb{Z}^d \\ &\iff \exists v \in \mathbb{D} : x = f_v(y). \end{aligned}$$

Item 1 follows.

Fix $v \in \mathbb{D}$. For every $k \in \mathbb{Z}^d$ and $y \in D$,

$$f_v(y) = A^{-1}y + A^{-1}v - k \iff A^{-1}y + A^{-1}v - k \in D \iff y \in AD - v + Ak.$$

Hence the map $y \mapsto f_v(y) - A^{-1}y$ is constant on $(AD - v + Ak) \cap D$.

Furthermore, if y is a discontinuity point of Δ_v , then $A^{-1}y + A^{-1}v$ is a discontinuity point of p_D , so $A^{-1}y + A^{-1}v \in \Delta_D$ and $y \in \Delta_v = A \Delta_D - v$. Item 2 follows.

Fix $v \in \mathbb{D}$ and $B \in \mathcal{B}(D)$. Then

$$P_v \cap T_A^{-1}(B) = f_v(B) = \bigcup_{k \in \mathbb{Z}^d} f_v(B \cap (AD - v + Ak)) = \bigcup_{k \in \mathbb{Z}^d} (A^{-1}B + A^{-1}v - k) \cap D.$$

This is a Borel subset, and since we have a disjoint union, we get

$$\begin{aligned} \lambda(P_v \cap T_A^{-1}(B)) &= \sum_{k \in \mathbb{Z}^d} \lambda((A^{-1}B + A^{-1}v - k) \cap D) \\ &= \sum_{k \in \mathbb{Z}^d} \lambda((A^{-1}B + A^{-1}v) \cap (D + k)) \\ &= \lambda(A^{-1}B + A^{-1}v) = r^{-1}\lambda(B). \end{aligned}$$

In particular, $\lambda(P_v) = \lambda(P_v \cap T_A^{-1}(D)) = r^{-1}$, so we get that π is independent of $T_A^{-1}\mathcal{B}$. A recursion yields the independence of $\pi, T_A^{-1}\pi, \dots, T_A^{-n}\pi, T_A^{-n-1}\mathcal{B}$ for every $n \geq 0$. Items 3 and 4 follow. \square

Before studying the discontinuity set of iterates $f_{v_n} \circ \dots \circ f_{v_1}$, we prove a simple lemma.

Lemma 11. *Let $v \in \mathbb{D}$. For every $B \in \mathcal{B}(D)$, $f_v^{-1}(B) \subset AB - v + AZ^d \subset AB + Z^d$.*

Proof. Since f_v viewed from D to P_v is the inverse of the bijection $T_A|_{P_v}$, one has

$$f_v^{-1}(B) = T_A(B \cap P_v) = p_D(AB \cap AP_v).$$

By definition of P_v ,

$$AP_v = Ap_D(A^{-1}D + A^{-1}v) \subset Ap_D(A^{-1}D + A^{-1}v - Z^d) = D + v - AZ^d.$$

On each set $D + v - Ak$ with $k \in \mathbb{Z}^d$, the projection p_D coincides with the translation of $-v + Ak$. Hence

$$f_v^{-1}(B) \subset p_D(AB \cap (D + v - AZ^d)) = AB - v + AZ^d.$$

This yields the first inclusion. The second one is immediate. \square

From Proposition 4 and Lemma 11, we get by recursion the next result.

Corollary 12. *Let $n \geq 1$ and $(v_1, \dots, v_n) \in \mathbb{D}^n$.*

1. *One has $(f_{v_2} \circ \dots \circ f_{v_n})^{-1}(\Delta_{v_1}) \subset A^n \Delta_D + Z^d$.*
2. *The discontinuity set of $f_{v_n} \circ \dots \circ f_{v_1}$ is contained in*

$$\Delta_{v_1} \cup f_{v_1}^{-1}(\Delta_{v_2}) \cup \dots \cup (f_{v_{n-1}} \circ \dots \circ f_{v_1})^{-1}(\Delta_{v_n}),$$

which is contained in $(A\Delta_D + Z^d) \cup \dots \cup (A^n \Delta_D + Z^d)$.

3. *If ∂D is a null set, all those sets are null sets.*

2.3 General results on Markov chains

In the proof of Theorem 5, a key argument is the general theorem below, which is very close to Theorem 3 and Corollary 4 in [1] (paper written in French).

Theorem 13. *Let (E, \mathcal{E}) be a Polish space endowed with its Borel σ -field, (F, \mathcal{F}) be any measurable space, and $f : E \times F \rightarrow E$ be any measurable map. On probability space $(\Omega, \mathcal{A}, \mathbb{P})$, consider a (possibly non-stationary) Markov chain $X = (X_n)_{n \in \mathbb{Z}}$ indexed by the set of all relative integers, taking values in (E, \mathcal{E}) , whose evolution is governed by some sequence $V = (V_n)_{n \in \mathbb{Z}}$ of independent random variables taking values in (F, \mathcal{F}) as follows: for every $n \in \mathbb{Z}$,*

- V_{n+1} is independent of $\mathcal{F}_n^{X,V} := \sigma((X_k, V_k)_{k \leq n})$;
- $X_{n+1} = f(X_n, V_{n+1})$.

Assume that the tail σ -field $\mathcal{F}_{-\infty}^{X,V} := \bigcap_{n \in \mathbb{Z}} \mathcal{F}_n^{X,V}$ is trivial. Then for every $n \in \mathbb{Z}$, there exists some random variable U_n which is uniform on $[0, 1]$ or some finite set (not depending on n), independent of \mathcal{F}_n^V , and such that $\mathcal{F}_n^{X,V} = \mathcal{F}_n^V \vee \sigma(U_n)$.

Note $X_{\leq n} := (X_k)_{k \leq n}$ and $V_{\leq n} := (V_k)_{k \leq n}$. Assuming that E is a Polish space ensures the existence of the conditional law $\nu_n := \mathcal{L}(X_{\leq n} | V_{\leq n})$ and the possibility to order in a measurable way the atoms of ν_n (when ν_n has many atoms). Another way to state the conclusion is to say that the conditional laws ν_n are almost surely diffuse (for all n simultaneously) or uniform on some random finite set with constant size (not depending on n). To keep the present paper self-contained, we give a proof now.

Proof. Let Y be a copy of X , such that X and Y are i.i.d. conditionally on V , namely

$$\mathcal{L}((X, Y) | V) = \mathcal{L}(X | V) \otimes \mathcal{L}(X | V).$$

Then the recursion relations $Y_{n+1} = f(Y_n, V_{n+1})$ hold almost surely; by restricting the probability space, we may and we do assume that they hold on the whole space Ω . Therefore, the event $[X_{\leq n} = Y_{\leq n}]$ does not depend on the integer n , so it equals the event $X = Y$. By Lemma 14 below, for each $n \in \mathbb{Z}$, V_{n+1} is independent of $(X_{\leq n}, Y_{\leq n}, V_{\leq n})$.

$$\begin{aligned} \mathbb{P}[X_{\leq n+1} = Y_{\leq n+1} | \mathcal{F}_{n+1}^{X,V}] &= \mathbb{P}[X_{\leq n} = Y_{\leq n} | \mathcal{F}_{n+1}^{X,V}] \\ &= \mathbb{P}[X_{\leq n} = Y_{\leq n} | \mathcal{F}_n^{X,V} \vee \sigma(V_{n+1})] \\ &= \mathbb{P}[X_{\leq n} = Y_{\leq n} | \mathcal{F}_n^{X,V}] \text{ a.s..} \end{aligned}$$

Thus, the random variable $\mathbb{P}[X_{\leq n} = Y_{\leq n} | \mathcal{F}_n^{X,V}]$ does not depend on n (almost surely), so it is $\mathcal{F}_{-\infty}^{X,V}$ -measurable, hence almost surely constant, since $\mathcal{F}_{-\infty}^{X,V}$ is trivial.

Call p this constant (not depending on n). The random variables $X_{\leq n}$ and $Y_{\leq n}$ are i.i.d. conditionally on V , and also i.i.d. conditionally on $V_{\leq n}$, since the additional information given by $V_{\geq n+1}$ is independent of $(X_{\leq n}, Y_{\leq n}, V_{\leq n})$ (by Lemma 14 again). Thus $\mathcal{L}(Y_{\leq n} | (X_{\leq n}, V_{\leq n})) = \mathcal{L}(Y_{\leq n} | V_{\leq n}) = \nu_n$ almost surely and

$$p = \mathbb{E}[\mathbf{1}_{[X_{\leq n} = Y_{\leq n}]} | \mathcal{F}_n^{X,V}] = \nu_n\{X_{\leq n}\} \text{ a.s..}$$

Therefore, ν_n is almost surely diffuse if $p = 0$, and almost surely purely atomic if $p > 0$. In the latter case, ν_n is almost surely uniform on some random finite set with size $1/p$ since all atoms have the same mass p . \square

Lemma 14. *Keep the notations and the assumptions of Theorem 13. Let $Y = (Y_n)_{n \in \mathbb{Z}}$ be a copy of X such that X and Y are i.i.d. conditionally to V . Then for every $n \in \mathbb{Z}$, V_{n+1} is independent of $\mathcal{F}_n^{X,Y,V}$.*

Moreover, if the process $(X_n, V_n)_{n \in \mathbb{Z}}$ is stationary, $(X_n, Y_n, V_n)_{n \in \mathbb{Z}}$ is also stationary.

Proof. Fix $v \in \mathbb{D}$ and consider an event of the form $A \cap B \cap C$, where A, B, C belong to $\mathcal{F}_n^X, \mathcal{F}_n^Y, \mathcal{F}_n^V$ respectively. Since X and Y are independent conditionally on $\sigma(V)$, and since $\sigma(V) = \mathcal{F}_n^V \vee \sigma(V_{n+1}, V_{n+2}, \dots)$ where $\sigma(V_{n+1}, V_{n+2}, \dots)$ is independent of $\mathcal{F}_n^{X,V}$ and of $\mathcal{F}_n^{Y,V}$, one has

$$\begin{aligned} \mathbb{E}[\mathbf{1}_A \mathbf{1}_B \mathbf{1}_C \mathbf{1}_{[V_{n+1}=v]} | \sigma(V)] &= \mathbb{E}[\mathbf{1}_A | \sigma(V)] \mathbb{E}[\mathbf{1}_B | \sigma(V)] \mathbf{1}_C \mathbf{1}_{[V_{n+1}=v]} \\ &= \mathbb{E}[\mathbf{1}_A | \mathcal{F}_n^V] \mathbb{E}[\mathbf{1}_B | \mathcal{F}_n^V] \mathbf{1}_C \mathbf{1}_{[V_{n+1}=v]} \end{aligned}$$

Taking expectations and using that V_{n+1} is independent of \mathcal{F}_n^V , we get

$$\mathbb{P}(A \cap B \cap C \cap [V_{n+1} = v]) = \mathbb{E}[\mathbb{E}[\mathbf{1}_A | \mathcal{F}_n^V] \mathbb{E}[\mathbf{1}_B | \mathcal{F}_n^V] \mathbf{1}_C] \mathbb{P}[V_{n+1} = v].$$

Summation over all $v \in \mathbb{D}$ yields $\mathbb{P}(A \cap B \cap C) = \mathbb{E}[\mathbb{E}[\mathbf{1}_A | \mathcal{F}_n^V] \mathbb{E}[\mathbf{1}_B | \mathcal{F}_n^V] \mathbf{1}_C]$. Hence

$$\mathbb{P}(A \cap B \cap C \cap [V_{n+1} = v]) = \mathbb{P}(A \cap B \cap C) \mathbb{P}[V_{n+1} = v],$$

which proves that V_{n+1} is independent of $\mathcal{F}_n^{X,Y,V}$.

Now, assume that the process $(X_n, V_n)_{n \in \mathbb{Z}}$ is stationary. Its law $\mathbb{P}_{X,V}$ is invariant by the shift S on $(E \times F)^{\mathbb{Z}}$. With an abuse of notation, call also S the shifts on the factors $E^{\mathbb{Z}}$ and $F^{\mathbb{Z}}$. Fix a regular version $(\nu_v)_{v \in F^{\mathbb{Z}}}$ of the conditional law of Y given V . For every $A \in \mathcal{E}^{\otimes \mathbb{Z}}, B \in \mathcal{E}^{\otimes \mathbb{Z}}, C \in \mathcal{F}^{\otimes \mathbb{Z}}$,

$$\begin{aligned} \mathbb{P}[(S(X), S(Y), S(V)) \in A \times B \times C] &= \mathbb{P}[X \in S^{-1}(A); Y \in S^{-1}(B); V \in S^{-1}(C)] \\ &= \int_{S^{-1}(C)} \nu_v(S^{-1}(A)) \nu_v(S^{-1}(B)) d\mathbb{P}_V(v) \\ &= \int_C \nu_{S^{-1}(u)}(S^{-1}(A)) \nu_{S^{-1}(u)}(S^{-1}(B)) d\mathbb{P}_V(u), \end{aligned}$$

since S preserves \mathbb{P}_V . The probability measures defined by $\nu'_u(A) := \nu_{S^{-1}(u)}(S^{-1}(A))$ still form a regular version of the conditional laws, since for every $A \in \mathcal{E}^{\otimes \mathbb{Z}}$ and $C \in \mathcal{F}^{\otimes \mathbb{Z}}$,

$$\begin{aligned} \int_C \nu'_u(A) d\mathbb{P}_V(u) &= \int_{S^{-1}(C)} \nu_v(S^{-1}(A)) d\mathbb{P}_V(v) \\ &= \mathbb{P}_{X,V}[S^{-1}(A) \times S^{-1}(C)] \\ &= \mathbb{P}_{X,V}[A \times C]. \end{aligned}$$

Hence $\nu'_u = \nu_u$ for \mathbb{P}_V -almost every $u \in F^{\mathbb{Z}}$, so the previous calculation yields

$$\begin{aligned} \mathbb{P}[(S(X), S(Y), S(Z)) \in A \times B \times C] &= \int_C \nu_u(A) \nu_u(B) d\mathbb{P}_V(u) \\ &= \mathbb{P}[(X, Y, Z) \in A \times B \times C]. \end{aligned}$$

We are done. □

3 Utilisation of Theorem 13

In this section, we prove Theorems 5, 7, 8 and Example 6.

3.1 Proof of Theorem 5

On some suitable probability space $(\Omega, \mathcal{A}, \mathbb{P})$, we consider a stationary Markov chain $X = (X_n)_{n \in \mathbb{Z}}$ taking values in D , whose evolution is governed by some sequence $V = (V_n)_{n \in \mathbb{Z}}$ of independent uniform random variables taking values in \mathbb{D} as follows. For every $n \in \mathbb{Z}$,

- X_n is uniform on D ;
- V_{n+1} is independent of $\mathcal{F}_n^{X,V} := \sigma((X_k, V_k))_{k \leq n}$;
- $X_{n+1} = f_{V_{n+1}}(X_n)$.

The last equality implies $T_A(X_{n+1}) = X_n$ and $\pi(X_{n+1}) = V_{n+1}$ by definition of the maps $(f_v)_{0 \leq v \leq r-1}$. Hence for every $n \in \mathbb{Z}$, $\mathcal{F}_n^{X,V} = \sigma(X_n)$. Moreover,

$$\Psi(X_0) = (\pi(T_A^n(X_0)))_{n \geq 0} = (\pi(X_{-n}))_{n \geq 0} = (V_{-n})_{n \geq 0}.$$

Hence, to prove that Ψ is almost surely s -to one for some positive integer s , it suffices to prove that $\mathcal{L}(X_0 | \mathcal{F}_0^V)$ is almost surely uniform on some random set with constant size. Note that $\mathcal{L}(X_0 | \mathcal{F}_0^V) = \mathcal{L}(X_0 | V)$ almost surely since $(V_n)_{n \geq 1}$ is independent of $\mathcal{F}_0^{X,V}$.

First, we prove that the tail σ -field $\mathcal{F}_{-\infty}^{X,V}$ is trivial. Let $E \in \mathcal{F}_{-\infty}^{X,V}$. For every $n \leq 0$, $E \in \sigma(X_n)$, so $E = [X_n \in B_n] = [X_0 \in T_A^{-n}(B_n)]$ for some $B_n \in \mathcal{B}(D)$. Hence

$$E = [X_0 \in B] \text{ where } B = \liminf_{n \rightarrow -\infty} T_A^{-n}(B_n)$$

Since T_A is exact (Proposition 10), we derive $\mathbb{P}(E) = \lambda(B) \in \{0, 1\}$.

Therefore, Theorem 13 applies and shows that the conditional law $\mathcal{L}(X_0 | V)$ is almost surely diffuse or almost surely uniform on some finite set with constant size. It remains to rule out the first possibility. We do that by using a coupling argument.

Consider another Markov chain $Y = (Y_n)_{n \in \mathbb{Z}}$ taking values in D such that X and Y are i.i.d. conditionally on V , namely $\mathcal{L}((X, Y) | V) = \mathcal{L}(X | V) \otimes \mathcal{L}(Y | V)$. In particular, the recursion relations $Y_{n+1} = f_{V_{n+1}}(Y_n)$ hold almost surely. By restricting the probability space, we may - and we do - assume that they hold on the whole space Ω . For each $v \in \mathbb{D}$, the map $y \mapsto f_v(y) - A^{-1}y$ takes finitely many values on D . Call α_v the partition of D associated to this map.

For every $n \geq 0$, let Σ_n be the random partition of D defined by

$$\Sigma_n = \alpha_{V_1} \vee f_{V_1}^{-1}(\alpha_{V_2}) \vee \cdots \vee (f_{V_{n-1}} \circ \cdots \circ f_{V_1})^{-1}(\alpha_{V_n}).$$

For every $y \in D$, call $\Sigma_n(y)$ the unique block of Σ_n which contains y . View figure 1.

On each block of Σ_n , the maps $y \mapsto f_{V_1}(y) - A^{-1}y$, $y \mapsto (f_{V_2} \circ f_{V_1})(y) - A^{-1}f_{V_1}(y), \dots$, $y \mapsto (f_{V_n} \circ \cdots \circ f_{V_1})(y) - A^{-1}(f_{V_{n-1}} \circ \cdots \circ f_{V_1})(y)$ are constant, hence the map $y \mapsto (f_{V_n} \circ \cdots \circ f_{V_1})(y) - A^{-n}y$ is constant. And since $(f_{V_n} \circ \cdots \circ f_{V_1})(X_0) = X_n$ we derive

$$(f_{V_n} \circ \cdots \circ f_{V_1})(\Sigma_n(X_0)) = X_n + A^{-n}(\Sigma_n(X_0) - X_0).$$

We have $\Sigma_n(X_0) \neq \Sigma_{n+1}(X_0)$ if and only if $\Sigma_n(X_0)$ is not contained in some block of the partition $(f_{V_n} \circ \cdots \circ f_{V_1})^{-1}(\alpha_{V_{n+1}})$, i.e. $(f_{V_n} \circ \cdots \circ f_{V_1})(\Sigma_n(X_0))$ is not contained in some block of the partition $\alpha_{V_{n+1}}$.

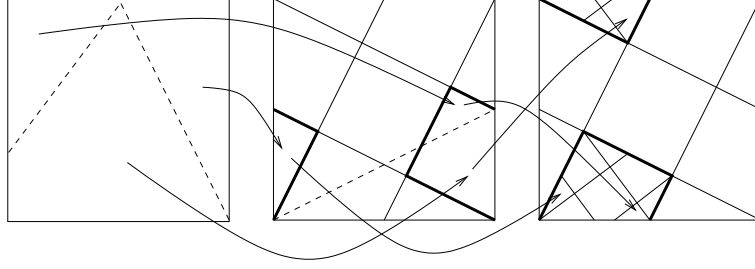


Figure 1: Example where $A = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}$, $D = [0, 1]^2$, $V_1 = (-1, 0)$ and $V_2 = (0, 0)$. The first square represents the partition $\Sigma_2 = \alpha_{V_1} \vee f_{V_1}^{-1}(\alpha_{V_2})$. The second square represents the subset $f_{V_1}(D)$ and the partition α_{V_2} . The third square represents the subset $f_{V_2}(D)$ when $V_2 = (1, 0)$. The arrows represent the effect of $f_{V_2} \circ f_{V_1}$ on each block of Σ_2 .

Let us endow \mathbb{R}^d with some norm $|\cdot|$ and $\mathcal{M}_d(\mathbb{R})$ with the associated operator norm. $(f_{V_n} \circ \dots \circ f_{V_1})(\Sigma_n(X_0))$ is contained in the closed ball $\bar{B}(X_n, \|A^{-n}\|\text{diam}(D))$, where diam stands for diameter. We derive the implications

$$\begin{aligned} \Sigma_n(X_0) \neq \Sigma_{n+1}(X_0) &\implies f_{V_{n+1}} \text{ is not constant on } \bar{B}(X_n, \|A^{-n}\|\text{diam}(D)) \\ &\implies \bar{B}(X_n, \|A^{-n}\|\text{diam}(D)) \cap \Delta_{V_{n+1}} \neq \emptyset \\ &\implies \text{dist}(X_n, \Delta_{V_{n+1}}) \leq \|A^{-n}\|\text{diam}(D). \end{aligned}$$

But X_n and V_{n+1} are independent, X_n is uniform on D and V_{n+1} is uniform on D , so

$$\mathbb{P}[\Sigma_n(X_0) \neq \Sigma_{n+1}(X_0)] \leq \frac{1}{r} \sum_{v \in \mathbb{D}} \lambda(\{x \in D : \text{dist}(x, \Delta_v) \leq \|A^{-n}\|\text{diam}(D)\}).$$

For every subset S of \mathbb{R}^d , and every $\varepsilon > 0$, we note $S_\varepsilon := \{x \in \mathbb{R}^d : \text{dist}(x, S) < \varepsilon\}$ and $S_{\varepsilon+} := \{x \in \mathbb{R}^d : \text{dist}(x, S) \leq \varepsilon\}$. Given $v \in \mathbb{D}$, by proposition 4,

$$\Delta_v = A\Delta_D - v = \bigcup_{k \in \mathbb{Z}^d} A\partial D + Ak - v.$$

Since Δ_v is closed, the lower bound defining $\text{dist}(x, \Delta_v)$ is achieved, so for every $\varepsilon > 0$,

$$(\Delta_v)_{\varepsilon+} = \bigcup_{k \in \mathbb{Z}^d} (A\partial D - v + Ak)_{\varepsilon+}$$

and

$$\lambda(D \cap (\Delta_v)_{\varepsilon+}) \leq \sum_{k \in \mathbb{Z}^d} \lambda(D \cap (A\partial D - v + Ak)_{\varepsilon+}).$$

Since D and ∂D are bounded, the fundamental domain D intersects only finitely many, m_i say, subsets $(A\partial D - v + k)_1$ with $k \in \mathbb{Z}^d$. Hence, for $\varepsilon \in]0, 1[$,

$$\lambda(D \cap (\Delta_v)_{\varepsilon+}) \leq m_i \lambda((A\partial D)_{\varepsilon+}).$$

Let $\alpha > 0$ such that $\dim_{\text{upper box}}(\partial D) < d - \alpha$. Since $A\partial D$ and ∂D have the same upper box dimension,

$$\liminf_{\varepsilon \rightarrow 0} \frac{|\ln \lambda((A\partial D)_{\varepsilon+})|}{|\ln \varepsilon|} = \liminf_{\varepsilon \rightarrow 0} \frac{|\ln \lambda((A\partial D)_\varepsilon)|}{|\ln \varepsilon|} > \alpha,$$

so $\lambda((A\partial D)_\varepsilon) \ll \varepsilon^\alpha$ as $\varepsilon \rightarrow 0$.

Putting things together yields

$$\mathbb{P}[\Sigma_n(X_0) \neq \Sigma_{n+1}(X_0)] \leq \frac{1}{r} \sum_{i=0}^{r-1} m_i \lambda((A\partial D)_{\|A^{-n}\|\text{diam}(D)_+}) \ll \|A^{-n}\|^\alpha \text{ as } n \rightarrow +\infty.$$

Since $\|A^{-n}\|^{1/n} \rightarrow \rho(A^{-1}) < 1$ as $n \rightarrow +\infty$, the series $\sum_n \mathbb{P}[\Sigma_n(X_0) \neq \Sigma_{n+1}(X_0)]$ converges, so Borel-Cantelli Lemma applies. Almost surely, the sequence $(\Sigma_n(X_0))_{n \geq 0}$ is eventually constant.

Let Σ_∞ be the random partition $\bigvee_{n \geq 1} \Sigma_n$ and Σ_∞^+ be the collection of all blocs of positive measure in Σ_∞ . Then $\lambda(\Sigma_\infty(X_0)) > 0$ i.e. $\Sigma_\infty(X_0) \in \Sigma_\infty^+$ almost surely. Conditionally on V , the random variables X_0 and Y_0 are independent and equidistributed. Since Σ_∞ is a function of $(V_n)_{n \geq 1}$, we have almost surely

$$\begin{aligned} \mathbb{P}[\Sigma_\infty(X_0) = \Sigma_\infty(Y_0) | V] &\geq \sum_{B \in \Sigma_\infty^+} \mathbb{P}[\Sigma_\infty(X_0) = \Sigma_\infty(Y_0) = B | V] \\ &= \sum_{B \in \Sigma_\infty^+} \mathbb{P}[X_0 \in B; Y_0 \in B | V] = \sum_{B \in \Sigma_\infty^+} \mathbb{P}[X_0 \in B | V]^2, \end{aligned}$$

whereas

$$\sum_{B \in \Sigma_\infty^+} \mathbb{P}[X_0 \in B | V] = \sum_{B \in \Sigma_\infty^+} \mathbb{P}[\Sigma_\infty(X_0) = B | V] = \mathbb{P}[\Sigma_\infty(X_0) \in \Sigma_\infty^+ | V] = 1.$$

Thus $\mathbb{P}[\Sigma_\infty(X_0) = \Sigma_\infty(Y_0) | V] > 0$ almost surely.

On the event $[\Sigma_\infty(X_0) = \Sigma_\infty(Y_0)]$, we have for every $n \geq 0$,

$$|Y_n - X_n| \leq \|A\|^{-n} |Y_0 - X_0| \leq \|A\|^{-n} \text{diam}(D).$$

By stationarity, we derive

$$\begin{aligned} \mathbb{P}[|Y_0 - X_0| \leq \|A\|^{-n} \text{diam}(D)] &= \mathbb{P}[|Y_n - X_n| \leq \|A\|^{-n} \text{diam}(D)] \\ &\geq \mathbb{P}[\Sigma_\infty(X_0) = \Sigma_\infty(Y_0)] \end{aligned}$$

Letting n go to infinity yields $\mathbb{P}[Y_0 = X_0] \geq \mathbb{P}[\Sigma_\infty(X_0) = \Sigma_\infty(Y_0)] > 0$. Therefore, $\mathbb{P}[Y_0 = X_0 | V] > 0$ with positive probability, so the conditional law $\mathcal{L}(X_0 | V)$ has atoms with positive probability. The proof is complete.

3.2 Proof of Theorem 7

Set $Q = [0, 1]^d$. We now assume that $D = c + UQ$ for some $c \in \mathbb{R}^d$ and some matrix $U \in \mathcal{M}_d(\mathbb{Z})$ with determinant ± 1 .

For each $v \in \mathbb{D}$, call α_v the partition of D associated to this map $y \mapsto f_v(y) - A^{-1}y$. Let $(V_n)_{n \geq 1}$ be a sequence of independent uniform random variables on \mathbb{D} . For every $n \geq 0$, let Σ_n be the random partition of D defined by

$$\Sigma_n = \alpha_{V_1} \vee f_{V_1}^{-1}(\alpha_{V_2}) \vee \cdots \vee (f_{V_{n-1}} \circ \cdots \circ f_{V_1})^{-1}(\alpha_{V_n}).$$

In the proof of Theorem 5, we viewed that given a random variable X_0 uniform on D and independent of $(V_n)_{n \geq 1}$, the sequence $(\Sigma_n(X_0))_{n \geq 0}$ is stationary. Thus for almost every $x_0 \in D$, the sequence $(\Sigma_n(x_0))_{n \geq 0}$ is stationary. We are going to prove that the restriction ‘almost’ can be removed.

Lemma 15. *For every $x_0 \in D$, the sequence $(\Sigma_n(x_0))_{n \geq 0}$ is stationary.*

Proof. Replacing A and D with $U^{-1}AU$ and $U^{-1}D$ preserves the assumptions, so we may and we do assume (without loss of generality) that $D = c + Q$. Then ∂D is the set of all $x \in \mathbb{R}^d$ such that $x - c$ has at least one coordinate in \mathbb{Z} .

Since A has integer entries, its adjugate matrix \tilde{A} also has integer entries. Since $A^{-1} = (\det A)^{-1} \tilde{A} = \pm r^{-1} \tilde{A}$, we derive that for every $v \in \mathbb{D}$,

$$\begin{aligned} \Delta_v &= A\partial D + AZ^d - v \\ &= \{y \in \mathbb{R}^d : \exists i \in \llbracket 1, d \rrbracket, (A^{-1}(y + v - c))_i \in \mathbb{Z}\} \\ &= \{y \in \mathbb{R}^d : \exists i \in \llbracket 1, d \rrbracket, (\tilde{A}(y + v - c))_i \in r\mathbb{Z}\} \\ &\subset \{y \in \mathbb{R}^d : \exists i \in \llbracket 1, d \rrbracket, \tilde{A}_{i,\cdot}(y - c) \in \mathbb{Z}\}, \end{aligned}$$

where $\tilde{A}_{i,\cdot}$ denotes the i -th row of \tilde{A} .

For every $n \geq 0$, set $Z_n := (f_{V_n} \circ \dots \circ f_{V_1})(x_0)$. Then $(f_{V_n} \circ \dots \circ f_{V_1})(\Sigma_n(x_0)) = Z_n + A^{-n}(\Sigma_n(x_0) - x_0)$. Adapting the arguments given in the proof of Theorem 5, we get

$$\begin{aligned} \Sigma_n(x_0) \neq \Sigma_{n+1}(x_0) &\iff f_{V_{n+1}} \text{ is not constant on } \Sigma_n(x_0) \\ &\implies Z_n + A^{-n}(\Sigma_n(x_0) - x_0) \cap \Delta_{V_{n+1}} \neq \emptyset \\ &\implies \exists i \in \llbracket 1, d \rrbracket, \tilde{A}_{i,\cdot}(Z_n + v - c + A^{-n}(\Sigma_n(x_0) - X_0)) \cap r\mathbb{Z} \neq \emptyset. \end{aligned}$$

Let us endow \mathbb{R}^d with the usual norm $|\cdot|_\infty$. The associated operator norm $\|\cdot\|_\infty$ on $\mathcal{M}_d(\mathbb{R})$ is given by

$$\|M\|_\infty = \max_{i \in \llbracket 1, d \rrbracket} \|M_{i,\cdot}\|_1, \text{ where } \|M_{i,\cdot}\|_1 := \sum_{j=1}^d |M_{i,j}|.$$

The diameter of $\Sigma_n(x_0)$ is at most $\text{diam}(D) = 1$. Since for every $i \in \llbracket 1, d \rrbracket$,

$$\|\tilde{A}_{i,\cdot} A^{-n}\|_1 = \|(\det A)(A^{-n-1})_{i,\cdot}\|_1 \leq r \|A^{-n-1}\|_\infty,$$

the diameter of $\tilde{A}_{i,\cdot}(Z_n - c + A^{-n}(\Sigma_n(x_0) - x_0))$ in \mathbb{R} is at most $r \|A^{-n-1}\|_\infty$. Therefore

$$\Sigma_n(x_0) \neq \Sigma_{n+1}(x_0) \implies \exists i \in \llbracket 1, d \rrbracket, \text{dist}(\tilde{A}_{i,\cdot}(Z_n - c), \mathbb{Z}) \leq r \|A^{-n-1}\|_\infty.$$

For every $x \in \mathbb{R}^d$ (respectively $x \in \mathbb{R}$), call \bar{x} its equivalence class in $\mathbb{R}^d/\mathbb{Z}^d$ (respectively \mathbb{R}/\mathbb{Z}). Since the matrix \tilde{A} has integer entries, the linear forms $\phi_i : x \mapsto \tilde{A}_{i,\cdot}x$ on \mathbb{R}^d yield group morphisms $\bar{\phi}_i : \mathbb{R}^d/\mathbb{Z}^d \rightarrow \mathbb{R}/\mathbb{Z}$ by taking quotients.

By proposition 4,

- the random variable Z_n is uniform on the set $T_{A,D}^{-n}(\{x_0\})$,
- the random variable $\overline{Z_n}$ is uniform on $T_A^{-n}(\{\bar{x}_0\}) = \overline{A^{-n}x_0} + (A^{-n}\mathbb{Z}^d)/\mathbb{Z}^d$,
- the random variable $\overline{Z_n - A^{-n}x_0}$ is uniform on the finite group $(A^{-n}\mathbb{Z}^d)/\mathbb{Z}^d$.
- the random variable $\overline{\phi_i(Z_n - A^{-n}x_0)} = \overline{\phi_i(\overline{Z_n A^{-n}x_0})}$ is uniform on the finite group $\overline{\phi_i}((A^{-n}\mathbb{Z}^d)/\mathbb{Z}^d) = \overline{\phi_i}(A^{-n}\mathbb{Z}^d)$.

The set $\phi_i(\mathbb{Z}^d)$ is subgroup of \mathbb{Z} , and also a subgroup of $\phi_i(A^{-n}\mathbb{Z}^d)$, with index $\leq r^n$, since \mathbb{Z}^d is a subgroup of $A^{-n}\mathbb{Z}^d$ with index r^n . Moreover, since A^{-n} is invertible, $\phi_i(A^{-n}e_j) \neq 0$ for at least one $j \in \llbracket 1, d \rrbracket$, where (e_1, \dots, e_d) is the canonical basis of \mathbb{R}^d . As $|\phi_i(A^{-n}e_j)| \leq \|\tilde{A}_i \cdot A^{-n}\|_1 \leq r\|A^{-n-1}\|_\infty$, we derive that

$$\phi_i(A^{-n}\mathbb{Z}^d) = \alpha_{n,i}\mathbb{Z} \text{ for some positive rational number } \alpha_{n,i} < r\|A^{-n-1}\|_\infty.$$

Set $\alpha_{n,i} = p_{n,i}/q_{n,i}$ where $p_{n,i}$ and $q_{n,i}$ are positive and relatively prime integers. Then

$$\overline{\phi_i(A^{-n}\mathbb{Z}^d)} = (q_{n,i}^{-1}\mathbb{Z})/\mathbb{Z}.$$

Note that any interval with length $2r\|A^{-n-1}\|_\infty$ contains at most $\lfloor q_{n,i}2r\|A^{-n-1}\|_\infty \rfloor + 1$ points of $q_{n,i}^{-1}\mathbb{Z}$. Putting things together, we derive

$$\begin{aligned} \mathbb{P}[\Sigma_n(x_0) \neq \Sigma_{n+1}(x_0)] &\leq \sum_{i=1}^d \mathbb{P}[\text{dist}(\tilde{A}_i \cdot (Z_n - c), \mathbb{Z}) \leq r\|A^{-n-1}\|_\infty] \\ &\leq d \frac{q_{n,i}2r\|A^{-n-1}\|_\infty + 1}{q_{n,i}} \\ &\leq d(2r\|A^{-n-1}\|_\infty + \alpha_{n,i}) \\ &\leq 3dr\|A^{-n-1}\|_\infty. \end{aligned}$$

The series $\sum_n \mathbb{P}[\Sigma_n(x_0) \neq \Sigma_{n+1}(x_0)]$ converges and Borel - Cantelli lemma yields the result. \square

The geometric decay of $\mathbb{P}[\Sigma_n(x_0) \neq \Sigma_{n+1}(x_0)]$ as $n \rightarrow +\infty$ lead to conjecture a stronger result.

Conjecture 16. *For every $x_0 \in D$, the sequence $(\Sigma_n)_{n \geq 0}$ is stationary.*

Now, let us prove Theorem 7. Fix a sequence $v_0, v_{-1}, v_{-2}, \dots$ and x_0 as in the assumptions, and keep the notations of the proof of Theorem 5.

For every $n \geq 0$, the random map $f_{V_n} \circ \dots \circ f_{V_1}$ is continuous at x_0 , so x_0 is in the interior (in D) of the block $\Sigma_n(X_0)$. By lemma 15, almost surely, the sequence $(\Sigma_n(x_0))_{n \geq 1}$ is eventually constant equal to $\Sigma_\infty(x_0)$. Thus the random variable $R_0 := \text{dist}(x_0, D \setminus \Sigma_\infty(x_0))$ is positive, and the the open ball $B(x_0, R_0)$ is contained in $\Sigma_\infty(x_0)$.

Fix $\delta > 0$ such that $\mathbb{P}[R_0 \geq \delta] > 0$. Thus, on the event $[R_0 \geq \delta]$, the maps $y \mapsto f_{V_n} \circ \dots \circ f_{V_1}(y) - A^{-n}y$ are constant on the ball $B(x_0, \delta)$. By assumption, one can fix $n_0 \geq 1$ such that $f_{v_0} \circ \dots \circ f_{v_{-n_0+1}}(D) \subset B(x_0, \delta)$. Since the event $[R_0 \geq \delta]$ depends only on $(V_k)_{k \geq 1}$, one has

$$\mathbb{P}[R_0 \geq \delta ; (V_0, \dots, V_{-n_0+1}) = (v_0, \dots, v_{-n_0+1})] = r^{-n_0} \mathbb{P}[R_0 \geq \delta] > 0.$$

Moreover, on the event $[R_0 \geq \delta ; (V_0, \dots, V_{-n_0+1}) = (v_0, \dots, v_{-n_0+1})]$, one has

$$\forall k \geq 0, \quad |X_k - f_{V_k} \circ \dots \circ f_{V_1}(x_0)| \leq \|A^{-k}\| \times |X_0 - x_0| \leq \|A^{-k}\| \delta.$$

For each $n \in \mathbb{Z}$, one can define in a same way a random variable R_n depending only on $(V_{n+k})_{k \geq 1}$: R_n is the largest radius such that the open ball $B(x_0, R_n)$ is contained in the block containing x_0 in the partition

$$\bigvee_{k \geq 1} (f_{V_{n+k-1}} \circ \dots \circ f_{V_{n+1}})^{-1}(\alpha_{V_{n+k}}).$$

The ergodicity of the uniform Bernoulli shift on $\mathbb{D}^{\mathbb{Z}}$ shows that almost surely, the event $E_n := [R_n \geq \delta ; (V_n, \dots, V_{n-n_0+1}) = (v_0, \dots, v_{-n_0+1})]$ occurs for infinitely many $n \leq 0$.

To prove that the process $(V_n)_{n \leq 0}$ can be recovered as an almost everywhere continuous function of $(X_n)_{n \leq 0}$, fix a time interval $\llbracket -L, 0 \rrbracket$ and a precision level $\varepsilon > 0$. In the construction above, one may fix $\delta > 0$ such that $\delta \max\{\|A^{-n}\| : n \geq 0\} \leq \varepsilon$ and choose n_0 accordingly. Then the random variable $-M := \sup\{n \leq -L : E_n \text{ occurs}\}$ is almost surely finite, and the knowledge of $(V_n)_{-M-n_0 \leq n \leq 0}$ suffices to recover $(X_n)_{-L \leq n \leq 0}$ with an error whose norm is at most ε . Theorem 7 follows.

3.3 Proof of Theorem 8

Assume that $\|A^{-1}\|_{\mathbf{u}, \infty} < 1$ for some \mathbb{Z} -basis $\mathbf{u} = (u_1, \dots, u_d)$ of \mathbb{Z}^d . Take $c \in \mathbb{R}^d$ and $D = c + P_{\mathbf{u}}$. Then one checks that for every $x \in \mathbb{R}^d$,

$$p_D(x) = c + \sum_{i=1}^d \left(u_i^*(x - c) - \lfloor u_i^*(x - c) + 1/2 \rfloor \right) u_i.$$

The discontinuity set of p_D is $\Delta_D = \{x \in \mathbb{R}^d : \exists i \in \llbracket 1, d \rrbracket, u_i^*(x - c) + 1/2 \in \mathbb{Z}\}$.

By Corollary 12, for every $n \geq 1$ and (v_1, \dots, v_n) in $\llbracket 0, r-1 \rrbracket$, the discontinuity set of $f_{v_n} \circ \dots \circ f_{v_1}$ is contained in $(A\Delta_D + \mathbb{Z}^d) \cup \dots \cup (A^n \Delta_D + \mathbb{Z}^d)$. Thus for every $y \in D$,

$$\begin{aligned} y \in \text{Disc}(f_{v_n} \circ \dots \circ f_{v_1}) &\implies \exists j \in \llbracket 1, n \rrbracket, \exists k \in \mathbb{Z}^d : A^{-j}(y - k) \in \Delta_D \\ &\implies \exists i \in \llbracket 1, d \rrbracket, \exists j \in \llbracket 1, n \rrbracket, \exists k \in \mathbb{Z}^d : u_i^*(A^{-j}(y - k) - c) \in 1/2 + \mathbb{Z}. \end{aligned} \quad (1)$$

Since A has integer entries, its adjugate matrix \tilde{A} also has integer entries. The equality $A^{-1} = (\det A)^{-1} \tilde{A} = \pm r^{-1} \tilde{A}$, shows that $u_i^*(A^{-j}k) \in r^{-j} \mathbb{Z}$ for every $i \in \llbracket 1, d \rrbracket$ and $j \in \llbracket 1, n \rrbracket$. Hence implication (1) shows that 0 cannot be a discontinuity of $f_{v_n} \circ \dots \circ f_{v_1}$ when $(c = 0$ and r is odd) neither when $1, c_1, \dots, c_d$ are linearly independent over \mathbb{Q} . This proves item 1.

For every $y \in D$, we have $y - c \in P_{\mathbf{u}}$, so $|y - c|_{\mathbf{u}, \infty} \leq 1/2$ and

$$\begin{aligned} |A^{-1}y - c|_{\mathbf{u}, \infty} &\leq \|A^{-1}\|_{\mathbf{u}, \infty} |y|_{\mathbf{u}, \infty} + |c|_{\mathbf{u}, \infty} \\ &\leq \|A^{-1}\|_{\mathbf{u}, \infty} \times (|c|_{\mathbf{u}, \infty} + 1/2) + |c|_{\mathbf{u}, \infty} \\ &\leq (1/2) \|A^{-1}\|_{\mathbf{u}, \infty} + 2|c|_{\mathbf{u}, \infty}. \end{aligned}$$

If $|c|_{\mathbf{u}, \infty} < (1 - \|A^{-1}\|_{\mathbf{u}, \infty})/4$, we derive that for every $y \in D$, $|A^{-1}y - c|_{\mathbf{u}, \infty} < 1/2$, so $A^{-1}y \in D$ and $f_0(y) = A^{-1}y$. By recursion, for every $n \geq 1$, $f_0^n(y) = A^{-n}y$, so $f_0^n(D) \subset \overline{B}(0, \|A^{-n}\|R)$ where $R = \sup\{|y| : y \in D\}$. Item 2 follows.

Item 3 is a direct consequence of items 1 and 2 and of Theorem 7.

3.4 Proof of Example 6

Let

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

Then $A^{-1} = (1/2)A$. The linear map $x \mapsto Ax$ from \mathbb{R}^2 to \mathbb{R}^2 is the composition of $\sqrt{2}\text{Id}$ with the reflexion with regard to the line $\mathbb{R}(\cos \pi/8, \sin \pi/8)$.

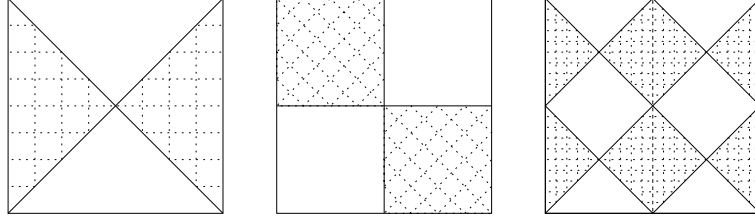


Figure 2: The partitions π , $T_A^{-1}\pi$, $T_A^{-2}\pi$ when $D = [0, 1]^2$. The shaded areas represent P_1 , $T_A^{-1}(P_1)$, $T_A^{-2}(P_1)$.

Call (e_1, e_2) the canonical basis of \mathbb{R}^2 . Take $\mathbb{D} = \{0, e_1\}$. Given a fundamental domain D , the corresponding maps f_0 and $f_1 := f_{e_1}$ from D to D are given by $f_0(y) = p_D(A^{-1}y)$ and $f_1(y) = p_D(A^{-1}y + (e_1 + e_2)/2)$. The associated partition is $\pi = \{P_0, P_1\}$ where $P_0 = f_0(D)$ and $P_1 := f_1(D)$. We want to describe the partitions $(T_A^{-k}\pi)_{k \geq 0}$. Given $x = (x_1, x_2) \in D$, we denote by $\pi(x)$ the index of the block of the partition π containing x . Since $\pi(x) \in \{0, 1\}$, congruences modulo 2 suffice to determine it.

Case where $D = [0, 1]^2$. One has $T_A(x) = (x_1 + x_2 - k, x_1 - x_2 - \ell)$, where $k := \lfloor x_1 + x_2 \rfloor$ and $\ell := \lfloor x_1 - x_2 \rfloor$. One checks that $\pi(x) \equiv \lfloor x_1 + x_2 \rfloor + \lfloor x_1 - x_2 \rfloor \pmod{2}$.

Given an integer $n \geq 0$, if $\pi(T_A^{2n}(x)) \equiv \lfloor 2^n(x_1 + x_2) \rfloor + \lfloor 2^n(x_1 - x_2) \rfloor \pmod{2}$, then

$$\begin{aligned} \pi(T_A^{2n+1}(x)) &\equiv \lfloor 2^n((x_1 + x_2 - k) + (x_1 - x_2 - \ell)) \rfloor \\ &\quad + \lfloor 2^n((x_1 + x_2 - k) - (x_1 - x_2 - \ell)) \rfloor \\ &\equiv \lfloor 2^{n+1}x_1 \rfloor - 2^n(k + \ell) + \lfloor 2^{n+1}x_2 \rfloor - 2^n(k - \ell) \\ &\equiv \lfloor 2^{n+1}x_1 \rfloor + \lfloor 2^{n+1}x_2 \rfloor \pmod{2}, \end{aligned}$$

since the integers $2^n(k + \ell)$ and $2^n(k - \ell)$ have the same parity. Thus

$$\begin{aligned} \pi(T_A^{2n+2}(x)) &\equiv \lfloor 2^{n+1}(x_1 + x_2 - k) \rfloor + \lfloor 2^{n+1}(x_1 - x_2 - \ell) \rfloor \\ &\equiv \lfloor 2^{n+1}(x_1 + x_2) \rfloor - 2^{n+1}k + \lfloor 2^{n+1}(x_1 - x_2) \rfloor - 2^{n+1}\ell \\ &\equiv \lfloor 2^{n+1}(x_1 + x_2) \rfloor + \lfloor 2^{n+1}(x_1 - x_2) \rfloor \pmod{2}, \end{aligned}$$

By recursion, those formulas hold for every $n \geq 0$. See figure 2.

As a result, for every $n \geq 1$, the partition $\pi \vee \dots \vee T_A^{-(n-1)}\pi$ has 2^n blocks, and each block is the union of two isosceles right triangles with small side $2^{-n/2}$, which are symmetric with regard to $(1/2, 1/2)$ (up to the boundaries). Hence, the missing information in the partitions $(T_A^{-k}\pi)_{k \geq 0}$ can be coded by a uniform random variable having two possible values.

Case where $D = [-1/2, 1/2]^2$. This time, one has $T_A(x) = (x_1 + x_2 - k, x_1 - x_2 - \ell)$, where $k := \lfloor x_1 + x_2 + 1/2 \rfloor$ and $\ell := \lfloor x_1 - x_2 + 1/2 \rfloor$. One checks that for every $n \geq 0$,

$$\begin{aligned} \pi(T_A^{2n}(x)) &\equiv \lfloor 2^n(x_1 + x_2) + 1/2 \rfloor + \lfloor 2^{n+1}(x_1 - x_2) + 1/2 \rfloor \pmod{2}, \\ \pi(T_A^{2n+1}(x)) &\equiv \lfloor 2^{n+1}x_1 + 1/2 \rfloor + \lfloor 2^{n+1}x_2 + 1/2 \rfloor \pmod{2}. \end{aligned}$$

See figure 3.

As a result, for every $n \geq 1$, the partition $\pi \vee \dots \vee T_A^{-(n-1)}\pi$ has 2^n blocks, and each block is the union of eight isosceles right triangles with small side $2^{-n/2-1}$. The eight

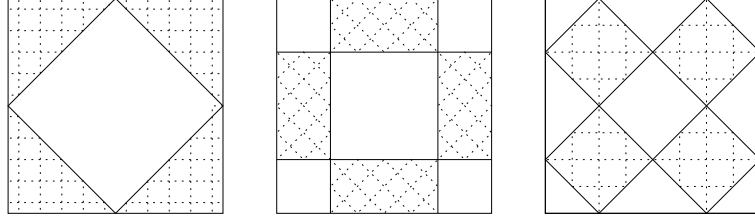


Figure 3: The partitions π , $T_A^{-1}\pi$, $T_A^{-2}\pi$ when $D = [-1/2, 1/2]^2$. The shaded areas represent the blocks P_1 , $T_A^{-1}(P_1)$, $T_A^{-2}(P_1)$.

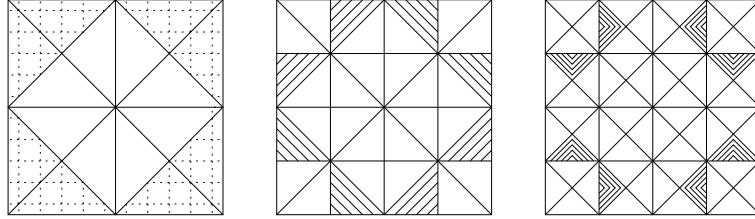


Figure 4: Refinement of the partitions π , $\pi \vee T_A^{-1}\pi$, $\pi \vee T_A^{-1}\pi \vee T_A^{-2}\pi$ when $D = [-1/2, 1/2]^2$. The shaded areas represent P_1 , $P_1 \cap T_A^{-1}(P_1)$, $P_1 \cap T_A^{-1}(P_1) \cap T_A^{-2}(P_1)$. Each one of this block is a union of eight isosceles right triangles.

isometries of the square $[-1/2, 1/2]^2$ preserves each block, up to the boundaries. Hence, the missing information in the partitions $(T_A^{-k}\pi)_{k \geq 0}$ can be coded by a uniform random variable having eight possible values. See figure 4.

Case where $D = [0, 1[e_1 + [0, 1[(e_1 + e_2)$. This parallelogram is a fundamental domain because the couple $(u_1, u_2) := (e_1, e_1 + e_2)$ is a \mathbb{Z} -basis of \mathbb{Z}^2 .

If $x \in D$, then $x = \xi_1 u_1 + \xi_2 u_2$ with ξ_1 and ξ_2 in $[0, 1[$. Since $Au_1 = u_2$ and $Au_2 = 2u_1$, we get $T_A(x) = (2\xi_2 - \lfloor 2\xi_2 \rfloor)u_1 + \xi_1 u_2$ and $T_A^2(x) = (2\xi_1 - \lfloor 2\xi_1 \rfloor)u_1 + (2\xi_2 - \lfloor 2\xi_2 \rfloor)u_2$. The parallelograms $A^{-1}D = [0, 1[u_1 + [0, 1/2[u_2$ and $A^{-1}D + A_1^{-1}u_1 = [0, 1[u_1 + [1/2, 1[u_2$ are contained in D , so those parallelograms are exactly the sets P_0 and P_1 .

One checks that for every $n \geq 1$, the partition $\pi \vee \dots \vee T_A^{-(2n-1)}\pi$ has 4^n blocks, namely the subsets $2^{-n}(D + k_1 u_1 + k_2 u_2)$ where k_1 and k_2 vary in $\llbracket 0, 2^n - 1 \rrbracket$. Hence, the partitions $(T_A^{-k}\pi)_{k \geq 0}$ provide the whole information. See figure 5.

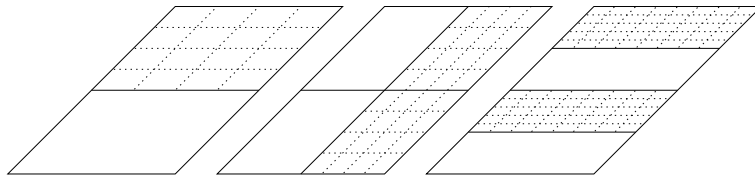


Figure 5: The partitions π , $T_A^{-1}\pi$, $T_A^{-2}\pi$ when $D = [0, 1[e_1 + [0, 1[(e_1 + e_2)$. The shaded areas represent P_1 , $T_A^{-1}(P_1)$, $T_A^{-2}(P_1)$.

4 The approach using radix expansions

In this section, we fix a subset \mathbb{D} of \mathbb{Z}^d containing exactly one element in each equivalence class modulo $A\mathbb{Z}^d$, i.e. such that $\mathbb{Z}^d = \mathbb{D} \oplus A\mathbb{Z}^d$. A recursion yields that for every $n \geq 1$,

$$\mathbb{Z}^d = \mathbb{D} \oplus \dots \oplus A^{n-1}\mathbb{D} \oplus A^n\mathbb{Z}^d.$$

By analogy with the decimal numeration system, we will view \mathbb{D} as the set of all possible digits. By convenience, we assume that $0 \in \mathbb{D}$.

4.1 Hutchinson's map $\tau_{\mathbb{D}}$

In [6], Hutchinson works with finitely many contraction maps in any given complete metric space. Such a family is currently called an *iterated function system*. In our situation, we work with the affine maps $(g_v)_{v \in \mathbb{D}}$ defined on \mathbb{R}^d by $g_v(x) := A^{-1}x + A^{-1}v$. Since $\rho(A^{-1}) < 1$, we can - and we do - endow \mathbb{R}^d with some norm $|\cdot|$ such that $\|A^{-1}\| < 1$, where $\|\cdot\|$ denotes the associated operator norm on $\mathcal{M}_d(\mathbb{R})$. Hence the affine maps $(g_v)_{v \in \mathbb{D}}$ are contractions and Hutchinson's theory applies.

To every Borel subset B of \mathbb{R}^d , we associate the Borel subset

$$\tau_{\mathbb{D}}(B) := A^{-1}B + A^{-1}\mathbb{D} = \bigcup_{v \in \mathbb{D}} (A^{-1}B + A^{-1}v).$$

The Hutchinson's map $\tau_{\mathbb{D}}$ thus defined preserves the inclusion order, the almost everywhere equality (for the Lebesgue measure) and many properties: if B is bounded, open, closed, compact then map $\tau_{\mathbb{D}}(B)$ is still bounded, open, closed, compact. Since \mathbb{D} is finite, the map $\tau_{\mathbb{D}}$ also commutes with the closure operator. Note that if D is a fundamental domain, then $\tau_{\mathbb{D}}(D)$ is still a fundamental domain, since

$$\mathbb{R}^d = D \oplus \mathbb{Z}^d = D \oplus (\mathbb{D} \oplus A\mathbb{Z}^d) = (D \oplus \mathbb{D}) \oplus A\mathbb{Z}^d = A\tau_{\mathbb{D}}(D) \oplus A\mathbb{Z}^d,$$

so $\mathbb{R}^d = A^{-1}\mathbb{R}^d = \tau_{\mathbb{D}}(D) \oplus \mathbb{Z}^d$.

Call \mathcal{K} the collection of all non-empty compact subsets of \mathbb{R}^d . Endow \mathbb{R}^d with the metric given by the norm $|\cdot|$. The associated Hausdorff metric d_H on \mathcal{K} is defined by

$$d_H(K, L) := \max \left(\sup_{x \in K} \text{dist}(x, L), \sup_{y \in L} \text{dist}(y, K) \right),$$

and (\mathcal{K}, d_H) is a complete metric space. One checks that for every K and L in \mathcal{K} ,

$$d_H(\tau_{\mathbb{D}}(K), \tau_{\mathbb{D}}(L)) \leq d_H(A^{-1}K, A^{-1}L) \leq \|A^{-1}\| d_H(K, L).$$

Thus, $\tau_{\mathbb{D}}$ is a contraction map on (\mathcal{K}, d_H) and Banach fixed point theorem applies: for every $K \in \mathcal{K}$, the sequence $(\tau_{\mathbb{D}}^n(K))_{n \geq 0}$ converges to the unique fixed point of $\tau_{\mathbb{D}}$. Actually, this fixed point is the set $K_{\mathbb{D}}$ defined in the introduction.

Indeed, one defines a continuous map $\Phi : \mathbb{D}^{\mathbb{Z}_+^*} \rightarrow \mathbb{R}^d$ by

$$\Phi(v) := \sum_{k \geq 1} A^{-k} v_k,$$

since the series converge normally with regard to $v \in \mathbb{D}^{\mathbb{Z}_+^*}$. Hence the set $K_{\mathbb{D}} = \Phi(\mathbb{D}^{\mathbb{Z}_+^*})$ is compact and, by construction, $K_{\mathbb{D}} = A^{-1}K_{\mathbb{D}} + A^{-1}\mathbb{D}$. So the compact set $K_{\mathbb{D}}$ is the unique fixed point of $\tau_{\mathbb{D}}$ on \mathcal{K} . View figure 6.

We will also use other invariant sets.

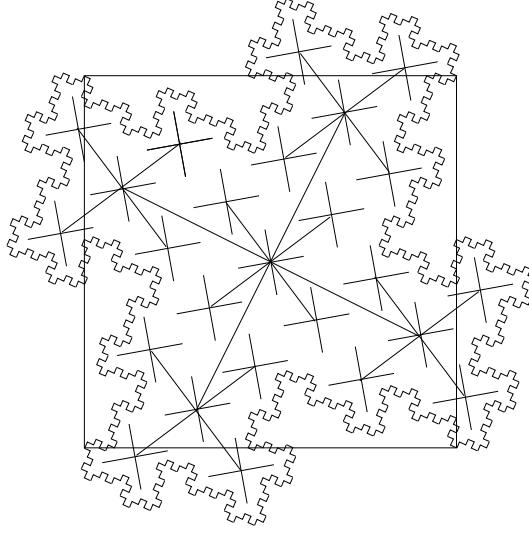


Figure 6: The square $[-1/2, 1/2]^2$ and the compact set $K_{\mathbb{D}}$ when $A = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}$ and $\mathbb{D} = \{(0, 0), (0, 1), (0, -1), (1, 0), (-1, 0)\}$. The partial sums $A^{-1}v_1$, $A^{-1}v_1 + A^{-2}v_2$ and $A^{-1}v_1 + A^{-2}v_2 + A^{-3}v_3$ where $(v_1, v_2, v_3) \in \mathbb{D}^3$ are drawn.

Lemma 17. *For any Borel set B , the set*

$$\limsup_{n \rightarrow +\infty} \tau_{\mathbb{D}}^n(B) := \{x \in \mathbb{R}^d : x \in \tau_{\mathbb{D}}^n(B) \text{ for infinitely many } n\}$$

is invariant by $\tau_{\mathbb{D}}$.

Proof. Let $L = \limsup_{n \rightarrow +\infty} \tau_{\mathbb{D}}^n(B)$. We prove that $\tau_{\mathbb{D}}(L) = L$ by double inclusion.

If $x \in \tau_{\mathbb{D}}(L)$, then $Ax = y + z$ with $y \in L$ and $z \in \mathbb{D}$. For infinitely many n , $y \in \tau_{\mathbb{D}}^n(B)$, so $x \in A^{-1}(\tau_{\mathbb{D}}^n(B) + \mathbb{D}) = \tau_{\mathbb{D}}^{n+1}(B)$. Thus $x \in L$.

Conversely, if $x \in L$, then Ax belongs to $A\tau_{\mathbb{D}}^n(B) = \tau_{\mathbb{D}}^{n-1}(B) + \mathbb{D}$ for infinitely many $n \geq 1$. For those n , let $Ax = y_n + z_n$ with $y_n \in \tau_{\mathbb{D}}^{n-1}(B)$ and $z_n \in \mathbb{D}$. Since \mathbb{D} is finite, the sequence $(z_n)_{n \geq 1}$ achieves some value z infinitely many times. Hence $y_n = Ax - z$ for infinitely many n , so $Ax - z$ belongs to L and x belongs to $\tau_{\mathbb{D}}(L)$. \square

4.2 A measure-preserving map $T_{A,E}$ which is isomorphic to the uniform Bernoulli shift on \mathbb{D}^∞

The results and the arguments given in the next two subsections are very similar to those given by Hacon, Saldanha, Veerman in [4]. Yet, our presentation differs slightly since we focus on the measure-preserving map T_A . Moreover, we show that many properties of the self-affine tile $K_{\mathbb{D}}$ also hold for sets of the form $\limsup \tau_{\mathbb{D}}^n(D)$, where D is a bounded fundamental domain.

Proposition 18. *Let $L = K_{\mathbb{D}}$ or $L = \limsup \tau_{\mathbb{D}}^n(D)$, where D is a bounded fundamental domain. Then*

1. *One has $\bar{L} = K_{\mathbb{D}}$.*
2. *One has $\mathbb{R}^d = L + \mathbb{Z}^d$.*

3. One has $0 < \lambda(L) < +\infty$.
4. The set L is the union of the sets $(A^{-1}L + A^{-1}v)_{v \in \mathbb{D}}$ and this union is almost disjoint.
5. The subsets $E_0 := \{x \in L : \exists!(y, z) \in L \times \mathbb{D}, x = A^{-1}y + A^{-1}z\}$, $(\tau^n(E_0))_{n \geq 0}$ and $E := \bigcap_{n \geq 0} \tau^n(E_0)$ have full measure.
6. For every $x \in E$, the vector Ax has unique decomposition $y + z$ with $(y, z) \in L \times \mathbb{D}$, and the vector $T_{A,E}(x) := y$ actually belongs to E .

Proof. 1. Since L is non-empty bounded and invariant by $\tau_{\mathbb{D}}$, its closure is non-empty, compact and invariant by $\tau_{\mathbb{D}}$, so $\bar{L} = K_{\mathbb{D}}$.

2. Since $K_{\mathbb{D}}$ is compact, the set $K_{\mathbb{D}} + \mathbb{Z}^d$ is closed. But for all $n \geq 1$

$$K_{\mathbb{D}} + \mathbb{Z}^d \supset A^{-n}\mathbb{D} \oplus \cdots \oplus A^{-1}\mathbb{D} + \mathbb{Z}^d = A^{-n}\mathbb{Z}^d.$$

By Lemma 9, we derive $\mathbb{R}^d = K_{\mathbb{D}} + \mathbb{Z}^d$.

Now assume that $L = \limsup \tau_{\mathbb{D}}^n(D)$, where D is a bounded fundamental domain, and let us check that $L + \mathbb{Z}^d$ equals the whole space \mathbb{R}^d . Fix $x \in \mathbb{R}^d$. For every $n \geq 1$, the set $\tau_{\mathbb{D}}^n(D)$ is still a fundamental domain, so $x = y_n + z_n$ for some (unique) $y_n \in \tau_{\mathbb{D}}^n(D)$ and $z_n \in \mathbb{Z}^d$. Since D and \mathbb{D} are bounded, one checks that the sequence $(y_n)_{n \geq 1}$ is bounded, so the sequence $(z_n)_{n \geq 1}$ varies in some finite set. Thus it achieves some value z infinitely many times, so $y_n = x - z$ for infinitely many n , so $x - z \in L$ and $x \in L + \mathbb{Z}^d$.

3. Item 2 shows that \mathbb{R}^d is the union of the translated sets $L + z$ over all $z \in \mathbb{Z}^d$. Thus $\lambda(L) > 0$. Moreover, $0 < \lambda(L) < +\infty$ since L is bounded.
4. By Lemma 17, $L = \tau_{\mathbb{D}}(L)$ is the union of the sets $(A^{-1}L + A^{-1}v)_{v \in \mathbb{D}}$. This union is almost disjoint since

$$\sum_{v \in \mathbb{D}} \lambda(A^{-1}L + A^{-1}v) = \sum_{v \in \mathbb{D}} r^{-1} \lambda(L) = \lambda(L).$$

5. Item 5 directly follows from item 4.
6. Let $x \in E$ and $(y, z) \in L \times \mathbb{D}$ be the unique couple such that $Ax = y + z$. Then for infinitely many $n \geq 0$, we have $Ax \in \tau^{n+1}(E_0) = \tau^n(E_0) + \mathbb{D}$, so $y \in \tau^n(E_0)$ by uniqueness of the decomposition above, since $\tau^n(E_0) \subset \tau^n(L) = L$. Thus $y \in E$.

The proof is complete. \square

Last item of Proposition 18 provides a measurable map $T_{A,E} : E \rightarrow E$. Let us view some of its properties.

Proposition 19. *Let L , E and $T_{A,E} : E \rightarrow E$ be like in proposition 18. Define a map $\Psi : E \rightarrow \mathbb{D}^\infty$ by*

$$\Psi(x) := (AT_{A,E}^{n-1}(x) - T_{A,E}^n(x))_{n \geq 1}.$$

Then

1. The map $T_{A,E} : E \rightarrow E$ is measurable and preserves $\mathcal{U}_E := \lambda(\cdot|E)$, the uniform measure on E .
2. For every $x \in E$, $\Psi(T_{A,E}(x)) = S(\Psi(x))$, where S is the shift operator on \mathbb{D}^∞ .
3. Given $n \geq 1$ and $(v_1, \dots, v_n) \in \mathbb{D}^n$, the sequence $\Psi(x)$ begins by (v_1, \dots, v_n) if and only if x belongs to $A^{-n}E + A^{-n}v_n + \dots + A^{-1}v_1$. As a result, Ψ is measurable and transforms $\lambda(\cdot|E)$ into the uniform measure $\mathcal{U}_{\mathbb{D}}^{\otimes \infty}$ on \mathbb{D}^∞ .
4. For every $x \in E$, $\Phi(\Psi(x)) = x$. Therefore, the factor map Ψ is injective and the set $\Psi(E) = \{x \in \Psi^{-1}(E) : x = \Phi(\Psi(x))\}$ is Borel.

Hence, Ψ is an isomorphism transforming the measure-preserving map $T_{A,E}$ into the Bernoulli shift S .

Proof. For every Borel subset $B \subset E$,

$$T_{A,E}^{-1}(B) = A^{-1}B \oplus A^{-1}\mathbb{D} = \bigcup_{v \in \mathbb{D}} (A^{-1}B + A^{-1}v).$$

The union above is almost disjoint since $B \subset K_{\mathbb{D}}$. Hence $T_{A,E}^{-1}(B)$ has the same Lebesgue measure as B . Item 1 follows.

Items 2 and 3 are immediate.

Let $x \in E$. Then $A^{-n}T_{A,E}^n(x) \rightarrow 0$ as $n \rightarrow +\infty$, because E is bounded. Thus

$$\begin{aligned} \Phi(\Psi(x)) &= \sum_{n=1}^{+\infty} A^{-n} (AT_{A,E}^{n-1}(x) - T_{A,E}^n(x)) \\ &= \sum_{n=1}^{+\infty} (A^{-(n-1)}T_{A,E}^{n-1}(x) - A^{-n}T_{A,E}^n(x)) = x. \end{aligned}$$

Item 4 follows. □

4.3 The measure-preserving map T_A as a factor of $T_{A,E}$

Recall that for every $x \in E$, $T_{A,E}(x)$ is the only element of $y \in E$ (and also the only element of $y \in L$) such that $Ax - y \in \mathbb{D}$. Calling $p_{\mathbb{T}^d}$ the canonical projection from \mathbb{R}^d onto $\mathbb{T}^d = \mathbb{R}^d/\mathbb{Z}^d$, we derive $T_A(p_{\mathbb{T}^d}(x)) = p_{\mathbb{T}^d}(Ax) = p_{\mathbb{T}^d}(T_{A,E}(x))$. Thus

$$p_{\mathbb{T}^d}|_E \circ T_{A,E} = T_A \circ p_{\mathbb{T}^d}|_E,$$

so the measure $p_{\mathbb{T}^d}(\mathcal{U}_E)$ is invariant by T_A .

For every $z \in \mathbb{R}^d/\mathbb{Z}^d$, call $N(z)$ denotes the size of $p_{\mathbb{T}^d}^{-1}\{z\} \cap E$. Then a computation yields $p_{\mathbb{T}^d}(\mathcal{U}_E) = (N/\lambda(E)) \cdot \eta$, where η is the Haar measure on $\mathbb{R}^d/\mathbb{Z}^d$. In particular, $p_{\mathbb{T}^d}(\mathcal{U}_E)$ is absolutely continuous with regard to η .

By ergodicity of T_A for the Haar measure η , we derive $p_{\mathbb{T}^d}(\mathcal{U}_E) = \eta$, i.e. $N/\lambda(E) = 1$ η -almost everywhere. This shows the next result.

Proposition 20. *Let L , E and $T_{A,E}$ be like in proposition 18. Then*

1. The measure $\lambda(E) = \lambda(L)$ is a positive integer m .

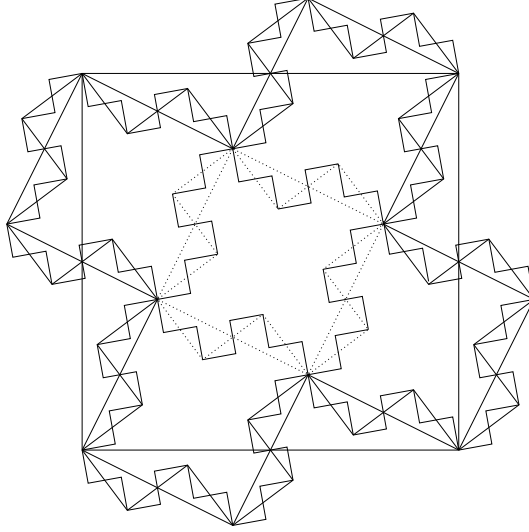


Figure 7: The fundamental domains D_0, D_1, D_2, D_3 when $A = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}$ and $\mathbb{D} = \{(0, 0), (0, 1), (0, -1), (1, 0), (-1, 0)\}$. The set D_0 is the square $[-1/2, 1/2]^2$, the set D_1 is a the big cross. The set D_2 is the union of five small copies of D_1 . The set D_3 is the union of five small copies of D_2 .

2. The transformation T_A is a factor of $T_{A,E}$, hence a factor of the uniform Bernoulli shift on \mathbb{D}^∞ .
3. The factor map $p_{\mathbb{T}^d}|_E$ is m -to-one almost everywhere.

Propositions 19 and 20 show that, up to null sets, $p_{\mathbb{T}^d}|_E \circ \Phi|_{\Psi(E)}$ is a $\lambda(L)$ -to-one factor map transforming the uniform Bernoulli shift on \mathbb{D}^∞ into T_A . If $\lambda(L) = 1$, we have thus an explicit isomorphism. When L equals $K_{\mathbb{D}}$, this fact was already observed by Hacon, Saldanha, Veerman at the end of the first section of [4].

Hence, we look for sufficient conditions A and \mathbb{D} to ensure that $\lambda(K_{\mathbb{D}}) = 1$, or conditions on A and \mathbb{D} and D which ensure that $\lambda(\limsup \tau_{\mathbb{D}}^n(D)) = 1$. The next subsection explains why the case where $L = \limsup \tau_{\mathbb{D}}^n(D)$ (where D is a bounded fundamental domain) is a bit simpler than the case where $L = K_{\mathbb{D}}$.

4.4 Comparison of $K_{\mathbb{D}}$ and $\limsup \tau_{\mathbb{D}}^n(D)$

Fix a bounded fundamental domain D_0 , and for every $n \geq 0$ set

$$D_n = \tau_{\mathbb{D}}^n(D) = A^{-n}D_0 + A^{-n}\mathbb{D} + \dots + A^{-1}\mathbb{D}.$$

Figure 7 represent $K_{\mathbb{D}}$ and D_0, D_1, D_2 when $d = 2$, $r = 5$, $A = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}$, $\mathbb{D} = \{(0, 0), (0, 1), (0, -1), (1, 0), (-1, 0)\}$ and $D = [-1/2, 1/2]^2$.

First, we establish general properties of the sets

$$\limsup_{n \rightarrow +\infty} D_n := \{x \in \mathbb{R}^d : x \in D_n \text{ for infinitely many } n\},$$

$$\liminf_{n \rightarrow +\infty} D_n := \{x \in \mathbb{R}^d : x \in D_n \text{ for all large enough } n\}.$$

Proposition 21. (First properties)

1. The fundamental domains $(D_n)_{n \geq 0}$ are contained in a same closed ball $\overline{B}(0, R)$.
2. The Borel set $\limsup_n D_n$ is invariant.
3. $K_{\mathbb{D}}$ is the closure of $\limsup_n D_n$.
4. The set $\liminf_n D_n$ contains at most one point in each equivalence class of $\mathbf{R}^d / \mathbf{Z}^d$.
5. The set $\limsup_n D_n$ contains at least one point in each equivalence class of $\mathbf{R}^d / \mathbf{Z}^d$.
6. $\lambda(\liminf_n D_n) \leq 1 \leq \lambda(\limsup_n D_n)$.

Proof. 1. Endow \mathbb{R}^d with the usual Euclidean metric. Let $M = \max\{|v| : v \in \mathbb{D}\}$. For every $n \geq 0$, $A^{-n}\mathbb{D} \subset \overline{B}(0, \|A^{-n}\|M)$ and $A^{-n}D_0 \subset \overline{B}(0, \|A^{-n}\|\sqrt{d}/2)$. Since $D_n = A^{-n}D_0 + A^{-n}\mathbb{D} + \dots + A^{-1}\mathbb{D}$, the triangle inequality yields

$$D_n \subset \overline{B}(0, R_n), \text{ where } R_n := \|A^{-n}\|\sqrt{d}/2 + \sum_{k=1}^n \|A^{-k}\|M.$$

Since $\|A^{-n}\|^{1/n} \rightarrow \rho(A^{-1}) < 1$ as $n \rightarrow +\infty$, the quantity $R := \sup_{n \geq 0} R_n$ is finite, and the ball $\overline{B}(0, R)$ contains D_n for every $n \geq 0$.

2. This item follows from Lemma 17.
3. Since $\limsup_n D_n$ is a non-empty bounded invariant subset, its closure is a non-empty compact invariant subset, hence it equals $K_{\mathbb{D}}$.
4. Let x and y be in $\liminf_n D_n$. Assume that x and y belong to the same equivalence class modulo \mathbb{Z}^d . Since x and y belong to D_n for every large enough n and since D_n is a fundamental domain, we derive that $x = y$. Item 4 follows.
5. Let $x \in \mathbb{Z}^d$. The sequence $(p_{D_n}(x))_{n \geq 0}$ varies in the finite set $(x + \mathbb{Z}^d) \cap B_{\mathbb{D}}(0, R)$, hence achieves infinitely many times some value a . This value a belongs to $\limsup_n D_n$ and to $x + \mathbb{Z}^d$. Item 5 follows.
6. Inequality $\lambda(\liminf_n D_n) \leq 1$ follows from Fatou's Lemma applied to the functions $(\mathbf{1}_{D_n})_{n \geq 1}$. Inequality $\lambda(\limsup_n D_n) \geq 1$ follows from Proposition 20.

The proof is complete. □

4.5 A symmetric graph structure on \mathbb{Z}^d

We now fix a finite subset E of \mathbb{Z}^d , containing 0, such that $-E = E$. We associate a symmetric graph structure on \mathbb{Z}^d as follows: given x and y in \mathbb{Z}^d , we say that (x, y) is an edge if and only if $y - x \in E$. Given any subset S of \mathbb{Z}^d , we define the interior, the internal boundary and the external boundary of S by

$$\text{Int}(S) := \{v \in S : \forall e \in E, v + e \in S\},$$

$$\partial_{\text{int}} S := \{v \in S : \exists e \in E, v + e \notin S\},$$

$$\partial_{\text{ext}} S := \{v \in S^c : \exists e \in E, v + e \in S\}.$$

Observe that $\partial_{\text{ext}} S = (S - E) \setminus S = (S + E) \setminus S$.

Recall that for every $\ell \geq 1$, $\mathbb{Z}^d = \mathbb{D}_\ell \oplus A\mathbb{Z}^d$, where $\mathbb{D}_\ell = \mathbb{D} \oplus A\mathbb{D} \oplus \dots \oplus A^{\ell-1}\mathbb{D}$.

We can now state sufficient conditions to have $\lambda(\limsup D_n) = 1$.

Theorem 22. *Assume that there exists $\ell \geq 1$ such that*

1. $D_1 \subset D_0 + E$
2. $E \subset \mathbb{D}_\ell - \mathbb{D}_\ell$
3. $\mathbb{D}_\ell + E \subset \mathbb{D}_\ell + A^\ell E$.

Then $\lambda(\limsup D_n) = 1$. Hence, the map $p_{\mathbb{T}^d}|_E \circ \Phi|_{\Psi(E)}$ provided by propositions 18, 19 and 20 is an isomorphism transforming T_A into the uniform Bernoulli shift on \mathbb{D}^∞ .

Before proving Theorem 22, observe that the assumptions are fulfilled when $A = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}$ and $\mathbb{D} = E = \{(0, 0), (0, 1), (0, -1), (1, 0), (-1, 0)\}$ and $\ell = 1$. We will view a general setup in which conditions 1, 2, 3 hold.

Let us also comment those assumptions. First, the set E must be sufficiently large for D_1 to be covered by $D_0 + E$, but not too large (because of condition 2). Next, if conditions 2 and 3 hold for some integer ℓ , they still hold for any larger integer, because $\mathbb{D}_\ell \subset \mathbb{D}_{\ell+1}$ and $\mathbb{D}_{\ell+1} = \mathbb{D}_\ell + A^\ell \mathbb{D}$. Last, conditions 2 and 3 give the possibility to make some additions with carries.

Indeed, let $n \geq 1$, $x \in \mathbb{D}_{\ell n}$ and $e_0 \in E$. Since $\mathbb{D}_{\ell n} = \mathbb{D}_\ell \oplus A^\ell \mathbb{D}_\ell \oplus \dots \oplus A^{\ell(n-1)} \mathbb{D}_\ell$, the vector x has a unique decomposition

$$x = v_0 + A^\ell v_1 + \dots + (A^\ell)^{n-1} v_{n-1} \text{ with } (v_0, \dots, v_{n-1}) \in \mathbb{D}_\ell^n.$$

By applying repeatedly assumption 3, we get the existence of $v'_0 \in \mathbb{D}_\ell$, $e_1 \in E$, ... , $v'_{n-2} \in \mathbb{D}_\ell$, $e_{n-1} \in E$ such that

$$\begin{aligned} x + e_0 &= (v_0 + e_0) + A^\ell v_1 + \dots + (A^\ell)^{n-1} v_{n-1} \\ &= v'_0 + A^\ell (v_1 + e_1) + \dots + (A^\ell)^{k-1} v_{k-1} \\ &= \dots \\ &= v'_0 + A^\ell v'_1 + \dots + (A^\ell)^{n-2} v'_{n-2} + (A^\ell)^{n-1} (v_{n-1} + e_{n-1}). \end{aligned}$$

By assumption 2, there exist vectors f_0, \dots, f_{n-1} in \mathbb{D}_ℓ such that $f_0 + e_0, \dots, f_{n-1} + e_{n-1}$ are still in D_n . Hence, most of the time, the sum $x + e_0$ belongs to $\mathbb{D}_{\ell n}$. Indeed,

$$x + e_0 \notin \mathbb{D}_{\ell n} \implies (v_0 \neq f_0 \text{ and } \dots \text{ and } v_{n-1} \neq f_{n-1}).$$

The next lemma follows.

Lemma 23. *If the assumptions 2 and 3 hold, then for every $n \geq 1$ and every $e \in E$,*

$$|\mathbb{D}_{\ell n} \setminus (\mathbb{D}_{\ell n} + e)| = |(\mathbb{D}_{\ell n} + e) \setminus \mathbb{D}_{\ell n}| \leq (r^\ell - 1)^n.$$

For every $n \geq 1$,

$$|\partial_{\text{int}} \mathbb{D}_{\ell n}| \leq |E|(r^\ell - 1)^n \text{ and } |\partial_{\text{ext}} \mathbb{D}_{\ell n}| \leq |E|(r^\ell - 1)^n.$$

Proof. The equality and the first inequality follow from the equality $|\mathbb{D}_{\ell n} + e| = |\mathbb{D}_{\ell n}|$ and from the discussion above. The last two inequalities follow by taking an union bound. \square

Lemma 24. *Let S be any subset of \mathbb{Z}^d . If assumption 1 holds, then*

$$\begin{aligned}(S + D_1) \setminus (S + D_0) &\subset \partial_{\text{ext}} S + D_0, \\ \lambda((S + D_1) \setminus (S + D_0)) &\leq |\partial_{\text{ext}} S|, \\ \lambda((S + D_0) \setminus (S + D_1)) &\leq |\partial_{\text{ext}} S|.\end{aligned}$$

Proof. The inclusion stated follows from the inclusions

$$(S + D_1) \setminus (S + D_0) \subset (S + E + D_0) \setminus (S + D_0) \subset ((S + E) \setminus S) + D_0.$$

For every finite subset S of \mathbb{Z}^d , and any fundamental domain D , the sum $S + D$ is direct, so $\lambda(S + D) = |S|\lambda(D) = |S|$. Therefore

$$\lambda((S + D_1) \setminus (S + D_0)) \leq \lambda(\partial_{\text{ext}} S + D_0) = |\partial_{\text{ext}} S|.$$

And since $S + D_0$ and $S + D_1$ have the same and finite Lebesgue measure, the differences $(S + D_1) \setminus (S + D_0)$ and $(S + D_0) \setminus (S + D_1)$ have also the same Lebesgue measure. The proof is complete. \square

Lemma 25. *For every Borel subsets B and C of \mathbb{R}^d ,*

$$\lambda(\tau_{\mathbb{D}}(B) \Delta \tau_{\mathbb{D}}(C)) \leq \lambda(B \Delta C).$$

Proof. It follows from the inclusion

$$\tau_{\mathbb{D}}(B) \Delta \tau_{\mathbb{D}}(C) \subset \bigcup_{v \in \mathbb{D}} (A^{-1}(B \Delta C) + A^{-1}v).$$

by taking an union bound. \square

Proposition 26. *If the assumptions 1, 2, 3 hold with $\ell \geq 1$, then*

$$\lambda(D_{n+1} \Delta D_n) = O((1 - r^{-\ell})^{n/\ell}) \text{ as } n \rightarrow +\infty.$$

Proof. By lemma 25, the sequence $(\lambda(D_{n+1} \Delta D_n))_{n \geq 0}$ is non-increasing. Hence, it is enough to bound above $\lambda(D_{\ell n+1} \Delta D_{\ell n})$ for $n \geq 0$.

We observe that for every $n \geq 0$,

$$A^{\ell n} D_{\ell n} = D_0 + \mathbb{D} + \dots + A^{\ell n-1} \mathbb{D} = D_0 + \mathbb{D}_{\ell n}$$

and

$$A^{\ell n} D_{\ell n+1} = A^{-1} D_0 + A^{-1} \mathbb{D} + \mathbb{D} + \dots + A^{\ell n-1} \mathbb{D} = D_1 + \mathbb{D}_{\ell n}.$$

Hence, by Lemmas 24 and 23,

$$\lambda(A^{\ell n} D_{\ell n+1} \setminus A^{\ell n} D_{\ell n}) \leq |\partial_{\text{ext}} \mathbb{D}_{\ell n}| \leq |E|(r^\ell - 1)^n.$$

Since $|\det A^{\ell n}| = r^{\ell n}$, we derive

$$\lambda(D_{\ell n+1} \Delta D_{\ell n}) = 2\lambda(D_{\ell n+1} \setminus D_{\ell n}) \leq 2|E|(1 - r^{-\ell})^n.$$

We are done. \square

Theorem 22 directly follows. Indeed, the last proposition ensures that the series $\sum_n \|\mathbf{1}_{D_{n+1}} - \mathbf{1}_{D_n}\|_1 = \sum_n \lambda(D_{n+1} \Delta D_n)$ converges, so the series $\sum_n (\mathbf{1}_{D_{n+1}} - \mathbf{1}_{D_n})$ converges almost everywhere and in $L^1(\lambda)$. As a result, the sequence $(\mathbf{1}_{D_n})_{n \geq 0}$ converges almost everywhere and in $L^1(\lambda)$. In particular, $\lambda(\limsup D_n) = \lim \lambda(D_n) = 1$.

We viewed in the introduction that if D is any fundamental domain, then $AD \cap \mathbb{Z}^d$ is a system of representatives of $\mathbb{Z}^d / A\mathbb{Z}^d$. Hence Theorem 3 follows from Theorem 22 and the theorem below.

Theorem 27. *Assume that $\|A^{-1}\|_{\mathbf{u}, \infty} < 1$ for some \mathbb{Z} -basis $\mathbf{u} = (u_1, \dots, u_d)$ of \mathbb{Z}^d . Let*

$$c := (1/2)A^{-1}(u_1 + \dots + u_d), \quad D_0 := c + \sum_{i=1}^d [-1/2, 1/2]u_i,$$

$$\mathbb{D} := AD_0 \cap \mathbb{Z}^d, \quad E := \sum_{i=1}^d \{-1, 0, 1\}u_i.$$

Then conditions of Theorem 22 apply with $\ell = 1$.

Proof. By an unimodular change of coordinates, we may and we do assume that \mathbf{u} is the canonical basis. Thus we omit the index \mathbf{u} in the norms.

First, we observe that

$$|c|_\infty \leq (1/2)\|A^{-1}\|_\infty \times |(1, \dots, 1)|_\infty < 1/2.$$

By the triangle inequality, $D_0 \subset]-1, 1[^d$, so $D_0 \subset]-1, 1[^d$ since $\|A^{-1}\|_{\mathbf{u}, \infty} < 1$. Moreover, Since $\mathbb{D} \subset AD_0$,

$$\begin{aligned} D_1 &= A^{-1}\mathbb{D} + A^{-1}D_0 \\ &\subset D_0 + A^{-1}D_0 \\ &\subset c + [-1/2, 1/2[^d +]-1, 1[^d \\ &\subset c + [-3/2, 3/2]^d. \end{aligned}$$

whereas

$$D_0 + E = c + [-1/2, 1/2]^d + \{-1, 0, 1\}^d = c + [-3/2, 3/2]^d.$$

Thus, condition 1 holds.

Next, by the definition of c and since $\|A^{-1}\|_\infty < 1$, we have

$$A^{-1}[0, 1]^d = c + A^{-1}[-1/2, 1/2]^d \subset c + [-1/2, 1/2]^d = D_0.$$

Thus, $[0, 1]^d \subset AD_0$ so $\mathbb{D} := AD_0 \cap \mathbb{Z}^d$ contains $\{0, 1\}^d$ and $\mathbb{D} - \mathbb{D}$ contains $E := \{-1, 0, 1\}^d$. Thus, condition 2 holds.

Last, since $\|A^{-1}\|_\infty < 1$, we have $A^{-1}E \subset [-1, 1]^d$, so

$$D_0 + A^{-1}E \subset c + [-1/2, 1/2]^d + [-1, 1]^d = c + [-3/2, 3/2]^d = D_0 + E.$$

Thus

$$\mathbb{D} + E \subset AD_0 + E \subset AD_0 + AE.$$

Since $\mathbb{D} + E$ and AE contain only integer points, we derive

$$\mathbb{D} + E \subset \mathbb{Z}^d \cap (AD_0 + AE) = (\mathbb{Z}^d \cap AD_0) + AE = \mathbb{D} + AE.$$

Thus, condition 3 holds. □

4.6 Proof of Theorem 1

We define a map $\phi : \mathbb{Z}^d \rightarrow \mathbb{Z}^d$ as follows: for every $x \in \mathbb{Z}^d$, call $v(x)$ the only element of \mathbb{D} such that $x - v(x) \in A\mathbb{Z}^d$, and set $\phi(x) = A^{-1}(x - v_x)$. The vectors $\phi(x)$ and $v(x)$ can be viewed as the quotient and the remainder in the Euclidean division of x by A . Note that $x \in \mathbb{D}_\infty$ if and only $\phi(x) \in \mathbb{D}_\infty$ and that for every $n \geq 1$, $\phi(\mathbb{D}_n) = \mathbb{D}_{n-1}$ with the convention $\mathbb{D}_0 = \{0\}$.

Moreover, for every $x \in \mathbb{Z}^d$, $|\phi(x)| \leq |A^{-1}x| + |A^{-1}v_x| \leq \|A^{-1}\| |x| + M$. Since $0 < \|A^{-1}\| < 1$, we can set $R_0 := M/(1 - \|A^{-1}\|)$ and we get

$$\begin{aligned} |\phi(x)| &< |x| \text{ whenever } |x| > R_0, \\ |\phi(x)| &\leq R_0 \text{ whenever } |x| \leq R_0. \end{aligned}$$

Since every ball of \mathbb{R}^d contains only finitely many vectors of \mathbb{Z}^d , the sequence $(\phi^n(x))_{n \geq 0}$ eventually reaches the absorbing finite set $\{y \in \mathbb{Z}^d : |y| \leq R_0\}$ and is eventually periodic. The equivalence (1) \iff (2) follows.

Given $x \in \mathbb{Z}^d$, let $q \geq 0$ be the least integer such that the value $\phi^q(x)$ is reached twice and $p \geq 1$ the least integer $p \geq 1$ such that $\phi^{q+p}(x) = \phi^q(x)$. Since

$$\begin{aligned} \phi^q(x) &= v(\phi^q(x)) + A\phi^{q+1}(x) \\ &= \dots \\ &= v(\phi^q(x)) + \dots + A^{p-1}v(\phi^{q+p-1}(x)) + A^p\phi^{q+p}(x), \end{aligned}$$

we derive $(I - A^q)\phi^q(x) = v(\phi^q(x)) + \dots + A^{p-1}v(\phi^{q+p-1}(x))$. If statement 3 holds, this vector is null, so $\phi^q(x)$ is null (because the matrix $I - A^q$ is invertible) and $x \in \mathbb{D}_\infty$. This shows the implication (3) \implies (2).

Conversely, if $\mathbb{D}_\infty = \mathbb{Z}^d$, then for every $x \in \mathbb{Z}^d$, the sequence $(\phi^n(x))_{n \geq 0}$ is eventually null. Therefore, for each $n \geq 1$, the only fixed point of ϕ^n is 0. If y is an element of $\mathbb{D}_n \cap (I - A^n)\mathbb{Z}^d$, then $y = v_0 + \dots + A^{n-1}v_{n-1}$ with $(v_0, \dots, v_{n-1}) \in \mathbb{D}^n$ and $y = x - A^n x$ for some $x \in \mathbb{Z}^d$. The equality $x = v_0 + \dots + A^{n-1}v_{n-1} + A^n x$ yields $\phi^n(x) = x$, so $x = 0$, so $y = 0$. This shows the implication (2) \implies (3).

Last, assume that $\mathbb{D}_\infty = \mathbb{Z}^d$ and fix a cube $[-R, R]^d$ containing the compact set $K_{\mathbb{D}}$. For every integer $N \geq 1$,

$$\bigcup_{z \in [-N, N]^d} (K_{\mathbb{D}} + z) \subset [-N - R, N + R]^d \quad (2)$$

and the finite set $[-N, N]^d$ is contained in \mathbb{D}_n for every large enough n . Since $AK_{\mathbb{D}}$ is the almost disjoint union of the sets $K_{\mathbb{D}} + v$ over all $v \in \mathbb{D}$, a recursion shows that for every $n \geq 1$, $A^n K_{\mathbb{D}}$ is the almost disjoint union of the sets $K_{\mathbb{D}} + z$ over all $z \in \mathbb{D}_n$. Thus the union in equation (2) is almost disjoint. Taking Lebesgue measures yields $(2N + 1)^d \lambda(K_{\mathbb{D}}) \leq (2N + 2R)^d$. Dividing by $(2N)^d$ and letting N go to infinity yields $\lambda(K_{\mathbb{D}}) \leq 1$, so $\lambda(K_{\mathbb{D}}) = 1$. The proof is complete.

4.7 Using Lagarias and Wang's theorem

Call $\mathbb{Z}[A, \mathbb{D}]$ the smallest sublattice which contains $\mathbb{D} - \mathbb{D}$ and is stable under A . By Cayley - Hamilton theorem, A^d is a linear combination of I, A, \dots, A^{d-1} with integer coefficients. Thus $\mathbb{Z}[A, \mathbb{D}]$ is also the sublattice of \mathbb{Z}^d generated by $\mathbb{D} \cup A\mathbb{D} \dots \cup A^{d-1}\mathbb{D}$ since we assumed that $0 \in \mathbb{D}$.

Lemma 28. *The set $\mathbb{Z}[A, \mathbb{D}]$ is a lattice of \mathbb{R}^d , i.e. its rank is d .*

Proof. We argue by contradiction. Call d_1 the rank of $\mathbb{Z}[A, \mathbb{D}]$, assume that $d_1 < d$, and set $d_2 = d - d_1$. By the theory of lattices, there exist a \mathbb{Z} -basis (u_1, \dots, u_d) of \mathbb{Z}^d and positive integers $\alpha_1, \dots, \alpha_{d_1}$ such that $(\alpha_1 u_1, \dots, \alpha_{d_1} u_{d_1})$ is a \mathbb{Z} -basis of $\mathbb{Z}[A, \mathbb{D}]$. Call $U \in GL_d(\mathbb{Z})$ the matrix whose columns are u_1, \dots, u_d . Then $B := U^{-1}AU$ is the matrix of the endomorphism $x \mapsto Ax$ in the basis (u_1, \dots, u_d) . Since $\mathbb{Z}[A, \mathbb{D}]$ is the linear space spanned by (u_1, \dots, u_{d_1}) and is stable by the endomorphism $x \mapsto Ax$, one has

$$B = \begin{pmatrix} B_1 & C \\ 0 & B_2 \end{pmatrix},$$

with $B_1 \in \mathcal{M}_{d_1}(\mathbb{Z})$, $B_2 \in \mathcal{M}_{d_2}(\mathbb{Z})$, $C \in \mathcal{M}_{d_2, d_1}(\mathbb{Z})$. Denoting by χ the characteristic polynomial, we get $\chi_A = \chi_B = \chi_{B_1} \chi_{B_2}$, so the matrices B_1 and B_2 are expanding. In particular, the lattice $B_2 \mathbb{Z}^{d_2}$ is strictly contained in \mathbb{Z}^{d_2} . Furthermore, on the one hand,

$$U^{-1}A\mathbb{Z}^d = BU^{-1}\mathbb{Z}^d = B\mathbb{Z}^d \subset \mathbb{Z}^{d_1} \times B_2\mathbb{Z}^{d_2}.$$

On the other hand, $\mathbb{D} \subset \mathbb{Z}[A, \mathbb{D}] \subset \mathbb{Z}u_1 \oplus \dots \oplus \mathbb{Z}u_{d_1} = U(\mathbb{Z}^{d_1} \times \{0_{d_2}\})$, so

$$U^{-1}\mathbb{D} \subset \mathbb{Z}^{d_1} \times \{0_{d_2}\}.$$

By addition

$$\mathbb{Z}^d = U^{-1}\mathbb{Z}^d = U^{-1}(\mathbb{D} \oplus A\mathbb{Z}^d) \subset \mathbb{Z}^{d_1} \times B_2\mathbb{Z}^{d_2},$$

which yields a contradiction. \square

Definition 29. *One says that (A, \mathbb{D}) is primitive when $\mathbb{Z}[A, \mathbb{D}] = \mathbb{Z}^d$.*

Remark 30. *When $r = 2$, the set \mathbb{D} has exactly two elements, 0 and v , say. Then (A, \mathbb{D}) is primitive if and only if $(v, Av, \dots, A^{d-1}v)$ is a \mathbb{Z} -base of \mathbb{Z}^d .*

The next result enlightens the interest of the notion of primitivity.

Proposition 31. (Lagarias - Wang) *A necessary condition to have $\lambda(K_d) = 1$ is that (A, \mathbb{D}) is primitive.*

Here is a proof of this fact which is more elementary than Lagarias and Wang's one.

Proof. By lemma 28 and by the theory of lattices, there exist a \mathbb{Z} -basis (u_1, \dots, u_d) of \mathbb{Z}^d and positive integers $\alpha_1, \dots, \alpha_d$ such that $(\alpha_1 u_1, \dots, \alpha_d u_d)$ is a \mathbb{Z} -basis of $\mathbb{Z}[A, \mathbb{D}]$. Call $Q \in \mathcal{M}_d(\mathbb{Z})$ the matrix whose columns are $\alpha_1 u_1, \dots, \alpha_d u_d$. Then $\det Q = \pm \alpha_1 \dots \alpha_d \neq 0$ and $\mathbb{D} \subset \mathbb{Z}[A, \mathbb{D}] = Q\mathbb{Z}^d$, so $\mathbb{D} = Q\mathbb{D}'$ for some $\mathbb{D}' \subset \mathbb{Z}^d$. Since $AQ\mathbb{Z}^d = A\mathbb{Z}[A, \mathbb{D}] \subset Q\mathbb{Z}^d$, there exists some matrix $A' \in \mathcal{M}_d(\mathbb{Z})$ such that $AQ = QA'$. The matrix $A' = Q^{-1}AQ$ has the same characteristic polynomial as A , hence it is expansive. Moreover,

$$\mathbb{R}^d = Q^{-1}\mathbb{R}^d = Q^{-1}(\mathbb{D} \oplus A\mathbb{Z}^d) = Q^{-1}\mathbb{D} \oplus Q^{-1}A\mathbb{Z}^d = \mathbb{D}' \oplus A'\mathbb{Z}^d,$$

since $\mathbb{Z}^d = Q\mathbb{Z}^d$. Thus \mathbb{D}' is a system of representatives of $\mathbb{Z}^d/A'\mathbb{Z}^d$. By proposition 20, the Lebesgue measure of the self-affine tile

$$K'_{\mathbb{D}'} := \left\{ \sum_{k \geq 1} (A')^{-k} v'_k : (v'_k)_{k \geq 1} \in \mathbb{D}'^{\infty} \right\}$$

is a positive integer. The equalities $\mathbb{D} = Q\mathbb{D}'$ and $A^{-k}Q = Q(A')^{-k}$ yield $K_{\mathbb{D}} = QK'_{\mathbb{D}'}$, so $\lambda(K_{\mathbb{D}}) = |\det(Q)|\lambda'(K'_{\mathbb{D}'})$ is a multiple of $|\det(Q)|$.

Hence, if $\lambda(K_{\mathbb{D}}) = 1$, then $|\det(Q)| = 1$, so $\mathbb{Z}[A, \mathbb{D}] = \mathbb{Z}^d$. \square

Proposition 31 enables us to show that choosing $\mathbb{D} := AP \cap \mathbb{Z}^d$ where P is a fundamental parallelopete (containing 0) does not guarantee that $\lambda(K_d)$ equals 1.

Example 32. Let $A := \begin{pmatrix} 2 & -1 \\ 4 & -1 \end{pmatrix}$, $P := [0, 1]^2$ and $\mathbb{D} := AP \cap \mathbb{Z}^d$. Then $\chi_A = X^2 - X + 2$, the matrix A is expanding, and $AP \cap \mathbb{Z}^d = \{0, v\}$ where $v = (1 \ 2)^\top$. Since $Av = (0 \ 2)^\top$, one has $\mathbb{Z}[A, \mathbb{D}] \subset \mathbb{Z} \times 2\mathbb{Z}$. Hence (A, \mathbb{D}) is not primitive, so $\lambda(K_d) > 1$.

Actually, assuming that (A, \mathbb{D}) is primitive does not guarantee that $\lambda(K_d) = 1$. Some other obstructions may occur, although they are quite rare.

Lagarias and Wang give a necessary and sufficient condition to have $\lambda(K_d) > 1$ when (A, \mathbb{D}) is primitive. This condition provides the existence of a unimodular matrix P such that PAP^{-1} is block-trigonalisable while $P\mathbb{D}$ (which is a complete residue system modulo $PAP^{-1}\mathbb{Z}^d$) has a ‘skew-product structure’. Hence the condition is rarely satisfied, although in some situations, it may be difficult to disprove it.

Theorem 33. (Theorem 6.1 of [9]). Assume that (A, \mathbb{D}) is primitive.

Then $\lambda(K_d) > 1$ if and only if there exist

- an unimodular matrix $P \in GL_d(\mathbb{Z})$,
- two positive integers d_1, d_2 with sum d ,
- four matrices $B_1 \in \mathcal{M}_{d_1}(\mathbb{Z})$, $B_2 \in \mathcal{M}_{d_2}(\mathbb{Z})$, $C \in \mathcal{M}_{d_1, d_2}(\mathbb{Z})$, $Q \in \mathcal{M}_{d_2}(\mathbb{Z})$,
- three families $(a_i)_{1 \leq i \leq r_1} \subset \mathbb{R}^{d_1}$, $(b_i)_{1 \leq i \leq r_1} \subset \mathbb{R}^{d_2}$ and $(c_{i,j})_{1 \leq i \leq r_1, 1 \leq j \leq r_2} \subset \mathbb{R}^{d_2}$, where $r_1 := |\det(B_1)|$ and $r_2 := |\det(B_2)|$.

such that

1. $PAP^{-1} = \begin{pmatrix} B_1 & 0 \\ C & B_2 \end{pmatrix}$,
2. $|\det Q| \geq 2$ and $Q^{-1}B_2Q \in \mathcal{M}_{d_2}(\mathbb{Z})$,
3. $P\mathbb{D} = \left\{ \begin{pmatrix} a_i \\ b_i + Qc_{i,j} \end{pmatrix} : 1 \leq i \leq r_1, 1 \leq j \leq r_2 \right\}$,
4. The family $(a_i)_{1 \leq i \leq r_1}$ is a complete residue system modulo $B_1\mathbb{Z}^{d_1}$.
5. For each $i \in \llbracket 1, |\det(B_1)| \rrbracket$, the family $(Qc_{i,j})_{1 \leq j \leq r_2}$ is a complete residue system modulo $B_2\mathbb{Z}^{d_2}$.

In this statement, proving the ‘if’ part is rather simple and uses the same kind of arguments as Proposition 31, together with Fubini’s theorem. Actually, the case where (A, \mathbb{D}) is not primitive could be viewed as the case where $d_1 = 0$ in the conditions above. Yet, the ‘only if’ part is highly non-trivial, and relies on the existence of some lattice $\Lambda \subset \mathbb{Z}^d$ which is a tiling set for $K_{\mathbb{D}}$, i.e. such that \mathbb{R}^d is the almost disjoint union of the translated tiles $(K_{\mathbb{D}} + s)_{s \in S}$.

Note that condition 1 above implies $\chi_A = \chi_{B_1}\chi_{B_2}$ and $r = r_1r_2$. Thus, the matrices B_1 and B_2 must also be expansive, and the integers $r_1 = |\det(B_1)|$, $r_2 = |\det(B_2)|$ must be larger than or equal to 2. Such a situation cannot occur when r is a prime number, or when the characteristic polynomial χ_A is irreducible in $\mathbb{Z}[X]$.

When $r_1 \geq 2$ and $r_2 \geq 2$, conditions 3, 4, 5 prevent the set \mathbb{D} from being contained in some line. This remark provides a notable consequence.

Corollary 34. *Assume that for some vector $v_1 \in \mathbb{Z}^d$, the family $(v_1, Av_1, \dots, A^{d-1}v_1)$ is a \mathbb{Z} -basis of \mathbb{Z}^d . Then $\mathbb{D} := \{0, v_1, \dots, (r-1)v_1\}$ is a system of representatives of $\mathbb{Z}^d/A\mathbb{Z}^d$. Furthermore, for this choice of \mathbb{D} , one has $\lambda(K_{\mathbb{D}}) = 1$.*

Proof. By assumption, $(v_1, Av_1, \dots, A^{d-1}v_1)$ is a \mathbb{Z} -basis of \mathbb{Z}^d , so $(Av_1, A^2v_1, \dots, A^d v_1)$ is a \mathbb{Z} -basis of $A\mathbb{Z}^d$. Let $X^d - (\alpha_0 + \alpha_1 X + \dots + \alpha_{d-1} X^{d-1})$ be the characteristic polynomial of A . Then $\alpha_0 = (-1)^{d-1} \det A = \pm r$, and $A^d v_1 = \alpha_0 v_1 + \alpha_1 Av_1 + \dots + \alpha_{d-1} A^{d-1} v_1$. As a result, $(Av_1, \dots, A^{d-1} v_1, r v_1)$ is a \mathbb{Z} -basis of $A\mathbb{Z}^d$ and $\mathbb{D} := \{0, v_1, \dots, (r-1)v_1\}$ is a system of representatives of $\mathbb{Z}^d/A\mathbb{Z}^d$.

The subgroup $\mathbb{Z}[A, \mathbb{D}]$ contains $\mathbb{Z}v_1 + \mathbb{Z}Av_1 + \dots + \mathbb{Z}A^{d-1}v_1 = \mathbb{Z}^d$. Hence (A, \mathbb{D}) is primitive. Moreover, for every $P \in GL_d(\mathbb{Z})$, the subset $P\mathbb{D}$ is contained in $\mathbb{Z}Pv_1$, so the conditions of Theorem 33 cannot be fulfilled. Thus $\lambda(K_{\mathbb{D}}) = 1$. \square

Corollary 35. *If A is similar in $\mathcal{M}_d(\mathbb{Z})$ to some block-diagonal matrix in which all diagonal blocks are companion matrices, then one can find a system \mathbb{D} of representatives of $\mathbb{Z}^d/A\mathbb{Z}^d$ such that $\lambda(K_{\mathbb{D}}) = 1$.*

Proof. By an unimodular change of coordinates, we may - and we do - assume that $A = \text{Diag}(C_1, \dots, C_n)$ where C_1, \dots, C_n are companion matrices. Call d_1, \dots, d_n the sizes of C_1, \dots, C_n and r_1, \dots, r_n the absolute value of their determinants.

For each $k \in [1, n]$, the set $\mathbb{D}_k := [0, r_k - 1](1, 0, \dots, 0)$ is a system of representatives of $\mathbb{Z}^{d_k}/C_k\mathbb{Z}^{d_k}$. The Cartesian product $\mathbb{D} := \mathbb{D}_1 \times \dots \times \mathbb{D}_n$ is a system of representatives of $\mathbb{Z}^d/A\mathbb{Z}^d$ and $K_{\mathbb{D}}$ is the Cartesian product of the compact sets $K_{C_1, \mathbb{D}_1}, \dots, K_{C_n, \mathbb{D}_n}$ associated to $(C_1, \mathbb{D}_1), \dots, (C_n, \mathbb{D}_n)$. Hence $\lambda(K_{\mathbb{D}}) = \lambda(K_{C_1, \mathbb{D}_1}) \cdots \lambda(K_{C_n, \mathbb{D}_n}) = 1$. \square

Unfortunately, Corollary 35 does not cover all cases, since Frobenius reduction applies only to square matrices with entries in a field. Actually, the classification of all matrices of $\mathcal{M}_d(\mathbb{Z})$ up to \mathbb{Z} -similarity is a difficult and still open problem: no complete system of invariants is known. We now state an important result in this topic. Given any integral domain D , we define an equivalence relation on all non-zero ideals by

$$I \sim J \iff \exists a, b \in D \setminus \{0\}, \quad aI = bJ.$$

The equivalence classes for this relation are called *ideal classes*. For example, the ideal class of the ideal D is precisely the collection of all principal ideals.

Theorem 36. (Latimer - MacDuffee theorem) *Let $f \in \mathbb{Z}[X]$ be a monic irreducible polynomial with integer coefficients and degree d . Then, among the matrices of $\mathcal{M}_d(\mathbb{Z})$ whose characteristic polynomial is f , the number of \mathbb{Z} -similarity classes equals the number of ideal classes in the integral domain $\mathbb{Z}[X]/f\mathbb{Z}[X]$.*

Taussky's paper [13] provides a simple proof via an explicit correspondence between the similarity classes and the ideal classes. We will only use the following corollary.

Corollary 37. *Let $f \in \mathbb{Z}[X]$ be a monic irreducible polynomial with integer coefficients and degree d . Then, the two statements below are equivalent:*

1. All matrices of $\mathcal{M}_d(\mathbb{Z})$ whose characteristic polynomial is f are \mathbb{Z} -similar.

2. The integral domain $\mathbb{Z}[X]/f\mathbb{Z}[X]$ is principal.

To keep the paper self-contained, we give a proof of Corollary 37.

Proof. Fix a complex root α of f . Then α is a simple root of f . Indeed, f is irreducible in $\mathbb{Z}[X]$ and also in $\mathbb{Q}[X]$. Hence the greatest common divisor of f and f' in $\mathbb{Q}[X]$, and also in $\mathbb{C}[X]$ (by Bezout's identity) equals 1. Hence $(X - \alpha)^2$ cannot divide f .

The evaluation map $g \mapsto g(\alpha)$ from $\mathbb{Z}[X]$ to \mathbb{C} is a morphism of integral domains with range $\mathbb{Z}[\alpha]$ and with kernel $f\mathbb{Z}[X]$. Thus the integral domain $\mathbb{Z}[X]/f\mathbb{Z}[X]$ is isomorphic to $\mathbb{Z}[\alpha]$. Moreover, since f is irreducible, it is the minimal polynomial of α . Therefore, $(1, \alpha, \dots, \alpha^{d-1})$ is a \mathbb{Z} -basis of $\mathbb{Z}[\alpha]$.

Assume that condition 1 holds. Let I be a non-zero ideal of $\mathbb{Z}[\alpha]$. Then I is a subgroup of $\mathbb{Z}[\alpha]$, with same rank as $\mathbb{Z}[\alpha]$. Indeed, given a non-zero element $x \in I$, the elements $x, \alpha x, \dots, \alpha^{d-1}x$ are \mathbb{Z} -linearly independent, since for every $g \in \mathbb{Z}[X]$,

$$g(\alpha)x = 0 \iff g(\alpha) = 0 \iff f|g. \quad (3)$$

Thanks to equation (3), the minimal polynomial, and also the characteristic polynomial of the endomorphism $x \mapsto \alpha x$ on I is f . By condition 1, the matrix of this endomorphism in some \mathbb{Z} -basis (v_1, \dots, v_d) is a companion matrix. Hence $v_2 = \alpha v_1, \dots, v_d = \alpha v_{d-1}$, so

$$\mathbb{Z}[\alpha]v_1 \subset I = \mathbb{Z}v_1 \oplus \dots \oplus \mathbb{Z}v_d \subset \mathbb{Z}[\alpha]v_1,$$

i.e. $I = \mathbb{Z}[\alpha]v_1$ is principal.

Conversely, assume that condition 2 holds. Let $A \in \mathcal{M}_d(\mathbb{Z})$ be any matrix whose minimal polynomial is f . Since α is a simple root of f , the matrix $A - \alpha I$ has rank $d - 1$ and its adjugate matrix M has at least one non-zero entry $M(i_0, j_0)$, say. Since $M(A - \alpha I) = \chi_A(\alpha)I_d = 0$, the row $w := M(i_0, \cdot)$ is a row eigenvector of A associated to α , whose coordinates belong to $\mathbb{Z}[\alpha]$.

Let $I = w_1\mathbb{Z} + \dots + w_d\mathbb{Z}$. Since the entries of A belong to \mathbb{Z} and since for all $j \in \llbracket 1, d \rrbracket$,

$$\alpha w_j = (wA)_j = \sum_{i=1}^d w_i A(i, j), \quad (4)$$

one has $\alpha I \subset I$. Thus I is an ideal of $\mathbb{Z}[\alpha]$. By condition 2, one can find $u \in I$ such that $I = u\mathbb{Z}[\alpha]$. Then $(u, \alpha u, \dots, \alpha^{d-1}u)$ is a \mathbb{Z} -basis of I . In this basis, the matrix of the endomorphism $x \mapsto \alpha x$ on I is a companion matrix. But (w_1, \dots, w_d) is also a \mathbb{Z} -basis of I and in this basis, the matrix on this endomorphism is A , thanks to equation (4). As a result, A is \mathbb{Z} -similar to a companion matrix.

The proof is complete. □

4.8 The low-dimensional case

Let us introduce a notion of convexity in \mathbb{Z}^d , which will be useful for us when $d = 2$.

Definition 38. Let S be a subset S of \mathbb{Z}^d . One says that S is convex in \mathbb{Z}^d if the intersection of \mathbb{Z}^d with the convex hull of S in \mathbb{R}^d is contained in S . Equivalently, S is convex in \mathbb{Z}^d if and only if S is the intersection of \mathbb{Z}^d with some convex subset of \mathbb{R}^d .

When $d = 2$, the conditions 1–5 of Theorem Lagarias and Wang condition imply $d_1 = d_2 = 1$, so $B_1 = r_1$, $B_2 = r_2$ and Q must be an integer relatively prime with r_2 , such that $|Q| \geq 2$. Moreover, the first components of $P\mathbb{D}$ can take r_1 different values and, when the first component a_i is known, the second can take r_2 different values, all of them belonging to the same coset $b_i + Q\mathbb{Z}$. Since $r_2 \geq 2$, this prevents $P\mathbb{D}$ and \mathbb{D} from being convex in \mathbb{Z}^d . We derive the following corollary.

Corollary 39. *Assume that $d = 2$. If \mathbb{D} is convex in \mathbb{Z}^2 (in particular if $\mathbb{D} := AD \cap \mathbb{Z}^2$ where D be a fundamental parallelogram containing 0), and if (A, \mathbb{D}) is primitive, then $\lambda(K_{\mathbb{D}}) = 1$.*

Remark 40. *The argument above does not work anymore when $d \geq 3$. Indeed, Lagarias and Wang conditions may hold with $d_2 = 2$, $B_2 = \begin{pmatrix} 0 & 2 \\ 1 & 3 \end{pmatrix}$ and $Q = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, since $Q^{-1}B_2Q$ has integer coefficients. Then $\{0, e_1 + e_2\}$ is contained in $Q\mathbb{Z}^2$ and is a system of representatives of $\mathbb{Z}^2/B_2\mathbb{Z}^2$. Yet, it is convex in \mathbb{Z}^2 .*

We are now able to prove Theorem 2.

Proof. Assume that $d = 2$. We have to show that it is always possible to choose the system \mathbb{D} of representatives so that $\lambda(K_{\mathbb{D}}) = 1$. We distinguish two cases. Both of them split into subcases.

Case where $r \geq 3$. Since $A\mathbb{Z}^2$ is a lattice contained in \mathbb{Z}^2 , one can find a \mathbb{Z} -basis (u_1, u_2) of \mathbb{Z}^2 and two positive integers α_1, α_2 such that $(\alpha_1 u_1, \alpha_2 u_2)$ is a \mathbb{Z} -basis of $A\mathbb{Z}^2$. One has $\alpha_1 \alpha_2 = r$. Moreover, the set $\mathbb{D} := \llbracket 0, \alpha_1 - 1 \rrbracket u_1 \oplus \llbracket 0, \alpha_2 - 1 \rrbracket u_2$ is a system of residues modulo $A\mathbb{Z}^2$ and is convex in \mathbb{Z}^2 .

If $\alpha_1 \geq 2$ and $\alpha_2 \geq 2$, then (A, \mathbb{D}) is primitive since $\mathbb{D} - \mathbb{D}$ contains u_1 and u_2 .

Otherwise, by symmetry, one may assume that $\alpha_2 = 1$ and $\alpha_1 = r \geq 3$, so $u_2 \in A\mathbb{Z}^2$. Then $\mathbb{D}' := \llbracket 0, \alpha_1 - 2 \rrbracket u_1 \cup \{(\alpha_1 - 1)u_1 + u_2\}$ is also a system of residues modulo $A\mathbb{Z}^2$, and is also convex in \mathbb{Z}^2 . Moreover (A, \mathbb{D}) is primitive since $\mathbb{D} - \mathbb{D}$ contains u_1 and $u_1 + u_2$ (here we use the assumption $r \geq 3$).

Hence Corollary 39 applies in both subcases.

Case where $r = 2$. Call t the trace of A . Then $\chi_A = X^2 - tX + \det A$.

If $\det A = -2$, the eigenvalues of A are $(-t \pm \sqrt{t^2 + 8})/2$. Since A is expanding, one has $\sqrt{t^2 + 8} > |t| + 2$. Squaring both sides and simplifying yields $|t| < 1$, namely $t = 0$.

If $\det A = 2$, the discriminant of χ_A is $t^2 - 8$. If we had $|t| \geq 3$, we would have $|t| - 2 \leq \sqrt{t^2 - 8} \leq |t|$, which would contradict the assumption that A is expansive. Thus $|t| \leq 2$, the discriminant of χ_A is negative, and both eigenvalues have modulus $\sqrt{2}$.

As a result, χ_A is one of the polynomials $X^2 - 2$, $X^2 + 2$, $X^2 \pm X + 2$, $X^2 \pm 2X + 2$. One checks that the integral domain $\mathbb{Z}[X]/\chi_A\mathbb{Z}[X]$ is Euclidean hence principal. By Corollary 37, χ_A is similar to a companion matrix. Equivalently, one can find a vector $v_1 \in \mathbb{Z}^2$ such that (v_1, Av_1) is a \mathbb{Z} -basis of \mathbb{Z}^2 . Thus Corollary 34 applies.

The proof is complete. □

Remark 41. *The coefficients of the polynomial $X^d \chi_A(1/X)$ are those of χ_A written in the reverse order, and its roots (i.e. the eigenvalues of A^{-1}) belong to the open unit disk. Thus the relations between the coefficients and the roots show that the coefficients of χ_A have only finitely many possible values when d and $|\det A| = r$ are fixed.*

For example, when $d = 3$ and $r = 2$, the possible characteristic polynomials are $X^3 - X^2 - X + 2$, $X^3 - 2X + 2$, $X^3 - X + 2$, $X^3 + 2$, $X^3 + X^2 + 2$, $X^3 + X^2 + X + 2$, $X^3 + 2X^2 + 2X + 2$, and the polynomial deduced from them by the transformation $P \mapsto -P(-X)$. One can check that the integer domain $\mathbb{Z}[X]/\chi_A\mathbb{Z}[X]$ is principal, and the same proof as in the two-dimensional case shows that it is possible to choose the system \mathbb{D} of representative such that $\lambda(K_{\mathbb{D}}) = 1$.

Unfortunately, it is not always possible to choose a system of representatives such that $\lambda(K_{\mathbb{D}}) = 1$. Here is a counterexample.

Example 42. *If z is a complex number such that $|z| \leq 1$, then $|z^4 + z^2| \leq |z|^4 + |z|^2 \leq 2$, and equality can hold only when $z^4 = z^2$ and $|z| = 1$, namely when $z = \pm 1$. Thus the polynomial $f := X^4 + X^2 + 2$ has no root in the closed unit disk. One checks that the integer domain $\mathbb{Z}[X]/f\mathbb{Z}[X]$ is not principal. By corollary 37, there exists some matrix $A \in \mathcal{M}_d(\mathbb{Z})$ with characteristic polynomial f which is not \mathbb{Z} -similar to a companion matrix. By Remark 30 and Proposition 31, we derive that $\lambda(K_{\mathbb{D}}) > 1$ for every system \mathbb{D} of representatives of $\mathbb{Z}^4/A\mathbb{Z}^4$. An example of such a matrix is*

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

Indeed, for every vector $v = (x \ y \ z \ t)^\top \in \mathbb{Z}^4$, the determinant

$$\det(v, Av, A^2v, A^3v) = \begin{vmatrix} x & -t & -2z + t & -2y + t \\ y & x & -t & 2z + t \\ z & y + z - t & x + y - z & x - y - z \\ t & 2z - t & 2y - t & 2x - 2z - t \end{vmatrix}$$

is always even, since the last two columns have the same parity. Hence (v, Av, A^2v, A^3v) cannot be a \mathbb{Z} -basis of \mathbb{Z}^4 .

Remark 43. *Similar arguments provide a counterexample whenever $d = 4n$ for some integer $n \geq 1$. The polynomial $f_n := X^{4n} + X^{2n} + 2 = f \circ X^n$ has no root in the closed unit disk and is irreducible in $\mathbb{Z}[X]$. Indeed, if $f_n = PQ$ with P and Q in $\mathbb{Z}[X]$, then up to a switch and a multiplication by -1 , the polynomials P and Q are monic, with constant terms ± 1 and ± 2 . The product of the roots of P have modulus 1, so it is an empty product since the modulus of every root of P is larger than 1. Hence P must be constant (equal to 1).*

Let α be a root of f_n and set $\beta := \alpha^n$. The integral domain $\mathbb{Z}[\alpha]$ is isomorphic to $\mathbb{Z}[X]/f_n\mathbb{Z}[X]$. By construction, the number $\gamma := (\beta^3 - \beta^2)/2$ belongs to the field of fractions of $\mathbb{Z}[\alpha]$, but not to $\mathbb{Z}[\alpha]$ itself. Yet

$$\begin{aligned} 4\gamma^2 = \beta^4(\beta - 1)^2 &= -(\beta^2 + 2)(\beta^2 - 2\beta + 1) \\ &= -\beta^4 + 2\beta^3 - 3\beta^2 + 4\beta - 2 \\ &= 2\beta^3 - 2\beta^2 + 4\beta \\ &= 4\gamma + 4\beta, \end{aligned}$$

so $\gamma^2 - \gamma = \beta$ is a root of $X^4 + X^2 + 2$ and γ is a root of the monic polynomial $(X^2 - X)^4 + (X^2 - X)^2 + 2$, which belongs to $\mathbb{Z}[X]$, therefore to $\mathbb{Z}[\alpha][X]$. Hence, the integral domain $\mathbb{Z}[\alpha]$ is not integrally closed, therefore it cannot be principal.

4.9 Remarks on the explicitness of the isomorphism

In this subsection, we assume that $\lambda(K_{\mathbb{D}}) = 1$ and we keep the notations of subsections 4.1 and 4.2. For every $n \geq 1$, we note $\mathbb{D}_n = \mathbb{D} \oplus \dots \oplus A^{n-1}\mathbb{D}$.

Applying Proposition 19 to the set $L = K_{\mathbb{D}}$ show that $p_{\mathbb{T}^d} \circ \Phi : \mathbb{D}^{\infty} \rightarrow K_{\mathbb{D}}$ is an isomorphism transforming the uniform Bernoulli shift on \mathbb{D}^{∞} into T_A . Although this map is simple and explicit, its inverse is much more involved. To make it explicit, we have to answer the following questions: given an element of $\mathbb{R}^d/\mathbb{Z}^d$, how to find its (η -almost surely unique) representative in $K_{\mathbb{D}}$? given an element of $K_{\mathbb{D}}$, how to find its $\mathcal{U}(K_{\mathbb{D}})$ -almost surely unique (A, \mathbb{D}) expansion (in base A for the system of digits \mathbb{D})?

These questions can be answered for almost every point, once we effectively know two Borel bounded subsets B_1, B_2 with positive Lebesgue measure such that $B_1 \subset K_{\mathbb{D}} \subset B_2$. Indeed, each element of $\mathbb{R}^d/\mathbb{Z}^d$ has only finitely many representatives in B_2 , and the representative in $K_{\mathbb{D}}$ should be searched among them. Hence, the questions above can be reformulated as follows: given $x \in \mathbb{R}^d$, and v_1, v_2, \dots in \mathbb{D} prove or disprove that x belongs to $K_{\mathbb{D}}$, to $A^{-1}v_1 + A^{-1}K_{\mathbb{D}}$, to $A^{-1}v_1 + A^{-2}v_2 + A^{-2}K_{\mathbb{D}}$... Equivalently, prove or disprove that the vectors $x, Ax - v_1, A^2x - Av_1 - v_2 \dots$ belong to $K_{\mathbb{D}}$.

Fix a norm $|\cdot|$ on \mathbb{R}^d and denote by $\|\cdot\|$ the associated operator norm on $\mathcal{M}_d(\mathbb{R})$. For every $x \in \mathbb{R}^d$ and $n \geq 0$,

$$\text{dist}(x, K_{\mathbb{D}}) \leq \text{dist}(x, A^{-n}\mathbb{D}_n) \leq \|A^{-n}\| \text{dist}(A^n x, \mathbb{D}_n).$$

Since $K_{\mathbb{D}}$ is closed and $\|A^{-n}\| \rightarrow 0$ as $n \rightarrow +\infty$, we derive

$$x \notin K_{\mathbb{D}} \implies \text{dist}(x, K_{\mathbb{D}}) > 0 \implies \text{dist}(A^n x, \mathbb{D}_n) \rightarrow \infty \text{ as } n \rightarrow +\infty.$$

Thus, if $x \notin K_{\mathbb{D}}$, provided the integer n is sufficiently large, all differences $A^n x - s$ with $s \in \mathbb{D}_n$ are outside B_2 . This gives us the certainty that x does not belong to $K_{\mathbb{D}}$.

Indeed, when $x \in K_{\mathbb{D}}$, i.e. $x = \sum_{k \geq 1} A^{-k} v_k$ for some sequence $(v_k)_{k \geq 1} \in \mathbb{D}^{\infty}$, we have for every $n \geq 1$,

$$A^n x - \sum_{k=1}^n A^{n-k} v_k = \sum_{k \geq n+1} A^{-(k-n)} v_k \in K_{\mathbb{D}} \subset B_2.$$

Moreover, if $x \in E$, the (A, \mathbb{D}) -expansion of x is unique, and for every $n \geq 0$,

$$A^n x - \sum_{k=1}^n A^{n-k} v_k = T_{A,E}^n(x).$$

The ergodicity of $T_{A,E}$ for $\mathcal{U}(E)$ entails that for almost every $x \in E$ (hence for almost every $x \in K_{\mathbb{D}}$), the orbit $(T_{A,E}^n(x))_{n \geq 0}$ visits B_1 infinitely many times. Thus, by computing finitely many differences $A^n x - (A^{n-1}v_1 + \dots + v_n)$, we get at the same time the certainty that x belongs to $K_{\mathbb{D}}$ and the first digits of its (A, \mathbb{D}) -expansion.

Yet, providing an explicit Borel subset $B_1 \subset K_{\mathbb{D}}$ is not simple. To illustrate the difficulty, consider again the rather simple example where $A = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}$ and $\mathbb{D} = \{(0,0), (0,1), (0,-1), (1,0), (-1,0)\}$. Figure 7 shows the first fundamental domains obtained by applying iteratively Hutchinson's map to $D_0 := [-1/2, 1/2]^2$. When \mathbb{R}^2 is endowed with the usual Euclidean metric, the map $x \mapsto Ax$ multiplies all distances by

$\sqrt{5}$. Figure 7 suggests that all points whose distance to D_n^c is larger than $\sqrt{5}^{-n} \times (1/5)$ belong to D_{n+1} , so $K_{\mathbb{D}}$ contains the square $] - b, b[$, where

$$b = \frac{1}{2} - \sum_{n \geq 0} \frac{1}{5} \left(\frac{1}{\sqrt{5}} \right)^n = \frac{1}{2} - \frac{1}{5 - \sqrt{5}}.$$

However, proving rigorously this statement is not obvious.

Acknowledgements

I thank my colleagues A. Coquio, D. Piau, J. Brossard for their constructive remarks, and G. Berhuy, who simplified my original proof for the case where $d = 2$ and $r = 2$ and drew my attention on Latimer and MacDuffee theorem and found Example 42.

References

- [1] Brossard J., Leuridan C., *Chaînes de Markov constructives indexées par \mathbb{Z}* , Annals of Probability **35-2**, 715–731 (2007).
- [2] Duda J., *Complex base numeral systems*. arxiv:0712.1309
- [3] Gabardo J.P., Yu X., *Natural tiling, lattice tiling and Lebesgue measure of integral self-affine tiles*. Journal of London Mathematical Society (2) **74**, 184–204 (2006).
- [4] Hacon D., Saldanha C., Veerman J.J.P. *Remarks on Self-Affine Tilings*. Experimental mathematics 317–327 (1996).
- [5] Hoffman C., Rudolph D., Uniform endomorphisms which are isomorphic to a Bernoulli shift, Annals of Math., **156**, 79–101 (2002).
- [6] Hutchinson J., *Fractals and self similarity*, Indiana University Mathematical Journal **30**, 713–747 (1981).
- [7] Katznelson Y. *Ergodic automorphisms of \mathbb{T}^n are Bernoulli shifts*, Israel Journal of Mathematics, 10, 186–195 (1971).
- [8] Knuth D., *A imaginary number system*. Journal of the Association for Computing Machinery, **3-4**, 245–247 (1960).
- [9] Lagarias J., Wang Y. *Integral self-affine tiles in \mathbb{R}^n II. Lattice tilings*. Journal of Fourier Analysis and Applications. **3**, 83–102 (1997)
- [10] Matula D., *Basic digit sets for radix representation*. Journal of the Association for Computing Machinery, **29-4**, 1131–1143 (1982).
- [11] Mihailescu E., *Higher dimensional expanding maps and toral extensions*, De Gruyter Proc. Math. 81–92 (2014).
- [12] Penney W., *A ‘binary system’ for complex numbers*. Journal of the Association for Computing Machinery, **12-2**, 247–248 (1965).
- [13] Taussky O., *On a theorem of Latimer and MacDuffee*, Canadian Journal of Mathematics, bf 1-3, 300–302 (1949).