Lyapunov exponent of random dynamical systems on the circle

DOMINIQUE MALICET

Laboratoire d'Analyse et de Mathématiques Appliquées, Université Gustave Eiffel,
5 Boulevard Descartes, 77420 Champs-sur-Marne, France
(e-mail: mdominique@crans.org)

(*Received* 9 *September* 2020 *and accepted in revised form* 15 *February* 2021)

Abstract. We consider products of an independent and identically distributed sequence in a set $\{f_1, \ldots, f_m\}$ of orientation-preserving diffeomorphisms of the circle. We can naturally associate a Lyapunov exponent λ. Under few assumptions, it is known that $\lambda \leq 0$ and that the equality holds if and only if $f_1, \ldots, f_m$ are simultaneously conjugated to rotations. In this paper, we state a quantitative version of this fact in the case where $f_1, \ldots, f_m$ are C^k perturbations of rotations with rotation numbers $\rho(f_1), \ldots, \rho(f_m)$ satisfying a simultaneous diophantine condition in the sense of Moser [On commuting circle mappings and simultaneous diophantine approximations. *Math. Z.* **205**(1) (1990), 105–121]: we give a precise estimate of λ (Taylor expansion) and we prove that there exist a diffeomorphism g and rotations r_i such that $\operatorname{dist}(gf_ig^{-1}, r_i) \ll |\lambda|^{1/2}$ for $i = 1, \ldots, m$. We also state analogous results for random products of 2×2 matrices, without any diophantine condition.

Key words: random dynamics, one dimensional dynamics, KAM theory, Lyapunov exponents
2020 Mathematics Subject Classification: 37C05, 37C75, 37E10, 37H12, 37H15 (Primary)

1. *Statement of results*

1.1. *Lyapunov exponent of random product of diffeomorphisms of the torus.*

We consider the random compositions $g_n = f_{n-1} \circ \cdots \circ f_0$, where $(f_k)_{k\in\mathbb{N}}$ is a sequence of independent and identically distributed (i.i.d.) copies of some random diffeomorphism f of the one-dimensional torus $\mathbb{T} = \mathbb{R}/\mathbb{Z}$. The general expected behaviour under few assumptions is that, almost surely (a.s.), the random orbits $(g_n(x))_{n\in\mathbb{N}}$ distribute themselves toward a unique *stationary probability measure* μ on $\mathbb{T}$ and that the derivatives $g_n'(x)$ decrease toward 0 with a fixed exponential rate given by a *Lyapunov exponent* λ (we will recall the precise definitions). The objective is to estimate the measure μ and the number λ when

f is the perturbation of a random rotation and to obtain by an explicit estimate that λ is an obstruction to the existence of a linearization of f, that is to say, a deterministic diffeomorphism g such that gfg^{-1} is a rotation.

Let us begin by introducing some notation: the circle is identified with the torus $\mathbb{T} = \mathbb{R}/\mathbb{Z}$. For $k \in \mathbb{N}$, we identify $C^k(\mathbb{T})$ with the space of 1-periodic C^k maps from $\mathbb{R}$ into $\mathbb{R}$ endowed with its standard norm $\|\cdot\|_k$ defined by $\|\varphi\|_k = \sup_{j\le k, x\in\mathbb{R}} |\phi^{(j)}(x)|$. In the same way $\mathrm{Diff}^k_+(\mathbb{T})$ is the space of increasing diffeomorphisms f from $\mathbb{R}$ onto $\mathbb{R}$ of the form $f = \mathrm{Id} + \varphi$ with $\varphi \in C^k(\mathbb{T})$. Noting that the difference of two elements of $\mathrm{Diff}^k_+(\mathbb{T})$ belongs to $C^k(\mathbb{T})$ allows one to naturally endow $\mathrm{Diff}^k_+(\mathbb{T})$ with the metric d_k defined by $d_k(f, g) = \|f - g\|_k$. With these definitions, a rotation of $\mathbb{T}$ of angle α is simply the translation $\mathrm{Id} + \alpha$, which we denote r_α.

A random diffeomorphism of $\mathbb{T}$ is a random variable valued in $\mathrm{Diff}_+(\mathbb{T})$. In the paper all the random variables are implicitly assumed to be defined on the same probability space $(\Omega, \mathcal{F}, \mathbb{P})$. Let us recall the notions of stationary measure and Lyapunov exponent for a random diffeomorphism.

Definition 1.1. Let f be a random diffeomorphism of $\mathbb{T}$ valued in $\mathrm{Diff}^k_+(\mathbb{T})$ such that $\ln_+ \|f'\|_0 \in L^1(\Omega)$. A probability measure μ on $\mathbb{T}$ is stationary for f if $\mathbb{E}[f_*\mu] = \mu$ (such a measure always exists by the Kakutani fixed point theorem). The associated (mean) Lyapunov exponent is

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

We recall some known facts about stationary measures and Lyapunov exponents. We will not use them in this paper but it may enlighten the reader on their meaning and their interest.

PROPOSITION 1.1. *Let f be a random diffeomorphism valued in $\mathit{Diff}^1_+(\mathbb{T})$ such that $\ln_+ \|f'\|_0 \in L^1(\Omega)$ and let $g_n = f_{n-1} \circ \cdots \circ f_0$, where $(f_k)_{k\in\mathbb{N}}$ is a sequence of i.i.d. copies of f.*

- *If f is minimal in the sense that the unique closed sets of $\mathbb{T}$ almost surely invariant by f are $\emptyset$ and $\mathbb{T}$, then the stationary measure is unique (see* [5, 10]*).*
- *If there is a unique stationary measure μ for f and so a unique Lyapunov exponent $\lambda = \lambda(\mu)$, then for every x in $\mathbb{T}$ we have*
$$\frac{1}{n}\ln(g_n'(x)) \xrightarrow[n\to+\infty]{} \lambda \text{ a.s.}$$
- *$\lambda(\mu)$ is a negative number unless maybe if almost every (a.e.) realization of f preserves μ (it is an early version due to Crauel* [4] *of the so-called 'invariance principle' of Ávila and Viana* [2]*, both inspired by the linear version in the seminal paper* [9] *of Ledrappier).*

  If f is minimal, it implies the existence of a homeomorphism h of $\mathbb{T}$ such that hfh^{-1} is almost surely a rotation and so implies in particular that almost all realizations of f commute.

We are going to give an estimate for $\lambda(\mu)$ when f is a perturbation of a random rotation. We need an arithmetical condition on the angle of the random rotation. We recall that a number α is diophantine if for some $A, \sigma > 0$ we have $\mathrm{dist}(q\alpha, \mathbb{Z}) \geq A/|q|^{\sigma}$ for any q in $\mathbb{Z} - \{0\}$. By the generalized definition of Moser in [11], m numbers $\alpha_1, \ldots, \alpha_m$ are said to be simultaneously diophantine if for some $A, \sigma > 0$ we have $\sup_i \mathrm{dist}(q\alpha_i, \mathbb{Z}) \geq A/|q|^{\sigma}$ for any q in $\mathbb{Z} - \{0\}$ (in particular, it holds if at least one of the α_i is diophantine). Here we introduce a definition generalizing the classical notion of diophantine number for random variables.

Definition 1.2. Let α be a random variable in $\mathbb{T}$. For any $A > 0$ and $\sigma \geq 0$, we say that α is diophantine of type (A, σ) if for any q in $\mathbb{Z} - \{0\}$,

$$\|\mathrm{dist}(q\alpha, \mathbb{Z})\|_{L^2(\Omega)} \geq \frac{A}{|q|^{\sigma}}. \tag{1}$$

We say that α is diophantine if there exist $A > 0$ and $\sigma \geq 0$ such that α is diophantine of type (A, σ).

Remark 1.1.

- If α is deterministic (that is, is a constant random variable), then we obtain the classical definition of diophantine number and, if the set of realizations of α is a finite set $\{\alpha_1, \ldots, \alpha_m\}$, then α is diophantine if and only if $\alpha_1, \ldots, \alpha_m$ are simultaneously diophantine.
- If α has positive probability to be a diophantine number, then α is a diophantine random variable.
- Contrary to the deterministic case, it can happen that $\sigma = 0$. It is for example the case if α is uniform on $\mathbb{T}$ by a simple computation (or more generally if the law of α is not Lebesgue singular, by a consequence of the Riemann Lebesgue lemma).

To check the second point, consider the sets $E_{A,\sigma}$ of x in $\mathbb{T}$ such that for every q in $\mathbb{Z}^*$, $\mathrm{dist}(qx, \mathbb{Z}) \geq A/|q|^{\sigma}$. If α has positive probability to be diophantine, then there must exist A and σ such that α belongs to $E_{A,\sigma}$ with positive probability p and then for all $q \in \mathbb{Z}^*$, $\|\mathrm{dist}(q\alpha, \mathbb{Z})\|_{L^2(\Omega)} \geq (A/|q|^{\sigma})\sqrt{p}$.

Our first theorem gives a precise estimate for the Lyapunov exponent of a random diffeomorphism $f = r_\alpha + \zeta$ when f is a perturbation (in a smooth sense) of order ε of a random rotation r_α with α diophantine. We obtain a quadratic estimate $\lambda = O(\varepsilon^2)$ (instead of the obvious bound $\lambda = O(\varepsilon)$) and a formula for the quadratic term. In the statement of the theorem, a term $O(M)$ means a term bounded by CM with C a constant depending only on A and σ.

THEOREM 1. *Let α be a diophantine random variable of type (A, σ). Then there exists an integer k depending only on σ such that for any random diffeomorphism in $\mathrm{Diff}^k_+(\mathbb{T})$ of the form $f = r_\alpha + \zeta$ and for any Lyapunov exponent λ associated to any stationary measure of f, we have*

$$\lambda = -\frac{1}{2}\mathbb{E}\int_{\mathbb{T}} (\zeta' + \eta' - \eta' \circ r_\alpha)^2 \, dx + O(\varepsilon^3)$$

(and so $\lambda = O(\varepsilon^2)$), where $\varepsilon = \|d_k(f, r_\alpha)\|_{L^3(\Omega)} = \mathbb{E}[d_k(f, r_\alpha)^3]^{1/3}$, and where η is a deterministic map depending linearly on ζ and satisfying $|\eta'| = O(\varepsilon)$. The non-zero

https://doi.org/10.1017/etds.2021.22 Published online by Cambridge University Press

Fourier coefficients of η *are given by the formula*

$$\hat{\eta}(p) = \frac{\mathbb{E}[\hat{\zeta}(p)e^{-2i\pi p\alpha}]}{1 - \mathbb{E}[e^{-2i\pi p\alpha}]}. \tag{2}$$

The formula (2) can also be rewritten by the Parseval identity as

$$\lambda = -\frac{1}{2}\mathbb{E}\sum_{p\in\mathbb{Z}^*} p^2\bigg|\hat{\zeta}(p) + \frac{\mathbb{E}[\hat{\zeta}(p)e^{-2i\pi p\alpha}]}{1 - \mathbb{E}[e^{-2i\pi p\alpha}]}(1 - e^{2i\pi\alpha})\bigg|^2 + O(\varepsilon^3).$$

Remark 1.2. Our method can actually allow us to obtain the higher terms in the Taylor expansion of λ, of the form $\lambda = \sum_{j=2}^{n-1} q_j(\zeta) + O(\varepsilon^n)$, where $q_j(\zeta)$ is a j-linear form evaluated at $(\zeta, \ldots, \zeta)$.

In the next theorem we prove that if f is a random diffeomorphism close to rotations whose rotation number $\rho(f)$ is diophantine, then λ measures in an explicit sense how close to rotations f can be (smoothly) conjugated by a deterministic diffeomorphism. Note that λ is indeed a natural obstruction to the existence of such a diffeomorphism because λ is invariant under conjugation.

THEOREM 2. *Let* (A, σ) *be a couple of positive real numbers. There exists an integer* r *depending only on* σ *such that for any integer* K *larger than* r*, there exists in* $\mathit{Diff}_+^K(\mathbb{T})$ *a neighbourhood* $\mathcal{U}$ *of the set of rotations such that for any random diffeomorphism* f *valued in* $\mathcal{U}$ *whose rotation number* $\alpha = \rho(f)$ *is* (A, σ)*-diophantine, there exists in* $\mathit{Diff}_+^{K-r}(\mathbb{T})$ *a (non-random) diffeomorphism* h *such that*

$$\|d_0(hfh^{-1}, r_\alpha)\|_{L^2(\Omega)} \leq 3|\lambda|^{1/2}$$

for any Lyapunov exponent λ *associated to a stationary measure of* f*, with* h *satisfying* $d_{K-r}(h, \mathrm{Id}) \leq C\|d_K(f, r_\alpha)\|_{L^2(\Omega)}$ *for some* C *depending on* A*,* σ *and* K*.*

The constant 3 in the inequality above is not optimal. By analysing carefully our proof we could actually replace it by any number larger than $\sqrt{2}$. However, the bound $|\lambda|^{1/2}$ is essentially optimal since, by Theorem 1, $|\lambda|^{1/2} = O(d_k(hfh^{-1}, r_\alpha))$ for some integer k. The number r represents the 'loss of derivative'. As a result of our proof it can be made explicit as an affine function of σ, though we did not try to obtain an optimal expression.

Remark 1.3. If $\lambda = 0$ and f is valued in a finite set $\{f_1, \ldots, f_m\}$, the theorem gives a smooth diffeomorphism h conjugating simultaneously $f_1, \ldots, f_m$ to rotations. This particular case can actually be obtained by using a succession of already known results: f is minimal by the Denjoy theorem (the diophantine condition implies that at least one of the rotation numbers $\rho(f_i)$ is irrational), so if $\lambda = 0$ the maps f_i are simultaneously C^0-conjugated to rotations $r_1, \ldots, r_m$ and so pairwise commute (see Proposition 1.1). Then one can use a result of Moser [11] which generalizes the classical works of Arnold [1] and Moser on the linearization of a single map close to rotations in the case of several commuting maps, and which states that under the diophantine condition given in the assumption, the conjugacy h can be taken smooth and close to the identity with the estimate $d_{K-r}(h, \mathrm{Id}) = O(\sup_j d_K(f_j, r_j))$.

https://doi.org/10.1017/etds.2021.22 Published online by Cambridge University Press

Since the maps close to rotations almost commute, we can deduce from Theorem 2 the following corollary.

COROLLARY 1. *Let (A, σ) be a couple of positive real numbers. Then there exist an integer k and a neighbourhood $\mathcal{U}$ of the set of rotations in $\mathrm{Diff}^k_+(\mathbb{T})$ such that for any random diffeomorphism f valued in $\mathcal{U}$, if $\alpha = \rho(f)$ is (A, σ)-diophantine, then, by denoting by $\tilde{f}$ an independent copy of f, we have*

$$\|d_0(f \circ \tilde{f}, \tilde{f} \circ f)\|_{L^2(\Omega)} \leq C|\lambda|^{1/2}$$

for any Lyapunov exponent λ associated to a stationary measure of f, where C is a universal constant.

By Theorem 2, there exist an integer k and a neighbourhood $\mathcal{U}$ of rotations in $\mathrm{Diff}^k(\mathbb{T})$ such that for f valued in $\mathcal{U}$, there exists h in $\mathrm{Diff}^1_+(\mathbb{T})$ with $\max(h', (h^{-1})') \leq 2$ such that $f_1 = hfh^{-1}$ satisfies $\|d_0(f_1, r_\alpha)\|_{L^2(\Omega)} \leq 3|\lambda|^{1/2}$. Then, setting $\tilde{f}_1 = h\tilde{f}h^{-1}$ and $\tilde{\alpha} = \rho(\tilde{f})$, we deduce that $\|d_0(\tilde{f}_1 \circ f_1, r_{\alpha+\tilde{\alpha}})\|_{L^2(\Omega)} \leq 6|\lambda|^{1/2}$ and so $\|d_0(f_1 \circ \tilde{f}_1, \tilde{f}_1 \circ f_1)\|_{L^2(\Omega)} \leq 12|\lambda|^{1/2}$ and finally by the mean value inequality $\|d_0(f \circ \tilde{f}, \tilde{f} \circ f)\|_{L^2(\Omega)} \leq 48|\lambda|^{1/2}$.

Remark 1.4. One could expect a converse inequality by using Moser's ideas [11] to obtain a diffeomorphism h such that $\|d_{K-r}(hfh^{-1}, r_\alpha)\|_{L^2(\Omega)} \ll \|d_K(f \circ \tilde{f}, \tilde{f} \circ f)\|_{L^2(\Omega)}$ and then deduce from Theorem 1 that $|\lambda|^{1/2} \ll \|d_K(f \circ \tilde{f}, \tilde{f} \circ f)\|_{L^2(\Omega)}$ for some K.

The proof of Theorem 2 follows a 'KAM scheme' (from the so-called Kolmogorov–Arnold–Moser theory): in the same way as the Arnold linearization theorem [1] for a single diffeomorphism or the Moser linearization theorem [11] for commuting diffeomorphisms, we linearize the equation $hfh^{-1} = r_\alpha$ at $h = \mathrm{Id}$, $f = r_\alpha$ so that a solution of the linear equation gives an approximate solution of the initial equation and thus define a conjugation h such that hfh^{-1} is closer to rotations than f. We prove that this can be achieved if the obstruction λ is small enough by using the estimate given by Theorem 1. Then we reiterate the process in order to conjugate f to random diffeomorphisms f_n closer and closer to rotations. Thanks to the diophantine condition, we bound the C^k norms of the conjugations (though there is a loss of derivatives phenomenon as almost always in these kinds of KAM schemes but that can be handled by standard methods). The assumption $\rho(f) = \alpha$ ensures that the diophantine condition is satisfied at each step of the process. Finally, if $\lambda = 0$, we check that the sequence of conjugations converges and gives a conjugation between f and r_α and, if $\lambda \neq 0$, we stop the process when λ becomes large in front of $\mathrm{dist}(f_n, r_\alpha)$ and it gives the wanted conjugation.

This scheme of the proof is similar to the one in the paper of Dolgopyat and Krikorian [6], where they proved an analogous result on the sphere S^d for $d \geq 2$ (though only for the case $\lambda = 0$).

1.2. *Lyapunov exponent of random product of matrices.*

Our techniques also apply to estimate the Lyapunov exponent of the product of i.i.d. random 2×2 matrices close to rotation matrices, by studying the action on the projective line, identified to $\mathbb{T}$. And in this case we do not require a diophantine condition on the angle of the rotation but only a weak non-degeneracy condition.

Let $\|\cdot\|$ be a norm in $\mathcal{M}_2(\mathbb{R})$. Let M be a random variable in $\mathrm{GL}_2(\mathbb{R})$ such that $\mathbb{E}[|\ln_+\|M\||] < +\infty$. It is a well-known result of Furstenberg and Kesten [8] that if $(M_n)_{n\in\mathbb{N}}$ is a sequence of independent copies of M, then the limit

$$\Lambda = \lim_{n\to\infty} \frac{\ln \|M_{n-1}\cdots M_0\|}{n}$$

exists almost surely, is not random and does not depend on the norm. We call this number the Lyapunov exponent of M.

For $\alpha \in \mathbb{T}$, we denote by R_α the rotation matrix of angle $\pi\alpha$, that is to say,

$$R_\alpha = \begin{pmatrix} \cos \pi\alpha & -\sin \pi\alpha \\ \sin \pi\alpha & \cos \pi\alpha \end{pmatrix}.$$

The following theorem is the analogue of Theorem 1 for a random product of matrices.

THEOREM 3. *Let α be a random variable in $\mathbb{T}$ which does not belong almost surely to $\{0, \frac{1}{2}\}$. Let M be a random variable in $\mathrm{SL}_2(\mathbb{R})$ of the form $M = R_\alpha + E$. Let $\varepsilon = \mathbb{E}[\|E\|^3]^{1/3}$, which we assume to be finite, and let Λ be the Lyapunov exponent of M. Then*

$$\Lambda = \frac{1}{8}\mathbb{E}\bigg(\bigg|Ze^{i\pi\alpha} - \mathbb{E}[Ze^{i\pi\alpha}]\bigg(\frac{1-e^{2i\pi\alpha}}{1-\mathbb{E}[e^{2i\pi\alpha}]}\bigg)\bigg|^2\bigg) + O(\varepsilon^3),$$

where

$$Z = (a+d) + i(b-c) = \mathrm{Tr}(E) + i\mathrm{Tr}(ER_{1/2})$$

(in particular, $\Lambda = O(\varepsilon^2)$). If α is constant (that is, non-random), the formula simplifies and becomes

$$\Lambda = \frac{1}{8}\mathbb{E}[|Z - \mathbb{E}[Z]|^2] + O(\varepsilon^3) = \frac{\mathrm{Var}(Z)}{8} + O(\varepsilon^3).$$

The term $O(\varepsilon^3)$ represents here a quantity bounded by $C\varepsilon^3$, where C is a constant depending only on α (and is actually uniformly bounded on the sets $\{\|d(\alpha, \{0, \frac{1}{2}\}\|_{L^2(\Omega)} \geq$ const.$\}$).

Remark 1.5.

- In the general case $M \in \mathrm{GL}_2(\mathbb{R})$ (instead of $\mathrm{SL}_2(\mathbb{R})$), we can also obtain a Taylor expansion of its Lyapunov exponent Λ by applying the theorem to estimate the Lyapunov exponent $\widetilde{\Lambda}$ of $\widetilde{M} = M/\sqrt{\det(M)}$, since then $\Lambda = \widetilde{\Lambda} + \frac{1}{2}\mathbb{E}[\ln(\det(M))]$.
- As in Theorem 1, the method can be generalized to obtain a Taylor expansion of any order, but it requires more restrictions on α: to obtain an expansion of order q, α must not belong a.s. to $\{0, 1/q, \ldots, (q-1)/q\}$.
- We can obtain from the theorem an estimate of Pastur and Figotin [12] for the Lyapunov exponent of a Schrodinger matrix with small random potential: if $M = \left(\begin{smallmatrix} E-gV & -1 \\ 1 & 0 \end{smallmatrix}\right)$, with $E = 2\cos(\theta) \in\ ]-2, 2[- \{0\}$ and V a random real variable having a third moment, then M is conjugated to $R_\theta + gV\left(\begin{smallmatrix} 1 & \cot\theta \\ 0 & 0 \end{smallmatrix}\right)$ and then, by Theorem 1,

https://doi.org/10.1017/etds.2021.22 Published online by Cambridge University Press

when g tends to 0,

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

The following theorem is the analogue of Theorem 2 for a random product of matrices.

THEOREM 4. *Let $\mathcal{R}$ be the set of rotation matrices. For any $\delta > 0$, there exists a neighbourhood $\mathcal{U}$ of $\mathcal{R}$ in $\mathrm{SL}_2(\mathbb{R})$ such that for any random variable M in $\mathcal{U}$ satisfying $\|\mathrm{Tr}(M)\|_{L^2(\Omega)} \leq 2-\delta$, there exists $P \in \mathrm{SL}_2(\mathbb{R})$ such that*

$$\|d(PMP^{-1}, \mathcal{R})\|_{L^2(\Omega)} \leq C\Lambda^{1/2},$$

where Λ is the Lyapunov exponent of M and C is a constant depending only on the chosen norm on $\mathcal{M}_2(\mathbb{R})$. Moreover, $\|P - I_2\| \leq C'\|d(M, \mathcal{R})\|_{L^2(\Omega)}$ for some C' depending on δ and the norm.

From the proof it should not be difficult to obtain an explicit constant C for a given norm. The assumption $\|\mathrm{Tr}(M)\|_{L^2(\Omega)} \leq 2-\delta$ gives a control of the average ellipticity of M and should be seen as the analogue of the the diophantine condition on $\rho(f)$ in the nonlinear case.

We also deduce the same corollary as in the nonlinear case (with the same proof).

COROLLARY 2. *For any $\delta > 0$, there exists a neighbourhood $\mathcal{U}$ of $\mathcal{R}$ in $\mathrm{SL}_2(\mathbb{R})$ such that for any random variable M in $\mathcal{U}$ satisfying $\|\mathrm{Tr}(M)\|_{L^2(\Omega)} \leq 2-\delta$, if $\widetilde{M}$ is an independent copy of M, we have*

$$\mathbb{E}[\|M\widetilde{M} - \widetilde{M}M\|^2] \leq C\Lambda,$$

where Λ is the Lyapunov exponent of M and C is a constant depending only on the chosen norm on $\mathcal{M}_2(\mathbb{R})$.

From the proof it should not be difficult to obtain an explicit constant C for a given norm. Moreover, by using compactness arguments in $\mathcal{M}_2(\mathbb{R})$, we can deduce global results in more specific contexts, but then one can no longer hope to obtain explicit constants without additional work. Here is an example of a global result.

COROLLARY 3. *Let m be an integer and let δ and C_0 be two positive numbers. Then there exists $C > 0$ such that for any matrices $A_1, \ldots, A_m$ in $\mathrm{SL}_2(\mathbb{R})$ satisfying $|\mathrm{Tr}(A_i)| \leq 2-\delta$ (control of the ellipticity) and $\|A_i\| \leq C_0$ (control of the norm), we have*

$$\sup_{i,j} \|A_iA_j - A_jA_i\| \leq C\Lambda^{1/2},$$

where Λ is the Lyapunov exponent of the uniformly distributed random matrix in $\{A_1, \ldots, A_m\}$.

Proof. Let us consider Λ as a function of $A_1, \ldots, A_m$ on $\mathrm{SL}_2(\mathbb{R})^{\mathrm{m}}$. It is known by [3] that this function is continuous. In particular, it is continuous on the compact subset

$$\mathcal{K} = \{(A_1, \ldots, A_m), \|A_i\| \leq C_0, |\mathrm{Tr}(A_i)| \leq 2-\delta\}$$

https://doi.org/10.1017/etds.2021.22 Published online by Cambridge University Press

(the continuity of Λ is actually a lot easier to prove on this subset $\mathcal{K}$ thanks to the ellipticity condition $|\mathrm{Tr}(A_i)| \leq 2 - \delta$).

Moreover, if the function Λ vanishes at a point $(A_1, \ldots, A_m)$, then by the classical Furstenberg theorem [7] (and the ellipticity condition) the matrices A_i commute. Thus, there exists P in $\mathrm{SL}_2(\mathbb{R})$ such that PA_iP^{-1} is a rotation for every i and, using that $\|A_i\| \leq C_0$ and $|\mathrm{Tr}(A_i)| \leq 2 - \delta$, one can actually choose P with a bound $\|P\| \leq C_1$ for some constant C_1 depending only on C_0 and δ (we leave this detail to the reader).

Let $\mathcal{U}$ be the open set given by Corollary 2 and let

$$\mathcal{V} = \bigcup_{\|P\| \leq C_1} (P\mathcal{U}P^{-1})^m \subset \mathrm{SL}_2(\mathbb{R})^{\mathrm{m}}.$$

Then Λ is continuous and does not vanish on the compact set $\mathcal{K} \setminus \mathcal{V}$; hence, $\Lambda \geq m$ for some $m > 0$. Then:

- if $(A_1, \ldots, A_m) \in \mathcal{V}$, there is P in $Sl_2(\mathbb{R})$ with $\|P\| \leq C_1$ such that $B_i = PA_iP^{-1} \in \mathcal{U}$ for every i, by Corollary 2 $\|B_iB_j - B_jB_i\| \leq C\Lambda^{1/2}$ for some constant C, and then $\|A_iA_j - A_jA_i\| \leq C'\Lambda^{1/2}$ for some new constant $C' = CC_1^2$;
- if $(A_1, \ldots, A_m) \notin \mathcal{V}$, then $\Lambda \geq m$ so $\|A_iA_j - A_jA_i\| \leq 2C_0^2 \leq C\Lambda^{1/2}$ with $C = 2C_0^2/m^{1/2}$. □

Remark 1.6. In the corollary above, one can actually obtain also a converse inequality $\sup_{i,j} \|A_iA_j - A_jA_i\| \geq c\Lambda^{1/2}$, by using that we can find P with bounded norm and rotation matrices R_i so that $\sup_i \|PA_iP^{-1} - R_i\| \ll \sup_{i,j} \|A_iA_j - A_jA_i\|$ and then by using Theorem 3 to get $\Lambda \ll (\sup_i \|PA_iP^{-1} - R_i\|)^2$.

2. *Preliminaries*

2.1. *Some C^k estimates.*

We begin by stating various estimates in $\mathrm{Diff}_+^k(\mathbb{T})$. All of them are classical estimates of KAM theory. Nevertheless, we give proofs in an appendix (§A).

A key tool is the so-called *Kolmogorov inequality*.

PROPOSITION 2.1. (*Kolmogorov inequality*) *For any integers $j \leq k$ and for any φ in $C^k(\mathbb{T})$,*

$$\|\varphi\|_j \leq C\|\varphi\|_k^{j/k}\|\varphi\|_0^{1-j/k}, \tag{3}$$

where C is a constant depending only on k.

The three following propositions give C^k estimates of gfg^{-1} when f is a diffeomorphism close to a rotation r_α and g is a diffeomorphism close to Id. The first estimate allows us to bound the large C^k norms of such a conjugation.

PROPOSITION 2.2. *Let f, g be in $\mathit{Diff}_+^k(\mathbb{T})$ and let α be in $\mathbb{T}$ with $d_1(f, r_\alpha) \leq 1$ and $d_1(g, \mathrm{Id}) \leq \frac{1}{2}$. Then*

$$d_k(gfg^{-1}, r_\alpha) \leq C(d_k(f, r_\alpha) + d_k(g, \mathrm{Id})),$$

where C is a constant depending only on k.

https://doi.org/10.1017/etds.2021.22 Published online by Cambridge University Press

The assumption of the bound 1 for $d_1(f, \mathrm{Id})$ is arbitrary and could be replaced by any other number. In the same way the bound $\frac{1}{2}$ for $d_1(g, \mathrm{Id})$ could be replaced by any number less than 1.

The second estimate bounds the distance between two conjugations in a function of the distance between the conjugacies.

PROPOSITION 2.3. *Let f, g and $\tilde{g}$ be in $\mathit{Diff}^1_+(\mathbb{T})$ and let α be in $\mathbb{T}$, with $d_1(f, r_\alpha) \leq 1$, $d_1(g, \mathrm{Id}) \leq \frac{1}{2}$ and $d_1(\tilde{g}, \mathrm{Id}) \leq \frac{1}{2}$. Then*

$$d_0(gfg^{-1}, \tilde{g}f\tilde{g}^{-1}) \leq C_0 d_0(g, \tilde{g}),$$

where C_0 is an absolute constant.

Remark 2.1. It is actually more generally possible to bound $d_k(gfg^{-1}, \tilde{g}f\tilde{g}^{-1})$ as a function of $d_k(g, \tilde{g})$, but we will not need it.

The third estimate gives a classical linear approximation of gfg^{-1}.

PROPOSITION 2.4. *Let $k \geq 2$, let f, g be in $\mathit{Diff}^2_+(\mathbb{T})$ and let α be in $\mathbb{T}$. Writing $f = r_\alpha + \zeta$, $g = \mathrm{Id} + \eta$ and denoting $\varepsilon = \max(\|\zeta\|_2, \|\eta\|_2)$, we have*

$$gfg^{-1} = r_\alpha + (\zeta + \eta \circ r_\alpha - \eta) + R,$$

where R is a quadratic remainder satisfying $\|R\|_1 \leq C\varepsilon^2$ for some absolute constant C.

Remark 2.2. The ε^2 upper bound can actually be replaced by the more precise term $\max(\|\zeta\|_2, \|\eta\|_2) \cdot \max(\|\zeta\|_0, \|\eta\|_0)$. There also exists a C^k version of this estimate.

We conclude with a last required estimate.

PROPOSITION 2.5. *Let f, g, h be in $\mathit{Diff}^k_+(\mathbb{T})$ with $d_k(h, \mathrm{Id}) \leq 1$. Then*

$$d_k(f \circ h, g \circ h) \leq C d_k(f, g),$$

where C is a constant depending only on k.

Remark 2.3. The assumption $d_k(h, \mathrm{Id}) \leq 1$ is strong (in the previous propositions we only assumed bounds on C^1 distances). Under the weaker assumption $d_1(h, \mathrm{Id}) \leq 1$ we actually have $d_k(f \circ h, g \circ h) \leq C(1 + d_k(h, \mathrm{Id}))d_k(f, g)$.

2.2. *Cohomological equation.* We fix a random rotation $r_\alpha = \mathrm{Id} + \alpha$ and a perturbation $f = r_\alpha + \zeta$ of r_α. We assume that α is (A, σ)-diophantine. We will assume that σ is an integer, in order to avoid the use of C^k-norms with k a non-integer. It is obviously not a restriction since we can replace σ by $[\sigma] + 1$.

We denote respectively by T_0 and T the transfer operators of r_α and f. That is, for any map $\varphi : \mathbb{T} \to \mathbb{R}$,

$$T_0\varphi = \mathbb{E}[\varphi \circ r_\alpha], \ T\varphi = \mathbb{E}[\varphi \circ f].$$

Since f is a perturbation of r_α, T is a perturbation of T_0. Note also that a measure μ is stationary for f if and only if $\int \varphi \, d\mu = \int T\varphi \, d\mu$ for any map $\varphi \in C(\mathbb{T})$.

https://doi.org/10.1017/etds.2021.22 Published online by Cambridge University Press

The understanding of stationary measures is naturally related to the understanding of the cohomological equation $\varphi - T\varphi = \psi$. Our main ingredient in our proofs is that the approximated cohomological equation $\varphi - T_0\varphi = \psi$ is easily solvable in φ by Fourier methods, in the same way as in the classical deterministic case: the equation can be rewritten

$$\text{for all } q \in \mathbb{Z}, \hat{\varphi}(q)(1 - \mathbb{E}[e^{2i\pi q\alpha}]) = \hat{\psi}(q).$$

For $q = 0$, we get the obvious restriction $\hat{\psi}(0) = \int_{\mathbb{T}} \psi(x)\,dx = 0$ and, for $q \neq 0$, if $q\alpha$ is not almost surely an integer (which is the case for α diophantine), then $\mathbb{E}[e^{2i\pi q\alpha}] \neq 1$ and we obtain $\hat{\varphi}(q) = \hat{\psi}(q)/(1 - \mathbb{E}[e^{2i\pi q\alpha}])$. It leads us to define the following operator U: for $\psi : \mathbb{T} \to \mathbb{R}$,

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

a priori well defined at least if ψ is a trigonometric polynomial. If $\phi = U\psi$ is well defined, then it is the unique solution of the equation

$$\varphi - T_0\varphi = \psi - \int_{\mathbb{T}} \psi(x)\,dx$$

such that $\int_{\mathbb{T}} \varphi\,dx = 0$.

It is also convenient to define its adjoint $\overline{U}$ by

$$\overline{U}\psi(x) = \sum_{q\in\mathbb{Z}^*} \frac{\hat{\psi}(q)}{1 - \mathbb{E}[e^{-2i\pi q\alpha}]} e^{2i\pi qx},$$

so that for any trigonometric polynomials ψ_1 and ψ_2 we have

$$\int_{\mathbb{T}} U\psi_1(x)\psi_2(x)\,dx = \int_{\mathbb{T}} \psi_1(x)\overline{U}\psi_2(x)\,dx.$$

The following lemma states that under the diophantine condition, U and $\overline{U}$ are actually well defined on sufficiently smooth maps and are bounded up to some loss of derivative.

LEMMA 2.1. *Let $k_0 = 2\sigma + 2$. Then the operators U and $\overline{U}$ are well defined on $C^{k_0}(\mathbb{T})$ and, for any integer k, if $\psi \in C^{k+k_0}(\mathbb{T})$, then $U\psi \in C^k(\mathbb{T})$ and $\|U\psi\|_k \leq (1/A^2)\|\psi\|_{k+k_0}$. The same estimate holds if we replace U by $\overline{U}$.*

Proof. It is enough to prove that for any integer k the inequality $\|U\psi\|_k \leq (1/A^2)\|\psi\|_{k+k_0}$ holds for any trigonometric polynomial ψ (the same estimate for $\overline{U}$ follows by replacing α with $-\alpha$). To estimate $\|U\psi\|_k$, we are going to bound for $q \neq 0$ the Fourier coefficient

$$|\widehat{U\psi}(q)| = \left|\frac{\hat{\psi}(q)}{1 - \mathbb{E}[e^{2i\pi q\alpha}]}\right|.$$

The numerator can be bounded from above by

$$|\hat{\psi}(q)| \leq \frac{\|\psi\|_{k+k_0}}{(2\pi|q|)^{k+k_0}}. \tag{4}$$

https://doi.org/10.1017/etds.2021.22 Published online by Cambridge University Press

To bound the denominator from below, we use that for any real number x, writing $x = k + \theta$ with $k \in \mathbb{Z}$ and $|\theta| = d(x, \mathbb{Z}) \leq \frac{1}{2}$, we have

$$1 - \cos(2\pi x) = 2(\sin(\pi x))^2 = 2(\sin(\pi\theta))^2 \geq 2\bigg(\frac{2}{\pi}\pi\theta\bigg)^2 = 8d(x, \mathbb{Z})^2 \geq d(x, \mathbb{Z})^2$$

and hence, by using the diophantine condition (1),

$$\begin{aligned} |1 - \mathbb{E}[e^{2i\pi q\alpha}]| &\geq 1 - \mathbb{E}[\cos(2\pi q\alpha)] \\ &\geq \mathbb{E}[d(q\alpha, \mathbb{Z})^2] \\ &\geq \frac{A^2}{|q|^{2\sigma}}. \end{aligned} \tag{5}$$

Thus, (4) and (5) give, using that $k_0 = 2\sigma + 2$,

$$|\widehat{U\psi}(q)| \leq \frac{\|\psi\|_{k+k_0}}{(2\pi)^{k+k_0}A^2|q|^{k+2}}.$$

Consequently,

$$\|U\psi\|_k \leq \sum_{q\in\mathbb{Z}^*} |2\pi q|^k |\widehat{U\psi}(q)| \leq \frac{1}{(2\pi)^{k_0}A^2}\bigg(\sum_{q\in\mathbb{Z}^*}\frac{1}{|q|^2}\bigg)\|\psi\|_{k+k_0} \leq \frac{1}{A^2}\|\psi\|_{k+k_0}$$

since $1/(2\pi)^{k_0}\sum_{q\in\mathbb{Z}^*}(1/|q|^2) \leq (1/(2\pi)^2)(\pi^2/3) = 1/12$. □

3. *Proof of Theorem 1*

We fix a random rotation r_α and a perturbation $f = r_\alpha + \zeta$, and we assume that α is (A, σ)-diophantine. The operators T_0, T, U and $\overline{U}$ are defined as in the previous section. We are going to obtain a Taylor expansion for the stationary measures of f and the associated Lyapunov exponents.

3.1. *Estimate of the stationary measures.*

PROPOSITION 3.1. *If μ is a stationary measure for f, then*

$$\int_{\mathbb{T}} \varphi\, d\mu = \int_{\mathbb{T}} \varphi\, dx + O(\varepsilon\|\varphi\|_{k_1}) = \int_{\mathbb{T}} \varphi\, dx + \int_{\mathbb{T}} (\overline{U}\bar{\zeta})\varphi'\, dx + O(\varepsilon^2\|\varphi\|_{k_2}),$$

where $k_1 = 2\sigma + 3$, $k_2 = 4\sigma + 6$, $\bar{\zeta} = \mathbb{E}[\zeta \circ r_{-\alpha}]$ and $\varepsilon = \mathbb{E}[\|\zeta\|_{k_1}^2]^{1/2}$.

(As before, $O(M)$ is a notation for a quantity bounded by CM, where C is a constant depending only on A and σ.)

Proof. To prove the first equality of the statement, we start from the Taylor formula of order 0: $\varphi \circ f = \varphi \circ r_\alpha + O(\|\zeta\|_0\|\varphi\|_1)$ and we take the expectation, so

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

Then we use the invariance of μ:

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

https://doi.org/10.1017/etds.2021.22 Published online by Cambridge University Press

For ψ in $C^{2\sigma+3}(\mathbb{T})$, we apply the previous formula to $\varphi = U\psi$ and we get, thanks to Lemma 2.1 with $k = 1$,

$$\int_{\mathbb{T}} \psi \, d\mu = \int_{\mathbb{T}} \psi \, dx + O(\varepsilon \|\psi\|_{2\sigma+3}). \tag{6}$$

That gives the first equality.

To prove the second equality of the statement, we use this time a Taylor formula of order 1:

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

Using the invariance of μ, the first estimate (6) and the inequality $\|uv\|_k \leq 2^k \|u\|_k \|v\|_k$ (a consequence of the Leibniz formula), we get

$$\begin{aligned}\int_{\mathbb{T}} (\varphi - T_0\varphi)\, d\mu &= \int_{\mathbb{T}} \mathbb{E}[(\varphi' \circ r_\alpha)\zeta]\, d\mu + O(\varepsilon^2 \|\varphi\|_2) \\ &= \int_{\mathbb{T}} \mathbb{E}[(\varphi' \circ r_\alpha)\zeta]\, dx + O(\varepsilon^2 \|\varphi\|_2 + \varepsilon \|\mathbb{E}[(\varphi' \circ r_\alpha)\zeta]\|_{2\sigma+3}) \\ &= \int_{\mathbb{T}} \varphi' \bar{\zeta}\, dx + O(\varepsilon^2 \|\varphi\|_{2\sigma+4}).\end{aligned}$$

As before, for ψ in $C^{4\sigma+5}(\mathbb{T})$, we take $\varphi = U\psi$ to get, thanks to Lemma 2.1 with $k = 2\sigma + 4$,

$$\begin{aligned}\int_{\mathbb{T}} \psi\, d\mu &= \int_{\mathbb{T}} \psi\, dx + \int_{\mathbb{T}} (U\psi)' \bar{\zeta}\, dx + O(\varepsilon^2 \|U\psi\|_{2\sigma+4}) \\ &= \int_{\mathbb{T}} \psi\, dx + \int_{\mathbb{T}} \psi' (\overline{U}\bar{\zeta})\, dx + O(\varepsilon^2 \|\psi\|_{4\sigma+6}).\end{aligned}$$ □

Remark 3.1. We got that μ can be approximated by the density $h_0 = 1$ with accuracy ε, and by the density $h_1 = 1 - \overline{U}\bar{\zeta}'$ with accuracy ε^2 (omitting the detail of the C^k-norms involved). We can easily generalize the method to have higher accuracy. Once having defined an approximation h_{n-1} with accuracy ε^{n-1}, we write $T\varphi = T_0\varphi + T_1\varphi + \cdots + T_{n-1}\varphi + O(\varepsilon^n \|\varphi\|)$, where $T_k\varphi = (1/k!)\mathbb{E}[(\varphi^{(k)} \circ r_\alpha)\zeta^k]$. By a computation similar to the one in the proof, we get $\int (\varphi - T_0\varphi)\, d\mu = \sum_{k=1}^{n-1} \int_{\mathbb{T}} \varphi \overline{T_k} h_{n-k}\, dx + O(\varepsilon^n \|\varphi\|)$, where $\overline{T_k}\varphi = (-1^k/k!)\mathbb{E}[(\varphi^{(k)}\zeta^k) \circ r_\alpha^{-1}]$. Then we apply this to $\varphi = U\psi$ and we obtain that the density $h_n = 1 + \sum_{k=1}^{n-1} \overline{U}\, \overline{T_k} h_{n-k}$ approximates μ with accuracy ε^n.

3.2. *Estimate of the Lyapunov exponents.* Thanks to Proposition 3.1, we can estimate the Lyapunov exponents of f.

PROPOSITION 3.2. *Let $k_0 = 4\sigma + 7$. If μ is a stationary probability for f and λ is the associated Lyapunov exponent, then*

$$\lambda = -\frac{1}{2}\mathbb{E} \int_{\mathbb{T}} (\zeta' - (\overline{U}\bar{\zeta})' \circ r_\alpha + (\overline{U}\bar{\zeta})')^2\, dx + O(\varepsilon^3),$$

where $\bar{\zeta} = \mathbb{E}[\zeta \circ r_{-\alpha}]$ and $\varepsilon = \mathbb{E}[\|\zeta\|_{k_0}^3]^{1/3}$.

This will conclude the proof of Theorem 1, setting $\eta = \overline{U}\bar{\zeta}$.

https://doi.org/10.1017/etds.2021.22 Published online by Cambridge University Press

Proof. Let $\eta = \overline{U}\bar{\zeta}$, $g = \mathrm{Id} - \eta$, $\tilde{f} = gfg^{-1}$ ($\|\eta\|_1 = O(\varepsilon)$, so g is invertible if ε is small enough), $\tilde{\zeta} = \tilde{f} - r_\alpha$ and $\tilde{\mu} = g_*\mu$. If φ is in $C^{4\sigma+5}(\mathbb{T})$, then, thanks to Proposition 3.1, writing $\varphi \circ g = \varphi - \varphi'\eta + O(\varepsilon^2)$, we have, keeping the notation $k_1 = 2\sigma + 3$ and $k_2 = 4\sigma + 6$,

$$\begin{aligned}\int_{\mathbb{T}} \varphi \, d\tilde{\mu} &= \int_{\mathbb{T}} \varphi \circ g \, d\mu \\ &= \int_{\mathbb{T}} \varphi \, d\mu - \int_{\mathbb{T}} \varphi'\eta \, d\mu + O(\varepsilon^2 \|\varphi\|_2) \\ &= \bigg(\int_{\mathbb{T}} \varphi \, dx + \int_{\mathbb{T}} \varphi'\eta \, dx \bigg) - \int_{\mathbb{T}} \varphi'\eta \, dx + O(\varepsilon^2 \|\varphi\|_{k_2} + \varepsilon \|\eta\|_{k_1} \|\varphi'\|_{k_1}) \\ &= \int_{\mathbb{T}} \varphi \, dx + O(\varepsilon^2 \|\varphi\|_{k_2}),\end{aligned}$$

where we used Lemma 2.1 to get $\|\eta\|_{k_1} = O(\|\bar{\zeta}\|_{k_1+2\sigma+2}) = O(\varepsilon)$. Thus, $\tilde{\mu}$ is 'ε^2-close' to Lebesgue measure.

The Lyapunov exponent λ of f associated to μ is equal to the Lyapunov exponent of $\tilde{f}$ associated to $\tilde{\mu}$ (this invariance of Lyapunov exponent under conjugation follows by taking the expectation and integrating with respect to μ the equality $\ln((gfg^{-1})') \circ g = \ln f' + (\ln g' \circ f - \ln g')$). We use this fact and the previous computation to estimate λ. We also use that by Proposition 2.2, $\|\tilde{\zeta}\|_k = O(\|\zeta\|_k + \|\eta\|_k)$ and that, by Proposition 2.4, $\tilde{\zeta}' = (\zeta' - \eta' \circ r_\alpha + \eta') + R$ with $\mathbb{E}[R^2]^{1/2} = O(\varepsilon^2)$. Then

$$\begin{aligned}\lambda &= \mathbb{E} \int_{\mathbb{T}} \ln(1 + \tilde{\zeta}') \, d\tilde{\mu} \\ &= \mathbb{E} \int_{\mathbb{T}} (\tilde{\zeta}' - \tilde{\zeta}'^2/2) \, d\tilde{\mu} + O(\varepsilon^3) \\ &= \mathbb{E} \int_{\mathbb{T}} (\tilde{\zeta}' - \tilde{\zeta}'^2/2) \, dx + O(\varepsilon^3) \\ &= -\frac{1}{2} \mathbb{E} \int_{\mathbb{T}} \tilde{\zeta}'^2 \, dx + O(\varepsilon^3) \\ &= -\frac{1}{2} \mathbb{E} \int_{\mathbb{T}} (\zeta' - \eta' \circ r_\alpha + \eta')^2 \, dx + O(\varepsilon^3). \qquad \square\end{aligned}$$

Remark 3.2. A quicker way to obtain an estimate of λ is to skip the construction of the conjugacy g and to directly expand $\mathbb{E} \int \ln f'(x) \, d\mu(x)$ by using Proposition 3.1. The method we used has two advantages, though: it makes appear a main term clearly non-positive in the expansion of λ, and in the context of Theorem 2 the conjugation by g will be the first step of the KAM scheme in order to conjugate f to a diffeomorphism closer to rotations.

4. *Proof of Theorem 2*

4.1. *Preliminaries.*

We begin by introducing some convenient notation: if u is a random variable valued in $C^k(\mathbb{T})$, we set

$$|||u|||_k = \mathbb{E}[\|u\|_k^2].$$

https://doi.org/10.1017/etds.2021.22 Published online by Cambridge University Press

To avoid the profusion of constants, if k is an integer, we write $X \ll_k Y$ if $X \leq CY$ with C a constant depending only on A, σ and k, or simply $X \ll Y$ if C depends only on A and σ.

Another important tool is the smoothing operators, allowing us to fix the loss of derivative phenomenon which will occur in the KAM scheme. Here we are going to simply use Fourier truncation, which does not give the optimal estimates but is sufficient for our purpose. So, for $\varphi : \mathbb{T} \to \mathbb{R}$ and $T \geq 0$, we denote

$$\begin{cases} S_T\varphi(x) = \displaystyle\sum_{|p|\leq T} \hat{\varphi}(p)e^{2i\pi px}, \\ R_T\varphi(x) = \displaystyle\sum_{|p|> T} \hat{\varphi}(p)e^{2i\pi px}. \end{cases}$$

Then we have the standard Fourier estimates.

PROPOSITION 4.1. *For any integers j and k with $j < k$, we have*

$$\begin{cases} \text{for all } \varphi \in C^j(\mathbb{T}), & \|S_T\varphi\|_k \ll_k T^{k-j+1}\|\varphi\|_j, \\ \text{for all } \varphi \in C^k(\mathbb{T}), & \|R_T\varphi\|_j \ll_k \dfrac{\|\varphi\|_k}{T^{k-j-1}}. \end{cases} \tag{7}$$

4.2. *First conjugation.* In this section we fix a random diffeomorphism $f = r_\alpha + \zeta$ with $\alpha = \rho(f)$ diophantine of type (A, σ), and λ a Lyapunov exponent of f associated to some stationary measure μ. We assume that f is valued in the open set

$$\mathcal{U}_0 = \left\{h \in \mathrm{Diff}^1_+(\mathbb{T}), |h' - 1| < \tfrac{1}{2}\right\}.$$

In other words, $\mathcal{U}_0$ is the $\frac{1}{2}$-neighbourhood of the set of rotations in $\mathrm{Diff}^1_+(\mathbb{T})$.

LEMMA 4.1. *Let $k_0 = 4\sigma + 7$ and $r = 2\sigma + 2$. There exists $C_0 > 0$ depending only on A and σ so that f is conjugated by a deterministic diffeomorphism $g = \mathrm{Id} - \eta$ to $\tilde{f} = gfg^{-1} = r_\alpha + \tilde{\zeta}$ such that either*

$$|||\tilde{\zeta}|||_0 \leq 3|\lambda|^{1/2} \quad \text{or} \quad |||\tilde{\zeta}|||_0 \leq C_0|||\zeta|||_{k_0}^{3/2},$$

with η satisfying that for any integer $K \geq r$,

$$\|\eta\|_{K-r} \ll_K |||\zeta|||_K.$$

Proof. We begin with the same setting as in Proposition 3.2. First we set $\eta = \overline{U\zeta}$, which satisfies the inequality $\|\eta\|_{K-r} \ll_K |||\zeta|||_K$ by Lemma 2.1. In particular, $\|\eta\|_1 \ll |||\zeta|||_{k_0}$, so we can assume that $|||\zeta|||_{k_0}$ is small enough so that $\|\eta\|_1 < 1/7$ (if not, then $g = \mathrm{Id}$ satisfies the conclusion of the statement). Then we set $g = \mathrm{Id} - \eta$, which is invertible, $\tilde{f} = gfg^{-1}$, $\tilde{\zeta} = \tilde{f} - r_\alpha$ and $\tilde{\mu} = g_*\mu$.

Now we follow the computation of the proof of Proposition 3.2 with one slight difference: we cannot expand $\ln(1 + \tilde{\zeta}')$ at order 3 because we do not have a good bound for the third moment of $\|\zeta\|_1$. Instead we use that for every t in $]-1, 1[$, we have

https://doi.org/10.1017/etds.2021.22 Published online by Cambridge University Press

$\ln(1+t) \leq t - \frac{1}{4}t^2$. We can apply this inequality to $t = \tilde{\zeta}'$ because $f \in \mathcal{U}_0$, so

$$\tilde{f}' \leq \sup(f')(\sup(g')/\inf(g')) < (1+\tfrac{1}{2})\frac{1+1/7}{1-1/7} = 2$$

and so $-1 < \tilde{\zeta}' < 1$. We get

$$\lambda = \mathbb{E}\int_{\mathbb{T}} \ln(1+\tilde{\zeta}')\, d\tilde{\mu} \leq \mathbb{E}\int_{\mathbb{T}} (\tilde{\zeta}' - \tilde{\zeta}'^2/4)\, d\tilde{\mu} = -\frac{1}{4}\int_{\mathbb{T}} \tilde{\zeta}'^2\, dx + O(|||\zeta|||_{k_0}^2)$$

and hence there exists C depending only on A and σ such that

$$\mathbb{E}\int_{\mathbb{T}} \tilde{\zeta}'^2\, dx \leq 4|\lambda| + C|||\zeta|||_{k_0}^3.$$

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 we get

$$|||\tilde{\zeta}|||_0 \leq (4|\lambda| + C|||\zeta|||_{k_0}^3)^{1/2} \leq (\max(8|\lambda|, 2C|||\zeta|||_{k_0}^3))^{1/2} = \max(3|\lambda|^{1/2}, \sqrt{2C}|||\zeta|||_{k_0}^{3/2}),$$

which concludes the proof with $C_0 = \sqrt{2C}$. □

In view of the dichotomy given by this lemma, we will say that 'λ is an obstruction for the linearization of f' if $|\lambda|^{1/2} \geq C_0/3|||\zeta|||_{k_0}^{3/2}$, where C_0 and k_0 are defined in the lemma. Thus, if λ is an obstruction, then one can find a conjugacy as stated in Theorem 2 and, if it is not an obstruction, then f is conjugated to a new random diffeomorphism $\tilde{f}$ closer to r_α and we can hope to iterate the process. However, we cannot directly use the lemma in an iterating process because of the loss of regularity in the inequality $|||\tilde{\zeta}|||_0 \leq C_0|||\zeta|||_{k_0}^{3/2}$. We fix that by replacing the conjugation g by a good C^∞ approximation. In that way, there will be no loss of regularity any more (at the cost of a less sharp bound). Precisely, we have the following result.

LEMMA 4.2. *Let $k_0 = 4\sigma + 7$ and $r = 6\sigma + 11$. If λ is not an obstruction for f, then, for any $T \geq 1$, f is conjugated by a diffeomorphism $g_T = \mathrm{Id} - \eta_T$ to $\tilde{f}_T = g_T f g_T^{-1} = r_\alpha + \tilde{\zeta}_T$ such that*

$$\text{for all } K \geq r, \quad \begin{cases} |||\tilde{\zeta}_T|||_{k_0} \ll_K T^r|||\zeta|||_{k_0}^{3/2} + \dfrac{1}{T^{K-r}}|||\zeta|||_K, \\ |||\tilde{\zeta}_T|||_K \ll_K T^r|||\zeta|||_K. \end{cases}$$

Moreover,

$$\text{for all } K \geq r, \quad \|\eta_T\|_{K-r} \ll_K |||\zeta|||_K.$$

Proof. Let $k_0 = 4\sigma + 7$ and $s = 2\sigma + 2$. Let $g = \mathrm{Id} - \eta$ be the diffeomorphism given by Lemma 4.1. We set $\eta_T = S_T\eta$ and $g_T = \mathrm{Id} - \eta_T$. By Lemma 4.1 and Proposition 4.1, we have for $K \geq s+1$,

$$\|\eta_T\|_{K-(s+1)} \ll_K \|\eta\|_{K-s} \ll_K |||\zeta|||_K. \tag{8}$$

Applying with $K = s + 2 \leq k_0$, we have $\|\eta\|_1 \ll |||\zeta|||_{k_0}$, so we can assume that $|||\zeta|||_{k_0}$ is small enough so that $\|\eta\|_1 \leq \frac{1}{2}$ (if not, we set instead $g_T = \mathrm{Id}$). Then g_T is invertible and we can set $f_T = g_T f g_T^{-1} = r_\alpha + \zeta_T$. We also have for any $K \geq s+1$,

$$\|\eta_T\|_K \ll_K T^{s+1}\|\eta\|_{K-s} \ll_K T^{s+1}|||\zeta|||_K,$$

so, by Proposition 2.2,

$$|||\tilde{\zeta}_T|||_K \ll_K |||\zeta|||_K + \|\eta_T\|_K \ll_K T^{s+1}|||\zeta|||_K. \tag{9}$$

On the other hand, since λ is assumed not to be an obstruction for f, we have, by Lemma 4.1,

$$|||gfg^{-1} - r_\alpha|||_0 \ll |||\zeta|||_{k_0}^{3/2}$$

and, by Proposition 2.3,

$$|||g_T f g_T^{-1} - gfg^{-1}|||_0 \ll \|g_T - g\|_0 = \|R_T \eta\|_0 \ll_K \frac{1}{T^{K-s-1}}\|\eta\|_{K-s} \ll_K \frac{1}{T^{K-s-1}}|||\zeta|||_K.$$

The combination of the two last inequalities gives

$$|||\tilde{\zeta}_T|||_0 = |||g_T f g_T^{-1} - r_\alpha|||_0 \ll_K |||\zeta|||_{k_0}^{3/2} + \frac{1}{T^{K-s-1}}|||\zeta|||_K. \tag{10}$$

Finally, we write $\tilde{\zeta}_T = S_T\tilde{\zeta}_T + (\tilde{\zeta}_T - S_T\tilde{\zeta}_T)$ to use Proposition 4.1 and then by using (9) and (10) we get

$$|||\tilde{\zeta}_T|||_{k_0} \ll_K T^{k_0+1}|||\tilde{\zeta}_T|||_0 + \frac{1}{T^{K-k_0-1}}|||\tilde{\zeta}_T|||_K \ll_K T^{k_0+1}|||\zeta|||_{k_0}^{3/2} + \frac{1}{T^{K-k_0-s-2}}|||\zeta|||_K. \tag{11}$$

Thus, with $r = k_0 + s + 2 = 6\sigma + 11$, (8), (9) and (11) give all the estimates claimed in the statement. □

4.3. *KAM iteration.* Now we begin the KAM scheme by iterating the conjugation process given by Lemma 4.2. We fix the numbers k_0 and r given by Lemma 4.2, and we fix a sequence of numbers $(T_n)_{n\in\mathbb{N}}$. We initialize the construction with $f_0 = f$, $\zeta_0 = \zeta$. Then, assuming that $f_{n-1} = r_\alpha + \zeta_{n-1}$ is defined, if we have the two conditions:

(1) $f_{n-1} \in \mathcal{U}_0$ a.s.;

(2) λ is not an obstruction for f_{n-1}, that is, $|\lambda|^{1/2} \leq C_0/3|||\zeta_{n-1}|||_{k_0}^{3/2}$,

then Lemma 4.2 applies, so that by choosing $T = T_n$ we get a conjugation $g_{n-1} = \mathrm{Id} - \eta_{n-1}$ and a random diffeomorphism $f_n = g_{n-1}f_{n-1}g_{n-1}^{-1} = r_\alpha + \zeta_n$ satisfying for $K \geq r$

$$\begin{cases} |||\zeta_n|||_K \ll_K T_n^r|||\zeta_{n-1}|||_K, \\[2ex] |||\zeta_n||n|_{k_0} \ll_K T_n^r|||\zeta_{n-1}|||_{k_0}^{\frac{3}{2}} + \dfrac{1}{T_n^{K-r}}|||\zeta_{n-1}|||_K \end{cases}$$

and

$$\|\eta_{n-1}\|_{K-r} \ll_K T_n^r|||\zeta_{n-1}|||_K.$$

If one of the two conditions is not satisfied, then we stop the process. Thus, we get a sequence of random diffeomorphisms $(f_n)_{n<N}$, where $N \in \mathbb{N}\cup\{+\infty\}$.

We choose T_n as follows: $T_n = 2^{Q^n}$, where Q is any number in $(1, \frac{3}{2})$. With this choice, we prove that the large C^k-norms of ζ do not blow up too fast while the small C^k-norms decrease quickly. Note that in the following we consider Q as fixed, for example, $Q = \frac{4}{3}$, so we will not explicitly state the dependence of the constants on Q.

LEMMA 4.3. *There exist integers p and K_0 depending only on σ such that for any $K \geq K_0$, if $\varepsilon = |||\zeta|||_K$ is small enough, then, for any $n < N$,*

$$\begin{cases} |||\zeta_n|||_K \ll_K T_n^p \varepsilon, \\ |||\zeta_n|||_{k_0} \ll_K \dfrac{1}{T_n^{K-p}} \varepsilon. \end{cases}$$

Proof. There exists a constant C depending only on A, σ and K such that for any $n < N$,

$$\begin{cases} |||\zeta_n|||_K \leq C T_n^r |||\zeta_{n-1}|||_K, \\ |||\zeta_n|||_{k_0} \leq C\left(T_n^r |||\zeta_{n-1}|||_{k_0}^{3/2} + \dfrac{1}{T_n^{K-r}} |||\zeta_{n-1}|||_K \right). \end{cases}$$

By iteration of the first inequality we have for any $n \geq 1$,

$$|||\zeta_n|||_K \leq C^n (T_n \cdots T_1)^r |||\zeta_0|||_K \leq C^n 2^{r(Q+Q^2+\cdots+Q^n)} \varepsilon \leq C^n 2^{(rQ/(Q-1))Q^n} \varepsilon$$

and hence $|||\zeta_n|||_K \ll_K T_n^s \varepsilon$, where $s = (2rQ/(Q-1))$. That proves the first part of the statement if $p \geq s$.

Let $\varepsilon_n = |||\zeta_n|||_{k_0}$. Using in the second inequality that $|||\zeta_{n-1}|||_K \ll_K T_n^s \varepsilon$, we obtain, up to modifying the constant C,

$$\varepsilon_n \leq C\left(T_n^r \varepsilon_{n-1}^{3/2} + \frac{1}{T_n^{K-p}} \varepsilon \right),$$

where we have set $p = r + s$. If K is large enough and ε small enough, we are going to prove by induction that for every $n < N$,

$$\varepsilon_n \leq \frac{2C\varepsilon}{T_n^{K-p}}. \tag{12}$$

It holds for $n = 0$ if $C \geq 2^K$, which we can assume up to changing C one more time. Now, for $n < N$, let us assume that $\varepsilon_{n-1} \leq (2C\varepsilon/(T_{n-1}^{K-p}))$. Then if ε is small enough, we have

$$\varepsilon_{n-1}^{3/2} \leq \frac{1}{T_{n-1}^{3/2(K-p)}} (2C\varepsilon)^{3/2} \leq \frac{1}{T_n^{3/2Q(K-p)}} \varepsilon$$

and so

$$\varepsilon_n \leq C\varepsilon \left(\frac{1}{T_n^{(3/2Q)(K-p)-r}} + \frac{1}{T_n^{K-p}} \right),$$

which implies that

$$\varepsilon_n \leq \frac{2C\varepsilon}{T_n^{K-p}}$$

provided that $3/2Q(K-p) - r \geq K - p$ or equivalently (since $3/2Q > 1$)

$$K \geq p + s \frac{1}{(3/2Q) - 1}.$$

If it is satisfied, then (12) is proved by induction for any $n < N$. That concludes the proof of the lemma, choosing $K_0 = \lceil p + s(1/(3/2Q) - 1)\rceil$. □

In the following we fix the integer K_0 given by Lemma 4.3, and an integer $K \geq K_0$.

LEMMA 4.4. *There exists q depending only on σ such that if $\varepsilon = |||\zeta|||_K$ is small enough, then, for any $n < N$, $|||\zeta_n|||_{K-q} \ll_K (1/T_n)\varepsilon$ and $\|\eta_n\|_{K-q} \ll_K (1/T_n)\varepsilon$.*

Proof. Let p be as in the previous lemma and let $K \geq K_0$. If ε is small enough, we have $|||\zeta_n|||_K \ll_K T_n^p\varepsilon$ and $|||\zeta_n|||_0 \ll_K (1/T_n^{K-p})\varepsilon$, so by the Kolomogorov inequality (Proposition 2.1), for any $k \leq K$, we have

$$|||\zeta_n|||_{K-k} \ll_K |||\zeta_n|||_0^{k/K}\,|||\zeta_n||n|_K^{K-k/K} \ll_K \frac{\varepsilon}{T_n^\tau}$$

with

$$\tau = \frac{k}{K}(K-p) - \left(\frac{K-k}{K}\right)p = k - p.$$

In particular, $|||\zeta_n|||_{K-q} \ll_K (1/T_n)\varepsilon$ if $q \geq p+1$, and $\|\eta_n\|_{K-q} \ll_K |||\zeta_n|||_{K-q+r} \ll_K (1/T_n)\varepsilon$ if $q - r \geq p + 1$. So, we get the result with $q = p + 1 + r$. □

Now we consider the compositions $h_n = g_{n-1} \circ \cdots \circ g_0$, so that $f_n = h_n f h_n^{-1}$. The diffeomorphisms h_n satisfy the following estimates.

LEMMA 4.5. *Let q be as in the previous lemma. If $\varepsilon = |||\zeta|||_K$ is small enough, then, for any $n < N$, $d_{K-q}(h_n, \mathrm{Id}) \ll_k \varepsilon$ and $\sum_{n<N} d_{K-q}(h_n, h_{n-1}) \ll_K \varepsilon$.*

Proof. Let $\delta_n = d_{K-q}(h_n, \mathrm{Id})$. For a fixed n, let us assume that $\delta_j \leq 1$ for $j = 0, \ldots, n-1$. Then, by Proposition 2.5 and Lemma 4.4,

$$d_{K-q}(h_n, h_{n-1}) \ll_K d_{K-q}(g_n, \mathrm{Id}) \ll_K \frac{\varepsilon}{T_n}$$

and so

$$\delta_n \leq \sum_{j<n} d_{K-q}(h_j, h_{j-1}) \ll_K \varepsilon.$$

So, if ε is small enough, we get $\delta_n \leq 1$. Thus, we get by induction that for all $n < N$, $\delta_n \leq 1$. In particular, the estimates above hold for every n and the result follows. □

We are now ready to finish the proof of Theorem 2.

Proof of Theorem 2. We fix K_0 and q as above, an integer $K \geq K_0$, we assume that $\varepsilon = |||\zeta|||_K$ is small enough so that the lemmas above apply and we also assume that $|f' - 1| \leq \frac{1}{4}$. We separate the cases $N = +\infty$ and $N < +\infty$.

- If $N = +\infty$, then $\sum_n d_{K-q}(h_n, h_{n-1}) \ll_K \varepsilon$ and hence $(h_n)_{n\in\mathbb{N}}$ converges in $\mathrm{Diff}_+^{K-q}(\mathbb{T})$ to a limit h satisfying $d_{K-q}(h, \mathrm{Id}) \ll_K \varepsilon$. In particular, if ε is small enough, h is invertible and $hfh^{-1} = \lim_n h_n f h_n^{-1} = \lim_n f_n = r_\alpha$ almost surely.

https://doi.org/10.1017/etds.2021.22 Published online by Cambridge University Press

- If $N < +\infty$, then $f_{N-1} = h_{N-1} f h_{N-1}^{-1}$ with $d_{K-q}(h_{N-1}, \mathrm{Id}) \ll_K \varepsilon$. Moreover, one of the two conditions stated at the beginning of the section does not hold for f_{N-1}, that is, either $f_{N-1} \notin \mathcal{U}_0$ or λ is an obstruction for f_{N-1}. Since $|f' - 1| \leq \frac{1}{4}$ and $|h'_{N-1} - 1| \ll_K \varepsilon$, we deduce that the condition $f_{N-1} \in \mathcal{U}_0$ is satisfied if ε is small enough. So, it means that λ is an obstruction for f_{N-1}, that is, $|\lambda|^{1/2} \geq (C_0/3)\varepsilon_n^{3/2}$. Then Lemma 4.1 gives a diffeomorphism g satisfying $d_{K-q}(g, \mathrm{Id}) \ll_K \varepsilon$ conjugating f_{N-1} to $\tilde{f} = r_\alpha + \tilde{\zeta}$ such that $|||\tilde{\zeta}|||_0 \leq 3|\lambda|^{1/2}$ and then the conjugation $h = g \circ h_{N-1}$ satisfies the conclusion of Theorem 2.

Choosing $\overline{\varepsilon}$ in $(0, \frac{1}{2})$ so that the lemmas above and the final argument apply for $|||\zeta|||_K \leq \overline{\varepsilon}$, we get the conclusion of Theorem 2 for any random diffeomorphism f such that $\rho(f)$ is (A, σ)-diophantine and valued in the open set

$$\mathcal{U} = \left\{ h \in \mathrm{Diff}_+^K(\mathbb{T}), d_K(h, \mathcal{R}) < \frac{\overline{\varepsilon}}{2} \right\},$$

where $\mathcal{R}$ is the set of rotations: for such an f, we obviously have $|f' - 1| \leq \frac{1}{4}$, and $d_K(f, r_\beta) < (\overline{\varepsilon}/2)$ for some β, so actually $|\beta - \alpha| < (\overline{\varepsilon}/2)$ with $\alpha = \rho(f)$, so $d_K(f, r_\alpha) < \overline{\varepsilon}$ and in particular $|||\zeta|||_K \leq \overline{\varepsilon}$. Hence, the argument above applies to f and gives the conjugation stated in Theorem 2. □

5. *Random products of matrices (Theorems 3 and 4)*

5.1. *Generalities.* We consider $\mathcal{M}_2(\mathbb{R})$ equipped with any norm $\|\cdot\|$. By identifying the complex plane with $\mathbb{R}^2$, any matrix M in $\mathcal{M}_2(\mathbb{R})$ naturally acts on $\mathbb{C}$.

We denote by $\mathcal{T}$ the space of trigonometric polynomials $p : \mathbb{T} \to \mathbb{R}$, generated by the maps $x \mapsto \cos(2k\pi x)$ and $x \mapsto \sin(2k\pi x)$. We denote by $\mathcal{T}_n$ the space of trigonometric polynomials of $\mathcal{T}$ of degree at most n. We fix a norm $\|\cdot\|$ on $\mathcal{T}$.

To any M in $\mathrm{GL}_2(\mathbb{R})$ we naturally associate a diffeomorphism f_M of $\mathbb{T}$ by

$$e^{i\pi f_M(x)} = \frac{M(e^{i\pi x})}{|M(e^{i\pi x})|}.$$

We admit the following elementary lemma.

LEMMA 5.1. *There exists a constant $A_0 > 0$ depending only on the norm on $\mathcal{M}_2(\mathbb{R})$ such that for any M in $\mathrm{SL}_2(\mathbb{R})$ and α in $\mathbb{T}$,*

$$\frac{1}{A_0} d_0(f_M, r_\alpha) \leq \|M - R_\alpha\| \leq A_0 d_0(f_M, r_\alpha).$$

In particular, if M is a perturbation of R_α of order ε, then f_M is a perturbation of r_α of order ε. The next lemma specifies the form of the perturbation.

LEMMA 5.2. *If $M = R_\alpha + E$, then, writing $f_M = r_\alpha + \zeta$, we can write $\zeta = \zeta_1 + \zeta_2 + \zeta_3$, where $\zeta_1 \in \mathcal{T}_1$ and $\|\zeta_1\| = O(\|E\|)$, $\zeta_2 \in \mathcal{T}_2$ and $\|\zeta_2\| = O(\|E\|^2)$, $\zeta_3 \in C^\infty(\mathbb{T})$ and $\|\zeta_3\|_1 = O(\|N\|^3)$. Moreover,*

$$\zeta_1(x) = \frac{1}{\pi} \mathrm{Im}(E(e^{i\pi x}) e^{-i\pi(x+\alpha)}).$$

https://doi.org/10.1017/etds.2021.22 Published online by Cambridge University Press

Proof. From $e^{i\pi f_M(x)} = M(e^{i\pi x})/|M(e^{i\pi x})|$, we obtain the formula

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

where the (complex) logarithm is well defined for $\|E\|$ small. Then the result follows by doing Taylor expansions. □

The following lemma is a counterpart of the previous lemma when $\alpha = 0$ that we will use to create a conjugation matrix in the proof of Theorem 4.

LEMMA 5.3. *If ζ belongs to $\mathcal{T}_1$, then one can find M in* $\mathrm{SL}_2(\mathbb{R})$ *such that $\|M - I_2\| = O(\|\zeta\|)$ and*

$$f_M(x) = x + \zeta(x) + O(\|\zeta\|^2).$$

Proof. By assumption, $\zeta(x) = A + B\cos(2\pi x) + C\sin(2\pi x)$ for some A, B, C. Let us set $M = I_2 + E$ with $E = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, where a, b, c have to be chosen, and d is determined so that $\det M = 1$. Since $\det(M) = 1 + \mathrm{Tr}(E) + O(\|E\|^2)$, in particular $d = -a + O(\|E\|^2)$. From Lemma 5.2 and a simple computation, we have

$$\begin{aligned} f_M(x) &= x + \frac{1}{\pi} + \mathrm{Im}(E(e^{i\pi x})e^{-i(\pi x+\alpha)}) + O(\|E\|^2) \\ &= x + \frac{c-b}{\pi} + \frac{c+b}{\pi}\cos(2\pi x) + \frac{d-a}{\pi}\sin(2\pi x) + O(\|E\|^2) \\ &= x + \frac{c-b}{\pi} + \frac{c+b}{\pi}\cos(2\pi x) - \frac{2a}{\pi}\sin(2\pi x) + O(\|E\|^2). \end{aligned}$$

By choosing a, b, c so that $c - b = \pi A$, $c + b = \pi B$ and $-2a = \pi C$, we obviously have $\|E\| = O(\|\zeta\|)$ and so $f_M(x) = x + \zeta(x) + O(\|\zeta\|^2)$. □

LEMMA 5.4. *Let M be a random matrix in* $\mathrm{SL}_2(\mathbb{R})$ *with $\mathbb{E}[\ln_+ \|M\|] < +\infty$, and let Λ be the Lyapunov exponent of M. Then there exists a stationary measure μ of the random diffeomorphism f_M so that the corresponding Lyapunov exponent $\lambda(\mu)$ satisfies $\Lambda = -\frac{1}{2}\lambda(\mu)$.*

Proof. Since $M \in \mathrm{SL}_2(\mathbb{R})$, we have for every θ and θ' in $\mathbb{T}$,

$$\det(M(e^{i\pi\theta}), M(e^{i\pi\theta'})) = \det(e^{i\pi\theta}, e^{i\pi\theta'})$$

that we can rewrite as

$$|\sin(\pi(\theta - \theta'))| = |M(e^{i\pi\theta})|\,|M(e^{i\pi\theta'})|\,|\sin(\pi(f_M(\theta) - f_M(\theta')))|,$$

which leads to

$$1 = |M(e^{i\pi\theta})|^2\,|f_M'(\theta)|.$$

It is well known that there exists a stationary measure μ such that we have $\Lambda = \mathbb{E}\int_{\mathbb{T}} \ln|M(e^{i\pi\theta})|\,d\mu(\theta)$ (see, for example, [7]), so the result follows. □

https://doi.org/10.1017/etds.2021.22 Published online by Cambridge University Press

5.2. *Proof of Theorem 3.* We fix a random variable α in $\mathbb{T}$ and a random matrix $M = R_\alpha + E$ of $\mathrm{SL}_2(\mathbb{R})$. We naturally get a random diffeomorphism $f_M = r_\alpha + \zeta$ of $\mathbb{T}$, and Lemma 5.2 gives a decomposition $\zeta = \zeta_1 + \zeta_2 + \zeta_3$.

We assume that α does not belong almost surely to $\{0, \frac{1}{2}\}$. So, $\|d(2\alpha, \mathbb{Z})\|_{L^2(\Omega)} \geq \delta$ for some $\delta > 0$. In the following, a term $O(M)$ means a term bounded by CM with C depending only on δ (and the chosen norms on $\mathcal{T}$ and $\mathcal{M}_2(\mathbb{R})$).

We keep the notation of the previous sections for the operators T, T_0, U and $\overline{U}$, that is to say, $T\varphi(x) = \mathbb{E}[\varphi \circ f_M(x)]$, $T_0\varphi(x) = \mathbb{E}[\varphi \circ r_\alpha(x)]$, $U\varphi(x) = \sum_{q\in\mathbb{Z}^*}(\hat{\varphi}(q)/(1 - \mathbb{E}[e^{2i\pi q\alpha}]))e^{2i\pi qx}$ and $\overline{U}\varphi(x) = \sum_{q\in\mathbb{Z}^*}(\hat{\varphi}(q)/(1 - \mathbb{E}[e^{-2i\pi q\alpha}]))e^{2i\pi qx}$.

LEMMA 5.5. *The operators U and $\overline{U}$ are well defined and bounded on $\mathcal{T}_2$. Moreover, $\|U\|$ and $\|\overline{U}\|$ can be bounded by a constant depending only on δ (and the norm $\|\cdot\|$ on $\mathcal{T}_2$).*

Proof. The operators U and $\overline{U}$ are well defined on $\mathcal{T}_2$ since the denominators $1 - \mathbb{E}[e^{2i\pi q\alpha}]$ do not vanish for $q = -2, -1, 1, 2$ thanks to the assumption that α does not belong almost surely to $\{0, \frac{1}{2}\}$. These operators are automatically bounded since $\mathcal{T}_2$ is finite dimensional. Finally, the uniform bound of $\|U\|$ and $\|\overline{U}\|$ follows from the inequality $|1 - \mathbb{E}[e^{2i\pi q\alpha}]| \geq 8\mathbb{E}[d(q\alpha, \mathbb{Z})^2]$ (obtained in the proof of Lemma 2.1) applied to $q = -2, -1, 1, 2$. □

LEMMA 5.6. *We have*

$$\Lambda = \frac{1}{4}\mathbb{E}\int_{\mathbb{T}}(\zeta_1' + (\overline{U}\bar{\zeta}_1)' - (\overline{U}\bar{\zeta}_1)' \circ r_\alpha)^2\, dx + O(\varepsilon^3),$$

where $\bar{\zeta}_1 = \mathbb{E}[\zeta_1 \circ r_\alpha^{-1}]$ with ζ_1 given by Lemma 5.2 and $\varepsilon = \mathbb{E}[\|E\|^3]^{1/3}$.

Proof. By Lemma 5.4, we have $\Lambda = -\frac{1}{2}\lambda(\mu)$ for some stationary probability measure μ on $\mathbb{T}$. If α is diophantine, the expansion in the statement is a consequence of Proposition 1. We are going to check that the estimate is still valid without the diophantine assumption by mimicking the proof of Proposition 1, noticing that we only need to estimate μ on trigonometric polynomials of small degrees, and so we only need the boundedness of U on $\mathcal{T}_2$ given by Lemma 5.5.

- For every ψ in $\mathcal{T}_2$ with $\varphi = U\psi$ $(\in \mathcal{T}_2)$, we have

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

- For every ψ in $\mathcal{T}_1$ with $\varphi = U\psi$ $(\in \mathcal{T}_1)$, we have

$$\begin{aligned}\int_{\mathbb{T}}\psi\, d\mu - \int_{\mathbb{T}}\psi\, dx &= \int_{\mathbb{T}}(T\varphi - T_0\varphi)\, d\mu \\ &= \int_{\mathbb{T}}\mathbb{E}[(\varphi' \circ r_\alpha)\zeta]\, d\mu + O(\varepsilon^2\|\varphi\|) \\ &= \int_{\mathbb{T}}\mathbb{E}[(\varphi' \circ r_\alpha)\zeta_1]\, dx + O(\varepsilon^2\|\varphi\|)\end{aligned}$$

$$= \int_{\mathbb{T}} \varphi' \bar{\zeta}_1 \, dx + O(\varepsilon^2 \|\varphi\|)$$

$$= \int_{\mathbb{T}} \psi' \overline{U} \bar{\zeta}_1 \, dx + O(\varepsilon^2 \|\psi\|)$$

(for the third equality we used that $(\varphi' \circ r_\alpha)\zeta_1$ belongs to $\mathcal{T}_2$).

- Denoting $\eta = \overline{U}\bar{\zeta}_1$ ($\in \mathcal{T}_1$), $g = \mathrm{Id} - \eta$ and $\tilde{\mu} = g_* \mu$, we have for ψ in $\mathcal{T}_2$,

$$\int_{\mathbb{T}} \psi \, d\tilde{\mu} = \int_{\mathbb{T}} \psi \, d\mu + O(\varepsilon \|\psi\|) = \int_{\mathbb{T}} \psi \, dx + O(\varepsilon \|\psi\|)$$

and, for ψ in $\mathcal{T}_1$,

$$\int_{\mathbb{T}} \psi \, d\tilde{\mu} = \int_{\mathbb{T}} \psi \, d\mu - \int_{\mathbb{T}} \psi' \overline{U} \bar{\zeta}_1 \, d\mu + O(\varepsilon^2 \|\psi\|) = \int_{\mathbb{T}} \psi \, dx + O(\varepsilon^2 \|\psi\|).$$

- Denoting $\tilde{f} = g \circ f_M \circ g^{-1} = r_\alpha + \tilde{\zeta}$ (g is invertible if ε is small enough since $\|\eta\| = O(\varepsilon)$), by using the decomposition $\zeta = \zeta_1 + \zeta_2 + \zeta_3$ and Taylor expansions, we can write $\tilde{\zeta} = \tilde{\zeta}_1 + \tilde{\zeta}_2 + \tilde{\zeta}_3$ with

$$\begin{cases} \tilde{\zeta}_1 = \zeta_1 - \eta \circ r_\alpha + \eta, \ \tilde{\zeta}_1 \in \mathcal{T}_1, \ \|\tilde{\zeta}_1\| = O(\max(\|E\|, \|\eta\|)), \\ \tilde{\zeta}_2 \in \mathcal{T}_2, \ \|\tilde{\zeta}_2\| = O(\max(\|E\|^2, \|\eta\|^2)), \\ \|\tilde{\zeta}_3\|_1 = O(\max(\|E\|^3, \|\eta\|^3)). \end{cases}$$

- We conclude that

$$\begin{aligned} \lambda(\mu) &= \mathbb{E} \int_{\mathbb{T}} \ln \tilde{f}' \, d\tilde{\mu} \\ &= \mathbb{E} \int_{\mathbb{T}} \tilde{\zeta}_1' \, d\tilde{\mu} + \mathbb{E} \int_{\mathbb{T}} \tilde{\zeta}_2' \, d\tilde{\mu} - \frac{1}{2} \mathbb{E} \int_{\mathbb{T}} \tilde{\zeta}_1'^2 \, d\tilde{\mu} + O(\varepsilon^3) \\ &= -\frac{1}{2} \int_{\mathbb{T}} \tilde{\zeta}_1'^2 \, dx + O(\varepsilon^3), \end{aligned}$$

from which the result follows since $\Lambda = -\frac{1}{2}\lambda(\mu)$. □

We can deduce Theorem 3 by a series of simple computations. Starting from the equality $E(e^{i\pi x}) = \frac{1}{2}(Ze^{i\pi x} + Z'e^{-i\pi x})$ with $Z = (a+d) + i(c-b)$ and $Z' = (a-d) + i(b+c)$, we successively obtain (using Lemma 5.2):

- $\zeta_1(x) = (1/\pi)\mathrm{Im}(E(e^{i\pi x})e^{-i\pi(x+\alpha)}) = (1/2\pi)\mathrm{Im}(Ze^{i\pi(2x+\alpha)}) + \text{constant}$;
- $\bar{\zeta}_1(x) = (1/2\pi)\mathrm{Im}(\mathbb{E}[Ze^{-i\pi\alpha}]e^{2i\pi x}) + \text{constant}$;
- $\overline{U}\bar{\zeta}_1(x) = (1/2\pi)\mathrm{Im}((\mathbb{E}[Ze^{-i\pi\alpha}])/(1 - \mathbb{E}[e^{-2i\pi\alpha}])e^{2i\pi x})$;
- $(\zeta_1 + \overline{U}\bar{\zeta}_1 - \overline{U}\bar{\zeta}_1 \circ r_\alpha)(x) = (1/2\pi)\mathrm{Im}(Xe^{2i\pi x}) + \text{constant}$, where $X = Ze^{i\pi\alpha} + ((\mathbb{E}[Ze^{-i\pi\alpha}])/(1 - \mathbb{E}[e^{-2i\pi\alpha}])) - (\mathbb{E}[Ze^{-i\pi\alpha}])/(1 - \mathbb{E}[e^{-2i\pi\alpha}])$ $e^{2i\pi\alpha}$;
- $(\zeta_1' + (\overline{U}\bar{\zeta}_1)' - (\overline{U}\bar{\zeta}_1)' \circ r_\alpha)(x) = \mathrm{Re}(Xe^{2i\pi x})$;
- $$\Lambda = \frac{1}{4}\mathbb{E} \int_{\mathbb{T}} (\zeta_1' + (\overline{U}\bar{\zeta}_1)' - (\overline{U}\bar{\zeta}_1)' \circ r_\alpha)^2 \, dx + O(\varepsilon^3) = \frac{1}{8}\mathbb{E}(|X|^2) + O(\varepsilon^3).$$

The result follows by simply rewriting $\mathbb{E}(|X|^2) = \mathbb{E}(|\overline{X}e^{2i\pi\alpha}|^2)$.

5.3. *Proof of Theorem 4.* We are going to prove Theorem 4 by mimicking the proof of Theorem 2. Let $\delta > 0$ and let M be a random matrix in $\mathrm{SL}_2(\mathbb{R})$ such that $\|\mathrm{Tr}(M)\|_{L^2(\Omega)} \leq 2-\delta$. Let α in $\mathbb{T}$ be so that $d(M,\mathcal{R}) = \|M - R_\alpha\|$, and let $f_M = r_\alpha + \zeta$ be the associated random diffeomorphism of $\mathbb{T}$. We assume that M is valued in the open set

$$\mathcal{U}_0 = \{N \in Sl_2(\mathbb{R}), d(N,\mathcal{R}) < \beta\},$$

where β is a constant depending only on δ and $\|\cdot\|$ chosen so that for M in $\mathcal{U}_0$ we have $|f'_M - 1| \leq \frac{1}{2}$ and $|\mathrm{Tr}(M) - \mathrm{Tr}(R_\alpha)| \leq (\delta/2)$. The second inequality implies that $\|\mathrm{Tr}(R_\alpha)|\|_{L^2(\Omega)} \geq 2-(\delta/2)$ and so $\|d(2\alpha,\mathbb{Z})\|_{L^2(\Omega)} \geq \delta'$ for some positive δ' ($\approx \sqrt{\delta}$) depending on δ, so the techniques used to prove Theorem 3 still work.

Let us construct the first conjugation.

LEMMA 5.7. *There exists P in $\mathrm{SL}_2(\mathbb{R})$ such that either $\|d(PMP^{-1},\mathcal{R})\|_{L^2(\Omega)} \leq 4A_0\Lambda^{1/2}$ or $\|d(PMP^{-1},\mathcal{R})\|_{L^2(\Omega)} \leq C\|d(M,\mathcal{R})\|^{3/2}_{L^2(\Omega)}$, where A_0 is the constant of Lemma 5.1, and C is a constant depending only on δ and the norms. Moreover, $\|P - I_2\| \leq C\|d(M,\mathcal{R})\|_{L^2(\Omega)}$.*

Proof. From the proof of Lemma 5.6, setting $\eta = \overline{U}\overline{\zeta}_1$, $g = \mathrm{Id} - \eta$, $\tilde{f} = gf_Mg^{-1} = r_\alpha + \tilde{\zeta}$ and $\varepsilon = \|d(M,\mathcal{R})\|_{L^2(\Omega)}$, we have

$$\Lambda \geq \frac{1}{8}\int_{\mathbb{T}} \tilde{\zeta}'^2\,dx + O(\varepsilon^3),$$

using that if ε is small enough, $\tilde{f}' < 2$, so $\ln(\tilde{f}') \leq \tilde{\zeta}' - \frac{1}{4}\tilde{\zeta}'^2$. So, there exists a constant C such that

$$\mathbb{E}\int_{\mathbb{T}} \tilde{\zeta}'^2\,dx \leq 8\Lambda + C\varepsilon^3,$$

so

$$\|d_0(\tilde{f}, r_{\tilde{\alpha}})\|_{L^2(\Omega)} \leq 3\Lambda^{1/2} + C^{1/2}\varepsilon^{3/2},$$

where $\tilde{\alpha} = \alpha + \int_{\mathbb{T}} \tilde{\zeta}\,dx$.

By Lemma 5.3, there exists P in $\mathrm{SL}_2(\mathbb{R})$ such that $\|P - I_2\| = O(\varepsilon)$ and $f_P(x) = x - \eta(x) + O(\|\eta\|^2) = g(x) + O(\varepsilon^2)$. Let us set $\widetilde{M} = PMP^{-1}$. Since $d_0(f_P, g) = O(\varepsilon^2)$, we deduce from Proposition 2.3 that $d_0(f_{\widetilde{M}}, \tilde{f}) = d_0(f_Pf_Mf_P^{-1}, gf_Mg^{-1}) = O(\varepsilon^2)$. Hence,

$$\|d_0(f_{\widetilde{M}}, r_{\tilde{\alpha}})\|_{L^2(\Omega)} \leq 3\Lambda^{1/2} + C\varepsilon^{3/2}$$

for some new constant C. So, either $\|d_0(f_{\widetilde{M}}, r_{\tilde{\alpha}})\|_{L^2(\Omega)} \leq 4\Lambda^{1/2}$ or $\|d_0(f_{\widetilde{M}}, r_{\tilde{\alpha}})\|_{L^2(\Omega)} \leq 4C\varepsilon^{3/2}$ and the conclusion follows from the inequality $\|\widetilde{M} - R_{\tilde{\alpha}}\| \leq A_0 d_0(f_{\widetilde{M}}, r_{\tilde{\alpha}})$. □

We can now prove Theorem 4.

Proof of Theorem 4. Let M be a random matrix with Lyapunov exponent Λ. We are going to assume that $d(M,\mathcal{R}) < (\beta/2)$ a.s. (in particular, $M \in \mathcal{U}_0$). We construct a sequence of random matrices $(M_n)_n$ by induction: we set $M_0 = M$; then, for all n in $\mathbb{N}$, if $\|d(M_n,\mathcal{R})\|_{L^2(\Omega)} \leq 4A_0\Lambda^{1/2}$ or if M_n does not belong almost surely to $\mathcal{U}_0$, then we stop the sequence, and if not then we use Lemma 5.7 and set $M_{n+1} = P_nM_nP_n^{-1}$, where P_n is

https://doi.org/10.1017/etds.2021.22 Published online by Cambridge University Press

given by the lemma. Thus, we get a sequence $(M_n)_{n\leq N}$, where N belongs to $\mathbb{N}\cup\{+\infty\}$. Finally, we set $Q_n = P_{n-1}\cdots P_0$, so that $M_n = Q_n M Q_n^{-1}$.

Let $\varepsilon_n = \|d(M_n, \mathcal{R})\|_{L^2(\Omega)}$. Due to invariance under conjugation, the Lyapunov exponent of M_n is Λ. So, from the construction and Lemma 5.7, we deduce that for every $n < N$, $\varepsilon_{n+1} \leq C\varepsilon_n^{3/2}$ and, for every $n \leq N$, $\|P_n - I_2\| \leq C\varepsilon_n$. It is then straightforward that there are a constant C_1 and a positive number $\bar{\varepsilon}$ such that if $\varepsilon_0 \leq \bar{\varepsilon}$, then, for every $n \leq N$, $\varepsilon_n \leq C_1 2^{-(3/2)^n}\varepsilon_0$ and also $\|Q_n - I_2\| \leq C_1\varepsilon_0$, and then that $d(M_n, \mathcal{R}) \leq \beta$, that is, $M_n \in \mathcal{U}_0$ (so the sequence will only stop if $\|d(M_n, \mathcal{R})\|_{L^2(\Omega)} \leq 4A_0\Lambda^{1/2}$).

Two cases can occur.

- If $\Gamma > 0$, then $N < +\infty$. So, $\|d(M_N, \mathcal{R})\|_{L^2(\Omega)} \leq 4A_0\Lambda^{1/2}$ with $M_N = Q_N M Q_N^{-1}$, and $\|Q_N - I_2\| \leq C_1\varepsilon_0$.
- If $\Lambda = 0$, then $N = +\infty$. Since $\|Q_{n+1} - Q_n\| = O(\|Q_n\|\cdot\|P_n - I_2\|) = O(\varepsilon_n)$, (Q_n) converge to some matrix Q such that $\|Q - I_2\| = O(\varepsilon_0)$ and, since $\|d(Q_n M Q_n^{-1}, \mathcal{R})\|_{L^2(\Omega)} = \varepsilon_n \to 0$, we conclude that $QMQ^{-1} \in \mathcal{R}$ almost surely.

Theorem 4 follows. □

A. *Appendix: C^k estimates*

In this section we give a quick proof of the propositions stated in §2 and state some other classical C^k estimates.

In the following propositions we consider maps $f : \mathbb{R} \to \mathbb{R}$. We denote by $\|\cdot\|_\infty$ the supremum norm, that is, $\|f\|_\infty = \sup_{\mathbb{R}} |f|$.

PROPOSITION A.1. (Kolmogorov inequality) *For any integers $j \leq k$ and for any f in $C^k(\mathbb{R})$,*

$$\|f^{(j)}\|_\infty \leq C\|f^{(k)}\|_\infty^{j/k}\|f\|_\infty^{1-j/k},$$

where C is a constant depending only on k.

Proof. Being given real numbers x and h, the Taylor–Lagrange formula gives the existence of c in $\mathbb{R}$ such that

$$f(x+h) = \sum_{n=0}^{k-1} f^{(n)}(x)\frac{h^n}{n!} + f^{(k)}(c)\frac{h^k}{k!}. \tag{A.1}$$

We fix real numbers $a_0, \ldots, a_{k-1}$ such that $\sum_{m=0}^{k-1} a_m n^m = \delta_{n,j}$ for $n = 1, \ldots, k-1$ by inverting a Vandermonde system. For given $t \in \mathbb{R}$, by a linear combinations of the formulas (A.1) with $h = 0, t, 2t, \ldots, (k-1)t$, we get

$$\sum_{m=0}^{k-1} a_m f(x+mt) = f^{(j)}(x)\frac{t^j}{j!} + \left(\sum_{m=0}^{n-1} a_m f^{(k)}(c_m)\right)\frac{t^k}{k!}$$

for some real numbers $c_1, \ldots, c_{k-1}$. In particular,

$$\|f^{(j)}\|_\infty \leq C(t^{-j}\|f\|_\infty + t^{k-j}\|f^{(k)}\|_\infty)$$

for some constant C and the result follows by optimizing in t. □

https://doi.org/10.1017/etds.2021.22 Published online by Cambridge University Press

PROPOSITION A.2. (Product of norms of derivatives) *For any f, g in $C^k(\mathbb{R})$ and any integer $j \leq k$,*

$$\|f^{(j)}\|_\infty \|g^{(k-j)}\|_\infty \leq C(\|f^{(k)}\|_\infty \|g\|_\infty + \|f\|_\infty \|g^{(k)}\|_\infty),$$

where C is a constant depending only on k.

Proof. It is a consequence of the Kolmogorov inequality and the convexity inequality $a^\theta b^{1-\theta} \leq \theta a + (1-\theta)b$,

$$\begin{aligned}\|f^{(j)}\|_\infty \|g^{(k-j)}\|_\infty &\leq C\|f^{(k)}\|_\infty^{j/k} \|f\|_\infty^{1-j/k} \|g^{(k)}\|_\infty^{1-j/k} \|g\|_\infty^{j/k} \\ &\leq C\bigg(\frac{j}{k}\|f^{(k)}\|_\infty \|g\|_\infty + \bigg(1 - \frac{j}{k}\bigg)\|f\|_\infty \|g^{(k)}\|_\infty\bigg).\end{aligned}$$ □

PROPOSITION A.3. (Derivative of a product) *For any integer k and any f, g in $C^k(\mathbb{R})$,*

$$\|(fg)^{(k)}\|_\infty \leq C(\|f^{(k)}\|_\infty \|g\|_\infty + \|f\|_\infty \|g^{(k)}\|_\infty),$$

where C is a constant depending only on k.

Proof. By the Leibniz formula, $\|(fg)^{(k)}\|_\infty \leq \sum_{j=0}^{k} \binom{k}{j} \|f^{(j)}\|_\infty \|g^{(k-j)}\|_\infty$ and, by the proposition above, $\|f^{(j)}\|_\infty \|g^{(k-j)}\|_\infty \leq C(\|f^{(k)}\|_\infty \|g\|_\infty + \|f\|_\infty \|g^{(k)}\|_\infty)$ for some C. □

PROPOSITION A.4. *(Derivative of a composition) Let $M \geq 1$. For any integer $k \geq 1$ and any f, g in $C^k(\mathbb{R})$ such that $|g'| \leq M$ on $\mathbb{R}$,*

$$\|(f \circ g)^{(k)}\|_\infty \leq CM^{k-1}(\|f^{(k)}\|_\infty \|g'\|_\infty + \|f'\|_\infty \|g^{(k)}\|_\infty),$$

where C is a constant depending only on k.

Proof. We proceed by induction on k. The statement is obvious for $k = 1$. Let $k \geq 2$. Since $(f \circ g)^{(k)} = (f' \circ g \cdot g')^{(k-1)}$, we obtain by Proposition A.3 for some constant C,

$$\|(f \circ g)^{(k)}\|_\infty \leq C\big(\|(f' \circ g)^{(k-1)}\|_\infty \|g'\|_\infty + \|f' \circ g\|_\infty \|(g')^{(k-1)}\|_\infty\big),$$

so

$$\|(f \circ g)^{(k)}\|_\infty \leq C\big(M\|(f' \circ g)^{(k-1)}\|_\infty + \|f'\|_\infty \|g^{(k)}\|_\infty\big).$$

By the induction hypothesis,

$$\|(f' \circ g)^{(k-1)}\|_\infty \leq CM^{k-2}(\|f^{(k)}\|_\infty \|g'\|_\infty + \|f''\|_\infty \|g^{(k-1)}\|_\infty)$$

for some constant C depending on k. So, for some new constant C,

$$\|(f \circ g)^{(k)}\|_\infty \leq CM^{k-1}\big(\|f^{(k)}\|_\infty \|g'\|_\infty + \|f''\|_\infty \|g^{(k-1)}\|_\infty + \|f'\|_\infty \|g^{(k)}\|_\infty\big).$$

By Proposition A.2,

$$\|f''\|_\infty \|g^{(k-1)}\|_\infty \leq C(\|f^{(k)}\|_\infty \|g'\|_\infty + \|f'\|_\infty \|g^{(k)}\|_\infty)$$

https://doi.org/10.1017/etds.2021.22 Published online by Cambridge University Press

for some constant C, so, finally, with a new constant C,

$$\|(f \circ g)^{(k)}\|_\infty \leq CM^{k-1}(\|f^{(k)}\|_\infty \|g'\|_\infty + \|f'\|_\infty \|g^{(k)}\|_\infty),$$

which completes the induction. □

From these general estimates, we deduce some more specific ones for our context. We reintroduce the C^k-norms: for ϕ in $C^k(\mathbb{R})$, we define its C^k-norm by $\|\phi\|_k = \max(\|\phi\|_\infty, \|\phi'\|_\infty, \ldots, \|\phi^{(k)}\|_\infty)$ (in particular, $\|\cdot\|_0$ is also the supremum norm). Alternatively, we could define $\|\phi\|_k = \max(\|\phi\|_\infty, \|\phi^{(k)}\|_\infty)$, which is an equivalent norm thanks to the Kolmogorov inequality.

LEMMA A.1. *Let k be an integer, let $M \geq 1$ and let f, g be in $C^k(\mathbb{R})$ such that $|f'|, |g'| \leq M$ on $\mathbb{R}$. Then*

$$\|f \circ g - \mathrm{Id}\|_k \leq CM^k(\|f - \mathrm{Id}\|_k + \|g - \mathrm{Id}\|_k),$$

where C is a constant depending only on k.

Proof. Let $\varphi = f - \mathrm{Id}$ and $\psi = g - \mathrm{Id}$. Since $f \circ g - \mathrm{Id} = \psi + \varphi \circ g$, we only need to bound $\|\varphi \circ g\|_k$. We have $\|\varphi \circ g\|_0 = \|\varphi\|_0$, $\|(\varphi \circ g)'\|_0 \leq \|g'\|_0 \|\varphi'\|_0 \leq M\|\varphi\|_1$ and, if $k \geq 2$, by Proposition A.4, for some constant C depending on k, we have

$$\|(\varphi \circ g)^{(k)}\|_0 \leq CM^{k-1}(\|\varphi^{(k)}\|_0 \|g'\|_0 + \|\varphi'\|_0 \|g^{(k)}\|_0),$$

with $\|\varphi'\|_0 \leq 1 + M \leq 2M$, $\|g'\|_0 \leq M$ and $\|g^{(k)}\|_0 = \|\psi^{(k)}\|_0$, so

$$\|\varphi \circ g\|_k \leq CM^k(\|\varphi\|_k + \|\psi\|_k) \tag{A.2}$$

for some new constant C depending on k and the statement follows. □

LEMMA A.2. *Let k be an integer, let $q < 1$ and let f be in $C^k(\mathbb{R})$ such that $|f' - 1| \leq \frac{1}{2}$ on $\mathbb{R}$. Then*

$$\|f^{-1} - \mathrm{Id}\|_k \leq C\|f - \mathrm{Id}\|_k,$$

where C is a constant depending only on k.

Proof. Let $g = f^{-1}$, $\varphi = f - \mathrm{Id}$ and $\psi = g - \mathrm{Id}$, so that the identity $f \circ g = \mathrm{Id}$ becomes $\psi = -\varphi \circ g$. We want to prove that $\|\psi\|_k \leq C\|\varphi\|_k$ for some constant C. It is straightforward if $k = 0$ or 1, so we assume that $k \geq 2$ and we make the induction assumption that for every $j < k$, $\|\psi\|_j \leq C\|\varphi\|_j$ for some constant C. Then

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

For $j = 0$,

$$\|\varphi' \circ g\|_0 \|g'\|_{k-1} \leq \|\varphi'\|_0 (1 + \|\psi'\|_{k-1}) \leq \|\varphi\|_1 + \tfrac{1}{2}\|\psi\|_k$$

and, for $j \neq 0$, by using inequality (A.2) (with $M = 2$) and the induction assumption, we can bound $\|\varphi' \circ g\|_j \leq C\|\varphi\|_j$ for some constant C, and then by using Proposition A.2 we get $\|\varphi' \circ g\|_j \|g'\|_{k-1-j} \leq C\|\varphi\|_k$ with a new constant C. So, we deduce finally that we have for some constant C,

$$\|\psi\|_k \leq \tfrac{1}{2}\|\psi\|_k + C\|\varphi\|_k$$

and so $\|\psi\|_k \leq 2C\|\varphi\|_k$, which completes the induction. □

LEMMA A.3. *(a C^k mean value inequality) Let $M \geq 1$, let f, g be in $C^k(\mathbb{R})$ such that $|f'|, |g'|, |f^{(k)}|, |g^{(k)}| \leq M$ on $\mathbb{R}$ and let $\phi \in C^{k+1}(\mathbb{R})$. Then*

$$\|\phi \circ f - \phi \circ g\|_k \leq C\|\phi\|_{k+1}\|f - g\|_k,$$

where C depends only on k and M.

Proof. We write

$$\phi \circ f - \phi \circ g = (f - g)\int_0^1 \phi' \circ h_t dt,$$

where $h_t = (1 - t)f + tg$. Thus,

$$\|\phi \circ f - \phi \circ g\|_k \leq C\|f - g\|_k \int_0^1 \|\phi' \circ h_t\|_k dt$$

for some constant C depending only on k. By Proposition A.4 (and the Kolmogorov inequality), $\|\phi' \circ h_t\|_k \leq C\|\phi\|_{k+1}$ for some constant C depending on k and M. The result follows. □

Finally, let us prove Propositions 2.2, 2.3, 2.4 and 2.5 of §2. Proposition 2.2 is an immediate consequence of Lemmas A.1 and A.2 and the fact that d_k is invariant under (left or right) composition by rotations. Proposition 2.5 is a straightforward consequence of inequality (A.2) since $d_k(f \circ h, g \circ h) = \|(f - g) \circ h\|_k$. To prove Proposition 2.4, we write $f = r_\alpha + \zeta$ and $g = \mathrm{Id} + \eta$ and then an algebraic computation gives

$$g \circ f \circ g^{-1} = r_\alpha + (\zeta \circ g^{-1} + \eta \circ (f \circ g^{-1}) - \eta \circ g^{-1}).$$

The difference between this map and the approximation $r_\alpha + (\zeta + \eta \circ r_\alpha - \eta)$ can be estimated in C^1-norm thanks to Lemma A.3 (with $k = 1$), which gives the result (alternatively, one can directly bound this difference and its derivative by elementary calculus). Finally, Proposition 2.3 is an elementary consequence of the invariance of d_0 under right composition and the mean value inequality:

$$\begin{aligned} d_0(gfg^{-1}, \tilde{g}f\tilde{g}^{-1}) &\leq d_0(gfg^{-1}, \tilde{g}fg^{-1}) + d_0(\tilde{g}f\tilde{g}^{-1}, \tilde{g}fg^{-1}) \\ &\leq d_0(g, \tilde{g}) + d_0(\tilde{g}f\tilde{g}^{-1}g, \tilde{g}f) \\ &\leq d_0(g, \tilde{g}) + d_0((\tilde{g}f\tilde{g}^{-1}) \circ g, (\tilde{g}f\tilde{g}^{-1}) \circ \tilde{g}) \\ &\leq (1 + \|(\tilde{g}f\tilde{g}^{-1})'\|_0)d_0(g, \tilde{g}), \end{aligned}$$

with $\|(\tilde{g}f\tilde{g}^{-1})'\|_0$ easily bounded from above.

https://doi.org/10.1017/etds.2021.22 Published online by Cambridge University Press

References

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

[2] A. Ávila and M. Viana. Extremal Lyapunov exponents: an invariance principle and applications. *Invent. Math.* **181**(1) (2010), 115–178.

[3] C. Bocker-Neto and M. Viana. Continuity of Lyapunov exponents for random two-dimensional matrices. *Ergod. Th. & Dynam. Sys.* **37**(5) (2017), 1413–1442.

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

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

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

[7] H. Furstenberg. Noncommuting random products. *Trans. Amer. Math. Soc.* **108** (1963), 377–428.

[8] H. Furstenberg and H. Kesten. Products of random matrices. *Ann. Math. Stat.* **31**(2) (1960), 457–469.

[9] F. Ledrappier. Positivity of the exponent for stationary sequences of matrices. *Lyapunov Exponents*. Springer, Berlin, 1986, pp. 56–73.

[10] D. Malicet. Random walks on Homeo(S^1). *Comm. Math. Phys.* **356**(3) (2017), 1083–1116.

[11] J. Moser. On commuting circle mappings and simultaneous Diophantine approximations. *Math. Z.* **205**(1) (1990), 105–121.

[12] L. Pastur and A. Figotin. *Spectra of Random and Almost-Periodic Operators (Grundlehren der mathematischen Wissenschaften, 297)*. Springer-Verlag, Berlin, 1992.

https://doi.org/10.1017/etds.2021.22 Published online by Cambridge University Press