



HAL
open science

On the affine random walk on the torus

Jean-Baptiste Boyer

► **To cite this version:**

| Jean-Baptiste Boyer. On the affine random walk on the torus. 2017. hal-01478016

HAL Id: hal-01478016

<https://hal.science/hal-01478016>

Preprint submitted on 27 Feb 2017

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.



Distributed under a Creative Commons Attribution - NonCommercial - ShareAlike 4.0 International License

ON THE AFFINE RANDOM WALK ON THE TORUS

JEAN-BAPTISTE BOYER

ABSTRACT. Let μ be a borelian probability measure on $\mathbf{G} := \mathrm{SL}_d(\mathbb{Z}) \times \mathbb{T}^d$. Define, for $x \in \mathbb{T}^d$, a random walk starting at x denoting for $n \in \mathbb{N}$,

$$\begin{cases} X_0 &= x \\ X_{n+1} &= a_{n+1}X_n + b_{n+1} \end{cases}$$

where $((a_n, b_n)) \in \mathbf{G}^{\mathbb{N}}$ is an iid sequence of law μ .

Then, we denote by \mathbb{P}_x the measure on $(\mathbb{T}^d)^{\mathbb{N}}$ that is the image of $\mu^{\otimes \mathbb{N}}$ by the map $((g_n) \mapsto (x, g_1x, g_2g_1x, \dots, g_n \dots g_1x, \dots))$ and for any $\varphi \in L^1((\mathbb{T}^d)^{\mathbb{N}}, \mathbb{P}_x)$, we set $\mathbb{E}_x \varphi((X_n)) = \int \varphi((X_n)) d\mathbb{P}_x((X_n))$.

Bourgain, Furmann, Lindenstrauss and Mozes studied this random walk when μ is concentrated on $\mathrm{SL}_d(\mathbb{Z}) \times \{0\}$ and this allowed us to study, for any hölder-continuous function f on the torus, the sequence $(f(X_n))$ when x is not too well approximable by rational points.

In this article, we are interested in the case where μ is not concentrated on $\mathrm{SL}_d(\mathbb{Z}) \times \mathbb{Q}^d/\mathbb{Z}^d$ and we prove that, under assumptions on the group spanned by the support of μ , the Lebesgue's measure ν on the torus is the only stationary probability measure and that for any hölder-continuous function f on the torus, $\mathbb{E}_x f(X_n)$ converges exponentially fast to $\int f d\nu$.

Then, we use this to prove the law of large numbers, a non-concentration inequality, the functional central limit theorem and it's almost-sure version for the sequence $(f(X_n))$.

In the appendix, we state a non-concentration inequality for products of random matrices without any irreducibility assumption.

CONTENTS

1. Introduction and main results	2
1.1. Some kind of diophantine assumption is necessary	7
1.2. Proof of theorem 1.4 given the results of sections 2 and 3	8
1.3. Proof of theorem 1.6	10
2. The non-equidistribution comes from the lower regularity of the measure	12
2.1. Spectral gap in $L^p(\mathbb{T}^d)$	13
2.2. Equidistribution, lower regularity and spectral gap.	18
3. Measure of points-stabilizers	21
4. Effective shadowing lemmas	23
Appendix A. Products of random matrices	30
References	37

Date: February 27, 2017.

1. INTRODUCTION AND MAIN RESULTS

Let $d \in \mathbb{N}$, $d \geq 2$ and $\mathbb{T}^d := \mathbb{R}^d/\mathbb{Z}^d$ be the torus of dimension d . Let μ be a borelian probability measure on $\mathbf{G} := \mathrm{SL}_d(\mathbb{Z}) \times \mathbb{T}^d$. Define, for any $x \in \mathbb{T}^d$, a random walk starting at x by denoting, for any $n \in \mathbb{N}$,

$$\begin{cases} X_0 &= x \\ X_{n+1} &= a_{n+1}X_n + b_{n+1} \end{cases}$$

where $((a_n, b_n)) \in \mathbf{G}^{\mathbb{N}}$ is an iid sequence of law μ .

Then, we denote by \mathbb{P}_x the measure on $\mathbf{X}^{\mathbb{N}}$ that is the image of the measure $\mu^{\otimes \mathbb{N}}$ on $\mathbf{G}^{\mathbb{N}}$ by the map $((g_n) \mapsto (x, g_1x, g_2g_1x, \dots, g_n \dots g_1x, \dots))$ and by \mathbb{E}_x the operator of integration against the measure \mathbb{P}_x .

We denote by P the Markov operator associated to μ . This is the operator defined for any borelian non-negative function f on \mathbb{T}^d and any $x \in \mathbb{T}^d$ by

$$Pf(x) = \int_{\mathbf{G}} f(gx) d\mu(g)$$

Thus, for any $n \in \mathbb{N}$, we have that

$$P^n f(x) = \int_{\mathbf{G}} f(gx) d\mu^{*n}(g) = \int_{\mathbb{T}^d} f(y) d\mu^{*n} * \delta_x(y) = \int_{(\mathbb{T}^d)^{\mathbb{N}}} f(X_n) d\mathbb{P}_x((X_n)) = \mathbb{E}_x f(X_n)$$

Where we noted μ^{*n} the n -th power of convolution of the measure μ (μ^{*0} is by convention the Dirac measure at $(I_d, 0)$).

Bourgain, Furmann, Lindenstrauss and Mozes studied in [BFLM11] the case where μ is concentrated on $\mathrm{SL}_d(\mathbb{Z}) \times \{0\}$ and they proved that, under assumptions on the support of μ , the only P -invariant probability measures on the torus where the Lebesgue's measure ν and the uniform measures on unions of rational orbits (which are finite). their result is even more precise since they give the rate of convergence of $\mathbb{E}_x f(X_n)$ to $\int f d\nu$ in terms of diophantine properties of x and this allowed us to study the sequence $(f(X_n))$ for starting points x that are not too well approximable by rational points in [Boy16].

In this article, we are interested in the case where μ is not concentrated on $\mathrm{SL}_d(\mathbb{Z}) \times \mathbb{Q}^d/\mathbb{Z}^d$. A result by Benoist-Quint (see [BQ11]) shows that in this case, under assumptions on the projection on $\mathrm{SL}_d(\mathbb{Z})$ of the subgroup spanned by the support of μ , the only P -invariant probability measure on the torus is Lebesgue's measures and this proves that for any continuous function f on \mathbb{T}^d and any $x \in \mathbb{T}^d$,

$$\frac{1}{n} \sum_{k=0}^{n-1} f(X_k) \rightarrow \int f d\nu \quad \mathbb{P}_x - \text{a.e.}$$

The aim of this article is to precise the previous convergence by proving a Central Limit Theorem, a Law of the Iterated Logarithm, etc.

To do so, we are going to make a few assumptions on the subgroup spanned by $\{a|(a, b) \in \mathrm{supp} \mu\}$.

In the sequel, we will say that a closed subgroup \mathbf{H} of $\mathrm{SL}_d(\mathbb{R})$ is strongly irreducible if it doesn't fix any finite union of non-trivial subspaces of \mathbb{R}^d . Moreover, we will say that \mathbf{H} is proximal if it contains an element g such that there is $v_g^+ \in \mathbb{R}^d \setminus \{0\}$, $\lambda \in \mathbb{R}$

and a g -invariant hyperplane $V_g^<$ in \mathbb{R}^d such that $\mathbb{R}^d = \mathbb{R}v_g^+ \oplus V_g^<$, $gv_g^+ = \lambda v_g^+$ and the spectral radius of g in $V_g^<$ is strictly smaller than $|\lambda|$. Finally, we will say that a probability measure μ on $\mathrm{SL}_d(\mathbb{R})$ is strongly irreducible and proximal if the closure of the subgroup spanned by the support of μ has these properties.

These two assumptions are actually assumptions on the Zariski-closure of \mathbf{H} and so, as an example, they are satisfied if \mathbf{H} is Zariski-dense in $\mathrm{SL}_d(\mathbb{R})$.

Finally, we will say that a measure μ on $\mathrm{SL}_d(\mathbb{R})$ has an exponential moment if there is some $\varepsilon \in \mathbb{R}_+^*$ such that

$$\int_{\mathrm{SL}_d(\mathbb{R})} \|g\|^\varepsilon d\mu(g) < +\infty$$

We will see in the sequel that our study of the random walk on the torus requires arguments of orbit closures. This is why we give a name to the property that we will use and we will see right after examples of measures satisfying it.

Definition 1.1. Let μ be a borelian probability measure on \mathbf{G} .

We say that μ satisfies an effective shadowing lemma if for any $C', t' \in \mathbb{R}_+^*$, there are $C_1, C_2, M, t, L \in \mathbb{R}_+^*$ such that for any $x, y \in \mathbb{T}^d$, any $r \in \mathbb{R}_+^*$ and any $n \in \mathbb{N}$, with $r \leq C_1 e^{-Ln}$, if

$$\mu^{*n}(\{g \in \mathbf{G} | d(gx, y) \leq r\}) \geq C_2 e^{-tn}$$

then, there are $x', y' \in \mathbb{T}^d$ such that $d(x, x'), d(y, y') \leq r e^{Mn}$ and

$$\mu^{*n}(\{g \in \mathbf{G} | gx' = y'\}) \geq C' e^{-t'n}$$

Remark 1.2. For a measure to satisfy this property means that if a lot of elements $g \in \mathrm{supp} \mu^{*n}$ send x close to y , it is only because x and y are close to points of the same orbit. The name comes from the theory of hyperbolic diffeomorphisms since when $\mu = \delta_{g_0}$, saying that μ satisfies an effective shadowing lemma means that there is some constant M such that for any large enough K , any $n \in \mathbb{N}$ and any $x, y \in \mathbb{T}^d$ with $d(g_0^n x, y) \leq e^{-Kn}$, there are $x', y' \in \mathbb{T}^d$ such that $d(x, x'), d(y, y') \leq e^{-(K-M)n}$ and $g_0^n x' = y'$.

Example 1.3. This is a technical definition but we will see in section 4 a criterion (the proposition 4.7) that allows to tell if a measure satisfies to an effective shadowing lemma and we will deduce examples from it.

In particular, we will see in example 4.4 that if $b_0 \in \mathbb{T}^1$ is such that there are $C, L \in \mathbb{R}_+^*$ such that for any $q \in \mathbb{N}^*$, $d(qb_0, 0) \geq \frac{C}{q^L}$, then, any borelian probability measure μ on \mathbf{G} whose projection on $\mathrm{SL}_d(\mathbb{Z})$ is strongly irreducible, proximal and has an exponential moment and such that $F(\mu) := \{\text{coefficients of } b | (a, b) \in \mathrm{supp} \mu\} \subset \{0, b_0\}$ satisfies an effective shadowing lemma.

Moreover, in example 4.6 we will prove that if $a_1, \dots, a_N \in \mathrm{SL}_d(\mathbb{Z})$ generate a strongly irreducible and proximal group, then for a.e. $b_1, \dots, b_N \in \mathbb{T}^d$, the measure $\mu = \frac{1}{N} \sum_{i=1}^N \delta_{(a_i, b_i)}$ satisfies an effective shadowing lemma.

For $\alpha \in]0, 1]$, we denote by $\mathcal{C}^{0, \alpha}(\mathbb{T}^d)$ the space of α -hölder-continuous functions f on \mathbb{T}^d endowed with the norm

$$\|f\|_\alpha := \|f\|_\infty + m_\alpha(f)$$

where

$$\|f\|_\infty := \sup_x |f(x)| \text{ and } m_\alpha(f) := \sup_{x \neq y} \frac{|f(x) - f(y)|}{d(x, y)^\alpha}$$

where d is the distance induced by some norm on \mathbb{R}^d .

Moreover, for any two borelian probability measures ϑ_1, ϑ_2 on \mathbb{T}^d , we denote by $\mathcal{W}_\alpha(\vartheta_1, \vartheta_2)$ the Kantorovich-Rubinstein's distance of ϑ_1 and ϑ_2 and this is defined by

$$\mathcal{W}_\alpha(\vartheta_1, \vartheta_2) := \sup_{\substack{f \in \mathcal{C}^{0, \alpha}(\mathbb{T}^d) \\ \|f\|_\alpha \leq 1}} \left| \int f d\vartheta_1 - \int f d\vartheta_2 \right|$$

This will allow us to prove the

Theorem 1.4. *Let μ be a borelian probability measure on $\mathbf{G} := \mathrm{SL}_d(\mathbb{Z}) \ltimes \mathbb{T}^d$ that is not concentrated on $\mathrm{SL}_d(\mathbb{Z}) \ltimes \mathbb{Q}^d/\mathbb{Z}^d$ and satisfies an effective shadowing lemma. Note μ_0 the projection of μ on $\mathrm{SL}_d(\mathbb{Z})$ and assume that μ_0 is strongly irreducible, proximal and has an exponential moment.*

Denote by P the Markov operator associated to μ .

Then, the Lebesgue's measure ν on \mathbb{T}^d is the only P -invariant borelian probability measure on the torus. Moreover, for any $\alpha \in]0, 1]$, there are $C, t \in \mathbb{R}_+^$ such that for any $f \in \mathcal{C}^{0, \alpha}(\mathbb{T}^d)$ and any $n \in \mathbb{N}$,*

$$\sup_{x \in \mathbb{T}^d} \mathcal{W}_\alpha(\mu^{*n} * \delta_x, \nu) \leq C e^{-tn} \|f\|_\alpha$$

In particular, for any α -hölder-continuous function f on the torus, there is a continuous function g such that

$$f - \int f d\nu = g - Pg \text{ and } \|g\|_\infty \leq C \|f\|_\alpha$$

Remark 1.5. We don't know if the function g that we construct in this theorem is hölder-continuous.

This theorem will allow us to prove a few of the classical results in probability theory for the sequence $(f(X_n))$ in the

Theorem 1.6. *Under the same assumptions than in theorem 1.4.*

Denote, for any continuous function f on the torus, $\bar{f} = f - \int f d\nu$ and, for any sequence $\underline{x} = (X_n) \in (\mathbb{T}^d)^\mathbb{N}$,

$$S_n f(\underline{x}) = \sum_{k=0}^{n-1} \bar{f}(X_k) = \sum_{k=0}^{n-1} f(X_k) - n \int f d\nu$$

Moreover, for any $t \in [0, 1]$, set

$$\xi_n(t) = \frac{1}{\sqrt{n}} \left(S_i f(\underline{x}) + n \left(t - \frac{i}{n} \right) f(X_i) \right) \text{ for } \frac{i}{n} \leq t \leq \frac{i+1}{n} \text{ and } 0 \leq i \leq n-1$$

Then, for any continuous function f on the torus and any $x \in \mathbb{T}^d$,

$$\frac{S_n f(\underline{x})}{n} \rightarrow 0 \text{ } \mathbb{P}_x - \text{a.e.}$$

Moreover, for any $\alpha \in]0, 1]$ there is $t \in \mathbb{R}_+^*$ such that for any $\varepsilon \in]0, 1]$ there is a constant C such that for any α -hölder-continuous function f on the torus, any $x \in \mathbb{T}^d$ and any $n \in \mathbb{N}$,

$$\mathbb{P}_x \left(\left\{ \underline{x} \in \mathbf{X}^{\mathbb{N}} \mid |S_n f(\underline{x})| > n\varepsilon \|f\|_\alpha \right\} \right) \leq C e^{-t\varepsilon^2 n}$$

Finally, set

$$\sigma^2(f) := \int_{\mathbb{T}^d} g^2 - (Pg)^2 d\nu$$

and then,

(1) If $\sigma^2(f) \neq 0$ then for any bounded continuous $F : \mathcal{C}^0([0, 1]) \rightarrow \mathbb{R}$ and any $x \in \mathbb{T}^d$,

$$\mathbb{E}_x F(\xi_n) \rightarrow \mathbb{E} F(W_{\sigma^2}) \quad \text{and} \quad \frac{1}{\ln n} \sum_{k=1}^n \frac{1}{k} F(\xi_k) \rightarrow \mathbb{E} F(W_{\sigma^2}) \quad \mathbb{P}_x - a.e.$$

Where W_{σ^2} denotes Wiener's measure of variance σ^2 .

And for any continuous function φ on \mathbb{R} such that $t^2\varphi(t)$ is bounded and for any $x \in \mathbb{T}^d$,

$$\frac{1}{\ln n} \sum_{k=1}^n \frac{1}{k} \varphi \left(\frac{S_k f(\underline{x})}{\sqrt{k}} \right) \rightarrow \mathbb{E} \varphi(W_{\sigma^2}(1)) \quad \mathbb{P}_x - a.e.$$

(2) If $\sigma^2(f) = 0$ then for any $x \in \mathbb{T}^d$ and any $n \in \mathbb{N}$, $S_n f \in L^\infty(\mathbb{P}_x)$ and

$$\|S_n f\|_{L^\infty(\mathbb{P}_x)} \leq 2C \|f\|_\alpha$$

Remark 1.7. The two convergences of $(F(\xi_n))$ in point (1) are respectively called *functional central limit theorem* (FCLT) and *almost-sure functional central limit theorem* (ASFCLT). There is no obvious link between the convergence in law of $(F(\xi_n))$ and the a.e. convergence of its logarithmic average (see [BC01] for a criterion). However, note that we have to take a logarithmic mean because of the arc sine law.

Remark 1.8. The FCLT and the ASFCLT have many corollaries such as the central limit theorem and the almost sure central limit theorem (taking $F_\varphi(\xi) = \varphi(\xi(1))$ for any continuous and bounded function φ on \mathbb{R}), the law of the iterated logarithm (see theorem 2.4 in [Cha96]), a control of $\frac{\max_{k \in [0, n]} S_k f(\underline{x})}{\sqrt{n}}$ (taking $F(\xi) := \sup_{t \in [0, 1]} \xi(t)$), or an estimation of $\sigma^2(f)$ (taking $\varphi(x) = x^2$).

Before we continue, we give an example where there is a non-constant function f such that $\sigma^2(f) = 0$.

Example 1.9. Let

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Then, the subgroup spanned by A and B is strongly irreducible and proximal.

Let $b_0 \in \mathbb{T}^1 \setminus \mathbb{Q}/\mathbb{Z}$ be a diophantine number¹, $b = (b_0, 0)$ and $\mu = \frac{1}{2}\delta_{(A,b)} + \frac{1}{2}\delta_{(BA, Bb)}$.

Then, according to proposition 4.7, the measure μ satisfies to the assumptions of theorem 1.4.

¹There are $C, L \in \mathbb{R}_+^*$ such that for any $q \in \mathbb{N}^*$, $d(qb_0, 0) \geq Cq^{-L}$.

Let g be the function defined for any $x \in \mathbb{T}^2$ by $g(x) = d(x, 0)$. We made everything so that for any $x \in \mathbb{T}^2$, $g(Bx) = g(x)$.

Then, for any $x \in \mathbb{T}^2$,

$$Pg(x) = \frac{1}{2}g(Ax + b) + \frac{1}{2}g(BAx + Bb) = g(Ax + b)$$

And,

$$\int_{\mathbf{X}} |Pg(x)|^2 d\nu(x) = \int_{\mathbf{X}} |g(Ax + b)|^2 d\nu(x) = \int_{\mathbf{X}} |g(x)|^2 d\nu(x)$$

Moreover, if we set $f = g - Pg$, then, we just saw that $\sigma^2(f) = \int g^2 - (Pg)^2 d\nu = 0$ and for any $x \in \mathbf{X}$, $n \in \mathbb{N}$ and any $(g_1, \dots, g_n) \in \{(A, b), (BA, Bb)\}^n$, we have that

$$g(g_{n+1} \dots g_1 x) = g(Ag_n \dots g_1 x + b)$$

And so,

$$\begin{aligned} \sum_{k=0}^{n-1} f(g_k \dots g_1 x) &= g(x) - g(g_n \dots g_1 x) + \sum_{k=0}^{n-1} g(g_{k+1} \dots g_1 x) - g(Ag_k \dots g_1 x + b) \\ &= g(x) - g(g_n \dots g_1 x) \end{aligned}$$

This proves that for any $x \in \mathbf{X}$, the sequence $(\sum_{k=0}^{n-1} f(g_k \dots g_1 x))$ is bounded in $L^\infty(\mathbb{P}_x)$.

The results in section 3 of [Boy16] actually prove that this example is really general.

We will see in sub-section 1.3 that theorem 1.6 is a quite general corollary of theorem 1.4 since we can easily study functions f on the torus that writes $f = g - Pg + \int f d\nu$ with g continuous and theorem 1.4 precisely says that any holder-continuous function can be written in this way.

Therefore, the main point of this article is the proof of theorem 1.4. To do so, we use the same method as Bourgain, Furmann, Lindenstrauss and Mozes. In section 2, we prove that the only obstacle in the equidistribution of the measure $\mu^{*n} * \vartheta$ is the lower regularity of ϑ i.e. the existence of points x such that for some r depending on n ,

$$\vartheta(B(x, r)) \geq r^\varepsilon$$

In particular, if $\mu^{*n+m} * \vartheta$ is far from Lebesgue's measure then there has to be points x such that

$$\mu^{*m} * \vartheta(B(x, r)) \geq r^\varepsilon$$

Then, our assumptions that μ satisfies an effective shadowing lemma and that $\text{supp } \mu$ is not a subset of $\text{SL}_d(\mathbb{Z}) \times \mathbb{Q}^d / \mathbb{Z}^d$ will allow us to prove in section 3 that this cannot happen when $r \ll e^{-m} \ll r^\varepsilon$.

The precise proof of the theorem is in subsection 1.2.

Finally, in section 4, we prove proposition 4.7 that is a criterion that shows that under some diophantine conditions on the translations in it's support, a measure satisfies an effective shadowing lemma and we will use this criterion to produce examples of such measures.

In the appendix, we state results on the products of random matrices in the case where the action is not irreducible and that we use in section 3.

1.1. Some kind of diophantine assumption is necessary. We already said (and we will prove in section 4) that a way to guarantee that a measure satisfies an affective shadowing lemma is to require diophantine conditions on the coefficients of the translations of it's support. In this sub-section, we prove that this kind of assumptions is indeed necessary to get theorem 1.4.

Proposition 1.10. *Let $a, b \in \mathrm{SL}_d(\mathbb{Z})$ and $v \in \mathbb{T}^d$. Set $\mu = \frac{1}{2}\delta_{(a,0)} + \frac{1}{2}\delta_{(b,v)}$.*

Assume that for some $\alpha \in]0, 1]$, there are $C, t \in \mathbb{R}_+^$ such that for any α -hölder-continuous function f on the torus and any $n \in \mathbb{N}$,*

$$\sup_{x \in \mathbb{T}^d} \left| P^n f(x) - \int f d\nu \right| \leq C e^{-tn} \|f\|_\alpha$$

Then, there are constants $C_0, L \in \mathbb{R}_+^$ such that for any rational point $\frac{p}{q} \in \mathbb{Q}^d/\mathbb{Z}^d$,*

$$d\left(v, \frac{p}{q}\right) \geq \frac{C_0}{q^L}$$

Proof. For $q \in \mathbb{N}^*$ and $x \in \mathbb{T}^d$, we set $X_q = \frac{1}{q}\mathbb{Z}^d/\mathbb{Z}^d$ and

$$f_q(x) = 1 - \min(1, q^{2\alpha} d(x, X_q)^\alpha)$$

This function is chosen so that it takes the value 1 on $\frac{1}{q}\mathbb{Z}^d/\mathbb{Z}^d$, it vanishes on the complementary of the $\frac{1}{q^2}$ -neighborhood of $\frac{1}{q}\mathbb{Z}^d/\mathbb{Z}^d$ and it is hölder-continuous with $\|f_q\|_\alpha \leq q^{2\alpha}$.

In particular, we have that, for some constant C depending only on d (and on the distance on \mathbb{T}^d),

$$\int f_q d\nu \leq \sum_{\frac{p}{q} \in \frac{1}{q}\mathbb{Z}^d/\mathbb{Z}^d} \nu\left(B\left(\frac{p}{q}, \frac{1}{q^2}\right)\right) \leq \frac{C}{q^d}$$

Moreover, for $\mu^{\otimes \mathbb{N}}$ -a.e. $((a_n, b_n))$, we have that

$$\begin{aligned} \left| f_q\left(\sum_{k=1}^n a_n \dots a_{k+1} b_k\right) - 1 \right| &\leq \|f_q\|_\alpha d\left(\sum_{k=1}^n a_n \dots a_{k+1} b_k, X_q\right)^\alpha \\ &\leq \frac{e^{\alpha M n}}{(e^M - 1)^\alpha} d(v, X_q)^\alpha q^{2\alpha} \end{aligned}$$

where we noted $e^M = \max(\|A\|, \|B\|)$. Indeed, for any $\frac{p}{q} \in X_q$, we have that $f_q(p/q) = 1$ and $\sum_{k=1}^n a_n \dots a_{k+1} b_k$ can be written Dv where D is a matrix with integer coefficients and $\|D\| \leq \sum_{k=1}^n \|a_n \dots a_{k+1}\| \leq \sum_{k=1}^n e^{M(n-k)}$. This proves that for any $n \in \mathbb{N}$,

$$|P^n f_q(0) - 1| = \left| \int_{\mathbf{G}} f_q(b) d\mu^{*n}(a, b) - 1 \right| \leq \frac{e^{\alpha M n}}{(e^M - 1)^\alpha} d(v, X_q)^\alpha q^{2\alpha}$$

But, by assumption, we also have that

$$\left| P^n f_q(0) - \int f_q d\nu \right| \leq C e^{-tn} \|f_q\|_\alpha \leq C e^{-tn} q^{2\alpha}$$

So, this proves that for any $n, q \in \mathbb{N}^*$,

$$1 - \frac{C}{q^d} - Ce^{-tn}q^{2\alpha} \leq \frac{e^{\alpha Mn}}{(e^M - 1)^\alpha} d(v, X_q)^\alpha q^{2\alpha}$$

Thus, for any $p \in \mathbb{Z}^d$, any $q \in \mathbb{N}^*$ such that $q^d \geq 4C$ and any n such that $Ce^{-tn} \leq q^{-2\alpha}/4$, we have that

$$d\left(v, \frac{p}{q}\right) \geq \frac{e^M - 1}{2^{1/\alpha} e^{Mn} q^2}$$

In particular, for $n = \lfloor \frac{1}{t} \ln(4Cq^{2\alpha}) \rfloor + 1$, we find that, for some constant C' depending only on M, α, t, C ,

$$d\left(v, \frac{p}{q}\right) \geq \frac{C'}{q^{2+2\alpha M/t}}$$

And this is what we intended to prove. \square

Remark 1.11. We can prove the same kind of results for rates more general than Ce^{-tn} and this shows that even convergences slower than exponential require some kind of diophantine assumption.

1.2. Proof of theorem 1.4 given the results of sections 2 and 3. Let $\alpha \in]0, 1]$ and $\varepsilon \in \mathbb{R}_+^*$.

According to theorem 2.1 there are constants $c_0, \varepsilon' \in \mathbb{R}_+^*$ with $\varepsilon' < \varepsilon$ such that for any $\vartheta \in \mathcal{M}^1(\mathbb{T}^d)$, any $t \in]0, 1]$ and any $n \in \mathbb{N}$ with $n \geq c_0(1 + |\ln t|)$,

$$\mathcal{W}_\alpha(\mu^{*n} * \vartheta, \nu) \geq t \Rightarrow \vartheta\left(\left\{x \in \mathbb{T}^d \mid \vartheta(B(x, r)) \geq r^\varepsilon\right\}\right) \geq t^{c_0}$$

where

$$r = e^{-(\Lambda_1 + \varepsilon')n} \left(\frac{t}{16}\right)^{1/\alpha}$$

In particular, for any $m, n \in \mathbb{N}$, any $\vartheta \in \mathcal{M}^1(\mathbb{T}^d)$ any $t \in \mathbb{R}_+^*$ small enough and any C large enough,

$$\mathcal{W}_\alpha(\mu^{*n+m} * \vartheta, \nu) \geq Ce^{-tn} \Rightarrow \mu^{*m} * \vartheta\left(\left\{x \in \mathbb{T}^d \mid \mu^{*m} * \vartheta(B(x, r)) \geq r^\varepsilon\right\}\right) \geq (Ce^{-tn})^{c_0}$$

for

$$r = \frac{e^{-(\Lambda_1 + \varepsilon' - \delta/\alpha)n}}{16^{1/\alpha}}$$

But, since the measure satisfies to an effective shadowing lemma, according to proposition 3.1, there are $C_1, C_2, t_0, L \in \mathbb{R}_+^*$ such that for any $x, y \in \mathbb{T}^d$, any $m \in \mathbb{N}$ and any $r \in \mathbb{R}_+^*$ with $r \leq C_1 e^{-Lm}$,

$$\mu^{*m}(\{g \in \mathbf{G} \mid d(gx, y) \leq r\}) \leq C_2 e^{-t_0 m}$$

And so, to get a contradiction, we only need to assume that

$$r = \frac{e^{-(\Lambda_1 + \varepsilon' - \delta/\alpha)n}}{16^{1/\alpha}} \leq C_1 e^{-Lm} \text{ and } r^\varepsilon = \frac{e^{-\varepsilon(\Lambda_1 + \varepsilon' - \delta/\alpha)n}}{16^{\varepsilon/\alpha}} \geq C_2 e^{-t_0 m}$$

And this is always possible for $n = Km$ with $K \in \mathbb{N}$ large enough and ε small enough.

We just proved that there are $C, t \in \mathbb{R}_+^*$ and $K \in \mathbb{N}^*$ such that for any borelian probability measure ϑ on \mathbb{T}^d and any $m \in \mathbb{N}$,

$$\mathcal{W}_\alpha \left(\mu^{*(K+1)m} * \vartheta, \nu \right) \leq C e^{-tm}$$

Let $n \in \mathbb{N}$ and let $m, L \in \mathbb{N}$ be such that $n = (K+1)m + L$ and $0 \leq L < K+1$. Then,

$$\begin{aligned} \mathcal{W}_\alpha (\mu^{*n} * \vartheta, \nu) &\leq \mathcal{W}_\alpha \left(\mu^{*(K+1)m} * \mu^{*L} * \vartheta, \nu \right) \leq C e^{-tm} = C e^{-\frac{t}{K+1}(n-L)} \\ &\leq C e^t e^{-tn/(K+1)} \end{aligned}$$

And this finishes the proof of the first part of the theorem.

In particular, with $\vartheta = \delta_x$ for some $x \in \mathbb{T}^d$, we get that for any α -h"older-continuous function f on \mathbb{T}^d and any $x \in \mathbb{T}^d$,

$$\left| P^n f(x) - \int f d\nu \right| \leq C e^{-tn} \|f\|_\alpha$$

Let f be an α -h"older-continuous function on \mathbb{T}^d . Set, for any $n \in \mathbb{N}$,

$$g_n = \sum_{k=0}^{n-1} P^k f - \int f d\nu$$

Then,

$$(I_d - P)g_n = f - \int f d\nu - \left(P^n f - \int f d\nu \right)$$

And so,

$$\lim_n g_n - P g_n = f - \int f d\nu$$

Moreover, the series is normally convergent since

$$\sum_n \left\| P^n f - \int f d\nu \right\|_\infty \leq \frac{C}{1 - e^{-t}} \|f\|_\alpha$$

And so, the function $g = \lim_n g_n$ exists, is continuous and satisfies

$$g - P g = f - \int f d\nu \text{ and } \|g\|_\infty \leq \frac{C}{1 - e^{-t}} \|f\|_\alpha$$

Now, let ϑ be a P -invariant borelian probability measure on \mathbb{T}^d . Then, for any h"older-continuous function f ,

$$\int f d\vartheta = \int P^n f d\vartheta \xrightarrow{n \rightarrow +\infty} \int f d\nu$$

Where we first used the P -invariance of ϑ and then the dominated convergence theorem since for any $x \in \mathbb{T}^d$, $\lim_n P^n f(x) = \int f d\nu$ according to the first part of the proof. And, finally, as the h"older-continuous functions are dense in the space of continuous functions on the torus, this proves that $\vartheta = \nu$ and so, ν is the unique P -invariant borelian probability measure on \mathbb{T}^d .

1.3. Proof of theorem 1.6.

Proof of the law of large numbers. This result is a consequence of the uniqueness of the P -invariant borelian probability measure seen in theorem 1.4. Indeed, if we manage to prove that for any x and \mathbb{P}_x -a.e. $\underline{x} = (X_n) \in (\mathbb{T}^d)^\mathbb{N}$, the accumulation points of $\nu_{n,\underline{x}} := \frac{1}{n} \sum_{k=0}^{n-1} \delta_{X_k}$ are P -invariant, we will get that they have to be the Lebesgue's measure and so, for any continuous function f on the torus,

$$\frac{1}{n} \sum_{k=0}^{n-1} f(X_k) \rightarrow \int f d\nu \quad \mathbb{P}_x - \text{a.e.}$$

For any continuous function f on the torus, we can compute,

$$\begin{aligned} \int f d\nu_{n,\underline{x}} - \int P f d\nu_{n,\underline{x}} &= \frac{1}{n} \sum_{k=0}^{n-1} f(X_k) - \frac{1}{n} \sum_{k=0}^{n-1} P f(X_k) \\ &= \frac{1}{n} \sum_{k=0}^{n-1} f(X_{k+1}) - P f(X_k) + \frac{1}{n} (f(X_0) - f(X_n)) \end{aligned}$$

But, $M_n = \sum_{k=0}^{n-1} f(X_{k+1}) - P f(X_k)$ is a martingale with bounded increments so $\frac{1}{n} M_n \rightarrow 0$ a.e. and as f is bounded, we also have that $\frac{1}{n} (f(X_0) - f(X_n)) \rightarrow 0$ in $L^\infty(\mathbb{P}_x)$.

Thus, we just proved that for any $x \in \mathbb{T}^d$ and any continuous function f on \mathbb{T}^d , there is $X_f \subset (\mathbb{T}^d)^\mathbb{N}$ such that $\mathbb{P}_x(X_f) = 1$ and for any $\underline{x} \in X_f$,

$$\lim_n \int f d\nu_{n,\underline{x}} - \int P f d\nu_{n,\underline{x}} = 0$$

Let (f_i) be a dense sequence in $\mathcal{C}^0(\mathbb{T}^d)$ and $X_\infty = \cap_i X_{f_i}$. Then, $\mathbb{P}_x(X_\infty) = 1$ and for any $\underline{x} \in X_\infty$ and any $i \in \mathbb{N}$,

$$\lim_n \int f_i d\nu_{n,\underline{x}} - \int P f_i d\nu_{n,\underline{x}} = 0$$

So, as the sequence (f_i) is dense, we get that for any continuous function f on \mathbb{T}^d and any $\underline{x} \in X_\infty$,

$$\lim_n \int f d\nu_{n,\underline{x}} - \int P f d\nu_{n,\underline{x}} = 0$$

This proves that for any $\underline{x} \in X_\infty$, the accumulation points of $(\nu_{n,\underline{x}})$ are P -invariant and so they are equal to ν and this proves the law of large numbers. \square

To prove the remaining part of the theorem, we are going to use Gordin's method and deduce the non-concentration inequality, the FCLT and the ASFCLT from these results for martingales. Indeed, according to theorem 1.4, for any $\alpha \in]0, 1]$, there is a constant C such that for any α -h"older-continuous function f on the torus there is a continuous function g such that

$$f - \int f d\nu = g - P g \text{ and } \|g\|_\infty \leq C \|f\|_\alpha$$

Set, for $\underline{x} = (X_n) \in \mathbf{X}^{\mathbb{N}}$,

$$S_n f(\underline{x}) = \sum_{k=0}^{n-1} f(X_k) - n \int f d\nu \text{ and } M_n = \sum_{k=0}^{n-1} g(X_{k+1}) - P g(X_k)$$

Then,

$$S_n f(\underline{x}) = M_n + g(X_0) - g(X_n)$$

And M_n is a martingale with bounded increments.

Proof of the non-concentration inequality. For any $n \in \mathbb{N}$, we have that

$$|M_n| \geq |S_n f(\underline{x})| - 2\|g\|_{\infty} \geq |S_n f(\underline{x})| - 2C\|f\|_{\alpha}$$

So, using Azuma-Hoeffding's inequality, if $n\varepsilon > 2C$, we get that

$$\begin{aligned} I_n(x) &:= \mathbb{P}_x(|S_n f(\underline{x})| > n\varepsilon\|f\|_{\alpha}) \leq \mathbb{P}_x(|M_n| \geq (n\varepsilon - 2C)\|f\|_{\alpha}) \\ &\leq 2 \exp\left(\frac{-(n\varepsilon - 2C)^2\|f\|_{\alpha}^2}{2n(2C\|f\|_{\alpha})^2}\right) = 2 \exp\left(-\frac{n\varepsilon^2}{8C^2} + \frac{\varepsilon}{4C} - \frac{1}{2n}\right) \end{aligned}$$

And this finishes the proof of this point. \square

Proof of points 1 and 2. As the function g is bounded, the sequence $(S_n f(\underline{x}) - M_n)$ is bounded in $L^{\infty}(\mathbb{P}_x)$ and so it is clear that to prove the FCLT and the AEFCLT, it is enough to study the martingale M_n (that has bounded increments). But, according to the functional central limit theorem for martingales (see corollary 4.1 in [HH80]) and it's almost sure extension (see [Cha96]), it is enough to prove the a.e. convergence of the variance (when the limit doesn't vanish). But, for any $n \in \mathbb{N}^*$,

$$\begin{aligned} \frac{1}{n} \sum_{k=0}^{n-1} \mathbb{E}_x \left[|M_{k+1} - M_k|^2 \middle| X_0, \dots, X_k \right] &= \frac{1}{n} \sum_{k=0}^{n-1} \mathbb{E}_x \left[|g(X_{k+1}) - P g(X_k)|^2 \middle| X_0, \dots, X_k \right] \\ &= \frac{1}{n} \sum_{k=0}^{n-1} P(g^2)(X_k) - (P g(X_k))^2 \end{aligned}$$

So, according to the law of large numbers that we already proved and applied to the continuous function $P(g^2) - (P g)^2$,

$$\frac{1}{n} \sum_{k=0}^{n-1} \mathbb{E}_x \left[|M_{k+1} - M_k|^2 \middle| X_0, \dots, X_k \right] \rightarrow \sigma^2(f) := \int g^2 - (P g)^2 d\nu \mathbb{P}_x - \text{a.e.}$$

(We used the P -invariance of ν to get that $\int P(g^2) d\nu = \int g^2 d\nu$).

And this proves point 1 since we suppose in it that $\sigma^2(f) \neq 0$.

To conclude, remark that, using the \mathbf{G} -invariance of ν , we can compute

$$\begin{aligned} \int_{\mathbf{G}} \int_{\mathbf{X}} |g(\gamma x) - P g(x)|^2 d\nu(x) d\mu(\gamma) &= \int_{\mathbf{G}} \int_{\mathbf{X}} g(\gamma x)^2 + g(x)^2 - 2P g(x)g(\gamma x) d\nu(x) d\mu(\gamma) \\ &= 2 \int_{\mathbf{X}} g^2 - (P g)^2 d\nu = 2\sigma^2(f) \end{aligned}$$

And so, if $\sigma^2(f) = 0$, then, as g is continuous, we get that for any $\gamma \in \text{supp } \mu$ and any $x \in \mathbb{T}^d$, $g(\gamma x) = Pg(x)$. This proves that for any $n \in \mathbb{N}$, $M_n = 0$ \mathbb{P}_x -a.e. and so, $S_n f(x) = g(X_0) - g(X_n)$. Thus, for any $x \in \mathbb{T}^d$, $S_n f \in L^\infty(\mathbb{P}_x)$ and

$$\sup_{x \in \mathbb{T}^d} \sup_{n \in \mathbb{N}} \|S_n f\|_{L^\infty(\mathbb{P}_x)} \leq 2\|g\|_\infty \leq 2C\|f\|_\alpha$$

This inequality finishes the proof of point 2. \square

2. THE NON-EQUIDISTRIBUTION COMES FROM THE LOWER REGULARITY OF THE MEASURE

Like Bourgain, Furmann, Lindenstrauss and Mozes did for the linear random walk on the torus, we are going to prove in this section that if the measure $\mu^{*n} * \vartheta$ is far from being equidistributed, it is only because of atoms i.e. of points $x \in \mathbb{T}^d$ such that

$$\vartheta(B(x, r)) \geq r^\varepsilon$$

for some $r \in \mathbb{R}_+^*$ depending on n .

More specifically, the aim of this section is to prove the

Theorem 2.1. *Let μ be a borelian probability measure on $\text{SL}_d(\mathbb{Z}) \times \mathbb{T}^d$. Denote by μ_0 the projection of μ on $\text{SL}_d(\mathbb{Z})$ and assume that μ_0 is strongly irreducible, proximal and has an exponential moment. Let $\lambda_1 \in \mathbb{R}_+^*$ be the largest Lyapunov exponent of μ_0 (see appendix A).*

Then for any $\alpha \in]0, 1]$ and any $\varepsilon \in \mathbb{R}_+^$, there is $c_0, \varepsilon' \in \mathbb{R}_+^*$ with $\varepsilon' < \varepsilon$ such that for any $\vartheta \in \mathcal{M}^1(\mathbb{T}^d)$, any $t \in]0, 1]$ and any $n \in \mathbb{N}$ with $n \geq c_0(1 + |\ln t|)$,*

$$\mathcal{W}_\alpha(\mu^{*n} * \vartheta, \nu) \geq t \Rightarrow \vartheta\left(\left\{x \in \mathbb{T}^d \mid \vartheta(B(x, r)) \geq r^\varepsilon\right\}\right) \geq t^{c_0}$$

Where we set

$$r = e^{-(\lambda_1 + \varepsilon')n} \left(\frac{t}{16}\right)^{1/\alpha}$$

In the case of the linear random walk, this statement is a reformulation of an intermediate result (propositions 7.1 and 7.2) of [BFLM11]. We could prove it for the affine random walk just like they do for the linear one that is to say, by studying, for any borelian probability measure ϑ on \mathbb{T}^d , the set of Fourier-coefficients of $\mu^{*n} * \vartheta$ and by remarking that for any $c \in \mathbb{Z}^d$,

$$\begin{aligned} \widehat{\mu^{*n} * \vartheta}(c) &= \int_{\mathbb{T}^d} \int_{\text{SL}_d(\mathbb{Z}) \times \mathbb{T}^d} e^{2i\pi\langle c, ax+b \rangle} d\mu^{*n}(a, b) d\nu(x) \\ &= \int_{\text{SL}_d(\mathbb{Z}) \times \mathbb{T}^d} e^{2i\pi\langle c, b \rangle} \widehat{\vartheta}(tac) d\mu^{*n}(a, b) \end{aligned}$$

And so,

$$\left| \widehat{\mu^{*n} * \vartheta}(c) \right| \leq \int_{\text{SL}_d(\mathbb{Z}) \times \mathbb{T}^d} \left| \widehat{\vartheta}(tac) \right| d\mu^{*n}(a, b) = \int_{\text{SL}_d(\mathbb{Z})} \left| \widehat{\vartheta}(tac) \right| d\mu_0^{*n}(a)$$

Where we recall that we denoted by μ_0 the projection of μ onto $\text{SL}_d(\mathbb{Z})$.

Thus, if $\left| \widehat{\mu^{*n} * \vartheta}(c) \right| \geq t$, then for many a , we also have that $\left| \widehat{\vartheta}(tac) \right| \geq t$ and this is the key remark in the proof of BFLM.

Instead, we are going to see that this result can also be obtained as a corollary of the one of BFLM for the linear walk : at first, we are going to prove that their result gives informations on the spectral radius of the operator P in $L^p(\mathbb{T}^d, \nu)$ (even for the affine random walk) and then, that this implies the theorem.

2.1. Spectral gap in $L^p(\mathbb{T}^d)$. Let \mathbf{G} be a second countable locally compact group acting measurably on a standard borelian space \mathbf{X} endowed with a \mathbf{G} -invariant probability measure ν .

Let μ be a borelian probability measure on \mathbf{G} and P the Markov operator associated to μ . This is the operator defined for any non-negative borelian function f on \mathbf{X} and any $x \in \mathbf{X}$ by

$$Pf(x) = \int_{\mathbf{G}} f(gx) d\mu(g)$$

As ν is a \mathbf{G} -invariant probability measure, it is clear that for any $p \in [1, +\infty]$, $1 \in L^p(\mathbf{X}, \nu)$ and $P1 = 1$. Moreover, we can prove, using Jensen's inequality that $\|P\|_p = 1$. So, we note, for any $p \in [1, +\infty]$,

$$L_0^p(\mathbf{X}, \nu) := \left\{ f \in L^p(\mathbf{X}, \nu) \mid \int f d\nu = 0 \right\}$$

and ρ_p the spectral radius of P in $L_0^p(\mathbf{X}, \nu)$. We say that P has a spectral gap in $L_0^p(\mathbf{X}, \nu)$ (or, by abuse of notations in $L^p(\mathbf{X}, \nu)$) if $\rho_p < 1$.

In the sequel, we will need a more flexible tool than the spectral gap. This is why, for any P -invariant subspace \mathbf{H} of $L^p(\mathbf{X}, \nu)$ endowed with a norm $\|\cdot\|_{\mathbf{H}}$ such that P is continuous on $(\mathbf{H}, \|\cdot\|_{\mathbf{H}})$ and the injection of $(\mathbf{H}, \|\cdot\|_{\mathbf{H}})$ into $(L^p, \|\cdot\|_p)$ is also continuous, we set

$$\kappa(\mu, \mathbf{H}, L^p(\mathbf{X}, \nu)) := -\ln \limsup_{n \rightarrow +\infty} \sup_{f \in \mathbf{H} \setminus \{0\}} \left(\frac{\|P^n f\|_p}{\|f\|_{\mathbf{H}}} \right)^{1/n}$$

Remark 2.2. The sequence $\left(\sup_{f \in \mathbf{H} \setminus \{0\}} \frac{\|P^n f\|_p}{\|f\|_{\mathbf{H}}} \right)$ is not sub-multiplicative in general so it may converge to 0 only at polynomial rate and in this case, we would have that $\kappa(\mu, \mathbf{H}, L^p(\mathbf{X}, \nu)) = 0$. This is impossible if $\mathbf{H} = L^p(\mathbf{X})$ because in this case, if it converges to 0, it has to be at exponential rate.

With this definition, if $(\mathbf{H}, \|\cdot\|_{\mathbf{H}}) = (L^p(\mathbf{X}, \nu), \|\cdot\|_p)$, then $e^{-\kappa(\mu, \mathbf{H}, L^p(\mathbf{X}, \nu))} = \rho_p$ and, for any $(\mathbf{H}, \|\cdot\|_{\mathbf{H}})$, we have, since the inclusion of \mathbf{H} into $L^p(\mathbf{X}, \nu)$ is supposed to be continuous,

$$\kappa(\mu, \mathbf{H}, L^p(\mathbf{X}, \nu)) \geq -\ln \rho_p$$

In particular, when \mathbf{H} is a subset of $L^\infty(\mathbf{X}, \nu)$, we can define and study the function $(p \mapsto \kappa(\mu, \mathbf{H}, L^p(\mathbf{X}, \nu)))$.

Remark 2.3. Remind that, according to Hölder's inequality, for any $1 \leq p \leq p'$ and any function $f \in L^\infty(\mathbf{X}, \nu)$ with $\|f\|_\infty \leq 1$,

$$\|f\|_{p'}^{p'} = \int_{\mathbf{X}} |f|^{p'} d\nu \leq \int_{\mathbf{X}} |f|^p d\nu = \|f\|_p^p \text{ and } \|f\|_p \leq \|f\|_{p'}$$

So, we get that the function $(p \mapsto \kappa(\mu, \mathbf{H}, L^p(\mathbf{X}, \nu)))$ is decreasing whereas the function $(p \mapsto p\kappa(\mu, \mathbf{H}, L^p(\mathbf{X}, \nu)))$ is non-decreasing.

In the same way that we defined $L_0^p(\mathbb{T}^d)$, we set

$$\mathcal{C}_0^{0,\alpha}(\mathbb{T}^d) := \left\{ f \in \mathcal{C}^{0,\alpha}(\mathbb{T}^d) \mid \int f d\nu = 0 \right\}$$

The definition of the function κ is made to get the

Proposition 2.4. *Let μ be a strongly irreducible and proximal probability measure on $\mathrm{SL}_d(\mathbb{Z})$ having an exponential moment.*

Then, for any $\alpha \in]0, 1]$ small enough,

$$\lim_{p \rightarrow +\infty} p \kappa \left(\mu, \mathcal{C}_0^{0,\alpha}(\mathbb{T}^d), L^p(\mathbb{T}^d, \nu) \right) = \lambda_1 d$$

This theorem implies in particular that for any $\varepsilon \in \mathbb{R}_+^*$, there are $p \in \mathbb{N}$ and $C \in \mathbb{R}_+$ such that for any $n \in \mathbb{N}$ and any $f \in \mathcal{C}_0^{0,\alpha}(\mathbb{T}^d)$,

$$\|P^n f\|_{L^p(\mathbb{T}^d)} \leq C e^{-(\lambda_1 d - \varepsilon)n/p} \|f\|_\alpha$$

Proof. First of all, since μ has an exponential moment, for any $\alpha \in]0, 1]$ small enough, any $f \in \mathcal{C}^{0,\alpha}(\mathbb{T}^d)$ and any $x \in \mathbb{T}^d$,

$$|Pf(x)| \leq \|f\|_\infty$$

and for any $y \in \mathbb{T}^d$,

$$\begin{aligned} |Pf(x) - Pf(y)| &\leq \int_{\mathbf{G}} |f(gx) - f(gy)| d\mu(g) \leq \|f\|_\alpha \int_{\mathbf{G}} d(gx, gy)^\alpha d\mu(g) \\ &\leq \|f\|_\alpha d(x, y)^\alpha \int_{\mathbf{G}} \|g\|^\alpha d\mu(g) \end{aligned}$$

So, Pf is α -hölder-continuous and P is a continuous operator on $\mathcal{C}_0^{0,\alpha}(\mathbb{T}^d)$.

According to the result of Bourgain, Furmann, Lindenstrauss and Mozes in [BFLM11] (that we use as stated in proposition 4.5 in [Boy16]), we have that for any $\alpha \in]0, 1]$ and any $\varepsilon \in \mathbb{R}_+^*$, there is a constant C such that for any $n \in \mathbb{N}$, any $t \in]0, 1]$ with $n \geq -C \ln t$ and any $f \in \mathcal{C}_0^{0,\alpha}(\mathbb{T}^d)$ with $\int f d\nu = 0$,

$$\{x \mid |P^n f(x)| \geq t \|f\|_\alpha\} \subset \bigcup_{\substack{\frac{p}{q} \in \mathbb{Q}^d / \mathbb{Z}^d \\ q \leq C t^{-C}}} B\left(\frac{p}{q}, e^{-(\lambda_1 - \varepsilon)n}\right)$$

In particular, for any $L \in \mathbb{N}^*$,

$$\begin{aligned} \int |P^n f|^L d\nu &\leq (t\|f\|_\alpha)^L + \nu(\{x \mid |P^n f(x)| \geq t\|f\|_\alpha\}) \|f\|_\infty^L \\ &\leq \left(t^L + (Ct^{-C})^d e^{-(\lambda_1 - \varepsilon)dn}\right) \|f\|_\alpha^L \end{aligned}$$

And so, taking $t = e^{-\delta n}$ with $\delta \in \mathbb{R}_+^*$ small enough and $L \in \mathbb{N}$ large enough, we find that for some constant C ,

$$\int |P^n f|^L d\nu \leq C e^{-(\lambda_1 - 2\varepsilon)dn} \|f\|_\alpha^L$$

And this proves (reminding that the limit exists according to remark 2.3) that

$$\lim_p p \kappa \left(\mu, C_0^{0,\alpha}(\mathbb{T}^d), L^p(\mathbb{T}^d, \nu) \right) \geq \lambda_1 d$$

We are now going to prove the other inequality. Let $\delta \in]0, 1/4]$, $f \in C^\infty(\mathbb{T}^d)$ such that $f = 1$ on $B(0, \delta)$, $\|f\|_\infty \leq 1$ and $\int f = 0$.

Then, for any $\varepsilon \in \mathbb{R}_+^*$ and any $x \in B(0, e^{-(\lambda_1 + \varepsilon)n}\delta)$, we have that

$$\begin{aligned} P^n f(x) &= \int_{\mathbf{G}} \mathbf{1}_{\|g\| \leq e^{(\lambda_1 + \varepsilon)n}} f(gx) d\mu^{*n}(g) + \int_{\mathbf{G}} \mathbf{1}_{\|g\| \geq e^{(\lambda_1 + \varepsilon)n}} f(gx) d\mu^{*n}(g) \\ &= \mu^{*n} \left(\left\{ g \mid \|g\| \leq e^{(\lambda_1 + \varepsilon)n} \right\} \right) + \int_{\mathbf{G}} \mathbf{1}_{\|g\| \geq e^{(\lambda_1 + \varepsilon)n}} f(gx) d\mu^{*n}(g) \\ &\geq 1 - 2\mu^{*n} \left(\left\{ g \mid \|g\| \geq e^{(\lambda_1 + \varepsilon)n} \right\} \right) \end{aligned}$$

But, according to theorem A.5, there are $C, t \in \mathbb{R}_+^*$ such that

$$\mu^{*n} \left(\left\{ g \mid \|g\| \geq e^{(\lambda_1 + \varepsilon)n} \right\} \right) \leq C e^{-tn}$$

And so, for $n \in \mathbb{N}$ large enough, we have that for any $x \in \mathbb{T}^d$,

$$|P^n f(x)| \geq (1 - 2C e^{-tn}) \mathbf{1}_{B(0, e^{-(\lambda_1 + \varepsilon)n}\delta)}(x)$$

In particular, for any $L \in \mathbb{N}$,

$$\int |P^n f(x)|^L d\nu \geq (1 - 2C e^{-tn})^L \nu(B(0, e^{-(\lambda_1 + \varepsilon)n}\delta)) = (1 - 2C e^{-tn})^L e^{-(\lambda_1 + \varepsilon)dn} \delta^d$$

And this proves that

$$\lim_p p \kappa \left(\mu, C_0^{0,\alpha}(\mathbb{T}^d), L^p(\mathbb{T}^d, \nu) \right) \leq \lambda_1 d$$

And this finishes the proof of the proposition. \square

We are now going to extend the previous result to measures on $\mathrm{SL}_d(\mathbb{Z}) \ltimes \mathbb{T}^d$ by proving the

Corollary 2.5. *Let μ be a borelian probability measure on $\mathbf{G} := \mathrm{SL}_d(\mathbb{Z}) \ltimes \mathbb{T}^d$. Let μ_0 be the projection of μ onto $\mathbf{G}_0 := \mathrm{SL}_d(\mathbb{Z})$ and assume that μ_0 is strongly irreducible, proximal and has an exponential moment.*

Then, for any $\alpha \in]0, 1]$ small enough,

$$\lim_{p \rightarrow +\infty} p \kappa \left(\mu, \mathcal{C}_0^{0,\alpha} \left(\mathbb{T}^d \right), \mathbb{L}^p \left(\mathbb{T}^d, \nu \right) \right) \geq \lambda_1 d$$

Remark 2.6. Theorem 1.4 actually proves that for any measure μ satisfying its assumptions we have that for any $f \in \mathcal{C}^{0,\alpha}(\mathbb{T}^d)$ with $\int f d\nu = 0$, any $n \in \mathbb{N}$ and any $p \in \mathbb{N}^*$,

$$\int |P^n f|^p d\nu \leq C^p e^{-tpn} \|f\|_\alpha^p$$

And so, for any $p \in [1, +\infty[$,

$$\kappa \left(\mu, \mathcal{C}_0^{0,\alpha} \left(\mathbb{T}^d \right), \mathbb{L}^p \left(\mathbb{T}^d, \nu \right) \right) \geq t$$

And, in particular,

$$\lim_{p \rightarrow +\infty} p \kappa \left(\mu, \mathcal{C}_0^{0,\alpha} \left(\mathbb{T}^d \right), \mathbb{L}^p \left(\mathbb{T}^d, \nu \right) \right) = +\infty$$

We are going to prove this result in three steps. First, we are going to prove it for trigonometric functions, then, for regular ones and last, for hölder-continuous functions.

Lemma 2.7. *Let μ be a borelian probability measure on \mathbf{G} and μ_0 its projection on \mathbf{G}_0 . Denote by P the Markov operator associated to μ and by P_0 the one associated to μ_0 .*

Then, for any $c \in \mathbb{Z}^d$, any $n \in \mathbb{N}$ and any $L \in \mathbb{N}$,

$$\int_{\mathbb{T}^d} |P^n e_c|^{2L} d\nu \leq \int_{\mathbb{T}^d} |P_0^n e_c|^{2L} d\nu$$

Where, for $c \in \mathbb{Z}^d$, e_c is the function defined for $x \in \mathbb{T}^d$ by

$$e_c(x) := e^{2i\pi \langle c, x \rangle}$$

Proof. Using Fubini's theorem, we can make the following computation

$$\begin{aligned} \int_{\mathbf{X}} |P_0^n e_c(x)|^{2L} d\nu(x) &= \int_{\mathbf{X}} (P_0^n e_c(x))^L \overline{(P_0^n e_c(x))^L} d\nu(x) \\ &= \int_{\mathbf{X}} \int_{\mathbf{G}^{2L}} e_c(a_1 x) \dots e_c(a_L x) \overline{e_c(a_{L+1} x) \dots e_c(a_{2L} x)} d\mu_0^{*n}(a_1) \dots d\mu_0^{*n}(a_{2L}) d\nu(x) \\ &= \int_{\mathbf{G}^{2L}} \int_{\mathbf{X}} e^{2i\pi \langle c, (a_1 + \dots + a_L - (a_{L+1} + \dots + a_{2L}))x \rangle} d\nu(x) d\mu_0^{*n}(a_1) \dots d\mu_0^{*n}(a_{2L}) \\ &= \int_{\mathbf{G}^{2L}} \mathbf{1}_{\{t(a_1 + \dots + a_L - (a_{L+1} + \dots + a_{2L}))c = 0\}} d\mu_0^{*n}(a_1) \dots d\mu_0^{*n}(a_{2L}) \end{aligned}$$

Doing the same kind of computations for the measure μ , and noting, to simplify notations, for $(a_1, b_1), \dots, (a_{2L}, b_{2L}) \in \text{supp } \mu$, $a_i^j = a_i + \dots + a_j$ and $b_i^j = b_i + \dots + b_j$, we find that

$$\begin{aligned} \int_{\mathbf{X}} |P^n e_c|^{2L} d\nu &= \int_{\mathbf{G}^{2L}} e^{2i\pi \langle c, b_1^L - b_{L+1}^{2L} \rangle} \mathbf{1}_{\{(a_1^L - a_{L+1}^{2L})c = 0\}} d\mu^{*n}(a_1, b_1) \dots d\mu^{*n}(a_{2L}, b_{2L}) \\ &\leq \int_{\mathbf{G}^{2L}} \mathbf{1}_{\{(a_1^L - a_{L+1}^{2L})c = 0\}} d\mu_0^{*n}(g_1) \dots d\mu_0^{*n}(g_{2L}) = \int_{\mathbf{X}} |P_0^n e_c|^{2L} d\nu \end{aligned}$$

Where the last inequality comes from the first part of the proof and precisely gives what we intended to prove. \square

For $s \in \mathbb{R}_+^*$, we denote by $\mathcal{H}^s(\mathbb{T}^d)$ the Sobolev space of exponent s .

Lemma 2.8. *With the same assumptions than in corollary 2.5, for any $s \in \mathbb{R}_+^*$ large enough and any $\varepsilon \in \mathbb{R}_+^*$, there is $L \in \mathbb{R}_+$ such that for any $f \in \mathcal{H}^s(\mathbb{T}^d)$ and any $n \in \mathbb{N}$,*

$$\int \left| P^n f - \int f d\nu \right|^{2L} d\nu \leq C e^{-(\lambda_1 d - \varepsilon)n} \|f\|_{\mathcal{H}^s(\mathbb{T}^d)}^{2L}$$

Proof. Let $f \in \mathcal{H}^s(\mathbb{T}^d)$. Then, by definition, we can expand f in Fourier series : $f = \sum_{c \in \mathbb{Z}^d} \widehat{f}(c) e_c$ with $\|f\|_{\mathcal{H}^s} := \left(\sum_{c \in \mathbb{Z}^d} (1 + \|c\|^2)^{s/2} |\widehat{f}(c)|^2 \right)^{1/2} < +\infty$ and so, for any $L \in \mathbb{N}^*$,

$$\left(\int_{\mathbb{T}^d} |P^n f|^{2L} d\nu \right)^{1/2L} \leq \sum_{c \in \mathbb{Z}^d} |\widehat{f}(c)| \left(\int_{\mathbb{T}^d} |P^n e_c|^{2L} d\nu \right)^{1/2L}$$

Using the previous lemma and proposition 2.4, we get that for any $\varepsilon \in \mathbb{R}_+^*$, there is $L \in \mathbb{R}_+$ such that for any $c \in \mathbb{Z}^d \setminus \{0\}$,

$$\int_{\mathbb{T}^d} |P^n e_c(x)|^{2L} d\nu(x) \leq C e^{-(\lambda_1 d - \varepsilon)n} \|c\|^{2L}$$

Combining this inequality with the previous one, we get that for any $f \in \mathcal{H}^s(\mathbb{T}^d)$ with $\widehat{f}(0) = \int f d\nu = 0$,

$$\left(\int_{\mathbb{T}^d} |P^n f|^{2L} d\nu \right)^{1/2L} \leq C^{1/2L} e^{-(\lambda_1 d - \varepsilon)n/2L} \sum_{c \in \mathbb{Z}^d \setminus \{0\}} |\widehat{f}(c)| \|c\| \leq C' e^{-(\lambda_1 d - \varepsilon)n/2L} \|f\|_{\mathcal{H}^s}$$

For some constant C' depending on d, s, μ, L but non on f . \square

End of the proof of corollary 2.5. According to Jackson-Bernstein's lemma, for any $\alpha \in]0, 1]$ and any $s \in \mathbb{R}_+$ large enough, there is a constant C such that for any $f \in \mathcal{C}^{0,\alpha}(\mathbb{T}^d)$, there is a sequence $(f_m) \in \mathcal{H}^s(\mathbb{T}^d)^{\mathbb{N}}$ such that for any $m \in \mathbb{N}^*$,

$$\int f d\nu = \int f_m d\nu, \quad \|f - f_m\|_{\infty} \leq \frac{C}{m^\alpha} \|f\|_{\alpha} \quad \text{and} \quad \|f_m\|_{\mathcal{H}^s} \leq C m \|f\|_{\alpha}$$

This implies that for any $x \in \mathbb{T}^d$ and any $m, n \in \mathbb{N}^*$,

$$|P^n f_m(x)| \geq |P^n f(x)| - \frac{C}{m^\alpha} \|f\|_{\alpha}$$

Let $\varepsilon \in \mathbb{R}_+^*$, $m \in \mathbb{N}^*$ and $t = \frac{2C}{m^\alpha}$. Then, using the equality $t - C/m^\alpha = t/2$ and lemma 2.8, we get that

$$\begin{aligned} \int |P^n f|^{2L} d\nu &\leq (t\|f\|_\alpha)^{2L} + \nu(\{|P^n f| \geq t\|f\|_\alpha\}) \|f\|_\infty^{2L} \\ &\leq \left(t^{2L} + \nu\left(\left\{|P^n f_m| \geq \left(t - \frac{C}{m^\alpha}\right)\|f\|_\alpha\right\}\right) \right) \|f\|_\alpha^{2L} \\ &\leq \left(t^{2L} + \left(\frac{2}{t\|f\|_\alpha}\right)^{2M} \int |P^n f_m|^{2M} d\nu \right) \|f\|_\alpha^{2L} \\ &\leq \left(t^{2L} + \left(\frac{2}{t\|f\|_\alpha}\right)^{2M} C^{2M} m^{2M} e^{-(\lambda_1 d - \varepsilon)n} \|f\|_\alpha^{2M} \right) \|f\|_\alpha^{2L} \end{aligned}$$

So, for $m = e^{\delta n}$, we get that for some constant C' ,

$$\int |P^n f|^{2L} d\nu \leq C' \left(e^{-\delta\alpha 2Ln} + e^{\delta(1+\alpha)2Mn - (\lambda_1 d - \varepsilon)n} \right) \|f\|_\alpha^{2L}$$

And so, for δ small enough and L large enough, we get that

$$\int |P^n f|^{2L} d\nu \leq C e^{-(\lambda_1 d - 2\varepsilon)n} \|f\|_\alpha^{2L}$$

And this is what we intended to prove. \square

2.2. Equidistribution, lower regularity and spectral gap. In this subsection, we finish the proof of theorem 2.1 by studying the link between equidistribution and the lower regularity of the measure when the spectral gap is large.

Lemma 2.9. *Under the same assumptions as in theorem 2.1, for any $\varepsilon \in \mathbb{R}_+^*$, there are $C, t \in \mathbb{R}_+^*$ such that for any $x, y \in \mathbb{T}^d$, any $f \in \mathcal{C}^{0,\alpha}(\mathbb{T}^d)$ and any $n \in \mathbb{N}$,*

$$|P^n f(x) - P^n f(y)| \leq \left(e^{\alpha(\lambda_1 + \varepsilon)n} d(x, y)^\alpha + C e^{-tn} \right) \|f\|_\alpha$$

Proof. Let's compute, for any $x, y \in \mathbb{T}^d$, $n \in \mathbb{N}$, $f \in \mathcal{C}^{0,\alpha}(\mathbb{T}^d)$ and $\varepsilon \in \mathbb{R}_+^*$,

$$\begin{aligned} |P^n f(x) - P^n f(y)| &= \left| \int_{\mathbf{G}} f(gx) - f(gy) d\mu^{*n}(g) \right| \\ &\leq \int_{\mathbf{G}} \mathbf{1}_{\|g\| \leq e^{(\lambda_1 + \varepsilon)n}} |f(gx) - f(gy)| d\mu^{*n}(g) \\ &\quad + \int_{\mathbf{G}} \mathbf{1}_{\|g\| \geq e^{(\lambda_1 + \varepsilon)n}} |f(gx) - f(gy)| d\mu^{*n}(g) \\ &\leq m_\alpha(f) \int_{\mathbf{G}} \mathbf{1}_{\|g\| \leq e^{(\lambda_1 + \varepsilon)n}} d(gx, gy)^\alpha d\mu^{*n}(g) \\ &\quad + 2\|f\|_\infty \mu^{*n}\left(\left\{g \in \mathbf{G} \mid \|g\| \geq e^{(\lambda_1 + \varepsilon)n}\right\}\right) \\ &\leq \left(d(x, y)^\alpha e^{\alpha(\lambda_1 + \varepsilon)n} + 2\mu^{*n}\left(\left\{g \in \mathbf{G} \mid \|g\| \geq e^{(\lambda_1 + \varepsilon)n}\right\}\right) \right) \|f\|_\alpha \end{aligned}$$

Where we used the fact that for any $x, y \in \mathbb{T}^d$ and any $g \in \mathbf{G}$,

$$d(gx, gy) \leq \|g\| d(x, y)$$

To conclude, we use theorem A.5 and we get that there are $C, t \in \mathbb{R}_+^*$ such that

$$\mu^{*n} \left(\left\{ g \in \mathbf{G} \mid \|g\| \geq e^{(\lambda_1 + \varepsilon)n} \right\} \right) \leq C e^{-tn} \quad \square$$

We are now ready to prove theorem 2.1.

The idea of the proof is that if we have some point x_0 of the torus such that $|P^n f(x_0)| \geq t$, then, on a neighborhood $B(x_0, r)$ for $r \approx e^{-\lambda_1 n}$ we also have that $|P^n f(x)| \approx t$. But, the control on $\kappa(\mu, \mathcal{C}^{0,\alpha}, L^p)$ implies that $\nu(x \mid |P^n f(x)| \geq t) \approx e^{-\lambda_1 d n}$ and so, we have that $\nu(x \mid |P^n f(x)| \geq t) \approx e^{-\lambda_1 d n} \approx \nu(B(x_0, r))$ and this proves that $\{x \mid |P^n f(x)| \geq t\}$ cannot be much bigger than $B(x_0, r)$.

Proof of theorem 2.1. Let $\alpha, t \in]0, 1]$, $\vartheta \in \mathcal{M}^1(\mathbb{T}^d)$ and $n \in \mathbb{N}$. As, for any $0 < \alpha' < \alpha$ the inclusion of $\mathcal{C}^{0,\alpha}(\mathbb{T}^d)$ into $\mathcal{C}^{0,\alpha'}(\mathbb{T}^d)$ is continuous, we may assume without any loss of generality that α is small enough so that corollary 2.5 holds.

Assume that $\mathcal{W}_\alpha(\mu^{*n} * \vartheta, \nu) \geq t$.

By definition, there is $f \in \mathcal{C}^{0,\alpha}(\mathbb{T}^d)$ with $\|f\|_\alpha \leq 1$ and such that

$$\left| \int P^n f d\vartheta - \int f d\nu \right| \geq \frac{t}{2}$$

We can assume without any loss of generality that $\int f d\nu = 0$ and $\|f\|_\alpha \leq 2$. And this proves that

$$\int_{\mathbb{T}^d} |P^n f(x)| d\vartheta(x) \geq \left| \int_{\mathbb{T}^d} P^n f(x) d\vartheta(x) \right| \geq \frac{t}{2}$$

We set, for any $n \in \mathbb{N}$ and $t \in]0, 1]$,

$$X_{n,t} := \left\{ x \in \mathbb{T}^d \mid |P^n f(x)| \geq t \right\}$$

Then, using that $\|P^n f\|_\infty \leq \|f\|_\infty \leq 2$, we find that

$$\frac{t}{2} \leq \int_{\mathbf{X}} |P^n f(x)| d\vartheta(x) \leq \frac{t}{4} + 2\vartheta(X_{n,t/4})$$

And so,

$$\vartheta(X_{n,t/4}) \geq \frac{t}{8}$$

Moreover, according to lemma 2.9, for any $\varepsilon_2 \in \mathbb{R}_+^*$, there are $C, t_0 \in \mathbb{R}_+^*$ such that for any $x \in X_{n,t/4}$ and any $y \in \mathbb{T}^d$, we have that

$$|P^n f(y)| \geq \frac{t}{4} - e^{\alpha(\lambda_1 + \varepsilon_2)n} d(x, y)^\alpha - C e^{-t_0 n} \geq \frac{t}{8} - e^{\alpha(\lambda_1 + \varepsilon_2)n} d(x, y)^\alpha$$

Since we can take c_0 so large that $C e^{-t_0 n} \leq \frac{t}{8}$ for $n \geq c_0(1 + |\ln t|)$.

In particular, noting $r = e^{-(\lambda_1 + \varepsilon_2)n} \left(\frac{t}{16}\right)^{1/\alpha}$, we have that for any $x \in X_{n,t/4}$, $B(x, r) \subset X_{n,t/16}$.

Moreover, according to the classical covering results, there is a constant $C(d)$, depending only on d and points $x_1, \dots, x_N \in \mathbb{T}^d$ such that

$$X_{n,t/4} \subset \bigcup_{i=1}^N B(x_i, r) \subset X_{n,t/16}$$

and the union has multiplicity at most $C(d)$.

This implies in particular that

$$\sum_{i=1}^N \mathbf{1}_{B(x_i, r)} \leq C(d) \mathbf{1}_{X_{n, t/16}}$$

And so, taking the integral against the measure ν and using the equality $\nu(B(x, r)) = r^d$, we get

$$Nr^d \leq C(d) \nu(X_{n, t/16})$$

To sum-up, we found points x_1, \dots, x_N with $N \leq \frac{C(d) \nu(X_{n, t/16})}{r^d}$, such that

$$\vartheta \left(\bigcup_{i=1}^N B(x_i, r) \right) \geq \frac{t}{8}$$

So, noting $\mathcal{I} := \{i \in [1, N] \mid \vartheta(B(x_i, r)) \geq \frac{t}{16N}\}$, we get that

$$\vartheta \left(\bigcup_{i \in \mathcal{I}} B(x_i, r) \right) \geq \frac{t}{16}$$

And finally, for any $x \in \bigcup_{i \in \mathcal{I}} B(x_i, r)$, there is, by definition of \mathcal{I} , some $i \in \mathcal{I}$ such that

$$B(x, 2r) \supset B(x_i, r)$$

And so,

$$\vartheta(B(x, 2r)) \geq \frac{t}{16N}$$

In conclusion, we proved that

$$\vartheta \left(\left\{ x \in \mathbb{T}^d \mid \vartheta(B(x, 2r)) \geq \frac{t}{16N} \right\} \right) \geq \frac{t}{16}$$

To finish, note that we have that

$$N \leq C(d) \frac{\nu(X_{n, t/16})}{r^d} = C(d) \left(\frac{16}{t} \right)^{d/\alpha} e^{(\lambda_1 + \varepsilon_2)dn} \nu(X_{n, t/16})$$

And that, according to Markov's inequality and corollary 2.5, for any $\varepsilon_1 \in \mathbb{R}_+^*$, there are $C, L \in \mathbb{R}_+$ such that

$$\begin{aligned} \nu(X_{n, t/16}) &\leq \left(\frac{16}{t} \right)^{2L} \int_{\mathbf{X}} |P^n f(x)|^{2L} d\nu(x) \leq \left(\frac{16}{t} \right)^{2L} C e^{-(\lambda_1 d - \varepsilon_1)n} \|f\|_{\alpha}^{2L} \\ &\leq \left(\frac{32}{t} \right)^{2L} C e^{-(\lambda_1 d - \varepsilon_1)n} \end{aligned}$$

This proves that for some constant C depending on ε_1, d, μ ,

$$N \leq \frac{C}{t^C} e^{(\varepsilon_1 + \varepsilon_2)d n}$$

And so, taking $\varepsilon_1, \varepsilon_2$ small enough and c_0 large enough, we get that

$$\frac{t}{16N} \geq \frac{t^{C+1}}{C} e^{-(\varepsilon_1 + \varepsilon_2)d n} \geq (2r)^\varepsilon$$

and this is what we intended to prove. \square

3. MEASURE OF POINTS-STABILIZERS

The aim of this section is to prove the following

Proposition 3.1. *with the same assumptions as in theorem 1.4, there are $C, t \in \mathbb{R}_+^*$ such that for any $x \in \mathbb{T}^d$ and any $n \in \mathbb{N}$,*

$$\mu^{*n} \otimes \mu^{*n} (\{g_1, g_2 \in \mathbf{G} | g_1 x = g_2 x\}) \leq C e^{-tn}$$

This proposition will be a direct corollary of lemmas 3.2 and 3.3 since if μ is not concentrated on $\mathrm{SL}_d(\mathbb{Z}) \times \mathbb{Q}^d$, then the measure μ_1 of lemma 3.2 is not concentrated on $\mathrm{SL}_d(\mathbb{R}) \times \{0\}$.

To evaluate the measure of the stabilizer of a point, we are going to lift the situation from \mathbb{T}^d to \mathbb{R}^d since we know better the products of random elements of $\mathrm{SL}_d(\mathbb{R}) \times \mathbb{R}^d$ (through the theory of products of random matrices since this group can be identified to a subgroup of $\mathrm{SL}_{d+1}(\mathbb{R})$) than those of elements of $\mathrm{SL}_d(\mathbb{Z}) \times \mathbb{T}^d$.

To understand what we are going to do, remark that if $\mu = \frac{1}{2}\delta_{(g_1, v_1)} + \frac{1}{2}\delta_{(g_2, v_2)}$ with $g_1, g_2 \in \mathrm{SL}_d(\mathbb{Z})$, $v_1 \in \mathbb{Q}^d/\mathbb{Z}^d$ and $v_2 \in \mathbb{T}^d$ such that the coefficients of v_2 and 1 are \mathbb{Q} -linearly independent, then, for μ^{*n} -a.e. $(g, v) \in \mathrm{SL}_d(\mathbb{Z}) \times \mathbb{T}^d$, we can write

$$v = M_1 v_1 + M_2 v_2$$

with $M_i \in \mathcal{M}_d(\mathbb{Z})$.

So, in particular, noting \vec{v}_1, \vec{v}_2 some representatives of v_1, v_2 in \mathbb{R}^d , we get that if $v = 0$ in \mathbb{T}^d , then there is $p \in \mathbb{Z}^d$, such that,

$$M_1 \vec{v}_1 + M_2 \vec{v}_2 = p$$

As we assumed that the coefficients of v_2 and 1 are \mathbb{Q} -linearly independent and that $v_1 \in \mathbb{Q}^d$, we get that $M_2 \vec{v}_2 = 0$ and $M_1 \vec{v}_1 = p$.

So, we set

$$\mu_1 = \frac{1}{2}\delta_{(g_1, 0)} + \frac{1}{2}\delta_{(g_2, \vec{v}_2)} \in \mathcal{M}^1(\mathrm{SL}_d(\mathbb{R}) \times \mathbb{R}^d)$$

and what we just proved is that

$$\mu^{*n}(\mathrm{SL}_d(\mathbb{Z}) \times \{0\}) \leq \mu_1^{*n}(\mathrm{SL}_d(\mathbb{R}) \times \{0\})$$

And so we are left with a problem on probability measures on $\mathrm{SL}_d(\mathbb{R}) \times \mathbb{R}^d$.

Thus, to lift the situation from \mathbb{T}^d to \mathbb{R}^d , we are going to project the translation part of elements in the support of μ onto a complementary subspace of \mathbb{Q}^d in the \mathbb{Q} -vector space \mathbb{R}^d . To do so, we fix some \mathbb{Q} -linear projection $\pi_{\mathbb{Q}} : \mathbb{R}^d \rightarrow \mathbb{R}^d$ onto \mathbb{Q}^d and we remark that for any $v \in \mathbb{R}^d/\mathbb{Z}^d$, $v - \pi_{\mathbb{Q}} v \in \mathbb{R}^d$ is well defined and the application $\mathrm{SL}_d(\mathbb{Z}) \times \mathbb{T}^d \ni (g, v) \mapsto (g, v - \pi_{\mathbb{Q}} v) \in \mathrm{SL}_d(\mathbb{Z}) \times \mathbb{R}^d$ is a group-morphism.

Now, we can prove the following

Lemma 3.2. *Let μ be a borelian probability measure on $\mathrm{SL}_d(\mathbb{Z}) \times \mathbb{T}^d$.*

Then, for any $n \in \mathbb{N}$ and any $y \in \mathbb{T}^d$,

$$\mu^{*n} \otimes \mu^{*n} (\{(g_1, g_2) | g_2^{-1} g_1 \in \mathrm{Stab}(y)\}) \leq \mu_1^{*n} \otimes \mu_1^{*n} (\{(g_1, g_2) | g_2^{-1} g_1 \in \mathrm{Stab}(y - \pi_{\mathbb{Q}} y)\})$$

where μ_1 is the measure on $\mathrm{SL}_d(\mathbb{Z}) \times \mathbb{R}^d$ defined by $\mu_1(A) = \mu(\varphi^{-1}(A))$ where $\varphi : \mathrm{SL}_d(\mathbb{Z}) \times \mathbb{T}^d \rightarrow \mathrm{SL}_d(\mathbb{Z}) \times \mathbb{R}^d$ is the function defined by

$$\varphi(g, v) = (g, v - \pi_{\mathbb{Q}}v)$$

and $\pi_{\mathbb{Q}}$ is some \mathbb{Q} -linear projection onto \mathbb{Q}^d .

Proof. As φ is a morphism, we only need to prove that for any $g \in \mathrm{SL}_d(\mathbb{Z}) \times \mathbb{T}^d$ and any $y \in \mathbb{T}^d$, if $gy = y$ then $\varphi(g)(y - \pi_{\mathbb{Q}}y) = (y - \pi_{\mathbb{Q}}y)$.

Write $g = (a, b)$ with $a \in \mathrm{SL}_d(\mathbb{Z})$ and $b \in \mathbb{T}^d$. Then, $\varphi(g) = (a, b - \pi_{\mathbb{Q}}b)$. So,

$$\varphi(g)(y - \pi_{\mathbb{Q}}y) = a(y - \pi_{\mathbb{Q}}y) + b - \pi_{\mathbb{Q}}b$$

But, $gy = y$, so, noting \vec{b}, \vec{y} some representatives of b, y , we get that there is $p \in \mathbb{Z}^d$ such that

$$a\vec{y} + \vec{b} = \vec{y} + p$$

Projecting onto \mathbb{Q}^d , we also get that

$$a\pi_{\mathbb{Q}}\vec{y} + \pi_{\mathbb{Q}}\vec{b} = \pi_{\mathbb{Q}}\vec{y} + p$$

And this proves that

$$a(I_d - \pi_{\mathbb{Q}})\vec{y} + (I_d - \pi_{\mathbb{Q}})\vec{b} = (I_d - \pi_{\mathbb{Q}})\vec{y}$$

Finally, as $(I_d - \pi_{\mathbb{Q}})\vec{y}$ and $(I_d - \pi_{\mathbb{Q}})\vec{b}$ don't depend on the choices of the representatives of y and b , this finishes the proof of the fact that

$$a(y - \pi_{\mathbb{Q}}y) + b - \pi_{\mathbb{Q}}b = y - \pi_{\mathbb{Q}}y$$

and this finishes the proof of the lemma. \square

Lemma 3.3. *Let μ be a borelian probability measure on $\mathrm{SL}_d(\mathbb{R}) \times \mathbb{R}^d$ that is not concentrated on $\mathrm{SL}_d(\mathbb{R}) \times \{0\}$ and has an exponential moment. Let μ_0 be the projection of μ onto $\mathrm{SL}_d(\mathbb{R})$ and assume that μ_0 is strongly irreducible and proximal.*

Then, there are $C, t \in \mathbb{R}_+^$ such that for any $x \in \mathbb{R}^d$ and any $n \in \mathbb{N}$,*

$$\mu^{*n} \otimes \mu^{*n} (\{(g_1, g_2) | g_1x = g_2x\}) \leq Ce^{-tn}$$

Proof. We denote by $\tilde{\mu}$ the measure on $\mathrm{SL}_d(\mathbb{R}) \times \mathbb{R}^d$ defined by $\tilde{\mu}(A) = \mu(A^{-1})$ for any borelian subset A of $\mathrm{SL}_d(\mathbb{R}) \times \mathbb{R}^d$ and where $A^{-1} := \{g^{-1} | g \in A\}$.

Let $\lambda_1 \geq \dots \geq \lambda_d$ be the Lyapunov exponents of μ_0 (see appendix A).

Then, the largest Lyapunov exponent of $\tilde{\mu}$ is $-\lambda_d$. Moreover, as $\lambda_1 \geq \dots \geq \lambda_d$, $\lambda_1 > 0$ and $\lambda_1 + \dots + \lambda_d = 0$, we have that $\lambda_d < 0$ and so, $-\lambda_d > 0$.

Let $n \in \mathbb{N}$, $\varepsilon \in \mathbb{R}_+^*$ and $x \in \mathbb{R}^d$. We can compute,

$$\begin{aligned} I_n(x) &:= \mu^{*n} \otimes \mu^{*n} (\{g_1, g_2 \in \mathbf{G} | g_1x = g_2x\}) = \mu^{*n} \otimes \tilde{\mu}^{*n} (\{(g_1, g_2) \in \mathbf{G}^2 | g_2g_1x = x\}) \\ &\leq \mu^{*n} \otimes \tilde{\mu}^{*n} \left(\left\{ (g_1, g_2) \left| \frac{1 + \|g_2^{-1}g_1x\|}{1 + \|x\|} \leq e^{(\lambda_1 - \lambda_d - \varepsilon)n} \right. \right\} \right) \end{aligned}$$

But

$$\frac{1 + \|g_2g_1x\|}{1 + \|x\|} = \frac{1 + \|g_2g_1x\|}{1 + \|g_1x\|} \frac{1 + \|g_1x\|}{1 + \|x\|}$$

So, we obtain that

$$I_n(x) \leq \mu^{*n} \left(\left\{ g_1 \left| \frac{1 + \|g_1 x\|}{1 + \|x\|} \leq e^{(\lambda_1 - \varepsilon/2)n} \right. \right\} \right) \\ + \int_{\mathbf{G}} \tilde{\mu}^{*n} \left(\left\{ g_2 \left| \frac{1 + \|g_2 g_1 x\|}{1 + \|g_1 x\|} \leq e^{(-\lambda_d - \varepsilon/2)n} \right. \right\} \right) d\mu^{*n}(g_1)$$

And we can conclude with corollary A.9 applied to the measures μ and $\tilde{\mu}$. \square

4. EFFECTIVE SHADOWING LEMMAS

The aim of this section is to prove a criterion to produce measures satisfying an effective shadowing lemma.

First of all, we recall the

Definition 4.1. Let μ be a borelian probability measure on \mathbf{G} .

We say that μ satisfies an effective shadowing lemma if for ant $C', t' \in \mathbb{R}_+^*$, there are $C_1, C_2, M, t, L \in \mathbb{R}_+^*$ such that for any $x, y \in \mathbb{T}^d$, any $r \in \mathbb{R}_+^*$ and any $n \in \mathbb{N}$ with $r \leq C_1 e^{-Ln}$, if

$$\mu^{*n}(\{g \in \mathbf{G} | d(gx, y) \leq r\}) \geq C_2 e^{-tn}$$

then there are $x', y' \in \mathbb{T}^d$ such that $d(x, x'), d(y, y') \leq r e^{Mn}$ and

$$\mu^{*n}(\{g \in \mathbf{G} | gx' = y'\}) \geq C' e^{-t'n}$$

The criterion that we are going to prove will use the diophantine properties of the translation parts of the elements in $\text{supp } \mu$. More specifically, we want a condition that ensures that if $(g_1, v_1), (g_2, v_2) \in \text{supp } \mu^{*n}$ are such that v_1 and v_2 are close (in some sense) then $v_1 = v_2$. This is why we make the following

Definition 4.2 (Diophantine subsets of \mathbb{T}^d). Let $d \in \mathbb{N}^*$ and $B \subset \mathbb{T}^d$ a finite subset.

We say that B is (C, L) -diophantine if for any non zero $(M_b) \in \mathbb{Z}^B$,

$$d \left(\sum_{b \in B} M_b b, 0 \right) \leq \frac{C}{\max_b |M_b|^L} \Rightarrow \sum_b M_b b = 0$$

More generally, we say that B is diophantine if it is (C, L) -diophantine for some $C, L \in \mathbb{R}_+^*$.

Remark 4.3. With this definition, a diophantine subset can contain rational points.

Example 4.4. Let $b \in \mathbb{T}^1 \setminus \mathbb{Q}/\mathbb{Z}$. Asking $\{b\}$ to be diophantine is asking for $C, L \in \mathbb{R}_+^*$ such that for any $q \in \mathbb{N}^*$,

$$d(qb, 0) > \frac{C}{q^L}$$

The name comes from this property.

Remark 4.5. Let $d \geq 2$ and B a subset of \mathbb{T}^d . It is not the same thing to say that B is diophantine and that $\{\text{coefficients of } b | b \in B\}$ is a diophantine subset of \mathbb{T}^1 (consider $B = \{(b_1, b_2)\}$ with b_1 diophantine and b_2 not). This last property is stronger but this is the one that we will need in the sequel and we refer to lemma 4.8 for more details.

Example 4.6. Let $N \in \mathbb{N}^*$. Then, for a.e. $b_1, \dots, b_N \in \mathbb{T}^1$, the set $\{b_1, \dots, b_N\}$ is diophantine.

We are now ready to state the main result of this section

Proposition 4.7. *Let μ be a borelian probability measure on $\mathrm{SL}_d(\mathbb{Z}) \times \mathbb{T}^d$ and let μ_0 be its projection on $\mathrm{SL}_d(\mathbb{Z})$. Assume that μ_0 is strongly irreducible, proximal and that it has an exponential moment and that $\{\text{coefficients of } b \mid (a, b) \in \text{supp } \mu\}$ is a diophantine subset of \mathbb{T}^1 .*

Then, μ satisfies an effective shadowing lemma.

To prove this proposition, we first come back to the difference for a subset B of \mathbb{T}^d between being diophantine and having elements whose coefficients form a diophantine subset of \mathbb{T}^1 .

Lemma 4.8. *Let B be a finite subset of \mathbb{T}^d and*

$$F := \{\text{coefficients of } B\} \subset \mathbb{T}^1$$

Then, F is (C, L) -diophantine if and only if there is $C' \in \mathbb{R}_+^$ such that for any non zero $(M_b) \in \mathcal{M}_d(\mathbb{Z})^B$,*

$$d\left(\sum_{b \in B} M_b b, 0\right) \leq \frac{C'}{(\max_b \|M_b\|)^L} \Rightarrow \sum_b M_b b = 0$$

Proof. First, assume that F is (C, L) -diophantine and set $C' = C/(d|B|)^L$.

Let $0 \neq (M_b) \in \mathcal{M}_d(\mathbb{Z})^B$ be such that

$$d\left(\sum_{b \in B} M_b b, 0\right) \leq \frac{C'}{(\max_b \|M_b\|)^L}$$

Each coefficient of $\sum_b M_b b$ is a sum of elements of F multiplied by integers that are smaller than $d|B| \max_b \|M_b\|$. In other words, for any coefficient of $\sum_b M_b b$, we get a sum $\sum_{f \in F} L_f f$ with $|L_f| \leq d|B| \max_b \|M_b\|$ and

$$d\left(\sum_f L_f f, 0\right) \leq \frac{C'}{\max_b \|M_b\|^L} \leq \frac{C'(d|B|)^L}{\max_f |L_f|^L} = \frac{C}{(\max_f |L_f|)^L}$$

And as F is (C, L) -diophantine, this implies that $\sum_f L_f f = 0$ and so, as this is true for any coefficient of $\sum_b M_b b$, we get that $\sum_b M_b b = 0$.

Reciprocally, if there is $C' \in \mathbb{R}_+^*$ such that for any $0 \neq (M_b) \in \mathcal{M}_d(\mathbb{Z})^B$

$$d\left(\sum_{b \in B} M_b b, 0\right) \leq \frac{C'}{(\max_b \|M_b\|)^L} \Rightarrow \sum_b M_b b = 0$$

Then, we set $C = C'/d^L$ and let $0 \neq (L_f) \in \mathbb{Z}^F$ be such that

$$d\left(\sum_{f \in F} L_f f, 0\right) \leq \frac{C}{(\max_f |L_f|)^L}$$

For any element f of F , choose an element $(b(f), i(f))$ in

$$\{(b, i) \in B \times [1, d] \mid f \text{ is the } i\text{-th coefficient of } b\}$$

Now, for any $b \in B$, we denote by M_b the matrix where we set L_f in the i -th column if there is $f \in F$ such that $(b(f), i(f)) = (b, i)$ and 0 otherwise.

Thus, by definition,

$$\sum_{b \in B} M_b b = \begin{pmatrix} \sum_f L_f f \\ \vdots \\ \sum_f L_f f \end{pmatrix}$$

And $\max_b \|M_b\| \leq d \max_f |L_f|$ so

$$d \left(\sum_b M_b b, 0 \right) \leq \frac{C}{(\max_f |L_f|)^L} \leq \frac{C'}{(\max_b \|M_b\|)^L}$$

And this proves, as B is (C, L) -diophantine, that $\sum_b M_b b = 0$ and so we also get that $\sum_f L_f f = 0$ and this finishes the proof of the lemma. \square

From now on, we set

$$(4.1) \quad B(\mu) := \{b \mid (a, b) \in \text{supp } \mu\} \text{ and } F(\mu) := \{\text{coefficients of } b \mid b \in B(\mu)\}$$

To prove proposition 4.7, we are going to use some control of the translation parts of elements of $\text{supp } \mu^{*n}$. To do so, for any $Q \in \mathbb{N}^*$ and any finite subset B of \mathbb{T}^d , we set

$$X_Q(B) = \left\{ \frac{p + \sum_{b \in B} M_b b}{q} \mid p \in \mathbb{Z}^d, q \in \mathbb{Z}, |q| \leq Q, (M_b) \in \mathcal{M}_d(\mathbb{Z})^B, \max_{b \in B} \|M_b\| \leq Q \right\}$$

Thus some $x \in \mathbb{T}^d$ belongs to $X_Q(B)$ if there is $q \in \mathbb{N}^*$ with $q \leq Q$ such that each coefficient of qx can be obtained from translations by coefficients of elements of B with multiplicities smaller than Q .

This definition is made so that for any M large enough we have that for any $n \in \mathbb{N}^*$, with large probability, any element $(g, v) \in \text{supp } \mu^{*n}$ is such that $v \in X_{e^{Mn}}(B(\mu))$.

To make this idea more precise, we set, for any $M \in \mathbb{R}_+^*$ and $n \in \mathbb{N}$,

$$\mathbf{G}_n^M := \left\{ (a_i) \in \mathbf{G}_0^n \mid \max_{k \in [1, n]} \max_{1 \leq i_1 < \dots < i_k \leq n} \|a_{i_k} \dots a_{i_1}\| \leq e^{Mn} \right\}$$

The aim of the following lemma is to prove that elements of \mathbf{G}_n^M are generic.

Lemma 4.9. *Let μ be a borelian probability measure on \mathbf{G} and let μ_0 be the image of μ on $\text{SL}_d(\mathbb{Z})$. Assume that μ_0 has an exponential moment.*

Then, for any $M \in \mathbb{R}_+^$ large enough, there is $t \in \mathbb{R}_+^*$ such that for any $n \in \mathbb{N}$,*

$$\mu_0^{\otimes n}(\mathbf{G}_n^M) \geq 1 - e^{-tn}$$

Moreover, if $B(\mu)$ is finite (see equation (4.1)), then, for any $(a_1, b_1), \dots, (a_n, b_n) \in \text{supp } \mu$ such that $(a_i) \in \mathbf{G}_n^M$,

$$\sum_{k=1}^n a_n \dots a_{k+1} b_k \in X_{e^{(M+1)n}}(B(\mu))$$

Proof. First, remark that as μ_0 is concentrated on $\mathrm{SL}_d(\mathbb{Z})$, for μ_0 -a.e. $g \in \mathbf{G}_0$, $\|g\| \geq 1$ and so, noting $\delta \in \mathbb{R}_+^*$ such that $\int_{\mathbf{G}_0} \|g\|^\delta d\mu_0(g) < +\infty$, we have that for any $M \in \mathbb{R}_+^*$ and any $n \in \mathbb{N}$,

$$\begin{aligned} \mu_0^{\otimes n}(\mathbf{G}_n^M) &:= \mu_0^{\otimes n} \left(\left\{ (g_i) \in \mathbf{G}_0^{\mathbb{N}} \left| \max_{k \in [1, n]} \max_{1 \leq i_1 < \dots < i_k \leq n} \|g_{i_k} \dots g_{i_1}\| \geq e^{Mn} \right. \right\} \right) \\ &\leq \mu_0^{\otimes n} \left(\left\{ (g_i) \in \mathbf{G}_0^{\mathbb{N}} \left| \|g_n\| \dots \|g_1\| \geq e^{Mn} \right. \right\} \right) \\ &\leq e^{-\delta M n} \left(\int_{\mathbf{G}_0} \|g\|^\delta d\mu_0(g) \right)^n \end{aligned}$$

And this finishes the proof of the first part of the lemma.

To prove the second one, take $(a_1, b_1), \dots, (a_n, b_n) \in \mathrm{supp} \mu$ such that $(a_i) \in \mathbf{G}_n^M$.

Then, we can write

$$\sum_{k=1}^n a_n \dots a_{k+1} b_k = \sum_{b' \in B(\mu)} \left(\sum_{k=1}^n \mathbf{1}_{b_k = b'} a_n \dots a_k \right) b'$$

and, for any $b' \in B(\mu)$,

$$\left\| \sum_{k=1}^n \mathbf{1}_{b_k = b'} a_n \dots a_k \right\| \leq n e^{Mn}$$

This proves that $\sum_{k=1}^n a_n \dots a_{k+1} b_k \in X_{n e^{Mn}}(B(\mu))$. \square

In the sequel, we will have to control sums of the form $\sum c_i a_i$ where the a_i are μ^{*n} -generic and $c_i \in \mathbb{Z}$. To do so, we will use the

Lemma 4.10 ([BFLM11]). *Let μ_0 be a strongly irreducible and proximal borelian probability measure on $\mathrm{SL}_d(\mathbb{Z})$ having an exponential moment.*

Set

$$\mathbf{G}_0^1 := \left\{ a \in \mathbf{G}_0 \left| \left| \frac{1}{n} \ln \|a\| - \lambda_1 \right| \leq \varepsilon \right. \right\}$$

and

$$\mathbf{G}_0^d := \left\{ (a_i) \in \mathbf{G}_0^d \left| \forall i \in [1, d], a_i \in \mathbf{G}_0^1 \text{ and } \det \left(\sum_i c_i a_i \right) \neq 0 \right. \right\}$$

where we put $c_1 = 1 - d$ and $c_i = 1$ for $i \in [2, d]$.

Then, for any $\varepsilon \in \mathbb{R}_+^*$, there are $C, t \in \mathbb{R}_+^*$ such that for any $n \in \mathbb{N}$,

$$\mu^{*n}(\mathbf{G}_0^1) \geq 1 - C e^{-tn} \text{ et } \mu^{*n} \otimes \dots \otimes \mu^{*n}(\mathbf{G}_0^d) \geq 1 - C e^{-tn}$$

Proof. In [BFLM11], this lemma is not stated as we do it here but it corresponds to the lemmas 4.3, 4.6 and 7.9 and to some part of the proof of proposition 7.3. \square

We are now ready to prove proposition 4.7. The proof consists in two lemmas. In lemma 4.11, we study points that are far from points of $X_{e^n}(B(\mu))$ and in lemma 4.12 we study points that are close to it.

Lemma 4.11. *With the assumptions of proposition 4.7, for any $M \in \mathbb{R}_+^*$ large enough there are $C, t \in \mathbb{R}_+^*$ such that for any $r \in]0, 1]$, any $n \in \mathbb{N}$, any $x, y \in \mathbb{T}^d$, if*

$$\mu^{*n}(\{g \in \mathbf{G} \mid d(gx, y) \leq r\}) \geq Ce^{-tn}$$

then there is $x' \in X_{e^{Mn}}(B(\mu))$ such that

$$d(x, x') \leq re^{Mn}$$

Proof. The idea that makes the demonstration work is that if $a_1x + b_1, \dots, a_dx + b_d$ are close to each-others, then setting $c_1 = 1 - d$ and $c_i = 1$ for $i \in [2, d]$, we get that $\sum_i c_i a_i x$ is close to $\sum_i c_i b_i$. But, according to lemma 4.10, with large probability, the matrix $\sum_i c_i a_i$ is invertible and, according to lemma 4.9, the b_i belong to $X_{e^{Mn}}(B(\mu))$, and so $x \in X_{e^{Mn}}(B(\mu))$.

We keep the notations \mathbf{G}_0^1 and \mathbf{G}_0^d from lemma 4.10 and the notation \mathbf{G}_n^M from lemma 4.9. Then, for any $\varepsilon \in \mathbb{R}_+^*$ and any large enough M we denote by C, t the constants given by lemma 4.10 and by t_0 the one given by lemma 4.9.

Then, we set

$$\mathbf{G}_* := \left\{ ((a_1, b_1), \dots, (a_d, b_d)) \in \mathbf{G}^d \mid (a_i) \in \mathbf{G}_0^d \text{ and for any } i, b_i \in X_{e^{(M+1)n}}(B(\mu)) \right\}$$

By definition, we have that

$$\mu^{*n} \otimes \dots \otimes \mu^{*n}(\mathbf{G}_*) \leq Ce^{-tn} + de^{-t_0n}$$

So, we can compute, for any $x, y \in \mathbb{T}^d$,

$$\begin{aligned} I_n(x, y) &:= (\mu^{*n}(\{g \in \mathbf{G} \mid d(gx, y) \leq r\}))^d \\ &= \int_{\mathbf{G}^d} \mathbf{1}_{B(y, r)}(a_1x + b_1) \dots \mathbf{1}_{B(y, r)}(a_dx + b_d) d\mu^{*n}(a_1, b_1) \dots d\mu^{*n}(a_d, b_d) \\ &\leq Ce^{-tn} + de^{-t_0n} + \int_{\mathbf{G}_*} \prod_{i=1}^d \mathbf{1}_{B(y, r)}(a_ix + b_i) d\mu^{*n}(a_1, b_1) \dots d\mu^{*n}(a_d, b_d) \end{aligned}$$

Thus, if M is large enough, we can find $C, t \in \mathbb{R}_+^*$ such that for any $r \in]0, 1]$, any $n \in \mathbb{N}$, if

$$\mu^{*n}(\{g \in \mathbf{G} \mid d(gx, y) \leq r\}) \geq Ce^{-tn}$$

then

$$\int_{\mathbf{G}_*} \prod_{i=1}^d \mathbf{1}_{B(y, r)}(a_ix + b_i) d\mu^{*n}(a_1, b_1) \dots d\mu^{*n}(a_d, b_d) > 0$$

In particular, there is $((a_1, b_1), \dots, (a_d, b_d)) \in \mathbf{G}_*$ such that for any i ,

$$d(a_ix + b_i, y) \leq r$$

Now, we let $\vec{x}, \vec{y}, \vec{b}_i$ be representatives of x, y, b_i in \mathbb{R}^d . We have that for any $i \in [1, d]$ there is $p_i \in \mathbb{Z}^d$ such that

$$\|a_i \vec{x} + \vec{b}_i - \vec{y} - p_i\| \leq r$$

So, noting $c_1 = 1 - d$ and $c_i = 1$ for $i \neq 1$, we get that

$$\left\| \left(\sum_i c_i a_i \right) x + \sum_i c_i b_i - \sum_i c_i p_i \right\| \leq 2dr$$

But, by definition of \mathbf{G}_0^d , $\det(\sum_i c_i a_i) \in \mathbb{Z}^*$.

So,

$$1 \leq \left| \det \left(\sum_i c_i a_i \right) \right| \leq \left\| \sum_i c_i a_i \right\|^d \leq d^{2d} e^{(\lambda_1 + \varepsilon)dn}$$

Let $U = \sum_i c_i a_i$. Then U is invertible and we can write,

$$U^{-1} = \frac{1}{\det U} V$$

with $V \in \mathcal{M}_d(\mathbb{Z})$ and for some constant $C(d)$ depending only on d , $\|V\| \leq C(d)\|U\|^{d-1}$.

Thus, we get that

$$\|x + U^{-1} \sum_i c_i b_i - U^{-1} \sum_i c_i p_i\| \leq 2dr\|U\|$$

To conclude, we only need to remark that we can write

$$b_i = \sum_{b \in B(\mu)} M_g^i b \text{ with } \max_b \|M_b^i\| \leq e^{(M+1)n}$$

And this proves that

$$-U^{-1} \sum_i c_i b_i + U^{-1} \sum_i c_i p_i = \frac{\sum_i c_i V p_i}{\det(U)} + \frac{\sum_{b \in B(\mu)} (\sum_i c_i V M_b^i) b}{\det(U)}$$

And that

$$\max_{b \in B(\mu)} \left\| \sum_i c_i V M_b^i \right\| \leq 2d\|V\| \max_b \|M_b^i\| \leq 2dC(d)e^{(M+1)n} e^{(\lambda_1 + \varepsilon)(d-1)n}$$

So, maybe for some $M' \geq M$ we get that

$$x' := -U^{-1} \sum_i c_i b_i + U^{-1} \sum_i c_i p_i \in X_{e^{M'n}}(\text{supp } \mu)$$

and $d(x, x') \leq r e^{M'n}$. □

Lemma 4.12. *With the same assumptions as in proposition 4.7, there are C_0, L such that for any $M \in \mathbb{R}_+$ large enough, there are $C, t \in \mathbb{R}_+$ such that for any $n \in \mathbb{N}^*$, any $r \in]0, 1]$ with*

$$r \leq \frac{C_0}{e^{MLn}}$$

we have that for any $y \in \mathbb{T}^d$, any $x' \in X_{e^{(M+1)n}}(B(\mu))$ and any $x \in \mathbb{T}^d$ with $d(x, x') \leq r$,

$$(\mu^{*n}(\{g \in \mathbf{G} | d(gx, y) \leq r\}))^2 \leq C e^{-tn} + \mu^{*n} \otimes \mu^{*n}(\{g_1, g_2 | g_1 x' = g_2 x'\})$$

Proof. To simplify our notations, we set $B = B(\mu)$ and $F = F(\mu)$. let $x, x', y \in \mathbb{T}^d$ as in the proposition. By definition of $X_Q(B)$, there is $(M_v) \in \mathcal{M}_d(\mathbb{Z})^B$ with $\max \|M_v\| \leq Q$, there is $p \in \mathbb{Z}^d$ and $q \in \mathbb{N}^*$ with $|q| \leq Q$ such that

$$x' = \frac{p + \sum_{b \in B} M_b b}{q}$$

Let, for any $\varepsilon \in \mathbb{R}_+^*$ and $M \in \mathbb{N}$,

$$\mathbf{G}_* := \left\{ (a, b) \in \mathbf{G} \mid \|a\| \leq e^{(\lambda_1 + \varepsilon)n} \text{ et } b \in X_{e^{(M+1)n}}(B) \right\}$$

Lemmas 4.10 and 4.9 prove that for any $\varepsilon \in \mathbb{R}_+^*$ and any $M \in \mathbb{R}_+$ large enough, there are $C, t \in \mathbb{R}_+^*$ such that for any $n \in \mathbb{N}$,

$$\mu^{*n}(\mathbf{G}_*) \geq 1 - Ce^{-tn}$$

Let's compute

$$\begin{aligned} I_n(x, y) &:= (\mu^{*n}(\{g \in \mathbf{G} \mid d(gx, y) \leq r\}))^2 \\ &= \int_{\mathbf{G}^2} \mathbf{1}_{B(y, r)}(g_1x) \mathbf{1}_{B(y, r)}(g_2x) d\mu^{*n}(g_1) d\mu^{*n}(g_2) \\ &\leq 2\mu^{*n}(\mathbf{G}_*) + \int_{\mathbf{G}^2} \mathbf{1}_{\mathbf{G}_*}(g_1) \mathbf{1}_{\mathbf{G}_*}(g_2) \mathbf{1}_{d(g_1x, g_2x) \leq 2r} d\mu^{*n}(g_1) d\mu^{*n}(g_2) \\ &\leq 2Ce^{-tn} + \int_{\mathbf{G}^2} \mathbf{1}_{\mathbf{G}_*}(g_1) \mathbf{1}_{\mathbf{G}_*}(g_2) \mathbf{1}_{d(g_1x, g_2x) \leq 2r} d\mu^{*n}(g_1) d\mu^{*n}(g_2) \end{aligned}$$

Moreover, for $g_1 = (a_1, b_1)$ and $g_2 = (a_2, b_2)$, we have that

$$d(g_1x', g_2x') \leq d(g_1x', g_1x) + d(g_1x, g_2x) + d(g_2x, g_2x') \leq \|a_1\|r + d(g_1x, g_2x) + \|a_2\|r$$

And this proves that

$$I_n(x, y) \leq 2Ce^{-tn} + \int_{\mathbf{G}^2} \mathbf{1}_{\mathbf{G}_*}(g_1) \mathbf{1}_{\mathbf{G}_*}(g_2) \mathbf{1}_{d(g_1x', g_2x') \leq 3re^{(\lambda_1 + \varepsilon)n}} d\mu^{*n}(g_1) d\mu^{*n}(g_2)$$

To conclude, we only need to prove that, under the diophantine condition, if $x' \in X_{e^{(M+1)n}}$, $g_1, g_2 \in \mathbf{G}_*$ are such that $d(g_1x', g_2x') \leq 3re^{(\lambda_1 + \varepsilon)n}$ then $g_1x' = g_2x'$.

To do so, remark that if $x' \in X_{e^{(M+1)n}}(B)$ and $g = (a, b) \in \mathbf{G}_*$, alors, $ax' + b \in X_{2e^{(M+1+\lambda_1+\varepsilon)n}}(B)$

Thus, we have that $(g_1 - g_2)x' \in X_{4e^{(M+1+\lambda_1+\varepsilon)n}}(B)$ and that $d((g_1 - g_2)x', 0) \leq 3re^{(\lambda_1 + \varepsilon)n}$.

In particular, there is $q \in \mathbb{N}^*$ with $q \leq 4e^{(M+1+\lambda_1+\varepsilon)n}$ such that $q(g_1 - g_2)x'$ is a sum of elements of b multiplied on the left by matrices of norm smaller than $(4e^{(M+1+\lambda_1+\varepsilon)n})^2$ and

$$d(q(g_1 - g_2)x', 0) \leq |q|3re^{(\lambda_1 + \varepsilon)n} \leq 12re^{(M+1+2\lambda_1+2\varepsilon)n}$$

So, as F is (C, L) -diophantine, according to lemma 4.8, there are constants C', L such that if

$$12re^{(M+1+2\lambda_1+2\varepsilon)n} \leq \frac{C'}{(4e^{(M+1+\lambda_1+\varepsilon)n})^2 L}$$

then we have that $qg_1x' = qg_2x'$. But, this proves that $g_1x' = g_2x' + \frac{p}{q}$ for some $p \in \mathbb{Z}^d$. And

$$d\left(\frac{p}{q}, 0\right) = d(g_1x', g_2x') \leq 3re^{(\lambda_1 + \varepsilon)n}$$

So, if $\frac{1}{|q|} > 3re^{(\lambda_1 + \varepsilon)n}$, we have that $\frac{p}{q} = 0$ and so, $g_1x' = g_2x'$. \square

End of the proof of proposition 4.7. According to lemma 4.11, we have that for any $M \in \mathbb{R}_+^*$ large enough, there are $C, t \in \mathbb{R}_+^*$ such that for any $r \in]0, 1]$, any $n \in \mathbb{N}$ and any $x, y \in \mathbb{T}^d$, if

$$\mu^{*n}(\{g \in \mathbf{G} \mid d(gx, y) \leq r\}) \geq Ce^{-tn}$$

then there is $x' \in X_{e^{Mn}}(B(\mu))$ such that

$$d(x, x') \leq re^{Mn}$$

But, in this case, we have, according to lemma 4.12, that if

$$re^{Mn} \leq \frac{C_0}{e^{LMn}},$$

then

$$(\mu^{*n}(\{g \in \mathbf{G} \mid d(gx, y) \leq r\}))^2 \leq Ce^{-tn} + \mu^{*n} \otimes \mu^{*n}(\{g_1, g_2 \mid g_1 x' = g_2 x'\})$$

And this is what we intended to prove since

$$\mu^{*n} \otimes \mu^{*n}(\{g_1, g_2 \mid g_1 x' = g_2 x'\}) = \int_{\mathbf{G}} \mu^{*n}(\{g_1 \mid g_1 x' = g_2 x'\}) d\mu^{*n}(g_2) \quad \square$$

APPENDIX A. PRODUCTS OF RANDOM MATRICES

In this section, we are going to recall some of the properties of products of random matrices.

To do so, we fix some finite dimensional \mathbb{R} -vector space \mathbb{V} that we endow with an euclidian norm.

Let μ be a borelian probability measure on $\mathbf{G} := \mathrm{GL}(\mathbb{V})$.

We set, for any $g \in \mathbf{G}$, $N(g) = \max(\|g\|, \|g^{-1}\|)$ and we say that μ has a moment of order 1 if

$$\int_{\mathbf{G}} \ln N(g) d\mu(g) < +\infty$$

and that it has an exponential moment if there is some $\varepsilon \in \mathbb{R}_+^*$ such that

$$\int_{\mathbf{G}} N(g)^\varepsilon d\mu(g) < +\infty$$

Remark that there is some constant C depending only on $\dim(\mathbb{V})$ such that for any $g \in \mathrm{SL}_d(\mathbb{V})$, $\|g^{-1}\| \leq C\|g\|^{\dim \mathbb{V}}$ and so, if μ is a measure on $\mathrm{SL}(\mathbb{V})$, it is enough to ask that for some $\varepsilon \in \mathbb{R}_+^*$,

$$\int_{\mathbf{G}} \|g\|^\varepsilon d\mu(g) < +\infty$$

We would like to study the product $g_n \dots g_1$ where (g_i) is an iid sequence of law μ .

The first result in this direction is Oseledec's theorem :

Theorem A.1. *Let μ be a borelian probability measure on $\mathbf{G} := \mathrm{GL}(\mathbb{V})$ having a moment of order 1.*

Then, there are $m_1, \dots, m_r \in \mathbb{N}^$ with $\sum_i m_i = \dim \mathbb{V}$, there is $\Lambda_1 > \dots > \Lambda_r \in \mathbb{R}$ and some measurable function from $\mathbf{G}^{\mathbb{N}}$ into the space of flags $\mathbb{V} := \mathbb{V}_1 \supset \dots \supset \mathbb{V}_{r+1} := \{0\}$ of \mathbb{V} such that $\dim \mathbb{V}_i = \sum_{j=i}^r m_j$ and such that for $\mu^{\otimes \mathbb{N}}$ -a.e. $\omega = (g_n) \in \mathbf{G}^{\mathbb{N}}$,*

- $g_1 \mathbb{V}_i^\omega = \mathbb{V}_i^{\vartheta \omega}$ where ϑ is the shift on $\mathbf{G}^{\mathbb{N}}$.

- For any $x \in \mathbb{V}_i^\omega \setminus \mathbb{V}_{i+1}^\omega$,

$$\lim_n \frac{1}{n} \ln \|g_n \dots g_1 x\| = \Lambda_i$$

We call *Lyapunov exponents* the parameters $\Lambda_1, \dots, \Lambda_r$ and we note

$$\lambda_1 = \dots = \lambda_{m_1} = \Lambda_1, \quad \lambda_{m_1+1} = \dots = \lambda_{m_1+m_2} = \Lambda_2, \quad \text{etc.}$$

However, if $x \in \mathbb{V}$, this theorem doesn't say anything on the behavior of $\|g_n \dots g_1 x\|$ for some generic $(g_n) \in \mathbf{G}^{\mathbb{N}}$ because we have no information on the sequences (g_n) such that $x \in \mathbb{V}_i^{(g_n)}$. To avoid this problem, we usually assume that the subgroup of \mathbf{G} spanned by the support of μ acts irreducibly on \mathbb{V} (it doesn't fix any non-trivial subspace of \mathbb{V}). And in this case, Furstenberg proved the

Theorem A.2 ([BL85]). *Let μ be a borelian probability measure on \mathbf{G} having a moment of order 1 and whose support generates a group acting irreducibly on \mathbb{V} .*

Then, for any $x \in \mathbb{V} \setminus \{0\}$,

$$\frac{1}{n} \ln \|g_n \dots g_1 x\| \rightarrow \lambda_1 \text{ a.e.}$$

This irreducibility assumption is not good enough for us since we will identify $\mathrm{SL}_d(\mathbb{R}) \ltimes \mathbb{R}^d$ with the subgroup

$$\left(\begin{array}{cc} \mathrm{SL}_d(\mathbb{R}) & \mathbb{R}^d \\ 0 & 1 \end{array} \right)$$

of $\mathrm{SL}_{d+1}(\mathbb{R})$ whose action on \mathbb{R}^{d+1} is not irreducible.

A first important case of reducible actions on \mathbb{V} is when the support of μ generates a group

$$\left\{ \left(\begin{array}{cc} \Gamma_1 & * \\ 0 & \Gamma_2 \end{array} \right) \right\}$$

where $\Gamma_i < \mathrm{SL}(\mathbb{V}_i)$ with $\mathbb{V}_1 \oplus \mathbb{V}_2 = \mathbb{V}$ and Γ_i acts irreducibly on \mathbb{V}_i . Indeed, in this case, we can study the action on \mathbb{V}_1 and on \mathbb{V}_2 to get the one on \mathbb{V} . This motivates the following

Definition A.3. Let μ be a borelian probability measure on $\mathrm{GL}(\mathbb{V})$.

We say that some subspace \mathbb{W} of \mathbb{V} is adapted to μ if it is proper, invariant by the subgroup of $\mathrm{GL}(\mathbb{V})$ spanned by the support of μ and if there are $\Delta_1 > \Delta_2 \in \mathbb{R}$ such that

- For any $x \in \mathbb{V}/\mathbb{W} \setminus \{0\}$,

$$\frac{1}{n} \ln \|g_n \dots g_1 x\| \rightarrow \Delta_1 \text{ a.e.}$$

- For any $x \in \mathbb{W} \setminus \{0\}$,

$$\limsup \frac{1}{n} \ln \|g_n \dots g_1 x\| \leq \Delta_2 \text{ a.e.}$$

This definition is only useful since there is always an adapted subspace.

Theorem A.4 ([FK83] or [Hen84]). *Let μ be a borelian probability measure on $\mathrm{GL}(\mathbb{V})$ having a moment of order 1.*

Then there is some subspace \mathbb{W} of \mathbb{V} that is adapted to μ .

This theorem proves that we can always block-triangularize the group \mathbf{G}_μ spanned by the support of μ . Indeed, we can find by induction $\Delta_1 > \dots > \Delta_s \in \mathbb{R}$ and a flag $\mathbb{V} = \mathbb{W}_1 \supset \dots \supset \mathbb{W}_{s+1} := 0$ adapted to $\mu : \mathbb{W}_i$ is \mathbf{G}_μ -invariant and for any i and any $x \in \mathbb{W}_i / \mathbb{W}_{i+1} \setminus \{0\}$,

$$(A.1) \quad \frac{1}{n} \ln \|g_n \dots g_1 x\| \rightarrow \Delta_i \text{ a.e.}$$

The flag that we obtain in this way is included in the flag given by Oseledec's theorem (it means that $\{\mathbb{W}_i\} \subset \{\mathbb{V}_i\}$ and that $\{\Delta_i\} \subset \{\Lambda_i\}$ with $\Delta_1 = \Lambda_1$) but it has the advantage of being invariant and the convergence in equation (A.1) gives us Furstenberg's law of large numbers without any irreducibility assumption.

We are going to precise the convergence in equation (A.1) through a non-concentration inequality that we state in next

Theorem A.5. *Let μ be a borelian probability measure on $\mathrm{GL}(\mathbb{V})$ having an exponential moment.*

Then, for any $\varepsilon \in \mathbb{R}_+^$, there are $C, t \in \mathbb{R}_+^*$ such that for any $n \in \mathbb{N}$,*

$$\mu^{*n} \left(\left\{ g \in \mathrm{GL}(\mathbb{V}) \left| \left| \frac{1}{n} \ln \|g\| - \Lambda_1 \right| \geq \varepsilon \right. \right\} \right) \leq C e^{-tn}$$

Moreover, if \mathbb{W} is adapted to μ then, for any $x \in \mathbb{V}$ and any $n \in \mathbb{N}$,

$$\mu^{*n} \left(\left\{ g \in \mathrm{GL}(\mathbb{V}) \left| e^{(\Lambda_1 - \varepsilon)n} d(x, \mathbb{W}) \leq \|gx\| \leq e^{(\Lambda_1 + \varepsilon)n} \|x\| \right. \right\} \right) \geq 1 - C e^{-tn}$$

where we noted

$$d(x, \mathbb{W}) = \inf_{y \in \mathbb{W}} \|x - y\|$$

To prove this theorem, we first prove the following

Lemma A.6. *Let μ be a borelian probability measure on $\mathrm{GL}(\mathbb{V})$ having an exponential moment.*

Let $\Delta_1 > \dots > \Delta_s \in \mathbb{R}$ and $\mathbb{V} := \mathbb{W}_1 \supset \dots \supset \mathbb{W}_{s+1} := \{0\}$ be the flag adapted to μ and given by induction by theorem A.4.

Then for any $\varepsilon \in \mathbb{R}_+^$, there are $C, t \in \mathbb{R}_+^*$ such that for any $n \in \mathbb{N}$ and any $x \in \mathbb{V} \setminus \{0\}$,*

$$\mu^{*n} \left(\left\{ g \in \mathrm{GL}(\mathbb{V}) \left| \Delta_s - \varepsilon \leq \frac{1}{n} \ln \frac{\|gx\|}{\|x\|} \leq \Delta_1 + \varepsilon \right. \right\} \right) \geq 1 - C e^{-tn}$$

Proof. The proof of this lemma is an adaptation of the proof of proposition 3.2 in [BQ16] where Benoist and Quint only have polynomial moments.

First, for $g \in \mathbf{G}$ and $X = \mathbb{R}x \in \mathbb{P}(\mathbb{R}^d)$, we set

$$\sigma(g, X) = \ln \frac{\|gx\|}{\|x\|}, \quad \varphi(X) = \int_{\mathbf{G}} \sigma(g, X) d\mu(g) \text{ et } \sigma'(g, X) = \sigma(g, X) - \varphi(X)$$

Then, for any $X = \mathbb{R}x \in \mathbb{P}(\mathbb{R}^d)$ and any sequence $(g_n) \in \mathrm{GL}(\mathbb{V})^{\mathbb{N}}$, noting $X_k = g_k \dots g_1 X$, we have that

$$\ln \frac{\|g_n \dots g_1 x\|}{\|x\|} = \sum_{k=0}^{n-1} \sigma(g_{k+1}, X_k) = \sum_{k=1}^n \sigma'(g_{k+1}, X_k) + \sum_{k=0}^{n-1} \varphi(X_k)$$

Now, let $M_n = \sum_{k=0}^{n-1} \sigma'(g_{k+1}, X_k)$.

We can compute

$$\mathbb{E}[M_{n+1} - M_n | X_0, \dots, X_n] = \mathbb{E}[\sigma'(g_{n+1}, X_n) | X_0, \dots, X_n] = \int_{\mathbf{G}} \sigma'(g, X_n) d\mu(g) = 0$$

This proves that M_n is a martingale. Moreover, for any $\varepsilon \in \mathbb{R}_+^*$,

$$\mathbb{E}\left[e^{\varepsilon|M_{n+1}-M_n|} | X_0, \dots, X_n\right] = \int_{\mathbf{G}} e^{\varepsilon|\sigma'(g, X_n)|} d\mu(g)$$

And the inequality

$$-\ln \|g^{-1}\| \leq \sigma(g, X) = \ln \frac{\|gx\|}{\|x\|} \leq \ln \|g\|$$

shows that

$$\mathbb{E}\left[e^{\varepsilon|M_{n+1}-M_n|} | X_0, \dots, X_n\right] \leq \int_{\mathbf{G}} e^{2\varepsilon \ln \max(\|g\|, \|g^{-1}\|)} d\mu(g)$$

And so, as μ has an exponential moment, there is $\varepsilon \in \mathbb{R}_+^*$ and some constant C_0 such that for any $X \in \mathbb{P}(\mathbb{V})$ and any $n \in \mathbb{N}$,

$$\mathbb{E}_X\left[e^{\varepsilon|M_{n+1}-M_n|} | X_0, \dots, X_n\right] \leq C_0 \text{ a.e.}$$

Thus, according to the non-concentration inequality for martingales (see theorem 1.1 in [LW09]), for any $\varepsilon \in \mathbb{R}_+^*$, there is $C, t \in \mathbb{R}_+^*$ such that for any $X \in \mathbb{P}(\mathbb{V})$ and any $n \in \mathbb{N}$,

$$\mathbb{P}_X(|M_n| \geq \varepsilon n) \leq Ce^{-tn}$$

(it is important to remark that the constants C, t don't depend on X but only on ε and C_0).

To conclude, we only need to study $\sum_{k=0}^{n-1} \varphi(X_k)$. To do so, we just proved (using Borel-Cantelli's theorem) that

$$\frac{1}{n} M_n \rightarrow 0 \text{ a.e.}$$

Moreover, by definition of $\Delta_1, \dots, \Delta_s$ and $\mathbb{W}_1, \dots, \mathbb{W}_s$, we have that for any $X \in \mathbb{P}(\mathbb{V})$,

$$\Delta_s \leq \liminf_n \frac{1}{n} \sum_{k=0}^{n-1} \sigma(g_{k+1}, X_k) \leq \limsup_n \frac{1}{n} \sum_{k=0}^{n-1} \sigma(g_{k+1}, X_k) \leq \Delta_1 \text{ a.e.}$$

This proves that

$$\Delta_s \leq \liminf_n \frac{1}{n} \sum_{k=0}^{n-1} \varphi(X_k) \leq \limsup_n \frac{1}{n} \sum_{k=0}^{n-1} \varphi(X_k) \leq \Delta_1 \text{ a.e.}$$

And so, for any stationary probability measure ν on $\mathbb{P}(\mathbb{V})$,

$$\Delta_s \leq \int \varphi d\nu = \lim_n \int \mathbb{E}_x \frac{1}{n} \sum_{k=0}^{n-1} \varphi(X_k) d\nu(x) \leq \Delta_1$$

Finally, using proposition 3.1 of [BQ16], we get that for any $\varepsilon \in \mathbb{R}_+^*$, there are $C, t \in \mathbb{R}_+^*$ such that for any $n \in \mathbb{N}$ and any $X \in \mathbb{P}(\mathbb{R}^d)$,

$$\mathbb{P}_X \left(\Delta_s - \varepsilon \leq \frac{1}{n} \sum_{k=0}^{n-1} \varphi(X_k) \leq \Delta_1 + \varepsilon \right) \leq C e^{-tn}$$

And this finishes the proof of the lemma. \square

End of the proof of theorem A.5. We refer to the proof of proposition 4.1 in [BQ16].

First, remark that for any basis (v_1, \dots, v_d) of \mathbb{V} there is a constant C such that for any $g \in \text{GL}(\mathbb{V})$,

$$\frac{1}{C} \|gv_1\| \leq \|g\| \leq C \max_{i \in [1, d]} \|gv_i\|$$

And so, the non-concentration inequality for $\ln \frac{\|gv\|}{\|v\|}$ for any $v \in \mathbb{V} \setminus \{0\}$ implies the one for $\ln \|g\|$.

Then, remark that according to lemma A.6, for any $\varepsilon \in \mathbb{R}_+^*$, there are $C, t \in \mathbb{R}_+^*$ such that for any $x \in \mathbb{V}$ and any $n \in \mathbb{N}$,

$$\mu^{*n} \left(\left\{ g \in \text{GL}(\mathbb{V}) \mid \|gx\| > e^{(\Lambda_1 + \varepsilon)n} \|x\| \right\} \right) \leq C e^{-tn}$$

We endow \mathbb{V}/\mathbb{W} with the norm

$$\|x\|_{\mathbb{V}/\mathbb{W}} := \inf_{y \in \mathbb{W}} \|x - y\|$$

Then, we have that for any $x \in \mathbb{V}$,

$$\|x\| \geq d(x, \mathbb{W}) = \|\pi x\|_{\mathbb{V}/\mathbb{W}}$$

where π is the projection onto \mathbb{V}/\mathbb{W} and, by definition, since \mathbb{W} is adapted to μ , for any $x \in \mathbb{V}/\mathbb{W} \setminus \{0\}$,

$$\frac{1}{n} \ln \|g_n \dots g_1 x\|_{\mathbb{V}/\mathbb{W}} \rightarrow \Lambda_1 \text{ a.e.}$$

This proves that $\{0\}$ is adapted to the image of μ in $\text{GL}(\mathbb{V}/\mathbb{W})$. And so, according to lemma A.6, for any $\varepsilon \in \mathbb{R}_+^*$, there are $C, t \in \mathbb{R}_+^*$ such that for any $n \in \mathbb{N}$ and any $x \in \mathbb{V}/\mathbb{W} \setminus \{0\}$,

$$\mu^{*n} \left(\left\{ g \mid \left| \frac{1}{n} \ln \frac{\|gx\|}{\|x\|} - \Lambda_1 \right| \geq \varepsilon \right\} \right) \leq C e^{-tn}$$

And this proves that for any $n \in \mathbb{N}$ and any $x \in \mathbb{V}$,

$$\mu^{*n} \left(\left\{ g \mid \|gx\| \leq e^{(\Lambda_1 - \varepsilon)n} d(x, \mathbb{W}) \right\} \right) \leq C e^{-tn}$$

And this finishes the proof of the theorem. \square

We end this section with the study, for a borelian probability measure μ on $\text{SL}_d(\mathbb{R}) \times \mathbb{R}^d$, of the translation part b of the μ^{*n} -generic elements $g = (a, b)$. The aim is to prove that if we make some assumptions on μ , for any n , with large μ^{*n} -probability, an element $g = (a, b) \in \text{SL}_d(\mathbb{R}) \times \mathbb{R}^d$ is such that $\|b\| \approx e^{\Lambda_1 n}$.

To do so, we first compare the Lyapunov exponents of μ and of its projection on $\text{SL}_d(\mathbb{R})$ in next

Lemma A.7. *Let μ be a borelian probability measure on $\mathrm{SL}_d(\mathbb{R}) \ltimes \mathbb{R}^d$ having an exponential moment and let μ_0 be the projection of μ onto $\mathrm{SL}_d(\mathbb{R})$.*

See μ as a probability measure on $\mathrm{SL}_{d+1}(\mathbb{R})$ and define $\Lambda_1(\mu)$ this way.

Then,

$$\Lambda_1(\mu) = \Lambda_1(\mu_0)$$

Proof. First for any $n \in \mathbb{N}^*$ and any $\varepsilon \in \mathbb{R}_+^*$,

$$\mu^{\otimes \mathbb{N}} \left(\left\{ \left| \frac{1}{n} \ln \|g_{2n} \dots g_{n+1}\| - \Lambda_1(\mu) \right| \geq \varepsilon \right\} \right) = \mu^{\otimes \mathbb{N}} \left(\left\{ \left| \frac{1}{n} \ln \|g_n \dots g_1\| - \Lambda_1(\mu) \right| \geq \varepsilon \right\} \right)$$

So, according to lemma A.5,

$$\frac{1}{n} \ln \|g_{2n} \dots g_{n+1}\| \rightarrow \Lambda_1(\mu) \quad \mu^{\otimes \mathbb{N}} - \text{a.e.}$$

We can write, for any $g \in \mathrm{SL}_d(\mathbb{R}) \ltimes \mathbb{R}^d$,

$$g = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

and if g has law μ , then a has law μ_0 .

Thus,

$$g_{2n} \dots g_1 = \begin{pmatrix} a_{2n} \dots a_1 & a_{2n} \dots a_{n+1} \sum_{k=1}^n a_n \dots a_{k+1} b_k + \sum_{k=n+1}^{2n} a_{2n} \dots a_{k+1} b_k \\ 0 & 1 \end{pmatrix}$$

And so,,

$$\|g_n \dots g_1\| \geq \|a_n \dots a_1\|$$

This proves that $\Lambda_1(\mu) \geq \Lambda_1(\mu_0)$.

Let now $\Omega \in \mathbf{G}^{\mathbb{N}}$ be such that $\mu^{\otimes \mathbb{N}}(\Omega) = 1$ and for any $(g_n) \in \Omega$,

$$\lim_n \frac{1}{n} \ln \|g_n \dots g_1\| = \lim_n \frac{1}{n} \ln \|g_{2n} \dots g_{n+1}\| = \Lambda_1(\mu)$$

and

$$\lim_n \frac{1}{n} \ln \|a_n \dots a_1\| = \lim_n \frac{1}{n} \ln \|a_{2n} \dots a_{n+1}\| = \Lambda_1(\mu_0)$$

This way, for any $\varepsilon \in \mathbb{R}_+^*$, there is N_ε such that for any $n \in \mathbb{N}$ with $n \geq N_\varepsilon$,

$$e^{(\Lambda_1(\mu) - \varepsilon)n} \leq \|g_n \dots g_1\|, \|g_{2n} \dots g_{n+1}\| \leq e^{(\Lambda_1(\mu) + \varepsilon)n}$$

and,

$$\|a_n \dots a_1\|, \|a_{2n} \dots a_{n+1}\| \leq e^{(\Lambda_1(\mu_0) + \varepsilon)n}$$

Thus, we have that for any $\varepsilon \in \mathbb{R}_+^*$ and any large enough n ,

$$e^{2(\Lambda_1(\mu) - \varepsilon)n} \leq \|g_{2n} \dots g_1\| \leq \max \left(e^{2(\Lambda_1(\mu_0) + \varepsilon)n}, e^{(\Lambda_1(\mu) + \Lambda_1(\mu_0) + 2\varepsilon)n} + e^{(\Lambda_1(\mu) + \varepsilon)n} \right)$$

This proves that for any $\varepsilon \in \mathbb{R}_+^*$,

$$2(\Lambda_1(\mu) - \varepsilon) \leq \max(2\Lambda_1(\mu_0) + \varepsilon, \Lambda_1(\mu) + \Lambda_1(\mu_0) + 2\varepsilon)$$

And so, we get that

$$2\Lambda_1(\mu) \leq \max(2\Lambda_1(\mu_0), \Lambda_1(\mu) + \Lambda_1(\mu_0))$$

Finally, as we already proved that $\Lambda_1(\mu_0) \leq \Lambda_1(\mu)$, the previous inequality actually is an equality and we get the expected result. \square

Until now, we didn't say anything on the positivity of Λ_1 .

If μ is a measure on $\mathrm{SL}(\mathbb{V})$, then, as for μ -a.e. $g \in \mathbf{G}$, $\det(g) = 1$, we have that $\lambda_1 + \dots + \lambda_{\dim(\mathbb{V})} = 0$ and so, $\lambda_1 = 0$ if and only if for any i , $\lambda_i = 0$.

To get conditions that ensure that $\lambda_1 > 0$, we will say that a subgroup \mathbf{H} of $\mathrm{SL}_d(\mathbb{R})$ is strongly irreducible if it doesn't fix any non trivial finite union of subspaces of \mathbb{R}^d .

We remind the following result

Theorem A.8 (see [BL85] or [Gui81]). *Let μ be a borelian probability measure on $\mathrm{SL}(\mathbb{V})$ having a moment of order 1 and such that the subgroup spanned by the support of μ is strongly irreducible and non-compact.*

$$\int_{\mathrm{SL}_d(\mathbb{R})} \ln \|g\| d\mu(g) < +\infty$$

Then, $\Lambda_1 > 0$.

Corollary A.9. *Let μ be a borelian probability measure on $\mathrm{SL}_d(\mathbb{R}) \times \mathbb{R}^d$ having an exponential moment and that is not concentrated on $\mathrm{SL}_d(\mathbb{R}) \times \{0\}$. Assume that the projection onto $\mathrm{SL}_d(\mathbb{R})$ of the subgroup spanned by the support of μ is strongly irreducible and non-compact.*

Then, for any $\varepsilon \in \mathbb{R}_+^*$, there are $C, t \in \mathbb{R}_+^*$ such that for any $n \in \mathbb{N}$ and any $x \in \mathbb{R}^d$,

$$\mu^{*n} \left(\left\{ g \in \mathrm{SL}_d(\mathbb{R}) \times \mathbb{R}^d \left| \left| \frac{1}{n} \ln \frac{1 + \|gx\|}{1 + \|x\|} - \Lambda_1 \right| \geq \varepsilon \right. \right\} \right) \leq C e^{-tn}$$

Proof. We see μ as a probability measure on $\mathrm{SL}_{d+1}(\mathbb{R})$ and we are going to prove that the subspace \mathbb{W} adapted to μ and given by theorem A.4 is $\{0\}$.

First, since the projection of $\mathrm{supp} \mu$ on $\mathrm{SL}_d(\mathbb{R})$ spans a group \mathbf{G}_μ that acts strongly irreducibly and non-compactly on \mathbb{R}^d , the only subspaces of \mathbb{R}^{d+1} that can be invariant by $\mathrm{supp} \mu$ are \mathbb{R}^{d+1} , $\mathrm{Vect}(e_1, \dots, e_d)$, $\mathrm{Vect}(e_{d+1})$ and $\{0\}$. But, assuming that $\mathrm{supp} \mu$ is not a subset of $\mathrm{SL}_d(\mathbb{R}) \times \{0\}$ implies that $\mathrm{Vect}(e_{d+1})$ is not invariant by the group spans by the support of μ . Moreover, according to theorem A.8, there is $\Lambda_1 \in \mathbb{R}_+^*$ such that for any $x \in \mathrm{Vect}(e_1, \dots, e_d) \setminus \{0\}$,

$$\frac{1}{n} \ln \|g_n \dots g_1 x\| \rightarrow \Lambda_1 \text{ a.e.}$$

Then, for any $x \in \mathbb{R}^{d+1} \setminus \mathrm{Vect}(e_1, \dots, e_{d+1})$, we have, according to lemma A.7 that

$$\limsup_n \frac{1}{n} \ln \|g_n \dots g_1 x\| \leq \Lambda_1$$

So we also have that $\mathbb{W} \neq \mathrm{Vect}(e_1, \dots, e_d)$ and, as \mathbb{W} is proper, we have that $\mathbb{W} = \{0\}$.

Thus, according to lemma A.5, for any $\varepsilon \in \mathbb{R}_+^*$, there are $C, t \in \mathbb{R}_+^*$ such that for any $x \in \mathbb{R}^{d+1} \setminus \{0\}$,

$$\mu^{*n} \left(\left\{ g \in \mathrm{SL}_d(\mathbb{R}) \times \mathbb{R}^d \left| \left| \frac{1}{n} \ln \frac{\|gx\|}{\|x\|} - \Lambda_1 \right| \geq \varepsilon \right. \right\} \right) \leq C e^{-tn}$$

And in particular, with $x = x_0 + e_{d+1}$ for $x_0 \in \mathrm{Vect}(e_1, \dots, e_d)$ we get the expected result. \square

REFERENCES

- [BC01] István Berkes and Endre Csáki, *A universal result in almost sure central limit theory*, Stochastic Processes and their Applications **94** (2001), no. 1, 105 – 134. [5](#)
- [BFLM11] Jean Bourgain, Alex Furman, Elon Lindenstrauss, and Shahar Mozes, *Stationary measures and equidistribution for orbits of nonabelian semigroups on the torus*, J. Amer. Math. Soc. **24** (2011), no. 1, 231–280. MR 2726604 (2011k:37008) [2](#), [12](#), [14](#), [26](#)
- [BL85] Philippe Bougerol and Jean Lacroix, *Products of random matrices with applications to Schrödinger operators*, Progress in Probability and Statistics, vol. 8, Birkhäuser Boston, Inc., Boston, MA, 1985. MR 886674 (88f:60013) [31](#), [36](#)
- [Boy16] J.-B. Boyer, *Central limit theorem and law of the iterated logarithm for the linear random walk on the torus*, ArXiv e-prints (2016). [2](#), [6](#), [14](#)
- [BQ11] Yves Benoist and Jean-François Quint, *Mesures stationnaires et fermés invariants des espaces homogènes*, Ann. of Math. (2) **174** (2011), no. 2, 1111–1162. MR 2831114 [2](#)
- [BQ16] Yves Benoist and Jean-François Quint, *Central limit theorem for linear groups*, Ann. Probab. **44** (2016), no. 2, 1308–1340. [32](#), [34](#)
- [Cha96] Faouzi Chaabane, *Version forte du théorème de la limite centrale fonctionnel pour les martingales*, C. R. Acad. Sci. Paris Sér. I Math. **323** (1996), no. 2, 195–198. MR 1402542 [5](#), [11](#)
- [FK83] H. Furstenberg and Y. Kifer, *Random matrix products and measures on projective spaces*, Israel Journal of Mathematics **46** (1983), no. 1, 12–32. [31](#)
- [Gui81] Yves Guivarc’h, *Sur les exposants de Liapounoff des marches aléatoires à pas markovien*, C. R. Acad. Sci. Paris Sér. I Math. **292** (1981), no. 5, 327–329. MR 608846 [36](#)
- [Hen84] H. Hennion, *Loi des grands nombres et perturbations pour des produits réductibles de matrices aléatoires indépendantes*, Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete **67** (1984), no. 3, 265–278. [31](#)
- [HH80] P. Hall and C. C. Heyde, *Martingale limit theory and its application*, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], New York, 1980, Probability and Mathematical Statistics. MR 624435 (83a:60001) [11](#)
- [LW09] Quansheng Liu and Frédérique Watbled, *Exponential inequalities for martingales and asymptotic properties of the free energy of directed polymers in a random environment*, Stochastic Processes and their Applications **119** (2009), no. 10, 3101 – 3132. [33](#)

E-mail address: maths@jbboyer.fr