A CRITERION FOR THE SIMPLICITY OF THE LYAPUNOV SPECTRUM OF SQUARE-TILED SURFACES

CARLOS MATHEUS, MARTIN MÖLLER, AND JEAN-CHRISTOPHE YOCCOZ

ABSTRACT. We present a Galois-theoretical criterion for the simplicity of the Lyapunov spectrum of the Kontsevich-Zorich cocycle over the Teichmüller flow on the $SL_2(\mathbb{R})$-orbit of a square-tiled surface. The simplicity of the Lyapunov spectrum has been proved by A. Avila and M.Viana with respect ot the so-called Masur-Veech measures associated to connected components of moduli spaces of translation surfaces, but is not always true for square-tiled surfaces of genus $\geqslant 3$. We apply our criterion to square-tiled surfaces of genus 3 with one single zero. Conditionally to a conjecture of Delecroix and Lelièvre, we prove with the aid of Siegel's theorem (on integral points on algebraic curves of genus > 0) that all but finitely many such square-tiled surfaces have simple Lyapunov spectrum.

CONTENTS

1. INTRODUCTION

1.1. **The KZ cocycle.** The Teichmüller flow on the moduli spaces of translation surfaces acts as renormalization dynamics for interval exchange transformations and translation flows. The Kontsevich-Zorich cocycle describes how the homology of the surface evolves along the orbits of the Teichmüller flow. The seminal works of A. Zorich [Zo1], [Zo2], [Zo3], [Zo4], [Zo5] and G. Forni [Fo1] have explicited an intimate relation between the deviations of Birkhoff sums from ergodic averages for interval exchange maps and translation flows and the Lyapunov spectrum of the Kontsevich-Zorich (KZ for short) cocycle.

The connected components of moduli spaces of unit area translation surfaces support natural probability measures invariant under the Teichmüller flow, the so-called Masur-Veech measures μ_{MV}. Based on numerical experiments, M. Kontsevich and A. Zorich [Ko] conjectured that Lyapunov spectra of KZ cocycle with respect to these measures are always simple, i.e. all Lyapunov exponents have multiplicity 1.

G. Forni obtained an important partial result [Fo1] in this direction: he proved that the KZ-cocycle is non-uniform hyperbolic w.r.t. μ_{MV}, i.e the Lyapunov exponents are different from 0. Then the conjecture of M. Kontsevich and A. Zorich was fully proved in the celebrated work of A. Avila and M. Viana [AV].

On the other hand, G. Forni and his coauthors (see [Fo2] and [FMZ1]) constructed two examples of translation surfaces with the following property: their orbits under the natural $SL_2(\mathbb{R})$-action on moduli space are closed and support $SL_2(\mathbb{R})$-invariant probability measures with respect to which all nontrivial Lyapunov exponents of the KZ cocycle vanish. In particular, these Lyapunov spectra are far from simple.

Partly motivated by this discussion, G. Forni [Fo3] recently provided a criterion for the non-uniform hyperbolicity of the Lyapunov spectrum of the KZ cocycle with respect to a given $SL_2(\mathbb{R})$-invariant ergodic probability measure μ essentially based on the geometry of the horizontal foliation of the translation surfaces in the support of μ. However, as it is pointed out in [Fo3] by means of concrete examples, this geometric criterion is not sufficient to ensure the simplicity of the Lyapunov spectrum in general.

1.2. **Main results.** As a matter of fact, the examples of non-simple Lyapunov spectrum in [Fo2], [FMZ1] and [Fo3] come from a class of translation surfaces (M, ω) called *square-tiled surfaces* or *origamis*.

Our main result, presented below, is a Galois-theoretical criterion for the simplicity of the Lyapunov spectrum of the KZ-cocycle, with respect to the natural $SL_2(\mathbb{R})$-invariant probability measure associated to an origami.

A translation surface (M, ω) is square-tiled if its group of relative periods is contained in $\mathbb{Z} \oplus i\mathbb{Z}$. Equivalently, there is a ramified covering $p : M \to \mathbb{T}^2 \equiv \mathbb{C}/(\mathbb{Z} \oplus i\mathbb{Z})$, unramified over $\mathbb{T}^2 - \{0\}$, such that ω is the pull back of the standard form dz on $\mathbb{T}^2$. The square-tiled surface (M, ω) is *reduced* if its group of relative periods is equal to $\mathbb{Z} \oplus i\mathbb{Z}$.

Let (M, ω) be a translation surface. An orientation-preserving homeomorphism A of M is *affine* if it is given locally by affine maps in the charts provided by local primitive of ω. Then, it has a *linear part* or *derivative* $DA \in SL_2(\mathbb{R})$. The derivatives of affine homeomorphisms form a subgroup of $SL_2(\mathbb{R})$ called the *Veech group* of (M, ω). When (M, ω) is reduced square-tiled, the Veech group is a subgroup of finite index in $SL_2(\mathbb{Z})$. An affine homeomorphism is an *automorphism* of (M, ω) if its derivative is the identity.

Let (M, ω) be a reduced square-tiled surface. There is a canonical splitting

$$H_1(M, \mathbb{Q}) = H_1^{st}(M, \mathbb{Q}) \oplus H_1^{(0)}(M, \mathbb{Q}),$$

which is invariant under the action of any affine homeomorphism. Here $H_1^{(0)}(M, \mathbb{Q})$ is the 2-codimensional kernel of the homomorphism $p_* : H_1(M, \mathbb{Q}) \to H_1^{st}(M, \mathbb{Q})$ and the summands are orthogonal for the symplectic intersection form. The action of an affine homeomorphism A on $H_1^{st}(M, \mathbb{Q}) \simeq H_1^{st}(M, \mathbb{Q}) \simeq \mathbb{Q}^2$ is through the standard action of $DA \in SL_2(\mathbb{Z})$ and correspond to the tautological extremal Lyapunov exponents of the KZ-cocycle.

The action of A on $H_1^{(0)}(M, \mathbb{Q})$ preserves the symplectic intersection form. It is given by a symplectic matrix with integer coefficients[1]. Its characteristic polynomial is reciprocal of degree $2g - 2$ (as usual, g denotes the genus of M). One says that A is *Galois-pinching* if the characteristic polynomial is irreducible over $\mathbb{Q}$, has only real roots, and its Galois group is largest possible, with order $2^{g-1}(g-1)!$ (being then isomorphic to the semi-direct product $S_{g-1} \ltimes (\mathbb{Z}/2\mathbb{Z})^{g-1}$, acting on the set of roots as the centralizer of the involution $\lambda \to \lambda^{-1}$).

We can now formulate a first version of our simplicity criterion.

Theorem 1.1. *Let (M, ω) be a reduced square-tiled surface having no nontrivial automorphism. Assume that there exist two affine homeomorphisms A, B of (M, ω) with the following properties:*

    i) *A is Galois-pinching and DA has trace > 2 ;*

    ii) *B acts on $H_1^{(0)}(M, \mathbb{Q})$ through an unipotent endomorphism distinct from the identity, such that the image of $B -$ id is not a lagrangian subspace of $H_1^{(0)}(M, \mathbb{Q})$.*

Then, the Lyapunov spectrum of the KZ-cocycle, relative to the $SL_2(\mathbb{R})$-invariant probability measure supported by the $SL_2(\mathbb{R})$-orbit of (M, ω) in moduli space, is simple.

Let (M, ω) be an origami. The union of the zeros of ω and the saddle-connections in a given rational direction disconnect M into a finite number of cylinders. The dimension of the (isotropic) subspace of $H_1(M, \mathbb{Q})$ spanned by the classes of the waist curves of these cylinders is the *homological dimension* of the given rational direction. It takes values in $\{1, \ldots, g\}$.

Corollary 1.2. *Let (M, ω) be a reduced square-tiled surface. Assume that*

    i) *The holomorphic 1-form ω has a single zero;*

    ii) *there exists a Galois-pinching affine homeomorphism A with $tr(DA) > 2$;*

    iii) *there exists a rational direction with homological dimension $\neq 1, g$.*

Then, the Lyapunov spectrum of the KZ-cocycle, relative to the $SL_2(\mathbb{R})$-invariant probability measure supported by the $SL_2(\mathbb{R})$-orbit of (M, ω) in moduli space, is simple.

In Section 5, we give another version of the criterion which involves two affine homeomorphism with hyperbolic linear part (Theorem 5.4).

In the second part of the paper, we give some application of our simplicity criterion.

For a square-tiled surface (M, ω) of genus 2, the Lyapunov exponents of the KZ-cocycle (w.r.t. to the $SL_2(\mathbb{R})$-invariant probability measure supported by the $SL_2(\mathbb{R})$-orbit of (M, ω)) are known (cf. [Ba]): the nontrivial exponents are $\pm\frac{1}{3}$ if ω has a double zero, $\pm\frac{1}{2}$ if ω has two simple zeros. In other words, they are equal to the Lyapunov exponents relative to the Masur-Veech measure of the stratum containing (M, ω).

In this paper, we consider the simplest case where the Lyapunov exponents are not known: origamis (M, ω) of genus 3 such that ω has a single zero (of order 4). The corresponding moduli space is denoted by $\mathcal{H}(4)$. Such origamis only have the identity as an automorphism (Proposition 2.4). Reduced origamis in $\mathcal{H}(4)$ fall in three different classes, related to the existence and the properties of an affine homeomorphism whose linear part is $-$id, called anti-automorphism below; because of Proposition 2.4, there is at most one such anti-automorphism.

---

[1]See however Remark 2.5.

- Origamis with no anti-automorphism are said to be of odd type[2].
- An anti-automorphism has either 4 or 8 fixed points. The origami is said to be of Prym type[3] in the first case, of hyperelliptic type in the second case.

The non trivial Lyapunov exponents for an origami of Prym type are known to be equal to $\pm\frac{1}{5}, \pm\frac{2}{5}$ (see Subsection 6.6), from [CM] and [EKZ]. The crucial fact, that allows to determine exactly the exponents, is that, for an origami of Prym type, there is a splitting of $H_1^{(0)}$ into two 2-dimensional summands which are invariant under any affine homeomorphism.

The Lyapunov exponents do not change when one replaces an origami by another in the same $SL_2(\mathbb{Z})$-orbit. To classify $SL_2(\mathbb{Z})$-orbits of origamis, several invariants have been introduced:

- A trivial invariant is the number of squares, i.e the degree of the ramified covering $p : M \to \mathbb{T}^2$.
- When there exists an anti-automorphism, its fixed points project to points of order 2 in $\mathbb{T}^2$. The distribution of the projections of fixed points was first considered by E. Kani [Ka] and P. Hubert-S. Lelièvre [HL]) in genus 2. This *HLK-invariant* for $\mathcal{H}(4)$ is described more precisely in Subsection 6.4.
- In all cases, following D. Zmiaikou ([Zm]), it is possible to associate to an N-square origami a subgroup of S_N called the *monodromy group* (see Subsection 2.3). Actually, for a large number of squares ($N \geqslant 7$ for $\mathcal{H}(4)$), the monodromy group is either the full symmetric group S_N or the alternating group A_N ([Zm, Theorem 3.12]).

Supported by some numerical experiments with SAGE, V. Delecroix and S. Lelièvre have conjectured that the invariants above are sufficient to classify $SL_2(\mathbb{Z})$-orbits in the odd and hyperelliptic cases (the Prym case had been settled earlier by E. Lanneau and D.-M. Nguyen [LN]). More precisely, they expect that, for $N > 8$

- There are two orbits of N-square reduced origamis of odd type, associated to the two possibilities for the monodromy group.
- There are four (for odd N) or three (for even N) orbits of N-square reduced origamis of hyperelliptic type, associated to the possible values of the HLK-invariant.

The complete statement of the conjecture is given in Subsection 6.5. Our result for $\mathcal{H}(4)$ is as follows.

Theorem 1.3. *For any large enough integer N, there exist two N-square reduced origami of odd type in $\mathcal{H}(4)$ with simple Lyapunov spectra whose monodromy groups are respectively the full symmetric group S_N and the alternating group A_N.*

For any large enough integer N, and any realizable value of the HLK-invariant, there exists a N-square reduced origami of hyperelliptic type in $\mathcal{H}(4)$ with simple Lyapunov spectrum having the prescribed HLK-invariant.

Corollary 1.4. *If the Delecroix-Lelièvre conjecture holds, then the Lyapunov spectrum of the KZ-cocycle for all but (possibly) finitely many reduced square-tiled surfaces in $\mathcal{H}(4)$ is simple.*

---

[2]Odd here denotes the parity of a spin structure which is crucial in the Kontsevich-Zorich classification [KZ] of connected components of strata.

[3]See Subsection 6.2.

1.3. **Questions and comments.**

Remark 1.5. Theorem 1.1 was used by V. Delecroix and the first author [DM] to show that there is no general converse to G. Forni's geometrical criterion for non-uniform hyperbolicity [Fo3].

Remark 1.6. The exact value of the Lyapunov exponents of the KZ cocycle are not known for a primitive square-tiled surface in $\mathcal{H}(4)$ except in the Prym case. On the other hand, Chen and Möller [CM] have shown that the *sum* of the nonnegative exponents depends only of the connected component of the moduli space which contains the surface, and is equal to the sum of the nonnegative exponents for the Masur-Veech measure of this component. The sum of the nonnegative exponents for Masur-Veech measures can be computed explicitly from Siegel-Veech constants [EKZ]. The sum of the nontrivial nonnegative exponents is therefore equal to $\frac{3}{5}$ for square-tiled surfaces of odd or Prym type, and to $\frac{4}{5}$ for origamis of hyperelliptic type.

Remark 1.7. While numerical methods to estimate the values of the Lyapunov exponents of the KZ-cocycle are quite effective for the Masur-Veech measures associated to components of the moduli space, they are much less so for the natural measures associated to individual square-tiled surfaces. For origamis in $\mathcal{H}(4)$ (not of Prym type), only the first two decimal places can be guaranteed with some degree of confidence. Within these limitations, no variation can be detected numerically for the Lyapunov exponents of origamis of the same type in $\mathcal{H}(4)$.

Remark 1.8. How effective are Theorem 1.3 and Corollary 1.4? The short answer is that they are effective in principle but not in a practical way. The construction in Sections 7 and 8 of one-parameter families of origamis with some of the required properties (prescribed monodromy group or HLK-invariant, rational direction of homological dimension 2) is valid as soon as the number of squares (which is an affine function of the parameter) is not too small. These origamis are equipped with an affine homeomorphism A satisfying $\text{tr}(A) > 2$. In order to apply Corollary 1.2, we have to prove that A is Galois-pinching. After some elementary Galois theory, this is equivalent to show that three quantities, which are explicit polynomials with integer coefficients in the parameter, are not squares. This can be done quite explicitly for the first quantity. However, to deal with the other two quantities, we have to appeal to Siegel's theorem (see, e.g., [HS]) on the finiteness of integral points on algebraic curves of genus > 0.

Siegel's theorem admits effective versions (see for instance [Bi]) but the bounds on the height of the integral points are currently, as far as the authors know, doubly exponential in the size of the coefficients of the polynomials involved. Thus, even assuming the conjecture of Delecroix and Lelièvre, a proof of the simplicity of the Lyapunov spectrum for *all* origamis in $\mathcal{H}(4)$ along these lines (completing Corollary 1.4 by a numerical investigation of the finitely many remaining origamis) is hopeless.

The invariance of the sum of nonnegative Lyapunov exponents for origamis in the same connected component of moduli space, as exemplified by the results of Bainbridge in genus 2 and of Chen-Möller (Remark 1.6) for $\mathcal{H}(4)$, does not extend to all moduli spaces. For instance, the moduli space of genus 3 translation surfaces with 4 simple zeroes contains the example cited earlier [Fo2] with totally degenerate Lyapunov spectrum.

In genus $\geqslant 3$, the relation between the Lyapunov spectra of the KZ-cocycle w.r.t. the probability measure associated to a square-tiled surface (M, ω) and w.r.t. the Masur-Veech measure associated with the connected component of moduli space containing (M, ω) is

poorly understood. The only general result is due to Eskin: in the appendix of [Ch], he proves that, as N goes to $+\infty$, the *average* of the *sum* of nonnegative Lyapunov exponents over all N-square origamis in a component of some moduli space converges to the *sum* of Lyapunov exponents w.r.t. the Masur-Veech measure of this component.

In connection with the results mentioned above and the recent works [EM] and [EMM], the following questions look natural. Consider a sequence of square-tiled surfaces (M_n, ω_n) in some connected component of some moduli space of translation surfaces. Denote by μ_n the natural invariant probability measure on the $SL_2(\mathbb{R})$-orbit of (M_n, ω_n) in moduli space. Assume that the sequence μ_n converges in the weak topology to some probability measure μ. Then, by Theorem 2.3 of [EMM], the measure μ is ergodic and the support of μ contains (M_n, ω_n) for all large n.

Question 1.9. Does *each* Lyapunov exponent w.r.t. μ_n converge towards the corresponding exponent w.r.t. μ?

Remark 1.10. As it was pointed out to us by A. Eskin, in the same context as above, the *sum* of the nonnegative Lyapunov exponents w.r.t. μ_n converges towards the *sum* of the nonnegative Lyapunov exponents w.r.t. μ by an argument along the following lines. The Kontsevich-Forni formula (cf. [EKZ] and [Fo1]) expresses the sum of Lyapunov exponents of an ergodic $SL(2, \mathbb{R})$-invariant probability measure ν in terms of an integral of a *continuous* function Λ defined on any given connected component $\mathcal{C}$ of moduli spaces of translation surfaces. Furthermore, Λ is uniformly bounded by the value g of the genus of translation surfaces in $\mathcal{C}$. On the other hand, Λ is *not* compactly supported (cf. [Fo1]), and thus the convergence of sum of Lyapunov exponents is not an immediate consequence of the definition of weak-$*$ convergence of measures. Nevertheless, the work of A. Eskin and H. Masur [EMas] implies that, for each $\varepsilon > 0$, there exists a compact set $K_\varepsilon \subset \mathcal{C}$ such that $\nu(K_\varepsilon) > 1 - \varepsilon$ for *all* ergodic $SL(2, \mathbb{R})$-invariant probability measure ν on $\mathcal{C}$. By combining this with the uniform bound on Λ, we see that the integral of Λ on the complement of K_ε w.r.t. *any* ergodic $SL(2, \mathbb{R})$-invariant ν is $< g \cdot \varepsilon$. In other words, the main contribution to the integral of Λ on $\mathcal{C}$ comes from the compact sets K_ε and therefore we can use the definition of weak-$*$ convergence to obtain the desired convergence of sums of Lyapunov exponents.

1.4. **Outline of the paper.** We recall in Section 2 the definition and some elementary properties of translation surfaces, the KZ-cocycle, and square-tiled surfaces. Then we state as Theorem 2.17 a variant of the simplicity criterion of A. Avila and M. Viana [AV] for locally constant integrable cocycles over full shifts on a countable alphabet, equipped with measures with bounded distortion. The simplicity criterion says that such cocycles have simple Lyapunov spectrum whenever they verify two conditions called pinching and twisting. The version of the simplicity criterion used here differs from the original one by A. Avila and M. Viana in a few details, such as the precise statement of the twisting property. For the convenience of the reader, we discuss in Appendices A and B the straightforward modifications one must perform in the original argument of A. Avila and M. Viana in order to get Theorem 2.17.

In order to apply Theorem 2.17 to the KZ-cocycle over the $SL_2(\mathbb{R})$-orbit of a square-tiled surface, we explain in Section 3 how to view the Teichmüller flow on such an orbit as the suspension of a full shift over a countable alphabet. This is derived from the classical relation between the continued fraction algorithm and the geodesic flow on the modular surface. The invariant Haar measure on the orbit has bounded distortion. The KZ-cocycle

corresponds in this setting to a locally constant integrable cocycle given by symplectic matrices with integer coefficients.

Section 4 provides the main step in the proof of Theorem 1.1. The pinching condition of Theorem 2.17 is replaced by the stronger hypothesis of Galois-pinching, which only makes sense for matrices with integer coefficients. For Galois-pinching matrices, we are able to replace the twisting condition of Theorem 2.17 by a weaker hypothesis, which is easily checked in the setting of Theorem 1.1. The proof of this fact (Theorem 4.5) is quite involved.

In Section 5, we complete the proof of Theorem 1.1 and Corollary 1.2. We also present and prove a variant of Theorem 1.1 .

In the last three sections of the paper, we explain how to apply Corollary 1.2 to prove Theorem 1.3.

In Section 6, we give some general background on origamis in $\mathcal{H}(4)$ which will be needed later. We extract from S. Lelièvre's classification of saddle configurations in Appendix C a characterization of 2-cylinder directions. We define the HLK-invariant for origamis of odd or Prym type, and formulate precisely the conjecture of Delecroix and Lelièvre. We recall what is known about origamis of Prym type. Finally, we present some elementary Galois theory of reciprocal polynomials of degree 4 which is instrumental in checking that an affine homeomorphism is Galois-pinching.

The proof of Theorem 1.3 is given in Section 7 for origamis of odd type, in Section 8 for origamis of hyperelliptic type. The method of the proof is the same in both cases. We define in each case a model geometry, consisting of origamis with three horizontal cylinders and three vertical cylinders with a very simple intersection pattern. These two families of origamis are parametrized by six integers, the heights of the horizontal and vertical cylinders. It is very easy to determine from the parameters the monodromy group (in the odd case) or the HLK-invariant (in the hyperelliptic case). The model geometry allows to construct explicitly, for any values of the six parameters, an affine homeomorphism A with $\text{tr}(A) > 2$.

We consider a finite number of one-parameter subfamilies, where only one of the six parameters is allowed to vary along an arithmetic progression. We get in this way enough origamis to get one with prescribed invariant (monodromy group or HLK-invariant) for any large number of squares. Also, in each of these families, a well-chosen rational direction has homological dimension 2. Finally, we apply the elementary Galois theory of Subsection 6.7 to show that A is Galois-pinching when the number of squares is large enough. Then Theorem 1.3 is a consequence from Corollary 1.2.

2. BACKGROUND AND NOTATION

The basic references for the next 4 subsections are [Zo6] and [Ve3] (see also Section 1 of [MY]), and for the last subsection is [AV].

2.1. Translation surfaces. Let

- M be a compact oriented topological surface of genus $g \geqslant 1$;
- $\Sigma := \{O_1, \ldots, O_\sigma\}$ be a non-empty finite subset of M;
- $\kappa = (k_1, \ldots, k_\sigma)$ be a non-increasing sequence of non-negative integers satisfying $\sum k_i = 2g - 2$.

A structure of *translation surface* on (M, Σ, κ) is a structure of Riemann surface on M, together with a non identically zero holomorphic 1-form ω which has at O_i a zero of order k_i. Observe that, by the Riemann-Roch theorem, all zeroes of ω belong to Σ. For example, taking $M = \mathbb{R}^2/\mathbb{Z}^2$, $\Sigma = \{0\}$, $k_0 = 0$, a structure of translation surface is defined by the complex structure inherited from $\mathbb{C} \equiv \mathbb{R}^2$ and the holomorphic 1-form ω_0 induced by dz.

The reason for the nomenclature "translation surface" comes from the fact that local primitives of ω on $M - \Sigma$ provides an atlas whose changes of charts are given by translations of the plane. Below, the charts of this atlas will be called *translation charts*.

Sometimes we will slightly abuse notation by denoting a translation surface by (M, ω) or simply ω when the structure of Riemann surface is unambiguous.

Denote by $\mathrm{Diff}^+(M, \Sigma, \kappa)$ the group of orientation-preserving homeomorphisms f of M which preserve Σ and κ (i.e if $f(O_i) = O_j$, then $k_i = k_j$). Denote by $\mathrm{Diff}_0^+(M, \Sigma, \kappa)$ the identity component of $\mathrm{Diff}^+(M, \Sigma, \kappa)$. The quotient

$$\Gamma(M, \Sigma, \kappa) := \mathrm{Diff}^+(M, \Sigma, \kappa)/\mathrm{Diff}_0^+(M, \Sigma, \kappa)$$

is the so-called *mapping-class group*.

The *Teichmüller space* $\mathfrak{T}(M, \Sigma, \kappa)$ is the quotient of the set of structure of translation surfaces on (M, Σ, κ) by the natural action of the group $\mathrm{Diff}_0^+(M, \Sigma, \kappa)$. Similarly, the *moduli space* $\mathcal{H}(M, \Sigma, \kappa)$ is the quotient of the same set by the natural action of the larger group $\mathrm{Diff}^+(M, \Sigma, \kappa)$. Thus the mapping class group acts on Teichmüller space and the quotient space is the moduli space.

The group $\mathrm{GL}_2^+(\mathbb{R})$ naturally acts on the set of structures of translation surfaces on (M, Σ, κ) by post-composition with the translation charts. This action commutes with the action of $\mathrm{Diff}^+(M, \Sigma, \kappa)$. Therefore it induces an action of $\mathrm{GL}_2^+(\mathbb{R})$ on both $\mathfrak{T}(M, \Sigma, \kappa)$ and $\mathcal{H}(M, \Sigma, \kappa)$.

The action of the 1-parameter diagonal subgroup $g_t := \mathrm{diag}(e^t, e^{-t})$ is the so-called *Teichmüller flow*.

Let ω define a structure of translation surface on (M, Σ, κ). The *automorphism group* $\mathrm{Aut}(\omega)$, resp. the *affine group* $\mathrm{Aff}(\omega)$, of the translation surface (M, ω) is the group of orientation-preserving homeomorphisms of M which preserve Σ and whose restrictions to $M - \Sigma$ read as translations, resp. affine maps, in the translation charts of (M, ω). The embedding of $\mathrm{Aut}(\omega)$ into $\mathrm{Aff}(\omega)$ is completed into an exact sequence

$$1 \longrightarrow \mathrm{Aut}(\omega) \longrightarrow \mathrm{Aff}(\omega) \longrightarrow \mathrm{SL}(\omega) \longrightarrow 1,$$

where $\mathrm{SL}(\omega) \subset SL(2, \mathbb{R})$ is the *Veech group* of (M, ω): it is the stabilizer of the point in moduli space represented by (M, ω), for the action of $\mathrm{GL}_2^+(\mathbb{R})$. The map from $\mathrm{Aff}(\omega)$ onto the Veech group is defined by associating to each homeomorphism $\phi \in \mathrm{Aff}(\omega)$ its derivative (linear part) $D\phi \in \mathrm{SL}(\omega)$ in translation charts.

Definition 2.1. Let (M, ω) be a translation surface. An *anti-automorphism* (or *central symmetry*) is an element of the affine group $\text{Aff}(\omega)$ whose derivative is $-\text{Id}$.

The square of an anti-automorphism is an automorphism.

2.2. **Teichmüller flow and Kontsevich-Zorich cocycle.** The total area $A(M, \omega)$ of a translation surface (M, ω) (namely $A(M, \omega) := (i/2) \int_M \omega \wedge \overline{\omega}$) is invariant under the commuting actions of $\text{SL}_2(\mathbb{R})$ and $\text{Diff}^+(M, \Sigma, \kappa)$. Thus it makes sense to consider the restriction of the action of $\text{SL}_2(\mathbb{R})$ to the Teichmüller space $\mathcal{T}^{(1)}(M, \Sigma, \kappa)$ of unit area translation surfaces, and to the moduli space $\mathcal{H}^{(1)}(M, \Sigma, \kappa)$ of unit area translation surfaces.

The dynamical features of the Teichmüller flow g_t on the moduli spaces $\mathcal{H}^{(1)}(M, \Sigma, \kappa)$ have important consequences in the study of interval exchange transformations, translation flows and billiards. For instance, H. Masur [Ma] and W. Veech [Ve1], [Ve2] constructed, on each connected component of the normalized moduli space $\mathcal{H}^{(1)}(M, \Sigma, \kappa)$, a $\text{SL}_2(\mathbb{R})$-invariant probability measure, nowadays called Masur-Veech measure. They used the recurrence properties of the Teichmüller flow with respect to this probability measure to confirm M. Keane's conjecture on the unique ergodicity of "typical" interval exchange transformations. We will denote the Masur-Veech measures by μ_{MV} in what follows.

After that, A. Zorich and M. Kontsevich (see [Zo1], [Zo2], [Zo3] and [Ko]) introduced the so-called *Kontsevich-Zorich cocycle* (KZ cocycle for short) partly motivated by the study of deviations of ergodic averages of interval exchange transformations.

Roughly speaking, the KZ cocycle G_t^{KZ} is obtained from the quotient of the trivial cocycle

$$\widehat{G}_t^{KZ} : \mathcal{T}^{(1)}(M, \Sigma, \kappa) \times H_1(M, \mathbb{R}) \quad \to \quad \mathcal{T}^{(1)}(M, \Sigma, \kappa) \times H_1(M, \mathbb{R}),$$
$$\widehat{G}_t^{KZ}(\omega, [c]) \quad := \quad (g_t(\omega), [c]),$$

by the (diagonal) action of the mapping-class group $\Gamma(M, \Sigma, \kappa)$. In other words, the KZ cocycle G_t^{KZ} acts on $H_1^{\mathbb{R}} := (\mathcal{T}^{(1)}(M, \Sigma, \kappa) \times H_1(M, \mathbb{R}))/\Gamma(M, \Sigma, \kappa)$, a non-trivial bundle over $\mathcal{M}^{(1)}(M, \Sigma, \kappa)$ called the *real Hodge bundle* in the literature.[4]

The action of $\Gamma(M, \Sigma, \kappa)$ on the $2g$-dimensional real vector space $H_1(M, \mathbb{R})$ preserves the natural symplectic intersection form on homology. Hence, G_t^{KZ} is a symplectic cocycle. In particular, the Lyapunov exponents of the KZ cocycle with respect to an ergodic g_t-invariant probability measure μ on $\mathcal{M}^{(1)}(M, \Sigma, \kappa)$ satisfy $\lambda_{g+i}^{\mu} = -\lambda_{g-i+1}^{\mu}$ for each $i = 1, \ldots, g$.

Moreover, it is possible to show that the top Lyapunov exponent λ_1^{μ} is equal to 1, and is simple, i.e., $1 = \lambda_1^{\mu} > \lambda_2^{\mu}$ (see e.g. [Fo1]). In summary, the Lyapunov spectrum of the KZ cocycle with respect to any ergodic g_t-invariant probability measure μ has the form:

$$1 = \lambda_1^{\mu} > \lambda_2^{\mu} \geqslant \ldots \geqslant \lambda_g^{\mu} \geqslant -\lambda_g^{\mu} \geqslant \ldots \geqslant -\lambda_2^{\mu} > -\lambda_1^{\mu} = -1$$

The relevance of the KZ cocycle to the study of deviations of ergodic averages of interval exchange transformations resides on the fact that, roughly speaking, the Lyapunov

---

[4]Some translation surfaces (M, ω) have a (finite but) non-trivial group of automorphisms, so that this definition of the KZ cocycle may not lead to a well-defined linear dynamical cocycle over certain regions of the moduli space. Over such regions, we only have a "cocycle up to a finite group", but this is not troublesome as far as Lyapunov exponents are concerned: in a nutshell, by taking finite covers, we can solve the ambiguity coming from automorphisms groups in the definition of KZ cocycle without altering Lyapunov exponents. See Subsection 2.3 below and/or [MYZ] for more discussion on this in the setting of square-tiled surfaces.

exponents of the KZ cocycle "control" the deviation of ergodic averages of interval exchange transformations. See [Zo1], [Zo2], [Zo3] and [Fo1] for more details. In particular, this fact is one of the motivation for the study of Lyapunov exponents of KZ cocycle.

Based on numerical experiments, M. Kontsevich and A. Zorich [Ko] conjectured that the Lyapunov spectrum of the KZ cocycle with respect to any Masur-Veech measure μ_{MV} is *simple*, that is, the multiplicity of all exponents $\lambda_i^{\mu_{MV}}$ is equal 1, and *a fortiori* the exponents are all non-zero (i.e., $\lambda_g^{\mu_{MV}} > 0$). This conjecture is nowadays known to be true after the celebrated works of G. Forni [Fo1], who proved that $\lambda_g^{\mu_{MV}} > 0$, and A. Avila and M. Viana [AV], who established the full conjecture.

On the other hand, G. Forni and his coauthors (see e.g. [Fo2] and [FMZ1]) constructed two instances of $SL_2(\mathbb{R})$-invariant ergodic probabilities μ_{EW} and μ_O whose Lyapunov spectra with respect to the KZ cocycle are totally degenerate in the sense that $\lambda_2^{\mu_{EW}} = \lambda_2^{\mu_O} = 0$, that is, all Lyapunov exponents vanish except for the extreme ("tautological") exponents $\lambda_1 = 1$, $\lambda_{2g} = -1$.

The main goal of this article is the proof of the simplicity of the Lyapunov spectrum of the KZ cocycle with respect to certain ergodic $SL_2(\mathbb{R})$-invariant probability measures supported on the $SL_2(\mathbb{R})$-orbits of a special kind of translation surfaces called *square-tiled surfaces* or *origamis*. For the reader's convenience, we recall some features of square-tiled surfaces in the next two subsections.

2.3. **Square-tiled surfaces.** A *square-tiled surface* (or *origami*) is a translation surface (M, ω) such that

$$\int_\gamma \omega \in \mathbb{Z} \oplus i\mathbb{Z}$$

for every relative homology class $\gamma \in H_1(M, \Sigma, \mathbb{Z})$.

Let (M, ω) be an origami and $O_j \in \Sigma$; the application

$$
\begin{aligned}
p : M &\rightarrow \mathbb{C}/\mathbb{Z} \oplus i\mathbb{Z} \equiv \mathbb{T}^2 \\
A &\rightarrow \int_{O_j}^A \omega \mod \mathbb{Z} \oplus i\mathbb{Z}
\end{aligned}
$$

is independent of j and is a ramified covering with the following properties:

- p is unramified over $\mathbb{T}^2 - \{0\}$;
- $\omega = p^*(\omega_0(\mathbb{T}^2))$;
- Σ is contained in the fiber $p^{-1}(0)$.

Conversely, a ramified covering with these properties defines an origami.[5]

Let (M, ω) be an origami and let $p : M \rightarrow \mathbb{T}^2$ be the associated ramified covering. A *square* of (M, ω) is a connected component of $p^{-1}((0, 1)^2)$. The cardinality of the set $Sq(\omega)$ of squares is the degree of p. One defines two bijections σ_h, σ_v from $Sq(\omega)$ to itself by sending a square to the square immediately to the right, resp. to the top, of it. The subgroup of the symmetric group over $Sq(\omega)$ generated by σ_h, σ_v is called the *monodromy group* of (M, ω) and acts transitively on $Sq(\omega)$.

The action of $SL_2(\mathbb{Z}) \subset GL_2^+(\mathbb{R})$ on the set of translation surfaces preserves the subset of square-tiled surfaces. In moduli space, the orbit of an origami for this action is finite. The action of $SL_2(\mathbb{Z})$ on origamis preserves the number of squares and the monodromy group (cf. [Zm]).

---

[5]For a square-tiled surface, it is more convenient to normalize the area of each square than the total area.

Definition 2.2. An origami (M, ω) is *reduced* if the group of relative periods $\int_\gamma \omega$, $\gamma \in H_1(M, \Sigma, \mathbb{Z})$ is equal to $\mathbb{Z} \oplus i\mathbb{Z}$. Equivalently, writing p for the associated ramified covering of $\mathbb{T}^2$, there does not exist a ramified covering $p' : M \to \mathbb{T}^2$ unramified over $\mathbb{T}^2 - \{0\}$ and a covering $\pi : \mathbb{T}^2 \to \mathbb{T}^2$ of degree > 1 such that $p = \pi \circ p'$.

We will only consider from now on reduced origamis. For later use, we also give the definition of *primitive* square-tiled surfaces.

Definition 2.3. A square-tiled surface (M, ω) is *primitive* if it is not a non-trivial ramified covering of another square-tiled surface (M', ω').

A primitive square-tiled surface is reduced (but the converse is not always true). The automorphism group of a primitive origami is trivial.

Let (M, ω) be a reduced square-tiled surface. The Veech group $\mathrm{SL}(\omega)$ is a finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$, and, *a fortiori*, it is a lattice in $\mathrm{SL}_2(\mathbb{R})$. Thus $\mathrm{SL}_2(\mathbb{R})/\mathrm{SL}(\omega)$ supports an unique $\mathrm{SL}_2(\mathbb{R})$-invariant probability measure. By a theorem of J. Smillie (cf. [SW]), the $\mathrm{SL}_2(\mathbb{R})$-orbit of (M, ω) is closed in the corresponding moduli space. Hence there exists exactly one $\mathrm{SL}_2(\mathbb{R})$-invariant probability measure supported by the $\mathrm{SL}_2(\mathbb{R})$-orbit of (M, ω) in moduli space.

The affine group $\mathrm{Aff}(\omega)$ embeds naturally in the mapping class group $\Gamma(M, \Sigma, \kappa)$ and its image is the stabilizer of the $\mathrm{SL}_2(\mathbb{R})$-orbit of (M, ω) in Teichmüller space. Therefore, the restriction of the KZ cocycle G_t^{KZ} to the $\mathrm{SL}_2(\mathbb{R})$-orbit of (M, ω) in moduli space can be thought as the quotient of the trivial cocycle (over the orbit of (M, ω) in Teichmüller space)

$$\widehat{G}_t^{KZ} : \mathrm{SL}_2(\mathbb{R}) \cdot (M, \omega) \times H_1(M, \mathbb{R}) \to \mathrm{SL}_2(\mathbb{R}) \cdot (M, \omega) \times H_1(M, \mathbb{R})$$

by the action of the affine group $\mathrm{Aff}(\omega)$. In other words, for recurrent times of the Teichmüller flow, the restriction of the KZ cocycle to the orbit of (M, ω) acts on the fibers $H_1(M, \mathbb{R})$ of the real Hodge bundle through certain elements of $\mathrm{Aff}(\omega)$. In particular, we see that:

- when the automorphism group $\mathrm{Aut}(\omega)$ is *trivial*, the Veech group $\mathrm{SL}(\omega)$ is canonically isomorphic to the affine group $\mathrm{Aff}(\omega)$. In this case, the KZ cocycle is a linear dynamical cocycle in the usual sense.
- on the other hand, when $\mathrm{Aut}(\omega)$ is *not* trivial, the action of the KZ cocycle on the fibers of the real Hodge bundle is only defined *up to* the action on homology of the finite group $\mathrm{Aut}(\omega)$. In order to remove this ambiguity and to recover a standard linear dynamical cocycle, one must introduce a *finite cover* of moduli space. Such a finite cover is constructed, for instance, in [MYZ] (by marking some horizontal separatrices).

In the sequel, we will avoid the technical issue pointed out in the last item by assuming from now on that *the origami under consideration has a trivial automorphism group*. We recall the following well-known fact.

Proposition 2.4. *A translation surface* (M, ω) *such that* $\#\Sigma = 1$ *has no nontrivial automorphism.*

Proof. The quotient of (M, ω) by a nontrivial automorphism would be a cyclic Galois ramified covering over another translation surface (N, ω') with a single marked point O'. A small loop around O' is a product of commutators in the fundamental group of $N - \{O'\}$,

hence would lift to a loop in M. Thus the covering would be unramified and Σ would have more than one point. $\square$

2.4. **Decomposition of the homology.** Let (M, ω) be a reduced square-tiled surface (with trivial automorphism group) and let $p : M \to \mathbb{T}^2$ be the associated covering. We denote by $H_1^{(0)}(M, \mathbb{Z})$ the kernel of the linear map

$$p_* : H_1(M, \mathbb{Z}) \longrightarrow H_1(\mathbb{T}^2, \mathbb{Z}) \simeq \mathbb{Z}^2$$

induced by p. We define similarly $H_1^{(0)}(M, \mathbb{R})$ as the kernel of the map on $\mathbb{R}$-homology, consequently $H_1^{(0)}(M, \mathbb{R}) = H_1^{(0)}(M, \mathbb{Z}) \otimes \mathbb{R}$.

The subspace $H_1^{(0)}(M, \mathbb{R})$ of $H_1(M, \mathbb{R})$ is symplectic with respect to the symplectic form induced by the natural intersection form on homology. Denoting by $H_1^{st}(M, \mathbb{R})$ its 2-dimensional symplectic orthogonal, one has[6]

$$H_1(M, \mathbb{R}) = H_1^{st}(M, \mathbb{R}) \oplus H_1^{(0)}(M, \mathbb{R}).$$

The action of the affine group $\mathrm{Aff}(\omega)$ on $H_1(M, \mathbb{R})$ preserves this splitting. The action on the first factor $H_1^{st}(M, \mathbb{R})$ (canonically identified with $\mathbb{R}^2$ via p_*) is through the standard action of the Veech group $\mathrm{SL}(\omega)$ on $\mathbb{R}^2$. The action on the second factor respects the integral lattice $H_1^{(0)}(M, \mathbb{Z})$.

The splitting above is extended as a constant splitting of the trivial bundle $\mathrm{SL}_2(\mathbb{R}) \cdot (M, \omega) \times H_1(M, \mathbb{R})$ over the orbit of (M, ω) in Teichmüller space. Going to the quotient by the action of the affine group, we get a well-defined splitting of the real Hodge bundle (over the orbit of $\mathrm{SL}_2(\mathbb{R})$-orbit of (M, ω) in moduli space) which is invariant under the KZ cocycle. We denote by $G_t^{KZ, st}$, resp. $G_t^{KZ, (0)}$, the action of the KZ cocycle on the two subbundles.

Let μ be an ergodic g_t-invariant probability measure supported on the $\mathrm{SL}_2(\mathbb{R})$ orbit of (M, ω) in moduli space. The action of $G_t^{KZ, st}$ on H_1^{st} is responsible for the "tautological" Lyapunov exponents $\lambda_1^{\mu} = 1$ and $\lambda_{2g}^{\mu} = -\lambda_1^{\mu} = -1$. One must focus on the action $G_t^{KZ, (0)}$ on $H_1^{(0)}$ to understand the nontrivial Lyapunov exponents $\lambda_2^{\mu} \geqslant \ldots \geqslant \lambda_g^{\mu}$.

The integral lattice $H_1^{(0)}(M, \mathbb{Z})$ is preserved by the affine group, and the restriction of the intersection form to this lattice is a non-degenerate integer-valued antisymmetric form Ω. Choosing a basis of $H_1^{(0)}(M, \mathbb{Z})$, we can think of $G_t^{KZ, (0)}$ as a cocycle over the Teichmüller flow with values in the matrix group $\mathrm{Sp}(\Omega, \mathbb{Z})$ of Ω-symplectic $(2g-2) \times (2g-2)$-matrices with integer coefficients.

Remark 2.5. The integer-valued symplectic form Ω on the $(2g - 2)$-dimensional integer lattice $H_1^{(0)}(M, \mathbb{Z})$ is in general not isomorphic to the standard symplectic form on $\mathbb{Z}^{2g-2}$. For an integer-valued symplectic forms on $\mathbb{Z}^{2d}$ there exist uniquely defined positive integers $\omega_1, \ldots, \omega_d$ with $\omega_i | \omega_{i+1}$ and a decomposition into Ω-orthogonal 2-dimensional planes

$$\mathbb{Z}^{2d} = \oplus_{i=1}^d E_i$$

such that each E_i has a basis (e_i, f_i) with $\Omega(e_i, f_i) = \omega_i$, see [BL, Section 3.1] and the references therein. In fact, in our situation $\omega_i = 1$ for $i < g - 2$ and $\omega_{g-1} | p$, see [BL, Corollary 12.1.5 and Proposition 11.4.3].

---

[6]One may define $H_1^{st}(M, \mathbb{Z})$ as the intersection $H_1^{st}(M, \mathbb{R}) \cap H_1(M, \mathbb{Z})$ but one should be aware that in general the direct sum $H_1^{st}(M, \mathbb{Z}) \oplus H_1^{(0)}(M, \mathbb{Z})$ is not equal to $H_1(M, \mathbb{Z})$, but only to a sublattice of this group.

In the sequel, we will study the simplicity of the Lyapunov spectrum of $G_t^{KZ,(0)}$ with respect to the (unique) $\mathrm{SL}_2(\mathbb{R})$-invariant probability measure μ_ω supported on the $\mathrm{SL}_2(\mathbb{R})$-orbit of (M, ω), for certain reduced origamis (M, ω) with $\mathrm{Aut}(\omega) = \{\mathrm{Id}\}$. During this task, we will use a (variant of a) simplicity criterion for cocycles over complete shifts (originally) due to A. Avila and M. Viana. The content of this criterion is quickly reviewed in the next subsection.

2.5. **The Avila-Viana simplicity criterion and its variants.** In this subsection we briefly recall the setting of the Avila-Viana simplicity criterion [AV], and we discuss some variants of it (of particular interest to our context). There are several versions of this criterion in the literature, notably by A. Avila and M. Viana themselves [AV2].

Let Λ be a finite or countable alphabet. Define $\Sigma := \Lambda^{\mathbb{N}}$, $\hat{\Sigma} := \Lambda^{\mathbb{Z}} = \Sigma_- \times \Sigma$. Denote by $f : \Sigma \to \Sigma$ and $\hat{f} : \hat{\Sigma} \to \hat{\Sigma}$ the natural (left) shift maps on Σ and $\hat{\Sigma}$ respectively. Also, let $p^+ : \hat{\Sigma} \to \Sigma$ and $p^- : \hat{\Sigma} \to \Sigma_-$ be the natural projections.

We denote by $\Omega = \bigcup_{n \geqslant 0} \Lambda^n$ the set of words of the alphabet Λ. Given $\underline{\ell} \in \Omega$, let

$$\Sigma(\underline{\ell}) := \{x \in \Sigma : x \text{ starts by } \underline{\ell}\}$$

and

$$\Sigma_-(\underline{\ell}) := \{x \in \Sigma_- : x \text{ ends by } \underline{\ell}\}$$

Given a f-invariant probability measure μ on Σ, we denote by $\hat{\mu}$ the unique $\hat{f}$-invariant probability measure satisfying $p^+_*(\hat{\mu}) = \mu$, and we define $\mu_- := p^-_*(\hat{\mu})$.

Following [AV], we will make the following bounded distortion assumption on μ:

Definition 2.6 (Bounded distortion). We say that the f-invariant probability measure μ on Σ has the *bounded distortion* property if there exists a constant $C(\mu) > 0$ such that

$$\frac{1}{C(\mu)} \mu(\Sigma(\underline{\ell}_1)) \mu(\Sigma(\underline{\ell}_2)) \leqslant \mu(\Sigma(\underline{\ell}_1 \underline{\ell}_2)) \leqslant C(\mu) \mu(\Sigma(\underline{\ell}_1)) \mu(\Sigma(\underline{\ell}_2))$$

for any $\underline{\ell}_1, \underline{\ell}_2 \in \Omega$.

Remark 2.7. It is not hard to check that the bounded distortion property implies that μ is f-ergodic.

In this subsection, such (f, μ) and $(\hat{f}, \hat{\mu})$ will be the base dynamics. We now discuss the class of cocycles we want to investigate over these base dynamics. Given a map A from Σ with values in a matrix group $\mathbb{G}$ acting on $\mathbb{K}^d$, the associated cocycle itself is given by

$$(f, A) : \Sigma \times \mathbb{K}^d \to \Sigma \times \mathbb{K}^d, \quad (f, A)(x, v) = (f(x), A(x) \cdot v).$$

Here, the *basefield* $\mathbb{K}$ may be $\mathbb{R}$, $\mathbb{C}$ or the quaternion skew field $\mathbf{H}$.

For $\underline{\ell} = (\ell_0, \ldots, \ell_{n-1}) \in \Omega$, we define

$$A^{\underline{\ell}} := A_{\ell_{n-1}} \ldots A_{\ell_0}$$

so that we have $(f, A)^n(x, v) = (f^n(x), A^{\underline{\ell}} \cdot v)$ for $x \in \Sigma(\underline{\ell})$ and $v \in \mathbb{K}^d$.

In the works [AV2] and [AV], A. Avila and M. Viana treat the cases of $\mathbb{K} = \mathbb{R}$, $\mathbb{G} = \mathrm{GL}(d, \mathbb{R})$ and $\mathbb{G} = \mathrm{Sp}(d, \mathbb{R})$ respectively. They use their criterion in the symplectic case to prove the Kontsevich-Zorich conjecture. In this paper we take the opportunity to show (in Appendices A and B) how the arguments of A. Avila and M. Viana can be adapted in a straightforward way to give a unified treatment of the following cases:

- $\mathbb{K} = \mathbb{R}$, $\mathbb{G} = \mathrm{GL}(d, \mathbb{R})$ and $\mathbb{G} = \mathrm{Sp}(d, \mathbb{R})$;
- $\mathbb{K} = \mathbb{R}$ and $\mathbb{G}$ is an orthogonal group $O(p, q) = U_{\mathbb{R}}(p, q)$, $p + q = d$;

- $\mathbb{K} = \mathbb{C}$ and $\mathbb{G}$ is an complex unitary group $U_{\mathbb{C}}(p,q)$, $p+q=d$;
- $\mathbb{K} = \mathbf{H}$ and $\mathbb{G}$ is an quaternionic unitary group $U_{\mathbf{H}}(p,q)$, $p+q=d$.

Our main motivation to consider these cases come from the recent works [MYZ], [FMZ2] and [AMY] where several examples of cocycles with values in these matrix groups appear naturally as "blocks" of the Kontsevich-Zorich cocycle over the closure of $\mathrm{SL}_2(\mathbb{R})$-orbits of certain "symmetric" translation surfaces.

Remark 2.8. In the unitary case $U(p,q)$, we will always assume without loss of generality that $p \geqslant q$.

Definition 2.9. (Locally constant integrable cocycles) A cocycle $A : \Sigma \to \mathbb{G}$ is said to be

- *locally constant* if $A(\underline{x}) = A_{x_0}$ depends only on the initial letter x_0 of $\underline{x}$;
- *integrable* if $\int_{\Sigma} \log \|A^{\pm 1}(\underline{x})\| \, d\mu(\underline{x}) < \infty$.

For a locally constant cocycle, the integrability condition can be rewritten as

$$\sum_{\ell \in \Lambda} \mu(\Sigma(\ell)) \log \|A_{\ell}^{\pm 1}\| < \infty.$$

In the sequel, let μ be a f-invariant measure on Σ with the bounded distortion property and let A be a locally constant integrable $\mathbb{G}$-valued cocycle. As μ is ergodic and the cocycle is integrable, the Oseledets theorem gives the existence of Lyapunov exponents

$$\theta_1 \geqslant \ldots \geqslant \theta_d.$$

Remark 2.10. The Lyapunov exponents are counted above with *essential* multiplicities: in the complex case $\mathbb{K} = \mathbb{C}$, $\mathbb{C}^d$ is a $2d$-dimensional vector space over $\mathbb{R}$ and there are $2d$ Lyapunov exponents from the real point of view. But each appears twice; the essential multiplicity is half the real multiplicity. Similarly, in the quaternionic case, each exponent appears 4 times from the real point of view and the essential multiplicity is $\frac{1}{4}$ times the real multiplicity.

The matrix group $\mathbb{G}$ determines *a priori constraints* for the Lyapunov exponents (see, e.g., [MYZ] and [FMZ2]):

- in the symplectic case $\mathbb{G} = \mathrm{Sp}(d, \mathbb{R})$, d even, one has $\theta_i = -\theta_{d+1-i}$ for $1 \leqslant i \leqslant d$;
- in the real, complex or quaternionic unitary cases $\mathbb{G} = U_{\mathbb{K}}(p,q)$, $q \leqslant p$, $p+q=d$, one has $\theta_i = -\theta_{d+1-i}$ for $1 \leqslant i \leqslant q$ and $\theta_i = 0$ for $q < i \leqslant p$.

Also, in each of this case, the unstable Oseledets subspace associated to positive Lyapunov exponents is *isotropic*. The same is true for the stable subspace associated to the negative exponents.

Definition 2.11. The Lyapunov spectrum of the cocycle A is *simple* if

- $\theta_i > \theta_{i+1}$ for $1 \leqslant i < d$ in the cases $\mathbb{G} = \mathrm{GL}(d, \mathbb{R})$ and $\mathbb{G} = \mathrm{Sp}(d, \mathbb{R})$, d even;
- $\theta_i > \theta_{i+1}$ for $1 \leqslant i \leqslant q$ in the cases $\mathbb{G} = U_{\mathbb{K}}(p,q)$, $\mathbb{K} = \mathbb{R}, \mathbb{C}, \mathbf{H}$.

In other words, we say that a cocycle is *simple* when its Lyapunov spectrum is *as simple as possible* given the constraints presented above.

To formulate the main hypotheses on the cocycle, we first need to introduce Grassmannian manifolds adapted to $\mathbb{G}$. We say that an integer k is *admissible* if

- $1 \leqslant k < d$ when $\mathbb{G} = \mathrm{GL}(d, \mathbb{R})$ or $\mathrm{Sp}(d, \mathbb{R})$;
- $1 \leqslant k \leqslant q$ or $p \leqslant k < d = p+q$ in the unitary case $\mathbb{G} = U_{\mathbb{K}}(p,q)$, $p \geqslant q$.

Let k be an admissible integer. We denote by $G(k)$ the following Grassmannian manifold:

- when $\mathbb{G} = \mathrm{GL}(d, \mathbb{R})$, the Grassmannian of k-planes of $\mathbb{R}^d$;
- when $\mathbb{G} = \mathrm{Sp}(d, \mathbb{R})$, d even, the Grassmannian of k-planes which are *isotropic* (if $1 \leqslant k \leqslant d/2$) or *coisotropic* (if $d/2 \leqslant k < d$);
- when $\mathbb{G} = U_{\mathbb{K}}(p, q)$, the Grassmannian of k-planes over $\mathbb{K}$ which are *isotropic* (if $1 \leqslant k \leqslant q$) or *coisotropic* (if $p \leqslant k < d$).

At this point, we introduce the following two fundamental concepts:

Definition 2.12. The cocycle A is:

- *pinching* if there exists $\underline{\ell}^* \in \Omega$ such that the spectrum of the matrix $A^{\underline{\ell}^*}$ is simple (we then say that $A^{\underline{\ell}^*}$ is a *pinching matrix*).
- *twisting* ("strong form") if for any $m \geqslant 1$, any admissible integers $k_1, \ldots, k_m$, any subspaces $F_i \in G(k_i)$, $F_i' \in G(d - k_i)$, $1 \leqslant i \leqslant m$, there exists $\underline{\ell} \in \Omega$ such that $A^{\underline{\ell}}(F_i) \cap F_i' = \{0\}$.

We can know state the Avila-Viana simplicity criterion (cf. [AV, Theorem 7.1]), $\mathbb{G}$ being one of the groups mentioned above.

Theorem 2.13 (A. Avila and M. Viana). *Let μ be a f-invariant probability measure on Σ with the bounded distortion property. Let A be a locally constant integrable $\mathbb{G}$-valued cocycle. Assume that A is pinching and twisting. Then, the Lyapunov spectrum of (f, A) with respect to μ is simple.*

We will use a variant of this criterion with a relative version of twisting.

Definition 2.14. Let k be an admissible integer. Let $A \in \mathbb{G}$ be a pinching matrix. A matrix $B \in \mathbb{G}$ is *k-twisting with respect to* A if one has

$$B(F) \cap F' = \{0\}$$

for every pair of A-*invariant* subspaces $F \in G(k)$ and $F' \in G(d - k)$.

Remark 2.15. The point of this definition is that, given a pinching matrix A and an admissible integer k, there are only finitely many A-invariant subspaces $F \in G(k)$:

- when $\mathbb{G} = \mathrm{GL}(d, \mathbb{R})$ or $\mathbb{G} = \mathrm{Sp}(d, \mathbb{R})$, the eigenvalues of A are real and simple, and F is spanned by eigenvectors of A;
- when $\mathbb{G} = U_{\mathbb{K}}(p, q)$, $q \leqslant p$, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, A has q unstable simple eigenvalues $\lambda_1, \ldots, \lambda_q \in \mathbb{K}$ with

$$|\lambda_1| > \ldots > |\lambda_q| > 1,$$

q stable eigenvalues $\lambda_m' = \bar{\lambda}_m^{-1}$, and $p - q$ eigenvalues of modulus 1. Denote by $v_1, \ldots, v_q, v_1', \ldots, v_q'$ eigenvectors associated to $\lambda_1, \ldots, \lambda_q, \lambda_1', \ldots, \lambda_q'$. An isotropic A-invariant subspace is spanned by some of these eigenvectors (not allowing both v_m and v_m'). A coisotropic A-invariant subspace is the orthogonal complement of an isotropic A-invariant subspace.

- when $\mathbb{G} = U_{\mathbf{H}}(p, q)$, $q \leqslant p$, consider A as complex unitary of signature $(2p, 2q)$. Counted with multiplicity, its unstable eigenvalues are $\lambda_1, \bar{\lambda}_1, \ldots, \lambda_q, \bar{\lambda}_q$ with

$$|\lambda_1| > \ldots > |\lambda_q| > 1.$$

Its stable eigenvalues are $\lambda_m' = \lambda_m^{-1}, \bar{\lambda}_m', 1 \leqslant m \leqslant q$. Denote by v_m, v_m' eigenvectors associated to λ_i, λ_i'. Then $v_m.j$, resp. $v_m'.j$ are eigenvectors associated to $\bar{\lambda}_m$, resp. $\bar{\lambda}_m'$. An isotropic A-invariant $\mathbf{H}$-subspace is spanned by some of the

eigenvectors $v_1, \ldots, v'_q$ (not allowing both v_m and v'_m). A coisotropic A-invariant **H**-subspace is the orthogonal of an isotropic A-invariant **H**-subspace.

In Appendix B we will show the following result which relates the strong and relative versions of twisting:

Proposition 2.16. *A cocycle A is pinching and twisting (in its strong form) if and only if there exists a word $\underline{\ell}^* \in \Omega$ such that $A^{\underline{\ell}^*}$ is a pinching matrix and, for each admissible integer k, there exists a word $\underline{\ell}(k) \in \Omega$ such that $A^{\underline{\ell}(k)}$ is k-twisting with respect to $A^{\underline{\ell}^*}$.*

By putting together Theorem 2.13 and Proposition 2.16, we obtain the following variant of the Avila-Viana simplicity criterion:

Theorem 2.17. *Let μ be a f-invariant probability measure on Σ with the bounded distortion property. Let A be a locally constant integrable $\mathbb{G}$-valued cocycle. Assume that there exists a word $\underline{\ell}^* \in \Omega$ with the following properties:*

- *the matrix $A^{\underline{\ell}^*}$ is pinching;*
- *for each admissible integer k, there exists a word $\underline{\ell}(k) \in \Omega$ such that the matrix $A^{\underline{\ell}(k)}$ is k-twisting with respect to $A^{\underline{\ell}^*}$.*

Then, the Lyapunov spectrum of (f, A) with respect to μ is simple.

At this stage, this background section is complete and we pass to the discussion (in the next 3 sections) of Theorem 1.1.

3. MODULI SPACE AND CONTINUED FRACTION ALGORITHM FOR SQUARE-TILED SURFACES

The $\mathrm{SL}_2(\mathbb{R})$-orbits of reduced square-tiled surfaces are finite covers of the moduli space $\mathrm{SL}_2(\mathbb{R})/\mathrm{SL}_2(\mathbb{Z})$ of unit area lattices in the plane. The Teichmüller (geodesic) flow on $\mathrm{SL}_2(\mathbb{R})/\mathrm{SL}_2(\mathbb{Z})$ is naturally coded by the continued fraction algorithm. Of course, this is classical and it is described (at least partly) in several places, see, e.g., [Ar], [Da], [HL], [Mc2], [Se], [Zo7], [FMZ2], and references therein. However, for our current purpose of coding the Teichmüller flow and KZ cocycle over the $\mathrm{SL}_2(\mathbb{R})$-orbit of a reduced square-tiled surface, we need a somewhat specific version of this coding that we were unable to locate in the literature.[7]

In the first subsection, we introduce this specific version for the diagonal flow on the modular curve $\mathrm{SL}_2(\mathbb{R})/\mathrm{SL}_2(\mathbb{Z})$. Then, we define a similar coding for the Teichmüller flow on the $\mathrm{SL}_2(\mathbb{R})$-orbit of a reduced square-tiled surface. The KZ-cocycle has a natural discrete-time version adapted to this coding. Finally, we explain why we may assume that the base dynamics satisfies the hypotheses of Theorem 2.17. The pinching and twisting conditions in this theorem are the subject of the next section.

3.1. **The torus case.** The continued fraction algorithm is generated by the *Gauss map*

$$\begin{aligned} G : (0,1) \cap (\mathbb{R} - \mathbb{Q}) &\rightarrow (0,1) \cap (\mathbb{R} - \mathbb{Q}) \\ G(\alpha) &= \{\alpha^{-1}\}, \end{aligned}$$

---

[7] When this paper was almost complete, A. Eskin and the first author [EMat] observed that the study of Lyapunov exponents of the KZ cocycle over *closed $SL(2,\mathbb{R})$*-orbits can be performed *without* the aid of a coding of the Teichmüller flow and KZ cocycle thanks to a profound theorem of H. Furstenberg on the Poisson boundary of homogenous spaces.

where $\{x\}$ is the fractional part of $x \in \mathbb{R}$. The *Gauss measure* $\frac{dt}{1+t}$ is up to normalization the only G-invariant finite measure on $(0, 1)$ which is absolutely continuous with respect to Lebesgue measure.

Defining

$$a(x) := \lfloor x^{-1} \rfloor \in \mathbb{Z}_{>0}, \quad \text{for } x \in (0, 1)$$

and

$$\underline{a}(\alpha) := (a(G^n(\alpha)))_{n \geqslant 0}, \quad \text{for } \alpha \in (0, 1) \cap (\mathbb{R} - \mathbb{Q}),$$

we obtain the classical conjugacy between the Gauss map and the shift map

$$f : (\mathbb{Z}_{>0})^{\mathbb{N}} \to (\mathbb{Z}_{>0})^{\mathbb{N}}$$

on infinitely many symbols. For further reference, we note that

Proposition 3.1. *The Gauss measure, transferred to $(\mathbb{Z}_{>0})^{\mathbb{N}}$ by the conjugacy, has bounded distortion.*

Proof. For $n > 0$, $a_0, \ldots, a_{n-1} \in \mathbb{Z}_{>0}$, the cylinder $\{\alpha, \, a(G^i(\alpha)) = a_i, \, \forall 0 \leqslant i < n\}$ is the Farey interval with endpoints $\frac{P}{Q}, \frac{p+P}{q+Q}$, with

$$\begin{pmatrix} p & P \\ q & Q \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & a_0 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & a_{n-1} \end{pmatrix}.$$

Observe that $Q \geqslant q, P \geqslant p$. As the density of the Gauss measure is bounded away from 0 and $+\infty$ on $(0, 1)$, the Gauss measure of this cylinder is of order Q^{-2}. Let $\{\alpha, \, a(G^j(\alpha)) = a_{n+j}, \, \forall 0 \leqslant j < m\}$ be another cylinder, and let $\frac{P'}{Q'}, \frac{p'+P'}{q'+Q'}$ be the endpoints of the associated Farey interval. For the cylinder

$$\{\alpha, \, a(G^i(\alpha)) = a_i, \, \forall 0 \leqslant i < m + n\},$$

the associated Farey interval has endpoints $\frac{\bar{P}}{\bar{Q}}, \frac{\bar{p}+\bar{P}}{\bar{q}+\bar{Q}}$, with

$$\begin{pmatrix} \bar{p} & \bar{P} \\ \bar{q} & \bar{Q} \end{pmatrix} = \begin{pmatrix} p & P \\ q & Q \end{pmatrix} \begin{pmatrix} p' & P' \\ q' & Q' \end{pmatrix}.$$

Its Gauss measure has order $\bar{Q}^{-2}$, and we have

$$QQ' \leqslant \bar{Q} = qP' + QQ' \leqslant 2QQ'.$$

The proof of the bounded distortion property is complete. $\qquad\square$

We will use the map $\tilde{G}$ derived from the Gauss map as follows:

$$\tilde{G} : \{t, b\} \times [(0, 1) \cap (\mathbb{R} - \mathbb{Q})] \quad \to \quad \{t, b\} \times [(0, 1) \cap (\mathbb{R} - \mathbb{Q})]$$
$$\tilde{G}(t, \alpha) = (b, G(\alpha)), \qquad G(b, \alpha) = (t, G(\alpha)).$$

(The letters t and b stand for top and bottom respectively.) Putting the Gauss measure on each copy of $(0, 1)$ gives a natural invariant measure that we still call the Gauss measure. For a symbolic model for $\tilde{G}$, we consider the graph Γ with two vertices called b, t and two countable families of arrows $(\gamma_{a,t})_{a \geqslant 1}$ from t to b and $(\gamma_{a,b})_{a \geqslant 1}$ from b to t. To a point (c, α), $c \in \{t, b\}$, we associate the path in Γ starting from c such that the first indices of the successive arrows are the $a(G^n(\alpha))$, $n \geqslant 0$. In this way, we get a conjugacy between $\tilde{G}$ and the shift map on the set of infinite paths in Γ.

To make the connection with the flow on the homogeneous space $\mathrm{SL}_2(\mathbb{R})/\mathrm{SL}_2(\mathbb{Z})$ (viewed as the space of normalized lattices in the plane) given by left multiplication by

the diagonal subgroup $\mathrm{diag}(e^t, e^{-t})$, we use the following lemma. Call a normalized lattice *irrational* if it intersects the vertical and horizontal axes only at the origin. The set of irrational lattices is invariant under the diagonal flow.

Lemma 3.2. *Let L be an irrational normalized lattice in $\mathbb{R}^2$. There exists a unique basis $v_1 = (\lambda_1, \tau_1)$, $v_2 = (\lambda_2, \tau_2)$ of L such that*

$$\text{either} \quad \lambda_2 \geqslant 1 > \lambda_1 > 0,\ 0 < \tau_2 < -\tau_1 \quad \text{or} \quad \lambda_1 \geqslant 1 > \lambda_2 > 0,\ 0 < -\tau_1 < \tau_2.$$

Proof. We look for non zero vectors of L in the squares $Q_+ := (0,1) \times (0,1)$ and $Q_- := (0,1) \times (-1,0)$. First observe that Q_+ cannot contain two independent vectors of L, because the absolute value of their determinant would belong to $(0,1)$. Similarly for Q_-. On the other hand, the union $Q_+ \bigcup Q_-$ must contain a vector of L by Minkowski's theorem. In fact, otherwise (using also that L is irrational), there would exist a set of area > 1 whose translates by L are disjoint. Therefore either $Q_+ \bigcup Q_-$ contains exactly one primitive vector of L or both Q_+ and Q_- contain exactly one primitive vector of L.

In the first case, we can assume that Q_- contains a primitive vector $v_1 = (\lambda_1, \tau_1)$. Let $v_2 = (\lambda_2, \tau_2) \in L$ such that $\lambda_1 \tau_2 - \lambda_2 \tau_1 = 1$ and $\tau_2 > 0$ is minimum. Then $0 < \tau_2 < -\tau_1 < 1$, hence $\lambda_2 > 0$. As Q_+ does not contain any vector of L, we have $\lambda_2 \geqslant 1$ and the basis (v_1, v_2) of L has the required properties. On the other hand, if a basis (v_1', v_2') has the required properties, either $\lambda_2' \geqslant 1 > \lambda_1' > 0$, $0 < \tau_2' < -\tau_1'$ holds or $\lambda_1' \geqslant 1 > \lambda_2' > 0$, $0 < -\tau_1' < \tau_2'$ holds. However, in the second case, the relation $\lambda_1' \tau_2' - \lambda_2' \tau_1' = 1$ would imply that $v_2' \in Q_+$, contrary to the assumption that Q_+ does not contain any vector of L. Thus we have that $\lambda_2' \geqslant 1 > \lambda_1' > 0$, $0 < \tau_2' < -\tau_1'$ holds. Then we must have $v_1' \in Q_-$, hence $v_1' = v_1$. From the inequality on τ_2', it follows then that $v_2' = v_2$, which concludes the proof of the lemma in this case.

In the second case we now assume that Q_- contains a (unique) primitive vector $V_1 = (\Lambda_1, T_1)$ of L and that Q_+ contains a (unique) primitive vector $V_2 = (\Lambda_2, T_2)$ of L. As $\Lambda_1 T_2 - \Lambda_2 T_1 \geqslant 1$, we have $\Lambda_1 + \Lambda_2 > 1$. Observe also that we have $\Lambda_1 T_2 - \Lambda_2 T_1 < 2$, hence $\Lambda_1 T_2 - \Lambda_2 T_1 = 1$. As L is irrational, we have that $T_1 + T_2 \neq 0$. If $T_1 + T_2 > 0$, we set $v_1 = V_1$, $v_2 = nV_1 + V_2$, where $n \geqslant 1$ is the largest integer such that $nT_1 + T_2 > 0$; if $T_1 + T_2 < 0$, we set similarly $v_2 = V_2$, $v_1 = V_1 + nV_2$, where $n \geqslant 1$ is the largest integer such that $nT_2 + T_1 < 0$. We obtain a basis of L satisfying the required conditions. Conversely, let (v_1', v_2') be a basis with the required properties. Assume for instance that $\lambda_2' \geqslant 1 > \lambda_1' > 0$, $0 < \tau_2' < -\tau_1'$ holds. Then $v_1' \in Q_-$, hence $v_1' = V_1$. Then we must have $v_2' = V_2 + mV_1$ for some integer $m \geqslant 1$, and the condition on τ_2' guarantees that $v_1' = v_1$, $v_2' = v_2$.

The proof of the lemma is complete. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Definition 3.3. We say that the irrational lattice L is of *top* type if the basis selected by the lemma satisfies $\lambda_2 \geqslant 1 > \lambda_1 > 0$, $0 < \tau_2 < -\tau_1$, of *bottom* type if it satisfies $\lambda_1 \geqslant 1 > \lambda_2 > 0$, $0 < -\tau_1 < \tau_2$.

Let L be an irrational normalized lattice, and let (v_1, v_2) be the basis of L selected by the lemma. Set $\alpha := \frac{\lambda_1}{\lambda_2}$ if L is of top type, $\alpha := \frac{\lambda_2}{\lambda_1}$ if L is of bottom type, so that $\alpha \in (0, 1)$.

Assume for instance that L is of top type. Let $(L_t)_{t \geqslant 0}$ be the positive orbit of L under the diagonal flow, and let $(v_1(t), v_2(t))$ be the basis of L_t obtained by applying $\mathrm{diag}(e^t, e^{-t})$ to v_1, v_2. For $0 \leqslant t < t^* := -\log \lambda_1$, the basis $v_1(t), v_2(t)$ of L_t satisfies the conditions of the lemma and L_t is of top type. For $t = t^*$, the lattice L_{t^*} is of bottom type and the basis selected by the lemma is $v_1^* = v_1(t^*)$, $v_2^* = v_2(t^*) - av_1(t^*)$, where

$a \geqslant 1$ is the integral part of α^{-1}. Thus, we have exchanged top and bottom with respect to the initial conditions and the new relevant ratio is

$$\alpha^* = \frac{\lambda_2^*}{\lambda_1^*} = \frac{\lambda_2 - a\lambda_1}{\lambda_1} = \frac{1}{\alpha} - a$$

according to the continued fraction algorithm recipe. We have thus shown the

Proposition 3.4. *The diagonal flow on irrational normalized lattices is the suspension over the shift map on bi-infinite paths in Γ, with roof function $\log \alpha^{-1}$.*

Here, a bi-infinite path is one which extends indefinitely in both past and future. The number α associated to a bi-infinite path $\underline{\gamma} = \underline{\gamma^-} * \underline{\gamma^+}$ in position $c \in \{t, b\}$ at time 0 is such that $\underline{\gamma^+}$ is associated to (c, α) in the coding of $\tilde{G}$ described above.

3.2. **A graph associated to a square-tiled surface.** Let now M be a reduced square-tiled surface, let $\mathrm{SL}(M)$ be its Veech group, and let $\ell = \ell(M)$ be the index of $\mathrm{SL}(M)$ in $\mathrm{SL}_2(\mathbb{Z})$. The $\mathrm{SL}_2(\mathbb{R})$-orbit of M in the moduli space of translation surfaces is the homogeneous space $\mathrm{SL}_2(\mathbb{R})/\mathrm{SL}(M)$, which is a covering of degree $\ell(M)$ of $\mathrm{SL}_2(\mathbb{R})/\mathrm{SL}_2(\mathbb{Z})$. We use this in order to encode the diagonal (Teichmüller) flow on the $\mathrm{SL}_2(\mathbb{R})$-orbit of M.

Let $M_1 = M, \ M_2, \ldots, M_\ell$ be the square-tiled surfaces (up to isomorphism) constituting the orbit of M under the action of $\mathrm{SL}_2(\mathbb{Z})$. Let $\Gamma(M)$ be the graph defined as follows

- the set of vertices $\mathrm{Vert}(\Gamma(M))$ is the product $\{M_1, \ldots, M_\ell\} \times \{t, b\}$;
- from every vertex (M_i, c) ($c \in \{t, b\}$) and every integer $a \geqslant 1$, there is an arrow $\gamma_{a,i,c}$ starting from (M_i, c), whose endpoint (M_j, c') is given by

$$M_j = \left(\begin{array}{cc} 1 & a \\ 0 & 1 \end{array} \right) \cdot M_i, \ c' = b, \qquad \text{if } c = t,$$

$$M_j = \left(\begin{array}{cc} 1 & 0 \\ a & 1 \end{array} \right) \cdot M_i, \ c' = t, \qquad \text{if } c = b.$$

- there are no other arrows.

When $\ell = 1$, i.e the Veech group of M is equal to $SL_2(\mathbb{Z})$, the graph $\Gamma(M)$ is the graph Γ of the last subsection.

Consider now the orbit under the Teichmüller flow of a point $g_0.M$ ($g_0 \in \mathrm{SL}_2(\mathbb{R})$) of the orbit of M. We first find the vertex of $\Gamma(M)$ associated to this initial point as follows. We apply Lemma 3.2 to $L = g_0(\mathbb{Z}^2)$ (we assume that this lattice is irrational). Denoting by (e_1, e_2) the canonical basis of $\mathbb{Z}^2$, we obtain from this lemma a matrix $g_0^* \in \mathrm{SL}_2(\mathbb{Z})$ such that the basis of L with the required (top or bottom) property is $v_1 = g_0((g_0^*)^{-1}e_1), v_2 = g_0((g_0^*)^{-1}e_2)$. The vertex associated to $g_0.M$ is then $(g_0^*.M, c)$ where c is the type of L.

When we flow from this initial condition under the Teichmüller flow, the lattice L evolves under the diagonal flow and first changes type at some time t^*. As explained at the end of the last subsection, the new selected basis is related to the old by **right** multiplication by

$$\left(\begin{array}{cc} 1 & -a \\ 0 & 1 \end{array} \right) (\text{if } c = t) \quad \text{or} \quad \left(\begin{array}{cc} 1 & 0 \\ -a & 1 \end{array} \right) (\text{if } c = b),$$

where a is the integral part of α^{-1}. This corresponds to the arrow of index a in $\gamma(M)$ starting from $(g_0^*.M, c)$.

This procedure allows to associate to every irrational orbit (i.e., one which neither starts nor ends in a cusp of $\mathrm{SL}_2(\mathbb{R})/\mathrm{SL}(M)$) a bi-infinite path in $\Gamma(M)$. Conversely, every bi-infinite path in $\Gamma(M)$ corresponds to a unique irrational orbit. Here, the time for the orbits and for the paths runs from $-\infty$ to $+\infty$.

If we consider instead infinite paths in $\Gamma(M)$ (with a starting point in $\mathrm{Vert}(\Gamma(M))$ at time 0), the shift map is conjugated to the map $\tilde{G}_M$ defined by

$$\tilde{G}_M : \mathrm{Vert}(\Gamma(M)) \times [(0,1) \cap (\mathbb{R} - \mathbb{Q})] \rightarrow \mathrm{Vert}(\Gamma(M)) \times [(0,1) \cap (\mathbb{R} - \mathbb{Q})]$$
$$\tilde{G}_M(M_i, c, \alpha) = (M_j, c', G(\alpha)),$$

where (M_j, c') is the endpoint of $\gamma_{a(\alpha),i,c}$.

Summing up

Proposition 3.5. *The diagonal flow on $SL_2(\mathbb{R})/SL(M)$ is the suspension over the shift map on bi-infinite paths in $\Gamma(M)$, with roof function $\log \alpha^{-1}$. The number α associated to a bi-infinite path $\underline{\gamma} = \underline{\gamma}^- * \underline{\gamma}^+$ is the second coordinate of the point associated to $\underline{\gamma}^+$ in the coding of $\tilde{G}_M$.*

Remark 3.6. The roof function is integrable w.r.t. the (transferred) Gauss measure on the space of paths because the homogeneous space $SL_2(\mathbb{R})/SL(M)$ has finite Haar measure.

3.3. **A discrete version of the KZ-cocycle.** Let M be a reduced square-tiled surface and let $A \in SL_2(\mathbb{Z})$. Recall that the preferred atlas of the square-tiled surface $M' = A.M$ is obtained from the preferred atlas of M by postcomposition of the $\mathbb{R}^2$-valued charts by A. Therefore, if we consider the identity map of M as a map from M to M', it becomes an affine map with derivative A. However, as we identify in moduli space isomorphic square-tiled surfaces, this map is only well-defined in general up to precomposition by an automorphism of M (or equivalently postcomposition by an automorphism of M'). From now on, we assume that the automorphism group of M is trivial.

To each arrow $\gamma_{a,i,c} : (M_i, c) \rightarrow (M_j, c')$ of $\Gamma(M)$, we associate the affine map $A_{a,i,c}$ from M_i to M_j whose linear part is

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} (\text{if } c = t) \quad \text{or} \quad \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} (\text{if } c = b).$$

When $\underline{\gamma}$ is a path in $\Gamma(M)$ (starting at a vertex (M_i, c), ending at a vertex (M_j, c')), which is the concatenation of arrows $\gamma_1, \ldots, \gamma_k$, we associate to $\underline{\gamma}$ the affine map $A_{\underline{\gamma}}$ which is the composition $A_k \circ \ldots \circ A_1$ of the affine maps $A_1, \ldots, A_k$ associated to $\gamma_1, \ldots, \gamma_k$. Then $A_{\underline{\gamma}}$ is an affine map from M_i to M_j.

We have given in Proposition 3.5 a description of the restriction of the Teichmüller flow to the $SL_2(\mathbb{R})$-orbit of M. The version of the KZ-cocycle which is adapted to this description is defined in the following way. The space is the vector bundle $\mathcal{H}_M$ over $\mathrm{Vert}(\Gamma(M)) \times [(0,1) \cap (\mathbb{R} - \mathbb{Q})]$ whose fiber over (M_i, c, α) is $H_1(M_i, \mathbb{R})$. The cocycle is the map G_M^{KZ} fibered over $\tilde{G}_M$ such that

$$G_M^{KZ}(M_i, c, \alpha, v) = (M_j, c', G(\alpha), (A_{a(\alpha),i,c})_*(v)),$$

where $(A_{a(\alpha),i,c})_*$ is the homomorphism from $H_1(M_i, \mathbb{R})$ to $H_1(M_j, \mathbb{R})$ induced by the affine map $A_{a(\alpha),i,c}$.

As the diagonal flow on $SL_2(\mathbb{R})/SL(M)$ is ergodic, the Lyapunov exponents of G_M^{KZ} are constant a.e and proportional to the Lyapunov exponents of the continuous time version of the KZ-cocycle (w.r.t. Haar measure on $SL_2(\mathbb{R})/SL(M)$). In order to determine whether the Lyapunov spectrum is simple, it is sufficient to consider G_M^{KZ}.

3.4. **Return map and full shift.** We intend to prove below the simplicity of the Lyapunov spectrum by applying Avila-Viana's criterion (Theorem 2.17). The base dynamics in the statement of this theorem is a full shift over an alphabet with at most countably many symbols. The base dynamics in the discrete version of the KZ-cocycle of the last subsection is the shift in the space of infinite paths in the graph $\Gamma(M)$ of Subsection 3.2. As $\Gamma(M)$ has more than one vertex, this is not a full shift.

Nevertheless, it is easy to fall back into the setting of theorem 2.17. Indeed, the map $\tilde{G}_M$ is ergodic (for the Gauss measure). Choose any vertex $\mathcal{V}$ of $\Gamma(M)$. Almost every path in $\Gamma(M)$ (with respect to the Gauss measure) goes through $\mathcal{V}$ infinitely many times. We consider the *return map* $\tilde{G}_{M,\mathcal{V}}$ for $\tilde{G}_M$ to the subset $\{\mathcal{V}\} \times [(0,1) \cap (\mathbb{R} - \mathbb{Q})]$. The Gauss measure (in the fiber over $\mathcal{V}$) is invariant by $\tilde{G}_{M,\mathcal{V}}$. The return map $\tilde{G}_{M,\mathcal{V}}$ is canonically conjugated to the full shift over the alphabet whose letters are the loops in $\Gamma(M)$ which go exactly once through $\mathcal{V}$.

Observe that these letters correspond to words in the natural coding of the Gauss map G considered in Subsection 3.1. Therefore the bounded distortion property in the new setting follows from the same property in that setting (proposition 3.1).

The cocycle over this full shift induced by the cocycle G_M^{KZ} of the previous subsection is clearly locally constant. It is also *integrable*. Indeed, by submultiplicativity of the norm, it is sufficient to show that G_M^{KZ} is integrable. For this purpose we use that the norm of $(A_{a,i,c})_*$ acting on homology has order at most a for large a, and the interval $(\frac{1}{a+1}, \frac{1}{a})$ of α such that $a(\alpha) = a$ has Gauss measure of order a^{-2}. As the series $\sum_{a \geqslant 1} a^{-2} \log a$ is convergent, the integrability follows.

3.5. **Loops in $\Gamma(M)$ and affine pseudo-Anosov maps.** To determine which affine self-maps of M correspond to **loops** in $\Gamma(M)$, we recall an elementary property of $SL(2, \mathbb{Z})$ related to the continued fraction algorithm.

Definition 3.7. A matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ is *b-reduced* if

$$a > \max(b, c) \geqslant \min(b, c) \geqslant d > 0.$$

The matrix A is *t-reduced* if

$$d > \max(b, c) \geqslant \min(b, c) \geqslant a > 0.$$

Equivalently, A is t-reduced if its conjugate by $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is b-reduced.

Proposition 3.8. *A matrix $A \in \mathrm{SL}_2(\mathbb{Z})$ is b-reduced if and only if there exist $k \geqslant 1$ and integers $a_1, \ldots, a_{2k} \geqslant 1$ such that*

$$A = \begin{pmatrix} 1 & a_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a_2 & 1 \end{pmatrix} \cdots \begin{pmatrix} 1 & a_{2k-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a_{2k} & 1 \end{pmatrix}.$$

Moreover, such a decomposition of a b-reduced matrix is unique.

Proof. An elementary calculation shows that the product of two b-reduced matrices is b-reduced. Also, for $a, b \geqslant 1$, the product

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

is b-reduced. Therefore, products of the form appearing in the proposition are b-reduced. Conversely, it is a classical elementary lemma that any $A \in \mathrm{SL}_2(\mathbb{Z})$ with nonnegative coefficients can be written in a unique way as

$$A = \begin{pmatrix} 1 & a_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a_2 & 1 \end{pmatrix} \cdots \begin{pmatrix} 1 & a_{2k-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a_{2k} & 1 \end{pmatrix},$$

with $k \geqslant 1$, and integers $a_1 \geqslant 0$, $a_{2k} \geqslant 0$, $a_i \geqslant 1$ for $0 < i < 2k$. It is now trivial to check that A is not b-reduced unless a_1 and a_{2k} are both $\geqslant 1$. $\qquad\square$

Corollary 3.9. *The affine self-maps of M associated to the loops of $\Gamma(M)$ based at (M, b) (resp. (M, t)) are exactly those which have a b-reduced (resp. t-reduced) linear part.*

Remark 3.10. It is a standard fact from Gauss theory of reduction of quadratic forms that any matrix in $SL_2(\mathbb{Z})$ with trace > 2 is conjugated in $SL_2(\mathbb{Z})$ to a b-reduced matrix.

4. GALOIS-PINCHING

4.1. **Galois-pinching matrices.** Let Ω be an integer-valued symplectic form on $\mathbb{Z}^{2d}$. We will denote by $Sp(\Omega, \mathbb{Z})$ the group of matrices in $SL(2d, \mathbb{Z})$ which preserve Ω.

Let $A \in Sp(\Omega, \mathbb{Z})$. The characteristic polynomial of A is a monic reciprocal polynomial P of degree $2d$ with integer coefficients. Let $\widetilde{R} = \{\lambda_i, \lambda_i^{-1} : 1 \leqslant i \leqslant d\}$ be the set of roots of P. For $\lambda \in \widetilde{R}$, define $p(\lambda) := \lambda + \lambda^{-1}$ and let $R := p(\widetilde{R})$.

Definition 4.1. The matrix $A \in Sp(\Omega, \mathbb{Z})$ is *Galois-pinching* if its characteristic polynomial P satisfies the following conditions
- P is irreducible over $\mathbb{Q}$;
- all roots of P are real, i.e $\widetilde{R} \subset \mathbb{R}$;
- the Galois group Gal of P is the largest possible, that is, Gal acts on R by the full permutation group of R, and the subgroup fixing each element of R acts by independent transpositions of each of the d pairs $\{\lambda_i, \lambda_i^{-1}\}$; in other words,

$$Gal \simeq S_d \ltimes (\mathbb{Z}/2\mathbb{Z})^d.$$

For each $\lambda \in \widetilde{R}$, we denote by $v_\lambda \in \mathbb{R}^{2d}$ an eigenvector of A corresponding to this eigenvalue with coordinates in the field $\mathbb{Q}(\lambda)$. We assume that the choices are coherent in the sense that $g(v_\lambda) = v_{g.\lambda}$ for $g \in Gal$.

Proposition 4.2. *A Galois-pinching matrix is pinching.*

Proof. Indeed, by the first two conditions, all eigenvalues are simple and real. The only possibility preventing A to be pinching would be to have both λ and $-\lambda$ as eigenvalues, but this is not compatible with the third condition: an element of the Galois group fixing λ will also fix $-\lambda$. $\qquad\square$

The following result will be used in the proof of Theorem 1.1.

Proposition 4.3. *Let A, B be two elements of $Sp(\Omega, \mathbb{Z})$. Assume that A is Galois-pinching, and that B is unipotent and distinct from the identity. If A, B share a common proper invariant subspace, then $(B - id)(\mathbb{R}^{2d})$ is a lagrangian subspace of $\mathbb{R}^{2d}$.*

Proof. A subspace of $\mathbb{R}^{2d}$ which is invariant under A is spanned by eigenvectors of A. Let $R^{\ddagger} \subset \widetilde{R}$ be a non-empty subset with minimal cardinality such that the subspace $E(R^{\ddagger})$ spanned by the vectors v_λ, $\lambda \in R^{\ddagger}$, is also invariant under B. As B has integer coefficients, the subset $\sigma(R^{\ddagger})$ has the same property, for any element σ of the Galois group Gal of P.

As the cardinal of $R^\ddagger$ was chosen to be minimal, we must have either $\sigma(R^\ddagger) = R^\ddagger$ or $\sigma(R^\ddagger) \cap R^\ddagger = \emptyset$.

The only proper subsets $R^\ddagger$ with this property are the 1-element subsets and the 2-elements subsets of the form $\{\lambda, \lambda^{-1}\}$.

The first case cannot occur: if one had $B(v_\lambda) = c v_\lambda$ for some $\lambda \in \widetilde{R}$, $c \in \mathbb{R}$, then c should be equal to 1 as B is unipotent, and B should fix all eigenvectors of A (applying the action of Gal) and thus be equal to the identity.

Therefore, B preserves some 2-dimensional subspace $E(\lambda, \lambda^{-1})$. Applying Gal, we see that B preserves each subspace of this form, and the restrictions of B to these subspaces are Galois-conjugated. As B is unipotent distinct from the identity, the image of each such 2-dimensional subspace by $(B - \mathrm{id})$ has dimension 1. These 2-dimensional subspaces are Ω-orthogonal. Therefore $(B - \mathrm{id})(\mathbb{R}^{2d})$ is Ω-lagrangian. $\qquad\square$

Remark 4.4. The proof is still valid if $B \in SL(2d, \mathbb{Z})$ instead of $Sp(\Omega, \mathbb{Z})$.

4.2. **A twisting criterion for Galois-pinching matrices.** The most important ingredient towards Theorem 1.1 is the following theorem:

Theorem 4.5. *Let A, B be two elements of $Sp(\Omega, \mathbb{Z})$. Assume that A is Galois-pinching, and that A and B^2 don't share a common proper invariant subspace. Then, there exist $m \geqslant 1$, and, for any ℓ^*, integers $\ell_1, \ldots, \ell_{m-1}$ larger than ℓ^* such that the product*

$$BA^{\ell_1} \cdots BA^{\ell_{m-1}} B$$

is k-twisting with respect to A for all $1 \leqslant k \leqslant d$.

The proof of this result occupies the rest of this section.

We keep the notations of Subsection 4.1. As A is assumed to be Galois-pinching, the set $\widetilde{R}$ has $2d$ elements and is contained in $\mathbb{R}$; the set R has d elements and is contained in $\mathbb{R} - [-2, 2]$.

For $1 \leqslant k \leqslant d$, denote by $\widetilde{R}_k$ the set of all subsets of $\widetilde{R}$ with k elements, by R_k the set of all subsets of R with k elements, and by $\widehat{R}_k$ the set of all subsets of $\widetilde{R}$ with k elements on which the restriction of p is injective (so that their images under p belong to R_k). We identify $\widetilde{R}_1 = \widehat{R}_1$ with $\widetilde{R}$.

For $\underline{\lambda} = \{\lambda_1 < \cdots < \lambda_k\} \in \widetilde{R}_k$, let $v_{\underline{\lambda}} := v_{\lambda_1} \wedge \cdots \wedge v_{\lambda_k} \in \wedge^k \mathbb{R}^{2d}$. It is an eigenvector of $\wedge^k A$ with eigenvalue $N(\underline{\lambda}) := \prod_i \lambda_i$. The $v_{\underline{\lambda}}$, for $\underline{\lambda} \in \widetilde{R}_k$, form a basis of $\wedge^k \mathbb{R}^{2d}$.

4.3. **Transversality condition.** Using these notations, we can now translate the condition that a matrix C is k-twisting with respect to A in terms of certain matrix entries of its kth exterior power $\wedge^k C$.

Lemma 4.6. *Let $C^{(k)}_{\underline{\lambda}\,\underline{\lambda}'}$, $\underline{\lambda}, \underline{\lambda}' \in \widetilde{R}_k$, be the coefficients of the matrix of $\wedge^k C$ in the basis $(v_{\underline{\lambda}})_{\underline{\lambda} \in \widetilde{R}_k}$. Then, C is k-twisting with respect to A if and only if for all $1 \leqslant k \leqslant d$ all coefficients $C^{(k)}_{\underline{\lambda}\,\underline{\lambda}'}$ with $\underline{\lambda}, \underline{\lambda}' \in \widehat{R}_k$ are non-zero.*

Proof. Let E, F be A-invariant subspaces of respective dimensions k and $2d - k$. Let $\underline{\lambda}_E \in \widetilde{R}_k$ be the subset such that E is generated by the v_λ with $\lambda \in \underline{\lambda}_E$. Observe that E is isotropic if and only if $\underline{\lambda}_E$ belongs to $\widehat{R}_k$. Similarly, let $\underline{\lambda}'_F \in \widetilde{R}_k$ be the subset such that F is generated by the v_λ with $\lambda \notin \underline{\lambda}'_F$. It belongs to $\widehat{R}_k$ if and only if F is coisotropic. Write $\underline{\lambda}_F$ for the complement of $\underline{\lambda}'_F$ in $\widetilde{R}$. Now $C(E)$ is transverse to F if and only if the exterior

product $\wedge^k C(v_{\underline{\lambda}_E}) \wedge v_{\underline{\lambda}_F}$ is nonzero. This happens precisely if and only if the coefficient $C^{(k)}_{\underline{\lambda}_E \underline{\lambda}'_F}$ is nonzero.   □

4.4. **Mixing graphs.** Recall that an oriented graph Γ (with a finite set of vertices) is *connected* if for every vertices x, y of Γ, there is an **oriented** path from x to y. It is *mixing* if there exists an integer m such that, for every vertices x, y of Γ, there is an oriented path of length m from x to y. If it is the case, any large enough integer m has this property.

Let $C \in \mathrm{Sp}(\Omega, \mathbb{Z})$. For $1 \leqslant k \leqslant d$, we define an oriented graph $\Gamma_k = \Gamma_k(C)$ as follows: the vertices of Γ_k are the elements of $\widehat{R}_k$; for $\underline{\lambda}_0, \underline{\lambda}_1 \in \widehat{R}_k$, there is an arrow from $\underline{\lambda}_0$ to $\underline{\lambda}_1$ if and only if the coefficient $C^{(k)}_{\underline{\lambda}_0 \underline{\lambda}_1}$ of the matrix of $\wedge^k C$, written in the basis $(v_{\underline{\lambda}})_{\underline{\lambda} \in \widetilde{R}_k}$, is nonzero. For later use, we observe that $\Gamma_k(C)$ is *invariant* under the natural action of the Galois group Gal.

By Lemma 4.6, C is k-twisting with respect to A if and only if the graph $\Gamma_k(C)$ is complete. In general, it is not easy to verify that $\Gamma_k(C)$ is a complete graph, but this is not an obstacle because, as we're going to see now, for our purposes it suffices to check the mixing property for $\Gamma_k(C)$.

More precisely, let $1 \leqslant k \leqslant d$ and **assume that $\Gamma_k(C)$ is mixing**. Let m be a positive integer such that, for every vertices $\underline{\lambda}_0, \underline{\lambda}_1$ of $\Gamma_k(C)$, there is an oriented path of length m from $\underline{\lambda}_0$ to $\underline{\lambda}_1$. For nonnegative integers $\ell_1, \cdots, \ell_{m-1}$, consider

$$D = CA^{\ell_1} \cdots CA^{\ell_{m-1}} C.$$

Proposition 4.7. *There are finitely many hyperplanes $V_1, \cdots, V_t$ in $\mathbb{R}^{m-1}$ such that, if $\underline{\ell} := (\ell_1, \cdots, \ell_{m-1}) \in \mathbb{Z}^{m-1}$ goes to infinity along a rational line not lying in any of the V_p, then, for $\|\underline{\ell}\|$ large enough, the matrix D is k-twisting with respect to A.*

Proof. We write $\wedge^k C$, $\wedge^k D$ in the basis $(v_{\underline{\lambda}})_{\underline{\lambda} \in \widetilde{R}_k}$. Define a graph Γ'_k with set of vertices $\widetilde{R}_k$ and an arrow from $\underline{\lambda}_0$ to $\underline{\lambda}_1$ if and only if the coefficient $C^{(k)}_{\underline{\lambda}_0 \underline{\lambda}_1}$ is nonzero. We have, for $\underline{\lambda}_0, \underline{\lambda}_m \in \widetilde{R}_k$

$$D^{(k)}_{\underline{\lambda}_0 \underline{\lambda}_m} = \sum_{\underline{\lambda}_1, \dots, \underline{\lambda}_{m-1}} C^{(k)}_{\underline{\lambda}_0 \underline{\lambda}_1} N(\underline{\lambda}_1)^{\ell_1} C^{(k)}_{\underline{\lambda}_1 \underline{\lambda}_2} \cdots N(\underline{\lambda}_{m-1})^{\ell_{m-1}} C^{(k)}_{\underline{\lambda}_{m-1} \underline{\lambda}_m}.$$

In this sum, the nonzero terms correspond exactly to the paths γ of length m in Γ'_k from $\underline{\lambda}_0$ to $\underline{\lambda}_m$. Writing $n(\underline{\lambda}) = \log |N(\underline{\lambda})|$, the absolute value of such a term is a nonzero constant independent of $\underline{\ell}$ times $\exp(\sum_{i=1}^{m-1} \ell_i n(\underline{\lambda}_i))$. Write L_γ for the linear form $(\sum_{i=1}^{m-1} \ell_i n(\underline{\lambda}_i))$ on $\mathbb{R}^{m-1}$. The important fact about these linear forms, which follows from our hypothesis on the Galois group Gal, is the following:

Lemma 4.8. *Let $\underline{\lambda}_0, \underline{\lambda}_m$ belong to $\widehat{R}_k \subset \widetilde{R}_k$; let γ be a path of length m in Γ_k from $\underline{\lambda}_0$ to $\underline{\lambda}_m$ (such a path exists by our choice of m) and let γ' be a path of length m in Γ'_k from $\underline{\lambda}_0$ to $\underline{\lambda}_m$ distinct from γ. Then the linear forms L_γ and $L_{\gamma'}$ are distinct.*

Proof. The assertion of the lemma is a consequence of the following stronger assertion. Let $\underline{\lambda}$ be an element of $\widehat{R}_k$, and let $\underline{\lambda}'$ be an element of $\widetilde{R}_k$ distinct from $\underline{\lambda}$. Then the absolute values of $N(\underline{\lambda})$ and $N(\underline{\lambda}')$ are distinct. Indeed, assume by contradiction that we have a non trivial relation

$$\lambda_1 \cdots \lambda_k = \pm \lambda'_1 \cdots \lambda'_k,$$

where $\underline{\lambda} = \{\lambda_1, \cdots, \lambda_k\}$, $\underline{\lambda}' = \{\lambda'_1, \cdots, \lambda'_k\}$. Choose $\lambda_i \in \underline{\lambda}$ not belonging to $\underline{\lambda}'$; let $g \in Gal$ be the element which exchanges λ_i and λ_i^{-1} and fixes all other roots. When we

apply g to both sides of the above relation, the left-hand side is multiplied by λ_i^{-2} (because λ_i^{-1} does not belong to $\underline{\lambda}$ as $\underline{\lambda} \in \widehat{R}_k$); the right-hand side is multiplied by λ_i^2 if $\lambda_i^{-1} \in \underline{\lambda}'$, by 1 otherwise. In any case, we obtain the required contradiction. $\qquad\square$

The hyperplanes $V_1, \ldots, V_t$ of the proposition are defined as follows: for every path γ of length m in Γ_k, every path $\gamma' \neq \gamma$ of length m in Γ_k' with the same endpoints as γ, we exclude (for the direction of $\underline{\ell}$) the hyperplane $V(\gamma, \gamma')$ where the linear forms L_γ and $L_{\gamma'}$ are equal. Then, along a rational line in $\mathbb{Q}^{m-1}$ not lying in any of these hyperplanes, none of the expressions above for the coefficients $D^{(k)}_{\underline{\lambda}_0 \underline{\lambda}_m}$, as finite linear combinations of exponentials of various rates, is identically zero; this completes the proof of the proposition. $\qquad\square$

4.5. The first step: transversality for $k = 1$.
Starting from the matrix B in the main theorem of this section (Theorem 4.5), we consider the graph $\Gamma_1 = \Gamma_1(B)$.

Claim 4.9. *The graph Γ_1 is mixing.*

Proof. First note that Γ_1 has at least one arrow as B is invertible. Next, for $d = 1$, since Γ_1 is Gal-invariant, Γ_1 is not mixing if and only if there are only two arrows in Γ_1 (either two loops or two arrows in both directions between λ and λ^{-1}). In both cases $\mathbb{R} v_\lambda$ is invariant under B^2, a contradiction.

We now consider the case that $d > 1$ and that the only arrows of Γ_1 join a vertex λ to λ or λ^{-1}. Then each 2-dimensional subspace generated by $v_\lambda, v_{\lambda^{-1}}$ is B-invariant, a contradiction.

Finally, assume that $d > 1$ and Γ_1 has one arrow joining a vertex λ to a vertex $\lambda' \neq \lambda^{\pm 1}$. Using the action of the Galois group Gal, every such arrow must be in Γ_1. This implies that Γ_1 is mixing when $d > 2$. When $d = 2$, the only case where Γ_1 is not mixing is when there is no other arrow in Γ_1; but then each 2-dimensional subspace generated by $v_\lambda, v_{\lambda^{-1}}$ is B^2-invariant, a contradiction. $\qquad\square$

Applying Proposition 4.7 above with $k = 1$, we find $m \geqslant 1$ and

$$C = BA^{\ell_1} \cdots BA^{\ell_{m-1}} B$$

a 1-twisting matrix with respect to A. Observe that $\Gamma_1(C)$ is then the complete graph on $2d$ vertices, in particular it is mixing.

Thus, Theorem 4.5 is now proven for $d = 1$, so we assume in the following that $d \geqslant 2$.

4.6. Existence of arrows in $\Gamma_k(C)$ for $k > 1$.
As $\widehat{R}_k$ is now a non-trivial subset of $\widetilde{R}_k$, the existence of an arrow in $\Gamma_k(C)$ is less trivial than for $k = 1$ and requires the symplecticity of C.

Lemma 4.10. *Let $C \in \mathrm{Sp}(\Omega, \mathbb{Z})$. Then, for $1 \leqslant k \leqslant d$, the graph $\Gamma_k(C)$ has at least one arrow.*

Proof. Let $1 \leqslant k \leqslant d$, $\underline{\lambda} \in \widehat{R}_k$. Let $\Gamma_k'(C)$ be the oriented graph with set of vertices $\widetilde{R}_k$ such that there is an arrow from $\underline{\lambda}_0$ to $\underline{\lambda}_1$ if and only if $C^{(k)}_{\underline{\lambda}_0 \underline{\lambda}_1} \neq 0$. In particular, $\Gamma_k(C)$ is a subgraph of $\Gamma_k'(C)$. As $\wedge^k C$ is invertible, there exists at least one arrow in $\Gamma_k'(C)$ starting from $\underline{\lambda} = \{\lambda_1 < \cdots < \lambda_k\}$. Consider such an arrow, with endpoint $\underline{\lambda}' = \{\lambda_1' < \cdots < \lambda_k'\}$, with the property that the cardinality k' of the image $p(\underline{\lambda}') \subset R$ is

the greatest possible. We want to prove that $k' = k$. Assume by contradiction that $k' < k$, i.e with appropriate indexing $\lambda_1' \lambda_2' = 1$. Write, for $\lambda \in \widetilde{R}$,

$$C(v_\lambda) = \sum_{\lambda'} C_{\lambda\,\lambda'} v_{\lambda'}.$$

By assumption, the minor of the matrix of C obtained by taking the lines in $\underline{\lambda}$ and the columns in $\underline{\lambda}'$ is nonzero. Therefore, we can find vectors $w_1, \ldots, w_k \in \mathbb{R}^{2d}$, generating the same isotropic subspace as $v_{\lambda_1}, \ldots, v_{\lambda_k}$, such that, for $1 \leqslant i \leqslant k$

$$C(w_i) = v_{\lambda_i'} + \sum_{\lambda' \notin \underline{\lambda}'} C_{i\,\lambda'}^* v_{\lambda'}.$$

We claim that, if λ' **and** λ'^{-1} do not belong to $\underline{\lambda}'$, then the coefficient $C_{1\,\lambda'}^*$ is equal to zero. Indeed, otherwise, the minor of C obtained by taking the lines in $\underline{\lambda}$ and the columns in $\underline{\lambda}_1' := (\underline{\lambda}' - \{\lambda_1'\}) \cup \{\lambda'\}$ would be nonzero, with $\#p(\underline{\lambda}_1') = k' + 1$, in contradiction with the definition of k'. Similarly, we have $C_{2\,\lambda'}^* = 0$. But then, we have

$$\Omega(C(w_1), C(w_2)) = \Omega(v_{\lambda_1'}, v_{\lambda_2'}) \neq 0$$

as $\lambda_1' \lambda_2' = 1$, while $\Omega(w_1, w_2) = 0$, a contradiction. $\square$

Remark 4.11. The action of the Galois group Gal has not been used; the assertion of this lemma is true for any $C \in \mathrm{Sp}(2d, \mathbb{R})$.

4.7. **Second step: transversality for** $1 \leqslant k < d$**.** For $d = 2$, there is nothing new to prove, so we may assume $d \geqslant 3$.

Proposition 4.12. *Let $C \in \mathrm{Sp}(2d, \mathbb{Z})$. If C is 1-twisting with respect to A, then $\Gamma_k(C)$ is mixing for all $1 \leqslant k < d$.*

By putting together this result with Proposition 4.7, one has:

Corollary 4.13. *Assume that $C \in \mathrm{Sp}(2d, \mathbb{Z})$ is 1-twisting with respect to A. Then, for any large enough integer m (depending only on d), the matrix*

$$D = CA^{\ell_1} \cdots CA^{\ell_{m-1}}C$$

is k-twisting with respect to A for all $1 \leqslant k < d$ provided $\underline{\ell} := (\ell_1, \cdots, \ell_{m-1}) \in \mathbb{Z}^{m-1}$ goes to infinity along a rational line not lying in a finite number of hyperplanes of $\mathbb{R}^{m-1}$.

Proof of Proposition 4.12. The graph $\Gamma_1(C)$ is complete on $2d$ vertices hence mixing. We assume now that $2 \leqslant k < d$. We list the orbits of the action of the Galois group Gal on $\widehat{R}_k \times \widehat{R}_k$ (an ordered pair being seen as the origin and the end of a possible arrow in Γ_k): for every pair of integers $\ell, \widetilde{\ell}$ with $0 \leqslant \widetilde{\ell} \leqslant \ell \leqslant k$ and $\ell \geqslant 2k - d$, there is an orbit $\mathcal{O}_{\widetilde{\ell}, \ell}$ formed by the pairs $(\underline{\lambda}, \underline{\lambda}')$ satisfying

$$\#(\underline{\lambda} \cap \underline{\lambda}') = \widetilde{\ell}, \qquad \#(p(\underline{\lambda}) \cap p(\underline{\lambda}')) = \ell.$$

A Gal-invariant graph with vertices $\widehat{R}_k$ is determined by which orbits $\mathcal{O}_{\widetilde{\ell}, \ell}$ are associated to arrows. We will prove in the next subsection the following:

Proposition 4.14. *A Gal-invariant graph with vertices $\widehat{R}_k$ is **not** mixing if and only if its arrows are associated to some of the $\mathcal{O}_{\widetilde{\ell}, k}$ ($0 \leqslant \widetilde{\ell} \leqslant k$) or, **when d is even and $k = \frac{d}{2}$**, to $\mathcal{O}_{0,0}$.*

We now finish the proof of the Proposition 4.12 by showing that the non-mixing cases above do not occur for $\Gamma_k(C)$ when C is 1-twisting with respect to A. We already know that $\Gamma_k(C)$ has a non empty set of arrows, so at least one orbit of the Gal-action on $\widehat{R}_k \times \widehat{R}_k$ must occur.

Case 1. Assume that the only occurring orbits have the form $\mathcal{O}_{\widetilde{\ell},k}$ $(0 \leqslant \widetilde{\ell} \leqslant k)$. Let $\underline{\lambda} = \{\lambda_1 < \cdots < \lambda_k\} \in \widehat{R}_k$; let γ be an arrow of $\Gamma_k = \Gamma_k(C)$ starting from $\underline{\lambda}$; its endpoint $\underline{\lambda}' = \{\lambda'_1 < \cdots < \lambda'_k\}$ satisfies $p(\underline{\lambda}) = p(\underline{\lambda}')$. As in the previous subsection, we can find vectors $w_1, \ldots, w_k \in \mathbb{R}^{2d}$, generating the same isotropic subspace as $v_{\lambda_1}, \ldots, v_{\lambda_k}$, such that, for $1 \leqslant i \leqslant k$

$$C(w_i) = v_{\lambda'_i} + \sum_{\lambda' \notin \underline{\lambda}'} C^*_{i\,\lambda'} v_{\lambda'}.$$

We claim that, if λ' **and** λ'^{-1} do not belong to $\underline{\lambda}'$, then the coefficient $C^*_{i\,\lambda'}$ is equal to zero for every $1 \leqslant i \leqslant k$. Indeed, otherwise, the minor of C obtained by taking the lines in $\underline{\lambda}$ and the columns in $\underline{\lambda}'_i := (\underline{\lambda}' - \{\lambda'_i\}) \cup \{\lambda'\}$ would be nonzero, and the corresponding arrow of $\Gamma_k(C)$ would not be as assumed. We conclude that the image $C(v_{\lambda_1})$ is a linear combination of the $2k$ vectors $v_{\lambda_i}, v_{\lambda_i^{-1}}$, $1 \leqslant i \leqslant k$, in contradiction with the fact that C is 1-twisting with respect to A.

Case 2. Assume that d is even $\geqslant 4$, $k = \frac{d}{2}$, and that the only occurring orbits are $\mathcal{O}_{0,0}$ and possibly some of the $\mathcal{O}_{\widetilde{\ell},k}$ $(0 \leqslant \widetilde{\ell} \leqslant k)$. Let γ be an arrow of Γ_k associated to $\mathcal{O}_{0,0}$. Let $\underline{\lambda} = \{\lambda_1 < \cdots < \lambda_k\} \in \widehat{R}_k$ be the origin of γ and let $\underline{\lambda}' = \{\lambda'_1 < \cdots < \lambda'_k\}$ be its endpoint. Then $p(\underline{\lambda})$ and $p(\underline{\lambda}')$ are complementary subsets of R. As above, we can find vectors $w_1, \ldots, w_k \in \mathbb{R}^{2d}$, generating the same isotropic subspace as $v_{\lambda_1}, \ldots, v_{\lambda_k}$, such that, for $1 \leqslant i \leqslant k$

$$C(w_i) = v_{\lambda'_i} + \sum_{\lambda' \notin \underline{\lambda}'} C^*_{i\,\lambda'} v_{\lambda'}.$$

Again, if λ' **and** λ'^{-1} do not belong to $\underline{\lambda}'$, the coefficient $C^*_{i\,\lambda'}$ is equal to zero for every $1 \leqslant i \leqslant k$. We conclude that the image $C(v_{\lambda_1})$ is a linear combination of the $2k = d$ vectors $v_{\lambda'_i}, v_{\lambda_i'^{-1}}$, $1 \leqslant i \leqslant k$, in contradiction with the fact that C is 1-twisting with respect to A. $\qquad\square$

4.8. **Proof of Proposition 4.14.** For convenience, we divide the proof in two steps. We first project down from $\widetilde{R}$ to R and state the result at this level.

Let $S(R)$ be the full permutation group of R. The orbits of its action on $R_k \times R_k$ are as follows: for each integer ℓ with $k \geqslant \ell \geqslant \max(0, 2k - d)$, one has an orbit $\mathcal{O}_\ell$ formed of the pairs $(\underline{\mu}, \underline{\mu}')$ with $\#(\underline{\mu} \cap \underline{\mu}') = \ell$. A $S(R)$-invariant oriented graph Γ with vertices R_k is determined by which of these orbits are associated to arrows of Γ.

Proposition 4.15. *We assume $d > 2$ and $1 \leqslant k < d$. Such a graph Γ is **not** mixing if and only if the orbits associated to the arrows of Γ are $\mathcal{O}_k$ and /or, **when d is even and $k = \frac{d}{2}$**, $\mathcal{O}_0$.*

Proof. The excluded cases are clearly not mixing. It is therefore sufficient to prove that the $S(R)$-invariant graph $\Gamma(\ell)$ (with $k > \ell \geqslant \max(0, 2k - d)$, $\ell > 0$ when $k = \frac{d}{2}$) whose arrows are associated to the single orbit $\mathcal{O}_\ell$ is mixing. By passing to complements, it is sufficient to consider the case where $k \leqslant \frac{d}{2}$.

We first show that $\Gamma(\ell)$ is connected. Let $\underline{\mu}_0$, $\underline{\mu}_1$ be two elements of R_k. Let $m = \#(\underline{\mu}_0 \cap \underline{\mu}_1)$. We want to find a path in $\Gamma(\ell)$ from $\underline{\mu}_0$ to $\underline{\mu}_1$. When $m = \ell$, a single arrow will do.

We deal with the case $m > \ell$ by ascending induction on m, assuming that the result is true for $m - 1$. Choose $\mu \in \underline{\mu}_0 \cap \underline{\mu}_1$, and two distinct elements μ_0, μ_1 in $R - (\underline{\mu}_0 \cup \underline{\mu}_1)$ (this is possible because of our restrictions on k, ℓ). Let $\underline{\mu}'_0 := (\underline{\mu}_0 - \{\mu\}) \cup \{\mu_0\}, \underline{\mu}'_1 := (\underline{\mu}_1 - \{\mu\}) \cup \{\mu_1\}$. We have $\#(\underline{\mu}_0 \cap \underline{\mu}'_1) = \#(\underline{\mu}'_0 \cap \underline{\mu}_1) = \#(\underline{\mu}'_0 \cap \underline{\mu}'_1) = m - 1$. By concatenation of three paths $\underline{\mu}_0 \to \underline{\mu}'_1 \to \underline{\mu}'_0 \to \underline{\mu}_1$, we obtain a path from $\underline{\mu}_0$ to $\underline{\mu}_1$.

We deal with the case $0 < m < \ell$ by descending induction on m, assuming that the result is true for larger values of m. Choose $\mu_0 \in \underline{\mu}_0 - \underline{\mu}_1, \mu_1 \in \underline{\mu}_1 - \underline{\mu}_0, \mu \in R - (\underline{\mu}_0 \cup \underline{\mu}_1)$. Define $\underline{\mu}'_0 = (\underline{\mu}_0 - \{\mu_0\}) \cup \{\mu\}, \underline{\mu}'_1 = (\underline{\mu}_1 - \{\mu_1\}) \cup \{\mu\}$. We have $\#(\underline{\mu}_0 \cap \underline{\mu}'_0) = \#(\underline{\mu}_1 \cap \underline{\mu}'_1) = k - 1, \#(\underline{\mu}'_0 \cap \underline{\mu}'_1) = m + 1$. By concatenation of three paths $\underline{\mu}_0 \to \underline{\mu}'_0 \to \underline{\mu}'_1 \to \underline{\mu}_1$, we obtain a path from $\underline{\mu}_0$ to $\underline{\mu}_1$. The same argument works when $m = 0, k < \frac{d}{2}$.

Consider finally the case $m = 0, k = \frac{d}{2}$. As $d > 2$, we have $k \geqslant 2$. Choose distinct elements $\mu_0, \mu'_0 \in \underline{\mu}_0$ and $\mu_1, \mu'_1 \in \underline{\mu}_1$. Define $\underline{\mu}'_0 = (\underline{\mu}_0 - \{\mu'_0\}) \cup \{\mu_1\}, \underline{\mu}'_1 = (\underline{\mu}_1 - \{\mu'_1\}) \cup \{\mu_0\}$. We have $\#(\underline{\mu}_0 \cap \underline{\mu}'_0) = \#(\underline{\mu}_1 \cap \underline{\mu}'_1) = k - 1, \#(\underline{\mu}'_0 \cap \underline{\mu}'_1) = 2$. By concatenation of three paths $\underline{\mu}_0 \to \underline{\mu}'_0 \to \underline{\mu}'_1 \to \underline{\mu}_1$, we obtain a path from $\underline{\mu}_0$ to $\underline{\mu}_1$.

We now show that $\Gamma(\ell)$ is mixing. If not, there is a prime number π such that all loops of $\Gamma(\ell)$ have length divisible by π. If $\underline{\mu}_0 \to \underline{\mu}_1$ is an arrow, so is $\underline{\mu}_1 \to \underline{\mu}_0$, so the only possibility is $\pi = 2$. On the other hand, the proof of connectedness has produced by induction between any vertices $\underline{\mu}_0, \underline{\mu}_1$ a path of odd length. Taking $\underline{\mu}_0 = \underline{\mu}_1$ (i.e $m = k$ above) gives a loop of odd length. $\qquad\square$

Proof of Proposition 4.14. Again, the excluded cases are clearly not mixing. Therefore, it is sufficient to prove that the oriented graph $\Gamma(\widetilde{\ell}, \ell)$ with vertex set $\widehat{R}_k$ and arrows associated to a single orbit $\mathcal{O}_{\widetilde{\ell}, \ell}$ (not of the excluded type) is mixing.

We first show that $\Gamma(\widetilde{\ell}, \ell)$ is connected. From the previous proposition, it is sufficient to connect any two vertices $\underline{\lambda}_0, \underline{\lambda}_1$ with the same image $\underline{\mu}$ by p. We can even further assume that $\#(\underline{\lambda}_0 \cap \underline{\lambda}_1) = k - 1$. Let $\underline{\mu}' \in R_k$ such that $\#(\underline{\mu} \cap \underline{\mu}') = k - 1$; by the previous proposition, there is a path in $\Gamma(\ell)$ from $\underline{\mu}$ to $\underline{\mu}'$; lifting this path gives a path γ in $\Gamma(\widetilde{\ell}, \ell)$ from $\underline{\lambda}_0$ to some vertex $\underline{\lambda}'$ with $p(\underline{\lambda}') = \underline{\mu}'$. Now, there is an element g of G sending $\underline{\lambda}_0$ to $\underline{\lambda}'$ and $\underline{\lambda}'$ to $\underline{\lambda}_1$. Concatenating γ and $g.\gamma$ gives a path from $\underline{\lambda}_0$ to $\underline{\lambda}_1$.

Finally, we show that $\Gamma(\widetilde{\ell}, \ell)$ is mixing. Again, the only possible divisor of the lengths of all loops is 2. To get a loop of odd length, we start from such a loop in $\Gamma(\ell)$, which we lift to get a path of odd length between two vertices $\underline{\lambda}_0, \underline{\lambda}_1$ with the same image by p. But we have just constructed above a path of even length from $\underline{\lambda}_1$ to $\underline{\lambda}_0$. By concatenation, we get the required loop. $\qquad\square$

4.9. **The last step: transversality for all** $1 \leqslant k \leqslant d$, $d \geqslant 3$. In this subsection, we assume $d \geqslant 3$.

Proposition 4.16. *Let* $D \in Sp(\Omega, \mathbb{Z})$. *If* D *is* k-twisting with respect to A for each $1 \leqslant k < d$, then $\Gamma_d(D)$ *is mixing.*

By putting this result together with Proposition 4.7, one has:

Corollary 4.17. *Assume that* $D \in \mathrm{Sp}(\Omega, \mathbb{Z})$ *is* k-twisting with respect to A for each $1 \leqslant k < d$. *Then, for any large enough integer* m (*depending only on* d), *the matrix*

$$E = DA^{\ell_1} \cdots DA^{\ell_{m-1}} D$$

is k-twisting with respect to A for all $1 \leqslant k \leqslant d$ provided $\underline{\ell} := (\ell_1, \cdots, \ell_{m-1}) \in \mathbb{Z}^{m-1}$ *goes to infinity along a rational line not lying in any of a finite number of hyperplanes of* $\mathbb{R}^{m-1}$.

Proof of Proposition 4.16. The orbits of the action of the Galois group on $\widehat{R}_d \times \widehat{R}_d$ are as described in Subsection 4.7 (now with $k = d$); the restriction $2k - d \leqslant \ell \leqslant k$ now forces $\ell = d$ and we are left with one parameter $0 \leqslant \widetilde{\ell} \leqslant d$. We write $\mathcal{O}(\widetilde{\ell})$ for $\mathcal{O}_{\widetilde{\ell},d}$.

A *Gal*-invariant graph Γ_d on $\widehat{R}_d$ is determined by the subset $J \subset \{0, \ldots, d\}$ of integers $\widetilde{\ell}$ indexing the orbits associated to the arrows of Γ_d.

Lemma 4.18. *If J contains two consecutive integers $\widetilde{\ell}$, $\widetilde{\ell} + 1$, then Γ_d is mixing.*

Proof of Lemma 4.18. We first show that Γ_d is connected. To prove this, it is sufficient to connect two vertices $\underline{\lambda}_0$, $\underline{\lambda}_1$ such that $\#(\underline{\lambda}_0 \cap \underline{\lambda}_1) = d - 1$. This is done by choosing a subset $\underline{\lambda}$ of size $d - \widetilde{\ell} - 1$ in $\underline{\lambda}_0 \cap \underline{\lambda}_1$ and calling $\underline{\lambda}_2$ the element of $\widehat{R}_d$ obtained from $\underline{\lambda}_0$ by replacing the elements of $\underline{\lambda}$ by their inverses; one has $\#(\underline{\lambda}_0 \cap \underline{\lambda}_2) = \widetilde{\ell} + 1$, $\#(\underline{\lambda}_1 \cap \underline{\lambda}_2) = \widetilde{\ell}$, hence there are arrows $\underline{\lambda}_0 \to \underline{\lambda}_2 \to \underline{\lambda}_1$.

As before, the only possible non trivial common divisor for the lengths of the loops is 2. But concatenating a single arrow associated to $\mathcal{O}(\widetilde{\ell})$ to $d - \widetilde{\ell}$ paths of length 2 as constructed above, we get a loop of odd length. This shows that Γ_d is mixing. $\qquad\square$

In view of this lemma, the proof of the proposition is complete as soon as we show that the subset J associated to $\Gamma_d(D)$ contains two consecutive integers. We assume by contradiction that this is not the case. From Lemma 4.10 we know that J is not empty. We consider successively several cases.

Case 1. Assume first that J contains an integer ℓ with $2 \leqslant \ell < d$. Let $\underline{\lambda}_0 \to \underline{\lambda}_1$ be an arrow of this type in $\Gamma_d(D)$, with $\underline{\lambda}_0 = \{\lambda_1, \cdots, \lambda_d\}, \underline{\lambda}_1 = \{\lambda_1, \cdots, \lambda_\ell, \lambda_{\ell+1}^{-1}, \ldots, \lambda_d^{-1}\}$.

We can find vectors $w_1, \ldots, w_d \in \mathbb{R}^{2d}$, generating the same Lagrangian subspace as $v_{\lambda_1}, \ldots, v_{\lambda_d}$, such that, for $1 \leqslant i \leqslant d$

$$D(w_i) = v(i) + \sum_1^d D_{ij}^* v'(j),$$

where $v(i) = v_{\lambda_i}, v'(i) = v_{\lambda_i^{-1}}$ for $1 \leqslant i \leqslant \ell$, $v(i) = v_{\lambda_i^{-1}}, v'(i) = v_{\lambda_i}$ for $\ell < i \leqslant d$. As $\ell \pm 1$ do not belong to J by hypothesis, there is no arrow in Γ_d from $\underline{\lambda}_0$ to any vertex obtained from $\underline{\lambda}_1$ by replacing one of its element by its inverse. This implies that the diagonal coefficients D_{ii}^* are zero for $1 \leqslant i \leqslant d$.

Next, take $1 \leqslant i \leqslant \ell < j \leqslant d$, and $\underline{\lambda}_1'$ to be the vertex obtained by replacing in $\underline{\lambda}_1$ both λ_i and λ_j^{-1} by their inverses. We have $\#(\underline{\lambda}_0 \cap \underline{\lambda}_1') = \ell$, hence there is an arrow from $\underline{\lambda}_0$ to $\underline{\lambda}_1'$ in $\Gamma_d(D)$. This implies , as $D_{ii}^* = D_{jj}^* = 0$, that $D_{ij}^* D_{ji}^* \neq 0$. On the other hand, as $\Omega(D(w_i), D(w_j)) = 0$, we have, writing $\Omega(v_{\lambda_i}, v_{\lambda_i^{-1}}) := \omega_i$

$$D_{ji}^* \omega_i + D_{ij}^* \omega_j = 0.$$

When we take instead $1 \leqslant i < j \leqslant \ell$, as $\Omega(D(w_i), D(w_j)) = 0$, we have

$$D_{ji}^* \omega_i - D_{ij}^* \omega_j = 0.$$

Now, let $\underline{\lambda}_1''$ be the vertex obtained by replacing (in $\underline{\lambda}_1$) λ_1, λ_2 and λ_d^{-1} by their inverses. We have $\#(\underline{\lambda}_0 \cap \underline{\lambda}_1'') = \ell - 1$, hence there is no arrow from $\underline{\lambda}_0$ to $\underline{\lambda}_1''$ in $\Gamma_d(D)$. Computing the corresponding 3×3 minor in D^* gives (as the diagonal terms vanish)

$$D_{12}^* D_{2d}^* D_{d1}^* + D_{1d}^* D_{d2}^* D_{21}^* = 0.$$

As the ω_i are nonzero, the symmetry/antisymmetry properties of the D_{ij}^* force

$$D_{12}^* D_{2d}^* D_{d1}^* = 0 = D_{1d}^* D_{d2}^* D_{21}^*.$$

As $D^*_{1\,d}, D^*_{d\,1}, D^*_{2\,d}, D^*_{d\,2}$ are non zero, we have $D^*_{1\,2} = D^*_{2\,1} = 0$. Take a nonzero linear combination w of w_1, w_2 which is also a linear combination of $v_{\lambda_1}, \ldots, v_{\lambda_{d-1}}$ (eliminating the coefficient of v_{λ_d}). The image $D(w)$ is then a linear combination of $v(1), v(2)$, and the $v'(j))$ for $2 < j \leqslant d$. This contradicts the fact that D is $(d-1)$-twisting with respect to A.

Case 2. The case where $1 \in J$ (with $d \geqslant 3$) is dealt with in a symmetric way.

Case 3. Assume that J contains no element except (possibly) the endpoints 0 and d. Assume that for instance $d \in J$. Let $\underline{\lambda}_0 = \{\lambda_1, \cdots, \lambda_d\}$. As the loop at $\underline{\lambda}_0$ is an arrow of $\Gamma_d(D)$, we can find vectors $w_1, \ldots, w_d \in \mathbb{R}^{2d}$, generating the same Lagrangian subspace as $v_{\lambda_1}, \ldots, v_{\lambda_d}$, such that, for $1 \leqslant i \leqslant d$

$$D(w_i) = v(i) + \sum_{1}^{d} D^*_{i\,j} v'(j),$$

where $v(i) = v_{\lambda_i}, v'(i) = v_{\lambda_i^{-1}}$ for $1 \leqslant i \leqslant d$.

As above, from $d - 1 \notin J$, we obtain that the diagonal coefficients $D^*_{i\,i}$ are zero for $1 \leqslant i \leqslant d$. But now, as $d - 2 \notin J$ (recall that $d \geqslant 3 > 2$), the 2×2 diagonal minors of D^* are zero, implying $D^*_{i\,j} D^*_{j\,i} = 0$ for $1 \leqslant i < j \leqslant d$. As we still have

$$D^*_{j\,i} \omega_i - D^*_{i\,j} \omega_j = 0,$$

we have in fact $D^*_{i\,j} = D^*_{j\,i} = 0$. We conclude as before that the fact that D is $(d-1)$-twisting with respect to A is violated.

The case where 0 is the unique element of J is treated in the same way.

This concludes the proof of the proposition. $\square$

At this point, by putting together the result of Subsection 4.5 and Corollaries 4.13, 4.17, our Theorem 4.5 is now proven for $d = 1$ and $d \geqslant 3$. Thus, it remains only to consider the special case $d = 2$. This is the content of the next subsection.

4.10. **The case** $d = 2$. The kernel K of the linear form $\wedge^2 \mathbb{R}^4 \to \mathbb{R}$ determined by the symplectic form Ω is invariant by the action of the symplectic group $Sp(\Omega, \mathbb{R})$ on $\wedge^2 \mathbb{R}^4$. A basis of K is formed by the four vectors $v_{\underline{\lambda}}, \underline{\lambda} \in \widehat{R}_2$ and

$$v_* := \frac{v_{\lambda_1} \wedge v_{\lambda_1^{-1}}}{\omega_1} - \frac{v_{\lambda_2} \wedge v_{\lambda_2^{-1}}}{\omega_2},$$

where $\widetilde{R} = \{\lambda_1, \lambda_1^{-1}, \lambda_2, \lambda_2^{-1}\}$ and $\omega_i := \Omega(v_{\lambda_i}, v_{\lambda_i^{-1}})$ for $i = 1, 2$. Observe that v_* is an eigenvector of $\wedge^2 A$ with eigenvalue 1. Thus, the eigenvalues of $\wedge^2 A$ on K are **distinct**. This would not be true for $d > 2$, as 1 is then a multiple eigenvalue.

Let $C \in \mathrm{Sp}(\Omega, \mathbb{Z})$. We define an oriented graph $\Gamma^*_2 = \Gamma^*_2(C)$ as follows: the vertices of Γ^*_2 are the four elements of $\widehat{R}_2$ and a special vertex $*$ (associated to the eigenvalue 1 of $\wedge^2 A$); for vertices $\underline{\lambda}_0, \underline{\lambda}_1$, there is an arrow from $\underline{\lambda}_0$ to $\underline{\lambda}_1$ if and only if the coefficient $C^{(2)}_{\underline{\lambda}_0 \underline{\lambda}_1}$ of the matrix of $\wedge^2 C$, written in the basis $(v_{\underline{\lambda}})$ of K, is nonzero.

Assume that $\Gamma^*_2(C)$ **is mixing**. Let m be a positive integer such that, for every vertices $\underline{\lambda}_0, \underline{\lambda}_1$ of $\Gamma^*_2(C)$, there is an oriented path of length m from $\underline{\lambda}_0$ to $\underline{\lambda}_1$. For nonnegative integers $\ell_1, \cdots, \ell_{m-1}$, consider

$$D = C A^{\ell_1} \cdots C A^{\ell_{m-1}} C.$$

Proposition 4.19. *There are finitely many hyperplanes $V_1, \cdots, V_t$ in $\mathbb{R}^{m-1}$ such that, if $\underline{\ell} := (\ell_1, \cdots, \ell_{m-1}) \in \mathbb{Z}^{m-1}$ goes to infinity along a rational line not lying in any of the V_p, then, for $\|\underline{\ell}\|$ large enough, the matrix D is 2-twisting with respect to A.*

Proof. The proof is the same as for Proposition 4.7, using that all eigenvalues of $\wedge^2 A$ are simple. □

In view of this proposition, in order to conclude the proof of Theorem 4.5 in the case $d = 2$, it suffices to prove the following statement.

Proposition 4.20. *Let $C \in \mathrm{Sp}(\Omega, \mathbb{Z})$. If C is 1-twisting with respect to A, then $\Gamma_2(C)$ or $\Gamma_2^*(C)$ is mixing.*

Proof. We start by considering $\Gamma_2(C)$. We can define $J \subset \{0, 1, 2\}$ as in the proof of Proposition 4.16. This non-empty subset determines the Gal-invariant graph $\Gamma_2(C)$. If J contains two consecutive integers, Lemma 4.18 (still valid for $d = 2$) implies that $\Gamma_2(C)$ is mixing. On the other hand, if J contains only 0 or 2, one proves as in the last subsection that C is not 1-twisting with respect to A, a contradiction.

Therefore, there are two remaining cases to be considered: $J = \{1\}$, and $J = \{0, 2\}$. In these cases, $\Gamma_2(C)$ is not mixing, but we will show that $\Gamma_2^*(C)$ is mixing. Notice that the mixing property follows from the existence of arrows in $\Gamma_2^*(C)$ from any vertex of $\widehat{R}_2$ to the special vertex $*$, and of arrows from this special vertex to any vertex of $\widehat{R}_2$.

Existence of arrows in $\Gamma_2^*(C)$ from any vertex of $\widehat{R}_2$ to the special vertex $*$. We assume that $J = \{1\}$, the other case is dealt in the same way. Let $\underline{\lambda}_0 = \{\lambda_1, \lambda_2\} \in \widehat{R}_2$. We can find vectors $w_1, w_2 \in \mathbb{R}^4$, generating the same Lagrangian subspace as $v_{\lambda_1}, v_{\lambda_2}$, such that

$$C(w_1) = v_{\lambda_1} + C_{11}^* v_{\lambda_1^{-1}} + C_{12}^* v_{\lambda_2},$$

$$C(w_2) = v_{\lambda_2^{-1}} + C_{21}^* v_{\lambda_1^{-1}} + C_{22}^* v_{\lambda_2}.$$

As $0, 2 \notin J$, we have $C_{11}^* = C_{22}^* = 0$. As $1 \in J$, we have $C_{12}^* C_{21}^* \neq 0$. It follows that there is an arrow from $\underline{\lambda}_0$ to the special vertex $*$ in $\Gamma_2^*(C)$.

Existence of arrows in $\Gamma_2^*(C)$ from the special vertex $*$ to any vertex of $\widehat{R}_2$. If there were no arrows from the special vertex $*$ to any other vertex in $\Gamma_2^*(C)$, then v_* would be an eigenvector of $\wedge^2 C$. By Proposition 4.21 in the next subsection (see below), the image by C of the symplectic plane generated by $v_{\lambda_1}, v_{\lambda_1^{-1}}$ is consequently either itself or the symplectic plane generated by $v_{\lambda_2}, v_{\lambda_2^{-1}}$. In any case, this contradicts the fact that C is 1-twisting with respect to A. □

4.11. **Symplectic 2-planes.** Let H_1, H_2 be orthogonal 2-planes in $\mathbb{R}^4$ equipped with the standard symplectic structure. Choose a basis e_1, f_1 of H_1, a basis e_2, f_2 of H_2, normalized by $\Omega(e_1, f_1) = \Omega(e_2, f_2) = 1$. The non-zero bivector

$$V(H_1) := e_1 \wedge f_1 - e_2 \wedge f_2$$

does not depend on the choices of the two bases of H_1 and its symplectic orthogonal H_2, i.e., it depends only on H_1.

Proposition 4.21. *The map $H \to V(H)$ from symplectic 2-planes in $\mathbb{R}^4$ to $\wedge^2 \mathbb{R}^4$ is injective. More precisely, if H, H' are symplectic 2-planes in $\mathbb{R}^4$ such that $V(H)$ and $V(H')$ are collinear, then H, H' are either equal or orthogonal.*

Proof. Let e_1, f_1, e_2, f_2 be the canonical basis of $\mathbb{R}^4$, and let H be a symplectic 2-plane. We have to show that, if $V(H)$ is proportional to $e_1 \wedge f_1 - e_2 \wedge f_2$, then H is either spanned by e_1, f_1 or by e_2, f_2. Let E_1, F_1 be a basis of H and E_2, F_2 be a basis of the orthogonal

H' of H, such that $\Omega(E_1, F_1) = \Omega(E_2, F_2) = 1$. Write

$$E_i = \sum_1^2 a_{i\,j}e_j + \sum_1^2 b_{i\,j}f_j,$$

$$F_i = \sum_1^2 c_{i\,j}e_j + \sum_1^2 d_{i\,j}f_j.$$

Let

$$M_{i\,j} = \left(\begin{array}{cc} a_{i\,j} & b_{i\,j} \\ c_{i\,j} & d_{i\,j} \end{array} \right).$$

By changing the symplectic bases of the planes $\langle e_1, f_1 \rangle$, $\langle e_2, f_2 \rangle$, $\langle E_1, F_1 \rangle$, $\langle E_2, F_2 \rangle$, we change the matrices $M_{i\,j}$ to $M'_{i\,j} = P_i M_{i\,j} Q_j$, where P_1, P_2, Q_1, Q_2 are arbitrary matrices in $SL(2, \mathbb{R})$.

Lemma 4.22. *For $i = 1, 2$, at least one of the matrices $M_{i\,1}, M_{i\,2}$ is invertible. For $j = 1, 2$, at least one of the matrices $M_{1\,j}, M_{2\,j}$ is invertible.*

Proof. We show that $M_{1\,1}$ or $M_{1\,2}$ is invertible. Otherwise, by an appropriate choice of Q_1, Q_2, we obtain $b_{1\,1} = d_{1\,1} = b_{1\,2} = d_{1\,2} = 0$, which contradicts $\Omega(E_1, F_1) = 1$.

The proof of the other cases is similar. $\square$

Changing H to its orthogonal H' changes $V(H)$ to $-V(H)$ and exchanges $M_{1\,j}$ and $M_{2\,j}$. From the lemma, we may thus assume after performing if necessary such a change, that $M_{1\,1}$ and $M_{2\,2}$ are invertible. Then, choosing appropriately $P_1, P_2, Q_1, Q_2 \in SL(2, \mathbb{R})$ allows to get

$$b_{11} = b_{1\,2} = b_{2\,2} = c_{1\,1} = c_{1\,2} = c_{2\,2} = 0,$$

$$a_{1\,1} = a_{2\,2} = 1, d_{1\,1} \neq 0, d_{2\,2} \neq 0.$$

Then, the relations $\Omega(E_1, E_2) = \Omega(F_1, F_2) = 0$ give also $b_{2\,1} = c_{2\,1} = 0$, so all $M_{i\,j}$ are diagonal. The relations $\Omega(E_1, F_2) = \Omega(F_1, E_2) = 0$ give

$$d_{2\,1} + a_{1\,2}d_{2\,2} = 0 = d_{1\,2} + a_{2\,1}d_{1\,1}.$$

On the other hand, the relations $\Omega(E_1, F_1) = \Omega(E_2, F_2) = 0$ give

$$d_{1\,1} + a_{1\,2}d_{1\,2} = 1 = d_{2\,2} + a_{2\,1}d_{2\,1}.$$

Finally, the assumption

$$E_1 \wedge F_1 - E_2 \wedge F_2 = k(e_1 \wedge f_1 - e_2 \wedge f_2)$$

give

$$d_{2\,1} - a_{1\,2}d_{2\,2} = 0 = d_{1\,2} - a_{2\,1}d_{1\,1},$$

$$d_{1\,1} - a_{1\,2}d_{1\,2} = k = d_{2\,2} - a_{2\,1}d_{2\,1}.$$

We obtain, as $d_{1\,1}, d_{2\,2}$ are non-zero, that $d_{1\,2} = d_{2\,1} = a_{1\,2} = a_{2\,1} = 0$, which is the required conclusion. $\square$

5. PROOF OF THE SIMPLICITY CRITERIA

In this Section, we will complete the proofs of Theorem 1.1 and Corollary 1.2. Then we will present and prove a variant of Theorem 1.1.

5.1. **Two lemmas.**

Lemma 5.1. *Let K be a field of characteristic zero and let B be a unipotent endomorphism of a finite-dimensional vector space E over K. Let m be a nonzero integer. Then, any subspace of E which is invariant under B^m is also invariant under B.*

Proof. Write $B = \mathrm{id} + N$ with N nilpotent, and $B^m = \mathrm{id} + N'$. Then N' is a polynomial function of N with no constant term and nontrivial linear term (as K has zero characteristic). Writing also the $(N')^j$ in terms of the N^i, $i \geqslant j$, we get a triangular system with nonzero diagonal terms that we can solve for N as a polynomial function of N'. Thus B is a polynomial function of B^m. The assertion of the lemma is an immediate consequence of this fact. $\square$

Lemma 5.2. *Let A, B be two elements of $SL_2(\mathbb{Z})$. Assume that A is b-reduced and that $\mathrm{tr}\,(B) = 2$. Then, after replacing if necessary B by B^{-1}, there exists n_0 such that, for any $n_1, n_2, n_3 \geqslant n_0$, the matrix $A^{n_1} B^{n_2} A^{n_3}$ is b-reduced.*

Proof. If $B = \mathrm{id}$, the assertion of the lemma follows from the fact that the product of b-reduced matrices is b-reduced. For the rest of the proof, we assume that $B \neq \mathrm{id}$, and denote by L a rational line which is fixed by B.

Define the cones in $\mathbb{R}^2$ (using the natural basis (e_1, e_2) and coordinates (x_1, x_2))

$$\mathcal{C}^+ := \{0 < x_2 < x_1\}, \quad \mathcal{C}^- := \{0 < -x_1 < x_2\}.$$

Observe that, if $C \in SL_2(\mathbb{Z})$ satisfies, for $i = 1, 2$, the two conditions

$$C(e_i) \in \mathcal{C}^+ \quad \text{and} \quad C^{-1}(e_i) \in \mathcal{C}^- \cup -\mathcal{C}^-$$

then C is b-reduced. Conversely, if C is b-reduced, its trace is $\geqslant 3$. Moreover, by a simple application of the Perron-Frobenius theorem (or a direct calculation), the cone $\mathcal{C}^+$ contains a unit eigenvector $e_u(C)$ of C associated to the eigenvalue > 1, and the cone $\mathcal{C}^-$ contains a unit eigenvector $e_s(C)$ associated to the eigenvalue in $(0, 1)$.

As L is rational and the line spanned by $e_s(A)$ is not rational, there exists a unit vector e generating L such that, in the decomposition $e = \alpha_s e_s(A) + \alpha_u e_u(A)$, one has $\alpha_u > 0$. Using next that the line spanned by $e_u(A)$ is distinct from L, we may assume, replacing B by B^{-1} if necessary, that the oriented direction of $B^n(e_u(A))$ for large n is close to e. Then the oriented direction of $A^{n_1} B^{n_2} A^{n_3}(e_i)$ is, for large n_1, n_2, n_3 and $i = 1, 2$, close to $e_u(A)$. The oriented direction of $A^{-n_3} B^{-n_2} A^{-n_1}(e_i)$ is close to $\pm e_s(A)$. Taking into account the remarks above on b-reduced matrices, the proof of the lemma is complete. $\square$

5.2. **Proof of Theorem 1.1.**
We want to show Theorem 1.1 by applying the version of the simplicity criterion of Avila-Viana restated as Theorem 2.17 .

Let M, A, B be as in Theorem 1.1. The linear part of A has trace > 2, hence is conjugated in $SL(2, \mathbb{Z})$ to a b-reduced matrix (cf. Remark 3.10). After replacing M if necessary by another origami in the same $SL_2(\mathbb{Z})$-orbit, we may assume that the linear part of A is b-reduced.

The full shift appearing in the statement of Theorem 2.17 is the one that has been considered in Subsection 3.4: the letters of the corresponding alphabet are the loops in $\Gamma(M)$ which go exactly once through (M, b). It was shown in that subsection that the version of the Gauss measure corresponding to this setting has the bounded distortion property, and that the KZ-cocycle is locally constant and integrable.

By Corollary 3.9, the affine map A is associated to some loop in $\Gamma(M)$ through (M, b), i.e to a word in this alphabet.

By Lemma 5.2, there exists $n_0 > 0$ such that, for $n_1, n_2, n_3 \geqslant n_0$, the linear part of $A^{n_1} B^{n_2} A^{n_3}$ is b-reduced. Define $B' := B^{n_0}$.

We claim that the hypotheses of Theorem 4.5 (with $d = g - 1$, Ω the symplectic intersection form on $H_1^{(0)}(M, \mathbb{Z})$) are satisfied by the endomorphisms of $H_1^{(0)}(M, \mathbb{Z})$ induced by A and B'. Indeed, the endomorphism induced by A is Galois-pinching from the hypothesis of Theorem 1.1. If there were a proper subspace of $H_1^{(0)}(M, \mathbb{R})$ invariant by the action of A and B'^2, it would also be invariant by B (Lemma 5.1). Applying Proposition 4.3 would give a contradiction with the hypothesis of Theorem 1.1.

Let $C = B' A^{\ell_1} \cdots B' A^{\ell_{m-1}} B'$ be an element (given by Theorem 4.5) whose linear part is k-twisting with respect to A for all $1 \leqslant k \leqslant g - 1$. We may assume, according to the statement of this theorem, that the integers $\ell_1, \ldots, \ell_{m-1}$ are $\geqslant 2n_0$. Observe that the linear part of $C' := A^{n_0} C A^{n_0}$ is also k-twisting with respect to A for all $1 \leqslant k \leqslant g - 1$.

By Lemma 5.2 (using also that the product of b-reduced matrices is b-reduced), the linear part of C' is b-reduced. Therefore, the affine map $C' \in \mathrm{Aff}(M)$ is associated to some loop through (M, b) in $\Gamma(M)$, i.e to some word in the alphabet.

Applying Theorem 2.17 , we conclude that the Lyapunov spectrum of the discrete version of the KZ-cocycle G_M^{KZ} discussed in Subsection 3.3 is simple. This concludes the proof of Theorem 1.1. $\qquad\square$

5.3. **Proof of Corollary 1.2.** By Proposition 2.4, the origami (M, ω) has no nontrivial automorphism. The hypotheses regarding A are the same in Theorem 1.1 and Corollary 1.2. To prove Corollary 1.2, it is therefore sufficient to find, assuming the existence of a rational direction with homological direction $\neq 1, g$, an affine homeomorphism B which acts on $H_1^{(0)}(M, \mathbb{Q})$ through a unipotent endomorphism distinct from the identity, and such that the image of $B - \mathrm{id}$ is not a lagrangian subspace of $H_1^{(0)}(M, \mathbb{Q})$.

We may assume that the rational direction in the hypothesis is the horizontal direction. Let E be the subspace of $H_1(M, \mathbb{Q})$ spanned by the waist curves of the horizontal cylinders of (M, ω). By hypothesis, we have

$$1 < \dim E < g.$$

On the other hand, the image of E under the map $p_* : H_1(M, \mathbb{Q}) \to H_1(\mathbb{T}^2, \mathbb{Q}) \simeq \mathbb{Q}^2$ is the one-dimensional horizontal subspace. Therefore the intersection of E with $H_1^{(0)}(M, \mathbb{Q})$ satisfies

$$0 < \dim(E \cap H_1^{(0)}(M, \mathbb{Q})) < g - 1.$$

Let $K > 0$ be an integer such that

- The matrix $\begin{pmatrix} 1 & K \\ 0 & 1 \end{pmatrix}$ belongs to the Veech group of (M, ω).

- The affine homeomorphism B of (M, ω) with linear part $\begin{pmatrix} 1 & K \\ 0 & 1 \end{pmatrix}$ fixes each horizontal separatrix.

We claim that B has the required properties.

Indeed, as the form ω has a single zero, the homology group $H_1(M, \mathbb{Q})$ is spanned by curves which either are horizontal saddle connections or cross upwards a horizontal cylinder without entering the other cylinders. A homology class of the first kind is fixed by B. An homology class γ of the second kind, crossing a cylinder C, satisfies

$$B_*(\gamma) - \gamma = m_C \sigma_C,$$

where σ_C is the class of the waist curve of C, oriented rightwards, and m_C is a positive integer. Observe that σ_C is a linear combination of classes of the first kind. Therefore $B_* - \text{id}$ on $H_1(M, \mathbb{Q})$ is nilpotent of degree 2. The image of $H_1^{(0)}(M, \mathbb{Q})$ under $B_* - \text{id}$ is contained in $E \cap H_1^{(0)}(M, \mathbb{Q})$, hence is not lagrangian. Finally, the restriction of B_* to $H_1^{(0)}(M, \mathbb{Q})$ is not equal to the identity: take two horizontal cylinders C, C' such that $\sigma_C, \sigma_{C'}$ are linearly independent, and two classes of the second kind $\gamma_C, \gamma_{C'}$ which cross respectively C, C'. An appropriate combination $\gamma := n_C \gamma_C - n_{C'} \gamma_{C'} + n\sigma_C$, with $n_C, n_{C'} > 0$ belongs to $H_1^{(0)}(M, \mathbb{Q})$ and satisfies

$$B_*(\gamma) - \gamma = m_C n_C \sigma_C - m_{C'} n_{C'} \sigma_{C'} \neq 0.$$

Remark 5.3. It is easy to construct a reduced square-tiled surface (M, ω) of genus 3 with two double zeroes and no nontrivial automorphism such that the horizontal direction has homological dimension 2 but such that any parabolic matrix in the Veech group which fixes the horizontal direction acts on $H_1^{(0)}$ by the identity. This means that the proof above is not valid if we replace in Corollary 1.2 the assumption that ω has a single zero by the weaker assumption that (M, ω) has no nontrivial automorphism.

5.4. **A variant of Theorem 1.1.** Instead of using one unipotent affine homeomorphism to obtain the twisting condition relative to the Galois-pinching homeomorphism A, one may use another pseudo-Anosov homeomorphism.

Theorem 5.4. *Let (M, ω) be a reduced square-tiled surface having no nontrivial automorphism. Assume that there exist two affine homeomorphisms A, B of (M, ω) with the following properties:*

  i) *Both linear parts DA, DB are b-reduced;*
  ii) *A is Galois-pinching;*
  iii) *The minimal polynomial of the endomorphism of $H_1^{(0)}(M, \mathbb{Q})$ induced by B has degree > 2, no irreducible even factor, and its splitting field is disjoint from the splitting field of the characteristic polynomial of the endomorphism of $H_1^{(0)}(M, \mathbb{Q})$ induced by A.*

Then, the Lyapunov spectrum of the KZ-cocycle, relative to the $SL_2(\mathbb{R})$-invariant probability measure supported by the $SL_2(\mathbb{R})$-orbit of (M, ω) in moduli space, is simple.

Proof. As in Subsection 5.2, we plan to apply Theorem 2.17, using Theorem 4.5 to get the twisting hypothesis. The Teichmüller flow restricted to the $SL_2(\mathbb{R})$-orbit of (M, Ω) is still viewed as a suspension over the full shift on a countable alphabet, whose letters are the loops in $\Gamma(M)$ (based at (M, b)). Then hypothesis i) means that A, B correspond to words in this alphabet (see Subsection 3.5). It has already been checked that the Haar measure has the bounded distortion property, and that the appropriate version of the KZ-cocycle is locally constant and integrable. So the proof of Theorem 5.4 reduces to the following lemma, where we write A_*, B_* for the endomorphisms of $H_1^{(0)}(M, \mathbb{Q})$ induced by A, B.

Lemma 5.5. *Under the hypotheses ii), iii) of the Theorem, A_* and B_*^2 do not share a common proper invariant subspace.*

We first prove that a subspace invariant under B_*^2 is invariant under B_*. Indeed, it is sufficient to prove this when the base field is $\mathbb{C}$. Then, a B_*-invariant subspace is the sum of its intersection with the characteristic subspaces of B_*, and the same holds for B_*^2. But B_* and B_*^2 have the same characteristic subspaces, because hypothesis iii) on the non existence of an irreducible even factor means that, for any $\lambda \in \mathbb{C}$, λ and $-\lambda$ cannot be

both eigenvalues of B_*. Thus it is sufficient to prove that a subspace contained in some characteristic subspace of B_* which is invariant under B_*^2 is also invariant under B_*. Up to a scalar factor, this is the unipotent case which was dealt with in Lemma 5.1.

To prove the lemma, it is therefore sufficient to see that A_* and B_* do not share a proper invariant subspace. Otherwise, as we have seen in the proof of Proposition 4.3, a proper common invariant subspace of minimal dimension has to be either one-dimensional, spanned by an eigenvector v_λ of A_*, or two-dimensional, spanned by two eigenvectors v_λ, $v_{\lambda^{-1}}$. In both cases, considering the action of the Galois group of the characteristic polynomial of A_*, we conclude that $H_1^{(0)}(M, \mathbb{Q})$ splits into 2-dimensional summands $\langle v_\lambda, v_{\lambda^{-1}} \rangle$ which are invariant under B_* (and A_*).

These subspaces are defined over the field $\mathbb{Q}(\lambda + \lambda^{-1})$. The trace and the determinant of the restriction of B_* to these subspaces belong to this field. In view of the hypothesis of disjointness of the splitting fields for A_* and B_*, the trace and the determinant must be rational. But then the minimal polynomial of B_* has degree $\leqslant 2$, in contradiction to hypothesis iii). $\qquad\square$

6. Origamis in $\mathcal{H}(4)$

Simplifying the full notation $\mathcal{H}(M, \Sigma, \kappa)$, we will denote by $\mathcal{H}(4)$ the moduli space of translation surfaces of genus 3 with a single marked point, which is a zero of order 4 of the associated 1-form.

6.1. **Some basic facts.** For origamis in $\mathcal{H}(4)$, it is equivalent to be primitive or reduced.

Proposition 6.1. *A reduced square-tiled surface in $\mathcal{H}(4)$ is primitive.*

Proof. Let (M, ω) be a reduced square-tiled surface in $\mathcal{H}(4)$, and let $p : (M, \omega) \to (N, \omega')$ be a ramified covering of degree > 1 over another square-tiled surface (N, ω'). The Riemann-Hurwitz formula states that

$$4 = 2g(M) - 2 = \deg(p)(2g(N) - 2) + \sum \operatorname{ord}(c),$$

where the sum is over critical points c of p and $\operatorname{ord}(c)$ is the ramification order. As $\deg(p) > 1$, we have either $g(N) = 2$, $\deg(p) = 2$ and no critical point or $g(N) = 1$. In the first case, as p is unramified, the 1-form ω has 2 or 4 zeros, contradicting the assumption that $(M, \omega) \in \mathcal{H}(4)$. In the second case, p has a single critical point of order 4. As (M, ω) is reduced, (N, ω') must be the standard torus and p must be the canonical covering associated to (M, ω). $\qquad\square$

The following result of Zmiaikou ([Zm, Theorem 3.12]) classifies monodromy groups.

Proposition 6.2. *The monodromy group of a primitive square-tiled surface in $\mathcal{H}(4)$ with $N \geqslant 7$ squares is equal to the full symmetric group S_N or to the alternating group A_N.*

6.2. **Connected components of $\mathcal{H}(4)$.** As a translation surface (M, ω) in $\mathcal{H}(4)$ has no nontrivial automorphism, it admits at most one anti-automorphism, which must be an involution. The unique zero O of ω is a fixed point of this involution (when it exists). Quotienting by this involution (denoted by ι), we get a ramified double cover $\pi : M \to N$; the ramification points are the fixed points of ι. The Riemann-Hurwitz formula relates the number $l(\iota)$ of fixed points of ι to the genus of N

$$4 = 2g_M - 2 = 2(2g_N - 2) + l(\iota).$$

As $l(\iota) > 0$, there are only two possibilities: $g_N = 0, l(\iota) = 8$ and $g_N = 1, l(\iota) = 4$.

Recall that the moduli space $\mathcal{H}(4)$, the simplest one which is not connected, has two connected components ([Ve4], [KZ]), which are respectively called the *hyperelliptic* and the *odd* component. A translation surface in $\mathcal{H}(4)$ belongs to the hyperelliptic component iff it admits an anti-automorphism with 8 fixed points. On the other hand, a translation surface in the odd component of $\mathcal{H}(4)$ may or may not admit an anti-automorphism. When it does, one says, following McMullen [Mc], that the translation surface belongs to the Prym locus or is simply Prym.[8]

Remark 6.3. The 1-form ω induces on the quotient N a quadratic differential q related to ω through $\pi^* q = \omega^2$. The quadratic differential q is not the square of a 1-form; it has a zero of order 3 at $\pi(O)$ and a simple pole at the images of the other fixed points.

6.3. **Cylinders and saddle configurations.** Let (M, ω) be a translation surface. A direction $v \in \mathbb{P}(\mathbb{R}^2)$ is *completely periodic* if every separatrix in direction v extends to a saddle connection. Then, the saddle connections (endpoints included) separate the surface into a finite number of *cylinders*. Each cylinder is foliated by periodic orbits of the linear flow in the v-direction.

For a square-tiled surface, the completely periodic directions are exactly the rational directions $v \in \mathbb{P}(\mathbb{Q}^2)$.

Let $v \in \mathbb{P}(\mathbb{R}^2)$ be a completely periodic direction for the translation surface (M, ω). Denote by $C_1, \ldots, C_m$ the associated cylinders and by $\gamma_1, \ldots, \gamma_m$ the homology classes in $H_1(M, \mathbb{Z})$ defined by the waist curves of these cylinders (oriented in a consistent way). As these curves do not intersect, the subspace of $H_1(M, \mathbb{R})$ generated by $\gamma_1, \ldots, \gamma_m$ is isotropic.

If moreover the translation surface (M, ω) has a single marked point O, the homology classes $\gamma_1, \ldots, \gamma_m$ are linearly independent: indeed, O belongs to both components of each cylinder C_i, hence one can find a loop at O which intersects once γ_i, but not the γ_j, $j \neq i$. A consequence is that the number of cylinders in this case is at most the genus of M. For $(M, \omega) \in \mathcal{H}(4)$, one can have between one and three cylinders in completely periodic directions.

Consider a completely periodic direction v for a translation surface $(M, \omega) \in \mathcal{H}(4)$. After applying if necessary an element of $SL_2(\mathbb{R})$, we may assume that v is the horizontal direction. Index in the cyclical order the 10 horizontal separatrices from the marked point O by $\mathbb{Z}_{10}$ (choosing an arbitrary separatrix as S_0). Each of the 5 saddle connections connect two separatrices S_i and S_j such that $j - i$ is odd. The pairing of separatrices determined by the saddle connections is called a *saddle configuration*.

S. Lelièvre has determined which saddle configurations occur in each component of $\mathcal{H}(4)$, and how many cylinders correspond to each saddle configuration. The full list of the 16 possible saddle configurations appears in Appendix C of this paper (by S. Lelièvre), and, for this reason, we will not discuss it in details in this section. Instead, we will only extract (in Proposition 6.5) from the list the information which is relevant for us in Sections 7 and 8.

Definition 6.4. A saddle-connection is *balanced* if it connects S_i and S_{i+5}.

---

[8]Prym varieties are certain abelian varieties constructed from morphisms of algebraic curves. When an algebraic curve is equipped with an holomorphic involution, one may consider the abelian subvarieties of the Jacobian obtained by duality from the eigenforms associated to the eigenvalues ± 1.

Proposition 6.5.   (1) *When (M,ω) belongs to the hyperelliptic component of $\mathcal{H}(4)$,
the number b of balanced saddle connections in a given saddle configuration and
the number c of cylinders generated by this saddle configuration satisfy $b+2c = 7$.*

(2) *When (M,ω) belongs to the odd component of $\mathcal{H}(4)$, if a saddle configuration has
at least 2 balanced saddle connections, then it has 3 such saddle connections and
they separate M into exactly 2 cylinders.*

6.4. **The HLK-invariant.** Assume now that (M,ω) is a reduced *square-tiled* surface in
$\mathcal{H}(4)$, and that ι is an anti-automorphism of (M,ω). Denote by $p : M \to \mathbb{T}^2$ the covering
associated to ω. Following the work of E. Kani [Ka] and P. Hubert -S. Lelièvre [HL] in
genus two, it is natural to partition the fixed points of ι in the following way. The anti-
automorphism ι is a lift under p of the anti-automorphism $\iota_0(z) := -z$ of $\mathbb{T}^2$. The fixed
points of ι are sent by p to fixed points of ι_0. The fixed points of ι_0 are the 4 points of order
2 in $\mathbb{T}^2$. Thus, it is natural to count, for each point of order 2 in $\mathbb{T}^2$, how many fixed points
of ι sit above it.

The action of $SL(2,\mathbb{Z})$ on the torus fixes the origin 0, and preserves the 3-element set of
points of exact order 2, acting on this set through the full symmetric group S_3. As we want
to define an invariant for the action of $SL_2(\mathbb{Z})$ on origamis, we define the HLK-invariant
$\ell(\iota)= \ell(M,\omega)$ to be $(l_0, [l_1, l_2, l_3])$ where

- l_0 is the number of fixed points of ι, distinct from the zero O of ω, sitting above
  the origin of $\mathbb{T}^2$;
- l_1, l_2, l_3 are the number of fixed points above the 3 points of $\mathbb{T}^2$ of exact order 2;
  they form an unordered triple that we write for convenience with the convention
  $l_1 \geqslant l_2 \geqslant l_3$.

Notice that $l_0 + l_1 + l_2 + l_3$ is equal to 7 in the hyperelliptic case and to 3 in the Prym
case. Another restriction is that $l_0 +1, l_1, l_2, l_3$ and the number N of squares are congruent
mod. 2: indeed, the fiber of p over a point of order 2 is preserved by the involution ι and
contains N elements. A further restriction is given by the

Proposition 6.6. *In the hyperelliptic case, at most one of the three numbers l_1, l_2, l_3 is
equal to zero.*

Proof. Assume on the contrary that at least two of these numbers are equal to 0. By
applying an appropriate element of $SL_2(\mathbb{Z})$ if necessary, we may assume that there is no
fixed point of ι above $(0, \frac{1}{2})$ and $(\frac{1}{2}, \frac{1}{2})$. There are between 1 and 3 horizontal cylinders.

Lemma 6.7. *Every horizontal cylinder is fixed by ι.*

Proof. Assume that there is at most one horizontal cylinder which is fixed by ι. Such a
cylinder would contain 2 fixed points of ι in its interior. The other fixed points of ι are O
(the zero of ω) and the middle points of every horizontal saddle-connection which is fixed
by ι. To account for the 8 fixed points, there must exist a horizontal cylinder C fixed by ι,
and every horizontal saddle-connection must be fixed by ι. Thus every horizontal saddle-
connection in the top boundary of C is also in the bottom boundary. This means that there
is only one horizontal cylinder and ends the proof of the lemma.   □

Each horizontal cylinder, being fixed by ι, contains two fixed points of ι. As these fixed
points sit over $(0,0)$ or $(\frac{1}{2},0)$, the height of each horizontal cylinder is even. But then
(M,ω) is not reduced.   □

The various restrictions leave the following possibilities for the HLK-invariant:

- In the hyperelliptic case, $(4, [1, 1, 1])$, $(2, [3, 1, 1])$, $(0, [5, 1, 1])$, $(0, [3, 3, 1])$ for an odd number of squares, and $(3, [2, 2, 0])$, $(1, [4, 2, 0])$, $(1, [2, 2, 2])$ for an even number.
- In the Prym case, $(0, [1, 1, 1])$ for an odd number of squares, and $(1, [2, 0, 0])$, $(3, [0, 0, 0])$ for an even number.

6.5. **A conjecture of Delecroix and Lelièvre.** On the basis of computer experiments (with SAGE), V. Delecroix and S. Lelièvre have formulated the following conjecture.

Conjecture 6.8. *For $N > 8$, the number of $\mathrm{SL}_2(\mathbb{Z})$-orbits of primitive N-square origamis in $\mathcal{H}(4)$ is as follows:*

- *there are precisely two such $\mathrm{SL}_2(\mathbb{Z})$-orbits in the odd component of $\mathcal{H}(4)$ outside of the Prym locus, distinguished by their monodromy group being A_N or S_N;*
- *for odd N, there are precisely four such $\mathrm{SL}_2(\mathbb{Z})$-orbits in the hyperelliptic component of $\mathcal{H}(4)$, distinguished by their HLK-invariant being $(4, [1, 1, 1])$, $(2, [3, 1, 1])$, $(0, [5, 1, 1])$ or $(0, [3, 3, 1])$;*
- *for even N, there are precisely three such $\mathrm{SL}_2(\mathbb{Z})$-orbits in the hyperelliptic component of $\mathcal{H}(4)$, distinguished by the HLK-invariant being $(3, [2, 2, 0])$, $(1, [4, 2, 0])$ or $(1, [2, 2, 2])$.*

6.6. **Prym covers.** We don't have any new result for origamis of Prym type in $\mathcal{H}(4)$. For the sake of completeness, we recall a couple of important facts.

Let (M, ω) be a square-tiled of Prym type in $\mathcal{H}(4)$. Denote by ι the anti-automorphism of (M, ω). It commutes with any affine homeomorphism of (M, ω). It acts as an involution on the space $H_1^{(0)}(M, \mathbb{Q})$. The eigenspaces $H_\pm$ associated with the eigenvalues ± 1 both have dimension 2, and the splitting

$$H_1^{(0)}(M, \mathbb{Q}) = H_+ \oplus H_-$$

into orthogonal symplectic subspaces is invariant under the affine group of (M, ω). It means that it is also invariant under the KZ-cocycle. Denote by $\pm\lambda_+$ (resp. $\pm\lambda_-$) the Lyapunov exponents of the restriction of the KZ cocycle to H_+ (resp. H_-), with $\lambda_\pm \geqslant 0$.

Chen and Möller have shown [CM] that $\lambda_+ + \lambda_- = \frac{3}{5}$, i.e the sum of the nontrivial exponents is the same than for the Masur-Veech measure of the odd component. On the other hand, Eskin, Kontsevich and Zorich have proved ([EKZ, Theorem 2]) that $\lambda_- - \lambda_+ = \frac{1}{5}$.

Put together, these results prove that the nontrivial exponents for an origami in $\mathcal{H}(4)$ of Prym type are $\pm\frac{1}{5}$, $\pm\frac{2}{5}$.

Regarding the classification of $SL_2(\mathbb{Z})$-orbits of primitive origamis of Prym type, this was settled by E. Lanneau and D.-M. Nguyen [LN] before the formulation of the conjecture of Delecroix-Lelièvre.

Theorem 6.9. *For $N > 8$, the number of $\mathrm{SL}_2(\mathbb{Z})$-orbits of primitive N-square origamis in the Prym locus of $\mathcal{H}(4)$ is as follows:*

- *for odd N, there is precisely one $\mathrm{SL}_2(\mathbb{Z})$-orbit; the HLK-invariant is $(0, [1, 1, 1])$;*
- *For $N \equiv 0 \bmod 4$, there is precisely one $\mathrm{SL}_2(\mathbb{Z})$-orbit; its HLK- invariant is equal to $(1, [2, 0, 0])$;*
- *If $N \equiv 2 \bmod 4$, there are precisely two $\mathrm{SL}_2(\mathbb{Z})$-orbits, distinguished by their HLK-invariant being $(1, [2, 0, 0])$ or $(3, [0, 0, 0])$.*

6.7. **Splitting fields of monic quartic reciprocal polynomials.** In the next two sections, we will construct certain affine maps of origamis in $\mathcal{H}(4)$ which potentially act on $H_1^{(0)}$ as Galois-pinching matrices. We present now some elementary Galois theory which is relevant to this question.

Let $P(x) = x^4 + ax^3 + bx^2 + ax + 1 \in \mathbb{Q}[x]$ be a reciprocal polynomial of degree 4. We define
$$t := -a - 4, \quad d := b + 2a + 2,$$
so that λ is a zero of P iff $\mu := \lambda + \lambda^{-1} - 2$ is a zero of $Q(y) := y^2 - ty + d$. The discriminant of Q is[9]
$$\Delta_1 := t^2 - 4d = a^2 - 4b + 8.$$
The following fact is an easy exercise.

Lemma 6.10. *The polynomial P is reducible over $\mathbb{Q}$ iff Δ_1 is a square.*

From now on, we assume that Δ_1 is *not* a square, hence P is irreducible. Denote by μ_1, μ_2 the roots of Q and by $\lambda_1^{\pm 1}, \lambda_2^{\pm 1}$ those of P, with $\mu_i = \lambda_i + \lambda_i^{-1} - 2$. Denote by Gal the Galois group of P, by $p : \text{Gal} \to S_2$ the surjective homomorphism corresponding to the action of Gal on $\{\mu_1, \mu_2\}$ and by Gal_0 the kernel of p. As Gal acts transitively on the roots of P, there are two possibilities:

(1) $\text{Gal}_0 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ has order 4, allowing independent switches of λ_i and λ_i^{-1}, $i = 1, 2$.

(2) $\text{Gal}_0 \simeq \mathbb{Z}_2$ has order 2, the nontrivial element switching simultaneously $\lambda_1, \lambda_1^{-1}$ and $\lambda_2, \lambda_2^{-1}$.

In case (1), the Galois group has order 8, is largest possible and is the centralizer of the permutation $(\lambda_1, \lambda_1^{-1})(\lambda_2, \lambda_2^{-1})$. In case (2), the Galois group has order 4 and there are 2 subcases:

(2a) $\text{Gal} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ is generated by $(\lambda_1, \lambda_2)(\lambda_1^{-1}, \lambda_2^{-1})$ and $(\lambda_1, \lambda_1^{-1})(\lambda_2, \lambda_2^{-1})$.

(2b) $\text{Gal} \simeq \mathbb{Z}_4$ is generated by the 4-cycle $(\lambda_1, \lambda_2, \lambda_1^{-1}, \lambda_2^{-1})$.

Define

$$
\begin{aligned}
\Delta_2 &:= (\lambda_1 - \lambda_1^{-1})^2 (\lambda_2 - \lambda_2^{-1})^2 \\
&= \mu_1 \mu_2 (\mu_1 + 4)(\mu_2 + 4) \\
&= d(d + 4t + 16) = (b + 2 + 2a)(b + 2 - 2a).
\end{aligned}
$$

Lemma 6.11. *Case (2a) occurs iff Δ_2 is a square.*

Proof. If case (2a) occurs, then $(\lambda_1 - \lambda_1^{-1})(\lambda_2 - \lambda_2^{-1})$ is invariant under the Galois group, hence is rational, and Δ_2 is a square. Conversely, assume that $\Delta_2 = \delta_2^2$ is a square. One has $\lambda_i^{\pm 1} = \frac{1}{2}(\mu_i + 2 \pm \sqrt{\mu_i(\mu_i + 4)})$. The splitting field of P is the quadratic extension of $\mathbb{Q}(\sqrt{\Delta_1}) = \mathbb{Q}(\mu_1) = \mathbb{Q}(\mu_2)$ generated by a square root of $\mu_1(\mu_1 + 4)$ because
$$\sqrt{\mu_2(\mu_2 + 4)} = \frac{\delta_2}{\sqrt{\mu_1(\mu_1 + 4)}}.$$
This extension has a Galois group isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. $\square$

Lemma 6.12. *Case (2b) occurs iff $\Delta_1 \Delta_2$ is a square.*

---

[9]We use the substitution $\mu := \lambda + \lambda^{-1} - 2$ rather than $\mu := \lambda + \lambda^{-1}$ because it appears naturally later.

Proof. Observe that $\Delta_1\Delta_2 = \delta^2$, with

$$\delta = (\lambda_1 + \lambda_1^{-1} - \lambda_2 - \lambda_2^{-1})(\lambda_1 - \lambda_1^{-1})(\lambda_2 - \lambda_2^{-1}).$$

If case (2b) occurs, then δ is invariant under the Galois group, hence is rational, and $\Delta_1\Delta_2$ is a square. Conversely, assume that $\Delta_1\Delta_2$ is a square. The splitting field of P is still the quadratic extension of $\mathbb{Q}(\sqrt{\Delta_1})$ generated by a square root of $\mu_1(\mu_1 + 4)$, because now

$$\sqrt{\mu_2(\mu_2 + 4)} = \frac{\delta}{\sqrt{\Delta_1}\sqrt{\mu_1(\mu_1 + 4)}}.$$

Thus the Galois group has order 4. As Δ_1 is not a square, Δ_2 is also not a square. By Lemma 6.11, case (2a) does not occur; hence case (2b) must occur. $\qquad\square$

We can now conclude:

Proposition 6.13. *The Galois group has maximal order 8 iff neither Δ_2 nor $\Delta_1\Delta_2$ is a square.*

Remark 6.14. In case (1), the Galois group of order 8 contains 3 subgroups of index 2, namely Gal_0 and the Galois groups of case (2a) and (2b). The three quadratic fields contained in the splitting field of P which correspond to these subgroups are easily seen to be $\mathbb{Q}(\sqrt{\Delta_1})$, $\mathbb{Q}(\sqrt{\Delta_2})$, and $\mathbb{Q}(\sqrt{\Delta_1\Delta_2})$ respectively.

Recall that a Galois-pinching matrix must have all its eigenvalues real. For a reciprocal polynomial of degree 4 (with real coefficients), we have the following observation

Proposition 6.15. *The roots of P are simple, real and positive iff $\Delta_1 > 0$, $d > 0$ and $t > 0$.*

Proof. Recall that λ is a root of P iff $\mu = \lambda + \lambda^{-1} - 2$ is a root of $Q(y) := y^2 - ty + d$. The roots λ are simple, real and positive iff the roots μ have the same property. The conclusion of the proposition follows. $\qquad\square$

In Sections 7 and 8, we will consider one-parameter families (M_n, ω_n) of origamis in $\mathcal{H}(4)$ indexed by an integer n. For each origami in the family, we will construct an element A_n of the affine group $\mathrm{Aff}(\omega_n)$. The characteristic polynomial of the action of A_n on $H_1^{(0)}(M_n, \mathbb{Q})$ is a monic reciprocal polynomial P_n of degree 4 with integer coefficients.

For each integer n, we will compute the quantities $\Delta_1(P_n)$, $\Delta_2(P_n)$ from the last subsection. The constructions of M_n, ω_n, A_n are such that both $\Delta_1(P_n)$ and $\Delta_2(P_n)$ will be *polynomial functions of the variable n with integer coefficients*. In order to claim that neither $\Delta_1(P_n)$ nor $\Delta_2(P_n)$ nor the product $\Delta_1(P_n)\Delta_2(P_n)$ are squares for all but finitely many n, we will appeal to Siegel's theorem on the finiteness of integral points on curves of genus > 0. In order to do this, we introduce the following definition.

Definition 6.16. Let $\Delta \in \mathbb{Z}[x]$ be a polynomial. Write $\Delta = \delta^2 \Delta^{\mathrm{red}}$ with $\delta, \Delta^{\mathrm{red}} \in \mathbb{Z}[x]$ and Δ^{red} square-free. The *reduced degree* of Δ, denoted by $\deg^{\mathrm{red}}(\Delta)$ is the degree of Δ^{red}.

The following result is then a special case of Siegel's theorem.

Proposition 6.17. *If $\deg^{\mathrm{red}}(\Delta) \geqslant 3$, there are only finitely many values of the integer n such that $\Delta(n)$ is a square.*

Proof. Indeed each such value of n gives an integral point on the curve $y^2 = \Delta^{\mathrm{red}}(x)$, which is nonsingular (except for a possible double point at ∞) of genus > 0. $\qquad\square$

7. THE ODD CASE

7.1. **A model for odd origamis in** $\mathcal{H}(4)$**.** Consider the origami $\mathcal{O}$ constructed as indicated on Figure 1 below. It depends on 6 parameters $H_1, H_2, H_3, V_1, V_2, V_3$ which are positive integers.
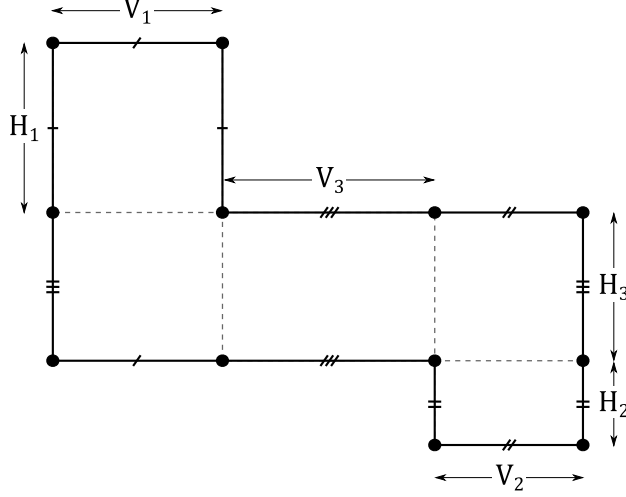
FIGURE 1. A origami in the odd component of $\mathcal{H}(4)$.

In the horizontal direction, there are 3 cylinders Ch_1, Ch_2, Ch_3. The height of these cylinders are respectively H_1, H_2, H_3, while the length of the waist curves are respectively $\ell(Ch_1) = V_1, \ell(Ch_2) = V_2, \ell(Ch_3) = V_1 + V_2 + V_3$.

In the vertical direction, there are also 3 cylinders Cv_1, Cv_2, Cv_3. The height of these cylinders are respectively V_1, V_2, V_3, while the length of the waist curves are respectively $\ell(Cv_1) = H_1 + H_3, \ell(Cv_2) = H_2 + H_3, \ell(Cv_3) = H_3$.

We will denote by σ_i, $i = 1, 2, 3$, the homology class of the waist curve of Ch_i, oriented rightwards, and by ζ_i , $i = 1, 2, 3$, the homology class of the waist curve of Cv_i, oriented upwards. The symplectic intersection form ι on $H_1(\mathcal{O}, \mathbb{Z})$ satisfies

$$\iota(\sigma_i, \sigma_j) = \iota(\zeta_i, \zeta_j) = 0, \quad \iota(\sigma_i, \zeta_j) = I_{ij},$$

with

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}.$$

We review some elementary properties of $\mathcal{O}$:
- $\mathcal{O}$ has a single conical singularity of total angle 10π, so it belongs to $\mathcal{H}(4)$.
- The number of squares is

$$N(\mathcal{O}) = H_1 V_1 + H_2 V_2 + H_3(V_1 + V_2 + V_3).$$

- $\mathcal{O}$ is reduced if and only if $\gcd(H_1, H_2, H_3) = \gcd(V_1, V_2, V_3) = 1$: indeed, the condition is clearly necessary. It is also sufficient because the vectors $(V_i, 0)$ and $(0, H_i)$ are periods for $i = 1, 2, 3$.
- The classes $\sigma_1, \sigma_2, \sigma_3, \zeta_1, \zeta_2, \zeta_3$ form a basis of the integral homology $H_1(\mathcal{O}, \mathbb{Z})$: indeed, the matrix I above is invertible over $\mathbb{Z}$.

- The origami $\mathcal{O}$ admits an affine involution with derivative $-\mathrm{Id}$ iff $H_1 = H_2$ and $V_1 = V_2$. Indeed, such an involution must send an horizontal cylinder to an horiziontal cylinder, and similarly for vertical cylinders. Therefore, it must preserve Ch_3 (the horizontal cylinder with the longest waist curve) , Cv_3 (the vertical cylinder with the shortest waist curve) and the rectangular intersection $Ch_3 \cap Cv_3$. As the derivative is $-\mathrm{Id}$, it must exchange Ch_1 and Ch_2, and also Cv_1 and Cv_2. This forces $H_1 = H_2$ and $V_1 = V_2$. Conversely, if these equalities hold, the central symmetry preserving $Ch_3 \cap Cv_3$ defines the required involution.
- $\mathcal{O}$ belongs to the odd component of $\mathcal{H}(4)$. When the parameters H_i, V_i vary among positive real numbers we get a family of translation surfaces in a single component of $\mathcal{H}(4)$. It cannot be the hyperelliptic component because most of these surfaces do not have the required affine involution.

We also recall that an origami in $\mathcal{H}(4)$ is primitive iff it is reduced (Proposition 6.1).

Proposition 7.1. *Assume that $\mathcal{O}$ is primitive with $N = N(\mathcal{O}) \geqslant 7$. Then the monodromy group is equal to A_N if $N, H_1 + H_2 + H_3$ and $V_1 + V_2 + V_3$ have the same parity, and it is equal to S_N otherwise.*

Proof. Indeed, by the theorem of Zmiaikou mentioned earlier (cf. Proposition 6.2), the monodromy group is equal to A_N or S_N. The signature of a permutation of N elements with c cycles is $(-1)^{N-c}$. For the permutations generating the monodromy group, the number of cycles is $H_1 + H_2 + H_3$ in the horizontal direction, $V_1 + V_2 + V_3$ in the vertical direction. The assertion of the proposition is now clear. $\square$

The map $p_* : H_1(\mathcal{O}, \mathbb{Z}) \to H_1(\mathbb{T}^2, \mathbb{Z}) = \mathbb{Z}^2$ induced by the canonical covering $p : \mathcal{O} \to \mathbb{T}^2$ is given by

$$p_*(\sigma_i) = (\ell(Ch_i), 0), \quad p_*(\zeta_i) = (0, \ell(Cv_i)), \quad i = 1, 2, 3.$$

Define, for $i = 1, 2$

$$\Sigma_i := \ell(Ch_3)\sigma_i - \ell(Ch_i)\sigma_3, \quad Z_i = \ell(Cv_3)\zeta_i - \ell(Cv_i)\zeta_3.$$

Then $\Sigma_1, \Sigma_2, Z_1, Z_2$ are elements of $H_1^{(0)}(\mathcal{O}, \mathbb{Z})$ which span a subgroup of finite index of this group; they form a basis of $H_1^{(0)}(\mathcal{O}, \mathbb{Q})$.

7.2. **Two parabolic elements in Aff$(\mathcal{O})$.** Set

$$L_h := \ell(Ch_1)\ell(Ch_2)\ell(Ch_3), \quad P_h := \begin{pmatrix} 1 & L_h \\ 0 & 1 \end{pmatrix}.$$

The matrix P_h belongs to the Veech group $SL(\mathcal{O})$. Indeed, the associated element p_h of the affine group acts on homology according to $p_h.\sigma_i = \sigma_i$ and

$$p_h.\zeta_i = \zeta_i + \sum_{j=1}^{3} I_{ji} H_j \frac{L_h}{\ell(Ch_j)} \sigma_j, \quad i = 1, 2, 3.$$

We deduce from this formula the action on $H_1^{(0)}(\mathcal{O}, \mathbb{Q})$. We have $p_h.\Sigma_i = \Sigma_i$ for $i = 1, 2$ and

$$p_h.Z_i = Z_i + \sum_{j=1}^{3} H_{ij} H_j \frac{L_h}{\ell(Ch_j)} \sigma_j, \quad i = 1, 2.$$

with

$$H_{ij} := \ell(Cv_3)I_{ji} - \ell(Cv_i)I_{j3}.$$

The last formula can be rewritten as

$$p_h.Z_i = Z_i + \sum_{j=1}^{2} H_{ij}H_j\ell(Ch_{3-j})\Sigma_j, \quad i = 1, 2.$$

Substituting the values of I_{ji}, $\ell(Ch_j)$, $\ell(Cv_j)$, we get

$$H_{11} = H_{22} = H_3, \quad H_{12} = H_{21} = 0,$$

$$\begin{aligned} p_h.Z_1 &= Z_1 + H_1H_3V_2\Sigma_1, \\ p_h.Z_2 &= Z_2 + H_2H_3V_1\Sigma_2. \end{aligned}$$

Turning to the vertical direction, we set

$$L_v := \ell(Cv_1)\ell(Cv_2)\ell(Cv_3), \quad P_v := \begin{pmatrix} 1 & 0 \\ L_v & 1 \end{pmatrix}.$$

The matrix P_v belongs to the Veech group $SL(\mathcal{O})$. The associated element p_v of the affine group acts on homology according to $p_v.\zeta_i = \zeta_i$ and

$$p_h.\sigma_i = \sigma_i + \sum_{j=1}^{3} I_{ij}V_j\frac{L_v}{\ell(Cv_j)}\zeta_j, \quad i = 1, 2, 3.$$

For the action on $H_1^{(0)}(\mathcal{O}, \mathbb{Q})$, we have $p_v.Z_i = Z_i$ for $i = 1, 2$ and

$$\begin{aligned} p_v.\Sigma_i &= \Sigma_i + \sum_{j=1}^{3} V_{ij}V_j\frac{L_v}{\ell(Cv_j)}\zeta_j \\ &= \Sigma_i + \sum_{j=1}^{2} V_{ij}V_j\ell(Cv_{3-j})Z_j, \end{aligned}$$

with

$$V_{ij} := \ell(Ch_3)I_{ij} - \ell(Ch_i)I_{3j}.$$

Substituting the values of I_{ij}, $\ell(Ch_j)$, $\ell(Cv_j)$, we get

$$V_{11} = V_2 + V_3, \quad V_{22} = V_1 + V_3, \quad V_{12} = -V_1, \quad V_{21} = -V_2,$$

$$\begin{aligned} p_v.\Sigma_1 &= \Sigma_1 + V_1(V_2 + V_3)(H_2 + H_3)Z_1 - V_1V_2(H_1 + H_3)Z_2, \\ p_v.\Sigma_2 &= \Sigma_2 - V_1V_2(H_2 + H_3)Z_1 + V_2(V_1 + V_3)(H_1 + H_3)Z_2. \end{aligned}$$

We define the shorthand notation $H_{13} = H_1 + H_3$, $H_{23} = H_2 + H_3$ and

$$Q_h := \begin{pmatrix} H_1H_3V_2 & 0 \\ 0 & H_2H_3V_1 \end{pmatrix}, \quad Q_v := \begin{pmatrix} V_1(V_2 + V_3)H_{23} & -V_1V_2H_{23} \\ -V_1V_2H_{13} & V_2(V_1 + V_3)H_{13} \end{pmatrix},$$

so that the matrices of p_h, p_v in the basis $\Sigma_1, \Sigma_2, Z_1, Z_2$ are respectively

$$\begin{pmatrix} 1 & Q_h \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ Q_v & 1 \end{pmatrix}.$$

We will investigate whether $A := p_v \circ p_h$ is Galois-pinching.

7.3. Eigenvalues and eigenvectors for $Q_h.Q_v$, $Q_v.Q_h$ and A. A vector

$$w = x_1 \Sigma_1 + x_2 \Sigma_2 + y_1 Z_1 + y_2 Z_2$$

is eigenvector of A associated to the eigenvalue λ iff $x := (x_1, x_2), y := (y_1, y_2)$ satisfy

$$x = \frac{1}{\lambda - 1} Q_h.y, \quad y = \frac{\lambda}{\lambda - 1} Q_v.x.$$

Then, x and y are eigenvectors of $Q_h.Q_v$, $Q_v.Q_h$ respectively, associated to the same eigenvalue

(7.1) $$\mu := \lambda + \lambda^{-1} - 2.$$

Let

$$\begin{aligned}
d_h &:= \det Q_h = H_1 H_2 H_3^2 V_1 V_2 =: H_3^2 V_1 V_2 \bar{d}_h, \\
d_v &:= \det Q_v = V_1 V_2 V_3 (V_1 + V_2 + V_3)(H_1 + H_3)(H_2 + H_3) =: V_1 V_2 \bar{d}_v, \\
d &:= d_h d_v, \quad \bar{d} := \bar{d}_h \bar{d}_v, \\
t &:= \text{tr}(Q_h.Q_v) = \text{tr}(Q_v.Q_h) \\
&= V_1 V_2 H_3 [H_1 H_2 (V_1 + V_2 + 2V_3) + H_1 H_3 (V_2 + V_3) + H_2 H_3 (V_1 + V_3)] \\
&=: V_1 V_2 H_3 \bar{t}.
\end{aligned}$$

The eigenvalues of $Q_h.Q_v$ are the solutions of $\mu^2 - t\mu + d = 0$ with discriminant

$$\Delta_1 := t^2 - 4d = V_1^2 V_2^2 H_3^2 (\bar{t}^2 - 4\bar{d}_h \bar{d}_v).$$

Thus, we get

$$\begin{aligned}
\bar{\Delta}_1 &:= \bar{t}^2 - 4\bar{d}_h \bar{d}_v \\
&= [H_1 H_2 (V_1 + V_2 + 2V_3) + H_1 H_3 (V_2 + V_3) + H_2 H_3 (V_1 + V_3)]^2 \\
&\quad - 4 H_1 H_2 (H_1 + H_3)(H_2 + H_3) V_3 (V_1 + V_2 + V_3).
\end{aligned}$$

With Proposition 6.13 in mind, we also define

$$\Delta_2 := d(d + 4t + 16), \quad \bar{\Delta}_2 := \bar{d}(d + 4t + 16).$$

7.4. One-parameter subfamilies. Until now, the parameters H_i, V_j have only be constrained by the condition $\gcd(H_1, H_2, H_3) = \gcd(V_1, V_2, V_3) = 1$.

We now restrict our attention to nine one-parameter subfamilies which will provide enough origamis to prove Theorem 1.3. In each subfamily, the values of H_1, H_2, H_3, V_1, V_2 are fixed and V_3 runs along an arithmetic progression.

In each of the nine one-parameter subfamilies, one has $V_1 = 1$, $V_2 = 2$, $H_3 = 1$. The values of H_1, H_2 for the nine families are $H_1 = 1, 2 \leqslant H_2 \leqslant 4$ and $H_1 = 2, 3 \leqslant H_2 \leqslant 8$. Finally, we write $V_3 = 3n$ when $H_1 = 1$, $V_3 = 6n$ when $H_1 = 2$ and H_2 is even, $V_3 = 6n + 3$ when $H_1 = 2$ and H_2 is odd.

It is clear that each origami in these families is reduced hence primitive.

Proposition 7.2. *For each origami in these nine families, the direction* $(3,1)$ *is a 2-cylinder direction, and therefore has homological dimension* 2.

Proof. Index the separatrices in the direction $(3,1)$ in cyclical order by $\mathbb{Z}_{10}$ as indicated in figure 2 below.
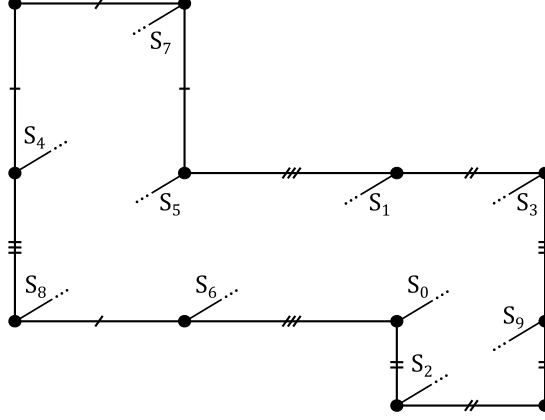
FIGURE 2. Separatrices in the direction $(3,1)$ of an origami in the odd component of $\mathcal{H}(4)$.

The saddle-connections in the $(3,1)$ direction join S_0 to S_5, S_6 to S_1, S_8 to S_3. By Proposition 6.5, it follows that $(3,1)$ is a 2-cylinder direction. $\square$

The number of squares is

$$N(\mathcal{O}) = 3 + H_1 + 2H_2 + V_3.$$

Next, we compute the monodromy group. We have

$$\begin{aligned} H_1 + H_2 + H_3 &= 1 + H_1 + H_2, \\ V_1 + V_2 + V_3 &= 3 + V_3, \end{aligned}$$

From Proposition 7.1, we obtain

Proposition 7.3. *The monodromy group of an origami in these subfamilies is the full symmetric group if* $H_1 = 1$, *the alternating group if* $H_1 = 2$.

Proof. When $H_1 = 1$, N and $V_1 + V_2 + V_3$ do not have the same parity. On the other hand, when $H_1 = 2$, H_2 and V_3 have the same parity, hence N, $H_1 + H_2 + H_3$ and $V_1 + V_2 + V_3$ have the same parity. $\square$

We plan to apply the elementary Galois theory of Subsection 6.7 in order to prove that, when n is large enough, the affine homeomorphism A constructed in subsection 7.2 is Galois-pinching. Specializing the formulas of the last subsection gives

$$\begin{aligned} d = 4\bar{d} &= 4H_1 H_2 (H_1 + 1)(H_2 + 1)V_3(V_3 + 3) \\ t = 2\bar{t} &= 2[V_3(2H_1 H_2 + H_1 + H_2) + 3H_1 H_2 + 2H_1 + H_2] \\ \Delta_1 = 4\bar{\Delta}_1 &= 4(\bar{t}^2 - 4\bar{d}) \\ \bar{\Delta}_1 &= [(H_2 - H_1)V_3 - (H_1 H_2 + 2H_1 - H_2)]^2 + \delta(H_1, H_2) \end{aligned}$$

with

$$\delta(H_1, H_2) = (3H_1 H_2 + 2H_1 + H_2)^2 - (H_1 H_2 + 2H_1 - H_2)^2 > 0.$$

We conclude that, for V_3 large enough, Δ_1 is not a square and the characteristic polynomial of A is irreducible (Lemma 6.10).

We also notice that, for all origamis in each of the nine one-parameter families, the quantities d, t, Δ_1 are positive, hence the eigenvalues of A are real and positive (Proposition 6.15).

Consider next

$$\Delta_2 = d(d + 4t + 16) = 16 \bar{d}(\bar{d} + 2\bar{t} + 4).$$

This is a polynomial of degree 4 in V_3 with integer coefficients. We will check that its reduced degree (see Subsection 6.7) is 4, which allows to apply Proposition 6.17. The roots of $\bar{d}$, as a polynomial in V_3, are 0 and -3. For $V_3 = 0$, one has

$$\bar{d} + 2\bar{t} + 4 = 2(3H_1 H_2 + 2H_1 + H_2) + 4 > 0.$$

For $V_3 = -3$, we have

$$\bar{d} + 2\bar{t} + 4 = 4 - 2(3H_1 H_2 + H_1 + 2H_2) < 0.$$

It remains to check that the degree two polynomial $\bar{d} + 2\bar{t} + 4 =: a_2 V_3^2 + a_1 V_3 + a_0$ has simple roots. Actually, for each of the nine subfamilies, the coefficients a_i are positive with $a_1 > 2 \max(a_2, a_0)$, hence the discriminant is positive. We conclude that the reduced degree of Δ_2 is equal to 4.

Finally, we claim that the reduced degree of the degree six polynomial $\Delta_1 \Delta_2$ is 6. Indeed the formula above for $\bar{\Delta}_1$ shows that it has no real roots, while we have seen that the roots of Δ_2 are real and simple. Applying Proposition 6.17, we get the following.

Proposition 7.4. *In each of the nine subfamilies, if V_3 is large enough, the affine homeomorphism A constructed in Subsection* 7.2 *is Galois-pinching.*

7.5. **Conclusion for the odd case.** We now have all the ingredients to prove Theorem 1.3 for origamis of odd type. Observe that for the origamis in the nine one-parameter subfamilies $V_1 \neq V_2$, hence they are not of Prym type. By Propositions 7.2 and 7.4, they satisfy for V_3 large enough the hypotheses of Corollary 1.2, hence their Lyapunov spectra are simple.

In the three subfamilies with $H_1 = 1$, the monodromy group is the full symmetric group (Proposition 7.3). The number of squares in this case is

$$N(\mathcal{O}) = 4 + 2H_2 + 3n$$

so the 3 choices for H_2 allow to get any large number of squares.

In the six subfamilies with $H_1 = 2$, the monodromy group is the alternating group (Proposition 7.3). The number of squares in this case is

$$
\begin{aligned}
N(\mathcal{O}) &= 5 + 2H_2 + 6n \quad \text{if } H_2 \text{ is even} \\
&= 8 + 2H_2 + 6n \quad \text{if } H_2 \text{ is odd}
\end{aligned}
$$

so the 6 choices for H_2 allow to get any large number of squares. The proof of Theorem 1.3 is complete in the odd case. $\qquad\square$
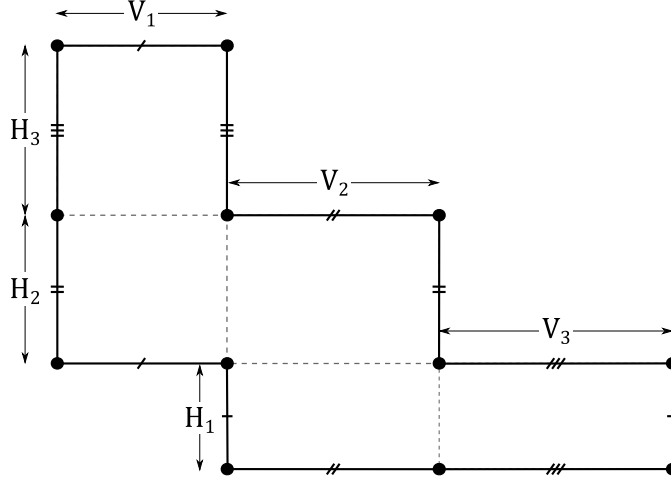
FIGURE 3. A origami in the hyperelliptic component of $\mathcal{H}(4)$.

8. THE HYPERELLIPTIC CASE

8.1. **A model for hyperelliptic origamis in** $\mathcal{H}(4)$**.** Consider the origami $\mathcal{O}$ constructed as indicated on Figure 3 below. It depends on 6 parameters $H_1, H_2, H_3, V_1, V_2, V_3$ which are positive integers.

In the horizontal direction, there are 3 cylinders Ch_1, Ch_2, Ch_3. The height of these cylinders are respectively H_1, H_2, H_3, while the length of the waist curves are respectively $\ell(Ch_1) = V_2 + V_3, \ell(Ch_2) = V_1 + V_2, \ell(Ch_3) = V_1$.

In the vertical direction, there are also 3 cylinders Cv_1, Cv_2, Cv_3. The height of these cylinders are respectively V_1, V_2, V_3, while the length of the waist curves are respectively $\ell(Cv_1) = H_2 + H_3, \ell(Cv_2) = H_1 + H_2, \ell(Cv_3) = H_1$.

We will denote by σ_i, $i = 1, 2, 3$, the homology class of the waist curve of Ch_i, oriented rightwards, and by ζ_i , $i = 1, 2, 3$, the homology class of the waist curve of Cv_i, oriented upwards. The symplectic intersection form ι on $H_1(\mathcal{O}, \mathbb{Z})$ satisfies

$$\iota(\sigma_i, \sigma_j) = \iota(\zeta_i, \zeta_j) = 0, \quad \iota(\sigma_i, \zeta_j) = I_{ij},$$

with

$$I = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

We review some elementary properties of $\mathcal{O}$:

- $\mathcal{O}$ has a single conical singularity of total angle 10π, so it belongs to $\mathcal{H}(4)$.
- The number of squares is

$$N(\mathcal{O}) = H_1(V_2 + V_3) + H_2(V_1 + V_2) + H_3V_1.$$

- $\mathcal{O}$ is reduced if and only if $\gcd(H_1, H_2, H_3) = \gcd(V_1, V_2, V_3) = 1$: indeed, the condition is clearly necessary. It is also sufficient because the vectors $(V_i, 0)$ and $(0, H_i)$ are periods for $i = 1, 2, 3$.
- The classes $\sigma_1, \sigma_2, \sigma_3, \zeta_1, \zeta_2, \zeta_3$ form a basis of the integral homology $H_1(\mathcal{O}, \mathbb{Z})$: indeed, the matrix I above is invertible over $\mathbb{Z}$.

- Proposition 7.1, determining the monodromy group of $\mathcal{O}$, is also valid in the hyperelliptic case, but will not be used.

The origami $\mathcal{O}$ admits an anti-automorphism with 8 fixed points, as indicated in Figure 4 below.
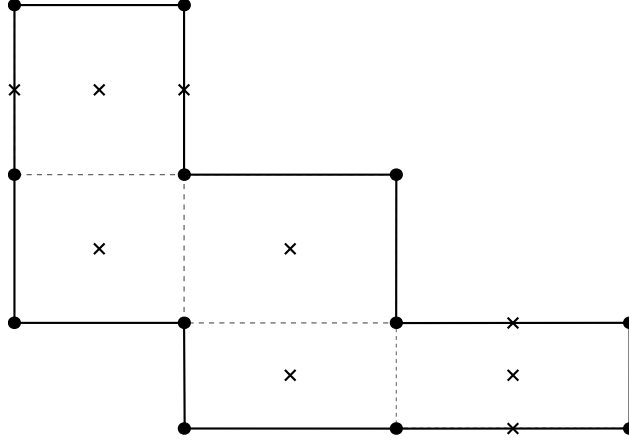
FIGURE 4. Fixed points of the anti-automorphism of a origami in the hyperelliptic component of $\mathcal{H}(4)$.

Therefore, it belongs to the hyperelliptic component of $\mathcal{H}(4)$. The anti-automorphism preserves each horizontal cylinder Ch_i and each vertical cylinder Cv_j. From Figure 4, we read off the Hubert-Lelièvre-Kani invariant of $\mathcal{O}$. It depends only on the classes in $\mathbb{Z}_2$ of the H_i and V_j. Writing these congruence classes as $\begin{pmatrix} \bar{H}_1 & \bar{H}_2 & \bar{H}_3 \\ \bar{V}_1 & \bar{V}_2 & \bar{V}_3 \end{pmatrix}$, the invariant is equal to

- $(4, [1, 1, 1])$ for $\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \end{smallmatrix}\right)$;

- $(2, [3, 1, 1])$ for $\left(\begin{smallmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \end{smallmatrix}\right)$;

- $(0, [5, 1, 1])$ for $\left(\begin{smallmatrix} 0 & 0 & 1 \\ 1 & 1 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{smallmatrix}\right)$;

- $(0, [3, 3, 1])$ for $\left(\begin{smallmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \end{smallmatrix}\right)$;

- $(3, [2, 2, 0])$ for $\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right)$;

- $(1, [4, 2, 0])$ for $\left(\begin{smallmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \end{smallmatrix}\right)$;

- $(1, [2, 2, 2])$ for $\left(\begin{smallmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \end{smallmatrix}\right)$.

The map $p_* : H_1(\mathcal{O}, \mathbb{Z}) \rightarrow H_1(\mathbb{T}^2, \mathbb{Z}) = \mathbb{Z}^2$ induced by the canonical covering $p :$ $\mathcal{O} \rightarrow \mathbb{T}^2$ is given by

$$p_*(\sigma_i) = (\ell(Ch_i), 0), \quad p_*(\zeta_i) = (0, \ell(Cv_i)), \quad i = 1, 2, 3.$$

Define , for $i = 1, 2$

$$\Sigma_i := \ell(Ch_3)\sigma_i - \ell(Ch_i)\sigma_3, \quad Z_i = \ell(Cv_3)\zeta_i - \ell(Cv_i)\zeta_3.$$

Then $\Sigma_1, \Sigma_2, Z_1, Z_2$ are elements of $H_1^{(0)}(\mathcal{O}, \mathbb{Z})$ which span a subgroup of finite index of this group; they form a basis of $H_1^{(0)}(\mathcal{O}, \mathbb{Q})$.

8.2. **Two parabolic elements in Aff$(\mathcal{O})$.** Set

$$L_h := \ell(Ch_1)\ell(Ch_2)\ell(Ch_3), \quad P_h := \begin{pmatrix} 1 & L_h \\ 0 & 1 \end{pmatrix}.$$

The matrix P_h belongs to the Veech group $SL(\mathcal{O})$. Indeed, the associated element p_h of the affine group acts on homology according to $p_h.\sigma_i = \sigma_i$ and

$$p_h.\zeta_i = \zeta_i + \sum_{j=1}^{3} I_{ji} H_j \frac{L_h}{\ell(Ch_j)} \sigma_j, \quad i = 1, 2, 3.$$

We deduce from this formula the action on $H_1^{(0)}(\mathcal{O}, \mathbb{Q})$. We have $p_h.\Sigma_i = \Sigma_i$ for $i = 1, 2$ and

$$p_h.Z_i = Z_i + \sum_{j=1}^{3} H_{ij} H_j \frac{L_h}{\ell(Ch_j)} \sigma_j, \quad i = 1, 2.$$

with

$$H_{ij} := \ell(Cv_3)I_{ji} - \ell(Cv_i)I_{j3}.$$

The last formula can be rewritten as

$$p_h.Z_i = Z_i + \sum_{j=1}^{2} H_{ij} H_j \ell(Ch_{3-j}) \Sigma_j, \quad i = 1, 2.$$

Up to now, the formulas were the same as in the odd case. Substituting the values of $I_{ji}, \ell(Ch_j), \ell(Cv_j)$, we get in the new setting

$$H_{12} = H_{22} = H_1, \quad H_{11} = -(H_2 + H_3), \quad H_{21} = -H_2,$$

$$\begin{aligned} p_h.Z_1 &= Z_1 - H_1(H_2 + H_3)(V_1 + V_2)\Sigma_1 + H_1 H_2(V_2 + V_3)\Sigma_2, \\ p_h.Z_2 &= Z_2 - H_1 H_2(V_1 + V_2)\Sigma_1 + H_1 H_2(V_2 + V_3)\Sigma_2. \end{aligned}$$

In the hyperelliptic model under consideration, the horizontal and the vertical direction play the same role. We define

$$L_v := \ell(Cv_1)\ell(Cv_2)\ell(Cv_3), \quad P_v := \begin{pmatrix} 1 & 0 \\ L_v & 1 \end{pmatrix}.$$

The matrix P_v belongs to the Veech group $SL(\mathcal{O})$. The associated element p_v of the affine group acts on $H_1^{(0)}$ accordind to $p_v.Z_i = Z_i$ and

$$
\begin{aligned}
p_v.\Sigma_1 &= \Sigma_1 - V_1(V_2 + V_3)(H_1 + H_2)Z_1 + V_1V_2(H_2 + H_3)Z_2, \\
p_v.\Sigma_2 &= \Sigma_2 - V_1V_2(H_1 + H_2)Z_1 + V_1V_2(H_2 + H_3)Z_2.
\end{aligned}
$$

We define

$$
\begin{aligned}
Q_h &:= \begin{pmatrix} -H_1(H_2 + H_3)(V_1 + V_2) & -H_1H_2(V_1 + V_2) \\ H_1H_2(V_2 + V_3) & H_1H_2(V_2 + V_3) \end{pmatrix}, \\
Q_v &:= \begin{pmatrix} -V_1(V_2 + V_3)(H_1 + H_2) & -V_1V_2(H_1 + H_2) \\ V_1V_2(H_2 + H_3) & V_1V_2(H_2 + H_3) \end{pmatrix},
\end{aligned}
$$

so that the matrices of p_h, p_v in the basis $\Sigma_1, \Sigma_2, Z_1, Z_2$ are respectively

$$
\begin{pmatrix} 1 & Q_h \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ Q_v & 1 \end{pmatrix}.
$$

We will investigate whether $A := p_v \circ p_h$ is Galois-pinching.

8.3. **Eigenvalues and eigenvectors for $Q_h.Q_v, Q_v.Q_h$ and A.** A vector

$$
w = x_1\Sigma_1 + x_2\Sigma_2 + y_1Z_1 + y_2Z_2
$$

is eigenvector of A associated to the eigenvalue λ iff $x := (x_1, x_2), y := (y_1, y_2)$ satisfy

$$
x = \frac{1}{\lambda - 1}Q_h.y, \quad y = \frac{\lambda}{\lambda - 1}Q_v.x.
$$

Then, x and y are eigenvectors of $Q_h.Q_v, Q_v.Q_h$ respectively, associated to the same eigenvalue

(8.1) $$ \mu := \lambda + \lambda^{-1} - 2. $$

Let

$$
\begin{aligned}
d_h &:= \det Q_h = -H_1^2H_2H_3(V_1 + V_2)(V_2 + V_3) =: H_1^2\bar{d}_h, \\
d_v &:= \det Q_v = -V_1^2V_2V_3(H_1 + H_2)(H_2 + H_3) =: V_1^2\bar{d}_v, \\
d &:= d_hd_v, \quad \bar{d} := \bar{d}_h\bar{d}_v, \\
t &:= \operatorname{tr}(Q_h.Q_v) = \operatorname{tr}(Q_v.Q_h) \\
&= H_1V_1[H_2^2V_3(V_1 + V_2) + H_1H_2V_1(V_2 + V_3) + H_1H_3(V_1 + V_2)(V_2 + V_3) \\
&\quad + H_2H_3(V_2^2 + V_1V_3 + 2V_2V_3)] \\
&=: H_1V_1\bar{t}.
\end{aligned}
$$

The eigenvalues of $Q_h.Q_v$ are the solutions of $\mu^2 - t\mu + d = 0$ with discriminant

$$
\Delta_1 := t^2 - 4d = H_1^2V_1^2(\bar{t}^2 - 4\bar{d}_h\bar{d}_v).
$$

Thus, we get

$$
\begin{aligned}
\bar{\Delta}_1 &:= \bar{t}^2 - 4\bar{d}_h\bar{d}_v \\
&= [H_2^2V_3(V_1 + V_2) + H_1H_2V_1(V_2 + V_3) + H_1H_3(V_1 + V_2)(V_2 + V_3) \\
&\quad + H_2H_3(V_2^2 + V_1V_3 + 2V_2V_3)]^2 \\
&\quad - 4H_2H_3(H_1 + H_2)(H_2 + H_3)V_2V_3(V_1 + V_2)(V_2 + V_3).
\end{aligned}
$$

With Proposition 6.13 in mind, we also define

$$\Delta_2 := d(d + 4t + 16), \quad \bar{\Delta}_2 := \bar{d}(d + 4t + 16).$$

8.4. **One-parameter subfamilies.** As in the odd case, we now restrict our attention to a finite number of one-parameter subfamilies. In each subfamily, we fix the values of H_2, H_3, V_1, V_2, V_3 , while H_1 runs along an arithmetic progression.

In all subfamilies, one has $V_1 = H_2 = 1$. The others parameters are as follows

- In the first four subfamilies, one has $V_2 = V_3 = 1$, $1 \leqslant H_3 \leqslant 4$, $H_1 = 2n$. The number of squares is $4n + 2 + H_3$.
- In the next eighteen subfamilies, one has $V_2 = 1, V_3 = 2, 1 \leqslant H_3 \leqslant 18, H_1 = 6n$. The number of squares is $18n + 2 + H_3$.
- Next, we take $V_2 = 2, V_3 = 1, H_3 \in \{1, 3, 5\}, H_1 = 2n$. The number of squares is $6n + 3 + H_3$.
- Then, we take $V_2 = V_3 = 2, 2 \leqslant H_3 \leqslant 16, H_3$ even, $H_1 = 4n$. The number of squares is $16n + 3 + H_3$.
- Finally, we take $V_2 = 3, V_3 = 1, 1 \leqslant H_3 \leqslant 15, H_3$ odd, $H_1 = 4n + 3$. The number of squares is $16n + 16 + H_3$.

These 41 families are divided into 5 groups distinguished by their values of V_2, V_3. As $V_1 = H_2 = 1$, all origamis in these families are reduced, hence primitive.

Proposition 8.1. *For each origami in these families, the direction $(1,1)$ is a 2-cylinder direction, and therefore has homological dimension 2.*

Proof. We label the separatrices in the direction $(1,1)$ in cyclic order by $\mathbb{Z}_{10}$ as indicated in Figure 5.
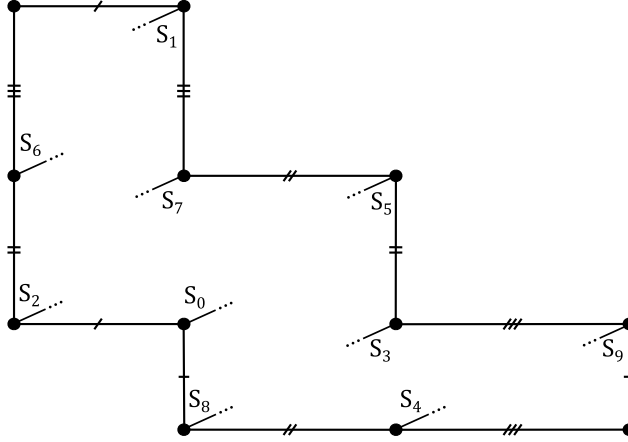
FIGURE 5. Separatrices in the direction $(1,1)$ of a origami in the hyperelliptic component of $\mathcal{H}(4)$.

We check in each case that there are exactly 3 balanced saddle connections, which correspond to the 2-cylinder case according to Proposition 6.5. Actually, the saddle connections from S_6 to S_1 and S_2 to S_7 are always there, hence it is sufficient to see that not all saddle connections are balanced. The separatrix S_8 is connected to S_9 in the first two groups and also in the fourth. The separatrix S_4 is connected to S_5 in the last group. Finally, in the

third group, there is a connection between S_8 and S_9 if $H_3 = 6n$, between S_0 and S_9 if $H_3 = 6n + 2$, and between S_8 and S_5 if $H_3 = 6n + 4$. $\qquad\square$

Next, we compute the HLK-invariant of the origamis in these families. We deduce from Subsection 8.1 the HLK-invariant of the families under consideration.

Proposition 8.2. *The HLK-invariant of the origamis in the families under consideration is equal to*

- $(0, [3, 3, 1])$ *for the families in the first group with H_3 odd;*
- $(1, [4, 2, 0])$ *for the families in the first group with H_3 even;*
- $(2, [3, 1, 1])$ *for the families in the second group with H_3 odd;*
- $(3, [2, 2, 0])$ *for the families in the second group with H_3 even;*
- $(1, [2, 2, 2])$ *for the families in the third group;*
- $(4, [1, 1, 1])$ *for the families in the fourth group;*
- $(0, [5, 1, 1])$ *for the families in the last group.*

As in the odd case, we plan to apply the elementary Galois theory of Subsection 6.7 in order to prove that, when n is large enough, the affine homeomorphism A constructed in Subsection 8.2 is Galois-pinching. Specializing the formulas of the last subsection gives

$$
\begin{aligned}
d &= H_1^2 \bar{d}, \quad t = H_1 \bar{t}, \quad \Delta_1 = H_1^2 \bar{\Delta}_1, \quad \Delta_2 = H_1^2 \bar{\Delta}_2, \\
\bar{d} &= V_2 V_3 (1 + V_2)(V_2 + V_3) H_3 (1 + H_3)(1 + H_1), \\
\bar{t} &= H_1 (V_2 + V_3)[1 + H_3(1 + V_2)] + V_3(1 + V_2) + H_3(V_2^2 + 2V_2 V_3 + V_3), \\
\bar{\Delta}_1 &= \bar{t}^2 - 4\bar{d}, \\
\bar{\Delta}_2 &= \bar{d}(H_1^2 \bar{d} + 4 H_1 \bar{t} + 16).
\end{aligned}
$$

Observe that d, t are always positive and Δ_1 is positive if H_1 is large enough. By Proposition 6.15 the eigenvalues of A acting on $H_1^{(0)}$ are real and positive for the origamis in these families if H_1 is large enough.

We now write $\bar{d}, \bar{t}, \bar{\Delta}_1$ more explicitly in each of the five groups of families:

- In the first group, we have $V_2 = V_3 = 1$ and

$$
\begin{aligned}
\bar{d} &= 4H_3(1 + H_3)(H_1 + 1), \\
\bar{t} &= (2 + 4H_3)(H_1 + 1), \\
\bar{\Delta}_1 &= 4(H_1 + 1)[(1 + 2H_3)^2 H_1 + 1].
\end{aligned}
$$

- In the third group, we have $V_2 = 2$, $V_3 = 1$ and

$$
\begin{aligned}
\bar{d} &= 18H_3(1 + H_3)(H_1 + 1), \\
\bar{t} &= (3 + 9H_3)(H_1 + 1), \\
\bar{\Delta}_1 &= 9(H_1 + 1)[(1 + 3H_3)^2 H_1 + (H_3 - 1)^2].
\end{aligned}
$$

- In the last group, we have $V_2 = 3$, $V_3 = 1$ and

$$
\begin{aligned}
\bar{d} &= 48H_3(1 + H_3)(H_1 + 1), \\
\bar{t} &= (4 + 16H_3)(H_1 + 1), \\
\bar{\Delta}_1 &= 16(H_1 + 1)[(1 + 4H_3)^2 H_1 + (2H_3 - 1)^2].
\end{aligned}
$$

- In the second group, we have $V_2 = 1$, $V_3 = 2$ and

$$
\begin{aligned}
\bar{d} &= 12H_3(1 + H_3)(H_1 + 1), \\
\bar{t} &= (3 + 6H_3)H_1 + 4 + 7H_3, \\
\bar{\Delta}_1 &= (3 + 6H_3)^2 H_1^2 + (36H_3^2 + 42H_3 + 24)H_1 + (H_3 + 4)^2.
\end{aligned}
$$

- In the fourth group, we have $V_2 = 2$, $V_3 = 2$ and

$$
\begin{aligned}
\bar{d} &= 48H_3(1 + H_3)(H_1 + 1), \\
\bar{t} &= (4 + 12H_3)H_1 + 6 + 14H_3, \\
\bar{\Delta}_1 &= (4 + 12H_3)^2 H_1^2 + (144H_3^2 + 64H_3 + 48)H_1 + (2H_3 - 6)^2.
\end{aligned}
$$

Proposition 8.3. *In each of the 41 families considered above, the quantity $\bar{\Delta}_1$ is not a square if H_1 is large enough.*

Proof. For each family, $\bar{\Delta}_1$ is a degree two polynomial in H_1 with integer coefficients. Moreover, the leading coefficient is always a square. The only way that the values of such a polynomial may be squares for infinitely many integers H_1 is that this polynomial is itself a square.

This is obviously not the case for families in the first, third or last group (recall that $H_3 > 0$). For families in the second group, we compute the discriminant of this degree two polynomial to be equal to $(24)^2 H_3(2H_3 - 1)(H_3 + 1)^2 \neq 0$. For families in the fourth group, we compute the discriminant to be equal to $6(32)^2 H_3(3H_3 - 1)(H_3 + 1)^2 \neq 0$. □

Lemma 8.4. *For each of the 41 families considered above, the third degree polynomial $H_1^2 \bar{d} + 4H_1 \bar{t} + 16$ is irreducible, except for the family in the first group with $H_3 = 2$, where it is equal to $8(H_1 + 2)(3H_1^2 + 2H_1 + 1)$, and the family in the second group with $H_3 = 3$, where it is equal to $4(H_1 + 1)(36H_1^2 + 21H_1 + 4)$.*

This is checked using any standard mathematical software, e.g. *Mathematica*.

Proposition 8.5.   (1) *For each family such that $H_1^2 \bar{d} + 4H_1 \bar{t} + 16$ is irreducible, the reduced degrees of Δ_2 and $\bar{\Delta}_2$, as a polynomials in H_1, are equal to 4. The reduced degrees of $\Delta_1 \Delta_2$ and $\bar{\Delta}_1 \bar{\Delta}_2$ are equal to 4 for families in the first, third and last group, and equal to 6 for families in the second and fourth group.*
   (2) *For the family in the first group with $H_3 = 2$, the reduced degrees of $\Delta_2, \bar{\Delta}_2$, $\Delta_1 \Delta_2$ and $\bar{\Delta}_1 \bar{\Delta}_2$ are equal to 4.*
   (3) *For the family in the second group with $H_3 = 3$, the reduced degrees of $\Delta_1 \Delta_2$ and $\bar{\Delta}_1 \bar{\Delta}_2$ are equal to 4. The reduced degrees of Δ_2 and $\bar{\Delta}_2$ are equal to 2 but these quantities are not squares for H_1 large enough.*

Proof.   (1) With $c = V_2 V_3(1 + V_2)(V_2 + V_3)H_3(1 + H_3)$, one has

$$
\bar{\Delta}_2 = c(H_1 + 1)(H_1^2 \bar{d} + 4H_1 \bar{t} + 16).
$$

As $H_1^2 \bar{d} + 4H_1 \bar{t} + 16$ is irreducible, it has no double root and does not vanish for $H_1 = -1$. Therefore the reduced degree of $\bar{\Delta}_2$ is equal to 4. The roots of $\bar{\Delta}_1$ are either rational or quadratic, hence cannot be roots of $H_1^2 \bar{d} + 4H_1 \bar{t} + 16$. For families in the first, third or last group $H_1 = -1$ is both a root of $\bar{d}$ and $\bar{t}$. This is not the case for families in the second or fourth group. As we have already seen that $\bar{\Delta}_1$ does not have double roots, we obtain the assertion on the reduced degree of $\bar{\Delta}_1 \bar{\Delta}_2$.

(2) In this case, one has

$$\begin{aligned} \bar{\Delta}_1 &= 4(H_1 + 1)(25H_1 + 1) \\ \bar{\Delta}_2 &= 192(H_1 + 1)(H_1 + 2)(3H_1^2 + 2H_1 + 1), \end{aligned}$$

which implies the assertion of the proposition.

(3) In this case, one has

$$\begin{aligned} \bar{\Delta}_1 &= 21^2 H_1^2 + 474H_1 + 7^2 \\ \bar{\Delta}_2 &= 24^2(H_1 + 1)^2(36H_1^2 + 21H_1 + 4), \end{aligned}$$

which implies the assertion on the reduced degrees. Also, as 36 is a square but the discriminant of $36H_1^2 + 21H_1 + 4$ does not vanish, $\bar{\Delta}_2$ is not a square when H_1 is large enough.

□

Applying the results of Subsection 6.7, we obtain the desired result.

Corollary 8.6. *In each of the 41 subfamilies, if H_1 is large enough, the affine homeomorphism A constructed in Subsection 8.2 is Galois-pinching.*

8.5. **Conclusion for the hyperelliptic case.**

We now have all the elements to prove Theorem 1.3 for origamis of hyperelliptic type. By Propositions 8.1 and 8.6, they satisfy for H_1 large enough the hypotheses of Corollary 1.2, hence their Lyapunov spectra are simple.

From proposition 8.2, families in the first group provide origamis with HLK-invariant equal to $(0, [3, 3, 1])$ or $(1, [4, 2, 0])$. The number of squares is $N = 4n + 2 + H_3$, with $1 \leqslant H_3 \leqslant 4$, hence any large number of squares is realizable by some family in the first group. Proposition 8.2 allows to deal similarly with the other values of the HLK-invariant. The proof of Theorem 1.3 is complete in the hyperelliptic case. □

APPENDIX A. A VERSION OF AVILA-VIANA SIMPLICITY CRITERION

In this appendix we will present a streamlined proof of Theorem 2.13. Here, we will use notations and definitions introduced in Subsection 2.5 without further comments.

We begin by noticing that one may consider the cocycle A over the invertible dynamics $\hat{f} : \hat{\Sigma} \to \hat{\Sigma}$ because the Lyapunov spectrum is not affected by this procedure.

A crucial fact from (bi)linear algebra allows to adapt the proof for $\mathbb{G} = GL(d, \mathbb{R})$ to other matrix groups $\mathbb{G}$ (symplectic or unitary). Let k be an admissible integer, $A \in \mathbb{G}$; denote by $\sigma_1(A) \geqslant \ldots \geqslant \sigma_d(A)$ the singular values of A, i.e the lengths of the semi-major axes of the ellipsoid $A(\{v : \|v\| = 1\})^{[10]}$. Then, the subspace ξ_A spanned by the k largest semi-major axes belongs to $G(k)^{[11]}$. This fact is a simple consequence of the polar decomposition of matrices in $\mathbb{G}$.

In the statement below, we use the following notations:

- $\underline{\ell}(x, n)$ is the terminal word of $x \in \Sigma_-$ of length n;
- For $\underline{\ell} \in \Omega$, we write $\xi_{\underline{\ell}}$ for $\xi_{A\underline{\ell}}$.

The main result towards the proof of Theorem 2.13 above is:

---

[10]As for Lyapunov exponents, singular values are counted with essential multiplicity, see Remark 2.10.

[11]This subspace is uniquely defined only when $\sigma_k(A) > \sigma_{k+1}(A)$. When $\sigma_k(A) = \sigma_{k+1}(A)$, what is meant is that it is possible to select the k largest semi-major axes in order that the subspace spanned by them belongs to $G(k)$.

Theorem A.1 (A. Avila and M. Viana)**.** *For every admissible integer k, there exists a map* $\Sigma_- \to G(k)$, $x \mapsto \xi(x)$ *verifying the properties:*

- Invariance*: the map $\hat{\xi} = \xi \circ p^-$ satisfies $A(x)\hat{\xi}(x) = \hat{\xi}(\hat{f}(x))$;*
- *for μ_--almost every $x \in \Sigma_-$, $\frac{\sigma_k(A^{\ell(x,n)})}{\sigma_{k+1}(A^{\ell(x,n)})} \to +\infty$ and $\xi_{\underline{\ell}(x,n)} \to \xi(x)$ as $n \to +\infty$;*
- *for all $F' \in G(d-k)$, we have $\xi(x) \cap F' = \{0\}$ for a set of positive μ_--measure.*

This result corresponds to [AV, Theorem A.1]. As the reader can check (see Subsection A.6 "Proof of Theorem 7.1" of [AV]), it is not hard to deduce Theorem 2.13 from Theorem A.1.

Sketch of proof of Theorem 2.13 *assuming Theorem* A.1. For each admissible integer k and each $x \in \Sigma_-$, Theorem A.1 provides us, with a subspace $\xi(x) \in G(k)$ verifying the properties above. By using the same theorem with the time "reversed", one gets for $y \in \Sigma_+$ a subspace $\xi_*(y) \in G(d-k)$ verifying similar properties. From the third property in the theorem, one deduces the transversality property $\xi(x) \cap \xi_*(y) = \{0\}$ for almost every $(x,y) \in \hat{\Sigma}$. The second property in the theorem implies that $\xi(x)$ is associated with the k largest exponents and $\xi_*(y)$ is associated with the $d-k$ smallest exponents. Then the transversality property permits to show that, for any admissible integer k, the kth Lyapunov exponent is strictly larger than the $(k+1)$th exponent . This shows that the Lyapunov spectrum of A is simple in the sense defined in Subsection 2.5. □

This reduces our considerations to the discussion of Theorem A.1. Let k be an admissible integer. We denote by p', p'' the natural projections from $\hat{\Sigma} \times G(k)$ onto $\hat{\Sigma}$ and $G(k)$ respectively.

Definition A.2. A *u-state* is a probability measure $\hat{m}$ on $\hat{\Sigma} \times G(k)$ such that $p'_*(\hat{m}) = \hat{\mu}$ and there exists a constant $C(\hat{m})$ with

$$\frac{\hat{m}(\Sigma_-(\underline{\ell}^0) \times \Sigma(\underline{\ell}) \times X)}{\mu(\Sigma(\underline{\ell}))} \leqslant C(\hat{m})\frac{\hat{m}(\Sigma_-(\underline{\ell}^0) \times \Sigma(\underline{\ell}') \times X)}{\mu(\Sigma(\underline{\ell}'))}$$

for any Borelian $X \subset G(k)$, $\underline{\ell}^0, \underline{\ell}, \underline{\ell}' \in \Omega$.

Roughly speaking, the previous condition says that u-states are almost product measures.

Example A.3. Given any probability measure ν on $G(k)$, $\hat{m} := \hat{\mu} \times \nu$ is a u-state with $C(\hat{m}) = C(\mu)^2$, where $C(\mu)$ is the constant appearing in the bounded distortion property (see Definition 2.6).

Proposition A.4. *There exists a u-state invariant under $(\hat{f}, A)$.*

Proof. The argument is very classical and we will only sketch its main steps. Even though the space $\hat{\Sigma}$ may not be compact (in the case of an alphabet Λ with countably many symbols), the space of probability measures on $\hat{\Sigma} \times G(k)$ projecting to $\hat{\mu}$ is compact in the weak-* topology. In particular, for each $C > 0$, it follows that the space of u-states $\hat{m}$ with $C(\hat{\mu}) \leqslant C$ is a convex compact set.

A short direct computation ([AV, Lemma A.2]) shows that, for any u-state $\hat{m}_0$ and any $n > 0$, $\hat{m}(n) := (\hat{f}, A)^n_* \hat{m}_0$ is a u-state with $C(\hat{m}(n)) \leqslant C(\hat{m})C(\mu)^2$. Then the standard Krylov-Bogolyubov argument completes the proof: any accumulation point of the Cesaro averages of $\hat{m}(n)$ is a u-state invariant under $(\hat{f}, A)$. □

The following result is a simple application of the martingale convergence theorem (see [AV, Lemma A.4] for a short proof). We recall that $\underline{\ell}(x, n)$ denotes the terminal word of $x \in \Sigma_-$ of length n.

Proposition A.5. *Let $\hat{m}$ be a probability measure on $\hat{\Sigma} \times G(k)$ with $p'_* \hat{m} = \hat{\mu}$. For any $x \in \Sigma_-$, and any Borelian subset $X \subset G(k)$, let*

$$\hat{m}_n(x)(X) := \frac{\hat{m}(\Sigma_-(\underline{\ell}(x, n)) \times \Sigma \times X)}{\hat{m}(\Sigma_-(\underline{\ell}(x, n)) \times \Sigma \times G(k))}$$

Then, for μ_--almost every $x \in \Sigma_-$, $\hat{m}_n(x)$ converges in the weak topology to some $\hat{m}(x)$.*

Let $\hat{m}$ be a $(\hat{f}, A)$-invariant u-state given by Proposition A.4. Define $\hat{m}_n(x)$ as in Proposition A.5. Let also $\nu = p''_* \hat{m}$. For any $x \in \Sigma_-$, define a sequence of probability measures on $G(k)$ by

$$\nu_n(x) := A_*^{\underline{\ell}(x, n)} \nu.$$

Let X be a Borelian subset of $G(k)$. As $\hat{m}$ is $(\hat{f}, A)$-invariant , we have

$$\hat{m}_n(x)(X) = \frac{\hat{m}(\Sigma_-(\underline{\ell}(x, n)) \times \Sigma \times X)}{\hat{m}(\Sigma_-(\underline{\ell}(x, n)) \times \Sigma \times G(k))} = \frac{\hat{m}(\Sigma_- \times \Sigma(\underline{\ell}(x, n)) \times A^{-\underline{\ell}(x, n)}(X))}{\hat{m}(\Sigma_- \times \Sigma(\underline{\ell}(x, n)) \times G(k))}$$

On the other hand, by definition, we have

$$\nu_n(x)(X) = \nu(A^{-\underline{\ell}(x, n)}(X)) = \hat{m}(\hat{\Sigma} \times A^{-\underline{\ell}(x, n)}(X)).$$

Since $\hat{m}$ is a u-state, we obtain

$$C(\hat{m})^{-2} \leqslant \hat{m}_n(x)(X)/\nu_n(x)(X) \leqslant C(\hat{m})^2.$$

In particular,

Corollary A.6. *For μ_--almost every $x \in \Sigma_-$, the probability measure $\hat{m}(x) = \lim \hat{m}_n(x)$ is equivalent to any accumulation point of the sequence $\nu_n(x)$.*

The crucial step in the proof of Theorem A.1 is given by the

Proposition A.7. *For μ_--almost every $x \in \Sigma_-$, there exists a subsequence $\nu_{n_k}(x)$, $n_k = n_k(x) \to \infty$, converging to a Dirac mass.*

Sketch of proof of Theorem A.1 *assuming Proposition* A.7. (see end of Subsection A.4 of [AV]). By Corollary A.6 and Proposition A.7, $\hat{m}(x)$ is a Dirac mass $\delta_{\xi(x)}$ for μ_--almost every $x \in \Sigma_-$.

Then $x \mapsto \xi(x)$ has the desired properties: the invariance property (first item of Theorem A.1) follows from the $(\hat{f}, A)$-invariance of $\hat{m}$; the other two items are a consequence of the the pinching and twisting assumptions on the cocycle A. $\qquad\square$

Proof of Proposition A.7. Let $\underline{\ell}^* \in \Omega$ be a word such that the matrix $A^{\underline{\ell}^*}$ is pinching. As there are only finitely many $A^{\underline{\ell}^*}$-invariant subspaces in $G(k)$ (see Remark 2.15), one can use the twisting hypothesis to choose $\underline{\ell}^0 \in \Omega$ such that, for each admissible integer k and for every pair of $A^{\underline{\ell}^*}$-invariant subspaces $F \in G(k), F' \in G(d - k)$, one has $A^{\underline{\ell}^0}(F) \cap F' = \{0\}$.

We claim that there exists $m \geqslant 1$, $\underline{\ell}_1, \ldots, \underline{\ell}_m \in \Omega$ and $\delta > 0$ such that, for each admissible integer k and for every $F' \in G(d - k)$, there exists $\underline{\ell}_i$ with $A^{\underline{\ell}_i}(F_+(A^{\underline{\ell}^*})) \cap F' = \{0\}$ and the angle between $A^{\underline{\ell}_i}(F_+(A^{\underline{\ell}^*}))$ and F' is $\geqslant \delta$. Here, $F_+(A^{\underline{\ell}^*})$ is the subspace associated to k largest exponents of $A^{\underline{\ell}^*}$. Indeed, it is sufficient to prove this for a given admissible integer k, in which case it follows from the twisting assumption and the compactness of $G(d - k)$.

Lemma A.8 (Lemma A.6 of [AV])**.** *Let $\varepsilon > 0$ and ρ a probability measure on $G(k)$. There exists $n_0 = n_0(\rho, \varepsilon)$ and, for each $\widetilde{\underline{\ell}} \in \Omega$, there exists $i = i(\widetilde{\underline{\ell}}) \in \{1, \dots, m\}$ such that, for $n \geqslant n_0$, we have*

$$A^{\underline{\ell}}_*(\rho)(B) > 1 - \varepsilon$$

where $\underline{\ell} := (\underline{\ell}^*)^n \underline{\ell}^0 (\underline{\ell}^*)^n \underline{\ell}_i \widetilde{\underline{\ell}}$ and B is the ball of radius $\varepsilon > 0$ centered at $\xi_{\underline{\ell}}$.

This lemma is harder to state than to explain: geometrically, it says that, although the word $\widetilde{\underline{\ell}}$ may be very long, we can choose an appropriate "start" $((\underline{\ell}^*)^n \underline{\ell}^0 (\underline{\ell}^*)^n \underline{\ell}_i)$ so that the word $\underline{\ell}$ obtained by the concatenation of $(\underline{\ell}^*)^n \underline{\ell}^0 (\underline{\ell}^*)^n \underline{\ell}_i$ and $\widetilde{\underline{\ell}}$ has the property that $A^{\underline{\ell}}$ concentrates most of the mass of any probability measure ρ on $G(k)$ (given in advance) in a tiny ball B.

We defer the proof of the lemma to the end of the appendix and first end the proof of Proposition A.7. The details are slightly different from [AV].

We will apply Lemma A.8 with $\rho = \nu$. As $\nu_n(x) := A^{\underline{\ell}(x,n)}_* \nu$, the conclusion of the lemma will imply the conclusion of Proposition A.7 if we can show that, for any $n \geqslant 0$ and μ_--almost every x, there are infinitely many integers N such that $(\underline{\ell}^*)^n \underline{\ell}^0 (\underline{\ell}^*)^n \underline{\ell}_i \underline{\ell}(x, N)$, with $i = i(\underline{\ell}(x, N))$, is a terminal word of x.

Assume that this is not true. Then there exist integers n, N_0 and a positive measure set $E \subset \Sigma_-$ such that, for any $x \in E$, $N \geqslant N_0$, the word $(\underline{\ell}^*)^n \underline{\ell}^0 (\underline{\ell}^*)^n \underline{\ell}_i \underline{\ell}(x, N)$, with $i = i(\underline{\ell}(x, N))$, is not a terminal word of x.

By the bounded distortion property, there exists $c > 0$ such that

(A.1) $$\mu_-(\Sigma_-((\underline{\ell}^*)^n \underline{\ell}^0 (\underline{\ell}^*)^n \underline{\ell}_i \widetilde{\underline{\ell}})) \geqslant c\mu_-(\Sigma_-(\widetilde{\underline{\ell}}))$$

for every $1 \leqslant i \leqslant m$ and $\widetilde{\underline{\ell}} \in \Omega$.

Let x_0 be a density point of E. There exists $N \geqslant N_0$ such that

$$\mu_-(\Sigma_-(\underline{\ell}(x_0, N)) \cap E^c) < \frac{c}{2} \mu_-(\Sigma_-(\underline{\ell}(x_0, N))),$$

where E^c is the complement of E.

Taking $\widetilde{\underline{\ell}} = \underline{\ell}(x_0, N)$, $i = i(\widetilde{\underline{\ell}})$ in (A.1) above, we find a point in E with terminal word $(\underline{\ell}^*)^n \underline{\ell}^0 (\underline{\ell}^*)^n \underline{\ell}_i \underline{\ell}(x_0, N)$. This contradiction to the definition of E proves the claim and ends the proof of Proposition A.7. $\qquad\square$

Proof of Lemma A.8. An elementary calculation shows that, as $A^{\underline{\ell}^*}$ is pinching, the sequence $(A^{\underline{\ell}^*})^n(\xi)$ converges for every $\xi \in G(k)$. The limit is one of the finitely many $A^{\underline{\ell}^*}$-invariant subspaces in $G(k)$. Moreover, the limit is the subspace $F_+(A^{\underline{\ell}^*})$ associated to the k largest exponents whenever ξ is transverse to every $A^{\underline{\ell}^*}$-invariant subspace in $G(d - k)$.

For any probability measure on $G(k)$, the sequence $(A^{\underline{\ell}^*})^n_*(\rho)$ converges, as n goes to $+\infty$, to a limit which is a convex combination of Dirac masses at the $A^{\underline{\ell}^*}$-invariant subspaces in $G(k)$. By definition of $\underline{\ell}^0$, the images under $A^{\underline{\ell}^0}$ of these invariant subspaces are transverse to every $A^{\underline{\ell}^*}$-invariant subspace in $G(d - k)$. We conclude that $(A^{\underline{\ell}^*})^n_*(A^{\underline{\ell}^0})_*(A^{\underline{\ell}^*})^n_*(\rho)$ converges to the Dirac mass at $F_+(A^{\underline{\ell}^*})$.

Let $\widetilde{\underline{\ell}} \in \Omega$ be given. Denote by $\xi^*_{\widetilde{\underline{\ell}}}$ the $(d - k)$-dimensional subspace which is least dilated by $A^{\widetilde{\underline{\ell}}}$, i.e whose image is spanned by the $(d - k)$ shortest semi-major axes of the ellipsoid $A^{\widetilde{\underline{\ell}}}(\{||v|| = 1\})$. Taking $F' = \xi^*_{\widetilde{\underline{\ell}}}$ in the defining property of $\ell_1, \dots, \ell_m$, we find i such that $A^{\ell_i}(F_+(A^{\underline{\ell}^*}))$ is transverse to $\xi^*_{\widetilde{\underline{\ell}}}$, the angle between these subspaces being $\geqslant \delta$.

From the claim below, we conclude that for large n (independently of $\widetilde{\ell}$), most of the mass of the probability measure

$$(A^{\widetilde{\ell}})_*(A^{\ell_i})_*(A^{\ell^*})_*^n(A^{\ell^0})_*(A^{\ell^*})_*^n(\rho)$$

is concentrated in a small ball in $G(k)$ around $A^{\widetilde{\ell}}A^{\ell_i}(F_+(A^{\ell^*}))$. Considering the case where ρ is the Lebesgue measure on $G(k)$, we conclude that this small ball is contained in a small ball around $\xi_{\underline{\ell}}$, where $\underline{\ell} := (\underline{\ell}^*)^n \underline{\ell}^0 (\underline{\ell}^*)^n \underline{\ell}_i \widetilde{\ell}$. $\qquad\square$

Claim: Let $A \in GL_d(\mathbb{K})$ act on the Grassmannian of k-dimensional subspaces. Denote by ξ_A^* the $(d-k)$ dimensional subspace which is least dilated by A, and by $K_\delta(A)$ the set of k-dimensional subspaces which form an angle $\geqslant \delta$ with ξ_A^*. Then the modulus of continuity of the restriction of A to $K_\delta(A)$ is controlled by δ only, independently of A.

Proof. This is an elementary computation: write any subspace in $K_\delta(A)$ as the graph of a linear map from $(\xi_A^*)^\perp$ to ξ_A^*, whose norm is bounded in terms of δ. After composing if necessary by an isometry, the action of A on the matrix of this linear map is given by the multiplication of each coefficient by a number $\in (0,1)$ (the ratio of two singular values of A). $\qquad\square$

APPENDIX B. TWISTING PROPERTIES

In Appendix A above, we studied a version of Avila-Viana simplicity criterion in the context of locally constant cocycles with values on

(B.1) $$\mathbb{G} = GL(d, \mathbb{R}), Sp(d, \mathbb{R}), U_{\mathbb{K}}(p, q), \mathbb{K} = \mathbb{R}, \mathbb{C}, \text{ or } \mathbb{H}$$

over shifts on at most countably many symbols.

In this way, based on the setting of Section 3 above, we can *already* get a simplicity criterion for the Kontsevich-Zorich cocycle over $\mathrm{SL}_2(\mathbb{R})$-orbits of square-tiled surfaces based on pinching and a strong form of twisting. However, such a simplicity criterion is not easy to apply directly, so it is desirable to replace the strong form of twisting by the relative form, with respect to some pinching matrix. This lead us to the statement of Proposition 2.16 whose proof is the main purpose of this appendix. But, before explaining the proof of Proposition 2.16, it is convenient to revisit a little bit the features of Noetherian topological spaces.

B.1. **Noetherian spaces.** Let $\mathbb{G}$ be as in (B.1). We use the notations and definitions introduced in Subsection 2.5. Let k be an admissible integer. For each $F' \in G(d-k)$, we define an hyperplane section as

$$\{F \in G(k) : F \cap F' \neq \{0\}\}$$

We consider then the coarsest topology on $G(k)$ such that the hyperplane sections are closed. The closed sets are the (arbitrary) intersections of finite unions of hyperplane sections. For sake of convenience, we will refer to this "pseudo-Zariski" topology as the *Schubert topology*.

Notice that the Schubert topology is coarser than the Zariski topology: hyperplane sections are defined by degree one (linear) equations while Zariski topology involves taking equations of arbitrary degree. In particular, this topology is not Hausdorff as the same is true for the Zariski topology.

Definition B.1. A topological space X is *Noetherian* if one of the following equivalent conditions is satisfied:

(i) any decreasing sequence $F_1 \supset F_2 \supset \ldots$ of closed sets is *stationary* (in the sense that there exists $m \in \mathbb{N}$ such that $F_i = F_m$ for all $i \geqslant m$).
(ii) any increasing sequence of open sets is stationary.
(iii) every intersection of a family (F_α) of closed sets is the intersection of a finite subfamily $F_1, \ldots, F_m$.
(iv) every union of a family (U_α) of open sets is the union of a finite subfamily $U_1, \ldots, U_m$.

Observe that any subspace of a Noetherian space is also Noetherian. A topology which is coarser than a Noetherian topology is also Noetherian.

Example B.2. It is a classical fact that the Zariski topology is Noetherian. Therefore the Schubert topology is also Noetherian.

Definition B.3. A Noetherian (topological) space X is irreducible if X is not the union of two proper closed sets.

The Grassmannian $G(k)$, equipped with the Zariski topology, is irreducible. It is a fortiori irreducible when it is equipped with the coarser Schubert topology.

We will need the following properties of Noetherian spaces.

Proposition B.4 (Proposition 1.5 in [Ha])**.** *A Noetherian space X can be written as a finite union $X = X_1 \cup \cdots \cup X_m$ of irreducible closed subsets X_i, $1 \leqslant i \leqslant m$. Moreover, this decomposition is unique (up to a permutation of the X_i's) if we ask that $X_i \not\subset X_j$ for $i \neq j$.*

Proposition B.5. *Let $X_1, \ldots, X_n$ be Noetherian spaces.*

(i) *The product space $X = X_1 \times \ldots \times X_n$ is Noetherian.*
(ii) *It is irreducible iff each X_i is irreducible.*
(iii) *Open subsets of X are exactly the finite unions of products of open subsets of the X_i.*
(iv) *Closed subsets of X are exactly the finite unions of products of closed subsets of the X_i.*
(v) *A closed subset of X is irreducible iff it is the product of closed irreducible subsets of the X_i.*

Proof. The first assertion is Exercise 8, p. 142 of [Bo]. Item (iii) is an immediate consequence of item (i) and Definition B.1, item (iv). Then item (iv) follows from some Boolean manipulations. From item (iv), it follows that a closed irreducible subset of X is the product of closed subsets of the X_i. It is also clear that if X is irreducible, then each X_i must be irreducible. Finally we show that a product of irreducible spaces is irreducible. Let

$$X = F_1 \cup \cdots \cup F_m$$

be the minimal decomposition of X into irreducible subsets. Each F_j is a product

$$F_j = F_j^{(1)} \times \cdots \times F_i^{(n)}$$

where each $F_j^{(i)}$ is an irreducible closed subset of X_i. For each $1 \leqslant i \leqslant n$, define

$$F^{(i)} := \bigcup_{F_j^{(i)} \neq X} F_j^{(i)}.$$

As X_i is irreducible, one has $F^{(i)} = X_i$ iff $F_j^{(i)} = X_i$ for all $1 \leqslant j \leqslant m$. For $1 \leqslant i \leqslant n$, choose $x_i \in X_i - F^{(i)}$ if $F^{(i)} \neq X_i$ and $x_i \in X_i$ otherwise. Let j be an index such that $x := (x_1, \ldots, x_n) \in F_j$. One must have $F_j^{(i)} = X_i$ for all $1 \leqslant i \leqslant n$, hence $F_j = X$. $\square$

B.2. **Twisting monoids.** Let $\mathcal{M}$ be a monoid acting on a Noetherian space X by homeomorphisms. Here, of course, our main example is:

Example B.6. Given a countable family of matrices $A_\ell \in \mathbb{G}$, $\ell \in \Lambda$, we consider the natural action of the monoid $\mathcal{M}$ generated by A_ℓ acting on the Grassmanian $X_k = G(k)$ equipped with the Schubert topology.

Proposition B.7. *If $g \in \mathcal{M}$, $F \subset X$ is closed and $gF \subset F$, then $gF = F$.*

Proof. Otherwise, $(g^n F)_{n \geqslant 0}$ would be a strictly decreasing infinite sequence of closed subsets of the Noetherian space X. $\square$

Proposition B.8. *Let $g \in \mathcal{M}$, let $F = F_1 \cup \cdots \cup F_n$ be the (minimal) decomposition of the closed subset $F \subset X$ into irreducible closed subsets $F_i \subset X$. If $gF = F$, then g permutes the irreducible pieces F_i.*

Proof. This follows from the uniqueness part of Proposition B.4. $\square$

Proposition B.9. *Assume that X is irreducible. Then, the following properties are equivalent:*
   (i) *there exists no proper closed $\mathcal{M}$-invariant subset of X;*
   (ii) *for every $x \in X$ and every non empty open subset $U \subset X$, there exists $g \in \mathcal{M}$ such that $gx \in U$;*
   (iii) *for every $N \geqslant 1$, $x_1, \ldots, x_N \in X$ and every non empty open subsets $U_1, \ldots, U_N \subset X$, there exists $g \in \mathcal{M}$ such that $gx_i \in U_i$. for all $1 \leqslant i \leqslant N$*

Proof. It is clear that $(iii) \implies (ii) \implies (i)$. We will prove by contradiction that (i) implies (iii). We let $\mathcal{M}$ act diagonally on X^N, for any $N \geqslant 1$.

Suppose that there exist $N \geqslant 1$, $x = (x_1, \ldots, x_N) \in X^N$ and non empty open subsets $U_1, \ldots, U_N \subset X$ such that

$$g.x \notin U^{(N)} := U_1 \times \cdots \times U_N$$

for all $g \in \mathcal{M}$.

Consider the closed set

$$F := \bigcap_{g \in \mathcal{M}} g^{-1}(X^N - U^{(N)}).$$

It is distinct from X^N and non empty because it contains x. It satisfies $gF \subset F$ for all $g \in \mathcal{M}$, hence $gF = F$ for all $g \in \mathcal{M}$ (Proposition B.7).

Let $F = F_1 \cup \cdots \cup F_m$ be the decomposition of F into irreducible closed sets $F_i \subset X^N$. By Proposition B.5, one has

$$F_i = F_i^{(1)} \times \cdots \times F_i^{(N)}$$

where each $F_i^{(l)}$ is an irreducible closed subset of X.

Since $gF = F$ for all $g \in \mathcal{M}$, Proposition B.8 implies that every $g \in \mathcal{M}$ permutes the subsets $F_i^{(l)}$.

Define the closed subset

$$F^* := \bigcup_{F_i^{(l)} \neq X} F_i^{(l)}.$$

As $\emptyset \neq F \neq X$, the subset F^* is not empty. As X is irreducible, one has $F^* \neq X$. As every $g \in \mathcal{M}$ permutes the subsets $F_i^{(l)}$, one has $gF^* = F^*$ for every $g \in \mathcal{M}$, so item (i) does not hold. $\qquad \square$

In view of Example B.6 and the discussion in Subsection 2.5 (related to Avila-Viana simplicity criterion), it is natural to call (iii) a ("strong form" of) *twisting condition* for an abstract monoid $\mathcal{M}$ acting by homeomorphisms on a Noetherian space X.

Remark B.10. The equivalent conditions of the proposition are satisfied by the monoid $\mathcal{M}$ if and only if they are satisfied by the group $\mathcal{G} = \langle g, g^{-1} : g \in \mathcal{M} \rangle$ generated by $\mathcal{M}$: this follows immediately from the statement of item (i).

B.3. **Twisting with respect to pinching matrices.** In the context of Example B.6 and aiming to the proof of Proposition 2.16, consider a word $\underline{\ell}^* \in \Omega = \bigcup_{n \geqslant 0} \Lambda^n$ such that $A_* := A^{\underline{\ell}^*}$ has simple spectrum (i.e., the cocycle is pinching). In this notation, Proposition 2.16 can be restated as:

Proposition B.11. *The (strong form of the) twisting condition is realized for the cocycle A if and only if, for each admissible integer k, there exists a word $\underline{\ell}(k) \in \Omega$ such that the matrix $B_k := A^{\underline{\ell}(k)}$ satisfies*

$$B_k(F) \cap F' = \{0\}$$

for every A_*-invariant subspaces $F \in G(k)$ and $F' \in G(d-k)$.

Proof. The condition is clearly necessary.

Conversely, assume that the condition in the proposition is satisfied. Let $\mathcal{M}$ denote the monoid generated by the matrices A_ℓ, $\ell \in \Lambda$. Recall that each $G(k)$ is irreducible.

Lemma B.12. *For each admissible integer k, the action of $\mathcal{M}$ on $G(k)$ satisfies the equivalent conditions of Proposition* B.9.

Proof of Lemma. We check that item (ii) in Proposition B.9 is satisfied. It is sufficient to show that, given $F \in G(k)$ and $F'_1, \ldots, F'_m \in G(d-k)$, there exists $C \in \mathcal{M}$ such that $C(F)$ is transverse to each F'_i. We claim that $C = A_*^n B_k A_*^n$ is an appropriate choice if n is large enough. Indeed, when n goes to $+\infty$, the sequence $(A_*^n(F))$ converges to some A_*-invariant subspace in $G(k)$, and each sequence $(A_*^{-n}(F'_i))$ converges to some A_*-invariant subspace in $G(d-k)$. As transversality is an open property, the claim follows from the property of B_k. $\qquad \square$

We now finish the proof of the proposition. Consider the diagonal action of $\mathcal{M}$ on the irreducible Noetherian space $X = \prod_{k \text{ admissible}} G(k)$. The strong form of the twisting condition will be satisfied if the action of $\mathcal{M}$ on X satisfies item (iii) in Proposition B.9. We check the equivalent item (i). Let F be a non-empty closed subset $F \subset X$ invariant under $\mathcal{M}$. Let $F = F_1 \cup \cdots \cup F_m$ be the minimal decomposition of F into irreducible closed sets $F_i \subset X$. By Proposition B.5, one has

$$F_i = \prod_{k \text{ admissible}} F_i^{(k)}$$

where each $F_i^{(k)}$ is an irreducible closed subset of $G(k)$. Define, for each admissible integer k,

$$F^{(k)} := \bigcup_{F_i^{(k)} \neq G(k)} F_i^{(k)}.$$

By Proposition B.8, the closed subset $F^{(k)}$ is invariant under $\mathcal{M}$. From Lemma B.12, $F^{(k)}$ must be either empty or equal to $G(k)$ for each admissible integer k. The first case cannot occur, and the second means that $F_i^{(k)} = G(k)$ for all k. We conclude that $F = X$, and the proof of the proposition is complete. $\qquad\qquad\square$

APPENDIX C. COMPLETELY PERIODIC CONFIGURATIONS IN $\mathcal{H}(4)$
BY SAMUEL LELIÈVRE

A surface in the stratum $\mathcal{H}(4)$ has one singularity of angle 10π. At this singularity, 5 outgoing separatrices start and 5 incoming separatrices end (see Figure 1). We label the outgoing separatrices from 1 to 5 (see Figure 1).
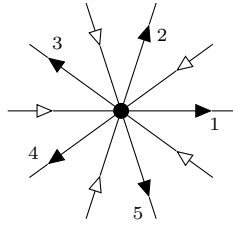
Fig. 1. Outgoing and incoming separatrices, and a numbering of outgoing separatrices.
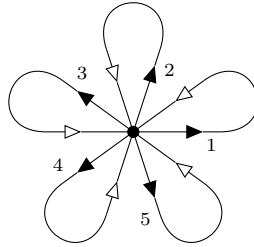
Fig. 2. There is no way to glue cylinders using this pairing of separatrices.
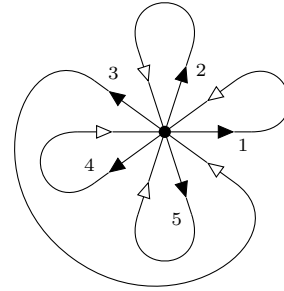
Fig. 3. With this pairing of separatrices there are two ways to glue cylinders.

In a completely periodic direction, outgoing separatrices pair with incoming separatrices. Define a permutation σ of $\{1, 2, 3, 4, 5\}$ by setting $\sigma(i) = j$ if the outgoing separatrix i comes back between the outgoing separatrices j and $j + 1 \mod 5$. We can enumerate permutations and draw the corresponding separatrix diagrams. Since the separatrix at which we start the labelling is arbitrary, we only need to enumerate permutations up to conjugation by cyclic permutations.

A diagram makes sense if the ribbons which follow unions of separatrices above or below form compatible bottoms and tops of cylinders. So, given a permutation, we look for the cycles of σ and of σ' defined by $\sigma'(i) = \sigma(i) + 1 \mod 5$ and then look for all the ways to match them.

A first example: $\sigma = $ id gives the diagram on Figure 2. In this example, σ has cycles $(1)(2)(3)(4)(5)$, while σ' has only one cycle (12345), therefore there is no possible pairing. We can't glue any cylinders on this separatrix diagram, there would need to be five bottoms of cylinders and only one top of cylinder.

Another example: $\sigma = (354)$ gives the diagram on Figure 3. In this example, σ has cycles $(1)(2)(354)$, while σ' has cycles $(123)(4)(5)$, and two pairings are possible: cylinders can fit on this separatrix diagram in two different ways.

As checked with Sage, there are exactly 16 permutations σ of $\{1, 2, 3, 4, 5\}$ (up to cyclic permutation) for which σ and σ' have the same number of cycles. The corresponding pairs (σ, σ') are listed below, expressed as products of nontrivial cycles. It turns out that each of them case gives one, two or three cylinder diagrams, and we get 22 cylinder diagrams in all.

$(354), (123)$	$(23)(45), (124)$	$(2345), (124)(35)$	$(2354), (1243)$
$(2453), (1254)$	$(2435), (1253)$	$(253), (12)(45)$	$(2534), (12)(354)$
$(25)(34), (12)(35)$	$(12)(345), (1354)$	$(12345), (13524)$	$(12453), (13254)$
$(124)(35), (13)(254)$	$(13524), (14253)$	$(13)(254), (1432)$	$(14253), (15432)$

Below, we list next to each of these 16 pairs (σ, σ') the associated cylinder diagrams and, furthermore, for each cylinder diagram, we put the letter H, resp. O, when the corresponding translation surfaces belong the the hyperelliptic, resp., odd, connected component of $\mathcal{H}(4)$.

1-4, 2-5, 354-123
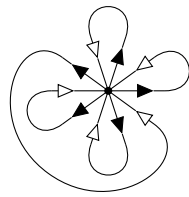
1-5, 2-4, 354-123

$\sigma : (354)$
$\sigma' : (123)$
$b : 1, 2, 354$
$t : 123, 4, 5$

1-3, 23-5, 45-124
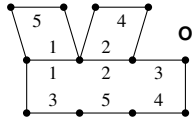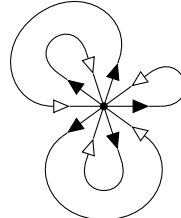
1-5, 23-124, 45-3

$\sigma : (23)(45)$
$\sigma' : (124)$
$b : 1, 23, 45$
$t : 124, 3, 5$
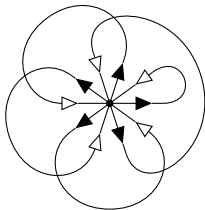
1-35, 2345-124

$\sigma : (2345)$
$\sigma' : (124)(35)$
$b : 1, 2345$
$t : 124, 35$
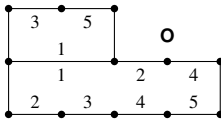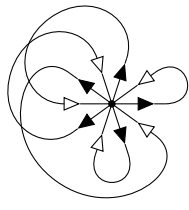
1-5, 2354-1243

$\sigma : (2354)$
$\sigma' : (1243)$
$b : 1, 2354$
$t : 1243, 5$
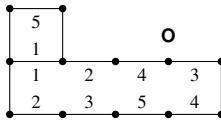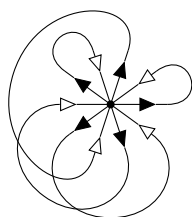
1-3, 2453-1254

σ: (2453)
σ': (1254)
b: 1, 2453
t: 1254, 3
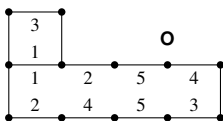
1-4, 2435-1253
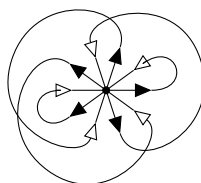
σ: (2435)
σ': (1253)
b: 1, 2435
t: 1253, 4
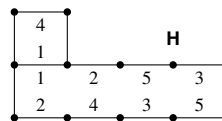
1-3, 253-45, 4-12
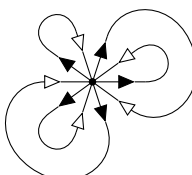
1-45, 253-12, 4-3

σ: (253)
σ': (12)(45)
b: 1, 253, 4
t: 12, 3, 45
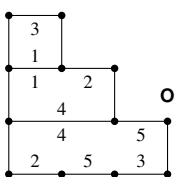
1-354, 2534-12
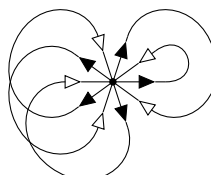
σ: (2534)
σ': (12)(354)
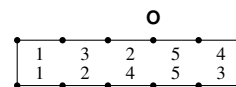b: 1, 2534
t: 12, 354
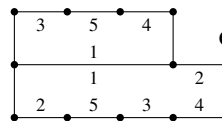
1-35, 25-4, 34-12
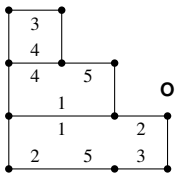
1-4, 25-12, 34-35
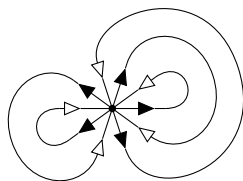
1-4, 25-35, 34-12

σ: (25)(34)
σ': (12)(35)
b: 1, 25, 34
t: 12, 35, 4
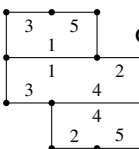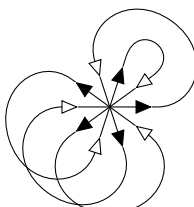
12-1354, 345-2

σ: (12)(345)
σ': (1354)
b: 12, 345
t: 1354, 2
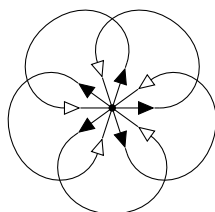
12345-13524

σ: (12345)
σ': (13524)
b: 12345
t: 13524
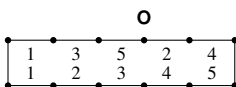
12453-13254
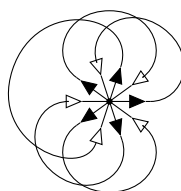
σ: (12453)
σ': (13254)
b: 12453
t: 13254
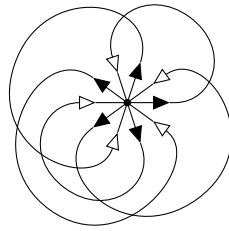
124-13, 35-254

124-254, 35-13
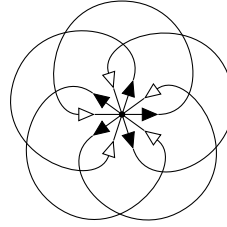
σ: (124)(35)
σ': (13)(254)
b: 124, 35
t: 13, 254

13524-14253

σ: (13524)
σ': (14253)
b: 13524
t: 14253
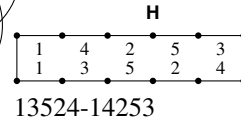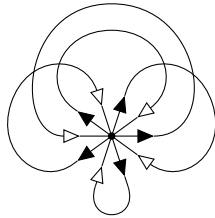
13-5, 254-1432

σ: (13)(254)
σ': (1432)
b: 13, 254
t: 1432, 5
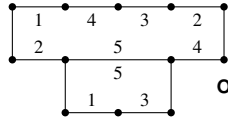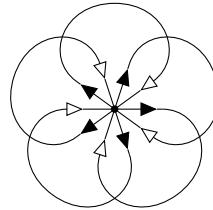
14253-15432

σ: (14253)
σ': (15432)
b: 14253
t: 15432
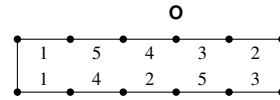
References

[Ar] P. Arnoux, *Le codage du flot géodésique sur la surface modulaire*, Enseign. Math. 40 (1994), 29–48.

[AMY] A. Avila, C. Matheus and J.-C. Yoccoz, *On the Kontsevich-Zorich cocycle over McMullen's family of symmetric translation surfaces*, in preparation.

[AV] A. Avila and M. Viana, *Simplicity of Lyapunov spectra: proof of the Zorich-Kontsevich conjecture*, Acta Math. **198** (2007), 1–56.

[AV2] A. Avila and M. Viana, *Simplicity of Lyapunov spectra: a sufficient criterion*, Port. Math. **64** (2007), 311–376.

[Ba] M. Bainbridge, *Euler characteristics of Teichmüller curves in genus two*, Geom. Topol. 11 (2007), 1887–2073.

[Bi] Y. Bilu, *Quantitative Siegel's theorem for Galois coverings*, Compositio Math. 106 (1997), 125–158.

[Bo] N. Bourbaki, *Elements of mathematics. Commutative algebra*, Translated from the French. Hermann, Paris; Addison-Wesley Publishing Co., Reading, Mass., 1972. xxiv+625 pp.

[BL] C. Birkenhake, H. Lange, *Complex abelian varieties*, Springer Grundlehren 302, 2nd. ed. (2003).

[Ch] D. Chen, *Square-tiled surfaces and rigid curves on moduli spaces*, Adv. Math. **228** (2011), 1135–1162.

[CM] D. Chen and M. Möller, *Non-varying sums of Lyapunov exponents of Abelian differentials in low genus*, Geometry and Topology **16** (2012), 2427–2479.

[Da] F. Dalbo, *Geodesic and horocyclic trajectories*, Translated from the 2007 French original. Universitext. Springer-Verlag London, Ltd., London; EDP Sciences, Les Ulis (2011) xii+176 pp.

[DM] V. Delecroix and C. Matheus, *Un contre-exemple à la réciproque du critère de Forni pour la positivité des exposants de Lyapunov du cocycle de Kontsevich-Zorich*, preprint arXiv:1103.1560 (2011), 1–5.

[EKZ]   A. Eskin, M. Kontsevich and A. Zorich, *Sum of Lyapunov exponents of the Hodge bundle with respect to the Teichmüller geodesic flow*, preprint arxiv: 1112.5872 (2011), 1–109.

[EMas]   A. Eskin and H. Masur, *Asymptotic formulas on flat surfaces*, Ergod. Theory Dynam. Systems **21** (2001), 443–478.

[EMat]   A. Eskin and C. Matheus, *A coding-free simplicity criterion for the Lyapunov exponents of Teichmüller curves*, preprint arXiv:1210.2157 (2012), 1–25.

[EM]   A. Eskin and M. Mirzakhani, *Invariant and stationary measures for the* $\mathrm{SL}(2,\mathbb{R})$ *action on moduli space*, preprint arXiv:1302.3320 (2013), 1–162.

[EMM]   A. Eskin, M. Mirzakhani and A. Mohammadi, *Isolation, equidistribution, and orbit closures for the* $\mathrm{SL}(2,\mathbb{R})$ *action on moduli space*, preprint (2012), available at http://www.math.uchicago.edu/~eskin/isolation.pdf.

[Fo1]   G. Forni, *Deviation of ergodic averages for area-preserving flows on surfaces of higher genus*, Ann. of Math. **155** (2002), 1–103.

[Fo2]   G. Forni, *On the Lyapunov exponents of the Kontsevich-Zorich cocycle*, Handbook of dynamical systems. Vol. 1B, 549–580, Elsevier B. V., Amsterdam, 2006.

[Fo3]   G. Forni, *A geometric criterion for the nonuniform hyperbolicity of the Kontsevich-Zorich cocycle*. With an appendix by C. Matheus. J. Mod. Dyn. **5** (2011), 355–395.

[FMZ1]   G. Forni, C. Matheus and A. Zorich, *Square-tiled cyclic covers*, J. Mod. Dyn. **5** (2011), 285–318.

[FMZ2]   G. Forni, C. Matheus and A. Zorich, *Zero Lyapunov exponents of the Hodge bundle*, preprint arXiv:1201.6075 (2012), 1–46, to appear in Comm. Math. Helv.

[Ha]   R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, **52**, Springer-Verlag, New York-Heidelberg, 1977. xvi+496 pp. ISBN: 0-387-90244-9

[HS]   M. Hindry and J. Silverman, *Diophantine geometry*, Graduate Texts in Mathematics, 201. Springer-Verlag, New York, 2000. xiv+558 pp. ISBN: 0-387-98975-7; 0-387-98981-1

[HL]   P. Hubert and S. Lelièvre, *Prime arithmetic Teichmüller discs in* $\mathcal{H}(2)$, Israel J. Math. **151** (2006), 281–321.

[Ka]   E. Kani, *The number of genus 2 covers of an elliptic curve*, Manuscripta Math. **121** (2006), 51–80.

[Ko]   M. Kontsevich, *Lyapunov exponents and Hodge theory*, in *The Mathematical Beauty of Physics* (Saclay 1996), *Adv. Ser. Math. Phys.* **24**, 318–332, World Sci. Publ., River Edge, NJ, 1997.

[KZ]   M. Kontsevich and A. Zorich, *Connected components of the moduli space of Abelian differentials with prescribed singularities*, Invent. Math. **153** (2003), 631–678.

[LN]   E. Lanneau and D.-M. Nguyen, *Teichmüller curves generated by Weierstrass Prym eigenforms in genus three and genus four*, preprint arXiv:1111.2299 (2011), 1–51.

[MY]   C. Matheus and J.-C. Yoccoz, *The action of the affine diffeomorphisms on the relative homology group of certain exceptionally symmetric origamis*, J. Mod. Dyn. **4** (2010), 453–486.

[MYZ]   C. Matheus, J.-C. Yoccoz and D. Zmiaikou, *Homology of origamis with symmetries*, preprint arXiv:1207.2423 (2012), 1–35.

[Ma]   H. Masur, *Interval exchange transformations and measured foliations*, Ann. of Math. **115** (1982), no. 1, 169–200.

[Mc]   C. McMullen, *Prym varieties and Teichmüller curves*, Duke Math. J. **133** (2006), 569–590.

[Mc2]   C. McMullen, *Teichmüller curves in genus two: discriminant and spin*, Math. Ann. **333** (2005), 87–130.

[Mo]   M. Möller, *Prym covers, theta functions and Kobayashi curves in Hilbert modular surfaces*, preprint arXiv:1111.2624 (2011), 1–25.

[Se]   C. Series, *Geometrical methods of symbolic coding*. Ergodic theory, symbolic dynamics, and hyperbolic spaces (Trieste, 1989), 125–151, Oxford Sci. Publ., Oxford Univ. Press, New York, 1991.

[SW]   J. Smillie and B. Weiss, *Characterizations of lattice surfaces*, Invent. Math. 180 (2010), 535–557.

[Ve1]   W. Veech, *Gauss measures for transformations on the space of interval exchange maps*, Ann. of Math. **115** (1982), 201–242.

[Ve2]   W. Veech, *The Teichmüller geodesic flow*, Ann. of Math. **124** (1986), 441–530.

[Ve3]   W. Veech, *Teichmüller curves in moduli space, Eisenstein series and an application to triangular billiards*, Invent. Math. **97** (1989), 533–583.

[Ve4]   W. Veech, *Moduli spaces of quadratic differentials*, J. Anal. Math. **55** (1990), 117–171.

[Zm]   D. Zmiaikou, *Origamis and permutation groups*, Ph.D thesis, Orsay, 2011, available at http://www.zmiaikou.com/research.

[Zo1]   A. Zorich, *Asymptotic flag of an orientable measured foliation on a surface*, in *Geometric Study of Foliations* (Tokyo, 1993), 479–498, World Sci. Pub., River Edge, NJ, 1994.

[Zo2]   A. Zorich, *Finite Gauss measure on the space of interval exchange transformations. Lyapunov exponents*, Ann. Inst. Fourier (Grenoble) **46** (1996), 325–370.

[Zo3]   A. Zorich, *Deviation for interval exchange transformations*, Ergod. Theory Dynam. Systems **17** (1997), 1477–1499.

[Zo4]   A. Zorich, *On hyperplane sections of periodic surfaces*, in *Solitons, Geometry and Topology: on the Crossroad*, A. M. S. Transl. **179**, 173–189, A. M. S., Providence, RI, 1997.

[Zo5]   A. Zorich, *How do the leaves of a closed* 1-*form wind around a surface?*, in *Pseudoperiodic Topology*, A. M. S. Transl. **197**, 135–178, A. M. S., Providence, RI, 1999.

[Zo6]   A. Zorich, *Flat surfaces*, "Frontiers in Number Theory, Physics, and Geometry", v. **I**, Springer (2006), 437–583.

[Zo7]   A. Zorich, *Square tiled surfaces and Teichmüller volumes of the moduli spaces of abelian differentials*, (English summary) Rigidity in dynamics and geometry (Cambridge, 2000), 459–471, Springer, Berlin, 2002.

CARLOS MATHEUS: UNIVERSITÉ PARIS 13, SORBONNE PARIS CITÉ, LAGA, CNRS (UMR 7539), F-93439, VILLETANEUSE, FRANCE.
E-mail address: matheus@impa.br.
URL: http://www.impa.br/∼cmateus

MARTIN MÖLLER: INSTITUT FÜR MATHEMATIK, GOETHE-UNIVERSITÄT FRANKFURT, ROBERT-MAYER-STR. 6-8, 60325 FRANKFURT AM MAIN, FRANKFURT, GERMANY.
E-mail address: moeller@math.uni-frankfurt.de.
URL: https://www.uni-frankfurt.de/fb/fb12/mathematik/ag/personen/moeller

JEAN-CHRISTOPHE YOCCOZ: COLLÈGE DE FRANCE (PSL), 3, RUE D'ULM, 75005 PARIS, FRANCE.
E-mail address: jean-c.yoccoz@college-de-france.fr.
URL: http://www.college-de-france.fr/site/jean-christophe-yoccoz