Combining chaotic dynamical systems using the fuzzy logic XOR operator.

Dr Rezki Chemlal [(1)] **and Dr Hacene Gharout** [(2)]

[(1,2)]Laboratoire de Mathématiques Appliquées, Faculté des Sciences Exactes,
Université de Bejaia, 06000 Bejaia, Algeria.
[(1)] rezki.chemlal@univ-bejaia.dz
[(2)] hacene.gharout@univ-bejaia.dz

Abstract
In this paper we explore whatever combining two chaotic dynamical systems using the fuzzy logic operator XOR can maintain or not the chaotic properties of the resulting dynamical system. This study is motivated by techniques used in applications to secure communications ,images encryption and cryptography.
Key words : Chaos, fuzzy logic, ergodic theory, full branch.

I INTRODUCTION

Chaotic dynamical systems are commonly used as models in a wide range of applications, cryptography [6, 1, 11, 13] image and speech encryption and retrieval [8, 7, 10, 2] and achievement of associative memory properties [4, 3, 5].

Extreme sensitivity to initial conditions is an interesting property of chaotic systems. This property makes chaotic systems a worthy choice for constructing cryptosystems or for image encryption.

Another idea is to mix two or more chaotic dynamical systems to gain more "unpredictably" in order to enhance encryption process [9, 7, 8].

We ask ourselves this question, whatever combining two chaotic dynamical systems permits to maintain chaotic property of the resulting one ? In particular whatever combining two chaotic dynamical systems by fuzzy logic operators, mainly the xor operator gives rise to a chaotic dynamical system.

In this paper we restrict our study to the xor operator this operator is widely suggested in literature although other operators have been considered and studied such as the exponential function [8].

In other words consider two chaotic dynamical systems (I, F) and (I, G) is the dynamical system $(I, F\ xor\ G)$ still chaotic?

We studied some combination of known chaotic dynamical systems and checked whatever the combination using xor operator is still chaotic or not. This gave us some preliminary remarks about how to combine chaotic dynamical systems in order to maintain the chaotic properties of the resulting dynamical system.

We provide a sufficient condition to check if the combination has chances to succeed. Rather than the popular Lyapunov exponents method used almost systematically in the applied mathematics literature we use a tool provided by ergodic theory [12].

II DYNAMICAL SYSTEMS

2.1 Topological dynamics

A dynamical system (X, F) consists of a compact metric space X and a continuous self–map F .

A point x is said periodic if there exists $p > 0$ with $F^p(x) = x$. The least p with this property is called the period of x. A point x is eventually or ultimately periodic if $T^m(x)$ is periodic for some $m \geq 0$.

In the same way a dynamical system is said periodic if there exists $p > 0$ with $F^p(x) = x$ for every $x \in X$ and eventually periodic if F^m is periodic for some $m \geq 0$.

A point $x \in X$ is said to be an equicontinuity point, or to be Lyapunov stable, if for any $\epsilon > 0$, there exists $\delta > 0$ such that if $d(x, y) < \delta$ one has $d(F^n(y), F^n(x)) < \epsilon$ for any integer $n \geq 0$.

We say that (X, F) is sensitive if for any $x \in X$ we have :

$$\exists \epsilon > 0, \forall \delta > 0, \exists y \in B_\delta(x), \exists n \geq 0 \text{ such that } d(F^n(y), F^n(x)) \geq \epsilon.$$

We say that (X, T) is expansive if we have :

$$\exists \epsilon > 0, \forall x \neq y \in X, \exists n \geq 0, d(F^n(x), F^n(y)) \geq \epsilon.$$

A dynamical system (X, T) is transitive if for any nonempty open sets $U, V \subset A^{\mathbb{Z}}$ there exists $n > 0$ with $U \cap F^{-n}(V) \neq \emptyset$. This is equivalent to the existence of a point with a dense orbit.

A dynamical system is said topologically mixing if for any nonempty open sets $U, V \subset A^{\mathbb{Z}}, U \cap F^{-n}(V) \neq \emptyset$ for all sufficiently large n.

Let (X, F) be a dynamical system, endow the set X with a sigma algebra $\mathbb{B}$. The function F preservers some measure μ on the sigma algebra $\mathbb{B}$ iff for every $B \in \mathbb{B}$ we have $\mu(F^{-1}(B)) = \mu(B)$. We say then that $(X, \mathbb{B}, F, \mu)$ is a measurable dynamical system.

The topological support of a measure is defined as the set of all points $x \in X$ for which every open neighborhood of x has positive measure.

A dynamical system $(X, \mathbb{B}, F, \mu)$ is ergodic if every invariant subset of X is either of measure 0 or of measure 1. Equivalently, if for any measurable $U, V \subset X$, there exists some $n \in \mathbb{N}$ such that $\mu(U \cap F^{-n}(V)) > 0$.

If a dynamical system is ergodic then it is transitive on the topological support of the measure.

For dynamical systems defined on the interval a common used measure is the Lebesgue measure, the topological support of the Lebesgue measure is $\mathbb{R}$.

2.2 Chaotic dynamical systems on the interval

Dynamical systems defined on the interval have a particular behavior, a rich literature is devoted to the subject, we will recall here some results about their properties.

In matter of chaos The Devaney's chaos is seen as a combination of unpredictably (sensitivity) and regular behaviors (periodic points), transitivity ensuring that the system is undecomposable.

Definition 1:
A topological dynamical system (X, f) is chaotic in the sense of Devaney if :
(1) Is transitive.
(2) The set of periodic points is dense in X.
(3) Is sensitive to initial conditions.

It is know that for every dynamical system the conditions (1) and (2) implies the condition (3) which lead to the so called modified Devaney definition of chaos which rather uses only conditions (1) and (2).

For interval maps transitivity is enough to imply the other two conditions.

Proposition 1:
An interval map is chaotic in the sense of Devaney if and only if it is transitive.

For the proof of this result you can look at [14].

III RESULTS

3.1 Preliminary remarks

One issue when using the fuzzy logic xor operator is preserving the invariance of the resulting dynamical system if we want to combine two dynamical systems they must be defined on the same interval but this is not enough to ensure invariance of the resulting combined dynamical system.

If the two dynamical systems are defined on the interval $[0, 1]$ it is easy to show that the result will be invariant on the interval $[0, 1]$. One solution to overcome the problem of the invariance is to rescale every dynamical system defined on a given interval to $[0, 1]$.

Below we give two examples the first one of an xor combination of two chaotic dynamical systems which is not chaotic and the second one where the result is a chaotic dynamical system.

Example 2:
Let us consider the two dynamical systems $([0, 1], f_r)$ and $([0, 1], T)$ where f_r and T are the logistic map and the tent map respectively.

$$f_r(x) = r.x.(1-x), T(x) = \begin{cases} -2x+1, 0 \leq x \leq 0.5 \\ 2x-1, 0.5 \leq x \leq 1 \end{cases}$$

These two dynamical systems are well known chaotic systems , let us consider their fuzzy xor combination H defined by

$$H(x) = \max(f_r(x), T(x)) - \min(f_r(x), T(x))$$

It possesses two fixed points, the fixed point 0 is unstable while the fixed point 0.23 is asymptotically stable. The basin of attraction of the point 0 contains 4 isolated points while the basin of attraction of 0.23 contain the hole interval except the basin of attraction of 0.

Example 3:
Consider the two following dynamical systems the two dynamical systems $([0,1], T)$ and $([0,1], ST)$ where T is the tent map and ST the map defined by

$$ST(x) = \begin{cases} -2x+1 : 0 \leq x \leq \frac{1}{2} \\ 2x-1 : \frac{1}{2} \leq x \leq 1 \end{cases}$$

The graph of the function ST is as an inverted Tent map graph. The map ST is chaotic as the point $\frac{\pi}{3.5}$ has a dense orbit. The map $T\ xor\ ST$ is chaotic .

3.2 Initial numerical investigation summary

Along with the two examples shown before we have tested some other dynamical systems, part of the results is shown in the following table :

xor	Doubling map B	Cubic map C	map f_r	Tent map T	Inverted Tent map ST
Doubling map B	.....	Non chaotic	Non chaotic	Non chaotic	Non chaotic
Cubic map C	.....	.....	Non chaotic	Non chaotic	Non chaotic
Logistic map f_r	.....	.....	.....	Non chaotic	Chaotic
Tent map T	.....	.....	.....	.....	Chaotic
Inverted Tent map ST	.....	.....	.....	.....	.....

We recall below the definitions of the classical and less classical maps used throughout this paper:

Map name	Doubling map B	Cubic map C	Logistic map $f_r(x)$
Expression	$2x\ mod(1)$	$16x^3 - 24x^2 + 9x$	$r.x.(1-x)$
Map name	Tent map T	Inverted Tent map ST	
Expression	$\begin{cases} -2x+1, 0 \leq x \leq 0.5 \\ 2x-1, 0.5 \leq x \leq 1 \end{cases}$	$\begin{cases} -2x+1 : 0 \leq x \leq \frac{1}{2} \\ 2x-1 : \frac{1}{2} \leq x \leq 1 \end{cases}$	

The observation of the results of the table suggests that combining two dynamical systems using the xor operator leads to the resulting dynamical system to be chaotic if their graphs have some form of symmetry to the horizontal line $y = \frac{1}{2}$.

3.3 Mirror effect and number of full branches

The aim of this section is to come with some criterion choice. The optimal situation is that the two dynamical systems have to be symmetrical to the horizontal line $y = \frac{1}{2}$ this is what we will call a mirror effect. In this situation we can show that the combination is a chaotic dynamical using tools from ergodic theory.

Definition 2:
Let $I \subset \mathbb{R}$ be an interval. A map $f : I \to I$ is a full branch map if there exists a finite or countable partition $\mathcal{P}$ of I into subintervals such that for each $w \in \mathcal{P}$ the map $f|_{int(w)} : int(w) \to int(I)$ is a bijection.
A map f is a piecewise continuous (resp $C^1, C^2, affine$) full branch map if for each $w \in \mathcal{P}$ the map $|f_{int(w)} : int(w) \to int(I)$ is a homeomorphism (resp C^1 diffeomorphism, C^2 diffeomorphism, affine).

Definition 3:
A full branch map has bounded distortion if

$$\sup_{n\in\{1,2\}} \sup_{w^{(n)}\in\mathcal{P}^{(n)}} \sup_{x,y\in w^{(n)}} \log \left| Df^{(n)}(x) / Df^{(n)}(y) \right| < \infty$$

here (n) stands for the nth derivative.

If the function is piecewise affine then the distortion is 0.

Theorem 4:
Let $f : I \to$I be a full branch map with bounded distortion. Then Lebesgue measure is ergodic.

For the proof of this result you may look at [12]

Example 5:
The tent map, the doubling map and the logistic map have two full branches with bounded distortion, the cubic map have three full branches with bounded distortion.

Proposition 6:
Consider $([0,1], f)$ and $([0,1], g)$ two dynamical systems, suppose that the graphs of f and g are symmetrical according to the horizontal line $y = \frac{1}{2}$ and that the number of full branches of f and g are equal to k.
The dynamical system $([0,1], f\ xor\ g)$ has $2k$ full branches hence is chaotic.

Proof:
Suppose that we have a partition $\mathcal{P}$ of $[0,1]$ into subintervals such that for each $w \in \mathcal{P}$ the map $f|_{int(w)} : int(w) \to]0,1[$ is a bijection.
As g is a mirror of f we obtain by symmetry

$$(f\ xor\ g)(x) = \begin{cases} 2|f(x) - 0.5| & if\ f(x) \leq 0.5 \\ 2|f(x) - 0.5| & if\ f(x) \geq 0.5 \end{cases}$$

As f is a bijection there is a partition $w = w_1 \cup w_2$ such that :

$$\begin{aligned}(f\ xor\ g)(x) &= \begin{cases} 2\left|f(x) - 0.5\right| & if\ x \in w_1 \\ 2\left|f(x) - 0.5\right| & if\ x \in w_2 \end{cases} \\ &\Rightarrow \begin{cases} (f\ xor\ g)(w_1) =]0,1] \\ (f\ xor\ g)(w_1) =]0,1[\end{cases}\end{aligned}$$

Thus $f\ xor\ g$ has two full branches on w.

Example 7:
Let us consider the chaotic cubic map $([0,1], C)$ where

$$C(x) = 16x^3 - 24x^2 + 9x.$$

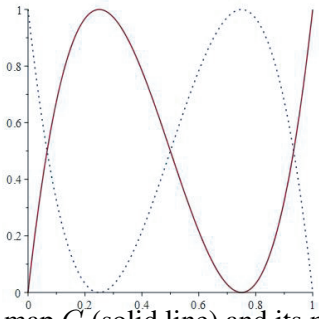

Figure 1: The cubic map C (solid line) and its mirror CM (points)

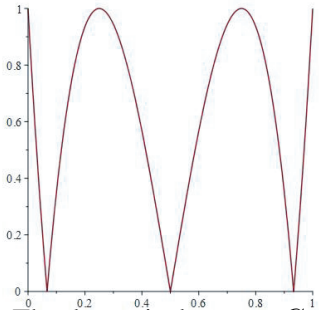

Figure 2: The dynamical system C xor CM

The partition $\left\{\left[0, \frac{1}{4}\right], \left[\frac{1}{4}, \frac{3}{4}\right], \left[\frac{3}{4}, 1\right]\right\}$ satisfies the conditions of the precedent definition, hence the cubic map is of three full branches. Its mirror CM has also three full branches (see the figure 1) .
The figure 2 is the graph of the function $C\ xor\ CM$ with six full branches.

Proposition 8:
Consider $([0,1], f)$ and $([0,1], g)$ two dynamical systems, suppose that the graphs of f and g are symmetrical according to the horizontal line $y = \frac{1}{2}$ and that f and g have the full branch property then $f\ xor\ g$ is chaotic .

Proof:
Suppose that f has k branches then $f\ xor\ g$ has $2k$ branches and a relevant partition w.
As the graph of g is symmetrical to the graph of f then they have the same distortion.
On each branch of the partition we have

$$\sup_{n\geq 1}\sup_{w^{(n)}\in\mathcal{P}^{(n)}}\sup_{x,y\in w^{(n)}}\log\left|D\left(f\ xor\ g\right)^{n}(x)/D\left(f\ xor\ g\right)^{n}(y)\right|\leq$$
$$\max\left(\begin{array}{l}\sup_{n\geq 1}\sup_{w^{(n)}\in\mathcal{P}^{(n)}}\sup_{x,y\in w^{(n)}}\log\left|Df^{(n)}(x)/D\left(f\right)^{n}(y)\right|\\ ,\sup_{n\geq 1}\sup_{w^{(n)}\in\mathcal{P}^{(n)}}\sup_{x,y\in w^{(n)}}\log\left|D\left(g\right)^{n}(x)/D\left(g\right)^{n}(y)\right|\end{array}\right)$$

Hence $f\ xor\ g$ is a full branch map with bounded distortion. Then the Lebesgue measure is ergodic [12].
As the Lebesgue measure is ergodic then f xor g is transitive on the topological support of the Lebesgue measure which is the whole interval. Hence it is chaotic.

Remark 9:
The two maps do not need to be perfectly symmetrical to each other.
Consider the cubic map and the map defined by

$$f(x)=\begin{cases}-4x+1, & 0\leq x\leq 0.25;\\ 2x-0.5, & 0.25\leq x\leq 0.75;\\ 4x-4, & 0\leq x\leq 1.\end{cases}$$

This map has been defined just by mirroring maximum and minimum points of the Cubic map to the line $y=\frac{1}{2}$. The result give us a 6 full branches map as shown in the figure 3 and the figure 4.

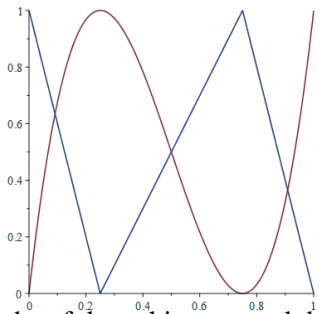

Figure 3: Graphs of the cubic map and the function f.

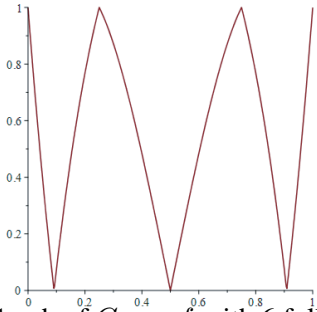

Figure 4: Graph of $C\ xor\ f$ with 6 full branches.

IV CONCLUSION

We investigated an ideal situation to combine chaotic one dimensional maps using the fuzzy logic xor operator.

Using tools from ergodic theory we were able to establish a result using slightly strong condition than Devaney's chaos, it is worth noting that this condition is satisfied by a majority of classical chaotic maps on the interval used in applications.

Acknowledgement 10:
We acknowledge support of "Direction Générale de la Recherche Scientifique et du Développement Technologique DGRSDT. MESRS, Algeria.

REFERENCES

[1] Baptista M. S. Cryptography with chaos, Baptista M. S. Physics Letters A. – 240(1-2). - 1998. – P. 50–54.

[2] R. Chemlal, I Djellit, Coding Information and Problems of storage in Dynamical Systems, FACTA UNIVERSITATIS, SER ELEC ENERG, Vol 17, December 2004, 355-363.

[3] Dmitriev A. S. "Storing and Recognizing Information with One-Dimensional Dynamic Systems" (In Russian). Radiotechnika i Elektrononika (1991), vol. 36, n°1, pp 101-108.

[4] A.A. Dmitriev Design of Message-Carrying Chaotic Sequences 2002 Nonlinear Phenomena in Complex Systems.

[5] H. K. Kwan,Three Layer Bi directional asymmetrical associative memory IEEE 2003.

[6] Kocarev L. Chaos-based cryptography: A brief overview, IEEE Circuits and Systems Magazine. 2001. N°1. P.6–21.

[7] Mykola Kushnir, Yuriy Fedkovych, Petro Kroialo, Hryhorii Kosovan. Encryption of the Images on the Basis of Two Chaotic Systems with the Use of Fuzzy Logic. 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET).

[8] S. Mokhnache, M. E. H. Daachi, T. Bekkouche, and N. Diffellah, "A Combined Chaotic System for Speech Encryption", Eng. Technol. Appl. Sci. Res., vol. 12, no. 3, pp. 8578–8583, Jun. 2022.

[9] N.K. Pareek a,b, Vinod Patidar. Cryptography using multiple one-dimensional chaotic maps , K.K. Sud. Communications in Nonlinear Science and Numerical Simulation 10 (2005) 715–723

[10] S.Rouabhi ”Storage of Information in One Dimensional Piecewise Continuous Maps” International Journal of Bifurcation and Chaos. (2000) vol 10(5) pp 1127-1137.

[11] Schwarz W. D. Chaos and cryptography / Schwarz W. D., Dachselt W. IEEE Trans. Circuits Syst. I. – 48 (12). - 2001.1498–1509.

[12] S.Luzzato,Introduction to smooth ergodic theory, available online at https://indico.ictp.it/event/a12289/session/2/contribution/1/material/0/0.pdf

[13] P.G. Vaidya , S. Angadi, Decoding chaotic cryptography without access to the superkey, , Chaos, Solitons and Fractals 17 (2003) 379–386.

[14] M. Vellekoop and R. Berglund. On intervals, transitivity = chaos. Amer. Math. Monthly,101(4):353-355, 1994.