System identification in communication with chaotic systems

System identification in communication with chaotic systems

H.J.C. Huijberts[◇*] H. Nijmeijer[**] R.M.A. Willems[◇]

◇ Faculty of Mathematics and Computing Science,
Eindhoven University of Technology,
P.O. Box 513, 5600 MB Eindhoven, The Netherlands.
Email: {hjch,willems}@win.tue.nl

** Faculty of Mathematical Sciences, University of Twente,
P.O. Box 217, 7500 AE Enschede, The Netherlands.
Email: H.Nijmeijer@math.utwente.nl

and

Faculty of Mechanical Engineering, Eindhoven University of Technology,
P.O. Box 513, 5600 MB Eindhoven, The Netherlands.

Abstract

Communication using chaotic systems is considered from a control point of view. It is shown that parameter identification methods may be effective in building reconstruction mechanisms, even when a synchronizing system is not available. Three worked examples show the potentials of the proposed method.

Keywords: Communication, chaotic systems, system identification

1 Introduction

In recent years there has been a tremendous interest in studying the behavior of chaotic systems. Two particularly interesting ideas which have emerged during this time are (chaos) synchronization and chaos control. Recent reviews on these subjects can be found in, for instance, two special issues devoted to the subject, see [4],[18] (where in fact [4] is a follow up of an earlier special issue on the same subject of the same journal ([3])).

Synchronization and controlled synchronization of chaotic systems is a topic that has become popular, among others, because of its possible use in communication, see [15],[14]. Recently, in [11] a control perspective on synchronization was given, which enables to resolve various synchronization problems as an observer problem. Thus, [11] illustrates, among others, the benefits of incorporating control theoretic ideas in the study of communication using chaotic systems.

*Part of the research of the first author was performed while visiting the Department of Electrical and Electronic Engineering, University of Western Australia, Nedlands, Australia, supported by the Australian Research Council.

It is the purpose of the present paper to further illustrate these benefits. More specifically, we will look at some problems in communication using chaotic systems for which (standard) synchronization-based schemes may not yield the reconstruction of encoded messages, but that can be resolved using control theoretic ideas. The present paper is an expanded version of the paper [8].

In communication using chaotic systems, one considers a transmitter system Σ_T of the form

$$\Sigma_T \left\{ \begin{array}{rcll} \dot{x} & = & f(x,\lambda), & x \in I\!R^n \\ y & = & h(x), & y \in I\!R \end{array} \right. \tag{1}$$

where λ is a time-varying message satisfying $\lambda_{\min} \leq \lambda(t) \leq \lambda_{\max}$ $(\forall t)$ and $y \in I\!R$ is the transmitted signal (i.e., the coded message). It is assumed that the system Σ_T is chaotic for all constant λ satisfying $\lambda_{\min} \leq \lambda \leq \lambda_{\max}$. The task is now to build a receiver system Σ_R that reconstructs the message $\lambda(t)$ from the coded message $y(t)$.

A possible advantage of using chaotic systems for communication is that the transmitted signal y will be a chaotic signal, which implies that it has a broad spectrum. This gives the opportunity to use the chaotic system under consideration for wideband communication (cf. [10]). Further, the fact that y is a chaotic (and thus seemingly random) signal gives the hope that chaotic systems may also be used for secure communication. All of this of course presupposes that y will also be a chaotic (or at least sufficiently complex) signal when λ is time-varying. In most publications on communication with chaotic systems (and this paper is no exception) this is tacitly assumed, although not always stated explicitly. However, it seems reasonable to expect that indeed y will be chaotic if λ is mainly slowly time-varying, meaning that is λ is slowly time-varying for most of the time, but may exhibit occasional jumps. Typically, this is the case for binary messages.

If one considers the problem of reconstruction of λ as described above from a control theoretic point of view, two possible ways to approach the problem come to mind. The first approach is that of system inversion. Interpreting λ in (1) as an input and y as a measurement, one sees that (1) gives a mapping from λ to y. In the problem of system inversion, the task is to find an (asymptotic) inverse of this mapping. This approach will be pursued in future research (note, however, that this idea has also been studied in [7]). The second approach, that will be pursued in this paper, and which in a sense was initiated for a particular case by Corron and Hahs in [6], is that of system identification. In system identification, the task is to estimate unknown (possibly slowly time-varying) parameters of a system, based on measurements taken from the system. For linear systems, system identification is well-established (for an overview, see e.g. [17]). In this paper, it will be shown on three examples that these identification methods may be helpful in communication using chaotic systems. Although all three examples concern chaotic, and thus nonlinear, systems, it is possible to use the standard "linear" identification algorithms once the systems are decomposed and/or transformed properly. Further, the communication schemes in the last two examples may be expected to be more secure than the scheme proposed by Corron and Hahs ([6]), as will be argued in the paper.

The organization of this paper is as follows. In the following section, we first introduce three examples that illustrate that parameter identification methods may be effective in commu-

nication with chaotic systems. After this, the essential identification background will be reviewed. In the following three sections, a reconstruction mechanism for each of the three examples will be derived. In the first example, it will be shown among others that the communication scheme that was proposed by Corron and Hahs in [6] fits well in the identification based approach to communication. In the last two examples, we will see that the existence of a synchronizing subsystem is not necessary for the existence of a reconstruction mechanism. Rather, one will typically have that (partial) synchronization occurs *after* message reconstruction. In Section 6, some conclusions will be drawn.

2 Parameter identification methods

In this section, we briefly introduce the so called *equation error identifier* that may be used to estimate unknown parameters for linear time-invariant systems.

At first sight, it may seem somewhat strange that parameter identification methods for linear systems may be used for building reconstruction mechanisms in communication with chaotic (and thus *nonlinear*) systems. Therefore, we will first look at three examples illustrating that indeed these *linear* parameter identification methods may be useful in the design of a reconstruction mechanism. After having introduced these examples, we will review the essential identification background.

Example 2.1 Consider the following set up for secure communication that was proposed by Corron and Hahs in [6]. The transmitter is a three-dimensional system Σ_T of the form

$$\Sigma_T \left\{ \begin{array}{rcl} \dot{x}_1 & = & f_1(x_1,x_2,x_3) + g(x_1,x_2,x_3)\lambda \\ \dot{x}_2 & = & f_2(x_1,x_2,x_3) \\ \dot{x}_3 & = & f_3(x_1,x_2,x_3) \\ y & = & x_1 \end{array} \right. \tag{2}$$

where λ is a message that is mainly slowly time-varying and satisfies $\lambda_{\min} \leq \lambda(t) \leq \lambda_{\max}$ $(\forall t)$. Further, $y \in \mathbb{R}$ is the transmitted signal (i.e., the coded message). Also, a second system is considered that has the form

$$\left\{ \begin{array}{rcl} \dot{\hat{x}}_2 & = & f_2(y,\hat{x}_2,\hat{x}_3) \\ \dot{\hat{x}}_3 & = & f_3(y,\hat{x}_2,\hat{x}_3) \end{array} \right. \tag{3}$$

It is assumed that the (x_2,x_3)-subsystem in (2) synchronizes with (3), in the sense that for Σ_T, together with the system (3) we have for all initial conditions that

$$\lim_{t\to+\infty} (x_i(t) - \hat{x}_i(t)) = 0 \quad (i = 2,3) \tag{4}$$

We now show that the problem of estimating λ may be viewed as a linear parameter identification problem. If one assumes that the systems (2) and (3) have synchronized, the dynamics of y in (2) are given by

$$\dot{y}(t) = u_1(t) + \lambda u_2(t) \tag{5}$$

where

$$\begin{array}{rcl} u_1(t) & := & f_1(y(t),\hat{x}_2(t),\hat{x}_3(t)) \\ u_2(t) & := & g(y(t),\hat{x}_2(t),\hat{x}_3(t)) \end{array} \tag{6}$$

We then see that (5) may be interpreted as a linear time-invariant system with output y and inputs u_1, u_2. Further, our task is now to obtain a mechanism that estimates λ for the linear system (5), based on the measurements y, u_1, u_2. This problem may be interpreted as a linear parameter identification problem, and will be treated as such in the sequel.

Note that in the above example the "distance" between the message λ and the transmitted message y is small, in the sense that already the first time-derivative of y explicitly depends on λ (in control theoretic terms, this is expressed by saying that the *relative degree* (cf. [9]) of y with respect to λ equals 1). If one would like to use the above scheme for *secure* communication, this might be a drawback since it might mean that λ is not hidden well enough. Indeed, a simple numerical differentiation scheme could be enough to allow eavesdroppers to decode the coded message. Therefore, from the point of view of secure communication, it might be worthwhile to consider schemes where the relative degree of y with respect to λ is greater than 1. The following two examples have this property. Further, these examples illustrate that when one considers systems with a relative degree that is greater than 1, the assumption of existence of a synchronizing subsystem will in general not be of use any more.

Example 2.2 In this example, we consider Chua's circuit, which, in dimensionless form, is described by the equations

$$\left\{\begin{array}{rcl} \dot{x}_1 &=& \alpha(-x_1 + x_2 - \phi(x_1)) \\ \dot{x}_2 &=& x_1 - x_2 + x_3 \\ \dot{x}_3 &=& -\lambda x_2 \end{array}\right. \tag{7}$$

where

$$\phi(x_1) = m_1 x_1 + \frac{m_0 - m_1}{2}(|x_1 + 1| - |x_1 - 1|)$$

This system is known to have a so called double scroll chaotic attractor for $\alpha = 15.6$, $m_0 = -\frac{8}{7}$, $m_1 = -\frac{5}{7}$, and $23 < \lambda < 31$ (see e.g. [1]). We assume that $y = x_2$ is the transmitted signal. Note that in this case the relative degree of y with respect to λ equals 2. Further note that, although it has been shown experimentally that for constant λ the (x_1, x_3)-subsystem synchronizes with the system

$$\left\{\begin{array}{rcl} \dot{\hat{x}}_1 &=& \alpha(-\hat{x}_1 + x_2 - \phi(\hat{x}_1)) \\ \dot{\hat{x}}_3 &=& -\lambda x_2 \end{array}\right. \tag{8}$$

(see e.g. [5]), we cannot use this synchronizing subsystem in our reconstruction mechanism, since it explicitly depends on the unknown parameter λ. In order to come up with a a reconstruction scheme for λ, we first assume that, besides x_2, we can also measure x_1. The equations for x_2 and x_3 in (7) then have the following form:

$$\left\{\begin{array}{rcl} \dot{x}_2 &=& -x_2 + x_3 + u \\ \dot{x}_3 &=& -\lambda x_2 \\ y &=& x_2 \end{array}\right. \tag{9}$$

where we interpret $u := x_1$ as a known input. Thus, (9) has the form of a linear control system depending on an unknown parameter λ, so that again linear parameter estimation methods may be used to obtain a reconstruction mechanism for λ.

Example 2.3 We consider the following Rössler system:

$$\left\{\begin{array}{rcl} \dot{x}_1 &=& -x_2 - x_3 \\ \dot{x}_2 &=& x_1 + \lambda x_2 \\ \dot{x}_3 &=& 2 + (x_1 - 4)x_3 \\ y &=& x_3 \end{array}\right. \tag{10}$$

where we assume that λ is a slowly time-varying message satisfying $0.3 < \lambda(t) < 0.5$ $(\forall t)$ and $x_3(0) > 0$. Note that in this case the relative degree of y with respect to λ equals 3. It is known (see e.g. [15]) that for (10) the (x_1, x_2)-subsystem does not synchronize with the system

$$\left\{\begin{array}{rcl} \dot{\hat{x}}_1 &=& -\hat{x}_2 - x_3 \\ \dot{\hat{x}}_2 &=& \hat{x}_1 + \lambda \hat{x}_2 \end{array}\right.$$

Thus, in this case no synchronizing subsystem that can be used in a reconstruction mechanism inspired by the scheme in [6] exists. However, it is possible to reconstruct λ based on the measurement y. A first step in this reconstruction is the observation that (10) may be transformed into a system with so called linearizable error dynamics (see e.g. [12],[11]). More specifically, note that, since $x_3(0) > 0$, we have that $x_3(t) > 0$ $(\forall t \geq 0)$. Thus, for (10) the coordinate change $\xi_1 = x_1$, $\xi_2 = x_2$, $\tilde{y} = \xi_3 = \log x_3$ is well-defined. In these new coordinates, (10) takes the form

$$\begin{array}{rcl} \begin{pmatrix} \dot{\xi}_1 \\ \dot{\xi}_2 \\ \dot{\xi}_3 \end{pmatrix} &=& \underbrace{\begin{pmatrix} 0 & -1 & 0 \\ 1 & \lambda & 0 \\ 1 & 0 & 0 \end{pmatrix}}_{A(\lambda)} \begin{pmatrix} \xi_1 \\ \xi_2 \\ \xi_3 \end{pmatrix} + \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix}}_{B} \underbrace{\begin{pmatrix} -\mathrm{e}^{\tilde{y}} \\ 2\mathrm{e}^{-\tilde{y}} - 4 \end{pmatrix}}_{\Phi(\tilde{y})} \\ \tilde{y} &=& \xi_3 \end{array} \tag{11}$$

Hence, (11) consists of a linear system $\dot{\xi} = A(\lambda)\xi + Bu$, where the matrix $A(\lambda)$ depends linearly on λ, interconnected with a static nonlinearity $u = \Phi(\tilde{y})$, that only depends on (a function of) the transmitted signal x_3. This gives that also in this case linear parameter identification methods may be used to build a reconstruction mechanism for λ.

Having illustrated the fact that linear parameter identification methods may be effective in communication with chaotic systems, we now describe how a so called *equation error identifier* may be obtained. We will restrict to linear time-invariant systems with one output and two inputs that depend on one unknown parameter. The restriction to systems with only one input and the extension to systems with more than two inputs are straightforward. The exposition is based on [17]. For further details, the reader is referred to this reference.

In the rest of the paper, we use the following notation and terminology. By $\mathbb{R}[s]$, we denote the set of all polynomials in the indeterminate s with real coefficients. Let $a \in \mathbb{R}[s]$. Then there exist an $n \in \mathbb{N}$ and $a_0, \cdots, a_n \in \mathbb{R}$ such that a has the form

$$a(s) = \sum_{j=0}^{n} a_j s^j \tag{12}$$

If $a_n \neq 0$, we define $\deg(a) := n$. The polynomial a is called *monic* if $a_n = 1$. Further, a is called *Hurwitz* if all zeros of a are in the open left half plane of the complex plane.

For a function $f(t)$ that is k times continuously differentiable, we define

$$f^{(k)}(t) := \frac{d^k f}{dt^k}(t)$$

Let $a \in \mathbb{R}[s]$ of the form (12) be given, and let $f(t)$ be n times continuously differentiable. We then define

$$a\left(\frac{d}{dt}\right) f := \sum_{j=0}^{n} a_j f^{(j)}$$

We now consider a linear time-invariant system Σ_λ depending on an unknown parameter λ with two inputs and one output, and transfer matrix

$$G_\lambda(s) = \begin{pmatrix} \frac{p_\lambda(s)}{q_\lambda(s)} & \frac{r_\lambda(s)}{q_\lambda(s)} \end{pmatrix} \tag{13}$$

As is well known (see e.g. [16]), the fact that the transfer matrix of Σ_λ is given by (13) implies that, given input functions $u_1(t)$, $u_2(t)$, the output $y(t)$ of Σ_λ satisfies the following linear differential equation:

$$q_\lambda\left(\frac{d}{dt}\right) y = p_\lambda\left(\frac{d}{dt}\right) u_1 + r_\lambda\left(\frac{d}{dt}\right) u_2 \tag{14}$$

We make the following assumptions:

- The polynomials $p_\lambda(s)$, $q_\lambda(s)$, $r_\lambda(s)$ depend linearly on λ.
- For all λ, we have that $\deg(q_\lambda) = n$ and q_λ is monic.
- For all λ, we have that $\deg(p_\lambda), \deg(r_\lambda) < n$.

As a consequence of these assumptions, the polynomials $p_\lambda, q_\lambda, r_\lambda$ have the following form.

$$\begin{aligned} p_\lambda(s) &= p_0(s) + p_1(s)\lambda \\ q_\lambda(s) &= q_0(s) + q_1(s)\lambda \\ r_\lambda(s) &= r_0(s) + r_1(s)\lambda \end{aligned} \tag{15}$$

where $p_0, p_1, r_0, r_1, q_0, q_1 \in \mathbb{R}[s]$ have the form

$$\begin{aligned} p_i(s) &= \sum_{j=0}^{n-1} p_{ij} s^j \qquad (i = 0, 1) \\ r_i(s) &= \sum_{j=0}^{n-1} r_{ij} s^j \qquad (i = 0, 1) \\ q_0(s) &= \sum_{j=0}^{n-1} q_{0j} s^j + s^n \\ q_1(s) &= \sum_{j=0}^{n-1} q_{1j} s^j \end{aligned} \tag{16}$$

In system identification, the task is now to build a reconstruction mechanism for λ, based on the measurements y, u_1, u_2. Note that in our description of Σ_λ with the transfer matrix $G_\lambda(s)$, we have a description that depends on λ in a nonlinear way, in spite of the fact that the polynomials p_λ, q_λ, r_λ depend on λ in a linear way. In the equation error method, a first

step in building a reconstruction mechanism for λ is to obtain a (asymptotic) description of Σ_λ that depends on λ in a *linear* way. This is achieved as follows. Let $u_1(t)$ and $u_2(t)$ be input signals for Σ_λ, and let $y(t)$ be a corresponding output signal of Σ_λ. Thus, $y(t)$ satisfies the differential equation (14). Let $k \in \mathbb{R}[s]$ be Hurwitz, and assume that $\deg(k) = n$. Further, let $\tilde{y}(t)$ be a signal satisfying the differential equation

$$k\left(\frac{d}{dt}\right)\tilde{y} = p_\lambda\left(\frac{d}{dt}\right)u_1 + r_\lambda\left(\frac{d}{dt}\right)u_2 + \left[k\left(\frac{d}{dt}\right) - q_\lambda\left(\frac{d}{dt}\right)\right]y \tag{17}$$

From the above, it follows that $\tilde{y}$ may be interpreted as the output of a linear time-invariant system with "inputs" y, u_1, u_2 and transfer matrix

$$H_\lambda(s) = \begin{pmatrix} \dfrac{k(s) - q_\lambda(s)}{k(s)} & \dfrac{p_\lambda(s)}{k(s)} & \dfrac{r_\lambda(s)}{k(s)} \end{pmatrix} \tag{18}$$

Writing

$$k(s) = \sum_{j=0}^{n-1} k_j s^j + s^n$$

and defining the row vectors

$$\begin{array}{rcll} p_i^* & := & (p_{i0} \ \cdots \ p_{in-1}) & (i = 0, 1) \\ p^* & := & p_0^* + p_1^*\lambda & \\ q_i^* & := & (q_{i0} \ \cdots \ q_{in-1}) & (i = 0, 1) \\ q^* & := & q_0^* + q_1^*\lambda & \\ r_i^* & := & (r_{i0} \ \cdots \ r_{in-1}) & (i = 0, 1) \\ r^* & := & r_0^* + r_1^*\lambda & \\ k^* & := & (k_0 \ \cdots \ k_{n-1}) & \end{array} \tag{19}$$

a realization ([16]) of $H_\lambda(s)$ is then given by

$$\left\{\begin{array}{rcll} \dot{\tilde{w}}_0 & = & K\tilde{w}_0 + Ly & \\ \dot{\tilde{w}}_i & = & K\tilde{w}_i + Lu_i & (i = 1, 2) \\ \tilde{y} & = & (k^* - q^*)\tilde{w}_0 + p^*\tilde{w}_1 + r^*\tilde{w}_2 & \end{array}\right. \tag{20}$$

where

$$K := \begin{pmatrix} 0 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 1 & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & \cdots & 0 & 1 \\ -k_0 & -k_1 & \cdots & \cdots & \cdots & -k_{n-1} \end{pmatrix}, \quad L := \begin{pmatrix} 0 \\ 0 \\ \vdots \\ \vdots \\ 1 \end{pmatrix}$$

Now note that from (14),(17), it follows that $\tilde{y}$ in fact satisfies the following differential equation.

$$k\left(\frac{d}{dt}\right)(\tilde{y} - y) = 0 \tag{21}$$

Since k is Hurwitz, this implies that we have

$$\lim_{t\to+\infty}(\tilde{y}(t)-y(t))=0 \tag{22}$$

where the convergence is exponential. From this fact and the fact that $H_\lambda(s)$ depends on λ in a linear way, we see that we now have indeed obtained an asymptotic description of Σ_λ that depends on λ in a linear way.

A next step in the procedure to obtain an equation error estimator for λ is to consider a copy of the system (20), where λ is replaced by its estimation $\hat{\lambda}$. Thus, we obtain a system

$$\left\{\begin{array}{rcl}\dot{w}_0 &=& Kw_0+Ly\\ \dot{w}_i &=& Kw_i+Lu_i \quad (i=1,2)\\ \hat{y} &=& (k^*-q_0^*-q_1^*\hat{\lambda})w_0+(p_0^*+p_1^*\hat{\lambda})w_1+(r_0^*+r_1^*\hat{\lambda})w_2\end{array}\right. \tag{23}$$

Making use of (20),(22),(23), it is then straightforwardly shown that

$$\hat{y}(t)-y(t)=\phi(w(t))(\hat{\lambda}(t)-\lambda)+\epsilon(t) \tag{24}$$

where $\epsilon(t)$ tends to zero exponentially for $t\to+\infty$, and $\phi(w)$ is defined by

$$\phi(w):=(-q_1^*w_0+p_1^*w_1+r_1^*w_2) \tag{25}$$

To (23), an update mechanism for $\hat{\lambda}$ of the following form is added:

$$\dot{\hat{\lambda}}=-\nu\psi(t,w)(\hat{y}-y),\quad \nu>0 \tag{26}$$

Using (24), it is then easily shown that we have

$$\frac{d}{dt}(\hat{\lambda}-\lambda)^2=-2\nu\psi(t,w)\phi(w)(\hat{\lambda}-\lambda)^2-2\nu\epsilon(t)\psi(t,w)(\hat{\lambda}-\lambda) \tag{27}$$

Exploiting the fact that $\epsilon(t)$ tends to zero exponentially, it may then be shown (see [17] for details) that $\hat{\lambda}(t)-\lambda\to 0$ $(t\to+\infty)$ exponentially, *if* the following conditions are satisfied.

- $\psi(t,w(t))$ is bounded on $[0,\infty)$.
- $\psi(t,w(t))\phi(w(t))\geq 0$ on $[0,\infty)$.
- $\psi(t,w(t))\phi(w(t))$ is *persistently exciting* (P.E.) on $[0,\infty)$, i.e., there exist $\alpha_1,\alpha_2,\delta>0$ such that for all $t\in[0,\infty)$ we have

$$\alpha_1\leq\int_t^{t+\delta}\psi(\tau,w(\tau))^2\phi(w(\tau))^2d\tau\leq\alpha_2 \tag{28}$$

In the literature, a wide range of possible choices of the function $\psi(t,w)$ is available. It goes without saying that each different choice of ψ will lead to a different estimator with different properties. An estimator that possesses good properties in many cases is the *least squares estimator with exponential forgetting factor*, that is obtained by choosing

$$\psi(t,w):=-\nu\phi(w)p(t),\quad(\nu>0) \tag{29}$$

where the function $p(t)$ is a solution of the differential equation

$$\dot{p} = -\nu(\phi(w)^2 p^2 - \gamma p), \quad (\gamma > 0,\ p(0) > 0) \tag{30}$$

In the sequel, we will tacitly assume that the signals $\psi(t, w(t))\phi(w(t))$ appearing in our reconstruction mechanisms are P.E. To a degree, this tacit assumption is justified by the fact that it has been shown in [2] that for quite a wide choice of functions $\psi(t, w)$ we will have that $\psi(t, w(t))\phi(w(t))$ is P.E. when the signals $y(t)$, $u_1(t)$ and $u_2(t)$ have a power spectrum that is not concentrated at too few a number of peaks. Since in the applications we will be looking at, the signals $y(t)$,$u_1(t)$,$u_2(t)$ will be produced by a chaotic system, it follows from the fact that chaotic systems produce signals with a broad continuous power spectrum (cf. [13]), that indeed $\psi(t, w(t))\phi(w(t))$ may be expected to be P.E.

3 The Corron-Hahs scheme with synchronization

We continue with Example 2.1. The transfer matrix $G_\lambda(s)$ of the system (5) is given by

$$G_\lambda(s) = \begin{pmatrix} \frac{1}{s} & \frac{\lambda}{s} \end{pmatrix}$$

Thus, we have in the notation of the previous section,

$$\begin{array}{rcl} p_\lambda(s) & = & 1 \\ q_\lambda(s) & = & s \\ r_\lambda(s) & = & \lambda \end{array}$$

Letting $\kappa > 0$, we have that the polynomial $k(s) := s + \kappa$ is Hurwitz. Thus, in this case the system (20) has the form

$$\left\{ \begin{array}{rcl} \dot{w}_0 & = & -\kappa w_0 + y \\ \dot{w}_1 & = & -\kappa w_1 + u_1 = -\kappa w_1 + f_1(y, \hat{x}_2, \hat{x}_3) \\ \dot{w}_2 & = & -\kappa w_2 + u_2 = -\kappa w_2 + g(y, \hat{x}_2, \hat{x}_3) \\ \hat{y} & = & \kappa w_0 + w_1 + \hat{\lambda} w_2 \end{array} \right. \tag{31}$$

Further, we have in this case that

$$\phi(w) = w_2 \tag{32}$$

Choosing

$$\psi(t, w) := \frac{\mathrm{sign}(w_2)}{1 + |w_2|} \tag{33}$$

we then obtain the following adaptation law for $\hat{\lambda}$:

$$\dot{\hat{\lambda}} = -\nu \frac{\mathrm{sign}(w_2)}{1 + |w_2|}(\hat{y} - y), \quad \nu > 0 \tag{34}$$

Remark 3.1 The reconstruction mechanism (31),(34) is not exactly the same as the reconstruction mechanism proposed in ([6]). However, if one looks at (31),(33) more closely, one sees that for the reconstruction one does not need to know w_0 and w_1 separately, but that knowledge of the linear combination $\kappa w_0 + w_1$ suffices. Thus, defining

$$\begin{aligned} \tilde{w}_0 &:= \kappa w_0 + w_1 \\ \tilde{w}_1 &:= w_2 \end{aligned}$$

one arrives at the following reconstruction mechanism:

$$\left\{ \begin{array}{rcl} \dot{\tilde{w}}_0 &=& -\kappa \tilde{w}_0 + \kappa y + f_1(y, \hat{x}_2, \hat{x}_3) \\ \dot{\tilde{w}}_1 &=& -\kappa \tilde{w}_1 + g(y, \hat{x}_2, \hat{x}_3) \\ \\ \dot{\hat{\lambda}} &=& -\nu \frac{\mathrm{sign}(\tilde{w}_1)}{1+|\tilde{w}_1|}(\hat{y} - y), \quad (\nu > 0) \end{array} \right. \tag{35}$$

which is exactly the reconstruction mechanism proposed in [6]. Note, however, that in [6] this reconstruction mechanism was obtained in a different way. Further, in [6] the authors do not require the function $\psi(t, w)$ in (33) to be persistently exciting. However, if one carefully checks the derivation in [6], it turns out that also in [6] this requirement is needed.

4 Chua's circuit with partial synchronization

In this section, we continue our investigation of the possibility to build a reconstruction scheme for λ for the Chua circuit (7) from Example 2.2. As we have seen in Example 2.2, λ may be reconstructed by using linear parameter identification techniques if, besides the transmitted signal $y = x_2$, also the signal x_1 is available for measurement. This may be done by setting $u := x_1$ in the linear system (9).

It is easily checked that the transfer function $G_\lambda(s)$ of (9) is given by

$$G_\lambda(s) = \frac{s}{s^2 + s + \lambda}$$

Thus, in the notation of Section 2 we have in this case

$$\begin{aligned} p_\lambda(s) &= s \\ q_\lambda(s) &= s^2 + s + \lambda \end{aligned}$$

For (9), the least squares estimator with exponential forgetting factor then takes the following form:

$$\left\{ \begin{array}{rcl} \dot{w}_{01} &=& w_{02} \\ \dot{w}_{02} &=& -k_0 w_{01} - k_1 w_{02} + y = -k_0 w_{01} - k_1 w_{02} + x_2 \\ \dot{w}_{11} &=& w_{12} \\ \dot{w}_{12} &=& -k_0 w_{11} - k_1 w_{12} + u = -k_0 w_{11} - k_1 w_{12} + x_1 \\ \hat{y} &=& (k_0 - \hat{\lambda}) w_{01} + (k_1 - 1) w_{02} + w_{12} \\ \dot{\hat{\lambda}} &=& \nu w_{01} p (\hat{y} - y), \quad (\nu > 0) \\ \dot{p} &=& -\nu (w_{01}^2 p^2 - \gamma p), \quad (\gamma > 0) \end{array} \right. \tag{36}$$

where $k_0, k_1 \in \mathbb{R}$ are such that the polynomial $k(s) := s^2 + k_1 s + k_0$ is Hurwitz.

From the above, it follows that, if x_1 could be measured, the reconstruction of λ could be achieved by employing the scheme (36). To achieve reconstruction when x_1 cannot be measured, we add the following estimator of x_1 to our reconstruction scheme:

$$\dot{\hat{x}}_1 = \alpha(-\hat{x}_1 + x_2 - \phi(\hat{x}_1)) \tag{37}$$

and let the reconstruction scheme (36) depend on $\hat{x}_1$ instead of x_1, i.e., we replace the reconstruction scheme (36) by the following reconstruction scheme:

$$\left\{\begin{array}{rcl} \dot{\bar{w}}_{01} &=& \bar{w}_{02} \\ \dot{\bar{w}}_{02} &=& -k_0\bar{w}_{01} - k_1\bar{w}_{02} + x_2 \\ \dot{\bar{w}}_{11} &=& \bar{w}_{12} \\ \dot{\bar{w}}_{12} &=& -k_0\bar{w}_{11} - k_1\bar{w}_{12} + \hat{x}_1 \\ \bar{y} &=& (k_0 - \bar{\lambda})\bar{w}_{01} + (k_1 - 1)\bar{w}_{02} + \bar{w}_{12} \\ \dot{\bar{\lambda}} &=& \nu\bar{w}_{01}\bar{p}(\bar{y} - y), \quad (\nu > 0) \\ \dot{\bar{p}} &=& -\nu(\bar{w}_{01}^2\bar{p}^2 - \gamma\bar{p}), \quad (\gamma > 0) \end{array}\right. \tag{38}$$

where now $\bar{\lambda}$ denotes the estimate of λ. We then have the following result that is proved in [19].

Theorem 4.1 *Assume that for (36) we have that*

$$\lim_{t\to+\infty}(\hat{\lambda}(t) - \lambda) = 0 \tag{39}$$

and that

$$\lim_{t\to+\infty}(\hat{x}_1(t) - x_1(t)) = 0 \tag{40}$$

Then for (38) we have that

$$\lim_{t\to+\infty}(\bar{\lambda}(t) - \lambda) = 0 \tag{41}$$

■

From Theorem 4.1, it follows that if only the transmitted signal $y = x_2$ can be measured, then λ can be reconstructed, provided $\hat{x}_1(t)$ approaches $x_1(t)$. In [5], it was shown experimentally that this will indeed be the case for constant λ. However, one needs to be somewhat careful here for the following reasons. Define the error signal $e(t) := \hat{x}_1(t) - x_1(t)$. Then, for the parameter values given above, e satisfies the following differential equation:

$$\dot{e} = 15.6(-\frac{2}{7}e + \frac{3}{7}(\mathrm{sat}(e + x_1) - \mathrm{sat}(x_1))) \tag{42}$$

where $\mathrm{sat}(\cdot)$ is the saturation function given by $\mathrm{sat}(x) = \frac{1}{2}(\mid x + 1 \mid - \mid x - 1 \mid)$. A first observation is that the equilibrium $e = 0$ of (42) is unstable when $x_1(t) \equiv 0$. This implies in particular that when (7) is initialized in the origin, we will not have that e tends to zero. It may be argued that from a practical point of view this is not a serious objection, since in practice one will have (7) "running" when communicating. However, as was shown in e.g. [3], the system (7) for the given parameter values is chaotic in the sense of Shil'nikov. This implies in particular that the origin is a homoclinic point for (7), which gives by the above that e will also not tend to zero when (7) is initialized on the homoclinic orbit. Further, this

implies that when (7) is initialized *near* the homoclinic orbit, we will at least not have that e will tend to zero quickly. This leads to the conclusion that the best one could hope is that e will tend to zero quickly for a *generic* choice of x_1.

Theoretical evidence for the asymptotic stability of $e = 0$ for (42) with a generic choice of x_1 is obtained in the following way. Consider in the (x_1, e)-plane the compact set S enclosed by the straight lines $e = -\frac{3}{2}(x_1 \pm 1)$, $e = -3(x_1 \pm 1)$, $e = \pm 3$ (see Figure 1). Further, consider

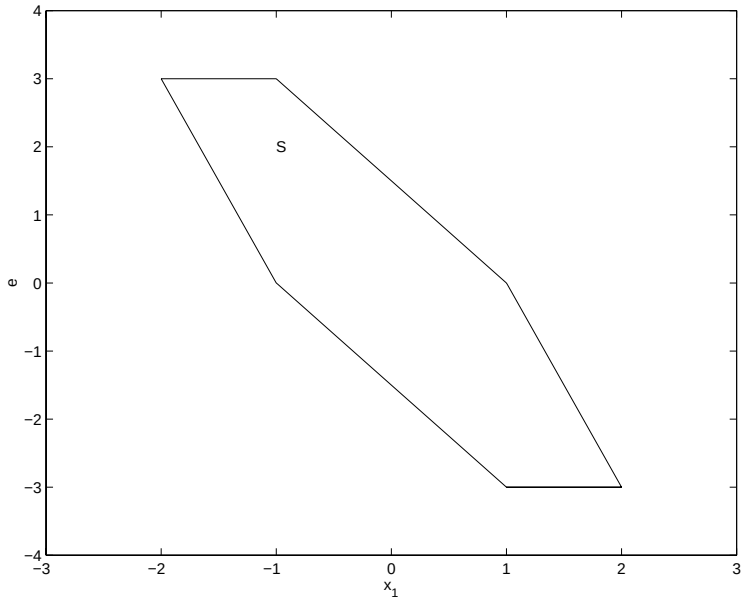

Figure 1: The set S in the (x_1, e)-plane

the function $V(e) := \frac{1}{2}e^2$. It may then be shown that $\dot{V} = e\dot{e} \geq 0$ on $S \cup \{x_1 - \text{axis}\}$, and $\dot{V} = 0$ on $\partial S \cup \{x_1 - \text{axis}\}$, while $\dot{V} < 0$ outside $S \cup \{x_1 - \text{axis}\}$. A first conclusion that may be drawn from this, is that $\{e \in I\!R \mid |e| \leq 3\}$ is a globally attracting invariant set of (42) for *all* x_1. Also, the location of S in the (x_1, e)-plane suggests that we will have asymptotic stability of $e = 0$ for (42) if the residence time of $x_1(t)$ in the region $|x_1| > 1$ is large in comparison with the residence time of $x_1(t)$ in the region $|x_1| \leq 1$. Simulations for constant values of λ between 23 and 31 indicate that (asymptotically) we will have that $|x_1(t)| \leq 1$ for about 20% of the time, while $x_1(t) < -1$ respectively $x_1(t) > 1$ for about 40% of the time.

In Figure 2 the proposed reconstruction scheme is illustrated by means of a simulation. Here, the parameters were chosen as $k_0 = 256$, $k_1 = 32$, $\nu = 800$, $\gamma = 0.001$.

In this section, we employed a partially synchronizing subsystem (37) rather than a completely synchronizing subsystem as is often the case in communication using chaotic systems. However, there is also another (partial) synchronization aspect present in the scheme. Namely, it follows that once we have that $\hat{\lambda} = \lambda$, we will have that $\hat{y} \to y$, or, in other words, we will have that $(k_0 - \lambda)w_{01} + (k_1 - 1)w_{02} + w_{12}$ and x_2 will synchronize. Taking time-derivatives, this gives on its turn that also $(k_0 - k_1\lambda)w_{01} + (k_0 - \lambda)w_{02} - k_0 w_{11}$ and x_3 will synchronize.

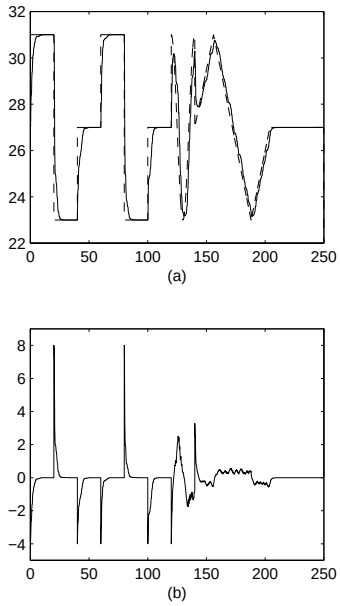

Figure 2: Simulation results for the Chua system: (a) λ (dashed) and $\hat{\lambda}$ (solid) (b) estimation error

Thus we see that, although our scheme is only based on partial synchronization beforehand, it will also exhibit partial synchronization once λ has been estimated correctly.

5 Rössler system without synchronization

In this section, we continue our investigation of the possibility to build a reconstruction scheme for the Rössler system (10) from Example 2.3. As we have seen in Example 2.3, λ may be reconstructed by applying linear parameter identification techniques to the transformed system (11).

It is easily checked that the transfer matrix $G_\lambda(s)$ of (11) is given by

$$G_\lambda(s) = \left(\frac{s-\lambda}{s^3-\lambda s^2+s} \quad \frac{s^2-\lambda s+1}{s^3-\lambda s^2+s} \right)$$

Thus, in the notation of Section 2 we have

$$\begin{aligned} p_\lambda(s) &= s-\lambda \\ q_\lambda(s) &= s^3-\lambda s^2+s \\ r_\lambda(s) &= s^2-\lambda s+1 \end{aligned}$$

The least squares estimator with exponential forgetting factor for (11) then takes the following

form:

$$\left\{\begin{array}{rcl} \dot{w}_i &=& Kw_i + Lu_i, \quad (i=0,1,2) \\ \hat{y} &=& \phi_0(w) + \hat{\lambda}\phi_1(w) \\ \dot{\hat{\lambda}} &=& -\nu\phi_1(w)p(\hat{y}-y), \quad \nu > 0 \\ \dot{p} &=& -\nu(\phi_1(w)^2 p^2 - \gamma p), \quad \gamma > 0 \end{array}\right. \tag{43}$$

where $u_0 := \log(x_3)$, $u_1 := -x_3$, $u_2 := \frac{2}{x_3} - 4$,

$$K = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -k_0 & -k_1 & -k_2 \end{pmatrix}, \quad L = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

$k_0, k_1, k_2 \in \mathbb{R}$ are such that the polynomial $\kappa(s) := s^3 + k_2 s^2 + k_1 s + k_0$ is Hurwitz, and $\phi_0(w) := k_0 w_{01} + (k_1 - 1)w_{02} + k_2 w_{03} + w_{12} + w_{21}$, $\phi_1(w) := w_{03} - w_{11} - w_{22}$.
In Figure 3, the proposed reconstruction scheme is illustrated by means of a simulation. Here, the parameters were chosen as $k_0 = 512$, $k_1 = 192$, $k_2 = 24$, $\nu = 800$, $\gamma = 0.002$.

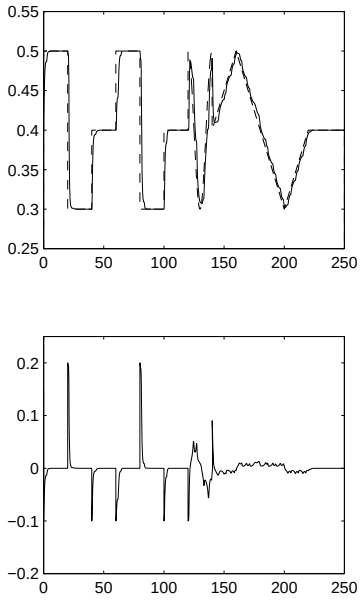

Figure 3: Simulation results for the Rössler system: (a) λ (dashed) and $\hat{\lambda}$ (solid) (b) estimation error

It may further be shown that, like in Section 3, the scheme (43) will exhibit partial synchronization once λ has been estimated correctly.

6 Conclusions

We have studied communication with chaotic systems using ideas from systems and control theory. Since in general the unknown message -which is to be reconstructed- is not available

beforehand, direct standard synchronization schemes may not be effective. We therefore propose an adaptive identification scheme that would enable the message reconstruction without explicitly assuming (partial) synchronization. This method forms a generalization of a method developed in [6] and is applicable in a far more general setting than in [6]. It should be noted that the message to be reconstructed has to be slowly time-varying, so that the identification scheme is fast enough for the reconstruction. Typically in communication this will be the case, in particular when dealing with piecewise constant (binary) messages. Moreover, the identification technique presented here is quite robust as far as channel noise is concerned, provided we are dealing with binary messages. It is clear that in this case the application of standard linear identification schemes may not provide a converging parameter estimation, but the estimator will tend towards a (small) neighborhood of the parameter. Obviously, the size of this region will depend on the measurement noise. We plan to come back on the issue of noise in communication and synchronization in a future publication. Two illustrative simulations of the proposed identification schemes are included, together with a discussion of the validity of the imposed conditions.

References

[1] Alligood, K.T., T.D. Sauer and J.A. Yorke, **Chaos - An introduction to dynamical systems**, Springer, New York, 1997.

[2] Boyd, S., and S.S. Sastry, *Necessary and sufficient conditions for parameter convergence in adaptive control*, Automatica, **22** (1986), pp. 629-639.

[3] Special Issue, *Chaos in nonlinear electrical circuits, Part A: Tutorials and reviews*, IEEE Trans. Circ. Syst. I, **40** (1993), pp. 637-786.

[4] Special Issue, *Chaos synchronization and control: theory and applications*, IEEE Trans. Circ. Syst. I, **44** (1997), pp. 853-1039.

[5] Chua, L.O., L. Kocarev, K. Eckert and M. Itoh, *Experimental chaos synchronization in Chua's circuit*, Int. J. Bif. Chaos, **2** (1992), pp. 705-708.

[6] Corron, N.J. and D.W. Hahs, *A new approach to communications using chaotic signals*, IEEE Trans. Circ. Syst. I, **44** (1997), pp. 373-382.

[7] Feldmann, U., M. Hasler and W. Schwarz, *Communication by chaotic signals: the inverse system approach*, Int. J. Circ. Theory Appl., **24** (1996), pp. 551-579.

[8] Huijberts, H.J.C, H. Nijmeijer and R.M.A. Willems, *A control perspective on communication using chaotic systems*, Proceedings CDC 1998, Tampa, USA, pp. 1957-1962.

[9] Isidori, A., **Nonlinear control systems** (2nd Edition), Springer, Berlin, 1989.

[10] Kolumbán, G., M.P. Kennedy and L.O. Chua, *The role of synchronization in digital communications using chaos – Part I: Fundamentals of digital communications*, IEEE Trans. Circ. Syst. I, **44** (1997), pp. 927-936.

[11] Nijmeijer, H., and I.M.Y. Mareels, *An observer looks at synchronization*, IEEE Trans. Circ. Syst. I, **44** (1997), pp. 882-890.

[12] Nijmeijer, H., and A.J. van der Schaft, **Nonlinear dynamical control systems**, Springer-Verlag, New York, 1990.

[13] Ott, E., **Chaos in dynamical systems**, Cambridge University Press, Cambridge, 1993.

[14] Ott, E., T. Sauer and J.A. Yorke (Eds.), **Coping with chaos: analysis of chaotic data and the exploitation of chaotic systems**, Wiley Interscience, New York, 1994.

[15] Pecora, L.M., and T.L. Carroll, *Synchronization in chaotic systems*, Phys. Review Lett., **64** (1990), pp. 821-824.

[16] Polderman, J.W., and J.C. Willems, **Introduction to mathematical systems theory - A behavioral approach**, Springer, New York, 1998.

[17] Sastry, S., and M. Bodson, **Adaptive control - Stability, convergence, and robustness**, Prentice Hall, Englewood Cliffs, 1989.

[18] Special Issue, *Control of chaos and synchronization*, Syst. Control Lett., **31** (1997), pp. 259-322.

[19] Willems, R.M.A., *Communication and synchronization for complex systems*, M.Sc. Thesis, Department of Mathematics and Computing Science, Eindhoven University of Technology, 1998.