Exact and asymptotic synchronization of a new weakly coupled maps system

Sebastien Hénaff, Ina Taralova, René Lozi

Journal of Nonlinear Systems and Applications (2009) 1–1

http://www.watam.org/JNSA/

EXACT AND ASYMPTOTIC SYNCHRONIZATION OF A NEW WEAKLY COUPLED MAPS SYSTEM

Sébastien Hénaff, Ina Taralova and René Lozi *†

Abstract. The paper deals with the synchronization of a new statistically highly performant function firstly introduced by Lozi. The synchronization is reached via observers which reconstruct all the states of the original system, using only a partial information of it. The map has been rewritten as a piece-wise affine one, which allows to design two types of observers: an exact (dead-beat) observer, and an asymptotic observer. Both observers have been analysed and compared; the dead-beat observer guarantees an exact convergence; however, synchronization can not be preserved in an autonomous regime (if the observer is switched off), because the map is highly chaotic, and the trajectories diverge due to the finite computer precision. The asymptotic observer is more robust in case of noise, but the convergence is slower, and the error converges to zero only asymptotically. In the latter case, several observers have to run in parallel, and the criteria to select the converging one are derived.
Keywords. chaos, synchronization, discrete-time, observer, pseudo-random generators.

1 Introduction

Chaos has recently received a growing interest in various fields of science and engineering, and in particular, in secure communications. Several chaotic cryptographic schemes have been proposed since [1], [2] and can be classified in three main categories : chaotic masking, chaotic modulation and chaotic shift keying.

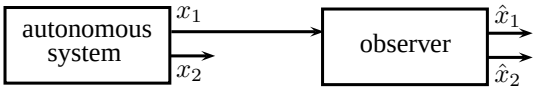
In the cryptographic application, the chaotic generator must exhibit appropriate features close to those of the pseudo-random generators. These adapted properties have been studied more precisely in [3], [4], [5].

Further researchers have then looked for finding appropriate systems testing different architectures : traditional chaotic maps (for example, the logistic map, the Hénon map, the generalized Hénon map) [6], piece-wise linear map, cascaded map [7] or coupled map lattice. In order to evaluate the features of the system, statistical tests developed for random and pseudo-random number generators (RNG and PRNG) can also be applied to chaotic maps, in order to gather evidence that the map generates "good" chaotic signals, i.e. having a considerable degree of randomness [3] [5].

It appears that most of the maps classically used for chaotic encryption do not pass successfully these tests, and don't exhibit the required features. However, most of the papers dealing with synchronization and observer synthesis consider precisely these kinds of maps, highly inefficient in the context of chaotic encryption. Unlike these models, Lozi introduced in 2008 a new ultra weakly coupled maps system [8] to generate pseudo-random signals which exhibits very good statistical properties.

Synchronization of chaotic systems has received a great interest since the pioneer work of Pecora and Carroll [9] and its application to secure communications attracted lots of works. There are two ways of achieving synchronization: it can be done by the inverse system [10] or by applying observers [11] [12]. Observers allows to reconstruct all the states of a system only with few components of it as shows figure 1. An overview of observers in the case of secure communications process is avaible in [13]

Figure 1: Observer



Our previous works on the new weakly coupled map function introduced by Lozi in 2008 [8] demonstrated its excellent statistical and spectral properties [14]; two kinds of observers have been proposed for the synchronization of the system: an inverse lag, and an exact observer. The latter consisted of 16 sub-observers which had to run in parallel in order to guarantee the exact convergence of one of them.

In comparison with these works, the present paper deepens and completes the previous results on exact observers, in particular by taking into account and exploiting the degrees of freedom in the choice of the observation matrices. The implementation issue related to the finite machine precision and its impact on the exact synchronization in the case of hyperchaotic maps is also discussed.

*Sébastien Hénaff and Ina Taralova are with Institut de Recherche en Communications et Cybernétique de Nantes IRCCyN UMR CNRS 6 597, École Centrale de Nantes, France. E-mails: sebastien.henaff@irccyn.ec-nantes.fr, ina.taralova@irccyn.ec-nantes.fr

†René Lozi is with Laboratoire J. A. Dieudonné UMR CNRS 6 621, Université de Nice Sophia-Antipolis, France. E-mail: r.lozi@unice.fr

In addition, this paper presents also the novel analytical and numerical results of the asymptotic synchronization of the weakly coupled map system. Indeed, the exact observers fail in the case of applications when (different kinds of) noise exist and has to be taken into account, but this problem can be successfully dealt with by the design of asymptotic observers.

This paper is organised as follows: after the presentation of the position of the problem in section two, section three analyses the observability of the system under consideration. Two types of observers are then designed in section four for exact convergence and asymptotic convergence. The problem of numerical synchronization is also discussed. A concluding section ends the paper.

2 Position of the problem

Lozi recently introduced a hyper chaotic system which generates signal with statistical features [8] competitive with the classical RNG. The aim of this work concerns the design of an observer of this particular system. Some preliminary results are available in [15]. A particular design of observers for the exact convergence is also available in [14]. This paper expands the previous results on exact observers analysis and deals with an additional problem: the asymptotic convergence and implementation aspects.

The system under consideration presented in [8] is composed by a chaotic weakly coupled map. The N-th order function f can be written as:

$$x(n+1) = f(x(n)) = A\ \Lambda(x(n))$$

with $x(n) = (x_1(n), x_2(n), \ldots, x_N(n))$
where A is a NxN matrix defined by:

$$A = A_a + A_b$$

$$A_a = \begin{pmatrix} \epsilon_1 \\ \epsilon_2 \\ \vdots \\ \epsilon_N \end{pmatrix} \begin{pmatrix} 1 & 1 & \ldots & 1 \end{pmatrix}$$

$$A_b = (N-1) \begin{pmatrix} \epsilon_1 & 0 & \ldots & 0 \\ 0 & \epsilon_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \epsilon_N \end{pmatrix}$$

and Λ is the tent function applied to each component of $x \in [-1;1]^N$:

$$\Lambda(x(n)) = \begin{pmatrix} \Lambda(x_1(n)) \\ \Lambda(x_2(n)) \\ \vdots \\ \Lambda(x_N(n)) \end{pmatrix}$$

$$\Lambda(x) = \begin{cases} 2x+1 & \text{if } x < 0 \\ -2x+1 & \text{else} \end{cases}$$

ϵ_i are positive parameters smaller than $1/(n-1)$.

Since the function is piece-wise affine, it can be rewritten under a matrix form, by rewriting the tent map. For the second order, the general system f is then governed by :

$$x(n+1) = 2A_i x(n) + B$$

where matrix A_i can take four possible values according to the regions of definition:

$$A_i = \begin{cases} A_1 & \text{if } x \in [0;1]^2 \\ A_2 & \text{if } x \in [-1;0] \times [0;1] \\ A_3 & \text{if } x \in [-1;0]^2 \\ A_4 & \text{if } x \in [0;1] \times [-1;0] \end{cases}$$

$$A_1 = \begin{pmatrix} -(1-\epsilon_1) & -\epsilon_1 \\ -\epsilon_2 & -(1-\epsilon_2) \end{pmatrix}$$

$$A_2 = \begin{pmatrix} 1-\epsilon_1 & -\epsilon_1 \\ \epsilon_2 & -(1-\epsilon_2) \end{pmatrix}$$

$$A_3 = \begin{pmatrix} 1-\epsilon_1 & \epsilon_1 \\ \epsilon_2 & 1-\epsilon_2 \end{pmatrix}$$

$$A_4 = \begin{pmatrix} -(1-\epsilon_1) & \epsilon_1 \\ -\epsilon_2 & 1-\epsilon_2 \end{pmatrix}$$

$$B = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Then, the output is defined by:

$$\begin{cases} x(n+1) = f(x(n)) \\ y(n) = Cx(n) \end{cases}$$

with $C = \begin{pmatrix} 1 & 0 \end{pmatrix}$

3 Observability

Observers allow the reconstruction of the evolution of a multi-component state thanks to a partial information, the output signal. But not all systems allow the realisation of this process: it must exhibit some particular features which are studied in detail by observability. It can be divided into two classes: global observability and local one. Global observability ensures that a given output describes only one internal state whereas local observability indicates that two closed states can be distinguished by the output.

3.1 Second order system

Local observability of the second order system has been studied in [14]. As we shall need it further on, the result is recalled here. An affine system can be written as :

$$\begin{cases} x(n+1) = f(x(n)) = A.x(n) + B \\ y(n) = Cx(n) \end{cases}$$

The function is piece-wise affine, then the matrix A can be re-written in a generic form by:

$$A_n = \begin{pmatrix} (1-\epsilon_1)s_{10} & \epsilon_1 s_{20} \\ \epsilon_2 s_{10} & (1-\epsilon_2)s_{20} \end{pmatrix}$$

where

$$s_{ij} = \begin{cases} 2 & \text{if } x_i(j) < 0 \\ -2 & \text{else} \end{cases}$$

A second order affine system is observable if its observability matrix is a full-rank one :

$$O = \begin{pmatrix} C \\ CA \end{pmatrix}$$

Here, the system is piece-wise affine, therefore the observability matrix shall be different according to the region to which belongs the system state. It is equal to:

$$O = \begin{pmatrix} 1 & 0 \\ 2(1-\epsilon_1)s_{10} & 2\epsilon_1 s_{10} \end{pmatrix}$$

which is full-rank since $\epsilon_1 > 0$ from the definition of the system. Therefore, the system is locally observable for all parameters and for all states, which is not the case of all systems. For example, the third order system is not locally observable for all configurations.

3.2 Third order system

A second order system needs the use of at least two iterations to determine weather this system is observable or not. Equivalently, at least, three iterations are necessary for a three order system. The observability matrix is:

$$O = \begin{pmatrix} C \\ CA \\ CA^2 \end{pmatrix}$$

The third order system is defined by the equation:

$$\begin{pmatrix} x_1(n+j+1) \\ x_2(n+j+1) \\ x_3(n+j+1) \end{pmatrix} = A_j \begin{pmatrix} x_1(n+j) \\ x_2(n+j) \\ x_3(n+j) \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

with:

$$A_j = \begin{pmatrix} (1-2\epsilon_1)s_{1j} & \epsilon_1 s_{2j} & \epsilon_1 s_{3j} \\ \epsilon_2 s_{1j} & (1-2\epsilon_2)s_{2j} & \epsilon_2 s_{3j} \\ \epsilon_2 s_{1j} & \epsilon_2 s_{2j} & (1-2\epsilon_2)s_{3j} \end{pmatrix}$$

By replacing these values, it comes:

$$O = \begin{pmatrix} 1 & 0 & 0 \\ (1-2\epsilon_1)s_{10} & \epsilon_1 s_{20} & \epsilon_1 s_{30} \\ a s_{11} & b\epsilon_1 s_{21} & c\epsilon_1 s_{31} \end{pmatrix}$$

with

$$\begin{cases} a = (1-2\epsilon_1)^2 s_{10} + \epsilon_1(\epsilon_2 s_{20} + \epsilon_3 s_{30}) \\ b = s_{10}(1-2\epsilon_1) + s_{20}(1-2\epsilon_2) + \epsilon_3 s_{30} \\ c = s_{10}(1-2\epsilon_1) + \epsilon_2 s_{20} + s_{30}(1-2\epsilon_3) \end{cases}$$

Out of singularity parameter region, that means $\epsilon_2 \neq \epsilon_3$, $3\epsilon_2 + 3\epsilon_3 \neq 4\epsilon_1$ and $4\epsilon_1 + 3\epsilon_2 + 3\epsilon_3 \neq 4$, this matrix is a full rank one for all possible s_{ij}. Then, the system is globally observable for all states in the whole phase plane if the parameter combination respects the above conditions.

4 Observer analysis

The aim of an observer is to recover a complete dynamics evolution thanks to a partial information only.

Since the considered system is piece-wise affine, the present section designs a piece-wise linear observer which would synchronise its dynamics with the original system and it is suitable to apply a Luenberger observer [16]. But the application of this observer supposes that the observer exactly "knows" how the states trajectories evolve and switch from one region to another, which is not the case. For this reason, some criteria have to be defined to identify the evolution of the state trajectories. But first of all, some adapted observers would be presented in this section, before caring out numerical applications and dealing with the criteria for exact and asymptotic convergence.

Before presenting the observer, the second order system should be rewritten under an affine form on each of the four domains where it is defined :

$$\begin{cases} x(n+1) = F(x(n)) = A.x(n) + B \\ y(n) = Cx(n) \end{cases}$$

$$\begin{cases} x(n+1) = \begin{pmatrix} (1-\epsilon_1)s_{10} & \epsilon_1 s_{20} \\ \epsilon_2 s_{10} & (1-\epsilon_2)s_{20} \end{pmatrix} x(n) + B \\ y(n) = \begin{pmatrix} 1 & 0 \end{pmatrix} x(n) \end{cases}$$

with $B = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

The Luenberger observer can be applied on a linear system. The observer is then defined as:

$$\hat{x}(n+1) = \hat{A}\hat{x}(n) + B + K(C\hat{x}(n) - y(n))$$

K is a predefined gain such that the error e, defined by $e = \hat{x} - x$, tends to zero. Let consider $\hat{x}(n)$ and $x(n)$ belonging to the same region of definition. In this case, $\hat{A} = A$ and therefore,

$$e(n+1) = (A + KC)e(n)$$

The value of the vector K determines the eigenvalues of the error matrix $(A + KC)$ and its speed of convergence: zero eigenvalues would imply that the observer converges in finite number of iterations whereas singular values less than one would impose an asymptotic convergence.

4.1 Exact or dead-beat observer

4.1.1 Analytical convergence

Hereafter, we deal with the second order system. One can identify the values of the gain K which cancel the eigenvalues of the matrix $(A+KC)$ as a function of the affine system model. In this case, since the matrix is of second order, $(A+KC)^2 = 0$ therefore if the system states x and its estimates $\hat{x}$ belong to the same region of the state space twice consecutively, the estimate shall synchronise with the original system in two steps.

This will ensure that if the dynamics falls into the same region twice consecutively, then the convergence is guaranteed. However, the observer should also synchronise when the state trajectories switch from one region of definition to another. The solution of vectors K that satisfy the synchronization has been found previously in [14]: for all $(i_1, i_2) \in [\![1;4]\!]$, there exist infinite vectors K_{j1} and K_{j2} such that $(A_{i1}+K_{j1}C)(A_{i2}+K_{j2}C) = 0$. For example, for $i_1 = i_2 = 1$, a formal resolution of the equation led to the following result:

$$K_{i1} = \begin{pmatrix} 2(2-\epsilon_1-\epsilon_2) \\ -2\frac{1-2\epsilon_2+\epsilon_2^2+\epsilon_1\epsilon_2}{\epsilon_1} \end{pmatrix}$$
$$K_{i2} = \begin{pmatrix} p \\ \frac{-2+p+2\epsilon_1+2\epsilon_2-p\epsilon_2}{\epsilon_1} \end{pmatrix}$$
$$\text{for } x(n) \in [0;1]^2 \text{ and } x(n+1) \in [0;1]^2$$

where p is a number arbitrarily chosen. In this paper, we go in-depth and enhance the previous studies on exact convergence, which did not consider the degree of freedom in the choice of K. Here, this degree of freedom shall be exploited as shown in the following section.

4.1.2 Implementation aspects

The previous development allows to synchronise exactly the states of the autonomous system in two iterations. This can be obtained by an ideal system but it is known that all processors represent the numbers with a finite precision so the calculation of an operation does not give the exact result and this approximation would not allow to synchronise perfectly. This section deals with the implementation problems and simulates numerically the synchronization. To design the final observer, some others are simulated to approach it step by step. All the simulations are performed under the parameters: $\epsilon_1 = 0.2$ and $\epsilon_2 = 0.1$.

Consider the autonomous piece-wise affine system:

$$\begin{cases} x(n+1) = f(x(n)) \\ y(n) = Cx(n) \end{cases}$$

From the analytical results, it comes that the synchronization can been achieved in two iterations, after what both observer and original autonomous system have the same dynamics and they evolve identically. In this first simulation, the observer system is then designed in two steps: the Luenberger observer is used for the two first iterations before leaving its states evolving autonomously. The following system is then only used for the two first iterations.

$$\hat{x}(n+1) = \hat{A}\hat{x}(n) + B + K(C\hat{x}(n) - y(n))$$

And, after being synchronised, the system runs autonomously.

$$\hat{x}(n+1) = f(\hat{x}(n))$$

In practice, to synchronise, the previous section has calculated all possible gains K for all possible evolution of states and it comes that sixteen observers need to run simultaneously and generate sixteen different trajectories two iterations later. But, not all of them are necessary: indeed, the output signal $y(n) = x_1(n)$ is a component of the state so that it brings an information on the current belonging domain of definition of definition. On the four possible domains, only two are possible, for example, if $y(n) = x_1(n) > 0$, then $x(n) \in [0;1]^2$ or $x(n) \in [0;1] \times [-1;0]$. It is an input-output linearisation [17]. Finally, the observer runs in parallel four different sub-observers and one of the four generated states converges exactly to the same dynamics as the autonomous one in two iterations. To identify it, it is possible to compare both outputs $\hat{y}$ and y, the one that is identical is the sub-observer that has converged.

Figure 2 shows the evolution the states, only the convergent sub-observer is represented. In two iterations, both systems have the same internal states and evolve identically.

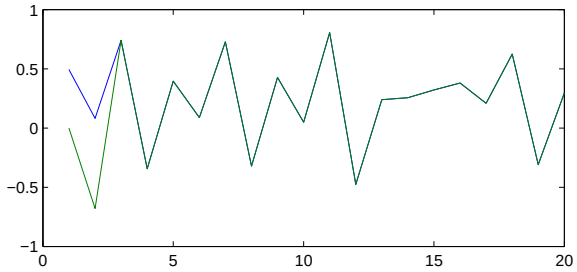


Figure 2: evolution of the output y and $\hat{y}$ - exact synchronisation

The error dynamics $e = \hat{x} - x$ is reported figure 3. In two iterations, the quadratic error does not cancel but only falls to 10^{-15} due to the finite precision of the computer. The system is chaotic and therefore sensitive to initial conditions, so the trajectories of two states initialised as close as wanted to each other would diverge exponentially. That is why, the residual error increases exponentially according to the Lyapunov exponents values until stabilizing to 1, which is the size of the chaotic attractor.

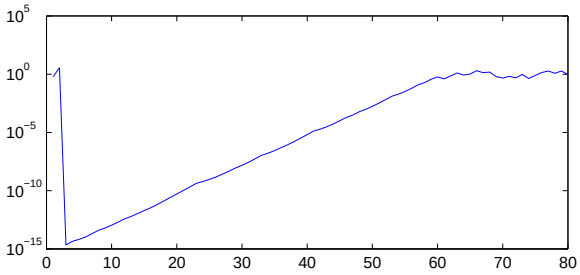


Figure 3: evolution of the quadratic error - synchronization only in the two first iterations (observer switched off after)

As a result, an initial synchronization is not sufficient to ensure its synchronization in time. This paragraph investigates the possibility of synchronising all the time. To do so, the convergence of the error during more than two iterations is considered. For example, in three iterations,

$$e(3) = (A_{i2} + K_{j2}C)(A_{i1} + K_{j1}C)(A_{i0} + K_{j0}C)e(0)$$

The value of the vectors K must be chosen such that:

$$\left\{ \begin{array}{l} (A_{i1} + K_{j1}C)(A_{i0} + K_{j0}C) = 0 \\ (A_{i2} + K_{j2}C)(A_{i1} + K_{j1}C) = 0 \end{array} \right.$$

The choice of any particular gains combination for the resolution of the first equation fixes both K_{j0} and K_{j1}. Then, as K_{j1} is fixed, K_{j2} must be chosen such that the second equation is satisfied if it is possible and so on... But the simplest solution of the system of equations is obtained if the vector K_{jn} depends only on the associated matrix A_{in}. In other words, we are looking for the existence of vectors K_i such that for all possible i and j, $(A_i + K_iC)(A_j + K_jC) = 0$. It is possible to have such a solution by loosing the degree of freedom p of the results given in the previous section. By calculating it, it comes the following gains:

$$K_1 = 2 \begin{pmatrix} (2 - \epsilon_1 - \epsilon_2) \\ \frac{1 - 2\epsilon_2 + \epsilon_2^2 + \epsilon_1\epsilon_2}{\epsilon_1} \end{pmatrix}$$

$$K_2 = 2 \begin{pmatrix} (\epsilon_1 - \epsilon_2) \\ \frac{1 - 2\epsilon_2 + \epsilon_2^2 - \epsilon_1\epsilon_2}{\epsilon_1} \end{pmatrix}$$

$$K_3 = -2 \begin{pmatrix} (2 - \epsilon_1 - \epsilon_2) \\ \frac{1 - 2\epsilon_2 + \epsilon_2^2 + \epsilon_1\epsilon_2}{\epsilon_1} \end{pmatrix}$$

$$K_4 = -2 \begin{pmatrix} (\epsilon_1 - \epsilon_2) \\ \frac{1 - 2\epsilon_2 + \epsilon_2^2 - \epsilon_1\epsilon_2}{\epsilon_1} \end{pmatrix}$$

These vectors are defined such that

$$\forall (i,j) \in \{1;4\}^2, (A_i + K_iC)(A_j + K_jC) = 0$$

The reconstruction of the states of the original system would be composed by a simpler algorithm than the one needed by the vectors defined before. A simulation of such results has been performed and the evolution of the quadratic error is reported in figure 4. Its value is related to the precision of the computer. On the contrary to the first simulation, this one keeps both systems synchronised.

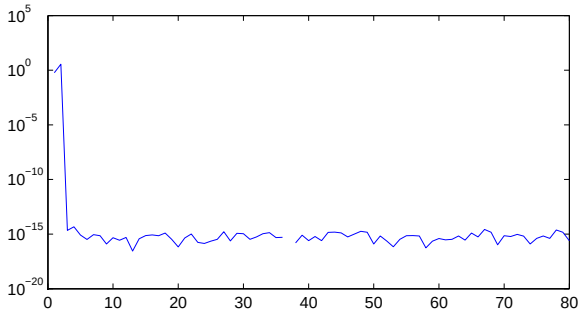


Figure 4: evolution of the reconstruction error - perpetual synchronisation

4.2 Asymptotic observer

Instead of using the exact convergence, it is also possible to converge asymptotically by positioning the singular values of the error matrix less than one to ensure its convergence to zero but greater than zero for the asymptotic aspect. This section analyses both cases of one iteration matrix and two iteration matrix.

4.2.1 Asymptotic convergence in one step

Let consider the following system:

$$\left\{ \begin{array}{l} x(n+1) = 2A_i x(n) + \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\ y(n) = \begin{pmatrix} 1 & 0 \end{pmatrix} x(n) \end{array} \right.$$

where A_i is one of the four matrices defined in section two. It is worth noting that the value of the output y can be an indicator of the value of the matrix A as for exact convergence:

$$\left\{ \begin{array}{l} y(n) \geq 0 \Rightarrow A_i \in \{A_1; A_4\} \\ y(n) < 0 \Rightarrow A_i \in \{A_2; A_3\} \end{array} \right.$$

The aim of the following is to construct an observer which converges asymptotically to the states of the original system.

The global system (original system and observer) is defined by:

$$\left\{ \begin{array}{l} x(n+1) = 2A_i x(n) + \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\ \hat{x}(n+1) = 2\hat{A}_i \hat{x}(n) + \begin{pmatrix} 1 \\ 1 \end{pmatrix} + K(\hat{y}(n) - y(n)) \\ y(n) = \begin{pmatrix} 1 & 0 \end{pmatrix} x(n) \\ \hat{y}(n) = \begin{pmatrix} 1 & 0 \end{pmatrix} \hat{x}(n) \end{array} \right.$$

where the matrices A_i and $\hat{A}_i$ are respectively determined by the values of the states $x(n)$ and $\hat{x}(n)$. The error of the dynamics is then given by:

$$e(n+1) = \hat{x}(n+1) - x(n+1)$$
$$e(n+1) = 2\hat{A}_i\hat{x}(n) - 2A_ix(n) + KCe(n)$$

If $\hat{A}_i = A_i$, then,

$$e(n+1) = (2A_i + KC)e(n)$$

The asymptotic convergence can be obtained by placing both singular values of $(2A_i+KC)$ less than 1. The norm of the error would then asymptotically decrease to zero.

The formal calculation of the minimum of the singular values gives that it is obtained for the parameter combination $\epsilon_1 = \epsilon_2 = 0.5$. Both singular values of $(2A_i + KC)$ are then equal to 0 and 2 for $K = (1 \;\; 1)^t$.

So one singular vector is compressed to zero while the second singular vector increases twice its norm under the matrix $(2A_i + KC)$, thus for any parameter combination and for any gain K, it is impossible to have both singular values less than one. The asymptotic convergence cannot be reached in this way.

4.2.2 Asymptotic convergence in two steps

An alternative approach consists in considering the system under two iterations. The evolution of the error is still governed by the equations:

$$e(n+2) = (2A_i(n+1) + K_1C)(2A_i(n) + K_2C)e(n)$$

As before, an asymptotic convergence can be obtained by placing both singular values of the matrix $(2A_i(n+1) + K_1C)(2A_i(n) + K_2C)$ less than 1. The smallest singular values are zero - that is also what has been tuned for the exact convergence.

It is possible to find an instance of gains K_1 and K_2 such that both singular values of $(2A_i(n+1) + K_1C)(2A_i(n) + K_2C)$ are less than one and also for the value of vectors K_3 and K_4 by considering the matrix $(2A_i(n+2)+K_3C)(2A_i(n+1)+K_4C)$ but all gains must be adapted to each other: K_4 must be chosen such that $K_3 = K_2$ for guaranteeing the overall convergence of the product of all matrices to zero. A particular numerical solution has been found out for parameters $\{\epsilon_1, \epsilon_2\} = \{0.2, 0.1\}$ such that for all possible i and j, the singular values of all matrix $(2A_i+K_iC)(2A_j+K_jC)$ are less than one.

$$\begin{cases} K_1 = \begin{pmatrix} 3.45 \\ 8.35 \end{pmatrix} \\ K_2 = \begin{pmatrix} 0.25 \\ 7.95 \end{pmatrix} \\ K_3 = \begin{pmatrix} -3.45 \\ -8.35 \end{pmatrix} \\ K_4 = \begin{pmatrix} -0.25 \\ -7.95 \end{pmatrix} \end{cases}$$

Under these values, the singular values are $\{0, 0.44\}$. Then, in each iteration, the euclidean norm of the error is multiplied by a factor of 0.44 maximum, that means that the error would decrease to zero with the time.

A simulation has been performed for these values. The evolution of both original state and observer state is reported in figure 5. The evolution of the output error is also represented figure 6. The error is converging exponentially to zero so there is an asymptotic convergence so this convergence is slower than the exact convergence case.

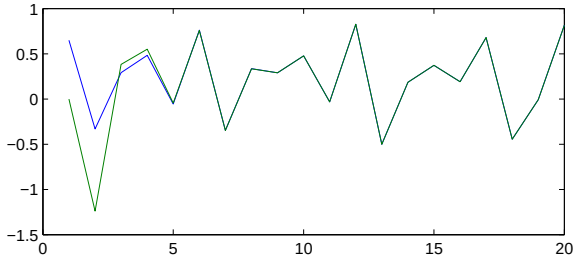


Figure 5: evolution of the outputs y and $\hat{y}$ in the case of asymptotic synchronization

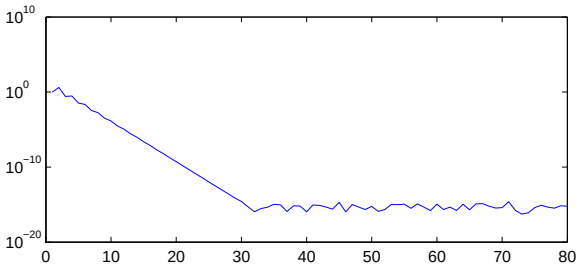


Figure 6: evolution of the error in the case of asymptotic synchronization

These simulations have been performed assuming that the observer knows exactly in which domain is located the state of the original system. But this assumption is not relevant. The following simulations do not suppose anything about the value of the state, as it is the case for all observation problems. The observer should consider all possibilities of the dynamics evolution.

However, there is no need of studying all these cases. Indeed, the transmitted output brings an information and allows to locate the states, for example,

$$y(n) = x_1(n) \geq 0 \Rightarrow \begin{cases} x(n) \in [0;1]^2 \\ \text{or} \\ x(n) \in [0;1] \times [-1;0] \end{cases}$$

The consideration of one of both domains lets the asymptotic synchronization be done whereas the other can increase the quadratic error. In the case of exact synchronization, the domain that puts the estimated output to the same value of the real transmitted output is

identified as being the correct domain but in the case of asymptotic convergence, the decreasing of the quadratic error does not give any tendency on the evolution of the output error $\hat{y}(n) - y(n)$. In other words, all possible domains of definition must be considered to be sure not to exclude the dynamics which is synchronising. Two cases have to be analysed per iteration so that the number of possible states increases exponentially.

Nevertheless, a criteria can be built to restrict the number of states to be considered. Let $\|e\|$ be the quadratic error between the state to estimate and the estimation from the observer. For all possible states,

$$\|e(n+1)\| < \lambda \|e(n)\|$$

$$\|e(n)\| < \lambda^n \|e(0)\|$$

where λ denotes the maximal singular value, 0.44 here. At the initialisation, the error is smaller than $\sqrt{2^2+2^2} = 2\sqrt{2}$ since the state is in the space $[-1;1]^2$. Then, $\|e(n)\| < \lambda^n 2\sqrt{2}$ for all iterations.
And $\|\hat{y}(n) - y(n)\| \|Ce(n)\| < \|e(n)\| < \lambda^n \|e(0)\|$.

This last inequality can be exploited to identify the observer which has converged to the original system. So if the calculated output error does not satisfy this inequality, the considered domain is not the good one.

This simulation has also been performed and the evolution of the output error is represented in figure 7. There is not only one observer state, as several crosses are plotted in the figure for a same instant. The continuous curve separates the convergence zone from the rest of the space as the discrimination is done. Figure 8 plots the same values but in the logarithmic scale.

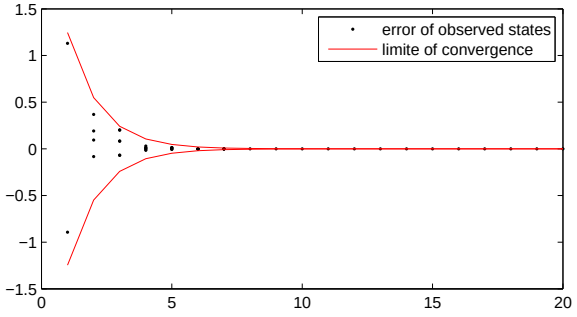


Figure 7: evolution of the output error in the case of asymptotic synchronization and discrimination criteria for convergence

In conclusion, both asymptotic and exact observers exhibit interesting properties, and the choice between the asymptotic and the exact one has to be done according to the particular application. If it is in telecommunications (e.g. for a chaotic encryption), and the noise could be assumed to be zero (i.e. already corrected by the physical layer), than an exact observer seems to be the most suitable. On the other hand, if the application is such

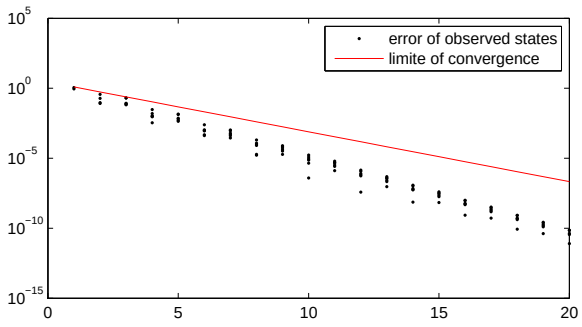


Figure 8: evolution of the output error in the case of asymptotic synchronization and discrimination criteria for convergence

that the system has to be robust to (different kinds of) noise, then an asymptotic observer would be more appropriate.

5 Conclusion

The majority of the papers devoted to synchronization and observer synthesis dealt with maps with poor statistical ans spectral properties. Unlike these authors, in this work we have proposed the observers design for a new weakly coupled and highly performant chaotic map, which beats most of the classical random number generators. Two kinds of observers have been synthesised: and exact - or dead-beat observer, and an asymptotic one. The exact convergence of the dead-beat observer has been theoretically demonstrated (e.g. two iterations for a second order system). In addition, it has been shown that the exact convergence is not guaranteed anymore if the system starts to work autonomously (when the observer is switched off), since the observation error increases up to the size of the chaotic attractor itself. The asymptotic observer is more robust in the case of noise, but the error convergence to zero is slower, and only in an asymptotic way. In the latter case, it has been shown that several observers have to run in parallel, and the criteria to identify the one which has synchronised have been proposed. In conclusion, both observers are performant but in a different way; therefore, the most appropriate one has to be chosen according to the particular application which will be envisaged.

References

[1] L. Kocarev, J. Makraduli, and P. Amato, "Public-key encryption based on chebyshev polynomials," *Circuits, systems, and signal processing*, vol. 24, pp. 497-517, 2005.

[2] P. Fei, Q. Shui-Sheng, and L. Min, "A secure digital signature algorithm based on elliptic curve and

chaotic mappings," *Circuits, Systems, and Signal Processing*, vol. 24, pp. 585-597, 2005.

[3] G. Álvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, pp. 2129-2151, 2006.

[4] M. Gotz, K. Kelber, and W. Schwarz, "Discrete-time chaotic encryption systems. i. statistical design approach," *Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on*, vol. 44, pp. 963-970, 1997.

[5] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications," *National Institute of Standards and Technology Special Publication 800-22 revision 1.*, Natl. Inst. Stand. Technol. Spec. Publ. 800-22rev1, 2001.

[6] D.R. Frey, "Chaotic digital encoding: an approach to secure communication," *Circuits and Systems II: Analog and Digital Signal Processing, IEEE Transactions on*, vol. 40, pp. 660-666, 1993.

[7] W.P. Tang and H.K. Kwan, "Chaotic communications using nonlinear transform-pairs," *Circuits and Systems, 2004. ISCAS'04. Proceedings of the 2004 International Symposium on*, vol.5, pp. 740-743, 2004.

[8] R. Lozi, "New enhanced chaotic number generators," *Indian Journal of Industrial and Applied Mathematics*, vol.1, pp. 1-23, 2008.

[9] T.L. Carroll and L.M. Pecora, "Synchronizing chaotic circuits," *Circuits and Systems, IEEE Transactions on*, vol. 38, pp.453-456, 1991.

[10] U. Feldmann, M. Hasler, and W. Schwarz, "Communication by chaotic signals: The inverse system approach," *International journal of circuit theory and applications*, vol. 24, pp. 551-579, 1996.

[11] A. De Angeli, R. Genesio, and A. Tesi, "Dead-beat chaos synchronization in discrete-time systems," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 42, pp. 54-56, 1995.

[12] M. Feki, B. Robert, G. Gelle, and M. Colas, "Secure digital communication using discrete-time chaos synchronization," *Chaos, Solitons and fractals*, vol. 18, pp. 881-890, 2003.

[13] G. Millerioux and J. Daafouz, "An observer-based approach for input-independent global chaos synchronization of discrete-time switched systems," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 50, pp.1270-1279, 2003.

[14] S. Hénaff, I. Taralova, and R. Lozi, "Statistical and spectral analysis of a new coupled maps systems," *Submitted to Indian Journal of Industrial and Applied Mathematics*.

[15] S. Hénaff, I. Taralova, and R. Lozi, "Observer design for a new weakly coupled map function," *In proceeding of the 3rd International Conference on Complex Systems and Applications ICCSA'09*, C. Bertelle, X. Liu, and M. A. Aziz-Alaoui (eds), Le Havre, pp. 47-50, 2009.

[16] David G Luenberger, "Optimization by vector space methods," *Wiley-Interscience*, 1969.

[17] G. Conte, C.H. Moog, and A.M Perdon, "Algrebraic Methods for Nonlinear Control Systems," *Springer*, 2007.