

RESUMEN DE TESIS DOCTORAL

Reconstrucción de Parámetros y Variables de Estado para una Clase de Sistemas Caóticos con Aplicación en Codificación y Decodificación de Información

Parameter and State Variable Reconstruction for a Class of Chaotic with Application to Information Codification and De-codification

Graduated: Miguel Santiago Suárez Castañón

Centro de Investigación en Computación del IPN

Av. Juan de Dios Bátiz s/n Esq. Miguel Othón de Mendizábal C.P. 07738 México D. F.

Graduado en febrero 24, 2005

Escuela Superior de Cómputo del IPN

Av. Juan de Dios Bátiz s/n Esq. Miguel Othón de Mendizábal C.P. 07738 México D. F.

[sasuaraz@prodigy.net.mx](mailto:sasuarez@prodigy.net.mx)

Advisor: Carlos Fernando Aguilar Ibáñez

Centro de Investigación en Computación del IPN

Av. Juan de Dios Bátiz s/n Esq. Miguel Othón de Mendizábal C.P. 07738 México D. F.

caguilar@cic.ipn.mx

Resumen

En este documento se presenta el empleo de reconstructores exactos de estado y de ecuaciones integrales paramétricas para la identificación de parámetros y variables de estado de sistemas dinámicos no lineales caóticos discretos y continuos, respectivamente. En ambos casos se evita el uso de observadores de estado asintóticos y el teorema de la reconstrucción de Takens. La identificación y reconstrucción de sistemas discretos se ilustra con el sistema Lozi. El esquema de reconstrucción de estados para sistemas discretos fue usado en el diseño de un mecanismo de codificación y decodificación de información. El enfoque de reconstructores se extiende para mapas hipercaóticos y el esquema de codificación / decodificación presenta una mejora, que consiste en emplear también la señal observable como portadora de la información codificada. Las ideas desarrolladas para sistemas discretos se trasladaron a sistemas continuos, tomando integrales iterativas de forma análoga a las salidas retrasadas usadas en el diseño de los reconstructores exactos. El proceso de reconstrucción de las variables no observables se llevó a cabo mediante el diseño de ecuaciones iterativas integrales; la identificación de los parámetros desconocidos se obtiene con la solución de un sistema de ecuaciones lineales en las que las incógnitas se forman con combinaciones lineales de tales parámetros. Estos procesos se ilustran con el oscilador de Duffing y el circuito de Chua.

Palabras Clave: Reconstrucción de parámetros, Sistemas caóticos, Codificación y decodificación de información.

Abstract

In this paper we describe how to use exact state and parametric integral equations re-constructors for the identification of the state variables of dynamic chaotic discrete and continuous non-linear systems. In both cases, we avoid the use of asymptotic observers and Takens Theorem.

Identification and reconstruction of discrete systems is illustrated with Lozi's system. The state reconstruction schema for discrete systems was used in the design of an information codification and de-codification mechanism.

The re-Constructor approach is extended for hyper-chaotic maps. The codification and de-codification schema presents an enhancement that consists on using the observable signal also as porter of the codified information. The developed ideas for discrete systems are translated to the continuous case, by taking iterative integrals in the same case as the delayed outputs were used in the designing of exact re-constructors. The non-observable reconstruction process was done by the design of iterative integral equations; identification of the unknown parameters is obtained by solving a linear equation system where the unknowns are formed as lineal combinations of such parameters. All these processes are illustrated with Duffing's oscillator and Chua's circuit.

Keywords: Parameter reconstruction, Chaotic systems, Information codification and de-codification.

1 Introducción

El objetivo de la investigación fue proponer mecanismos de sincronización y reconstrucción de variables de estado y parámetros para sistemas caóticos, tanto discretos como continuos y su aplicación en codificación y decodificación de información. Para el caso discreto, algunos de los sistemas que se analizaron fueron el sistema Lozi, el sistema de infección parasitaria y los conocidos como mapas hipercaóticos. Para el caso continuo se consideraron el sistema de Duffing y el circuito de Chua.

Se pretendía diseñar un mecanismo de codificación y decodificación cuyo grado de seguridad tomara ventaja de la naturaleza caótica que algunos sistemas dinámicos presentan. Para desarrollar esta idea inicial, se decidió tomar resultados de sincronización entre sistemas caóticos continuos, como el presentado en [1]. Finalmente, se logró un mecanismo de codificación y decodificación, mediante la sincronización del sistema de Lorenz y una pseudo-copia (que es un sistema observador) de éste. En este esquema uno de los estados del sistema de Lorenz es empleado como señal de sincronización o señal observada; los dos estados restantes se emplean como llaves de codificación. El proceso de codificación se realiza mediante la adición de los valores de los estados al valor numérico de cada unidad de información (p. ej. el valor ASCII de los caracteres de un texto), previamente escalada por un factor elegido de tal forma que los valores de las unidades de información sean mucho menores que los valores de los estados usados. La decodificación de la información se realiza estimando o reconstruyendo las variables de estado usadas como llaves y aplicando la operación inversa a la usada en la codificación. Sin embargo, una deficiencia de este resultado es la lentitud en los procesos de codificación y decodificación debido al gran número de operaciones aritméticas que el método numérico empleado demanda. De aquí que se buscara la forma de incrementar la velocidad de estos procesos. Esto dio origen a dos resultados, ambos empleando sistemas caóticos discretos. El primero de ellos, presenta la derivación y empleo de reconstructores exactos de estado, y su aplicación en un mecanismo de cifrado y descifrado de información análogo al presentado en las líneas anteriores. Sobre esta misma idea se desarrolló un segundo esquema de cifrado, también basado en reconstructores exactos de estado, pero para los sistemas discretos conocidos como mapas hipercaóticos, que como se explicará en secciones posteriores, poseen características que los hacen idóneos para codificación y decodificación. Los otros dos resultados que se obtuvieron, se centraron en la forma de reconstruir parámetros y variables de estado del sistema de Duffing y del circuito de Chua, ambos sistemas continuos. Es importante señalar que los mecanismos de reconstrucción que se diseñaron para estos sistemas no pueden ser aplicados de forma general. De ahí la trascendencia de los resultados, pues como es sabido, para el caso de sistemas no lineales aún no se cuenta con soluciones o métodos de reconstrucción e identificación que puedan ser empleados de forma general.

El resto de este documento se organiza de la siguiente manera. En la Sección 2 se presentan los dos resultados obtenidos para el caso discreto. En la Sección 3 se describe un mecanismo de reconstrucción de variables de estado e identificación de parámetros para el sistema de Duffing y para el circuito de Chua, basado en parametrizaciones integrales de la salida. Finalmente, se dan las conclusiones correspondientes.

2 Reconstructores Exactos de Estado para Sistemas Discretos Caóticos y su Aplicación en Mecanismos de Codificación / Decodificación

Quizá la aportación más importante del esquema de sincronización exacta para la reconstrucción del estado de un sistema caótico discreto radica en el hecho de que el estado de un sistema discreto no lineal caótico construido n -dimensional siempre puede ser reconstruido de forma exacta, bajo el supuesto de que $n-1$ valores retrasados de la salida del sistema se conocen con precisión. Este hecho se basa en resultados obtenidos en el estudio de observabilidad no lineal en problemas de control de sistemas desde el enfoque conocido como **álgebra diferencial**. El método de diseño de reconstructores propuesto, evita el empleo de sincronización asintótica. Como es sabido, no siempre es posible construir un observador asintótico para sistemas no lineales, incluso en el caso en que el sistema sea globalmente observable. Por otra parte, también se evitó el uso del teorema de Takens, que establece la posibilidad de reconstruir un atractor mediante medidas de la serie de tiempo de una de las variables del sistema. Dada la naturaleza discreta del

Los elementos en una secuencia finita de valores avanzados de la señal de salida, y_k , están dados por,

$$\begin{aligned}
 y_k &= h(x_k) = f^{[0]}(x_k) \\
 y_{k+1} &= h(x_{k+1}) = h(f(x_k)) = (h \circ f^{[1]})(x_k) \\
 y_{k+2} &= h(f(f(x_k))) = (h \circ f^{[2]})(x_k) \\
 &\vdots \\
 y_{k+(n-1)} &= (h \circ f^{[n-1]})(x_k)
 \end{aligned} \tag{4}$$

La siguiente proposición presenta el resultado principal de este trabajo, y que establece que un sistema observable es construible.

Proposición²: *Sea el sistema no lineal caótico, $x_{k+1} = f(x_k), y_k = h(x_k)$ localmente observable, y supóngase que para el valor constante, y_e , existe un único vector de estado de equilibrio, x_e . Entonces, el sistema es construible, i.e. existe un mapeo $\varphi: \mathfrak{R}^n \rightarrow \mathfrak{R}^n$ tal, que el estado x_k del sistema puede ser reconstruido de forma exacta, a partir del tiempo $k=0$ en adelante, en términos de la salida y_k y una secuencia de valores de la salida previamente obtenidos, en la forma:*

$$x_k = \varphi(y_k, y_{k-1}, \dots, y_{k-(n-1)}), k \geq 0 \tag{5}$$

en el supuesto que la serie de valores de la salida, $\{y_k\}$ para $-n+1 < k \leq 0$, se conoce completamente. Incluso, una inicialización de (5) con una elección arbitraria de valores, $y_{-i}, i = 1, 2, \dots, n-1$, y el valor real de y_0 , aún se logra la reconstrucción exacta de x_k para toda $k \geq n-1$.

Ejemplo Ilustrativo: sistema Lozi

Sea el sistema,

$$\begin{aligned}
 x_{k+1} &= z_k \\
 z_{k+1} &= -P|z_k| + Qx_{k+1} \\
 y_k &= x_k
 \end{aligned} \tag{6}$$

² La demostración correspondiente a la proposición anterior se puede consultar en el documento original de la publicación.

Reconstrucción de Parámetros y Variables de Estado para una Clase de Sistemas Caóticos

donde y_k es la salida medible que hace disponible a la variable de estado x_k . Los parámetros del sistema se eligieron como $P=1.8$ y $Q=0.4$. El sistema es globalmente observable a partir de y_k y para un valor constante $y_k = y_e > 0$ existe un único punto de equilibrio para x y z dado por $x_e = z_e = 1/(1 + P - Q)$.

El reconstructor exacto de estado del sistema (6), esta dado por,

$$\begin{aligned} x_k &= y_k \\ z_k &= -P|y_k| + Qy_{k-1} + 1 \end{aligned} \quad (7)$$

La Figura 1 muestra la evolución del estado del sistema (6) y la reconstrucción exacta del estado z_k para una inicialización arbitraria del reconstructor ($y_{-1} = x_{-1} = 0$). El sistema (6) fue inicializado con $x_0 = 0.5$ y $z_0 = -0.4$. El incremento en el tiempo se eligió como 0.1.

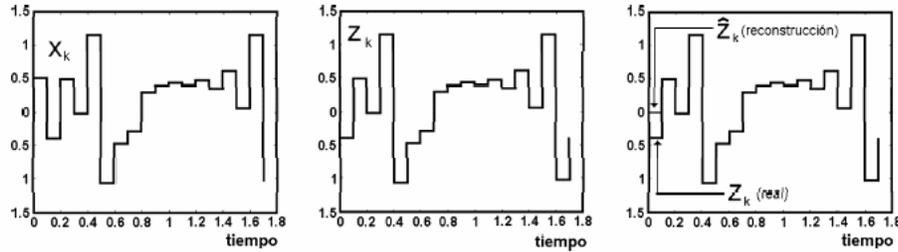


Fig. 1. Reconstrucción exacta del sistema Lozi.

3 Esquema de Codificación / Decodificación mediante Reconstructores Exactos de Estado

A partir del resultado obtenido se propuso un esquema de codificación y decodificación de información, basado en el empleo de sistemas no lineales caóticos y reconstructores exactos de estado. El esquema propuesto fue evaluado mediante un prototipo programado en el lenguaje de programación C.

Básicamente este prototipo constó de dos programas, uno para la codificación y otro para la decodificación. Las pruebas que se realizaron consistieron en codificar dos mensajes, uno formado por un texto y otro formado por una imagen en formato **bmp**. El mensaje codificado fue enviado vía correo electrónico a un destinatario remoto, quien contaba con el programa que realizaba la decodificación (este programa implantó el reconstructor exacto correspondiente al sistema caótico empleado). Después de llevar a cabo el proceso de decodificación, se constató que la recuperación fue perfecta.

El esquema de codificación / decodificación propuesto es el siguiente:

1. Las trayectorias de un sistema discreto, no lineal caótico de orden n son empleadas para codificar n diferentes mensajes $\{m_{1k}, m_{2k}, \dots, m_{nk}\}$ de forma simultánea. El proceso de codificación inicia en un tiempo k , tal que $k_i > n - 1$, es decir, $m_k = 0$, para $0 \leq k \leq n - 1$.

2. La trayectoria de salida del sistema discreto empleado, y_k es transmitida junto con los mensajes codificados.
3. En el destino, el conocimiento de los $n-1$ valores de la salida es suficiente para iniciar la reconstrucción exacta \hat{x}_k de la variable de estado $x_k, k = n, n+1, \dots$, i.e., $\hat{x}_k = x_k, k = n, n+1, \dots$.
4. El proceso de decodificación de los mensajes $x_k + m_k, k_i, k_{i+1}, \dots$, únicamente involucra remover, mediante una substracción, los valores exactos de $\hat{x}_k, k, k_{i+1}, \dots$ generados localmente, de las señales recibidas, $x_k + m_k, k_i, k_{i+1}, \dots$, obteniendo de esta forma los mensajes m_k , libres de errores.

La Figura 2 muestra el diagrama de bloques del esquema de codificación/ decodificación arriba descrito.

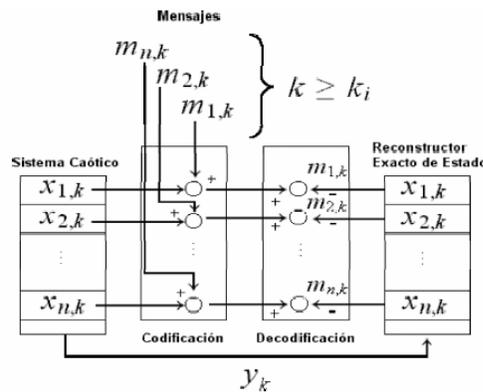


Fig. 2. Esquema de codificación / decodificación basado en reconstructores exactos de estado.

4 Sincronización de mapas Hipercaóticos para Codificación/Decodificación de Información³

En esta sección se presenta el segundo resultado obtenido en reconstrucción en sistemas discretos. Este resultado se basa en el presentado en la sección anterior. La idea principal es emplear el diseño de reconstructores exactos de estado para una clase de sistemas discretos no lineales con comportamiento hipercaótico, que tiene la particularidad de preservar volúmenes, sin importar si las condiciones iniciales de sus variables de estados se encuentran fuera del volumen. Este resultado presenta una ventaja adicional sobre el primer caso discreto previamente expuesto. Esta es que la señal de sincronización es también empleada como portadora del mensaje codificado, lo que simplifica la cantidad de información transmitida al receptor. Por otra parte, la naturaleza hipercaótica que para ciertos valores de sus parámetros presenta los mapas hipercaóticos, los hace adecuados para su empleo en codificación y decodificación de información pues presenta características como no tener atractores definidos o patrones, se pueden sincronizar en unos cuantos pasos y pueden ser fácilmente implantados en circuitos electrónicos.

Preliminares

Sea el siguiente sistema un clase de mapas iterativos no lineales, definidos como,

³ Este resultado fue presentado en WSEAS Conference en Corfú, Atenas, en Julio de 2003.

Reconstrucción de Parámetros y Variables de Estado para una Clase de Sistemas Caóticos

$$X(k+1) = F(X(k)) \quad (7)$$

donde $X(k) \in \mathfrak{R}^n$ dado por $X(k) = [x_1(k), x_2(k), \dots, x_n(k)]$, y $F(\cdot)$ es un mapa iterativo no lineal dado por,

$$F(X(k)) = [x_2(k), x_3(k), \dots, M(X(k))]^T$$

con

$$M(X(k)) = \left\{ \sum_{i=1}^{i=n} a_i x_i(k) + j \right\} \bmod 2j - j$$

$\{a_1, \dots, a_n\}$ es un conjunto de constantes y $k = \{1, 2, \dots, n\}$. En algunos casos $M(X(k))$ puede ser reemplazada por la función continua:

$$M(X(k)) = \sin\left(\sum_{i=1}^{i=n} a_i x_i(k)\right),$$

puesto que como en el caso de la función módulo, para cualquier punto x_i de la función seno que va mas allá de alguna región acotada, la función lo regresa a tal región.

Obsérvese que el polinomio característico del sistema linearizado está dado por $p(s) = a_1 + a_2 s + \dots + a_n s^{n-1}$.

Este tipo de sistemas exhiben un comportamiento caótico en los casos en los que el Jacobiano del mapa en (7) alrededor del punto de equilibrio tiene uno o mas eigenvalores fuera del círculo unitario. Es deseable que el Jacobiano de estos mapas tengan dos o mas eigenvalores fuera del círculo unitario. Cuando este es el caso, su comportamiento es hipercaótico. Otra característica muy importante de este tipo de sistemas, es que los valores de sus estados siempre están confinados en un hipercubo de dimensión n , sin importar cuales hayan sido las condiciones iniciales. Si las condiciones iniciales se encuentran fuera del hipercubo, eventualmente para alguna n -ésima iteración el vector de estado se encontrará dentro del hipercubo.

Considérese ahora una versión ligeramente modificada del sistema presentado en (7). Sea el sistema,

$$\begin{aligned} X(k+1) &= F(X(k)) = Bw(k) \\ y(k) &= H(X(k)) = x_1(k) \end{aligned} \quad (8)$$

donde $B \in \mathfrak{R}^n$ es un vector constante definido por $B = [0 \ 0 \ \dots \ \lambda]$ y $w(k) \in \mathfrak{R}$, son la salida y la perturbación externa, respectivamente, y $F(\cdot)$ es un mapa iterativo no lineal previamente definido.

Basados en la clase de sistemas descritos en (8) se propone un esquema de codificación / decodificación de información, bajo las siguientes suposiciones:

- A.1) Para cada k -iteración, se dispone de los valores de la salida $\{y(k-n), \dots, y(k-1), y(k)$, para toda $k > n$.
- A.2) La perturbación externa satisface los siguiente: $w_k = 0$, para toda $k \leq n$, y $w_k \neq 0$, para toda $k > n$.
- A.3) El conjunto de parámetros $\{a_1, \dots, a_n\}$ se seleccionan de tal manera que el polinomio característico tenga una o mas raíces fuera del círculo unitario. Las condiciones iniciales deben ser elegidas de tal forma que el sistema no presente un comportamiento periódico.

Sea el mapa iterativo caótico dado en (7). Esta clase de sistemas presentan dos propiedades importantes:

i) El mapa de observabilidad $\Psi = [h(x), h \circ F(x), \dots, h \circ F^{n-1}(x)] = X(k)$ satisface que el Jacobiano $\partial\Psi / \partial X$ es igual a la matriz identidad, por lo tanto el sistema (7) es fuertemente observable alrededor de $x=0$.

ii) Tienen un único punto de equilibrio que esta dado por $x_1(k) = x_2(k) = \dots = x_n(k) = x_e$

De acuerdo a la proposición presentada en el resultado anterior, el sistema (2.1) es construible con respecto a la salida $y(k)$. Entonces, el mapa $\Psi : \mathfrak{R}^n \rightarrow \mathfrak{R}^n$ existe, tal que el estado $X(k)$ puede ser reconstruido exactamente a partir del tiempo $k=0$, en términos de la salida $y(k)$ y una secuencia finita de valores de la salida previamente obtenidos, en la forma: $X(k) = \varphi(y(k), y(k-1), \dots, y(k-n-1)), k \geq 0$.

En la siguiente proposición se presenta el resultado principal que nos permite reconstruir la perturbación externa $w(k)$ de (8).

Proposition: Considérese el sistema (8), bajo las suposiciones **A.1** y **A.2**, entonces el siguiente estimados recupera la perturbación externa w , retrasada n -pasos con respecto a la salida y , como sigue:

$$\hat{w}(k-n) = y(k) - \left\{ \sum_{i=1}^{i=n} a_i y(k-(1+n)+i) + j \right\} \text{ mod } 2^j - j.$$

La demostración de la proposición anterior se encuentra en el documento original.

Basándose en la proposición anterior, se diseñó un esquema práctico de codificación / decodificación de información y de este esquema se desarrolló un aplicación para internet que permite establecer una comunicación segura entre dos ubicaciones remotas.

El grado de seguridad del esquema radica en la naturaleza caótica de la señal portadora y de la dificultad de reproducirla de forma exacta sin el conocimiento de las condiciones iniciales y de los parámetros empleados durante el proceso de codificación.

5 Reconstrucción de Parámetros y Variables de Estado del Oscilador Mecánico de Duffing⁴ y el Circuito de Chua⁵.

Oscilador Mecánico de Duffing.

El sistema de Duffing está formado por un barra flexible de metal colgada en el centro de una barra horizontal. En la parte inferior se encuentran dos electroimanes. Los electroimanes son excitados mediante una corriente alterna. Al circular la corriente alterna se forma un campo magnético que ocasiona que la barra flexible se mueva. La Figura 9 muestra un dibujo que ilustra el sistema. El modelo no lineal del oscilador de Duffing, está dado por:

⁴ Este resultado se publicó en la revista *Physics Letters A*, 308 (2003), pp. 47-53.

⁵ Este trabajo se publicó en la revista *Physics Letters A*, Vol. 317(2003), Issues 3-4, pp. 265-274.

Reconstrucción de Parámetros y Variables de Estado para una Clase de Sistemas Caóticos

$$\begin{aligned} \dot{x} &= v, \\ \dot{v} &= -p_1 v - p_3 x^3 + p_2 x + A \cos(\omega t) \end{aligned} \quad (9)$$

donde x mide el desplazamiento horizontal de la barra flexible. A es la magnitud de la función de fuerza, ω es la frecuencia de la fuerza, p_1 es el coeficiente de amortiguación, y p_2 y p_3 son valores constantes asociados a la función de rigidez no lineal de la barra flexible.

Para los valores de los parámetros en una vecindad de $\{p_1 = 0.4, p_2 = -1.1, A = 2.1, \omega = 1.8\}$, el sistema tiene un comportamiento caótico.

Reconstrucción de la velocidad

Considérese el sistema de Duffing y su salida $y=x$. La representación de la velocidad mediante una parametrización integral de la salida se obtiene integrando la ecuación (9) con respecto al tiempo, a partir de un tiempo inicial t_0 hasta un tiempo final t . Es decir,

$$v = v_0 - p_1(y - y_0) - p_3 \int y^3 + p_2 \int y \quad (10)$$

donde y_0 y v_0 , son las condiciones iniciales de los estados $x_0(t_0)$ y $v_0(t_0)$, respectivamente. Por lo tanto el sistema de Duffing es construible con respecto a la salida $y=x$.

Reconstrucción de los parámetros

Supóngase que los parámetros $\{p_1, p_2, p_3, A\}$ se desconocen, así como la condición inicial de v_0 . Integrando una vez con respecto al tiempo a partir de un tiempo inicial t_0 hasta un tiempo final t la ecuación (10), se obtiene la siguiente ecuación integral iterativa:

$$y - y_0 = v_0(t - t_0) + p_1 \left[y_0(t - t_0) - \int y \right] + p_2 \iint y - p_3 \iint y^3 - A \left[\frac{1}{\omega^2} \cos(\omega t) + \frac{1}{\omega} \sin(\omega t_0)(t - t_0) \right].$$

La ecuación integral iterativa anterior puede ser re-escrita de la siguiente manera:

$$\left(\frac{v_0 + p_1 y_0}{A} \right) \phi_1(t) + \left(\frac{p_1}{A} \right) \phi_2(t) + \left(\frac{p_2}{A} \right) \phi_3(t) + \left(\frac{p_3}{A} \right) \phi_4(t) + \left(-\frac{1}{A} \right) \phi_5(t) = \phi_0(t) \quad (11)$$

donde

$$\begin{aligned}
 \phi_1(t) &= t - t_0 \\
 \phi_2(t) &= -\int y \\
 \phi_3(t) &= \iint y \\
 \phi_4(t) &= -\iiint y^3 \\
 \phi_5(t) &= (y - y_0) \\
 \phi_0(t) &= \left[\frac{1}{w^2} \cos(wt) + \frac{1}{w} \sin(wt_0)(t - t_0) \right]
 \end{aligned}$$

Bajo las siguientes suposiciones, la siguiente proposición y el siguiente corolario se pueden calcular los parámetros desconocidos, cuando el sistema de Duffing tiene un comportamiento caótico.

Suposiciones:

A.1) Suponiendo que la secuencia de valores de la salida $y(t - k\tau)$ para un retardo fijo $\tau > 0$ y $k = \{0, 1, \dots, 4\}$ están disponibles para cualquier tiempo t , tal que $t > k\tau$.

A.2) Suponiendo que las funciones auxiliares $\phi_i(t - k\tau)$ para un retardo fijo $\tau > 0$ y $k = \{0, 1, \dots, 4\}$ definidas en (12), pueden ser almacenadas y calculadas.

A.3) El conjunto de parámetros del sistema no lineal (9) pertenecen a una vecindad $\{p_1 = 0.4, p_2 = -1.1, A = 2.1, w = 1.8\}$. Entonces, y debe satisfacer la siguiente ecuación diferencial canónica $\dot{y} = -p_1 y - p_3 y^3 + p_2 \dot{y} + A \cos(wt)$.

Proposición: Considérese el sistema de Duffing (9) y su parametrización integral equivalente dada por (11) y (12). Bajo las suposiciones a que nos referimos en el párrafo anterior, existe siempre un conjunto de tiempos $t_k = t - (k - 1)\tau$ para $k = \{1, 2, 3, 4, 5\}$, tal que la siguiente matriz

$$Y[t_1 : t_5] = \begin{bmatrix} \phi_1(t_1) & \cdots & \phi_5(t_1) \\ \phi_1(t_2) & \cdots & \phi_1(t_2) \\ \vdots & & \vdots \\ \phi_1(t_5) & \cdots & \phi_1(t_5) \end{bmatrix}, \tag{12}$$

tiene inversa.

La demostración puede consultarse en el documento original.

Corolario: El vector de los parámetros no disponibles $P^T = \left[\frac{v_0 - p_1 y_0}{A}, \frac{p_1}{A}, \frac{p_2}{A}, \frac{p_3}{A}, \frac{1}{A} \right]$, puede estimarse como:

$$P = Y^{-1}[t_1 : t_5] W Y[t_1 : t_5], \tag{13}$$

donde $W[t_1 : t_5] = [\phi_0(t_1), \dots, \phi_0(t_5)]$.

La demostración puede consultarse en el documento original.

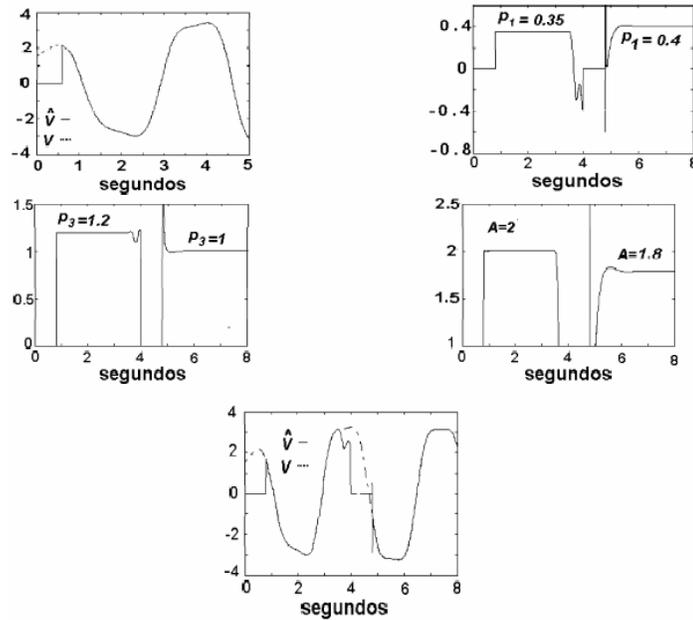


Fig. 3. Estimación de los parámetros y la velocidad.

La figura 3 muestra la velocidad estimada con respecto a la velocidad real y, la estimación de todos los parámetros al aplicar una variación abrupta en sus valores.

El método no es numéricamente intenso y es extremadamente simple para su implantación práctica. Incluso el método puede determinar variaciones lentas en los parámetros.

Circuito de Chua

En este apartado se presenta el método de reconstrucción para el circuito de Chua. El método, al igual que para el caso del sistema de Duffing, se basa en demostrar que el sistema es observable con respecto a una de sus salidas. A partir de esto, afirmamos que el sistema es construible y se puede obtener una parametrización integral de la salida medible. Empleando esta parametrización, se construye una ecuación integral iterativa de la salida. Esta ecuación contiene información necesaria para reconstruir los estados y los parámetros mediante medidas de la salida y sus respectivas integrales iterativas. Es importante destacar que este método evita el uso del teorema de Takens, que entre otras desventajas, requiere el cálculo de las derivadas de la salida, lo que introduce errores. El sistema no lineal caótico de Chua es un circuito RCL de tercer orden con cuatro elementos lineales. El sistema tiene dos capacitores, una resistencia, un inductor y un elemento no lineal. El sistema de Chua en su forma no-dimensional está dado por (ver [2]),

$$\begin{aligned}
 \dot{x}_1 &= \alpha(-x_1 + x_2 + \phi(x_1)) \\
 \dot{x}_2 &= x_1 - x_2 + x_3 \\
 \dot{x}_3 &= -\lambda x_2
 \end{aligned}
 \tag{14}$$

con

$$\phi(x) = -\left(m_1 x + \frac{m_0 - m_1}{2}(|x+1| - |x-1|)\right). \quad (15)$$

donde $x_1 = V_{C_1} / B_p, x_2 = V_{C_2} / B_p, x_3 = i_L R / B_p, u = U / B_p, \alpha = C_2 / C_1, \lambda = C_2 R^2 / L, m_1 = \bar{m}_1 R$ y $m_0 = \bar{m}$.

Para los valores constantes de los parámetros en una vecindad $\{\lambda = 28, \alpha = 15.6, m_0 = -8/7, m_1 = -5/7\}$ el sistema de Chua tiene un comportamiento caótico (ver [3])

Reconstrucción de los estados

Considérese el sistema (14). Este sistema es observable con respecto a la salida $y = x_1$, por lo tanto es construible. De ahí que sea posible obtener una parametrización integral de los estados x_2 y x_3 módulo las condiciones iniciales (ver [4]). De forma análoga a la parametrización integral del sistema de Duffing, se obtiene la parametrización integral para los estados x_2 y x_3 como:

$$\begin{aligned} x_3 &= -\frac{\lambda}{\alpha}(y - y_0) - \lambda \int [y - \phi(y)] + x_{30} \\ x_2 &= -\frac{\lambda}{\alpha}(y - y_0) + \int \phi(y) - \frac{\lambda}{\alpha} \int [y - y_0] - \lambda \iint [y - \phi(y)] + (t - t_0)x_{30} + x_{20} \end{aligned} \quad (16)$$

De (16) y (17), es posible afirmar que los estados x_2 y x_3 pueden ser medidos como funciones de la salida y módulo las condiciones iniciales.

Identificación de los parámetros

Para identificar los parámetros $\{\lambda, \alpha\}$ y las condiciones iniciales $\{x_{20}, x_{30}\}$ se obtiene la siguiente ecuación integral iterativa de la salida, donde los coeficientes de esta ecuación están formados por combinaciones de las condiciones iniciales desconocidas y los parámetros desconocidos,

$$(y - y_0) + \lambda \int [y - y_0] = \alpha \left(\iint \phi(y) + \int [\phi(y)] - y \right) - \lambda \alpha \iiint [y - \phi(y)] - \lambda \iint (y - y_0) + \frac{1}{2} x_{30} \alpha (t - t_0)^2 + x_{20} \alpha (t - t_0) \quad (17)$$

La ecuación (17) puede ser re-escrita como,

$$\sum_{i=1}^5 \lambda_i \Phi_i(t) = \Phi_0(t) \quad (18)$$

donde

$$\begin{aligned}
 \Phi_1(t) &= \iint \phi(y) + \int [\phi(y) - y], & \Phi_4(t) &= (t - t_0)^2 \\
 \Phi_2(t) &= \iiint [y - \phi(y)], & \Phi_5(t) &= t - t_0 \\
 \Phi_3(t) &= \iint [y - y_0], & \Phi_5(t) &= (y - y_0) + \int [y - y_0]
 \end{aligned}$$

y los parámetros constantes λ_i están redefinidos como:

$$\lambda_1 = \alpha, \lambda_2 = -\lambda\alpha, \lambda_3 = -\lambda, \lambda_4 = \alpha x_{30}, \lambda_5 = \alpha x_{20} \quad (19)$$

Bajo las siguientes suposiciones, la siguiente proposición y el siguiente corolario, se pueden calcular los parámetros desconocidos.

Suposiciones:

B.1) Suponiendo que la secuencia de valores de la salida $y(t - k\tau)$ para un retardo fijo $\tau > 0$ y $k = \{0, 1, \dots, 4\}$ están disponibles para todo tiempo t .

B.2) Suponiendo que las funciones auxiliares $\Phi_i(t - k\tau)$ para un retardo fijo $\tau > 0$ y $k = \{0, 1, \dots, 4\}$ definidas en (10), pueden ser almacenadas y calculadas.

Proposición: Considérese el sistema no lineal dado por (14) y sus parametrizaciones integrales iterativas dadas por (18) y (19). Bajo las suposiciones **B.1** y **B.2**, siempre existe un conjunto de tiempos $t_k = t - (k - 1)\tau$ para $k = \{0, 1, \dots, 5\}$, tal que la siguiente matriz

$$Y[t_1 : t_5] = \begin{bmatrix} \Phi_1(t_1) & \Phi_5(t_1) \\ \Phi_1(t_2) & \Phi_5(t_2) \\ \Phi_1(t_5) & \Phi_5(t_5) \end{bmatrix} \quad (20)$$

La demostración de la proposición anterior puede consultarse en el documento original.

Corolario: El vector de parámetros $\Lambda = [\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5]$ puede estimarse como, $\Lambda = Y^{-1}[t_1 : t_5]W[t_1 : t_5]$ donde $W^T[t_1 : t_5] = [\Phi_0(t_1), \dots, \Phi_0(t_5)]$.

La demostración del corolario anterior puede consultarse en el documento original.

6 Conclusiones

El objetivo fundamental de esta investigación fue proponer mecanismos de sincronización y reconstrucción para algunas clases de sistemas caóticos, tanto discretos así como continuos, y su posible aplicación a esquemas de codificación y decodificación. Se demostró que la identificación y reconstrucción es posible evitando el uso de observadores asintóticos, y por otra parte, sin el empleo del teorema de Takens, y las complicaciones inherentes al mismo, tales como

el cálculo de las derivadas, y la determinación, por ejemplo, de la dimensión del sistema caótico que se intenta reconstruir.

Quedó demostrado que es posible recuperar el estado n -dimensional de un sistema discreto no lineal caótico construible mediante un reconstructor estructural, si se cuenta con $n-1$ valores retrasados de la salida. En el caso en el que tal conjunto de valores retrasados de la salida no esté disponible, la reconstrucción aún es posible, si se permite que pasen $n-1$ pasos y los valores y_0, y_1, \dots, y_{n-1} , se vuelven disponibles. El método de diseño del reconstructor exacto, se basó en álgebra diferencial. Los resultados obtenidos en reconstrucción exacta, se probaron mediante dos sistemas discretos no lineales caóticos, y se llevaron a la práctica mediante un par de programas y se probó su efectividad en un experimento que involucró la transmisión vía Internet de un par de mensajes codificados. Los mensajes fueron codificados mediante dos de los estados del sistema que se empleó. Del lado del receptor, la decodificación se hizo empleando el programa que implantó el reconstructor exacto de estado.

Se mostró que es posible reconstruir el vector de estado de una clase de mapas iterativos, que tiene la peculiaridad de ser caóticos o hipercaóticos según los valores de sus eigenvalores, si se dispone de $(n-1)$ valores retrasados de la salida. La reconstrucción difiere completamente del enfoque tradicional que emplea observadores asintóticos, evitando así el error que éstos generan. El resultado de la reconstrucción para la clase de mapas iterativos fue aplicado a una versión modificada de los mismos, al incluir una señal de perturbación. Quedó claro que el vector de estado y la perturbación aplicada podían ser recuperadas. Además, el reconstructor únicamente requiere una señal para la sincronización, que también es la señal portadora de la información. Los resultados en reconstrucción, se verificaron con una aplicación que permite establecer comunicación segura a través de Internet. Esta aplicación permite que dos usuarios se comuniquen en línea y los mensajes que se intercambian viajan codificados.

Se propuso un método simple para revelar los parámetros desconocidos y estimar la velocidad del sistema de Duffing con base en el conocimiento de la variable de salida $y = x$ (que es la posición de la barra flexible). El método se fundamenta en el hecho de que el sistema de Duffing es observable y construible con respecto a una salida específica. Este hecho permite construir el estado restante mediante una integral iterativa de la salida del sistema. Para recuperar los parámetros desconocidos y las condiciones iniciales, primero se calcula la matriz formada por las integrales iterativas tomadas en distintos tiempos. Y luego se procede a introducir las cantidades estimadas dentro de la integral parametrizada de la salida. Este resultado permitió recuperar los parámetros desconocidos del circuito de Chua, a partir del conocimiento de la variable de salida $y = x_1$. Este método no es numéricamente intenso y es sumamente fácil de implantar. El método también es capaz de determinar pequeñas variaciones de los parámetros, además de evitar la evaluación de las derivadas de la salida.

7 Trabajo Futuro

Los resultados obtenidos para sistemas discretos fueron empleados en dos esquemas de codificación y decodificación de información, pero para el caso continuo el diseño de mecanismos de codificación y decodificación de información no se realizó por consideraciones de tiempo, por lo que tales mecanismos serán desarrollado posteriormente.

Para el caso continuo los resultados obtenidos se concretaron a el sistema de Duffing y el circuito de Chua, sistemas que son de tercer orden. Sin embargo, se considera que estos resultados pueden generalizarse para sistemas de cuarto orden. Esta línea de investigación no fue explorado en la presente tesis, por lo que será estudiada en el futuro.

Otra línea de investigación que queda abierta es la caracterización de, por lo menos de tercer orden, los sistemas caóticos que pueden ser identificables apoyándose en el teorema de Poincaré-Bendixon.

Referencias

1. **Pecora L.M. and Carroll T.L.**, Synchronization in chaotic systems, Phys. Rev. Lett., vol 64, pp. 821-824, 1990.
2. **Kapitaniak, T.**, "Chaos for engineers", Springer, second, revised edition, 2000.
3. **Alligood, T.D. Sauer, and Yorke J. A.**, "Chaos - An Introduction to Dynamical Systems" ,Springer-Verlag, New York, 1997.
4. **Fliess M. and R. Marquez**, "Continuous Time Linear Predictive Control and Flatness: A Module-Theoretic Setting with Examples", International Journal of Control, Vol. 73, pp. 606-623, 2000.



Miguel S. Suárez Castañón. *Nacido en la Ciudad de México, México. Obtuvo, en 1989, el título de Ingeniero en Cibernética y Ciencias de la Computación en la Universidad La Salle, A. C. Es Maestro en Ciencias de la Computación por parte de la Universidad Nacional Autónoma de México y obtuvo el grado de Doctor en Ciencias de la Computación, en el año 2005, en el Centro de Investigación en Computación del IPN. Recibió el premio a la Mejor Tesis de Posgrado 2005 del IPN. Actualmente es profesor de carrera en la Escuela Superior de Cómputo.*



Carlos F. Aguilar Ibáñez. *Nacido en Tuxpan, Ver., México. Obtuvo su licenciatura en física en la Escuela Superior de Física y Matemáticas del Instituto Politécnico Nacional (IPN) en 1990. Del Centro de Investigación y Estudios Avanzados (CINVESTAV) del IPN, recibió el grado de Maestro en Ingeniería Eléctrica en 1994, y de Doctor en 1999. Desde ese año y hasta la fecha ha sido investigador en el Centro de Investigación en Computación del IPN. Es miembro del Sistema Nacional de Investigadores de México desde el año 2000. Sus áreas de investigación se centran en sistemas no lineales, vibraciones mecánicas y teoría del caos.*