Communication by Chaotic Signals: the Inverse System Approach

Ute Feldmann*, Martin Hasler** and Wolfgang Schwarz*

*Technical University Dresden, Faculty of Electrical Engineering
** Swiss Federal Institute of Technology, Department of Electrical Engineering
phone +49 351 463 3326 fax +49 351 463 7042 e-mail feldmann@iee.et.tu-dresden.de

ABSTRACT

The inverse system approach is an uniform view on hiding and retrieving information from chaotic signals. A clue to the understanding of the system inversion is the relative degree and in connection with it a state transformation into a normal form, both presented in the paper. Inverse system examples published so far are classified with respect to this uniform view. A general structure for system inversion is introduced and applied in a novel circuit example.

I. Introduction

Recently, the idea to use chaotic systems for information transmission has received much attention. Some of the transmission system examples can be treated from the general viewpoint of the inverse system concept. It applies to analog, discrete-time and digital systems as well. The idea is to control a chaotic system, the transmitter, with an information signal. The output of the transmitter, a chaotic broad band signal where the information is hidden, becomes after transmission the input of the receiver which has to retrieve the information signal. In order to do this, the receiver has to have an input-output relation inverse to that of the transmitter. Therefore we call it the *inverse system*. Note that both the transmitter and the

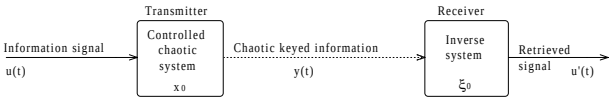

Figure 1: Inverse system principle

receiver are nonlinear dynamic systems, the former hiding the information in chaos and the latter extracting the information from chaos. Assume both are described by differential equations in case of analogue systems and by difference equations in case of discrete time systems. Further let the signals u(t) and y(t) belong to suitable signal spaces where the solution exists and is unique. Then the original system Σ and the inverse system Σ^{-1} realise the following transformations of an input signal u(t) into an output signal y(t) and vice versa:

$$y = \Sigma(u, \mathbf{x_0}) \tag{1}$$

$$u' = \Sigma^{-1}(y, \xi_0) \tag{2}$$

Thise transformations depend obviously on the initial state vector $\mathbf{x_0}$ and ξ_0 respectively. Further inverse systems meet by definition the following conditions:

$$\forall u, \mathbf{x_0}\ \exists \xi_0 : \mathbf{u = \Sigma^{-1}(y, \xi_0)\ with\ y = \Sigma(u, x_0)} \tag{3}$$

$$\forall y, \xi_0\ \exists \mathbf{x_0} : \mathbf{y = \Sigma(u', x_0)\ \ with\ u' = \Sigma^{-1}(y, \xi_0)} \tag{4}$$

i. e. an inverse system retrieves the original input exactly, at least if a suitable initial state is chosen.

In practice, the information can only be retrieved, if the inverse system reproduces every input of the original system, at least asymptotically in time, irrespective of the initial conditions of the receiver. In this case, we say that the inverse *synchronises* with the original system.

$$|u - u'| \longrightarrow 0 \text{ as } t \to \infty \tag{5}$$

Notice that the notation of inverse is symmetric in both systems, i. e. the original is the inverse of the inverse. But the notation of synchronisation is not symmetric, i. e. the original system does not necessarily synchronise with the inverse if the latter does.

Morover, an inverse system synchronises with its original if and only if it has unique asymptotic behaviour. This is clear having in mind that in case of unique asymptotic behaviour all solutions of the inverse system converge to each other and therefore also converge to the solution corresponding to the 'right' initial condition according to equ. 3. It follows that in order to serve our purpose the inverse system has to have unique asymptotic behaviour while the original has to produce a chaotic signal (which is the opposite extreme) and can obviously not synchronise.

This principle provides the exact retrieval of the original input signal under ideal transmission conditions as opposed to other proposed methods which only approximately recover the information signal (chaotic masking) or can transmit binary signals only (chaotic switching). A more thorough discussion is given in [12].

II. Relative Degree

As mentioned above one has to establish unique asymptotic behaviour of the inverse system in order to realise synchronisation. It is straight forward to regard the difference between any two solutions of the inverse system, i. e. to investigate whether the origin of the difference system is globally asymptotically stable.

In the following we will show that the inverse system can be of lower dimensionality than the original system. Thus it may be sufficient to investigate a lower dimensional difference system. The number by which the system dimension is decreased by inversion is the *relative degree* of the original system.

A. Analogue Systems

The relative degree, r, defined for bilinear systems, indicates, roughly speaking, the lowest output derivative that is directly influenced by the input. Equivalently, it is the minimal number of integrations the input signal undergoes until it reaches the output. Consider a bilinear system:

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}) + \mathbf{g}(\mathbf{x}) \cdot \mathbf{u} \tag{6}$$

$$y = h(\mathbf{x}) \tag{7}$$

Then the relative degree, r, is defined as follows [2]:

$$\mathbf{L_f L_g^{r-1}} h(\mathbf{x}) \neq \mathbf{0} \textbf{ and } \mathbf{L_f L_g^{r-2}} \mathbf{h}(\mathbf{x}) = \mathbf{0} \tag{8}$$

where $\mathbf{L_a^n} b(x)$ is the n-th Lie derivative, i. e. the n-th derivative of a real valued function $b(\mathbf{x})$ along the vector field $\mathbf{a}(\mathbf{x})$. Equs.8 express that the r-th derivative of the output is and the (r-1)th is not influenced by the input.

A clue to the understanding of the system inversion is a state transformation into a normal form according to the relative degree, r , where the output and its first r-1 derivatives are states [2]. This Transformation leads again to a bilinear system which is equivalent to the original in the sense that it has (provided a certain transformation between the initial states) the same input/output relation. The system of Fig. 3 is obviously an inverse of the system of Fig. 2. It shows that r integrators of the original system are converted into differentiators. We conclude:

(i) The inverse of an N-dimensional, relative degree equal to r system is N-r dimensional and it is therefore sufficient to consider an N-r dimensional difference system in order to decide whether synchronisation takes place or not.

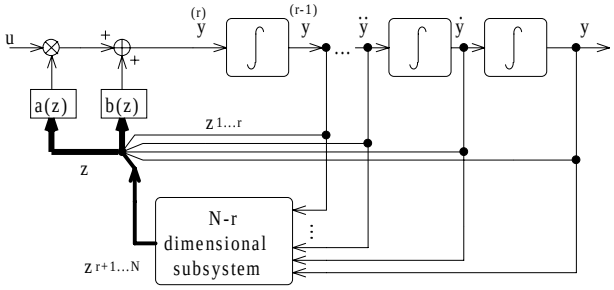

Figure 2: The structure into which every bilinear system can be transformed

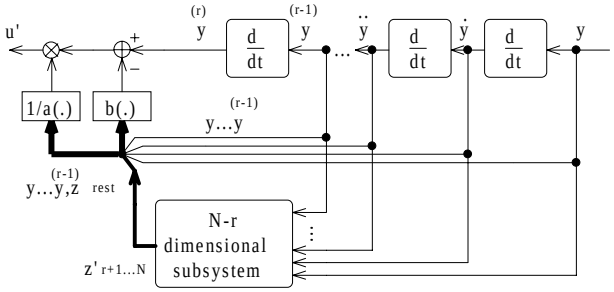

Figure 3: Inverse of the chain structure, where r former integrators have become differentiators

(ii) If the relative degree of an analogue system (assumed to be represented by state equations) is not zero then its inverse system has a generalised state representation [1], in which the state derivatives depend also on derivatives up to the r-1-th order of the input y. The output is a function of the *rest states* and the first r derivatives of y.

B. Discrete-time Systems

Translated to discrete-time systems the relative degree gives the number of time steps the current input is delayed until it directly influences the output. However, discrete-time systems with non zero relative degree cannot be directly inverted, since, as opposed to analogue systems, there is no practical realisation of an inverse of a memory element, i. e. there does not exist a causal inverse of a time delay. Therefore it is reasonable (having inversion in mind) to consider only zero relative degree discrete-time systems.

III. Classification of Known Inverse System Examples

A. Circuit Realisations

All examples published so far realize inversion by treating current and voltage of a 1-port alternatively as input and output. One of the two possible situations is depicted in

Fig. 4. The RLDiode circuit is such an example [3]. The

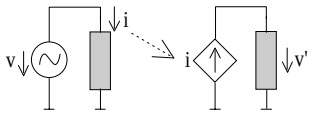

Figure 4: Inverse system realisation with a 1-port: the $V \to I \to V$ method

block diagram of the original system is shown in Fig. 5 and its inverse in Fig. 6. Obviously it is an r=1 exam-

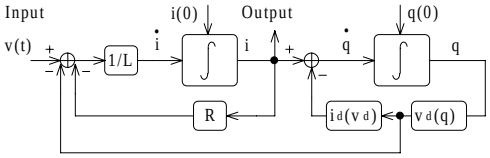

Figure 5: Block diagram of the RLDiode circuit with I: inductor current, Q: charge of the diode capacity and V_D : diode voltage

ple because there is one integrator (the inductor) between input and output which becomes a differentiator in the inverse system. Since N=2 the inverse system is N-r=1 dimensional. Asymptotic uniqueness for this is easy to

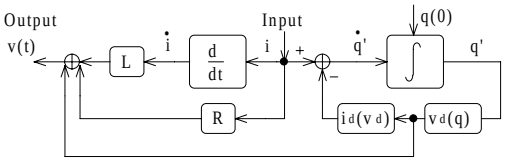

Figure 6: Inverse system of the RLDiode circuit

show with the Ljapunov function for the difference between two solutions:

$$W(Q_1, Q_2) = (Q_1 - Q_2)^2 \tag{9}$$

The derivative of 9 is negative definite which follows easily from the strictly increasing characteristics $V_D(Q)$ and $Id(V_D)$.

One simple way to realise synchronisation, i. e. unique asymptotic behaviour of the inverse system, is to choose it as an 'addition' of a linear passive circuit and a resistive element with unique response to the driving variable.

In case the inverse system is voltage driven 'addition' means a linear passiv circuit in parallel with a nonlinear voltage controlled resistor. This method was realised actually in [4] and [5] and the dual case (current driven inverse with such two elements in series) in [6] with the predestined to this Chua circuit.

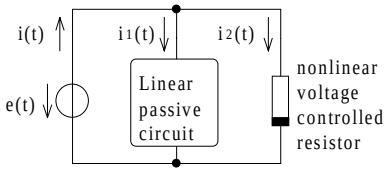

Figure 7: Circuit with unique asymptotic behaviour

Even though all examples are 1-port realisations they have different relative degrees, actually r=0 od r=1. This can be verified by drawing the block diagrams.

B. Discrete-time Systems

All discrete time system examples represent a chain structure see Fig. 8. Even old scrambling systems [9] turn out to belong to this class. The examples differ in the kind of state space and in the used nonlinear map $f(\mathbf{x}, \mathbf{u})$.

While in [3] and [7] real valued signals and the logistic map resp. the Henon map are used, in [8] and [9] digital signals and the nonlinear modular characteristic is used. Of course, due to the finiteness of state space the latter cannot be chaotic, but pseudo- random signals also serve the purpose. Since only zero relative degree systems make sense, the input immedately influences the output. The system inversion reduces to the inversion of the output equation. Since the inverse system is nonrecursive, at least

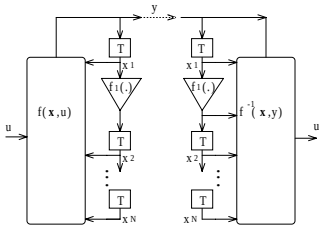

Figure 8: Chain structure and its inverse of the discrete-time system examples

after N time steps the states of both system are identical. Therefore synchronisation is obvious.

IV. Design of Inverse Systems

If a system has a relative degree r=N, its inverse is zero dimensional and simply realises a nonlinear static function of y and its derivatives. Since in this case one does not have to care about asymptotic uniqueness it seems desirable to choose input and output of a chaotic system so that r=N. However, in this case any added channel noise leads to serious errors in signal recovery because it is differentiated several times. Therefore we propose a zero relative degree structure in the sequel.

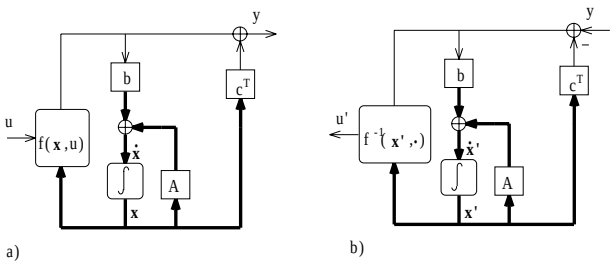

Figure 9: Genaral structure and its inverse, bold lines: vector instead of scalar, for discrete-time system the vector integrator has to be replaced by a vector delay

A. General Structure

Our proposed structure has the following features:

(1) Since it has zero relative degree, it is applicable to discrete-time systems as well.

(2) It is invertible if $f(\mathbf{x}, \mathbf{u})$ is invertible with respect to u.

(3) It contains a unique static nonlinear system which is real valued, i. e. it is similar to a Lur'e system [10].

(4) Its inverse and therefore also the difference system is a *linear* system with only a nonlinear output.

$$\Delta\dot{\mathbf{x}} = (\mathbf{A} - \mathbf{b} \cdot \mathbf{c^T}) \cdot \mathbf{\Delta x} \tag{10}$$

$$\Delta u = u_1 - u_2 = f^{-1}(\mathbf{x}, \mathbf{y} - \mathbf{c^T x_1}) - \mathbf{f^{-1}}(\mathbf{x}, \mathbf{y} - \mathbf{c^T x_2}) \tag{11}$$

(5) Synchronisation (asymptotic uniqueness of the inverse system behaviour) is because of (4) easy to establish.

(6) Provided $\mathbf{A}$ and $\mathbf{b}$ are controllable it is possible to design the synchronisation speed by setting the poles of the linear inverse system by applying the Ackermann formula in order to choose $\mathbf{c^T}$ [11].

Note an even more general structure is possible by replacing the linear function $\mathbf{c^T} \cdot \mathbf{\Delta x}$ by a common function $g(\mathbf{x})$ provided the inverse system has unique asymptotic bahaviour. At this point it becomes clear how the chaotic beaviour can be transformed into asymptotic uniqueness by system inversion:

While $\mathbf{c^T} \cdot \mathbf{\Delta x}$ (resp. $g(\mathbf{x})$) serves in the original system only as part of the output function ('forward') it becomes the recursive part in the inverse system, where it therefore decisively influences the system motion. And the nonlinear function $f(\mathbf{x}, \mathbf{u})$ obviously responsible for the chaotic motion of the original system serves in the inverse only for the output, i. e. the roles of the recursive part and the 'forward' part are exchanged under system inversion.

B. Design Example

Here we apply our general structure to Chua's circuit, which is evidently a Lur'e type system. Since its linear part is already passive we choose $\mathbf{c^T} = \mathbf{0}$. The resulting circuit and its inverse is depicted in Fig. 10. As opposed to the circuit examples published so far it is a non-1-port realisation. By simulation obtained good synchronisation results even under assumption of nonideal OPAmps.

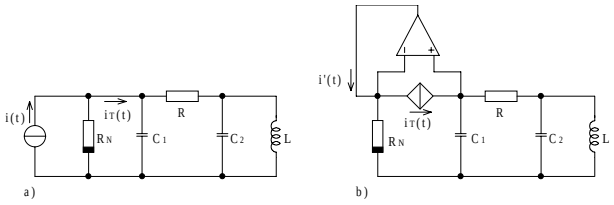

Figure 10: Design example: genaral structure applied to Chua circuit - a non-1-port realisation

References

[1] E. Delaleau and W. Respondek, 'Lowering the Orders of Derivatives of Controls in Generalized State Space Systems', to appear in Journal of Mathematical Systems, Estimation and Controll

[2] A. Isidori, 'Nonlinear control systems', 2nd edition, Springer Verlag Berlin.

[3] F. Bö hme and W. Schwarz, 'The Chaotizer-Dechaotizer-Channel', submitted to IEEE CAS I.

[4] K. S. Halle, C. W. Wu, M. Itoh and L. O. Chua, 'Spread Spectrum Communication through Modulation of Chaos', Int. J. Bifurcation & Chaos, vol. 3, no. 2, (1993) 469-477.

[5] M. Itoh, H. Murakami and L. O. Chua, 'Communication System via Chaotic Modulations', IEICE Trans. Fundamentals, vol. E77-A, no. 6 (1994) 1000-1005.

[6] C. W. Wu and L. O. Chua, 'A simple way to synchronize chaotic systems with applications to secure communication systems', Int. J. Bifurcation & Chaos, vol. 3, no. 6, (1993) 1619- 1627.

[7] P. A. Bernhardt, 'Communications using chaotic frequency modulation', Int. J. Bifurcation & Chaos, vol. 4, no. 2, (1994) 427-440.

[8] D. R. Frey, 'Chaotic Digital Encoding: An Approach to Secure Communication', IEEE CAS II, vol. 40, no. 10, (1993) 660-666.

[9] J. E. Savage, 'Some Simple Self-Synchronizing Digital Data Scramblers', Bell System Techn. J.,Febr. 1967, 449-487.

[10] M. Vidyasagar, 'Nonlinear Systems Analysis', Prentice-Hall, Englewood Cliffs N. J., 1978.

[11] G. F. Franklin, J. D. Powell, 'Digital control of dynamic systems', Addison-Wesley Publishing company, 1980.

[12] U. Feldmann, M. Hasler and W. Schwarz, 'Communication by Chaotic Signals: the Inverse System Approach', in preparation