Chaotic dynamical systems associated with tilings of R^N

Lionel Rosier

Chaotic dynamical systems associated with tilings of $\mathbb{R}^N$

Lionel Rosier *

February 3, 2010

Abstract

In this chapter, we consider a class of discrete dynamical systems defined on the homogeneous space associated with a regular tiling of $\mathbb{R}^N$, whose most familiar example is provided by the $N-$dimensional torus $\mathbb{T}^N$. It is proved that any dynamical system in this class is chaotic in the sense of Devaney, and that it admits at least one positive Lyapunov exponent. Next, a chaos-synchronization mechanism is introduced and used for masking information in a communication setup.

Key words: Chaotic dynamical system, regular tiling of $\mathbb{R}^N$, ergodicity, Lyapunov exponent, equidistributed sequence, chaos synchronization, cryptography.
AMS subject classifications: 34C28, 37A25, 93B55, 94A60

1 Introduction

Chaos synchronization has exhibited an increasing interest in the last decade since the pioneering works reported in [21, 22], and it has been advocated as a powerful tool in secure communication [31, 30, 10, 32, 3]. Chaotic systems are indeed characterized by a great sensitivity to the initial conditions and a spreading out of the trajectories, two properties which are very close to the Shannon requirements of confusion and diffusion [14].

There are basically two approaches when using chaotic dynamical systems for secure communications purposes. The first one amounts to numerically computing a great number of iterations of a discrete chaotic system, in using e.g. the message as initial data (see [29] and the references therein). The second one amounts to hiding a message in a chaotic dynamics. Only a part of the state vector (the "output") is conveyed through the public channel. Next, a synchronization mechanism is designed to retrieve the message at the receiver part (see [27] and the references therein).

In both approaches, the first difficulty is to "build" a chaotic system appropriate for encryption purposes. In this context, the corresponding chaotic signals must have no patterning, a broad-band power spectrum and an auto-correlation function that quickly drops to zero. In [23], a mean for synthesizing volume-preserving or volume expanding maps is provided. For such systems, there are several directions of expansion (stretching), while the discrete trajectories are folded back into a confined region of the phase space. Expansion can be carried out by unstable linear mappings

*Institut Élie Cartan, UMR 7502 UHP/CNRS/INRIA, B.P. 239, 54506 Vandœuvre-lès-Nancy Cedex, France. (rosier@iecn.u-nancy.fr). LR was partially supported by the "Agence Nationale de la Recherche" (ANR), Project CISIFS, grant ANR-09-BLAN-0213-02.

with at least one positive Lyapunov exponent. Folding can be carried out with modulo functions through shift operations, or with triangular, trigonometric functions through reflexion operations. Fully stretching piecewise affine Markov maps have also attracted interest because such maps are expanding in all directions and they have uniform invariant probability densities (see [28, 8]).

Besides, we observe that the word "chaotic" has not the same meaning everywhere, and that the chaotic behavior of a system is often demonstrated only by numerical evidences. The first aim of this chapter is to provide a rigorous analysis, based on the definition given by Devaney [6], of the chaotic behavior of a large class of affine dynamical systems defined on the homogeneous space associated with a regular tiling of $\mathbb{R}^N$. Classical piecewise affine chaotic transformations, as the *tent map*, belong to that class. The dimension N may be arbitrarily large in the theory developed below, but, for obvious reasons, most of the examples given here will be related to regular tilings of the plane ($N = 2$). The study of the subclass of (time-invariant or switched) affine systems on $\mathbb{T}^N$, the $N-$dimensional torus, is done in [25, 27]. The folding for this subclass is carried out with modulo maps, which, from a geometric point of view, amounts to "fold back" $\mathbb{R}^N$ to $[0,1)^N$ by means of translations by vectors in $\mathbb{Z}^N$. Those translations are replaced here by all the isometries of some crystallographic group for an arbitrary regular tiling of $\mathbb{R}^N$. Notice also that the fundamental domain used in the numerical implementation may be chosen with some degree of freedom. It may be a hypercube (as $[0,1)^N$ for $\mathbb{T}^N$), or a polyhedron, or a more complicated bounded, connected set in $\mathbb{R}^N$.

For ease of implementation and duplication, a cryptographic scheme must involve a map for which the parameters identification is expected to be a difficult task, while computational requirements for masking and unmasking information are not too heavy. The second aim of this chapter is to show that all these requirements are fulfilled for the class of dynamical systems considered here. The way of extracting the masked information is provided through an observer-based synchronization mechanism with a finite-time stabilization property.

Let us now describe the content of the chapter. Section 2 is devoted to the mathematical analysis of the chaotic properties of the following discrete dynamical system

$$x_{k+1} = Ax_k + B \pmod{G} \tag{1.1}$$

where $A \in \mathbb{Z}^{N\times N}$, $B \in \mathbb{R}^N$, and (mod G) means roughly that x_{k+1} is the point in the fundamental domain $\mathcal{T}$ derived from $Ax_k + B$ by some transformation g in the group G. (1.1) may be viewed as a "realization" in $\mathcal{T} \subset \mathbb{R}^N$ of an abstract dynamical system on the homogeneous space $\mathbb{R}^N/G$ of classes modulo G. The torus $\mathbb{T}^N$ corresponds to the simplest case when G is the group of all the translations of vectors $u \in \mathbb{Z}^N$ and the fundamental domain is $\mathcal{T} = [0,1)^N$. Note that most of the examples encountered in the literature are given only for the torus $\mathbb{T}^N$ with $N = 1$ and $|A| \geqslant 2$, or for $N = 2$ and $\det A = 1$ (see e.g. [9]). We give here a sufficient condition for (1.1) to be chaotic in the sense of Devaney for any given regular tiling of $\mathbb{R}^N$ ($N \geqslant 1$), and we investigate the Lyapunov exponents of (1.1) and the equirepartition of the trajectories of (1.1).

Finally, a masking/unmasking technique based on a dynamical embedding is proposed in Section 3.

2 Chaotic dynamical systems and regular tilings of $\mathbb{R}^N$

2.1 Chaotic dynamical system

Let (M, d) denote a compact metric space, and let $f : M \to M$ be a continuous map. The following definition of a chaotic system is due to Devaney [6].

Definition 1 *The discrete dynamical system*

$$(\Sigma) \qquad x_{k+1} = f(x_k)$$

is said to be chaotic *if the following conditions are fulfilled:*
(C1) (Sensitive dependence on initial conditions) *There exists a number* $\varepsilon > 0$ *such that for any* $x_0 \in M$ *and any* $\delta > 0$*, there exists a point* $y_0 \in M$ *with* $d(x_0, y_0) < \delta$ *and an integer* $k \geqslant 0$ *such that* $d(x_k, y_k) \geqslant \varepsilon$*;*
(C2) (One-sided topological transitivity) *There exists some* $x_0 \in M$ *with* $(x_k)_{k\geqslant 0}$ *dense in* M*;*
(C3) (Density of periodic points) *The set* $D = \{x_0 \in M;\ \exists k > 0,\ x_k = x_0\}$ *is dense in* M*.*

Recall [35, Thm 5.9], [34, Thm 1.2.2] that when f is *onto* (i.e., $f(M) = M$), the one-sided topological transitivity is equivalent to the condition:
(C2′) For any pair of nonempty open sets U, V in M, there exists an integer $k \geqslant 0$ such that $f^{-k}(U) \cap V \neq \emptyset$ ($\iff U \cap f^k(V) \neq \emptyset$).

2.2 Regular tiling of $\mathbb{R}^N$

An *isometry* g of $\mathbb{R}^N$ is a map from $\mathbb{R}^N$ into $\mathbb{R}^N$ such that $||g(X) - g(Y)|| = ||X - Y||$ for all $X, Y \in \mathbb{R}^N$. Let G be a group of isometries of $\mathbb{R}^N$ such that for any point $X \in \mathbb{R}^N$ the orbit of X under the action of G, namely the set

$$G \cdot X = \{g(X);\ g \in G\},$$

is closed and discrete. Let $P \subset \mathbb{R}^N$ be a compact, connected set with a nonempty interior. Following [2], we shall say that the pair (G, P) constitutes a *regular tiling* of $\mathbb{R}^N$ if the two following conditions are fulfilled:

$$\bigcup_{g\in G} g(P) = \mathbb{R}^N \tag{2.2}$$

$$\forall g, h \in G \quad \left(g(\overset{\circ}{P}) \cap h(\overset{\circ}{P}) \neq \emptyset \quad \Rightarrow \quad g = h\right). \tag{2.3}$$

Recall that $\overset{\circ}{P}$ stands for the *interior* of P, that is

$$\overset{\circ}{P} = \{x \in P;\ \exists \varepsilon > 0,\ B(x, \varepsilon) \subset P\}.$$

The set $P \subset \mathbb{R}^N$ is termed a *fundamental tile*, and the group G a *crystallographic group*. An example of a regular tiling of $\mathbb{R}^2$ with a triangular fundamental tile is represented in Fig. 1.

Note that a point $X \in \mathbb{R}^N$ may in general be obtained in several ways as the transformation of a point in P by an isometry in G. We introduce a set $\mathcal{T}$, called a *fundamental domain*, with $\overset{\circ}{P} \subset \mathcal{T} \subset P$ and such that

$$\bigcup_{g\in G} g(\mathcal{T}) = \mathbb{R}^N \tag{2.4}$$

$$\forall X, X' \in \mathcal{T},\ \forall g \in G \quad \left(X' = g(X) \quad \Rightarrow \quad X' = X\right). \tag{2.5}$$

Introducing the equivalence relation in $\mathbb{R}^N$

$$X \sim Y \quad \iff \quad \exists g \in G, \quad Y = g(X),$$

we denote by $x = \overline{X}$ the class of X for $\sim$, i.e. $x = \{g(X);\ g \in G\} = G \cdot X$. When several groups are considered at some time, we denote by $\overline{X}^G$ the class of X modulo G. Finally, we introduce the homogeneous space of cosets $\mathbb{H} = (\mathbb{R}^N/G) = \{x = \overline{X}; X \in \mathbb{R}^N\}$, and define on it the following metric

$$d(\overline{X}, \overline{Y}) = \inf_{g\in G} ||Y - g(X)||.$$

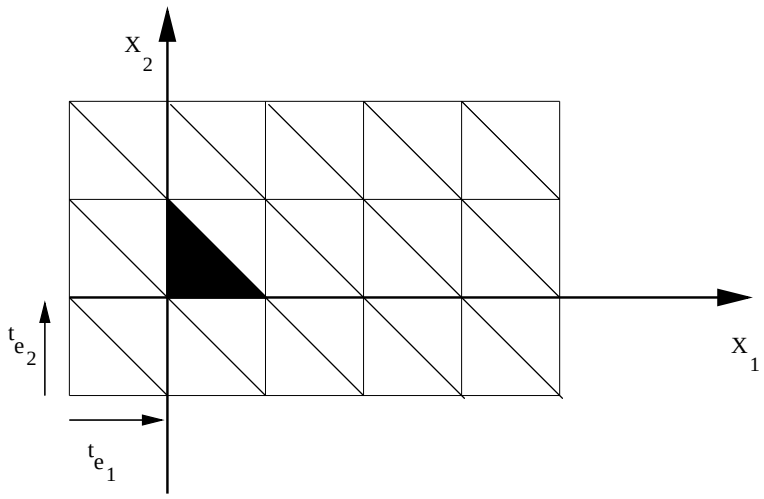

Figure 1: A regular tiling of $\mathbb{R}^2$ with a triangular fundamental tile.

The natural covering mapping $\pi : \mathbb{R}^N \to \mathbb{H}$, defined by $\pi(X) = \overline{X}$, satisfies

$$d(\pi(X), \pi(Y)) \leqslant ||X - Y||,$$

hence it is continuous. It follows that $\mathbb{H} = \pi(P)$ is a compact metric space. On the other hand, the restriction of π to $\mathcal{T}$ is a bijection from $\mathcal{T}$ onto $\mathbb{H}$. We may therefore define the projection $\varpi : \mathbb{R}^N \to \mathcal{T}$ by $\varpi(X) = (\pi_{|\mathcal{T}})^{-1}\pi(X)$. Note that ϖ is in general not continuous when $\mathcal{T}$ is equipped with the topology induced from $\mathbb{R}^N$, while it is continuous when $\mathcal{T}$ is endowed with the topology inherited from $\mathbb{H}$.

The simplest example of a regular tiling of $\mathbb{R}^N$ is provided by the group of translations by vectors with integral coordinates (which is isomorphic to the lattice subgroup)

$$G = \{t_u;\ u \in \mathbb{Z}^N\} \sim \mathbb{Z}^N, \tag{2.6}$$

where $t_u(X) = X + u$. In such a situation, a fundamental tile (resp. domain) is given by $P = [0,1]^N$ (resp. $\mathcal{T} = [0,1)^N$), and the homogeneous space $\mathbb{H}$ is the standard $N-$dimensional torus $\mathbb{T}^N$. A classification (up to isomorphism) of the crystallographic groups of $\mathbb{R}^N$ has been done for a long time for $N \leqslant 3$. There are 17 such groups in $\mathbb{R}^2$, and 230 groups in $\mathbb{R}^3$, see [2, 5].

2.3 Affine transformation

We aim to define "simple" chaotic dynamical systems on $M = \mathbb{H}$ by using affine transformations. Assume given a matrix $A \in \mathbb{Z}^{N\times N}$ and a point $B \in \mathbb{R}^N$. The following hypotheses will be used at several places in the chapter.
(H1)

$$\forall X, X' \in \mathbb{R}^n \quad (X \sim X' \Rightarrow AX + B \sim AX' + B)$$

i.e. $X' = g(X)$ for some $g \in G$ implies $AX' + B = g'(AX + B)$ for some $g' \in G$;
(H2) There exist a subgroup $G' \subset G$ of translations and a finite collection of isometries $(g_i)_{i=1}^k$ in G such that

(i) G is spanned as a group by the isometries in $G' \cup (g_i)_{i=1}^k$;

(ii) $G' = \{t_u; u = \sum_{i=1}^N y_i u_i,\ y = (y_i)_{i=1}^N \in \mathbb{Z}^N\}$ for some basis $(u_i)_{i=1}^N$ of $\mathbb{R}^N$;

(iii) Setting $P' := \cup_{1 \leqslant i \leqslant k}\ g_i(P)$ we have that (G', P') is a regular tiling of $\mathbb{R}^N$. We denote by $\mathcal{T}'$ a fundamental domain for (G', P').

(H1) is a compatibility condition needed to define a dynamical system on $\mathbb{H}$. If G is given by (2.6), then (H1) holds for any $A \in \mathbb{Z}^{N\times N}$ and any $B \in \mathbb{R}^N$. However, if

$$G = \{t_u; u = \sum_{i=1}^{N} y_i u_i,\ y = (y_i)_{i=1}^N \in \mathbb{Z}^N\} \tag{2.7}$$

for some basis $(u_i)_{i=1}^N$ of $\mathbb{R}^N$, then (H1) holds if and only if

$$U^{-1}AU \in \mathbb{Z}^{N\times N} \tag{2.8}$$

where U is the $N \times N$ matrix with u_i as ith column for $1 \leqslant i \leqslant N$.

(H2) allows to decompose the projection ϖ onto $\mathcal{T}$ into a projection onto $\mathcal{T}'$, a fundamental domain for the regular tiling (G', P') of $\mathbb{R}^N$ involving only translations, followed by a projection from $\mathcal{T}'$ onto $\mathcal{T}$.

Example 2 *Let* $G =< t_1, t_2, r >$ *and* $G' =< t_1, t_2 >$, *where* $t_1(X) = X + (1, -1)$, $t_2(X) = X + (1, 1)$, *and* $r(X_1, X_2) = (-X_2, X_1)$. *Pick* $k = 4$ *and* $(g_1, g_2, g_3, g_4) = (r, r^2, r^3, id)$. *Take as fundamental tiles* $P = \{X = (X_1, X_2); 1 \leqslant X_1 \leqslant 2,\ 0 \leqslant X_2 \leqslant 2 - X_1\}$ *(solid line) and* $P' = P \cup r(P) \cup r^2(P) \cup r^3(P)$ *(broken line) (see Fig. 2).*

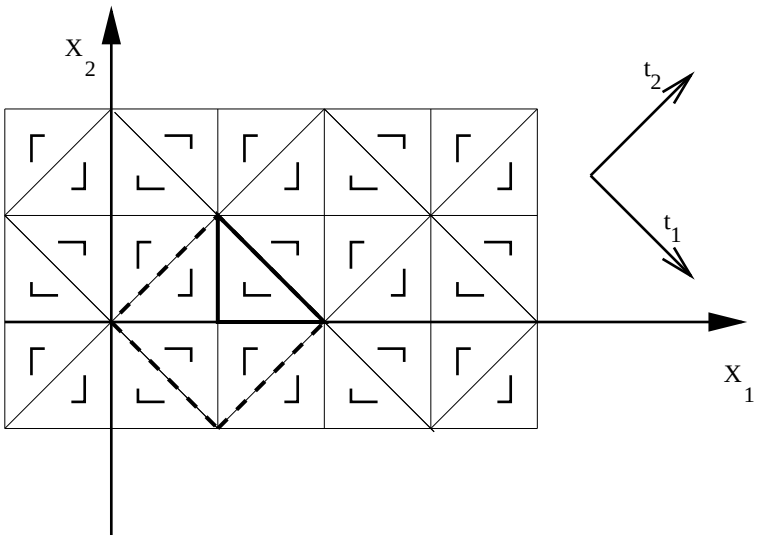

Figure 2: A regular tiling of $\mathbb{R}^2$ with a triangular fundamental tile.

Assume that (H1) holds. Then we may define

$$A\overline{X} + B := \overline{AX + B}$$

for any $X \in \mathbb{R}^N$. Thus we may consider the dynamical system $(\Sigma_{A,B})$ on $\mathbb{H}$ defined by

$$(\Sigma_{A,B})\ \begin{cases} x_{k+1} & = f(x_k) := Ax_k + B, \\ x_0 & \in \mathbb{H}. \end{cases} \tag{2.9}$$

The map f is called an *affine transformation* of $\mathbb{H}$.

Example 3 *Let $N = 1$, and let $G =< t, s >$ be the group spanned by the translation $t(X) = X + 2$ and the symmetry $s(X) = 2 - X$. Set $P = [0, 1]$. Then (G, P) constitutes a regular tiling of $\mathbb{R}$. Note that P is also a fundamental domain. Pick $(A, B) = (2, 0) \in \mathbb{R}^2$. (H1) and (H2) are satisfied with $G' = \{t_u;\ u \in 2\mathbb{Z}\}$, $k = 2$, $g_1 = s$ and $g_2 = s^2 = id$. Let us write the realization of (2.9) in P. Obviously, $AX \in P$ for $0 \leqslant X < 1/2$, while $s(AX) = 2(1 - X) \in P$ for $1/2 \leqslant X \leqslant 1$. Viewed in $P = [0, 1]$, the dynamics reads then*

$$x_{k+1} = h(x_k) \tag{2.10}$$

where h is the familiar tent map (see Fig. 3)

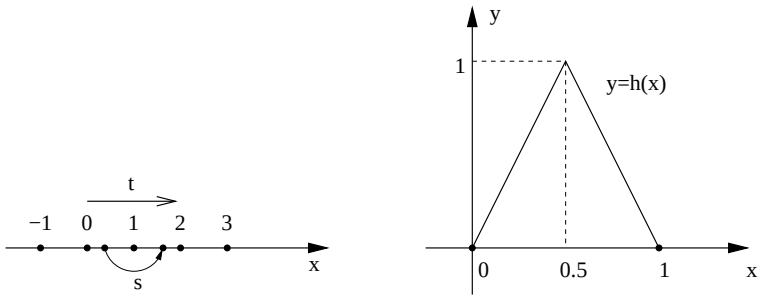

Figure 3: A : Action of s and t; B : the tent map

$$h(x) = \begin{cases} 2x & \text{if } 0 \leqslant x < \frac{1}{2}, \\ 2(1-x) & \text{if } \frac{1}{2} \leqslant x \leqslant 1. \end{cases}$$

It follows from Theorem 10 (see below) that (2.10) is chaotic on $[0, 1]$.

When $\mathbb{H} = \mathbb{T}^N$ and $B = 0$, f is nothing else than an endomorphism of the topological group $(\mathbb{T}^N, +)$, and f is onto (resp., an isomorphism) if and only if $\det A \neq 0$ (resp., $\det A = \pm 1$) (see [35, Thm 0.15]). Let $\mathrm{sp}(A)$ denote the spectrum of the matrix A, that is the set of the eigenvalues of A. A *root of unity* is any complex number of the form $\lambda = \exp(2\pi i t)$, with $t \in \mathbb{Q}$. To see whether a dynamical system $(\Sigma_{A,B})$ is chaotic, we need the following key result [35, Thm 1.11].

Proposition 4 *Let $f(x) = Ax + b$ ($b \in \mathbb{T}^N$, $A \in \mathbb{Z}^{N \times N}$ with $\det A \neq 0$) be an affine transformation of $\mathbb{T}^N$. Then the following conditions are equivalent:*

(i) *$(\Sigma_{A,b})$ is one-sided topologically transitive;*

(ii) *(a) A has no proper roots of unity (i.e., other than 1) as eigenvalues, and*
(b) $(A - I)\mathbb{T}^N + \mathbb{Z}b$ is dense in $\mathbb{T}^N$;

(iii) *f is* ergodic*; that is, f is* measure-preserving *(i.e. for any Borel set $E \subset \mathbb{T}^N$, $m(f^{-1}(E)) = m(E)$, where m denotes the Lebesgue measure on $\mathbb{T}^N$), and the only Borel sets $E \subset \mathbb{T}^N$ for which $f^{-1}(E) = E$ satisfy $m(E) = 0$ or $m(E) = 1$.*

Notice that (ii) reduces to "A has no roots of unity as eigenvalues" when $b = 0$. Indeed, it may be seen that $(A - I)\mathbb{T}^N$ is dense in $\mathbb{T}^N$ if and only if $(A - I)$ is invertible.

2.4 Endomorphism of $\mathbb{T}^N$

The first result in this chapter, which comes from [27], provides a necessary and sufficient condition for $\Sigma_{A,0}$ to be chaotic in $\mathbb{T}^N$.

Theorem 5 *Let $A \in \mathbb{Z}^{N \times N}$. Then $(\Sigma_{A,0})$ is chaotic in $\mathbb{T}^N$ if, and only if,* $\det \mathrm{A} \neq 0$ *and A has no roots of unity as eigenvalues.*

Proof. Assume first that $(\Sigma_{A,0})$ is chaotic. We first claim that A is nonsingular. Indeed, if $\det A = 0$, then the map f defined in (2.9) is not onto [35, Thm 0.15], i.e. $A\mathbb{T}^N \neq \mathbb{T}^N$. As $A\mathbb{T}^N$ is compact (hence equal to its closure), it is not dense in $\mathbb{T}^N$, hence we cannot find some state $x_0 \in \mathbb{T}^N$ such that the sequence $(x_k) = (A^k x_0)$ is dense in $\mathbb{T}^N$, which contradicts (C2). Thus $\det A \neq 0$. On the other hand, since $(\Sigma_{A,0})$ is one-sided topologically transitive, the matrix A has no roots of unity as eigenvalues by virtue of Proposition 4.

Conversely, assume that $\det A \neq 0$ and that A has no roots of unity as eigenvalues. As (C1) is a consequence of (C2) and (C3) (see [1],[34, Thm 1.3.1]), we only have to establish the later properties. (C2) follows from Proposition 4. To prove (C3) we need to prove two lemmas.

Lemma 6 *Let $A \in \mathbb{Z}^{N\times N}$ be such that $\det A \neq 0$, and pick any $p \in \mathbb{N}^*$ with $(p, \det A) = 1$ (i.e. p and $\det A$ are relatively prime). Then the map $T : x \in (\mathbb{Z}/p\mathbb{Z})^N \mapsto Ax \in (\mathbb{Z}/p\mathbb{Z})^N$ is invertible.*

Proof of Lemma 6. First, observe that the map T is well-defined. Indeed, if $X, Y \in \mathbb{Z}^N$ fulfill $X - Y \in (p\mathbb{Z})^N$, then $AX - AY \in (p\mathbb{Z})^N$ so that AX and AY belong to the same coset in $(\mathbb{Z}/p\mathbb{Z})^N = \mathbb{Z}^N/(p\mathbb{Z})^N$. As $(\mathbb{Z}/p\mathbb{Z})^N$ is a finite set, we only have to prove that T is one-to-one. Let $X, Y \in \mathbb{Z}^N$ be such that $AX = AY$ in $(\mathbb{Z}/p\mathbb{Z})^N$ (i.e., $A(X - Y) \in (p\mathbb{Z})^N$). We aim to show that $X = Y$ in $(\mathbb{Z}/p\mathbb{Z})^N$ (i.e., $X - Y \in (p\mathbb{Z})^N$). Set $U = X - Y$, and pick a vector $Z \in \mathbb{Z}^N$ such that $AU = pZ$. It follows that $U = \frac{p}{\det A}\tilde{A}Z$, where $\tilde{A} \in \mathbb{Z}^{N\times N}$ denotes the adjoint matrix of A (i.e. the transpose of the matrix formed by the cofactors). Since $U \in \mathbb{Z}^N$, each component of the vector $p\tilde{A}Z$ is divisible by $\det A$. Since $(p, \det A) = 1$, we infer the existence of a vector $V \in \mathbb{Z}^N$ such that $\tilde{A}Z = (\det A)V$. Then $X - Y = U = pV \in (p\mathbb{Z})^N$, as desired. ∎

Lemma 7 *Let A and p be as in Lemma 6, and let $E_p := \{\overline{0}, \overline{(\frac{1}{p})}, ..., \overline{(\frac{p-1}{p})}\} \subset \mathbb{T}$. Then each point $x \in E_p^N$ is periodic for $(\Sigma_{A,0})$. As a consequence, the set of periodic points of $(\Sigma_{A,0})$ is dense in $\mathbb{T}^N$ (i.e., (C3) is satisfied).*

Proof of Lemma 7. First, observe that for any $i, j \in \{0, ..., p-1\}$, $i/p \equiv j/p \pmod 1$ if and only if $i \equiv j \pmod p$. We infer from Lemma 6 that the map $\tilde{T} : x \in E_p^N \mapsto Ax \in E_p^N$ is well defined and invertible. Pick any $x \in E_p^N$. As the sequence $(\tilde{T}^k x)_{k\geqslant 1}$ takes its values in the (finite) set E_p^N, there exist two numbers $k_2 > k_1 \geqslant 1$ such that $\tilde{T}^{k_1}x = \tilde{T}^{k_2}x$. $\tilde{T}$ being invertible, we conclude that $A^{k_2-k_1}x = x$ (i.e., x is a periodic point). Finally, the set $E = \cup\{E_p^N;\ p \geqslant 1,\ (p, \det A) = 1\}$ is clearly dense in $\mathbb{T}^N$ (take for p any large prime number), and all its points are periodic. This completes the proof of Lemma 7 and of Theorem 5. ∎

For an affine transformation, we obtain a result similar to Theorem 5 when $1 \notin \mathrm{sp}(A)$.

Corollary 8 *Let $A \in \mathbb{Z}^{N\times N}$ and $b \in \mathbb{T}^N$. Assume that 1 is not an eigenvalue of A. Then $(\Sigma_{A,b})$ is chaotic in $\mathbb{T}^N$ if, and only if, $\det A \neq 0$ and A has no roots of unity as eigenvalues.*

Proof. Pick any $B \in \mathbb{R}^N$ with $\overline{B} = b$. As $1 \notin \mathrm{sp}(A)$, we may perform the change of variables

$$x = r - \overline{(A - I)^{-1}B}, \tag{2.11}$$

which transforms (2.9) into

$$\begin{cases} r_{k+1} &= Ar_k, \\ r_0 &= x_0 + \overline{(A - I)^{-1}B}. \end{cases} \tag{2.12}$$

Clearly, the conditions (C2) and (C3) are fulfilled for $(\Sigma_{A,b})$ if, and only if, they are fulfilled for (2.12). Therefore, the result is a direct consequence of Theorem 5. ∎

Corollary 9 *Let G be defined by* (2.7) *for some basis $(u_i)_{i=1}^N$ of $\mathbb{R}^N$. Let $A \in \mathbb{Z}^{N\times N}$ and $B \in \mathbb{R}^N$. Assume that* (2.8) *holds and that* 1 *is not an eigenvalue of A. Then $(\Sigma_{A,B})$ is chaotic in $\mathbb{H} = \mathbb{R}^N/G$ if, and only if,* $\det A \neq 0$ *and A has no roots of unity as eigenvalues.*

Proof. From Corollary 8, we know that the dynamical system on $\mathbb{T}^N$

$$z_{k+1} = \tilde{f}(z_k) := U^{-1}AUz_k + U^{-1}B \tag{2.13}$$

is chaotic if, and only if, $\det A \neq 0$ and A has no roots of unity as eigenvalues. To prove that the dynamical system on $\mathbb{H} = \mathbb{R}^N/G$

$$x_{k+1} = f(x_k) := Ax_k + B \tag{2.14}$$

is chaotic under the same conditions, it is sufficient to prove that the maps $f : \mathbb{H} \to \mathbb{H}$ and $\tilde{f} : \mathbb{T}^N \to \mathbb{T}^N$ are topologically conjugate; i.e., there exists a homeomorphism $h : \mathbb{H} \to \mathbb{T}^N$ such that $h \circ f = \tilde{f} \circ h$. Define h by $h(\overline{X}) = \overline{Z}$ where $Z = U^{-1}X$, $\overline{X} = G \cdot X$ is the class of X in $\mathbb{H}$ and $\overline{Z}$ is the class of Z in $\mathbb{T}^N$. Note first that h is well defined and continuous. Indeed, if $X' = X + UK$ with $K \in \mathbb{Z}^N$, then $Z' = U^{-1}X' = U^{-1}X + K = Z + K$, so that h is well defined. On the other hand, the map $X \in \mathbb{R}^N \mapsto \overline{U^{-1}X} \in \mathbb{T}^N$ is clearly continuous. Obviously, h is invertible with $h^{-1}(\overline{Z}) = \overline{X}$ for $X = UZ$. h is therefore a homeomorphism from $\mathbb{H}$ onto $\mathbb{T}^N$. Let us check now that $h \circ f = \tilde{f} \circ h$. Pick any $X \in \mathbb{R}^N$. Then

$$h \circ f(\overline{X}^G) = h(\overline{AX + B}^G) = \overline{U^{-1}(AX + B)}^{\mathbb{T}^N} = \tilde{f}(\overline{U^{-1}X}^{\mathbb{T}^N}) = \tilde{f} \circ h(\overline{X}^G)$$

and the result follows. ∎

We are in a position to state and prove the main result of this chapter.

Theorem 10 *Let (G, P) be a regular tiling of $\mathbb{R}^n$, and let $(A, B) \in \mathbb{Z}^{N\times N} \times \mathbb{R}^N$ be such that both the assumptions (H1) and (H2) are fulfilled. Assume in addition that* $\det A \neq 0$ *and that A has no roots of unity as eigenvalues. Then the discrete dynamical system in $\mathbb{R}^N/G$*

$$x_{k+1} = Ax_k + B \tag{2.15}$$

is chaotic.

Proof. Pick any fundamental domain $\mathcal{T}$ for (G, P), and let G' and $\mathcal{T}'$ be as in (H2). In addition to (2.15), we shall consider the discrete dynamical system in $\mathbb{R}^N/G'$

$$z_{k+1} = Az_k + B. \tag{2.16}$$

For any given $X_0 \in \mathbb{R}^N$, let $x_0 = \overline{X_0}^G$ and $z_0 = \overline{X_0}^{G'}$. Clearly, if $X \sim X'$ (mod G'), then $X \sim X'$ (mod G). Therefore, one can define a map $p : \mathbb{R}^N/G' \to \mathbb{R}^N/G$ by $p(\overline{X}^{G'}) = \overline{X}^G$. p is continuous and onto. We need two claims.

Claim 1. $x_k = p(z_k)$ for all k.

Indeed, this is true for $k = 0$, and if for some $k \geqslant 0$, $x_k = p(z_k)$ (i.e. for some $X_k \in \mathbb{R}^N$, $x_k = \overline{X_k}^G$ and $z_k = \overline{X_k}^{G'}$), then we have that

$$x_{k+1} = \overline{AX_k + B}^G = p(\overline{AX_k + B}^{G'}) = p(z_{k+1})$$

which completes the proof of Claim 1.

Claim 2. The image by p of any dense set in $\mathbb{R}^N/G'$ is a dense set in $\mathbb{R}^N/G$.

Let $A \subset \mathbb{R}^N/G'$ be a given dense set. Pick any $X \in \mathbb{R}^N$ and any $\varepsilon > 0$. Since A is dense in $\mathbb{R}^N/G'$, there exists $Y \in \mathbb{R}^N$ such that $\overline{Y}^{G'} \in A$ and

$$d(\overline{X}^{G'}, \overline{Y}^{G'}) = \inf_{g \in G'} ||Y - g(X)|| < \varepsilon.$$

It follows that

$$d(\overline{X}^{G}, \overline{Y}^{G}) = \inf_{g \in G} ||Y - g(X)|| < \varepsilon$$

for $G' \subset G$. Since $\overline{Y}^{G} = p(\overline{Y}^{G'}) \in p(A)$ and the pair (X, ε) was arbitrary, this demonstrates that $p(A)$ is dense in $\mathbb{R}^N/G$. Claim 2 is proved.

Let us complete the proof of Theorem 10. To prove that (2.15) is chaotic, it is sufficient (see [1]) to check that the conditions (C2) and (C3) are fulfilled. We know from Corollary 9 that (2.16) is chaotic. We may therefore pick $X_0 \in \mathbb{R}^N$ so that, setting $z_0 = \overline{X_0}^{G'}$, the sequence $\{z_k\}_{k \geqslant 0}$ defined by (2.16) is dense in $\mathbb{R}^N/G'$. By Claim 1 and Claim 2, the sequence $\{x_k\}$ defined by (2.15) and $x_0 = \overline{X_0}^{G}$ is dense in $\mathbb{R}^N/G$; that is, (C2) is fulfilled for (2.15). On the other hand, the set of periodic points for (2.16) is dense in $\mathbb{R}^N/G'$, since (C3) is fulfilled for (2.16). By Claim 1, any periodic point z_0 for (2.16) gives rise to a periodic point $x_0 = p(z_0)$ for (2.15). By Claim 2, the set of periodic points for (2.15) is dense in $\mathbb{R}^N/G$; i.e., (C3) is fulfilled for (2.15). The proof of Theorem 10 is complete. ■

Example 11 *(i) Let* $G =< t_{e_1}, t_{2e_2}, s >$ *where* $t_{e_1}(X) = X + (1,0)$, $t_{e_2}(X) = X + (0,2)$, $s(X_1, X_2) = (X_1, -X_2)$, *and* $P = [0,1] \times [0,1]$. *Pick* $G' =< t_{e_1}, t_{e_2} >$, $k = 2$, $(g_1, g_2) = (s, id)$ *(see Fig. 4). Finally, pick* $A = \begin{pmatrix} -2 & 0 \\ 0 & 3 \end{pmatrix}$ *and* $B = (0.5, -3.2)$. *Note that* $[A, S] := AS - SA = 0$, *where* $S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ *is the matrix corresponding to the symmetry* s. *Then (H1) and (H2) are satisfied,* $sp(A) = \{-2, 3\}$, *and by Theorem 10 the dynamical system* (2.9) *is chaotic in* $\mathbb{H} = \mathbb{R}^2/G$.

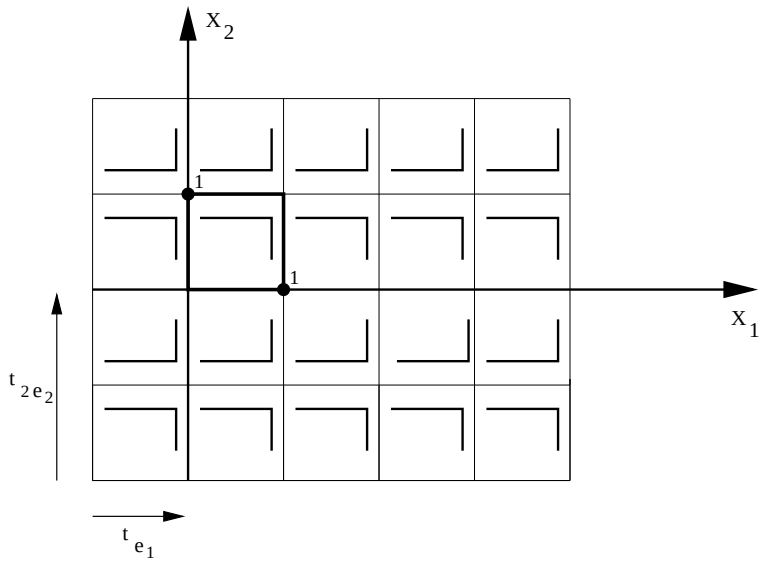

Figure 4: $G =< t_{e_1}, t_{2e_2}, s >$.

(ii) Let $G =< t_{2e_1}, t_{2e_2}, s_1, s_2 >$ *where* $t_{2e_1}(X) = X + (2,0)$, $t_{2e_2}(X) = X + (0,2)$, $s_1(X_1, X_2) = (-X_1, X_2)$, $s_2(X_1, X_2) = (X_1, -X_2) = -s_1(X_1, X_2)$, *and* $P = [0,1] \times [0,1]$. *Pick* $G' =< t_{2e_1}, t_{2e_2} >$, $k = 4$, $(g_1, g_2, g_3, g_4) = (s_1, s_2, s_2 \circ s_1, id)$. *(see Fig. 5). Finally, pick* $A = \begin{pmatrix} 0 & -3 \\ 4 & 0 \end{pmatrix}$ *and* $B = (-0.2, 1.7)$. *Note that* $AS = -SA$, *where* S *is as above. Then (H1) and (H2) are satisfied,* $sp(A) = \{\pm 2i\sqrt{3}\}$, *and by Theorem 10 the dynamical system* (2.9) *is chaotic in* $\mathbb{H} = \mathbb{R}^2/G$.

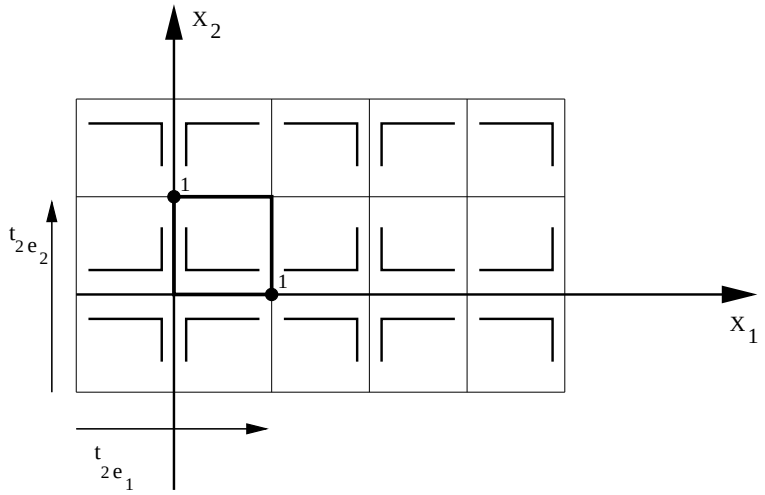

Figure 5: $G =< t_{2e_1}, t_{2e_2}, s_1, s_2 >$.

2.5 Lyapunov exponents

Let M denote a compact differentiable manifold endowed with a Riemann metric $< u, v >_m$, and let $f : M \to M$ be a map of class C^1. The following definition is borrowed from [13].

Definition 12 *A point* $x \in M$ *is said to be a* regular point *of* f *if there exist numbers* $\lambda_1(x) > \lambda_2(x) > \cdots > \lambda_m(x)$ *and a decomposition*

$$T_x M = E_1(x) \oplus \cdots \oplus E_m(x)$$

of the tangent space $T_x M$ *of* M *at* x *such that*

$$\lim_{k \to +\infty} \frac{1}{k} \ln ||(D_x f^k)u|| = \lambda_j(x)$$

for all $0 \neq u \in E_j(x)$ *and every* $1 \leqslant j \leqslant m$. *(*$||v||^2 :=< v, v >_x \ \ \forall v \in T_x M$*.) The numbers* $\lambda_j(x)$ *and the spaces* $E_j(x)$ *are termed the* Lyapunov exponents *and the* eigenspaces *of* f *at the regular point* x.

Assume now that the group G is such that each isometry $g \in G$ has no fixed point, i.e. $g(X) \neq X$ for all $X \in \mathbb{R}^N$. Then $\mathbb{H} = \mathbb{R}^N/G$ is a smooth flat Riemannian manifold. Before investigating the Lyapunov exponents of an affine transformation on $\mathbb{H}$, let us give a few examples.

Example 13 *(i)* $\mathbb{H} = \mathbb{T}^N$, *and more generally,* $\mathbb{H} = \mathbb{R}^N/G$ *where* G *is as in* (2.7)*;*

(ii) $\mathbb{H} = \mathbb{R}^2/G$ *for* $G =< t_{2e_1}, t_{e_2}, t_{e_1} \circ s >$ *where* (e_1, e_2) *is the canonical basis of* $\mathbb{R}^2$ *and* $s(X_1, X_2) = (X_1, -X_2)$ *(see Fig. 6).* $\mathbb{H}$ *is then the* Klein bottle. *The torus* $\mathbb{T}^2$ *and the Klein bottle* $\mathbb{H}$ *are the only smooth manifolds obtained in dimension 2. In dimension 3, there are 6 smooth manifolds (see [36, Section 3.5.5 p. 117]).*

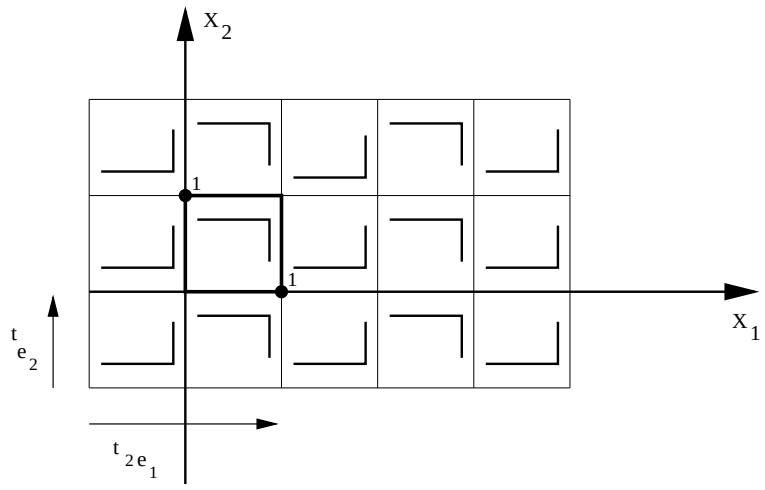

Figure 6: The regular tiling of $\mathbb{R}^2$ associated with the Klein bottle.

Consider now an affine transformation $f(\overline{X}) = \overline{AX + B}$ of $\mathbb{H}$, the pair (A, B) fulfilling (H1). Assume also that $\det A \neq 0$. Then for any $k \geqslant 1$,

$$f^k(\overline{X}) = \overline{A^k X + A^{k-1}B + \cdots + AB + B}.$$

Pick a point $X \in \overset{\circ}{P}$ such that

$$A^k X + A^{k-1}B + \cdots + AB + B \in \cup_{g \in G} g(\overset{\circ}{P})$$

(note that such a property holds for almost every $X \in \mathbb{R}^N$), and an isometry $g \in G$ such that

$$g(A^k X + A^{k-1}B + \cdots + AB + B) \in \overset{\circ}{P}\,.$$

For $||U||$ sufficiently small, we also have that

$$g(A^k(X + U) + A^{k-1}B + \cdots + AB + B) \in \overset{\circ}{P}\,.$$

Therefore $(D_{\overline{X}} f^k)\overline{U} = \overline{GA^kU}$, where $G = Dg \in \mathbb{R}^{N \times N}$. Since G is an orthogonal matrix, we have that $||\overline{GA^kU}|| = ||A^kU||$. Let $\mu_1 > \mu_2 > \cdots > \mu_m > 0$ denote the absolute values of the eigenvalues of A, and let $E_i(x)$ be the direct sum of the generalized eigenspaces (see [7]) associated with the eigenvalues whose absolute value is μ_i, for each $i \leqslant m$. Then, using the Jordan decomposition of A, we easily see that for any $U \in E_j \setminus \{0\}$

$$\lim_{k \to +\infty} \frac{1}{k} \ln ||A^kU|| = \ln \mu_j.$$

Observe now that if $\sigma(A)$ does not intersect the circle $\{z \in \mathbb{C};\ |z| = 1\}$, then A has at least one eigenvalue λ with $|\lambda| > 1$ (since the product of all the eigenvalues of A is $\det A \in \mathbb{Z} \setminus \{0\}$), hence f admits at least one *positive* Lyapunov exponent. Therefore, we have proved the following

Proposition 14 *Let (G, P) be a regular tiling of $\mathbb{R}^N$ such that any isometry $g \in G$ has no fixed point. Let $(A, B) \in \mathbb{R}^{N \times N} \times \mathbb{R}^N$ be such that (H1) is satisfied,* $\det A \neq 0$ *and each eigenvalue λ of A satisfies $|\lambda| \neq 1$, and let $f : \mathbb{H} = \mathbb{R}^N/G \to \mathbb{H}$ be defined by $f(x) = Ax + B$. Then almost every point $x \in \mathbb{H}$ is regular for f, with Lyapunov exponents $\ln \mu_1 > \cdots > \ln \mu_m$, where $\mu_1 > \cdots > \mu_m$ are the absolute values of the eigenvalues of A. Furthermore,* $\ln \mu_1 > 0$.

Notice that the existence of (at least) one positive Lyapunov exponent is often considered as a characteristic property of a chaotic motion [33]. That property quantifies the sensitive dependence on initial conditions.

2.6 Equidistribution

In this section, $\mathbb{H} = \mathbb{T}^N$. Let us consider a discrete dynamical system with an output

$$\left\{ \begin{array}{rl} x_{k+1} & = Ax_k + B \\ y_k & = Cx_k \end{array} \right. \tag{2.17}$$

where $x_0 \in \mathbb{T}^N$, $A \in \mathbb{Z}^{N\times N}$, $b \in \mathbb{T}^N$ and $C \in \mathbb{Z}^{1\times N}$. It should be expected that the output y_k inherits the chaotic behavior of the state x_k. However, Devaney's definition of a chaotic system cannot be tested on the sequence (y_k), since this sequence is not defined as a trajectory of a dynamical system. Rather, we may give a condition ensuring that the sequence (y_k) is equidistributed (hence dense) in $\mathbb{T}$ for a.e. x_0, a property which may be seen as an *ersatz* of (C2).

If $X = (X_1, ..., X_N), Y = (Y_1, ..., Y_N)$ are any given points in $[0,1)^N$ and $x = \overline{X}$, $y = \overline{Y}$, then we say that $x < y$ (resp., $x \leqslant y$) if $X_i < Y_i$ (resp., $X_i \leqslant Y_i$) for $i = 1, ..., N$. The set of points $z \in \mathbb{T}^N$ such that $x \leqslant z < y$ will be denoted by $[x, y)$. Let $(x_k)_{k\geqslant 0}$ be any sequence in $\mathbb{T}^N$. For any subset E of $\mathbb{T}^N$, let $S_K(E)$ denote the number of points x_k, $0 \leqslant k \leqslant K-1$, which lie in E.

Definition 15 *[11] We say that* (x_k) *is* uniformly distributed modulo 1 *(or* equidistributed in $\mathbb{T}^N$*) if*

$$\lim_{K\to\infty} \frac{S_K([x,y))}{K} = m([x,y)) = \prod_{i=1}^{N} (Y_i - X_i)$$

for all intervals $[x, y) \subset \mathbb{T}^N$.

The following result is very useful to decide whether a sequence is equidistributed or not.

Proposition 16 *(***Weyl criterion** *[11], [24]) The sequence* $(x_k)_{k\geqslant 0}$ *is equidistributed in* $\mathbb{T}^N$ *if, and only if, for every lattice point* $p \in \mathbb{Z}^N$, $p \neq 0$

$$\frac{1}{K} \sum_{0\leqslant k<K} e^{2i\pi p\cdot x_k} \to 0 \qquad \text{as } K \to +\infty.$$

The next result shows that under the same assumptions as in Corollary 8 the sequences (x_k) and (y_k) are respectively equidistributed in $\mathbb{T}^N$ and $\mathbb{T}$ for a.e. initial state $x_0 \in \mathbb{T}^N$.

Theorem 17 *Let* $A \in \mathbb{Z}^{N\times N}$, $b \in \mathbb{T}^N$ *and* $C \in \mathbb{Z}^{1\times N} \setminus \{0\}$. *Assume that* $\det A \neq 0$ *and that* A *has no roots of unity as eigenvalues (hence* $\Sigma_{A,b}$ *is chaotic). Then for a.e.* $x_0 \in \mathbb{T}^N$ *the sequence* (x_k) *(defined in (2.17)) is equidistributed in* $\mathbb{T}^N$*, and the sequence* $(y_k) = (Cx_k)$ *is equidistributed in* $\mathbb{T}$.

Proof: By virtue of Theorem 4, the map $f(x) = Ax + b$ is ergodic on $\mathbb{T}^N$. It follows then from Birkhoff Ergodic Theorem (see e.g. [35, Thm 1.14]) that for any $h \in L^1(\mathbb{T}^N, dm)$ and for a.e. $x_0 \in \mathbb{T}^N$

$$\frac{1}{K} \sum_{0\leqslant k<K} h(f^k(x_0)) \to \int_{\mathbb{T}^N} h(y)\, dm(y) \qquad \text{as } K \to +\infty.$$

Therefore, for every lattice point $p \in \mathbb{Z}^N$, $p \neq 0$, and for a.e. $x_0 \in \mathbb{T}^N$

$$\frac{1}{K} \sum_{0\leqslant k<K} e^{2\pi ip\cdot f^k(x_0)} \to \int_{\mathbb{T}^N} e^{2\pi ip\cdot y}\, dm(y) = 0 \qquad \text{as } K \to +\infty.$$

As $\mathbb{Z}^N \setminus \{0\}$ is countable, the same property holds for a.e. $x_0 \in \mathbb{T}^N$ and all $p \in \mathbb{Z}^N \setminus \{0\}$. Therefore, we infer from Weyl criterion that the sequence $(x_k) = (f^k(x_0))$ is equidistributed for a.e. $x_0 \in \mathbb{T}^N$. Pick any $x_0 \in \mathbb{T}^N$ such that (x_k) is equidistributed, and let us show that the output sequence

$(y_k) = (Cx_k)$ is also equidistributed provided that $C = (C_1, ..., C_N) \neq (0, ..., 0)$. Indeed, for any $p \in \mathbb{Z} \setminus \{0\}$

$$\frac{1}{K} \sum_{0 \leqslant k < K} e^{2\pi i p y_k} = \frac{1}{K} \sum_{0 \leqslant k < K} e^{2\pi i (pC)\, x_k} \to 0 \qquad \text{as } K \to +\infty,$$

hence the equidistribution of (y_k) follows again by Weyl criterion. ■

Remark 18 *For a regular tiling (G, P) of $\mathbb{R}^N$, even if the sequence (x_k) is equidistributed in $\mathbb{H}$, the output (y_k) fails in general to be equidistributed in $\mathbb{T}$. This is clear when one considers a regular tiling of $\mathbb{R}^2$ with the triangle $P = \{X = (X_1, X_2); \quad X_1 \geqslant 0,\ X_2 \geqslant 0,\ X_1 + X_2 \leqslant 1\}$ as fundamental tile, and $C = (1 \quad 0)$.*

3 Synchronization and information recovering

The aim of this section is to suggest a chaos-based encryption scheme involving affine transformations on the homogeneous space $\mathbb{H}$ associated with some regular tiling of $\mathbb{R}^N$. We shall provide conditions which guarantee a synchronization with a finite-time stability of the error despite the inherent nonlinearity of the chaotic systems under study.

3.1 Encryption setup

Assume given a regular tiling (G, P) of $\mathbb{R}^N$ and a pair $(A, B) \in \mathbb{R}^{N \times N} \times \mathbb{R}^N$ fulfilling the assumptions of Theorem 10. For the sake of simplicity, assume further that $\mathbb{R}^N / G' = \mathbb{T}^N$, so that $\mathcal{T}' = [0, 1)^N$. Let $\varpi : \mathbb{R}^N \to \mathcal{T}$ and $\varpi' : \mathbb{R}^N \to \mathcal{T}'$ denote the projections on the fundamental domains of (G, P) and (G', P'), respectively. Set for $k \in \mathbb{N}$ and $X \in \mathbb{R}^N$

$$\varpi_k(X) = \begin{cases} \varpi'(X) & \text{if } \ k \notin (N+1)\mathbb{N}; \\ \varpi(X) & \text{if } \ k \in (N+1)\mathbb{N}. \end{cases} \tag{3.18}$$

At each discrete time k, a symbol $m_k \in \mathbb{R}$ (the *plaintext*) of a sequence $(m_k)_{k \geqslant 0}$ is encrypted by a (nonlinear) encrypting function e which "mixes" m_k and X_k and produces a *ciphertext* $u_k = e(X_k, m_k)$. We also assume given a decrypting function d such that $m_k = d(X_k, u_k)$ for each k. Next, the ciphertext u_k is embedded in the dynamics (2.9). We shall consider the following encryption

$$(\Sigma_{A,B,M,C}) \qquad \begin{cases} X_{k+1} &= \varpi_k\{A(X_k + Mu_k) + B\} \\ Y_k &= C(X_k + Mu_k) \end{cases} \tag{3.19}$$

which corresponds to an embedding of the ciphertext in both the dynamics and the output. In (3.19), $A \in \mathbb{Z}^{N \times N}$, $M \in \mathbb{Z}^{N \times 1}$, and $C \in \mathbb{Z}^{1 \times N}$ are given matrices, and $B \in \mathbb{R}^N$. $Y_k \in \mathbb{R}$ is the output conveyed to the receiver through the channel.

From the definition of the decrypting function d, it is clear that to retrieve m_k at the decryption side we need to recover the pair (X_k, u_k), which in turn calls for reproducing a chaotic sequence $(\hat{X}_k)$ synchronized with (X_k) (i.e., such that $\hat{X}_k - X_k \to 0$). To this end, we propose a mechanism based on some suitable unknown input observers, inspired from the ones given in [17, 18, 25, 27]. We stress that the gain matrices have to be $\mathbb{Z}$-valued here.

For the encryption considered here, the decryption involves the following observer-like structure

$$(\hat{\Sigma}_{A,B,M,C}) \qquad \begin{cases} \hat{X}_{k+1} &= \varpi_k\{A\hat{X}_k + L(Y_k - \hat{Y}_k) + B\} \\ \hat{Y}_k &= C\hat{X}_k \end{cases} \tag{3.20}$$

where $L \in \mathbb{Z}^{N\times 1}$, $\hat{X}_k \in \mathbb{R}^N$ and $\hat{Y}_k \in \mathbb{R}$ ($\hat{X}_0$ being an arbitrary point in $\mathbb{R}^N$). Let $\overline{X}$ denote the class of X modulo G', i.e. in $\mathbb{T}^N$. Set $e_k = \overline{X_k} - \overline{\hat{X}_k}$ for all $k \geqslant 0$. Noticing that for all $X \in \mathbb{R}^N$

$$\overline{\varpi_k(X)} = \overline{\varpi'(X)} = \overline{X} \qquad \text{for } 1 \leqslant k \leqslant N,$$

we obtain by subtracting (3.20) from (3.19) that the error dynamics reads

$$e_{k+1} = (A - LC)e_k + \overline{(A - LC)Mu_k}, \qquad 1 \leqslant k \leqslant N. \tag{3.21}$$

Before proceeding to the design of the observers, we give a few definitions and a preliminary result.

3.2 Definitions and preliminary results

Definition 19 *A pair $(A^\flat, C^\flat)$ is said to be in a* companion canonical form *if it takes the form*

$$A^\flat = \begin{pmatrix} -\alpha^{N-1} & 1 & 0 & \cdots & 0 \\ -\alpha^{N-2} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -\alpha^1 & 0 & 0 & \cdots & 1 \\ -\alpha^0 & 0 & 0 & \cdots & 0 \end{pmatrix}, \qquad C^\flat = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \end{pmatrix}\cdot \tag{3.22}$$

It is well known that the characteristic polynomial of $A^\flat$ reads $\chi_{A^\flat}(\lambda) = \lambda^N + \alpha^{N-1}\lambda^{N-1} + \cdots + \alpha^1\lambda + \alpha^0$.

Definition 20 *Two pairs (A, C) and $(A^\flat, C^\flat)$ in $\mathbb{Z}^{N\times N} \times \mathbb{Z}^{1\times N}$ are said to be* similar over $\mathbb{Z}$ *if there exists a matrix $T \in \mathbb{Z}^{N\times N}$ with* $\det T = \pm 1$ *(hence $T^{-1} \in \mathbb{Z}^{N\times N}$ too) such that*

$$A = T^{-1}A^\flat T, \quad C = C^\flat T.$$

The following result provides a sufficient condition for an observable pair (A, C) to admit a $\mathbb{Z}$-valued gain matrix L such that $A - LC$ is Hurwitz.

Proposition 21 *Let $A \in \mathbb{Z}^{N\times N}$ and $C \in \mathbb{Z}^{1\times N}$ be two matrices such that (A, C) is similar over $\mathbb{Z}$ to a pair $(A^\flat, C^\flat) \in \mathbb{Z}^{N\times N} \times \mathbb{Z}^{1\times N}$ in a companion canonical form. Let us denote by $(-\alpha^{N-1} \ \cdots \ -\alpha^0)'$ the first column of $A^\flat$. Then there exists a unique matrix $L \in \mathbb{Z}^{N\times 1}$ such that the matrix $A-LC$ is Hurwitz (i.e., $sp(A-LC) \subset \{z \in \mathbb{C};\ |z| < 1\}$), namely $L = T^{-1}L^\flat$ with $L^\flat = (-\alpha^{N-1} \ \cdots \ -\alpha^0)'$. Furthermore, $(A - LC)^N = 0$.*

Proof. Write $A = T^{-1}A^\flat T$, $C = C^\flat T$, with $(A^\flat, C^\flat)$ as in (3.22) and $T \in \mathbb{Z}^{N\times N}$ with $\det T = \pm 1$. For any given matrix $L \in \mathbb{Z}^{N\times 1}$, we define the matrix $L^\flat = (l^{N-1} \cdots \ l^0)'$ by $L^\flat = TL$. Then, $A - LC = T^{-1}(A^\flat - L^\flat C^\flat)T$ with

$$A^\flat - L^\flat C^\flat = \begin{pmatrix} -\alpha^{N-1} - l^{N-1} & 1 & 0 & \cdots & 0 \\ -\alpha^{N-2} - l^{N-2} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -\alpha^1 - l^1 & 0 & 0 & \cdots & 1 \\ -\alpha^0 - l^0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Its characteristic polynomial reads

$$\chi_{A^\flat - L^\flat C^\flat}(\lambda) = \lambda^N + (\alpha^{N-1} + l^{N-1})\lambda^{N-1} + \cdots + (\alpha^1 + l^1)\lambda + (\alpha^0 + l^0).$$

If L is such that $A-LC$ is Hurwitz, then $A^\flat - L^\flat C^\flat = T(A-LC)T^{-1}$ is Hurwitz too, hence we may write $\chi_{A-LC}(\lambda) = \chi_{A^\flat - L^\flat C^\flat}(\lambda) = \lambda^p \chi(\lambda)$, where $p \in \{0,...,N\}$ and $\chi \in \mathbb{Z}[\lambda]$ has its roots $\lambda_1,...,\lambda_{N-p}$ in the set $\{z \in \mathbb{C};\ 0 < |z| < 1\}$. Assume that $p < N$, and denote by q the constant coefficient of χ. Then $q \neq 0$ (since $\chi(0) \neq 0$), and $|q| = \prod_{i=1}^{N-p} |\lambda_i| < 1$, which is impossible, since $q \in \mathbb{Z}$. Therefore $p = N$ and $l^j = -\alpha^j$ for any $j \in \{0,...,N-1\}$ (hence $L^\flat$ and L are unique). On the other hand

$$A^\flat - L^\flat C^\flat = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}. \tag{3.23}$$

For this choice of L, $\chi_{A-LC}(\lambda) = \lambda^N$ and $(A-LC)^N = 0$. ■

It should be emphasized that the above argument shows that a $\mathbb{Z}$-valued matrix $\mathcal{N}$ is Hurwitz if and only if it is nilpotent. In other words, the system $\nu_{k+1} = \mathcal{N}\nu_k$ is *asymptotically stable* if and only if it is *finite-time stable*.

We are now in a position to state the second main result of this chapter.

Theorem 22 *Let (G,P) be a regular tiling of $\mathbb{R}^N$, and let $(A,B) \in \mathbb{Z}^{N\times N} \times \mathbb{R}^N$ be such that (H1) and (H2) are fulfilled with $\mathbb{R}^N/G' = \mathbb{T}^N$. Assume given $C \in \mathbb{Z}^{1\times N}$ such that (A,C) is similar over $\mathbb{Z}$ to a pair $(A^\flat, C^\flat)$ in a companion canonical form. Then one can pick two matrices $L \in \mathbb{Z}^{N\times 1}$ and $M \in \mathbb{Z}^{N\times 1}$ so that $(A-LC)M = 0$ and $CM = 1$. Furthermore*

$$X_k = \hat{X}_k \text{ and } u_k = Y_k - \hat{Y}_k \qquad \forall k \geqslant N+1.$$

Proof. Let T, $A^\flat$, $C^\flat$, L and $L^\flat$ be as in the proof of Proposition 21. Set $M^\flat = (1\ 0\ \cdots 0)'$ and $M = T^{-1}M^\flat$. Then $(A-LC)M = T^{-1}(A^\flat - L^\flat C^\flat)T \cdot T^{-1}M^\flat = 0$ by (3.23), and $CM = C^\flat T \cdot T^{-1}M^\flat = 1$. On the other hand, it follows from (3.21) and the choice of M that

$$e_{k+1} = (A-LC)e_k \qquad \forall k \in \{1,...,N\}$$

hence $e_{N+1} = (A-LC)^N e_1 = 0$. Since X_{N+1} and $\hat{X}_{N+1}$ belong to $\mathcal{T}'$ by construction, we have that $\hat{X}_{N+1} = X_{N+1}$. To complete the proof, it is sufficient to prove the following

Claim. For any $k \geqslant 0$, $\hat{X}_k = X_k$ implies $\hat{X}_{k+1} = X_{k+1}$.

Indeed, using the fact that $(A-LC)M = 0$ and $\hat{X}_k = X_k$ we obtain that

$$\begin{aligned} \hat{X}_{k+1} &= \varpi_k(A\hat{X}_k + LC(X_k + Mu_k - \hat{X}_k) + B) \\ &= \varpi_k(AX_k + AMu_k + B) \\ &= X_{k+1}. \end{aligned}$$

This completes the proof of Theorem 22. ■

Remark 23 *(i) The projection $\varpi_k(x)$ allows to switch between the dynamics (2.15) and (2.16) in $\mathbb{R}/G$ and $\mathbb{R}/G'$, respectively. For a dynamics in $\mathbb{T}^N$ only ($G' = G$), one can replace $\varpi_k(x)$ by $\varpi'(x)$ (the projection onto $[0,1)^N$).*

(ii) The result in Theorem 22 remains true if we take $\varpi_k(x) = \varpi'(x)$ for $k \leqslant N$ and $\varpi_k(x) = \varpi(x)$ for $k \geqslant N+1$. However, the definition of $\varpi_k(x)$ in (3.18) guarantees that a finite time synchronization occurs even if the output Y_k is not transmitted at some times. Such a property may be useful for the secured transmission of video sequences.

(iii) The output $Y_k = C(X_k + Mu_k)$ may be replaced by $\tilde{Y}_k = h(Y_k)$, where $h : \mathbb{R} \to \mathbb{R}$ is a nonlinear invertible map. This renders the analysis of the dynamics of Y_k much more complicated.

(iv) In practice, when $\mathbb{H} = \mathbb{T}^N$, the matrices A, C, L and M may be constructed in the following way. Pick any matrix $\hat{T} = [\hat{T}_{i,j}] \in \mathbb{Z}^{N\times N}$ with $\hat{T}_{i,j} = 0$ for $i > j$ and $\hat{T}_{i,i} = 1$ for all i. We set $T = \hat{T}'\,\hat{T}$. Note that $\det \hat{T} = \det T = 1$. Next, we pick a pair $(A^\flat, C^\flat)$ in a companion canonical form so that the roots of $\chi_{A^\flat}$ do not belong to the set $\{0\} \cup \{z \in \mathbb{C};\ |z| = 1\}$. Then A, C, L and M are defined by

$$A = T^{-1}A^\flat T, \quad C = C^\flat T, \quad L = T^{-1}A^\flat (C^\flat)', \quad \text{and} \quad M = T^{-1}(C^\flat)'.$$

3.3 Numerical simulations

This section is borrowed from [26]. Assume $\mathbb{H} = \mathbb{T}^3$ and consider the dynamical system $(\Sigma_{A,b,M,C})$ with

$$A = \begin{pmatrix} -19 & 26 & 7 \\ -51 & 65 & 17 \\ 152 & -184 & -47 \end{pmatrix}, \quad C = (6\ \ -5\ \ -1), \quad b = 0.$$

$(\Sigma_{A,b})$ is chaotic by virtue of Theorem 5, since $\det A = 3$ (hence $\det A \neq 0$) and the eigenvalues of A are -3, -0.4142, 2.4142 (A has no roots of unity as eigenvalues). The pair (A, C) is similar over $\mathbb{Z}$ to the pair $(A^\flat, C^\flat)$ in companion canonical form, where

$$A^\flat = \begin{pmatrix} -1 & 1 & 0 \\ 7 & 0 & 1 \\ 3 & 0 & 0 \end{pmatrix},\ C^\flat = (1\ 0\ 0) \text{ and } \quad T = \begin{pmatrix} 6 & -5 & -1 \\ -5 & 10 & 3 \\ -1 & 3 & 1 \end{pmatrix}.$$

According to Proposition 21, the unique matrix $L \in \mathbb{Z}^{N\times 1}$ such that $A - LC$ is Hurwitz is $L = T^{-1}L^\flat$, with $L^\flat = (-1\ 7\ 3)^T$. We obtain $L = (-2\ \ -6\ 19)^T$. The corresponding matrix $M \in \mathbb{Z}^{3\times 1}$ such that $(A - LC)M = 0$ and $CM = 1$ is $M = (1\ 2\ \ -5)^T$.
The information to be masked is a flow corresponding to integers ranging from 0 to 255. The data are scaled to give an input u_k ranging from 0 to 1, and are embedded into the chaotic dynamics of $(\Sigma_{A,b,M,C})$. From a practical point of view, the transmitted signal y_k cannot be coded with an infinite accuracy and so it has to be truncated for throughput purpose. The observer $(\hat{\Sigma}_{A,b,M,C})$ is used in order to recover the information. Numerical experiments bring out that the number of digits of the conveyed output can actually be limited without giving rise to recovering errors. The results reported in Fig. 7 show a perfect recovering for a number of digits of y_k equal to 4 (this is the minimum number required for perfect retrieving). The recovering error reaches zero after 3 steps, a fact which is consistent with above theoretical results on finite time synchronization ($N = 3$). The figure highlights the fact that even though the state reconstruction may not be perfect (residual errors due to truncations), a perfect information reconstruction is nevertheless achieved.

Remark 24 *Actually, for* any *system $\Sigma_{A,B,M,C}$, the numerical computations can be performed* in an exact way*, i.e. without rounding errors, provided that the number of digits is sufficiently large.*

3.4 Concluding remarks

The *message-embedding* masking technique studied here does not originate from the conventional cryptography (see [15] for a good survey). Nevertheless, it seems to be highly related to some popular encryption schemes, the so-called *stream ciphers* [19]. Therefore, it is desirable that the proposed scheme be robust against both statistical and algebraic attacks. On one hand, the robustness against statistical attacks follows from the chaotic behavior of the output. On the other hand, the security against algebraic attacks rests on the difficulty to identify the parameters of the system. The identification of the parameters is here a hard task for two reasons:

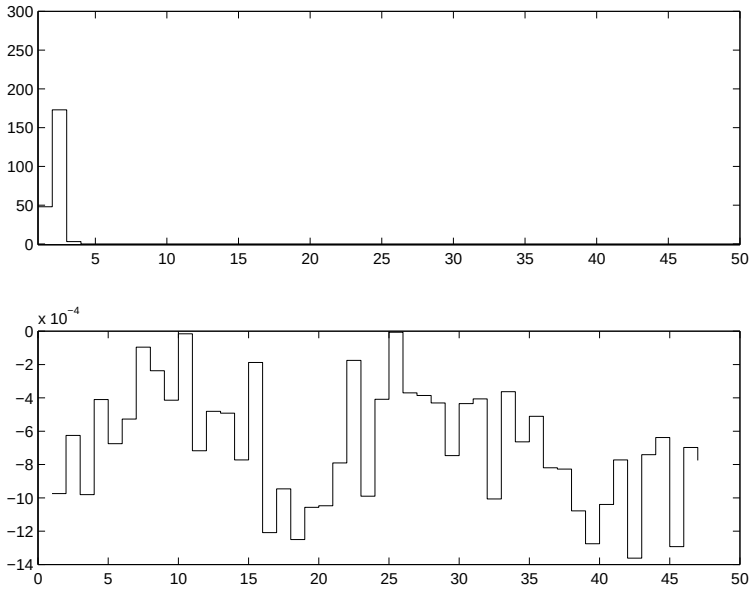

Figure 7: A : error on the recovered information $u_k - \hat{u}_k$; B : state reconstruction error $X_k - \hat{X}_k$

(i) The particular *structure* of the encryption system ($\Sigma_{A,B,M,C}$), that is the *dimension* of the matrix A and the tiling of the space used, is assumed to be unknown;

(ii) The ciphertext u_k actually results from a mixing between the plaintext m_k and the state X_k ($u_k = e(X_k, m_k)$). This generally results in a *nonlinear* dynamics ($\Sigma_{A,B,M,C}$), rendering the parameters hardly identifiable [12].

A real-time implementation has already been carried out on an experimental platform involving a secured multimedia communication. (For details about the platform, see e.g. [16]).

References

[1] J. Banks, J. Brooks, G. Cairns, G. Davis, and P. Stacey. On Devaney's definition of chaos. *Amer. Math. Monthly*, 99(4):332–334, 1992.

[2] M. Berger. *Geometry I*, Corrected Fourth Printing, Springer-Verlag, Berlin Heidelberg, 2009.

[3] I.I. Blekhman, E. Mosekilde, A. L. Fradkov, editors. *Special Issue on Chaos Synchronization and Control*, volume 58. Elsevier, 2002.

[4] V.D. Blondel, E. D. Sontag, M. Vidyasagar, and J. C. Willems. *Open Problems in Mathematical Systems and Control Theory*. Communication and Control Engineering. Springer Verlag, 1999.

[5] J.J. Burckhardt. *Die Bewegungsgruppen der Kristallographie*, Second Edition, Birkhäuser Verlag, Basel, 1966.

[6] R. Devaney. *An introduction to chaotic dynamical systems*. Studies in Nonlinearity. Westview Press, Boulder, CO, 2003. Reprint of the second (1989) edition.

[7] W. Greub. *Linear Algebra*, Fourth Edition, Graduate Texts in Mathematics, No. 23, Springer-Verlag, New-York, 1975.

[8] M. Hasler, M. Delgado-Restituto, and A. Rodriguez-Vasquez. Markov maps for communications with chaos. In *Proc. of the 1996's Nonlinear Dynamics in Electronic Systems, NDES'96*, pages 161–166, Sevilla, June 1996.

[9] A. Katok and B. Hasselblatt. *Introduction to the modern theory of dynamical systems*, volume 54 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1995. With a supplementary chapter by A. Katok and L. Mendoza.

[10] G. Kolumban, M. P. Kennedy, and L. O. Chua. The role of synchronization in digital communications using chaos - part I: Fundamentals of digital communications. *IEEE Trans. Circuits. Syst. I (Special issue on Chaos Synchronization and Control: Theory and applications)*, 44:927–936, October 1998.

[11] L. Kuipers and H. Niederreiter. *Uniform distribution of sequences*. Wiley-Interscience [John Wiley & Sons], New York, 1974. Pure and Applied Mathematics.

[12] L. Ljung and T. Glad. On global identifiability for arbitrary model parametrizations. *Automatica*, 30:265–276, 1994.

[13] R. Mañé. *Ergodic theory and differentiable dynamics*, volume 8 of *Ergebnisse der Mathematik and ihrer Grenzgebiete (3)* [Results in Mathematics and Related Areas (3)]. Springer-Verlag, Berlin, 1987. Translated from the Portuguese by Silvio Levy.

[14] J. L. Massey. *Contemporary cryptology: an introduction*. in : G.J. Simmons (Ed.), Contemporary Cryptology, IEEE Press, New York, 1992.

[15] A. J. Menezes, P. C. Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, October 1996.

[16] G. Millérioux, G. Bloch, J. M. Amigo, A. Bastos, and F. Anstett. Real-time video communication secured by a chaotic key stream cipher. In *Proc. of IEEE 16th European Conference on Circuits Theory and Design, ECCTD'03*, pages 245–248, Krakow, Poland, September 1-4 2003.

[17] G. Millérioux and J. Daafouz. An observer-based approach for input independent global chaos synchronization of discrete-time switched systems. *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl*, 50(10):1270–1279, 2003.

[18] G. Millérioux and J. Daafouz. Input independent chaos synchronization of switched systems. *IEEE Trans. on Automatic Control*, 49(7):1182–1187, July 2004.

[19] G. Millérioux, A. Hernandez, and J. M. Amigo. Conventional cryptography and message-embedding. In *Proc. of International Symposium on Nonlinear Theory and its Applications, NOLTA'2005*, Bruges, October 2005.

[20] H. Nijmeijer and I. M. Y. Mareels. An observer looks at synchronization. *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl*, 44:882–890, October 1997.

[21] L. M. Pecora and T. L. Carroll. Synchronization in chaotic systems. *Phys. Rev. Lett.*, 64:821–824, 1990.

[22] L. M. Pecora and T. L. Carroll. Driving systems with chaotic signals. *Phys. Rev. A*, 44(8):2374–2383, August 1991.

[23] L. M. Pecora, T. L. Carroll, G. Johnson, and D. Mar. Volume-preserving and volume-expanding synchronized chaotic systems. *Physical review E*, 56(5):5090–5100, November 1997.

[24] G. Rauzy. *Propriétés statistiques de suites arithmétiques*. Presses Universitaires de France, Paris, 1976. Le Mathématicien, No. 15, Collection SUP.

[25] L. Rosier, G. Millérioux, and G. Bloch. Chaos synchronization on the $N-$torus and cryptography. *Comptes Rendus Mécanique*, 332(12):969–972, 2004.

[26] L. Rosier, G. Millérioux, and G. Bloch. Chaos synchronization for a class of discrete dynamical systems on the N-dimensional torus, *Les prépublications de l'Institut Élie Cartan*, No. 23, 2004.

[27] L. Rosier, G. Millérioux, and G. Bloch. Chaos synchronization for a class of discrete dynamical systems on the N-dimensional torus. *Systems & Control Letters*, 55:223–231, 2006.

[28] R. Rovatti and G. Setti. On the distribution of synchronization times in coupled uniform piecewise-linear Markov maps. *IEICE Transactions on Fundamentals*, 81(9):1769–1776, 1998.

[29] R. Schmitz. Use of chaotic dynamical systems in cryptography. *Journal of the Franklin Institute*, 338:429–441, 2001.

[30] Special Issue. Chaos synchronization and control: theory and applications. *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl*, 44(10):853–1039, 1997.

[31] Special Issue. Control of chaos and synchronization. *Syst. Control Letters*, 31:259–322, 1997.

[32] Special Issue. Control and synchronization of chaos. *International Journal of Bifurcation and Chaos*, 10(4), 2000.

[33] M.A. van Wyk and W.-H. Steeb. *Chaos in electronics*, volume 2 of *Mathematical Modelling: Theory and Applications*. Kluwer Academic Publishers, Dordrecht, 1997

[34] E. Vesentini. An introduction to topological dynamics in dimension one. *Rend. Sem. Mat. Univ. Politec. Torino*, 55(4):303–357,1999. Jacobian conjecture and dynamical systems (Torino, 1997).

[35] P. Walters. *An introduction to ergodic theory*, volume 79 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982.

[36] J.A. Wolf. *Spaces of constant curvature*, Fifth Edition, *Publish or Perish, Inc.* Wilmington, Delaware, 1984.