Lyapunov exponent of random dynamical systems on the circle

Dominique MALICET

Abstract

Let $f_1, \dots, f_m$ be some diffeomorphisms of the circle close to rotations, and let γ a Lyapunov exponent of the Markov system $x_{n+1} = f_{i_n}(x_n)$, where (i_n) is an i.i.d. sequence of elements of $\{1, \dots, m\}$. Under a simultaneous diophantine condition on the rotation numbers $\rho(f_1), \dots, \rho(f_m)$, we prove that $\gamma \leq 0$ and that there exists a diffeomorphism g such that $\text{dist}(gf_ig^{-1}, r_i) \ll \sqrt{-\gamma}$ for $i = 1, \dots m$.

1 Introduction

Arnold has proved in 1961 that a smooth orientation preserving diffeomorphism of $\mathbb{T}$ close enough to a rotation in analytic topology, and whose rotation number is diophantine, is conjugated to a rotation, and that the conjugation is analytic and close to Identity (see [1]). In this paper, we will study the case where we have several such functions we want to simultaneously conjugate to rotations. More precisely, if $f_1, \dots, f_m$ are diffeomorphisms of $\mathbb{T}$ close enough to rotations whose rotation numbers $\rho(f_i)$ ($i = 1, \dots, m$) satisfy some diophantine condition, which assumption ensures that $f_1, \dots, f_m$ are simultaneously conjugated to rotations? An obvious necessary condition is that these m functions commute, and under the assumption that at least one of the numbers $\rho(f_i)(i$ in $\{1, \dots, m\})$ is diophantine, this condition is sufficient by Arnold's theorem: indeed, up to a simultaneous conjugation, we can assume that this function f_i is an irrational rotation, and the commutation hypothesis then implies that all the f_j's are rotations. Moser [8] proved in 1989 that under the commutation assumption, the diophantine assumption can be weakened in a simultaneous diophantine condition on $\rho(f_1), \dots, \rho(f_m)$ which basically says that for each denominator q, there is at least one number $\rho(f_i)$ which has a bad approximation by rationals of the form $\frac{p}{q}$. An other obvious necessary condition to simultaneous conjugation is that the Lyapunov exponents of the Markov system $x_{n+1} = f_{i_n}(x_n)$, where (i_n) is an i.i.d sequence in $\{1, \dots, m\}$, are equal to 0, and we want to prove in this paper that this is also a sufficient condition under the same diophantine condition as Moser's.

Actually, this fact is already known, even without perturbative assumptions. There exists several results ([4], [3], [2], [5]) whose one consequence is that the nullity of the Lyapunov exponent implies the existence of a probability μ invariant by all the f_i's (it is in some sense a nonlinear version of Furstenberg result on the characteristic Lyapunov exponent of a product of i.i.d. matrixes). One can easily proves that in consequence, there exists a common continuous conjugation from the f_i's to the rotations. Next a theorem of B. Fayad and K. Khanin [7] (or Moser [8] in the local context) ensures that thanks to the diophantine condition, the conjugation is in fact C^∞.

In this paper, we give a more straightforward proof of this fact (in the local case), using KAM methods to construct the conjugation, in the same spirit as the proof of Moser's theorem. As a gain from using such a method, we obtain a quantitative version, which states that when γ is non null but small then the diffeomorphisms $f_1, \dots, f_m$ are "almost" simultaneously conjugated to rotations, in some explicit sense.

See also the Dolgopyat and Krikorian's paper [6] which proves an analog of our result on S^d, $d \geq 2$, and which initially inspired this paper.

1.1 Notations and main results

We denote by $\mathbb{T}$ the 1-dimensional torus $\mathbb{R}/\mathbb{Z}$. We will identify functions on $\mathbb{T}$ with their lifting on $\mathbb{R}$ by the application $x \mapsto x + \mathbb{Z}$. We denote by $C^k(\mathbb{T})$ the space of the functions on $\mathbb{R}$ which are C^k and 1-periodic, and by $Diff_+^k(\mathbb{T})$ the space of increasing functions on $\mathbb{R}$ on the form $Id + \varphi$ with φ in $C^k(\mathbb{T})$. Setting for k in $\mathbb{N}$

$$\|\varphi\|_k = \sup_{x\in\mathbb{R}, 0\leq j\leq k} |\varphi^{(j)}(x)|,$$

we equip $C^k(\mathbb{T})$ and $Diff_+^k(\mathbb{T})$ with the metric

$$d_k(\varphi, \psi) = \|\varphi - \psi\|_k$$

if $k < +\infty$, and

$$d_\infty(\varphi, \psi) = \sum_{j=0}^{+\infty} \frac{1}{2^j} \inf(\|\varphi - \psi\|_j, 1)$$

if $k = +\infty$. Sometimes, for convenience, we will use the notations C^k, $\|\cdot\|_k$, d_k with k non integer to denote the corresponding quantity replacing k by its integer part.

If φ is a random C^k application on $\mathbb{T}$ (i.e. a random variable $\omega \mapsto \varphi^\omega$ valued in $C^k(\mathbb{T})$), we denote

$$|||\varphi|||_k = \mathbb{E}\left[\|\varphi\|_k^2\right]^{\frac{1}{2}}$$

and if φ and ψ are random elements of $C^k(\mathbb{T})$ or $Diff_+^k(\mathbb{T})$, we denote

$$\delta_k(\varphi, \psi) = \mathbb{E}\left[d_k(\varphi, \psi)^2\right]^{\frac{1}{2}}.$$

If f is a random diffeomorphism of $\mathbb{T}$, a probability measure μ on $\mathbb{T}$ is said to be *stationary* for f if it is invariant for the transition operator $T\varphi = \mathbb{E}[\varphi \circ f]$ (that is, $\int_{\mathbb{T}} T\varphi d\mu = \int_{\mathbb{T}} \varphi d\mu$ for every φ in $C^0(\mathbb{T})$). The associated *Lyapunov exponent* is

$$\gamma(f,\mu) = \mathbb{E}\int_{\mathbb{T}} \ln f'(x) d\mu(x).$$

This Lyapunov exponent is invariant by conjugation in the sense that if G belongs to $Diff_+(\mathbb{T})$, then $\gamma(f,\mu) = \gamma(GfG^{-1}, G_*\mu)$.

A real valued random variable α will be said *diophantine* if it satisfies for some $\sigma > 1$ and $A > 0$ the condition:

$$\forall q \in \mathbb{N}^*, \left\| \inf_{p\in\mathbb{Z}} \left(\alpha - \frac{p}{q}\right)\right\|_{L^2(\Omega)} \geq \frac{1}{Aq^\sigma}. \tag{1}$$

This is for exemple the case if the law of α charges a diophantine number, or if it is not Lebesgue-singular.

Theorem 1. *Let α a diophantine random variable and $r_\alpha = Id + \alpha$. There exists $\varepsilon_0 = \varepsilon_0(\alpha)$ such that for every random C^∞ diffeomorphism f of $\mathbb{T}$ satisfying $\rho(f) = \alpha$, $\delta_\infty(f, r_\alpha) < \varepsilon_0$ and $\|f - r_\alpha\|_1 \leq 1$ a.s., and for every stationary measure μ of f, the associated Lyapunov exponent $\gamma = \gamma(f,\mu)$ is non positive and there exists a (non random) diffeomorphism $H \in Diff_+^\infty(\mathbb{T})$ such that*

$$\delta_0(HfH^{-1}, r_\alpha) \leq \sqrt{-5\gamma}.$$

In particular, when $\gamma = 0$, H is a simultaneous conjugation of almost every realisations of f to rotations. Moreover, H can be chosen close to identity in the sense that $d_\infty(H, Id)$ tends to 0 when ε_0 tends to 0.

Corollary 1. *Under the same assumptions as Theorem 1 ($\alpha = \rho(f)$ diophantine, $\|f - r_\alpha\|_1 \leq 1$ a.s. and $\delta_\infty(f, r_\alpha)$ small enough), if $\tilde{f}$ is an independent copy of f, then*

$$\delta_0(f \circ \tilde{f}, \tilde{f} \circ f) \leq 10\sqrt{-\gamma}.$$

Proof. If $\delta_\infty(f, r_\alpha)$ is small enough, then by Theorem 1 we can find H in $Diff_+(\mathbb{T})$ with $9/10 < H' < 11/10$ such that $f_1 = HfH^{-1}$ satisfies $\delta_0(f_1, r_\alpha) \leq \sqrt{-5\gamma}$. Obviously, setting $\tilde{f}_1 = H\tilde{f}H^{-1}$ and $\tilde{\alpha} = \rho(\tilde{f})$, we also have $\delta_0(\tilde{f}_1, r_{\tilde{\alpha}}) \leq \sqrt{-5\gamma}$. Consequently, $\delta_0(\tilde{f}_1 \circ f_1, r_{\alpha+\tilde{\alpha}}) \leq \delta_0(f_1, r_\alpha) + \delta_0(\tilde{f}_1, r_{\tilde{\alpha}}) \leq 2\sqrt{-5\gamma}$ and $\delta_0(\tilde{f}_1 \circ f_1, r_{\alpha+\tilde{\alpha}}) \leq 2\sqrt{-5\gamma}$, hence $\delta_0(f_1 \circ \tilde{f}_1, \tilde{f}_1 \circ f_1) \leq 9\sqrt{-\gamma}$, which implies by the mean value inequality that $\delta_0(f \circ \tilde{f}, \tilde{f} \circ f) \leq 10\sqrt{-\gamma}$. □

Remark : In the same way, using Moser's ideas [8] we could get an analog result of theorem 1, which would quantitatively say that "f and $\tilde{f}$ almost

commutes $\Rightarrow f$ is almost conjugated to a rotation", and then deduce a converse inequality of Corollary 1, of the form $\sqrt{-\gamma} \leq C\delta_k(f \circ \tilde{f}, \tilde{f} \circ f)$. Thus the square root of $-\gamma$ seems to quantitatively represent the "default of commutativity" of realisations of f.

Let us briefly explain the scheme of the proof of Theorem 1. In a first part, we compute an explicit approximation of the Lyapunov exponent of the system, studying first its stationary measure. This approximation is interesting in itself, and can for example be applied to a random product of i.i.d. 2×2 matrices, naturally acting on the projective space $\mathcal{P}(\mathbb{R}^2)$ identified to $\mathbb{T}$. In a second part, we use this approximation to show that smallness of the Lyapunov exponent implies that the system is conjugated to another closer to rotations, and when Lyapunov exponent is null, we will see that we can iterate this process to get a simultaneous conjugation to rotations.

2 Proof of the main theorem

In all this section, we fix a random increasing diffeomorphism f of $\mathbb{T}$ and a random real variable α satisfying (1) for some σ and A, and up to replacing A by $\min(1, A)$, we will assume $A \geq 1$. We set $\zeta = f - r_\alpha$. We also define on $C^0(\mathbb{T})$ transition the operators T and T_0 by $T\varphi = \mathbb{E}[\varphi \circ f]$ and $T_0\varphi = \mathbb{E}[\varphi \circ r_\alpha]$. We will denote dx the Lebesgue measure on $\mathbb{T}$.

2.1 Cohomological equation

Lemma 1. *For any $\psi \in C^k(\mathbb{T})$ with $k \geq 2\sigma$, the equation*

$$\varphi - T_0\varphi = \psi - \int_{\mathbb{T}} \psi dx$$

has an unique solution φ such that $\int_{\mathbb{T}} \varphi dx = 0$. Moreover, this solution satisfies the inequality $\|\varphi\|_{k-2\sigma} \leq \dfrac{\|\psi\|_k}{A^2}$

Proof. The equality $\varphi - T_0\varphi = \psi - \hat{\psi}(0)$ is equivalent to the fact that for any p in $\mathbb{Z}^*$, $\hat{\varphi}(q)(1 - \mathbb{E}[e^{2i\pi q\alpha}]) = \hat{\psi}(q))$, that is $\hat{\varphi}(q) = \frac{\hat{\psi}(q)}{1-\mathbb{E}[e^{2i\pi q\alpha}]}$ ($\mathbb{E}[e^{2i\pi q\alpha}]$ can not be equal to 1 thanks to the diophantine condition on α). Thus the uniqueness is clear and to justify the existence, it is sufficient to prove that we can define the function

$$\varphi(x) = \sum_p \frac{\hat{\psi}(q)}{1 - \mathbb{E}[e^{2i\pi q\alpha}]} e^{2i\pi qx},$$

and hence we need to bound the Fourier coefficients $\frac{\hat{\psi}(q)}{1-\mathbb{E}[e^{2i\pi q\alpha}]}$. The modulus of the numerator $\hat{\psi}(q)$ is less than $\frac{\|\psi\|_k}{(2\pi|q|)^k}$. Using the diophantine condition (1), we

can estimate the modulus of the denominator $1 - \mathbb{E}[e^{2i\pi q\alpha}]$ as follows :

$$\begin{aligned} |1 - \mathbb{E}[e^{2i\pi q\alpha}]| &\geq 1 - \mathbb{E}[\cos(2\pi q\alpha)] \\ &\geq \mathbb{E}\left[\inf_{q\in\mathbb{Z}}\left(\frac{(2\pi(q\alpha - p))^2}{2}\right)\right] \\ &\geq \frac{2\pi^2 A^2}{|q|^{2\sigma-2}}. \end{aligned}$$

Thus finally,

$$\left|\frac{\hat{\psi}(q)}{1 - \mathbb{E}[e^{2i\pi q\alpha}]}\right| \leq \frac{2\|\psi\|_k}{(2\pi)^{k+2}A^2|q|^{k-2\sigma+2}}.$$

So φ is well defined, is $C^{k-2\sigma}$ and satisfies

$$\|\varphi\|_{k-2\sigma} \leq (2\pi)^{k-2\sigma}\sum_{q\in\mathbb{Z}}|q|^{k-2\sigma}|\hat{\varphi}(q)| \leq \frac{2}{(2\pi)^{2\sigma+2}A^2}\left(\sum_{q\in\mathbb{Z}^*}\frac{1}{|q|^2}\right)\|\psi\|_k \leq \frac{\|\psi\|_k}{A^2}$$

□

2.2 Estimation of T-invariant measure

We define U the operator which associate to a function ψ in $C^k(\mathbb{T})$ the solution φ of the cohomological equation $\varphi - T_0\varphi = \psi - \int_{\mathbb{T}}\psi dx$. Thus :

$$U\psi(x) = \sum_{q\neq 0}\frac{\hat{\psi}(q)}{1 - \mathbb{E}[e^{2i\pi q\alpha}]}e^{2i\pi qx}$$

By Lemma 1, U is well defined on $C^k(\mathbb{T})$ for $k \geq 2\sigma$ and satisfies the bound $\|U\psi\|_{k-2\sigma} \leq A^{-2}\|\psi\|_k$. We also define U^* the adjoint of U in $L^2(\mathbb{T})$ ($U^*\psi(x) = \sum_{q\neq 0}\frac{\hat{\psi}(q)}{1-\mathbb{E}[e^{-2i\pi q\alpha}]}e^{2i\pi qx}$). The operator U will allow us to obtain an approximation of stationary measures of f, and next of the associated Lyapunov exponents.

Proposition 1. *If μ is a T-invariant probability measure, then:*

$$\int_{\mathbb{T}}\varphi d\mu = \int_{\mathbb{T}}\varphi dx + O(\varepsilon\|\varphi\|_{2\sigma+1}) = \int_{\mathbb{T}}\varphi dx + \int_{\mathbb{T}}(U^*\bar{\zeta})\varphi' dx + O(\varepsilon^2\|\varphi\|_{4\sigma+2})$$

where $\bar{\zeta} = \mathbb{E}[\zeta \circ r_{-\alpha}]$ and $\varepsilon = |||\zeta|||_{4\sigma+2}$.

(Here and in the sequel, $O(M)$ is a notation for a quantity bounded by CM where C is a constant depending only on α)

Proof. First, we will obtain an expansion formula of μ at order 0. We start from a Taylor formula at order 0 :

$$\varphi \circ f = \varphi \circ r_\alpha + O(\|\zeta\|_0\|\varphi\|_1).$$

Taking the expectation, this becomes

$$T\varphi = T_0\varphi + O(\varepsilon\|\varphi\|_1).$$

Then, thanks to the invariance of μ :

$$\int_{\mathbb{T}} (\varphi - T_0\varphi)d\mu = O(\varepsilon\|\varphi\|_1).$$

For ψ in $C^{1+2\sigma}(\mathbb{T})$, we apply the previous formula to $\varphi = U\psi$ and we get :

$$\int_{\mathbb{T}} \psi d\mu = \int_{\mathbb{T}} \psi dx + O(\varepsilon\|\psi\|_{2\sigma+1}). \tag{2}$$

Now, to obtain an expansion formula of μ at order 1, we use this time a Taylor formula at order 1 :

$$T\varphi = T_0\varphi + \mathbb{E}[(\varphi' \circ r_\alpha)\zeta] + O(\varepsilon^2\|\varphi\|_2).$$

By μ-invariance and our first estimation of μ :

$$\begin{aligned}\int_{\mathbb{T}} (\varphi - T_0\varphi)d\mu &= \int_{\mathbb{T}} \mathbb{E}[(\varphi' \circ r_\alpha)\zeta]d\mu + O(\varepsilon^2\|\varphi\|_2) \\ &= \int_{\mathbb{T}} \mathbb{E}[(\varphi' \circ r_\alpha)\zeta]dx + O(\varepsilon^2\|\varphi\|_2 + \varepsilon\|\mathbb{E}[(\varphi' \circ r_\alpha)\zeta]\|_{2\sigma+1}) \\ &= \int_{\mathbb{T}} \varphi'\bar{\zeta}dx + O(\varepsilon^2\|\varphi\|_{2\sigma+2})\end{aligned}$$

As previously, for ψ in $C^{4\sigma+2}(\mathbb{T})$ we take $\varphi = U\psi$ to get

$$\begin{aligned}\int_{\mathbb{T}} \psi d\mu &= \int_{\mathbb{T}} \psi dx + \int_{\mathbb{T}} (U\psi)'\bar{\zeta}dx + O(\varepsilon^2\|U\psi\|_{2\sigma+2}) \\ &= \int_{\mathbb{T}} \psi dx + \int_{\mathbb{T}} \psi'(U^*\bar{\zeta})dx + O(\varepsilon^2\|\psi\|_{4\sigma+2})\end{aligned}$$

□

2.3 Estimate of the Lyapunov exponent

Thanks to Proposition 1 we can deduce an estimate of the Lyapunov exponent of f:

Proposition 2.

$$\gamma(f,\mu) = -\frac{1}{2}\mathbb{E}\int_{\mathbb{T}} \left(\zeta' - (U^*\bar{\zeta})' \circ r_\alpha + (U^*\bar{\zeta})'\right)^2 dx + O(\varepsilon^3)$$

where $\bar{\zeta} = \mathbb{E}[\zeta \circ r_{-\alpha}]$ *and* $\varepsilon^3 = \mathbb{E}[\|\zeta\|^3]$.

Proof. Let $g = U^*\bar{\zeta}$, $G = Id - g$, $f_1 = GfG^{-1}$ (G is invertible if $\|g\|_1 \leq \frac{1}{2}$, which is the case if ε is small enough), $\zeta_1 = f_1 - r_\alpha$ and $\mu_1 = G_*\mu$. If φ is in $C^{4\sigma+2}(\mathbb{T})$, then thanks to Proposition 1:

$$\begin{aligned}\int_{\mathbb{T}} \varphi d\mu_1 &= \int_{\mathbb{T}} \varphi \circ G d\mu \\ &= \int_{\mathbb{T}} \varphi d\mu - \int_{\mathbb{T}} \varphi' g d\mu + O(\varepsilon^2\|\varphi\|_2) \\ &= \left(\int_{\mathbb{T}} \varphi dx + \int_{\mathbb{T}} \varphi' g dx\right) - \int_{\mathbb{T}} \varphi' g dx + O(\varepsilon^2\|\varphi\|_{4\sigma+2} + \varepsilon\|g\|_{2\sigma+1}\|\varphi\|_{2\sigma+1}) \\ &= \int_{\mathbb{T}} \varphi dx + O(\varepsilon^2\|\varphi\|_{4\sigma+2}).\end{aligned}$$

Now, using invariance of Lyapunov exponent by conjugation and the estimates $|||\zeta_1|||_1 = O(\varepsilon)$ and $\zeta_1 = \zeta - g \circ r_\alpha + g + O(\varepsilon^2)$, we can compute $\gamma(f, \mu)$:

$$\begin{aligned}\gamma(f,\mu) &= \mathbb{E}\int_{\mathbb{T}} \ln(1+\zeta_1')d\mu_1 \\ &= \mathbb{E}\int_{\mathbb{T}} (\zeta_1' - \zeta_1'^2/2)d\mu_1 + O(\varepsilon^3) \\ &= -\frac{1}{2}\mathbb{E}\int_{\mathbb{T}} \zeta_1'^2 dx + O(\varepsilon^3) \\ &= -\frac{1}{2}\int_{\mathbb{T}} \mathbb{E}[(\zeta' - g' \circ r_\alpha + g')^2]dx + O(\varepsilon^3).\end{aligned}$$

□

Remark : We could avoid the conjugation by G to estimate γ and directly expand $\mathbb{E}\int \ln f'(x)d\mu(x)$ using Proposition 1, but the method we have used has the advantage to make appear a main term clearly non-positive in the expansion of γ. Moreover, in the context of Theorem 1 this conjugation G will correspond to the first step in order to conjugate f to a diffeomorphism closer to rotations.

Here is an application of Proposition 2, independent of the proof of the main Theorem, which allows to estimate the characteristic Lyapunov exponent of a product of i.i.d. 2×2 matrices close to rotation matrices.

Corollary 2. *Let (M_n) an i.i.d sequence of random matrix of $SL_2(\mathbb{R})$ on the form $M_n = R_{\alpha_n} + N_n$ with $R_{\alpha_n} = \begin{pmatrix} \cos\pi\alpha_n & -\sin\pi\alpha_n \\ \sin\pi\alpha_n & \cos\pi\alpha_n \end{pmatrix}$ and $N_n = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix}$, where $2\alpha_n$ is not almost surely an integer. Then the Lyapunov exponent of the sequence (M_n), given by $\Gamma = \lim_{n\to\infty} \mathbb{E}\left[\frac{\ln\|M_{n-1}\cdots M_0\|}{n}\right]$ satisfies, setting $\varepsilon^3 = \mathbb{E}[\|N_0\|^3]$, $z = e^{i\pi\alpha_0}$ and $s = a_0 i - b_0 + c_0 - d_0 i$:*

$$\Gamma = \frac{1}{8|1 - \mathbb{E}[\bar{z}^2]|^2}\mathbb{E}\left[\left|sz(1 - \mathbb{E}[\bar{z}^2]) + \mathbb{E}[s\bar{z}](1 - z)\right|^2\right] + O(\varepsilon^3).$$

In the particular case where α_0 is not random, this formula becomes

$$\Gamma = \frac{1}{8}\mathbb{E}\left[|s - \mathbb{E}[s]|^2\right] + O(\varepsilon^3) = \frac{Var(s)}{8} + O(\varepsilon^3).$$

($O(\varepsilon^3)$ represents here a quantity bounded by $C\varepsilon^3$ where C depends only on α_0)

Proof. We identify $\mathbb{C}$ and $\mathbb{R}^2$. Let $f = r_{\alpha_0} + \zeta \in Diff_+(\mathbb{T})$ defined by

$$e^{i\pi f(x)} = \frac{M_0(e^{i\pi x})}{|M_0(e^{i\pi x})|}$$

f can be seen as a perturbation of r_{α_0}, and thanks to the formula of area conservation $|\sin(\pi(\theta - \theta'))| = |M_0 e^{i\pi\theta}|\,|M_0 e^{i\pi\theta'}|\,|\sin(\pi(f(\theta) - f(\theta')))|$, leading to $1 = |M_0 e^{i\pi\theta}|^2\,|f'(\theta)|$, we deduce that the Lyapunov exponent of the system generated by f is $\gamma = -2\Gamma$, and we can estimate it by Proposition 2. We first need to estimate ζ : writing that

$$i\pi\zeta(x) = \ln\left(\frac{1 + N_0(e^{i\pi x})e^{-i\pi(x+\alpha_0)}}{|M_0(e^{-i\pi x})|}\right),$$

and using that $|M_0(e^{i\pi x})|^{-1} = \left(1 + 2Re(N_0(e^{i\pi x})e^{-i\pi(x+\alpha_0)}) + |N_0(e^{i\pi x})|^2\right)^{-1/2}$ and usual Taylor expansions, we get that $\zeta = \zeta_0 + \zeta_1 + \zeta_2$ where :

- $\zeta_0(x) = Im(N_0(e^{i\pi x})e^{-i\pi(x+\alpha_0)})$ is a trigonometrical polynomial of degree 1 satisfying $|||\zeta_0|||_0 = O(||N||)$
- ζ_1 is a trigonometrical polynomial of degree 2 satisfying $|||\zeta_1|||_0 = O(||N||^2)$
- $|||\zeta_2|||_0 = O(||N||^3)$

If we assume that α_0 satisfies the diophantine condition (1), then by Proposition 2,

$$\Gamma = \frac{1}{2}\int_{\mathbb{T}} \mathbb{E}[(\zeta_0' - (U^*\bar{\zeta}_0)' \circ r_\alpha + (U^*\bar{\zeta}_0)')^2]dx + O(\varepsilon^3).$$

Next simple computation gives

$$\begin{aligned}
\zeta_0(x) &= -(a_0\cos(\pi x) + b_0\sin(\pi x))\sin(\pi(x+\alpha_0)) \\
&\quad +(c_0\cos(\pi x) + d_0\sin(\pi x))\cos(\pi(x+\alpha_0)) \\
&= Re\left(\frac{s}{4}e^{i\pi(2x+\alpha_0)}\right) + \text{constant} \\
U^*\bar{\zeta}_0(x) &= Re\left(\frac{\mathbb{E}[s\bar{z}]}{4(1 - \mathbb{E}[\bar{z}^2])}e^{2i\pi x}\right),
\end{aligned}$$

hence using our estimation of Γ, the end of the proof is straightforward.

Now, in order to treat the case where α_0 does not satisfy (1), we must copy the proof of Proposition 2, remarking that we only need in this case to estimate μ on trigonometrical polynomials of small degrees, and so we do not need a uniform estimate on small divisors appearing in the definition of $U\varphi$. More precisely, if T_0 is transition operator associated to r_{α_0}, the cohomological equation $\varphi - T_0\varphi = \psi - \hat{\psi}(0)$ can be solve in the $\mathbb{R}_2[e^{2i\pi x}]$ space of trigonometrical polynomials of degree 2, allowing to define as before the operator U on this space, and U is continuous since this space has a finite dimension. Next, we successively deduce that:

- For every ψ in $\mathbb{R}_2[e^{2i\pi x}]$, denoting $\varphi = U\psi$ we have
$$\int_{\mathbb{T}} \psi d\mu - \int_{\mathbb{T}} \psi dx = \int_{\mathbb{T}} (\varphi - T_0\varphi) d\mu + O(\varepsilon \|\varphi\|_0) = O(\varepsilon \|\psi\|_0)$$
- For every ψ in $\mathbb{R}_1[e^{2i\pi x}]$,
$$\begin{aligned} \int_{\mathbb{T}} \psi d\mu - \int_{\mathbb{T}} \psi(x) dx &= \int_{\mathbb{T}} (\varphi - T_0\varphi) d\mu + \int_{\mathbb{T}} \mathbb{E}[\varphi'(x+\alpha)\zeta_0(x)] d\mu(x) + O(\varepsilon^2 \|\varphi\|_0) \\ &= \int_{\mathbb{T}} \psi'(x) U^* \bar{\zeta}_0(x) dx + O(\varepsilon^2 \|\psi\|_0) \end{aligned}$$
- Denoting $\mu_1 = (Id - U^*\bar{\zeta}_0)_*\mu$, we have for ψ in $\mathbb{R}_2[e^{2i\pi x}]$
$$\int_{\mathbb{T}} \psi d\mu_1 = \int_{\mathbb{T}} \psi d\mu + O(\varepsilon \|\psi\|_0) = \int_{\mathbb{T}} \psi dx + O(\varepsilon \|\psi\|_0)$$
and for ψ in $\mathbb{R}_1[e^{2i\pi x}]$,
$$\begin{aligned} \int_{\mathbb{T}} \psi d\mu_1 &= \int_{\mathbb{T}} \psi d\mu - \int_{\mathbb{T}} \psi' U^* \zeta_0 d\mu + O(\varepsilon^2 \|\psi\|_0) \\ &= \int_{\mathbb{T}} \psi dx + O(\varepsilon^2 \|\psi\|_0) \end{aligned}$$
- Denoting $\tilde{f} = (Id - U^*\bar{\zeta}_0) \circ f \circ (Id - U^*\bar{\zeta}_0)^{-1} = Id + \alpha_0 + \tilde{\zeta}$, we can write $\tilde{\zeta} = \tilde{\zeta}_0 + \tilde{\zeta}_1 + \tilde{\zeta}_2$ with
$$\begin{cases} \tilde{\zeta}_0 = \zeta - U^*(\zeta_0) \circ r_{\alpha_0} + U^*\zeta_0 \in \mathbb{R}_1[e^{2i\pi x}],\ |||\tilde{\zeta}_0|||_0 = O(\varepsilon) \\ \tilde{\zeta}_1 \in \mathbb{R}_2[e^{2i\pi x}],\ |||\tilde{\zeta}_1|||_0 = O(\varepsilon^2) \\ |||\tilde{\zeta}_2|||_0 = O(\varepsilon^3) \end{cases}$$
and next
$$\begin{aligned} \gamma &= \int_{\mathbb{T}} \ln f_1' d\mu_1 \\ &= \int_{\mathbb{T}} \tilde{\zeta}_0' d\mu_1 + \int_{\mathbb{T}} \tilde{\zeta}_1' d\mu_1 - \frac{1}{2} \int_{\mathbb{T}} \tilde{\zeta}_0'^2 d\mu_1 + O(\varepsilon^3) \\ &= -\frac{1}{2} \int_{\mathbb{T}} \tilde{\zeta}_0'^2 dx + O(\varepsilon^3) \end{aligned}$$

Thus, we can conclude that the claimed estimate on Γ is valid without diophantine assumptions on α_0. □

Remarks :
1) If (M_n) is not assumed to belong to $Sl_2(\mathbb{R})$ but only to $Gl_2(\mathbb{R})$, we still can obtain an asymptotic formula for the Lyapunov exponent of (M_n) applying the previous statement to $M_n/\sqrt{\det(M_n)}$.

2) If $M_n = \begin{pmatrix} E - gv_n & -1 \\ 1 & 0 \end{pmatrix}$, where $E = 2\cos(\theta) \in]-2, 2[-\{0\}$ and (v_n) is an i.i.d centred sequence of reals, then M_n is conjugated to $R_\theta + gv_n \begin{pmatrix} 1 & \cot\theta \\ 0 & 0 \end{pmatrix}$ and the previous result gives the Lyapunov exponent estimate of Figotin and Pastur [9] when g tends to 0 :

$$\Gamma = \frac{g^2 V}{8\sin^2\theta} + O(g^3) = \frac{g^2 V}{2(4-E^2)} + O(g^3)$$

$(V = Var(v_0))$

3 Simultaneous conjugation

We summarise tools we need to make functional calculus on C^k spaces in the following proposition :

Proposition 3. *We can find constants B_k depending only on k such that for any k, the following assertions are satisfied :*
1)There exists a family of linear operators $(P_\lambda)_{\lambda>0}$ such that for any φ in $C^k(\mathbb{T})$ and for any $j < k$:

$$\begin{cases} \|P_\lambda\varphi\|_k \leq B_k \lambda^{k-j}\|\varphi\|_j \\ \|\varphi - P_\lambda\varphi\|_j \leq \dfrac{B_k\|\varphi\|_k}{\lambda^{k-j}}. \end{cases} \tag{3}$$

2)(Kolmogorov inequality) For any integer $j \leq k$ and for any φ in $C^k(\mathbb{T})$,

$$\|\varphi\|_j \leq B_k \|\varphi\|_k^{j/k} \|\varphi\|_0^{1-j/k}. \tag{4}$$

3)For any φ, ψ in $C^k(\mathbb{T})$, and any integer $j \leq k$,

$$\|\varphi\|_j \|\psi\|_{k-j} \leq B_k(\|\varphi\|_k\|\psi\|_0 + \|\varphi\|_0\|\psi\|_k) \tag{5}$$

and

$$\|\varphi\psi\|_k \leq B_k(\|\varphi\|_k\|\psi\|_0 + \|\varphi\|_0\|\psi\|_k). \tag{6}$$

4)For any Φ, Ψ in $Dif_+^k(\mathbb{T})$ such that $\max\left(d_1(\Phi, r_\alpha), d_1(\Psi, r_\beta)\right) \leq 3$, and for any real numbers α and β,

$$d_k(\Phi \circ \Psi, r_{\alpha+\beta}) \leq B_k\left(d_k(\Phi, r_\alpha) + d_k(\Psi, r_\beta)\right) \tag{7}$$

and when $d_1(\Phi, r_\alpha) \leq 1/2$,

$$d_k(\Phi^{-1}, r_{-\alpha}) \leq B_k d_k(\Phi, r_\alpha) \tag{8}$$

Proof. Points 1), 2) and 3) are classical:

- P_λ is constructed using a convolution by an appropriate kernel.
- (4) is a consequence of (3), using the decomposition $\varphi = P_\lambda\varphi + (\varphi - P_\lambda\varphi)$ for an appropriate choice of λ.
- (5) is a direct consequence of (4) and the convexity inequality $a^\theta b^{1-\theta} \leq \theta a + (1-\theta)b$, and (6) is a direct consequence of Leibniz formula and (5).

Let's now prove the inequalities (7) and (8): writing $\Phi = r_\alpha + \varphi$ and $\Psi = r_\beta + \psi$, we have $d_k(\Phi \circ \Psi, r_{\alpha+\beta}) = \|\psi + \varphi \circ \Psi\|_k \leq \|\psi\|_k + \|\varphi \circ \Psi\|_k$. And

$$\|\varphi \circ \Psi\|_k \quad \leq \|\varphi\|_0 + \|\Psi'\varphi' \circ \Psi\|_{k-1} \leq \|\varphi\|_0 + B_{k-1}(\|\Psi'\|_0\|\varphi' \circ \Psi\|_{k-1} + \|\Psi'\|_{k-1}\|\varphi'\|_0)$$

thanks to (6). Now, using that $\|\Psi'\|_0 \leq 4$, an iteration of this inequality gives the existence of $C = C(k)$ such that

$$\|\varphi \circ \Psi\|_k \leq C\left(\|\varphi\|_k + \sum_{j=0}^{k-1} \|\Psi'\|_j \|\varphi'\|_{k-1-j}\right)$$

and so we obtain the inequality (7) using that

$$\|\Psi'\|_j\|\varphi'\|_{k-1-j} \leq B_{k-1}(\|\Psi'\|_0\|\varphi'\|_{k-1} + \|\Psi'\|_{k-1}\|\varphi'\|_0) \leq 3B_{k-1}(\|\varphi\|_k + \|\psi\|_k).$$

To prove the inequality (8), we set $\Psi = \Phi^{-1} = r_{-\alpha} + \psi$, and we make the induction assumption that for every $j < k$, $\|\psi\|_j \leq B_j\|\varphi\|_j$ for some constant B_j. Noticing that $\psi = -\varphi \circ \Psi$, we get

$$\|\psi\|_k = \|\varphi \circ \Psi\|_k \leq \|\varphi\|_0 + \|\Psi'\varphi' \circ \Psi\|_{k-1} \leq \|\varphi\|_0 + \sum_{j=0}^{k-1} \binom{k-1}{j} \|\varphi' \circ \Psi\|_j \|\Psi'\|_{k-1-j}.$$

Next, for $j = 0$, $\|\varphi' \circ \Psi\|_j\|\Psi'\|_{k-1-j}$ is bounded by above by $\frac{1}{2}\|\psi\|_k + \|\varphi\|_1$, and for $j \neq 0$, $\|\varphi' \circ \Psi\|_j\|\Psi'\|_{k-1-j}$ is bounded by above up to a multiplicative constant by $\|\varphi\|_k$ thanks to the inequality (7), induction assumption and the inequality (5). Thus, we get $\|\psi\|_k \leq \frac{1}{2}\|\psi\|_k + C\|\varphi\|_k$ for some $C = C(k)$, which implies that $\|\psi\|_k \leq 2C\|\varphi\|_k$. □

The following lemma is an easy consequence of Proposition 3 which will give us useful C^k-estimates of a conjugation:

Lemma 2. *Let $U = r_\alpha + u$, $V = Id + v$ and $W = Id + w$ in $Diff^+(\mathbb{T})$ with $\|u\|_1 \leq 2$, $\max(\|v\|_1, \|w\|_1) \leq 1/2$. Then :*

$$1) d_k(VUV^{-1}, r_\alpha) \leq B_k(\|u\|_k + \|v\|_k)$$
$$2) d_0(VUV^{-1}, WUW^{-1}) \leq B_0 d_0(V, W)$$

where B_k is a constant depending only on k.

Proof. 1) is a direct consequence of inequalities (7) and (8) of Proposition 3. To prove 2), we write that

$$\begin{aligned} d_0(VUV^{-1}, WUW^{-1}) &\leq d_0(VUV^{-1}, WUV^{-1}) + d_0(WUW^{-1}, WUV^{-1}) \\ &\leq d_0(V, W) + d_0(WUW^{-1}V, WU) \\ &\leq (1 + \|(WUW^{-1})'\|_0) d_0(V, W) \end{aligned}$$

and we bound $\|(WUW^{-1})'\|_0$ by the chain rule. □

For the sequel we assume that f satisfies assumptions of Theorem 1, that is $\rho(f) = \alpha$, $d_1(f, r_\alpha) \leq 1$ a.s. and $\delta_\infty(f, r_\alpha)$ small enough. We fix γ a Lyapunov exponent of f associated to some stationary measure μ.

3.1 First conjugation

Lemma 3. *If $|||\zeta|||_{4\sigma+2}$ is small enough, f is conjugated by some $G = Id - g$ to some $\tilde{f} = GfG^{-1} = r_\alpha + \tilde{\zeta}$ such that for any $K \geq 2\sigma$:*

- $\|g\|_{K-2\sigma} \leq C|||\zeta|||_K$
- $|||\tilde{\zeta}|||_0 \leq \sqrt{-4\gamma + C_0|||\zeta|||^3_{4\sigma+2}}$

where C depends only on α and K, and C_0 depends only on α.

Proof. We proceed in a same way as in Proposition 2. We set $g = U^*\bar{\zeta}$ which satisfies the first claimed inequality by Lemma 1, $G = Id - g$ and $\tilde{f} = GfG^{-1} = r_\alpha + \tilde{\zeta}$. Noticing that $|||\tilde{\zeta}|||_1 \leq |||\zeta|||_1(1 + O(\varepsilon)) \leq \frac{3}{2}$ if ε is small enough and that $\ln(1 + t) \leq t - \frac{t^2}{4}$ for t in $[0, \frac{3}{2}]$, we have

$$\gamma = \mathbb{E}\int_{\mathbb{T}} \ln(1 + \tilde{\zeta}')d\mu_1 \leq \mathbb{E}\int_{\mathbb{T}} \left(\tilde{\zeta}' - \frac{1}{4}\tilde{\zeta}'^2\right)d\mu_1 = -\frac{1}{4}\mathbb{E}\int_{\mathbb{T}} \tilde{\zeta}'^2 dx + O(\varepsilon^3)$$

where $\varepsilon = |||\zeta|||_{4\sigma+2}$. Thus there exists C_0 depending only on α such that

$$\mathbb{E}\int_{\mathbb{T}} \tilde{\zeta}'^2 dx \leq -4\gamma + C_0\varepsilon^3.$$

Next, we notice that for a fixed event, for every a, b, $|\tilde{\zeta}(a) - \tilde{\zeta}(b)| \leq \int_{\mathbb{T}} |\tilde{\zeta}'|dx$, and since $\rho(\tilde{f}) = \rho(f) = \alpha$, we have $\tilde{\zeta}(b) = 0$ for some b, and so $\|\tilde{\zeta}\|_0 \leq \int_{\mathbb{T}} |\tilde{\zeta}'|dx$. Thus, by Cauchy-Schwarz, $\|\tilde{\zeta}\|_0^2 \leq \int_{\mathbb{T}} \tilde{\zeta}'^2 dx$, and taking the expectation and using previous inequality gives the result. □

Lemma 4. *Let $k = 4\sigma + 2$. If $\gamma \geq -C_0|||\zeta|||_k^3$ and if $|||\zeta|||_k$ is small enough, f is conjugated by some $G_0 = Id - g_0$ to some $f_1 = G_0 f G_0^{-1} = r_\alpha + \zeta_1$ such that, for every $K \geq k$:*

- $\|g_0\|_{K-2\sigma} \leq C_1|||\zeta|||_K$
- $|||\zeta_1|||_K \leq C_1|||\zeta|||_K|||\zeta|||_k^{-a}$
- $|||\zeta_1|||_k \leq C_1|||\zeta_1|||_K^{\delta}|||\zeta|||_k^{\frac{3}{2}(1-\delta)}$

where $a = \frac{2\sigma}{k-2\sigma}$, $\delta = k/K$ and C_1 is a constant which depends only on K and α.

Proof. If g is the function given by Lemma 3, we set $g_0 = P_\lambda g$ for some $\lambda > 1$ we will choose later (where P_λ is defined in Proposition 3). The first inequality simply comes from $\|g_0\|_{K-2\sigma} \leq \|g\|_{K-2\sigma}$ and Lemma 3. Next, by Lemma 2 and 3,

$$|||\zeta_1|||_K \leq B_K(|||\zeta|||_K + \|g_0\|_K) \leq B_K(|||\zeta|||_K + B_K\lambda^{2\sigma}\|g\|_{K-2\sigma}) \leq C\lambda^{2\sigma}|||\zeta|||_K \qquad (9)$$

with $C = B_K(1 + B_K C_0)$. On another hand, still by Lemma 3,

$$|||GFG^{-1} - r_\alpha|||_0 \leq C'|||\zeta|||_k^{3/2}$$

with $C' = \sqrt{5C_0}$, and by Lemma 2,

$$|||G_0 f G_0 - GfG^{-1}|||_0 \leq B_0\|G_0 - G\|_0 = B_0\|g - P_\lambda g\|_0 \leq B_0 B_{k-2\sigma}\frac{\|g\|_{k-2\sigma}}{\lambda^{k-2\sigma}} \leq \frac{C''|||\zeta|||_k}{\lambda^{k-2\sigma}}$$

with $C'' = B_0 C_0 B_{k-2\sigma}$. Combining the two last inequalities we get

$$|||\tilde{\zeta}|||_0 = |||G_0 f G_0^{-1} - r_\alpha|||_0 \leq \max(C', C'')\left(|||\zeta|||_k^{3/2} + \frac{|||\zeta|||_k}{\lambda^{k-2\sigma}}\right),$$

and by Kolmogorov inequality (4),

$$|||\zeta_1|||_k \leq C'''|||\zeta_1|||_K^{\delta}\left(|||\zeta|||_k^{3/2} + \frac{|||\zeta|||_k}{\lambda^{k-2\sigma}}\right)^{1-\delta} \qquad (10)$$

with $C''' = B_K \max(C'', C''')$. Taking $\lambda^{k-2\sigma} = |||\zeta|||_k^{-1/2}$, (9) and (10) give the result. □

3.2 KAM iteration

Now we assume that $\gamma \geq 0$, and we will iterate the constructed conjugation, and verify the convergence of the scheme to get a conjugation of f to r_α, which will imply in particular that $\gamma = 0$. Thus, we fix $k = 4\sigma - 2$, we define $f_0 = f$, $\zeta_0 = \zeta$, and once constructed $f_n = r_\alpha + \zeta_n$, if Lemma 4 applies we set $G_n = Id - g_n$ the conjugation obtained and $f_{n+1} = G_n f_n G_n^{-1} = r_\alpha + \zeta_{n+1}$. We also fix a large integer K, and we set $\varepsilon_n = |||\zeta_n|||_k$ and $\gamma_n = |||\zeta_n|||_K$.

Lemma 5. *There exists an integer K_0 depending only on α such that if $K \geq K_0$, then for some constant C depending on α, K and γ_0, we have $\varepsilon_{n+1} \leq C^{n^2} \varepsilon_n^{\frac{4}{3}}$ and $\gamma_n \leq C^{n^2} \varepsilon_n^{-4a}$ as long as f_n can be defined.*

Proof. Using the notations of Lemma 4

$$\gamma_{n+1} \leq C_1 \gamma_n \varepsilon_n^{-a} \tag{11}$$

$$\varepsilon_{n+1} \leq C_1 \gamma_{n+1}^{\delta} \varepsilon_n^{\frac{3}{2}(1-\delta)} \tag{12}$$

We will assume K large enough so that $\frac{3}{2}(1-\delta) - 4a\delta > \frac{4}{3}$ where $\delta = \frac{k}{K}$. Let $P_n = \varepsilon_n \cdots \varepsilon_0$. By (11), we have $\gamma_{n+1} \leq C_1^n \gamma_0 P_n^{-a}$. So (12) becomes

$$\varepsilon_{n+1} \leq C_2^n \varepsilon_n^{\frac{3}{2}(1-\delta)} P_n^{-a\delta}. \tag{13}$$

with $C_2 = ((1+\gamma_0)C_1)^{\delta}$. If for some integer n and real $M > 1$, we have $\varepsilon_n \leq M P_n^{\frac{1}{4}}$, then the previous inequality becomes

$$\varepsilon_{n+1} \leq M C_2^n P_n^{\frac{3}{2}(1-\delta)-a\delta} \leq M C_2^n P_n^{\frac{1}{3}},$$

and multiplying left and right side by $\varepsilon_{n+1}^{\frac{1}{3}}$ and then taking the power $\frac{3}{4}$, we obtain $\varepsilon_{n+1} \leq M C_2^n P_{n+1}^{\frac{1}{4}}$. Thus

$$\varepsilon_n \leq M P_n^{\frac{1}{4}} \Rightarrow \varepsilon_{n+1} \leq M C_2^n P_{n+1}^{\frac{1}{4}},$$

which implies by induction that $\varepsilon_n \leq C_2^{n^2} P_n^{\frac{1}{4}}$, and (13) becomes

$$\varepsilon_{n+1} \leq C_2^{n^2} \varepsilon_n^{\frac{3}{2}(1-\delta)-4a\delta}.$$

Since $\frac{3}{2}(1-\delta)-4a\delta > \frac{4}{3}$, this proves the first inequality, and the second inequality is then a direct consequence of $\gamma_{n+1} \leq C_1^n \gamma_0 P_n^{-a}$ and $\varepsilon_n \leq C_2^{n^2} P_n^{\frac{1}{4}}$. □

Now we can finish the proof of Theorem 1 :
First we apply the lemma with $K = K_0$. Thus, if $|||\zeta|||_{K_0}$ is small enough, then f_n is defined for every n and $\varepsilon_n = O(\frac{\varepsilon_0}{2^{(4/3)^n}})$. Next, we apply the lemma with a larger integer K: if $l = \theta K$ is an integer such that $\theta < \frac{1}{2(1+4a)}$, then we have for some constant C

$$|||\zeta_n|||_l \leq B_l \varepsilon_n^{1-\theta} \gamma_n^{\theta} \leq B_l C^{n^2(1-\theta)} \varepsilon_n^{1-\theta(1+4a)} \leq C^{n^2} \varepsilon_n^{\frac{1}{2}}$$

hence $|||\zeta_n|||_l$ quickly decreases to 0. Since K can be chosen arbitraly large, this holds for every l.

Now we set $H_n = G_{n-1} \cdots G_0$, so that $f_n = H_n f H_n^{-1}$. We have $H_n = Id + h_n$ with

$$h_n = \sum_{j=0}^{n-1} g_j \circ H_{j-1}.$$

For every l, we have for some $C = C(l)$

$$\begin{aligned}\|h_n\|_l &\leq \sum_{j=0}^{n-1} \|g_j \circ H_j\|_l \\ &\leq C \sum_{j=0}^{n-1} \|g_j\|_l (1 + \|h_j\|_l) \\ &\leq C\varepsilon_0 \sup_{j<n} (1 + \|h_j\|_l).\end{aligned}$$

Using an induction we deduce that if ε_0 is small enough then $\|h_n\|_l \leq C\varepsilon_0$ for some $C = C(l)$, and next that

$$\sum_{j=0}^{n-1} \|g_j \circ H_j\|_l \leq C\varepsilon_0$$

for some $C = C(l)$. In consequence, h_n normally converges in $C^l(\mathbb{T}^2)$ to some limit h satisfying $\|h\|_l \leq C\varepsilon_0$, and $H = Id + h$ is thus C^∞, close to Id, invertible if ε_0 is small enough, and satisfies $HfH^{-1} = r_\alpha$ almost surely.

Now, if we assume that $\gamma < 0$, then we notice that in the previous construction, we can define f_{n+1} from f_n as long as $\gamma \geq -C_0\varepsilon_n^3$ since we can use Lemma 4. Thus we can conjugate f to f_n satisfying $\gamma \geq -C_0\varepsilon_n^3$. Then Lemma 3 allows us to conjugate f_n to some $\tilde{f} = r_\alpha + \tilde{\zeta}$ satisfying $|||\tilde{\zeta}|||_0 \leq \sqrt{-4\gamma + C_0\varepsilon_n^3} \leq \sqrt{-5\gamma}$. This completes the proof of Theorem 1.

References

[1] VI Arnold. Small divisors I: On mappings of the circle onto itself. *Amer. Math. Soc. Transl., Ser*, 2(46):213–284, 1965.

[2] A. Avila and M. Viana. Extremal lyapunov exponents: an invariance principle and applications. *Inventiones mathematicae*, 181(1):115–178, 2010.

[3] P.H. Baxendale. Lyapunov exponents and relative entropy for a stochastic flow of diffeomorphisms. *Probability Theory and Related Fields*, 81(4):521–554, 1989.

[4] H. Crauel. Extremal exponents of random dynamical systems do not vanish. *Journal of Dynamics and Differential Equations*, 2(3):245–291, 1990.

[5] B. Deroin, V. Kleptsyn, and A. Navas. Sur la dynamique unidimensionnelle en régularité intermédiaire. *Acta mathematica*, 199(2):199–262, 2007.

[6] D. Dolgopyat and R. Krikorian. On simultaneous linearization of diffeomorphisms of the sphere. *Duke Mathematical Journal*, 136(3):475–506, 2007.

[7] B. Fayad and K. Khanin. Smooth linearization of commuting circle diffeomorphisms. *Annals of Mathematics*, 170:101–101, 2009.

[8] J. Moser. On commuting circle mappings and simultaneous Diophantine approximations. *Mathematische Zeitschrift*, 205(1):105–121, 1990.

[9] L. Pastur and A. Figotin. Spectra of random and almost-periodic operators. *Grundlehren der mathematischen Wissenschaften*, 297.