

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

Capítulo 8

Conclusiones y Líneas Futuras

En esta Tesis se ha desarrollado un marco teórico para el planteamiento de estimadores óptimos y subóptimos de señales caóticas basado en la dinámica simbólica y el concepto de FDP invariante natural. Dentro de este contexto se han obtenido estimadores de máxima verosimilitud y Bayesianos de secuencias generadas mediante la iteración de mapas PWL, así como diversos estimadores subóptimos, aunque con mucho menor coste computacional. Adicionalmente, se ha discutido la aplicación de los métodos propuestos a la estimación de secuencias generadas por mapas no PWL, y se han propuesto estimadores para los mismos haciendo uso de los métodos MCMC.

Se ha estudiado igualmente, aunque de forma mucho menos detallada, la estimación de mapas caóticos a partir de un conjunto de muestras ruidosas. Dentro de esta línea de investigación se ha propuesto una aproximación al estimador ML de los parámetros de un mapa PWL cuya forma es conocida. Debido a la complejidad y elevado coste computacional del mismo, también se han desarrollado varios estimadores subóptimos, mucho más eficientes computacionalmente, basados en métodos bloque y algoritmos iterativos locales de gradiente estocástico usando una función de coste simplificada.

Por último, en el ámbito práctico se han analizado dos clases de técnicas adecuadas para transmitir información digital usando señales caóticas: la conmutación caótica y la codificación simbólica. En relación con la primera de ellas, se han propuesto diversos detectores subóptimos para esquemas de conmutación bien conocidos. En cuanto a la segunda, se ha propuesto una metodología de codificación novedosa que ofrece numerosas ventajas con respecto a las ya existentes. Este nuevo esquema de codificación es robusto frente al ruido Gaussiano, y puede combinarse fácilmente con OFDM para proporcionar un cierto grado de inmunidad frente a los efectos nocivos del canal.

A continuación, en la Sección 8.1 se resumen las principales aportaciones realizadas en la presente Tesis, junto con las conclusiones extraídas respecto a las diferentes líneas de investigación seguidas, organizadas alrededor de los tres problemas básicos abordados: la estimación de secuencias caóticas, la estimación de mapas caóticos, y el desarrollo de esquemas de comunicaciones caóticas. Las publicaciones resultantes de dichos trabajos de investigación se muestran en el Apéndice A. Para finalizar, en la Sección 8.2 se muestran las líneas futuras de investigación más relevantes.

8.1. Aportaciones y Conclusiones de la Tesis

8.1.1. Estimación de Secuencias Caóticas

En los capítulos 3–5 se ha detallado el marco teórico ideado para la obtención de estimadores óptimos y subóptimos de secuencias caóticas, el problema básico estudiado en esta Tesis. Dentro de esta serie de capítulos el más extenso, y el principal, es el Capítulo 3, en el que se presenta dicho marco teórico y se plantea la estimación de máxima verosimilitud. Las principales aportaciones presentadas en este capítulo son las siguientes:

1. La demostración de la equivalencia entre el problema de la estimación de la secuencia caótica y la de un único punto de la misma junto con su itinerario, y el desarrollo de una metodología, basada en la dinámica simbólica, para la aplicación de diversas técnicas de estimación estadística a la resolución del problema.
2. La obtención de expresiones cerradas para la iteración hacia delante y hacia atrás de una muestra cualquiera de la trayectoria de un mapa PWL, que permiten formular los distintos estimadores de manera cerrada.
3. El desarrollo de algoritmos para determinar la región del espacio de fases a la que debe pertenecer la muestra n -ésima de una secuencia caótica de modo que su itinerario coincida con uno dado.
4. La formulación del estimador ML de una secuencia caótica generada iterando un mapa caótico unidimensional cualquiera contaminado por AWGN, y la obtención de expresiones cerradas para mapas PWL cuando el itinerario es conocido (gracias a las ecuaciones cerradas para su iteración hacia delante y hacia atrás), y también cuando el itinerario es desconocido (gracias además a la determinación de la región del espacio de fases asociado a dicho itinerario).

En el Capítulo 4 se extiende la metodología de estimación introducida en el Capítulo 3 al ámbito Bayesiano, gracias al concepto de FDP invariante natural, que se puede asociar a cualquier mapa caótico unidimensional. En este sentido, entre las aportaciones fundamentales de este capítulo se pueden reseñar:

1. La utilización de la FDP invariante natural, obtenida teóricamente mediante el operador de Frobenius-Perron, como FDP a priori para el desarrollo de estimadores Bayesianos. En aquellos casos en que no se puede obtener una expresión analítica para dicha FDP, se propone una aproximación constante a tramos dentro de las regiones definidas por el itinerario del mapa.
2. El planteamiento del marco genérico de estimación Bayesiana de una secuencia caótica generada iterando un mapa caótico unidimensional cualquiera contaminado por AWGN, y la obtención de expresiones cerradas para los estimadores MAP y MMSE o MS de mapas PWL cuando el itinerario es conocido, así como cuando es desconocido.

3. El desarrollo de un algoritmo de estimación basado en los métodos MCMC que permite obtener tanto estimadores Bayesianos (MAP y MS) como de máxima verosimilitud (ML) para mapas caóticos unidimensionales PWL o no.

Para finalizar con esta línea de investigación, en el Capítulo 5 se proponen y analizan diversas técnicas subóptimas de estimación. Las aportaciones más destacadas de este capítulo se enumeran a continuación:

1. El estudio detallado del coste computacional de los estimadores óptimos, y la constatación de que su crecimiento exponencial con la longitud de la secuencia es intrínseco a la naturaleza de las señales caóticas, y en consecuencia irreducible para un mapa genérico.
2. La extensión del algoritmo de Papadopoulos y Wornell (al que se ha denominado FB-ML), planteado como estimador ML exacto para secuencias generadas con el TM y $\beta = 2$, a cualquier mapa PWL, aunque como estimador subóptimo en general.
3. El planteamiento de un algoritmo basado en la estimación usando la secuencia simbólica extraída directamente a partir de las observaciones ruidosas (HC-ML). Adicionalmente, este algoritmo se ha mejorado considerando la modificación únicamente de aquellos símbolos con mayor probabilidad de error, lo que permite alcanzar un compromiso entre rendimiento y coste computacional.
4. El desarrollo de varios estimadores iterativos basados en los algoritmos E-M y SAGE, y su aplicación a la estimación de secuencias generadas por mapas PWL.
5. La utilización del algoritmo de Viterbi como estimador subóptimo de la señal caótica usando un número limitado de estados (que puede ser tan reducido como el número de intervalos del mapa caótico), y como muestra de referencia la última observación de la secuencia.

Por último, como conclusiones generales más relevantes en relación con el problema de la estimación de la secuencia caótica y los diferentes estimadores analizados, se pueden destacar las siguientes:

1. Desde el punto de vista teórico es irrelevante la muestra de referencia seleccionada para la estimación, como se ha mostrado en el Capítulo 3 para secuencias cortas. No obstante, desde un punto de vista práctico puede resultar ventajoso escoger como referencia la última muestra de la secuencia, especialmente en el caso de secuencias “largas”, por tres motivos:
 - Evitar la inestabilidad numérica característica de la iteración hacia delante de mapas caóticos.
 - Eludir los problemas numéricos relacionados con las regiones cada vez más estrechas de $x[0]$ asociadas a cada itinerario conforme aumenta la longitud de la secuencia.

- Reducir el coste computacional en el caso de mapas cuyos intervalos de la partición natural se proyectan en todo el espacio de fases, ya que en este caso la región asociada a $x[N]$ es el espacio de fases completo del mapa para cualquier itinerario.
2. La clave para la obtención de una buena estima de una secuencia caótica reside en la correcta estimación de su itinerario. En consecuencia, el principal esfuerzo a la hora de desarrollar estimadores de señales caóticas debe concentrarse en plantear buenos estimadores de su secuencia simbólica. Si se dispone de una estima adecuada de la misma, cualquier valor de la muestra de referencia dentro de la región asociada proporcionará una secuencia estimada de calidad similar, en especial para señales caóticas “largas”.
 3. En todos los estimadores, tanto en los óptimos como en los subóptimos, se aprecia un “efecto umbral”: el rendimiento de los estimadores típicamente presenta uno o más saltos cuantitativos en determinados valores de SNR, hasta alcanzar el CRLB a partir de una cierta SNR. Este efecto es debido a la presencia (inevitable) de muestras de la secuencia muy cercanas al límite entre dos regiones, para las que es muy probable cometer un error a la hora de determinar su símbolo asociado por debajo de un cierto valor de SNR.
 4. Todos los estimadores propuestos alcanzan el CRLB asintóticamente conforme la SNR tiende a infinito. El valor concreto de SNR para el que se llega en la práctica al CRLB es aquel en el que no se comete virtualmente ningún error en la estimación del itinerario, y depende del mapa caótico (función y parámetros) y de la secuencia a estimar (condición inicial y longitud).
 5. La inclusión de información a priori mejora el rendimiento de los estimadores en promedio para SNRs medias/bajas (para una SNR suficientemente alta todos alcanzan el CRLB). Esta mejora de los estimadores Bayesianos con respecto al ML será mayor cuanto menos parecida sea la FDP invariante del mapa en cuestión a una FDP uniforme y cuanto menor sea la longitud de la secuencia.
 6. Los estimadores óptimos presentan un coste computacional excesivamente elevado para su uso en aplicaciones prácticas. Esto es debido a que tienen que considerar todos los posibles itinerarios de la señal, no pudiendo dejar de explorar ninguno si se desea garantizar la consecución de la secuencia óptima. No obstante, se ha comprobado que es posible obtener un rendimiento similar al de los métodos óptimos usando algoritmos subóptimos mucho más eficientes computacionalmente. En concreto, las técnicas basadas en el algoritmo de Viterbi y el SAGE son las que ofrecen un rendimiento más cercano al de los estimadores óptimos con tan sólo una fracción de su coste computacional.

8.1.2. Estimación de Mapas Caóticos

En el Capítulo 6 se estudia el problema complementario del anterior: la estimación de los parámetros de un mapa caótico. Aunque esta cuestión ha recibido una menor atención dentro de la Tesis, se han realizado una serie de aportaciones destacadas que se resumen a continuación:

1. El planteamiento y análisis del problema de la estimación de máxima verosimilitud de los parámetros de un mapa caótico. Este problema resulta mucho más difícil de resolver que el de la estimación de la secuencia caótica, ya que, incluso aunque el mapa sea lineal en sus parámetros, su iteración n -ésima nunca lo es. No se aborda la obtención de estimadores Bayesianos puesto que en esta ocasión no suponen ninguna ventaja desde el punto de vista del rendimiento, al no existir ninguna FDP a priori natural de los parámetros.
2. El desarrollo de algoritmos para determinar la región del espacio de parámetros a la que debe pertenecer el parámetro de bifurcación de un mapa unimodal y uniparamétrico de modo que su itinerario coincida con uno dado.
3. La proposición de un algoritmo que permite obtener el estimador ML de manera aproximada del parámetro de bifurcación para los mapas indicados anteriormente, y su aplicación a la familia de mapas de tienda de campaña (TM y S-TM). Además, utilizando la estima del itinerario obtenida directamente a partir de la señal ruidosa, se ha planteado un estimador HC-ML del parámetro de bifurcación similar al propuesto para la estimación de la secuencia caótica en el Capítulo 5.
4. La relajación de la función de coste a minimizar y la consideración de diversas técnicas bloque subóptimas basadas en la relación entre muestras consecutivas de la secuencia (LS, MBE y TLS), así como métodos iterativos locales, para estimar los parámetros de mapas con dependencia lineal de los mismos.
5. La formulación de un marco de estimación competitivo, aplicable a problemas distintos de los discutidos en la Tesis tales como la igualación ciega o la separación ciega de fuentes, y la obtención de un algoritmo de gradiente estocástico que proporciona buenas estimas para mapas con dependencia lineal en los parámetros. Este algoritmo permite estimar aquellos parámetros que definen los límites de la partición, como ocurre por ejemplo con el BSM, el SK-TM o el BSK-TM.

Para finalizar este apartado, seguidamente se muestran las principales conclusiones obtenidas respecto al problema de la estimación de los parámetros de mapas caóticos.

1. La estimación de los parámetros de mapas caóticos es un problema mucho más complejo que la estimación de la secuencia a causa de dos motivos principalmente:
 - En el caso de la estimación de la secuencia el problema se limita a obtener una muestra de referencia y su correspondiente itinerario, resultando su formulación similar para cualquier mapa caótico. En el caso de la estimación

de los parámetros resulta complicado plantear una formulación uniforme del problema a partir de la cual desarrollar los estimadores, ya que existen diferentes clases de parámetros. En consecuencia, habitualmente se considera la estimación de cada clase de parámetros por separado, proponiéndose técnicas de estimación específicas para cada tipo. Por ejemplo, para mapas PWL existen dos tipos de parámetros cuya obtención se discute por separado: la pendiente y el “offset” en cada intervalo, y los límites de los intervalos.

- En el caso de la estimación de la secuencia existe una clase amplia de sistemas, los mapas PWL, cuya iteración k -ésima depende linealmente de la muestra de referencia que se desea estimar, lo que permite obtener expresiones cerradas para los estimadores óptimos. En el caso de la estimación de los parámetros la relación de la iteración k -ésima del mapa con los mismos es no lineal incluso aunque la dependencia de $f(x)$ con ellos sea lineal, de modo que no se pueden formular analíticamente los estimadores óptimos ni siquiera para los mapas más sencillos.

2. La utilización de estimadores óptimos no parece viable en este caso por dos motivos:

- Se ha comprobado que el estimador ML no se puede formular analíticamente ni siquiera para los mapas más sencillos (los mapas PWL unimodales con un único parámetro), y, aunque se ha desarrollado un estimador ML aproximado, resulta muy costoso computacionalmente.
- No parece interesante el planteamiento de estimadores Bayesianos en general, ya que no existe una FDP a priori natural con la que se vayan a mejorar sustancialmente las prestaciones del estimador ML.

En consecuencia, el problema se debe abordar en general mediante algoritmos subóptimos.

3. Para secuencias cortas y mapas sencillos se ha podido estudiar el comportamiento del estimador ML aproximado. Al igual que en el caso de la estimación de la secuencia, se observa un “efecto umbral” en los estimadores ML y HC-ML: por debajo de un cierto valor de SNR el rendimiento de los estimadores es similar al de los métodos subóptimos, mientras que por encima de dicho umbral presentan un salto cuantitativo, alcanzando el CRLB a partir de entonces.
4. Las diversas técnicas subóptimas de estimación de parámetros (tanto los métodos bloque como los iterativos locales) para mapas con dependencia lineal en los mismos presentan un buen rendimiento, que mejora conforme aumenta la SNR sin llegarse a un punto de saturación aparentemente. Sin embargo, no parece que vayan a alcanzar el CRLB para valores finitos de SNR, ya que muestran unas curvas de rendimiento paralelas al mismo.

5. El algoritmo competitivo desarrollado para estimar aquellos parámetros que influyen en los límites entre regiones presenta un comportamiento similar al del resto de métodos subóptimos: su rendimiento aumenta conforme disminuye la varianza del ruido, sin observarse síntomas de saturación del mismo, pero sin alcanzarse el CRLB tampoco. Adicionalmente, en el caso de mapas con múltiples parámetros como los de Bernouilli, se ha notado la presencia de mínimos locales que indican la necesidad de un cuidadoso proceso de inicialización del mismo.

8.1.3. Comunicaciones Caóticas

Los estimadores propuestos en los capítulos 3–6 se han aplicado, en el Capítulo 7, al diseño de receptores para sistemas de comunicaciones digitales seguras y de espectro ensanchado. Las aportaciones más destacadas para esta aplicación son las siguientes:

1. La obtención de receptores subóptimos mejorados para distintos esquemas de CSK basados en los algoritmos de estimación computacionalmente eficientes propuestos en los capítulos 5 y 6.
2. El desarrollo de un esquema novedoso de comunicaciones digitales seguras y de espectro ensanchado usando señales caóticas, basado en la iteración hacia atrás y la secuencia simbólica. Para la generación de las secuencias caóticas se han analizado varios mapas, comparándolos tanto desde el punto de vista de la seguridad como del rendimiento (BER).
3. El diseño de un mapa caótico con un parámetro de control, c , que permite intercambiar rendimiento y seguridad. Cuando $c = 1$ la tasa de error del sistema es la misma que la de un modulador de BPSK, pero su seguridad es mínima. Por otro lado, cuando $c = 0$ el valor de E_b/N_0 necesario para obtener una probabilidad de error dada se incrementa en varios dB, pero a cambio la señal transmitida es más caótica, lo que presumiblemente va a dar lugar a un mayor grado de seguridad frente a la detección e interceptación del mensaje.
4. La propuesta de combinar el esquema de modulación/codificación caótica con otro esquema de comunicaciones digitales convencional, OFDM, de tal modo que se consiga simultáneamente un cierto grado de seguridad en la comunicación y protección frente a la distorsión multicamino típica de los canales de RF.

Y por último, las principales conclusiones en relación con la aplicación práctica de los estimadores y mapas caóticos considerados se muestran a continuación.

1. El mecanismo de comunicaciones caóticas propuesto presenta unas buenas prestaciones para el canal Gaussiano, pero su rendimiento se ve gravemente perjudicado cuando se considera una respuesta del canal selectiva en frecuencia.

2. La combinación del esquema de codificación caótica con OFDM proporciona los resultados previstos: inmunidad frente a desvanecimiento multicamino (es decir, una tasa de error similar a la del canal Gaussiano para canales más realistas) y seguridad frente a la interceptación por parte de usuarios indeseados.
3. El núcleo del esquema de comunicaciones planteado está formado por el mapa caótico utilizado para realizar la iteración. Su elección resulta fundamental a la hora de obtener un alto grado de seguridad y una baja tasa de error simultáneamente. En general se ha observado que existe un compromiso entre ambos parámetros de diseño: los mapas que proporcionan un alto grado de seguridad presentan peor tasa de error y viceversa. Por desgracia, aún no se ha podido encontrar un mapa óptimo que ofrezca buenos valores para ambas variables.
4. La clave de usuario que va a proporcionar la seguridad al esquema de comunicaciones ha de ser el parámetro o parámetros del mapa. Se ha comprobado que la seguridad en la condición final para la iteración hacia atrás es muy baja, mientras que existen indicios de que se puede conseguir un alto grado de seguridad en sus parámetros, ya que estos resultan mucho más complicados de estimar.

8.2. Líneas Futuras de Investigación

En esta sección se exponen diversas líneas futuras de investigación que se consideran interesantes. En primer lugar se muestran dos líneas relacionadas con la estimación de secuencias caóticas que se encuentran más desarrolladas: la estimación de una cierta clase de mapas caóticos no PWL utilizando la propiedad de conjugación topológica en la Sección 8.2.1, y la utilización de algoritmos genéticos para estimar de manera eficiente el itinerario de secuencias “largas” en la Sección 8.2.2. Y, a continuación, en la Sección 8.2.3, se agrupan otra serie de líneas futuras en torno a las tres líneas de investigación principales de la Tesis: estimación de secuencias caóticas, estimación de mapas caóticos, y aplicaciones de las señales caóticas en procesamiento de señal y comunicaciones.

8.2.1. Estimación de Secuencias Caóticas Generadas por Mapas Topológicamente Conjugados con Mapas PWL

La *topología* es una rama de la matemática, creada por Henri Poincaré a principios del siglo XX, que estudia las propiedades de las formas geométricas que permanecen inalteradas frente a deformaciones continuas. Su premisa básica es que dos objetos son equivalentes si se pueden transformar de manera suave el uno en el otro. En el caso de los mapas caóticos esta equivalencia se expresa mediante el concepto de conjugación topológica. En esencia se dice que los mapas $f(x)$ y $g(x)$ son topológicamente conjugados si existe una función $h(x)$ continua e invertible tal que

$$h(f(x)) = g(h(x))$$

para cualquier punto del espacio de fases de $f(x)$ [Devan1989]. En consecuencia, $f(x)$ se puede expresar en función de $g(x)$ y $h(x)$ o viceversa:

$$f(x) = h^{-1}(g(h(x))) \quad \Leftrightarrow \quad g(x) = h(f(h^{-1}(x))).$$

En la Figura 8.1 se muestra el esquema de las relaciones que se establecen entre dos mapas conjugados topológicamente. Puesto que $h(x)$ es invertible, a partir de un punto $x \in A$ resulta sencillo obtener el punto equivalente $y \in B$, y viceversa. Por consiguiente, la conjugación topológica es una herramienta potencialmente muy útil en el estudio de señales caóticas, puesto que permite obtener muestras de un mapa caótico a partir de otro cualquiera, siempre que se pueda encontrar una función $h(x)$ continua e invertible.

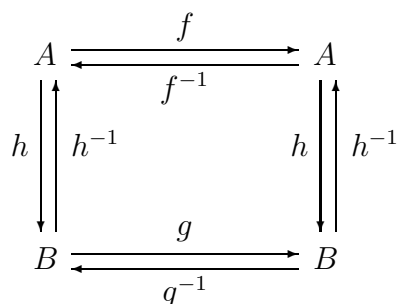


Figura 8.1: Interpretación de la conjugación topológica desde el punto de vista de la transformación entre aplicaciones matemáticas.

Estas relaciones son fácilmente extensibles a $f^k(x)$, de modo que si dos mapas, $f(x)$ y $g(x)$, son topológicamente conjugados, la trayectoria de un punto de un mapa es equivalente a la del punto apropiado del otro. Es decir, dada una condición inicial $x[0]$ para el mapa $f(x)$, su órbita presenta el mismo comportamiento cualitativo que la órbita de $h(x[0])$ para el mapa $g(x)$, y se puede obtener punto a punto la una a partir de la otra mediante la conjugación topológica $h(x)$ o su inversa $h^{-1}(x)$. La relación que se establece entre las órbitas de los dos mapas se muestra en la Figura 8.2.

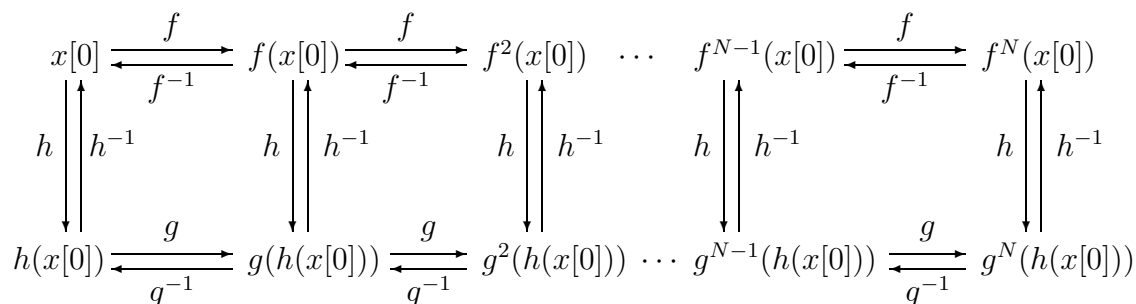


Figura 8.2: Relaciones de equivalencia entre las órbitas hacia adelante de dos mapas topológicamente conjugados.

Aunque esta forma de calcular el itinerario de una condición inicial puede parecer innecesariamente complicada, la conjugación topológica permite aprovechar los algoritmos desarrollados en los capítulos anteriores para mapas PWL con el fin de obtener estimadores ML y Bayesianos aproximados de mapas no PWL conjugados con algún mapa PWL. El planteamiento del problema es el siguiente: supóngase que se desea hallar la estima ML de la secuencia generada por un mapa caótico $g(x)$ observada en AWGN, a partir de una condición inicial desconocida $x[0]$. Si el mapa PWL $f(x)$ es topológicamente conjugado con $g(x)$ mediante $h(x)$, entonces la función de coste a minimizar para encontrar el estimador ML de la secuencia caótica se puede poner como

$$\begin{aligned} J(x[n], \mathbf{s}_{0:n-1}) &= \sum_{k=-n}^{N-n} (y[n+k] - g_{\mathbf{s}}^k(x[n]))^2 \\ &= \sum_{k=-n}^{N-n} (y[n+k] - h(f_{\mathbf{s}}^k(h^{-1}(x[n])))^2 \\ &= \sum_{k=-n}^{N-n} (y[n+k] - h(\alpha_{\mathbf{s}}^n[k]h^{-1}(x[n]) + \gamma_{\mathbf{s}}^n[k]))^2. \end{aligned}$$

El problema es que esta función de coste no es cuadrática para cada itinerario, de modo que no se puede garantizar la existencia de un único mínimo como en el caso de los mapas PWL. Además, incluso en el caso de que este mínimo sea único, resulta mucho más complicado de hallar, no existiendo una expresión analítica para el mismo en general. En consecuencia, no se consigue ninguna ventaja aplicando directamente la conjugación topológica de $g(x)$ con $f(x)$.

No obstante, cuando dos mapas son topológicamente conjugados, para cualquier órbita del primero existe una órbita equivalente del segundo. Por lo tanto, un posible procedimiento de estimación consiste en:

1. Transformar la secuencia de observaciones del mapa no PWL, $\mathbf{y} = [y[0], \dots, y[N]]^T$ en su equivalente del PWL mediante $h^{-1}(x)$, $\mathbf{z} = [h^{-1}(y[0]), \dots, h^{-1}(y[N])]^T = [z[0], \dots, z[N]]^T$.
2. Obtener la estima ML de la secuencia asociada al mapa PWL conjugado, $\hat{\mathbf{z}} = [\hat{z}[0], \dots, \hat{z}[N]]^T$, usando (3.33)–(3.35) si el itinerario es conocido o (3.44)–(3.48) si es desconocido.
3. Tomar como estima ML aproximada de \mathbf{x} la secuencia obtenida deshaciendo punto a punto la transformación mediante $h(x)$: $\hat{\mathbf{x}} = [h(\hat{z}[0]), \dots, h(\hat{z}[N])]^T$.

En el caso de los estimadores Bayesianos la idea se puede aplicar igualmente: se transforma la secuencia original al espacio del mapa PWL, se obtiene el estimador Bayesiano, y se vuelve a transformar al espacio del mapa original.

Sin embargo, aunque la conjugación topológica resulta una herramienta muy útil a priori, existen dos aspectos que dificultan su utilización en un caso práctico:

1. El conjunto de mapas no PWL interesantes conjugados topológicamente con algún mapa PWL es muy reducido. El caso más conocido es el del TM y el mapa logístico. Sea $f(x) = 1 - 2|x - 0,5|$, el TM con $\beta = 2$, y $g(x) = 4x(1 - x)$, el mapa logístico con $\lambda = 4$, la conjugación topológica entre estos dos mapas viene dada por [Devan1989]:

$$h(x) = \sin^2\left(\frac{\pi x}{2}\right) = \frac{1}{2}(1 - \cos(\pi x)).$$

Otros ejemplos son el del mapa de Ulam, $g(x) = 1 - \mu x^2$, con el TM mediante $h(x) = -\cos(\pi x)$ para $\mu = \beta = 2$ [Beck1993], o el del mapa de Isola [Isola2002],

$$f(x) = \begin{cases} \frac{x}{1-x}, & 0 \leq x \leq \frac{1}{2}; \\ \frac{1-x}{x}, & \frac{1}{2} \leq x \leq 1; \end{cases}$$

de nuevo con el TM para $\beta = 2$, mediante la función conocida como *signo de interrogación de Minkowski* (“Minkowski’s question mark function”), $?(x)$ [Vepsta2005].

2. Al aplicar una transformación no lineal a la secuencia ruidosa original para pasar al dominio del mapa PWL equivalente el ruido deja de ser Gaussiano, y además se introduce una correlación con la señal. Esto resulta evidente desarrollando $z[k] = h^{-1}(x[k] + w[k]) = h^{-1}(x[k]) + v[k]$ en serie de Taylor entorno a $x[k]$, y encontrando una expresión explícita para el ruido en el dominio transformado,

$$v[k] = \sum_{r=1}^{\infty} \frac{w[k]^r}{r!} \left. \frac{d^r h^{-1}(x)}{dx^r} \right|_{x=x[k]},$$

donde se aprecia claramente la correlación con la señal y la naturaleza no Gaussiana del ruido. En consecuencia, el rendimiento del estimador ML del Capítulo 3 podría empeorar notablemente en algunas ocasiones.

Obviamente, estas cuestiones se tienen que estudiar con mayor detalle. En primer lugar, se debe determinar la clase de mapas para los que se puede aplicar la técnica, considerándose la posibilidad de construir mapas no PWL con ciertas características deseadas a partir de mapas PWL. Y en segundo lugar, hay que analizar los efectos de la transformación sobre el ruido, estudiando la correlación y desviación de la Gaussianidad en cada caso, y como afectan al rendimiento del estimador.

8.2.2. Estimación Eficiente de Secuencias Caóticas Usando Algoritmos Genéticos

Los algoritmos genéticos fueron propuestos inicialmente por Holland en 1975 en un intento de desarrollar sistemas de inteligencia artificial inspirados en el principio biológico de la selección natural [Hollan1975]. El mecanismo de la *selección natural* fomenta la mejora de la especie mediante la supervivencia de los individuos más fuertes. Este proceso está compuesto por tres partes fundamentales:

1. Recombinación: El código genético de los progenitores se combina para generar descendientes únicos con una mezcla aleatoria del código genético de sus padres.
2. Mutación: Los genes de los hijos sufren múltiples mutaciones, que provocan que estos no sean una mera combinación de las características genéticas de los padres, y que permiten reinsertar material genético perdido en la especie.
3. Selección: Aquellos individuos que hayan heredado un material genético más adecuado tendrán una mayor probabilidad de sobrevivir, y en consecuencia de reproducirse, legando por tanto su material genético a sus descendientes y mejorando en el proceso la capacidad de adaptación y supervivencia de la especie.

Los algoritmos genéticos artificiales o simplemente *algoritmos genéticos* (GAs) son un equivalente simplificado de los algoritmos genéticos naturales, al igual que ocurre con las redes neuronales artificiales y naturales, y muchos otros métodos inspirados en principios físicos o biológicos. Dado un problema concreto, se considera su conjunto completo de soluciones como la *población total*, y cada solución particular como un *individuo* de la población. Supóngase que cada individuo viene caracterizado de manera completa y exclusiva por una serie de parámetros M -arios, es decir, que únicamente pueden tomar un número finito de M valores distintos. La idea básica consiste en partir de una población inicial de N_s individuos disponibles, muy inferior en número a la población total del problema, y aplicar sucesivamente los tres mecanismos presentes en los GAs naturales para obtener cada nueva generación:

1. Recombinación: Se seleccionan parejas de individuos, y se combinan los valores de sus parámetros de manera pseudoaleatoria para obtener la siguiente generación.
2. Mutación: Se fija una probabilidad de mutación (que puede variar a lo largo de las diferentes generaciones) y se determina aleatoriamente para cada gen de cada individuo su mutación o no.
3. Selección: Se escogen aquellos individuos (soluciones) más aptos para resolver el problema concreto planteado. En este caso, aquellas que minimicen una cierta función de coste, o equivalentemente que maximicen una determinada *función de idoneidad* (“fitness function”).

El gran interés por los algoritmos genéticos reside en que se trata de un método de búsqueda estocástica global aplicable en problemas de alta dimensión y que permite evitar mínimos locales mediante los mecanismos de recombinación y mutación. Es decir, el algoritmo va “saltando” por el espacio de soluciones aleatoriamente, obteniendo soluciones cada vez mejores en generaciones sucesivas. Si se ha diseñado de manera adecuada el algoritmo, en un tiempo infinito habrá probado todas las posibles soluciones del problema y llegará al mínimo global del mismo. En un tiempo finito lo único que se puede garantizar es que la solución final será de mejor o igual calidad que la inicial.

En el problema de la estimación de señales caóticas los diferentes individuos o soluciones del problema se encuentran caracterizados por su itinerario. Así pues, el algoritmo procede partiendo de un conjunto inicial de secuencias simbólicas y explorando el espacio de todos los posibles itinerarios mediante los mecanismos propios de los GAs, en busca del itinerario óptimo. Una vez hallado dicho itinerario, la estima ML de la secuencia caótica se puede obtener inmediatamente aplicando (3.34) y (3.35).

Para cualquier algoritmo genético se deben diseñar varios operadores. En primer lugar, hay que construir una función de idoneidad que se asociará a cada individuo de la población. Esta se puede obtener a partir de la función de coste cuadrática habitual, dada por (3.7), existiendo tres posibilidades básicas:

1. Una función de idoneidad que dependa linealmente de la función de coste,

$$I_1^i(\hat{\mathbf{x}}_{\text{ML}}^{i,k}) = \max_r J(\hat{\mathbf{x}}_{\text{ML}}^{i,r}) - J(\hat{\mathbf{x}}_{\text{ML}}^{i,k}), \quad (8.1)$$

donde i es el número de iteración (generación) y k es el individuo ($1 \leq k \leq N_s$).

2. Una función de idoneidad que dependa exponencialmente de la función de coste,

$$I_2^i(\hat{\mathbf{x}}_{\text{ML}}^{i,k}) = \exp\left(-\frac{1}{N+1}J(\hat{\mathbf{x}}_{\text{ML}}^{i,k})\right). \quad (8.2)$$

3. Una función de idoneidad basada en la posición de cada individuo dentro de la lista ordenada de acuerdo con su coste,

$$I_3^i(\hat{\mathbf{x}}_{\text{ML}}^{i,k}) = 1 + \sum_{\substack{l=1 \\ l \neq k}}^{N_s} [J(\hat{\mathbf{x}}_{\text{ML}}^{i,k}) \leq J(\hat{\mathbf{x}}_{\text{ML}}^{i,l})], \quad (8.3)$$

donde $[J(x_1) \leq J(x_2)]$ es uno si la condición lógica es cierta, y cero en caso contrario.

A continuación se tiene que diseñar el procedimiento de selección de individuos para su reproducción. La opción más simple consiste en seleccionar a los progenitores aleatoriamente de entre la población disponible de acuerdo con su idoneidad en relación con la idoneidad total. Siguiendo este procedimiento, la probabilidad de seleccionar al individuo k -ésimo dentro del conjunto de N_s individuos disponibles en la iteración i -ésima sería

$$p_s^i[k] = I_j^i(\hat{\mathbf{x}}_{\text{ML}}^{i,k})/I_T^i, \quad (8.4)$$

donde el subíndice j indica la función de idoneidad usada, e I_T es la idoneidad total de la población disponible en la iteración i -ésima:

$$I_T^i = \sum_{k=1}^{N_s} I_j^i(\hat{\mathbf{x}}_{\text{ML}}^{i,k}).$$

Nótese que, utilizando la función de idoneidad lineal de la ecuación (8.1) el peor miembro de cada generación nunca se seleccionará para tener descendencia, mientras que si se utiliza la función exponencial de la ecuación (8.2) todos tienen alguna posibilidad de ser seleccionados, aunque esta tiende a cero conforme aumenta su función de coste. Por último, usando la función basada en el ranking dada por (8.3) se evita la aparición de superindividuos cuya probabilidad sea mucho mayor que la del resto, y que por consiguiente sean seleccionados con mucha frecuencia.

Para finalizar, se deben proponer un operador de recombinación y otro de mutación. Respecto al mecanismo de recombinación, los más habituales son [Man1997]:

1. Seleccionar un punto al azar de ambos individuos e intercambiar sus genes, obteniendo de este modo los dos nuevos individuos (“one-point crossover”).
2. Generar una máscara de unos y ceros y combinar los genes de acuerdo con dicha máscara (“uniform crossover”). En este caso, la máscara se puede generar con ceros y unos equiprobables o de acuerdo con la idoneidad de cada progenitor, de tal modo que el progenitor más apto aporte un mayor número de genes.

Cualquiera de los dos métodos anteriores se puede utilizar de manera conjunta con una estrategia elitista en la que se seleccionen los N_p mejores progenitores y se propaguen directamente a la siguiente iteración sin modificación alguna, eliminándose los peores vástagos. Por último, respecto a la probabilidad de mutación, conviene mantenerla a un valor fijo y pequeño para todos los genes e iteraciones del algoritmo [Man1997].

En definitiva, las consideraciones anteriores sugieren que los algoritmos genéticos pueden resultar muy útiles como mecanismo subóptimo de estimación del itinerario, en especial para secuencias caóticas muy largas, para las que los estimadores óptimos son irrealizables y la mayoría de los estimadores subóptimos propuestos únicamente exploran un número muy reducido de secuencias simbólicas. Evidentemente, el rendimiento del algoritmo va a depender en gran medida de sus parámetros: el número de individuos de la población, la probabilidad de mutación, la función de idoneidad elegida, y los mecanismos de selección y recombinación de individuos utilizados. El estudio de las prestaciones del método para los diferentes valores de sus parámetros, y los distintos mapas y longitudes de la secuencia caótica, así como su comparación con otros métodos subóptimos, requieren un análisis más detallado.

8.2.3. Otras Líneas Futuras

En esta sección se recopilan, de manera más breve, otras ideas cuya exploración pudiera resultar interesante en el futuro. Sin embargo, en lugar de presentar estas materias al lector de manera caótica (en el sentido tradicional), se van a estructurar alrededor de los tres grandes temas tratados en la Tesis: estimación de secuencias caóticas, estimación de mapas caóticos y aplicaciones de los estimadores propuestos.

En primer lugar, en relación con el principal problema considerado en la Tesis, la estimación de señales caóticas, el planteamiento de estimadores óptimos (ML y

Bayesianos) de secuencias generadas por mapas PWL unidimensionales ha quedado completamente resuelto. En consecuencia, las líneas futuras de investigación en este área se centran en la extensión de los estimadores óptimos a otras clases de mapas, así como en el desarrollo de estimadores computacionalmente eficientes. Adicionalmente a las dos líneas presentadas con detalle en las secciones 8.2.1 y 8.2.2 cabe destacar las siguientes líneas de investigación:

1. La extensión de los estimadores desarrollados a secuencias generadas por mapas PWL d -dimensionales, probablemente usando la versión discontinua del modelo canónico de Chua (CPWL), propuesta originalmente en [Kang1978], para obtener una representación parsimoniosa del mapa.
2. La evaluación del rendimiento de los estimadores ML y Bayesianos de secuencias generadas por mapas no PWL usando métodos de rejilla o iterativos para obtener las estimas locales en cada región, y la determinación de la clase de mapas no PWL con un único mínimo por región (es decir, la clase para la que los métodos iterativos locales son capaces de proporcionar la estima ML o MAP exacta).
3. La utilización de técnicas de decodificación en esfera (“sphere decoding”, SD), introducidas originalmente para encontrar vectores con norma pequeña en celosías [Fincke1985] y usadas actualmente para resolver diversos problemas en el área de las comunicaciones digitales, como algoritmo computacionalmente eficiente para la estimación del itinerario. Adicionalmente, puede resultar interesante su combinación con el algoritmo de Viterbi de un modo similar al propuesto por Vikalo y Hassibi [Hassi2005, Vikalo2005] para limitar el coste computacional en el peor caso de los métodos SD.
4. El desarrollo de algoritmos para la predicción y el filtrado de señales caóticas basados en los métodos propuestos en la Tesis para problemas de suavizado (esto es, el caso en que se dispone a priori del bloque completo de estimaciones) y técnicas adaptativas de estimación del estado de un sistema dinámico tales como el filtro de Kalman o los filtros de partículas.
5. El estudio detallado del problema de la detección de señales caóticas, incluyendo sus semejanzas y diferencias con el problema de estimación abordado en la Tesis, y la aplicabilidad de los algoritmos planteados.

Respecto al segundo problema teórico abordado en la Tesis, la estimación de mapas caóticos, las líneas futuras se concentran en torno a dos temas: el planteamiento de estimadores subóptimos, y el estudio de los problemas de estimación conjunta y modelado.

1. El análisis detallado de la clase de mapas para los que la implementación eficiente del estimador ML, descrita en la Sección 6.3, proporciona resultados exactos. Es decir, la demostración de que para una determinada clase de mapas la función

de coste nunca puede tener más de un mínimo dentro de la región del espacio de parámetros asociada a un cierto itinerario.

2. El estudio de la convergencia del algoritmo de estimación competitivo presentado en la Sección 6.5 (en especial para mapas multimodales), y la consideración de su uso para otras aplicaciones distintas de la estimación de señales caóticas: igualación ciega, separación ciega de fuentes, problemas de “clustering”, etc.
3. El desarrollo de versiones adaptativas de los métodos de estimación bloque subóptimos propuestos en la Sección 6.4, basados en los algoritmos LMS y TLMS (versión adaptativa del TLS [Fheng1998]). Asimismo, puede resultar interesante la aplicación de técnicas de estimación del estado tales como el filtro de Kalman o el filtro extendido de Kalman (ya propuestos en [Leung1997] para un caso particular) o filtros de partículas.
4. La utilización del algoritmo E-M para la estimación conjunta de una señal caótica y los parámetros del mapa generador.
5. El estudio de la capacidad de modelado de señales caóticas mediante mapas PWL, prestando especial atención a dos aspectos:
 - La selección del orden del modelo, tratando de encontrar un criterio que combine la capacidad de modelado de la dinámica de la señal caótica (esto es, de sus medidas invariantes), el error cuadrático medio y la complejidad del modelo (es decir, el número de parámetros).
 - La extensión de los métodos de estimación de los parámetros propuestos al caso de mapas PWL d -dimensionales, usando de nuevo probablemente el modelo CPWL para su formulación, y el análisis de su capacidad de modelado para diferentes tipos de sistemas caóticos, tanto continuos como discretos.

Por último, en relación con las aplicaciones de los estimadores propuestos se consideran tres líneas futuras principales:

1. El análisis en profundidad de los esquemas de comunicaciones digitales propuestos, destacando los siguientes puntos de interés:
 - La comparación del grado de seguridad ofrecido por los distintos mapas y sistemas de comunicación posibles (desde el punto de vista de la detección e interceptación de la información transmitida) en función de la clave utilizada, y considerando mecanismos realistas para la estimación de la misma por parte de un intruso que no la conozca.
 - La búsqueda del mapa idóneo que ofrezca el mejor compromiso posible entre seguridad y buenas prestaciones, y que disponga de algún parámetro que permita regular ambas.

- El aprovechamiento de la existencia de secuencias simbólicas inválidas en algunos mapas caóticos para plantear un mecanismo de codificación de canal que mejore las prestaciones de los esquemas propuestos.
 - El estudio de los diferentes esquemas, combinados con OFDM, para canales más realistas, y con mecanismos prácticos de sincronización, estimación de canal, igualación, etc.
 - El análisis de otras características importantes de la señal OFDM, como por ejemplo la relación potencia de pico a potencia media (PAR o PAPR), obtenidas al utilizar señales caóticas para codificar la información de cada subportadora.
2. La consideración de esquemas de comunicaciones digitales caóticas alternativos a los aquí propuestos, así como el diseño de secuencias de espectro ensanchado a partir de señales caóticas o sus secuencias simbólicas asociadas.
 3. El diseño de algoritmos de filigranado (“watermarking”) caótico similares a los esquemas de comunicaciones caóticas propuestos, ya que el problema del “watermarking” puede verse como un problema de comunicaciones con información lateral [Cox1999]. Aún así, existen diferencias relevantes con un problema de comunicaciones convencional, que pueden requerir modificaciones importantes de los esquemas presentados en el Capítulo 7. Deben examinarse cuidadosamente, entre otros, los siguientes aspectos:
 - Las restricciones impuestas por la necesidad de que la filigrana no afecte a la calidad de la información marcada, intentando a su vez que sea transmitida con la mayor fiabilidad posible.
 - La robustez de la filigrana frente a manipulaciones por parte de usuarios malintencionados.
 - Los efectos de la distorsión introducida en la filigrana como resultado del procesado normal de la información.
 4. La aplicación de los mapas PWL al modelado y predicción de series temporales, para lo cual es necesario extender los estimadores propuestos para mapas unidimensionales al caso de mapas d -dimensionales, como ya se ha indicado previamente.

