UNIVERSIDAD DE CANTABRIA

DEPARTAMENTO DE INGENIERÍA DE COMUNICACIONES

TESIS DOCTORAL

ESTIMACIÓN ÓPTIMA DE SECUENCIAS CAÓTICAS CON APLICACIÓN EN COMUNICACIONES

David Luengo García

Septiembre de 2006

UNIVERSIDAD DE CANTABRIA

DEPARTAMENTO DE INGENIERÍA DE COMUNICACIONES

TESIS DOCTORAL

ESTIMACIÓN ÓPTIMA DE SECUENCIAS CAÓTICAS CON APLICACIÓN EN COMUNICACIONES

Autor : David Luengo García
Directores : Carlos Pantaleón Prieto
Ignacio Santamaría Caballero

Grupo de Tratamiento Avanzado de Señal

Septiembre de 2006

Tesis Doctoral: Estimación Óptima de Secuencias Caóticas con Aplicación en Comunicaciones

Autor: David Luengo García
Directores: Carlos Pantaleón Prieto
Ignacio Santamaría Caballero

El tribunal nombrado para juzgar la tesis doctoral citada, compuesto por los señores

Presidente:

Vocales:

Secretario:

Acuerda otorgarle la calificación de

Santander, a de de 2006

A la lluvia, purificadora de impurezas
y fuente de toda vida.

El cuerpo humano es un ensamblaje de formas fractales, geometría caótica: nuestros pulmones son árboles fractales, no bolsas de aire, y nuestros cerebros son redes fractales de neuronas que transportan pensamientos caóticos. Finalmente, nuestro universo entero está aglomerado en todas las escalas, desde lo pequeño a lo grande. Somos criaturas construidas a partir del caos y que habitamos en un mundo fractal.

Ian Stewart
"¿Juega Dios a los dados?"

Agradecimientos

La redacción de los agradecimientos es probablemente la parte más agradable de la escritura de una Tesis, puesto que significa que la labor iniciada años atrás se encuentra casi acabada finalmente. Además, suponen una oportunidad única de recordar a todos aquellos que han contribuido a su realización.

Siempre que mencionaba el tema de mi Tesis (la teoría del caos) la respuesta era, invariablemente, “muy apropiado”. De nada me valía el tratar de explicar que en realidad estudio señales aparentemente aleatorias e irregulares pero con un cierto orden subyacente, y que poco tenía que ver con la concepción tradicional del vocablo. El consenso generalizado era que, dada mi naturaleza personal un tanto desordenada (literalmente caótica a juzgar de la mayoría), el caos y yo estábamos hechos el uno para el otro. Afortunadamente este cruce de caminos ha llegado al fin a buen término, y existe una larga lista de personas que han contribuido a que esto haya sido posible.

En primer lugar, quiero dar las gracias a mis dos directores de Tesis, Carlos Pantaleón e Ignacio Santamaría. Agradezco sinceramente el apoyo y la ayuda prestados a lo largo de los más de diez años de colaboración con el Grupo de Tratamiento Avanzado de Señal (G.T.A.S.), primero como “proyectando”, después como becario, y por último como “doctorando”. Asimismo deseo recordar al resto de miembros (y ex-miembros) del G.T.A.S., con los que he pasado muy buenos ratos, tanto en el trabajo como fuera de él, y que proporcionaron el marco ideal para realizar esta obra.

Me gustaría mencionar especialmente a Carlos Pantaleón, porque esta Tesis es casi tan suya como mía. La teoría del caos y su aplicación en ingeniería era una de las grandes pasiones de Carlos en el ámbito investigador, y cualquiera que le conociera sabe que se entregaba a todo fervorosamente. Él fue el primero al que le oí hablar de la teoría del caos en un curso de doctorado. Él fue el que visionó esta Tesis allá en el año 1999, y el que guió mis pasos a lo largo de casi cinco años. Gracias Carlos. Lamento profundamente que no hayas podido ver esta Tesis acabada. También debo agradecerle a Ignacio Santamaría su paciencia a lo largo de los últimos dos años y medio, en los que ha soportado estoicamente la lectura de innumerables e interminables borradores. Aunque parezca increíble, gracias a él esta Tesis tiene un tamaño “casi razonable” y no resulta aún más larga e ilegible.

En un plano más personal, resulta inexcusable agradecer el apoyo de mi familia, en especial el de mis padres, sin los cuales nunca hubiera sido posible realizar la carrera universitaria, y mucho menos emprender unos estudios de doctorado. Asimismo debo reconocer la paciencia de mi hermano, que soportó mis trabajos frente al ordenador

durante demasiadas noches (especialmente durante la carrera) sin una queja. También deseo recordar a todos mis amigos, que sin duda han contribuido a retrasar la presentación de esta memoria, pero que a cambio han proporcionado numerosos momentos irrepetibles, y sin los cuales la vida resultaría mucho más aburrida.

Por último, quiero dedicar esta Tesis a quien piensa que no existe una estructura común en la forma de dos nubes o dos cordilleras montañosas; quien cree que esos conceptos tan extraños de fractales, caos o conjugación topológica no son sino una forma rebuscada de intentar encontrar un significado a algo que no lo tiene; y quien sin embargo ha permanecido a mi lado a lo largo de estos últimos tres años, dándome ánimos en los días malos y apoyándome en todo momento. Una gran parte de esta Tesis siempre te pertenecerá, Ethel.

Resumen

Históricamente las técnicas lineales han predominado en el área del procesado de señales. Los fenómenos no lineales habitualmente se trataban de evitar o de compensar, a pesar de la pérdida de eficiencia y rendimiento globales del sistema causados por la no linealidad de cualquier elemento real. Los sistemas lineales resultan una aproximación de primer orden adecuada en muchos casos, y la teoría de los sistemas lineales ha permitido resolver un gran número de problemas de índole práctica. Sin embargo, la progresiva constatación de las limitaciones de los modelos lineales ha provocado un interés creciente por la comprensión y el aprovechamiento de los fenómenos no lineales, de los que el más interesante es, sin duda, el conocido como caos determinista o simplemente caos. Dadas las condiciones adecuadas, un sistema no lineal determinista puede generar señales que presentan características propias de señales puramente aleatorias, a pesar de su naturaleza exclusivamente determinista. Estas señales caóticas se hallan presentes por doquier, y se han observado en áreas tan dispares como meteorología, biología, economía o electrónica. En particular, en ingeniería resultan potencialmente útiles en aplicaciones tales como comunicaciones digitales, criptografía, filigranado ("watermarking"), o modelado de series temporales.

De cualquier modo, con independencia del sistema caótico, el área de conocimiento y la aplicación considerados, la utilización de las señales caóticas requiere la extracción de la información relevante contenida en las mismas en presencia de algún tipo de contaminación. En esta Tesis se proponen estimadores óptimos para secuencias caóticas generadas mediante la iteración de mapas unidimensionales y contaminadas por ruido aditivo blanco Gaussiano. Aunque estas secuencias son las señales caóticas más simples existentes, presentan todas las características distintivas del caos, y permiten capturar la esencia de muchos sistemas de mayor orden. Además, resultan de utilidad práctica en la aplicación considerada al final de la Tesis: el diseño de sistemas de comunicaciones digitales de espectro ensanchado seguros (esto es, con una baja probabilidad de intercepción de la información transmitida por parte de un usuario no autorizado).

La Tesis comienza con un primer capítulo en el que se define el concepto de caos determinista y se proporciona una breve historia del desarrollo de la teoría del caos. Adicionalmente, en este capítulo se ofrece una visión general del conjunto de problemas considerados, se presentan los objetivos y líneas de investigación perseguidos, se describe la organización de la Tesis, y se enumeran sus principales contribuciones. A continuación, en el segundo capítulo, se realiza una revisión de los conceptos fundamentales necesarios dentro del ámbito de uno de los dos pilares teóricos básicos de la

Tesis: los sistemas no lineales y la teoría del caos. Con respecto al otro pilar teórico sobre el que se sustenta la Tesis (la inferencia estadística) no se ha considerado necesario realizar una revisión del mismo, ya que la teoría clásica de la detección/estimación estadística forma parte del conjunto de herramientas conocidas por cualquier ingeniero de telecomunicación, mientras que la formación en las herramientas propias de la teoría del caos no resulta tan habitual.

Los siguientes cuatro capítulos, que conforman el núcleo de la Tesis, abordan los dos problemas teóricos considerados: la estimación de secuencias caóticas conocido el mapa generador (Capítulos 3–5), y la estimación del mapa generador (esto es, de sus parámetros) a partir de la secuencia (Capítulo 6). El problema se plantea en ambos casos desde el punto de vista de los dos marcos teóricos clásicos de la inferencia estadística: considerando los parámetros a estimar como deterministas aunque desconocidos (estimación de máxima verosimilitud, ML) y considerándolos como aleatorios con una cierta función de densidad de probabilidad (FDP) a priori (estimación Bayesiana). Aunque muchas de las consideraciones realizadas son válidas para cualquier mapa caótico, la Tesis se concentra en el estudio de mapas lineales a tramos (mapas PWL), puesto que resultan tratables analíticamente y se ha demostrado que presentan un comportamiento dinámico tan variado como el de cualquier otro mapa unidimensional, permitiendo aproximar las señales generadas por los mismos con una precisión arbitrariamente buena.

En primer lugar, en el Capítulo 3 se considera la estimación de máxima verosimilitud de la secuencia caótica conocidos el mapa generador y sus parámetros. El estimador propuesto se basa en el concepto de partición natural, que permite dividir el espacio de fases del mapa en regiones y transformar el problema de estimación de la secuencia completa en otro consistente en estimar una muestra de referencia y la serie de regiones visitadas (esto es, su itinerario). En el caso de mapas PWL se obtiene una expresión cerrada para el estimador, mientras que para otro tipo de mapas la solución óptima requiere la minimización de una función de coste no cuadrática para cada itinerario. En este caso se debe recurrir a técnicas de rejilla o métodos iterativos locales en general.

En segundo lugar, en el Capítulo 4 se considera la estimación Bayesiana de la secuencia caótica. La base de los estimadores propuestos es la existencia de una función de densidad de probabilidad (FDP) invariante asociada a todo mapa caótico unidimensional. Puesto que en la mayor parte de los casos no resulta posible obtener una expresión cerrada de la misma, se propone una aproximación constante a tramos (PWC) cuyos intervalos coincidan con la partición natural. Nuevamente se obtiene una expresión cerrada para los estimadores de máxima probabilidad a posteriori (MAP) y mínimo error cuadrático medio (MMSE o MS) en el caso de mapas PWL. Para el resto de los mapas se pueden plantear alternativas similares a las del capítulo anterior: técnicas de rejilla y métodos iterativos locales. Adicionalmente, en este capítulo se presenta un algoritmo que utiliza métodos de Monte Carlo basados en muestreo sobre cadenas de Markov (métodos MCMC, en concreto el algoritmo de Metropolis-Hastings) y que permite encontrar tanto estimadores ML como Bayesianos para cualquier mapa PWL y no PWL.

Los estimadores presentados en el Capítulo 3 y en el Capítulo 4 son óptimos y proporcionan un buen rendimiento, alcanzando el límite de Cramer-Rao asintóticamente cuando la relación señal a ruido tiende a infinito. Sin embargo, adolecen de un defecto fundamental: su coste computacional crece exponencialmente con la longitud de la secuencia. Este inconveniente (inherente a la propia naturaleza de las señales caóticas, y por lo tanto inevitable) imposibilita su utilización práctica para secuencias caóticas de longitud media/alta, y motiva la búsqueda de algoritmos computacionalmente eficientes. En el Capítulo 5 se proponen diversos algoritmos subóptimos con un coste computacional reducido, pero que alcanzan asintóticamente las prestaciones de los óptimos para valores altos de relación señal a ruido. La clave para la obtención de una buena estima de la secuencia caótica reside en conseguir una estima adecuada de su itinerario. En consecuencia, los métodos propuestos en este capítulo se concentran en conseguir una buena estima del itinerario de manera eficiente. En concreto, se consideran desde métodos muy sencillos y de rendimiento limitado (la estimación del itinerario aplicando directamente un umbral a las observaciones ruidosas), hasta otros más sofisticados y con mucho mejor funcionamiento basados en los algoritmos E-M y SAGE o el algoritmo de Viterbi, pasando por la extensión del algoritmo de predicción hacia atrás y hacia delante propuesto por Papadopoulos y Wornell.

El segundo problema teórico planteado, la estimación del mapa caótico a partir de las observaciones, se aborda en el Capítulo 6. Este problema se puede dividir a su vez en tres subproblemas: la estimación de los parámetros de un mapa caótico conocido a partir de las observaciones ruidosas (inferencia paramétrica), la estimación conjunta de la señal y de los parámetros del mapa cuya forma sigue siendo conocida (problema de suavizado), y la búsqueda de un sistema caótico que se ajuste lo mejor posible a las observaciones (modelado caótico). El Capítulo 6 se concentra en el primero de estos tres problemas. En esta ocasión el estimador ML resulta muy complejo incluso en el caso de mapas PWL, aunque se ha desarrollado un algoritmo que permite su obtención de manera aproximada para mapas unimodales con un único parámetro. Además, no existe una FDP invariante asociada para los parámetros, por lo que no resulta apropiado plantear estimadores Bayesianos. En consecuencia, se debe recurrir a métodos subóptimos en general para determinar los parámetros de un mapa caótico. Los algoritmos propuestos en esta Tesis se basan en una función de coste simplificada, que únicamente tiene en cuenta la relación entre muestras consecutivas de la secuencia caótica, y para cuya minimización se han considerado dos tipos de técnicas: métodos bloque (mínimos cuadrados (LS), mínimos cuadrados totales (TLS) y método de los momentos (MBE)) y algoritmos iterativos locales (descenso de gradiente, Newton-Raphson y un algoritmo competitivo (CLMS)). Por último, también se propone un mecanismo de estimación iterativo muy simple para el problema de suavizado basado en inferir por separado los parámetros del mapa y a continuación la secuencia generada, e ir refinando sucesivamente las estimas utilizando la información disponible de la iteración anterior.

A lo largo de la Tesis se presentan numerosas simulaciones generadas de manera sintética mediante la iteración de diversos mapas unidimensionales. No obstante, de manera adicional, en el Capítulo 7 se muestra detalladamente una posible aplicación práctica: el diseño de sistemas de comunicaciones de espectro ensanchado con baja probabilidad de intercepción. En primer lugar, en este capítulo se revisan diversas alternativas de detección para un esquema de comunicaciones caóticas bien conocido (la conmutación caótica) utilizando los estimadores óptimos y subóptimos desarrollados en los capítulos anteriores. Y a continuación se propone un esquema de comunicaciones caóticas novedoso, que denominamos codificación simbólica o caótica, basado en la transmisión de información embebida en el itinerario asociado a la señal caótica. Ambos esquemas presentan un buen funcionamiento para el canal Gaussiano (AWGC), pero no para canales más realistas (como por ejemplo los canales multitrayecto típicos de las comunicaciones inalámbricas) al igual que ocurre con la mayoría de esquemas de comunicaciones digitales convencionales. En consecuencia, el capítulo se cierra analizando la combinación del esquema de codificación propuesto con una técnica de modulación convencional (OFDM) que permite proporcionar robustez frente a la distorsión introducida por canales más realistas.

Como conclusión, esta Tesis supone fundamentalmente una aportación al planteamiento de estimadores óptimos y subóptimos de señales y mapas caóticos. Entre sus aplicaciones inmediatas se encuentran el diseño de esquemas de codificación/modulación caóticos óptimos, el desarrollo de detectores óptimos y subóptimos para sistemas de comunicaciones caóticas, el desarrollo de esquemas de "watermarking" caótico y su detección en señales de voz/audio e imágenes, y el modelado de series temporales con características caóticas tales como el ruido de fondo de señales de radar.

Abstract

Historically linear techniques have prevailed within the signal processing area. Instead of being exploited, nonlinear phenomena were usually avoided or corrected, in spite of the loss of efficiency and global performance of the system due to the nonlinear nature of any real-world element. Linear systems are an adequate first-order approximation in many cases, and linear systems theory has allowed the solution of a great deal of practical problems. Nevertheless, the progressive realization of the limitations of linear models has caused an increasing interest in the understanding and exploitation of nonlinear phenomena. The most interesting nonlinear phenomenon is, without question, the so called deterministic chaos or simply chaos. Given the adequate conditions, a deterministic nonlinear system can generate signals which show features typical of purely random signals, in spite of their strictly deterministic nature. These chaotic signals are present everywhere, and have been observed in many different areas such as meteorology, biology, economy or electronics. Particularly, in the electrical engineering field they are potentially useful in applications such as digital communications, criptography, watermarking, or time series modeling.

Anyway, regardless of the chaotic system, the knowledge area, and the application considered, the practical use of chaotic signals is subject to the availability of methods to retrieve their relevant information in the presence of some sort of distortion. In this Thesis we propose optimum estimators for chaotic signals generated by the iteration of unidimensional maps and disturbed by additive white Gaussian noise. Although these sequences are the simplest kind of chaotic signals possible, they show all the distinctive features of chaos and capture the essential behaviour of most higher order systems. Moreover, they turn out to be of practical use in the application considered at the end of the Thesis: the design of secure spread spectrum digital communications systems (i.e. systems with a high bandwidth and a low probability of interception of the transmitted information by an unauthorized user).

The Thesis starts with a first chapter where we define the concept of deterministic chaos and provide a brief history of the development of chaos theory. Additionally, in this chapter we give an overview of the set of problems considered, introduce the goals and research lines followed, describe the organization of the Thesis, and enumerate its main contributions. Then, in the second chapter, we review the basic concepts required regarding one of the theoretical basis of the Thesis: nonlinear systems and chaos theory. A review of the other theoretical area that supports the Thesis (statistical inference) is not performed, since it is usually well-known by any electrical engineer, unlike the

tools specifically connected to the analysis of chaotic signals and systems.

The next four chapters, which conform the core of the Thesis, deal with the two theoretical problems considered: the estimation of a chaotic sequence when the generating map is known (Chapters 3 to 5), and the estimation of the generating map (i.e. of its parameter set) using the noisy observations (Chapter 6). The problem is discussed in both cases from the point of view of the two theoretical frameworks commonly used in statistical inference: considering the parameters as deterministic but unknown (maximum likelihood, ML, estimation), and considering them as random with a given a priori probability density function (Bayesian estimation). Many of the discussions performed in the sequel are valid for any chaotic map. However, in this Thesis we concentrate on the study of piecewise linear (PWL) maps, since they are analytically tractable and can provide a dynamical behaviour as rich as that of any other one-dimensional map, allowing the approximation of the signals generated by them with arbitrarily good precision.

In the first place, in Chapter 3 we study the maximum likelihood estimation of the chaotic sequence when the chaotic map and its parameters are known. The proposed estimator is based on the concept of natural partition, which allows the division of the map's phase space into regions and transforms the initial problem (estimating the whole sequence) into a simpler one: estimating a reference sample and the sequence of regions visited by the map (i.e. its itinerary). Using this approach we obtain a closed-form expression for the ML estimator of piecewise linear (PWL) maps. Unfortunately, finding the optimum solution for non-PWL maps requires the minimization of a non-quadratic cost function for each itinerary. Hence, in this case we must resort to grid-search and local iterative methods in general.

In the second place, in Chapter 4 we consider Bayesian estimation of the chaotic sequence. The basis for the proposed estimators is the existence of an invariant probability density function (PDF) which can be associated to any unidimensional chaotic map. Given that in most cases we cannot obtain a closed-form expression for this PDF, in this Thesis we propose a piecewise constant approximation using the intervals given by the natural partition. Once more we develop an analytic expression for maximum a posteriori (MAP) and minimum mean square error (MMSE or MS) estimators of PWL maps. For non-PWL maps similar alternatives to those proposed in the previous chapter can be used: grid-search and local iterative methods. Additionally, an algorithm based on Markov chain Monte Carlo (MCMC) methods (more precisely, based on the well-known Metropolis-Hastings algorithm) has been developed. This technique allows us to find ML and Bayesian estimators for any chaotic map (both PWL and non-PWL).

The estimators introduced in chapters 3 and 4 are optimum and show a good performance, attaining the Cramer-Rao lower bound asymptotically when the signal to noise ratio tends to infinity. However, they have a fundamental drawback: their computational cost grows exponentially with the length of the chaotic sequence. This disadvantage (inherent to the nature of chaotic signals and thus unavoidable) renders them useless for practical application with sequences of medium/high length, and motivates the search for computationally efficient algorithms. In Chapter 5 we propose several suboptimum algorithms with a reduced computational cost, but which achieve asymptotically the performance of the optimum estimators for high signal to noise ratios. The key for obtaining a good estimate of the chaotic sequence lies in getting an adequate estimate of its itinerary. Consequently, the methods proposed in this chapter try to solve this problem (i.e. obtaining a good estimate of the itinerary efficiently). In particular, we consider very simple techniques and with a limited performance (such as estimating the itinerary by hard-censoring the observations), iterative methods (based on the E-M and SAGE algorithms), and recursive techniques (based on the extension of Papadopoulos and Wornell's forward-backward algorithm and the Viterbi algorithm).

The second theoretical problem considered, the estimation of the chaotic map using the noisy observations, is discussed in Chapter 6. This problem can be divided into three subproblems: estimating the parameters of a well-known map given the noisy observations (parametric inference), joint estimation of the chaotic signal and the parameters of the map whose general shape is still known (smoothing problem), and searching the chaotic system that provides an adequate match to the observations (chaotic modeling). Chapter 6 concentrates on the first of these three problems. Although in this case the ML estimator turns out to be too complex even for the simplest PWL maps, an algorithm which finds an approximate ML solution for unimodal maps with a single parameter has been developed. Regarding Bayesian estimation, there is no invariant PDF associated to the parameters of the map. Hence, it does not seem appropriate to consider Bayesian estimators. Thus, in this chapter we turn to suboptimum methods in general to determine the parameters of a chaotic map. The suboptimum algorithms proposed in this Thesis are based on a simplified cost function, which only takes into account the relation between consecutive samples of the chaotic sequence. In order to minimize this error two types of techniques have been considered: block methods (least squares (LS), total least squares (TLS) and a moment-based estimator (MBE)) and local iterative algorithms (gradient descent, Newton-Raphson and a competitive least mean squares algorithm, CLMS). Finally, a very simple iterative estimation scheme is proposed for the smoothing problem, based on the separate inference of the parameters and the sequence, and their successive update using the information available up to that point.

A good deal of simulations performed with chaotic signals generated synthetically through the iteration of many different unidimensional chaotic maps are shown all along the Thesis. However, additionally in Chapter 7 a potential practical application is discussed in detail: the design of chaotic spread spectrum digital communication systems with a low probability of interception. In this chapter, we review first several alternative detectors for a well-known chaotic communications scheme, chaotic switching, making use of the optimum and suboptimum estimators developed in the previous chapters. Then we propose a novel communications system, named chaotic or symbolic switching, based on the transmission of information embedded in the itinerary associated to the chaotic sequence. Both systems show a good performance for the additive white Gaussian channel (AWGC), but suffer from severe degradation in the presence of more realistic channels (eg. multipath channels typical of radio communications), just like most conventional communications schemes. Therefore, the chapter is closed studying the combination of the chaotic coding scheme proposed with a conventional modulation technique (OFDM) in order to provide a certain degree of immunity against the distortion introduced by more complex real-world channels.

In conclusion, this Thesis represents basically a contribution to the development of optimum and suboptimum estimators of chaotic signals and maps. Among its immediate applications we can emphasize the following: the design of optimum chaotic coding/modulation schemes, the development of optimum and suboptimum detectors for chaotic communication systems, the design of chaotic watermarking systems and the optimum detection of the watermarks in audio/voice and image signals, and finally the modeling and prediction of time series with chaotic characteristics such as the sea clutter which appears in radar applications.

Índice