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 7

Aplicación: Comunicaciones de Espectro Ensanchado Caóticas

7.1. Introducción

En los capítulos anteriores no se ha mostrado ninguna aplicación práctica que justifique el interés por el problema de la estimación de señales y sistemas caóticos. En el campo de la ingeniería eléctrica y electrónica, al igual que en otras muchas disciplinas, existen múltiples áreas en las que el caos presenta numerosas aplicaciones potenciales: el diseño de nuevos dispositivos electrónicos con mejores características (menor consumo, mayor rapidez de funcionamiento y/o ancho de banda, compatibilidad electromagnética mejorada, etc.), el análisis y modelado de comportamientos anómalos y/o transitorios de dispositivos electrónicos convencionales, el análisis de señales biomédicas, la generación de números aleatorios, el filigranado ("watermarking"), la criptografía, etc. No obstante, este capítulo se concentra en el análisis de una sola aplicación: el diseño de sistemas de comunicaciones digitales de espectro ensanchado usando señales caóticas.

Este capítulo consta únicamente de dos secciones adicionales. En primer lugar, en la Sección 7.2 se exponen las principales características de las señales y sistemas caóticos que resultan interesantes en comunicaciones, así como algunas de las cuestiones más importantes que deben resolverse aún para que los sistemas de comunicaciones caóticos puedan competir con los sistemas convencionales. A continuación se revisan brevemente los esquemas de comunicaciones caóticas más relevantes propuestos hasta la fecha, haciendo especial énfasis en sus ventajas e inconvenientes.

Y en segundo lugar, en la Sección 7.3 se proponen dos posibles esquemas de sistemas de comunicaciones digitales caóticas, analizándose su rendimiento al utilizar los estimadores desarrollados en los capítulos 3–6. En concreto, para el canal aditivo Gaussiano se han considerado dos esquemas distintos. El primero de ellos se basa en la conmutación de alguno de los parámetros de un mapa caótico en función del símbolo a transmitir. En el receptor se debe decidir cual de los K conjuntos de parámetros ha generado la señal recibida con mayor probabilidad. En el segundo se genera la señal transmitida iterando hacia atrás un mapa caótico cuya secuencia simbólica viene determinada por los

símbolos a transmitir. En el receptor se utiliza el algoritmo de Viterbi con un número de estados reducido para detectar los símbolos transmitidos. Por último, para canales multitrayecto, en lugar de tratar de diseñar un igualador en el dominio temporal que elimine la distorsión introducida por el mismo, se ha estudiado la combinación del segundo esquema propuesto con un técnica de modulación/multiplexación convencional que proporciona una cierta inmunidad frente a la distorsión del canal: la modulación por división en frecuencias ortogonales (OFDM). En este caso la igualación resulta mucho más sencilla y se puede llevar a cabo en el dominio frecuencial.

7.2. Sistemas de Comunicaciones Caóticas

El interés por los sistemas de comunicaciones caóticas surge a raíz de un descubrimiento clave realizado por Pecora y Carroll en 1990 [Pecora1990]: la posibilidad de sincronizar dos sistemas caóticos independientes utilizando una señal unidimensional procedente del primero como entrada del segundo. Apenas dos años después Chua, Oppenheim y colaboradores proponían los primeros esquemas de comunicaciones caóticas: sistemas de conmutación y enmascaramiento caótico [Kocar1992, Oppen1992, Parlit1992]. Desde entonces numerosas variantes de los mismos han sido propuestas y una gran cantidad de mecanismos novedosos para la transmisión de información usando señales caóticas desarrollados. En la Sección 7.2.2 se revisan los principales esquemas presentados a lo largo de los últimos tres lustros agrupados en cuatro categorías:

1. Sistemas que usan la señal caótica para ocultar la verdadera señal de información transmitida: **enmascaramiento caótico**.

2. Sistemas que transmiten la información modulando algún parámetro de la señal caótica: **conmutación caótica** y **CSK**.

3. Sistemas en los que la señal de información se encuentra contenida en la secuencia simbólica de la señal caótica generada: **codificación simbólica** o **caótica**.

4. Sistemas de espectro ensanchado (SS) convencionales, tanto por secuencia directa (DS) como por salto en frecuencia (FH) o en el tiempo (TH), que utilizan secuencias de ensanche obtenidas a partir de señales y sistemas caóticos en lugar de las clásicas secuencias PN: **espectro ensanchado caótico**.

Sin embargo, con anterioridad, en la Sección 7.2.1 se enumeran las características más destacadas de las señales y sistemas caóticos que han provocado un amplio interés por el desarrollo de sistemas de comunicaciones caóticas. En dicha sección se discuten igualmente los principales desafíos y problemas generales que deben resolverse para conseguir que dichos sistemas sean competitivos frente a los esquemas de comunicaciones convencionales. Los problemas específicos de cada esquema propuesto se mencionan posteriormente, en la Sección 7.2.2, conforme se revisan los mismos.

7.2.1. Comunicaciones Caóticas: Ventajas y Desafíos

A continuación se discuten las principales ventajas e inconvenientes de los sistemas de comunicaciones caóticas. Debe tenerse en cuenta que las comunicaciones caóticas distan mucho de ser un área madura de investigación, encontrándose por el contrario todavía en su infancia. En consecuencia, la mayoría de las ventajas enumeradas pueden considerarse potenciales: son puramente teóricas o han sido confirmadas únicamente en condiciones experimentales. Otro tanto ocurre con sus inconvenientes: es posible que muchos de ellos no supongan dificultades serias reales, siendo resueltos fácilmente a corto o medio plazo. Así pues, en resumen, aunque en la actualidad el rendimiento de los sistemas caóticos aún no sea competitivo con el de los sistemas convencionales, desde el punto de vista de su robustez y tasa de errores, resulta difícil predecir su evolución futura.

7.2.1.1. Características y Ventajas de las Señales Caóticas

Las señales caóticas son señales generadas por sistemas estrictamente deterministas pero que presentan muchas características propias de señales puramente aleatorias. Esta naturaleza dual, determinista/aleatoria, provoca que exhiban una combinación de propiedades típicas de ambas clases de señales, de las cuales resultan interesantes en el ámbito de las comunicaciones las siguientes [Kenne1997, Silva2000b, Lau2003]:

1. La posibilidad de generarlas mediante reglas deterministas muy simples, especialmente en el caso de señales discretas: un sencillo mapa unidimensional y unimodal es capaz de generar secuencias caóticas.

2. Su sensibilidad extrema a las condiciones iniciales, a los parámetros del sistema generador e incluso a la implementación, que se manifiesta en la capacidad de generar secuencias completamente diferentes a medio/largo plazo realizando cambios mínimos en el sistema caótico.

3. Su carácter aperiódico, aunque con la presencia de patrones reconocibles cuasi repetitivos, pero con frecuencias de aparición y amplitudes muy variables.

4. Su aspecto similar al ruido blanco, con una función de autocorrelación de tipo impulsivo (esto es, con una caída muy rápida, típicamente exponencial) y una densidad espectral de potencia continua y de banda ancha (es decir, con una distribución de potencia que decae muy lentamente con la frecuencia y que muestra una cantidad de potencia significativa a lo largo de un amplio rango frecuencial).

5. La baja correlación cruzada entre distintas señales caóticas, tanto entre las generadas por distintos sistemas como entre las generadas por el mismo sistema pero con distintos parámetros y/o condiciones iniciales.

Estas propiedades características de las señales caóticas son las causantes de su atractivo a la hora de implementar sistemas de comunicaciones digitales. En particular,

su aspecto similar al ruido, con una autocorrelación de tipo impulsivo y una densidad espectral de potencia de banda ancha, y su baja correlación cruzada provocan que los sistemas de comunicaciones caóticas compartan las siguientes ventajas de los sistemas de espectro ensanchado frente a los sistemas de banda estrecha [Kenne1996, Kenne1997, Lau2003]:

1. Su baja probabilidad de detección ("Low Probability of Detection", LPD) e intercepción ("Low Probability of Interception", LPI) debido al bajo nivel de su DEP, que puede ser incluso inferior al nivel del ruido de fondo, y a la necesidad de conocer la secuencia de ensanche en el receptor para poder recuperar la señal de información.

2. Un cierto grado de protección frente a los efectos del multicamino, causante del desvanecimiento selectivo en frecuencia, así como frente a interferencias de banda estrecha, tanto intencionadas ("jamming") como no intencionadas, debido a que la potencia de la señal está repartida a lo largo de un amplio rango de frecuencias.

3. Mucha menor interferencia tanto con otros sistemas de comunicaciones de espectro ensanchado (caóticos o no) como con sistemas de banda estrecha, lo que les convierte en ideales para su uso en las bandas de transmisión sin licencia (bandas ISM, "Industrial, Scientific and Medical") utilizadas actualmente por las redes de área local inalámbricas (WLANs) o Bluetooth por ejemplo, y que facilitaría la migración de los sistemas convencionales a los caóticos en el futuro.

Además, la baja correlación cruzada entre señales caóticas permite diseñar sistemas de acceso múltiple caóticos similares al CDMA, con las ventajas que esto supone frente a otras alternativas de acceso multiusuario (como FDMA o TDMA) [Lau2003]:

1. Aumento de la capacidad del sistema (se ha estimado que la capacidad de una red celular basada en CDMA es entre 3 y 7 veces superior a la de una red basada en TDMA [Gilhou1991]), con mayor flexibilidad a la hora introducir nuevos usuarios.

2. Simplificación del diseño del sistema celular, ya que se trata generalmente de redes de una sola frecuencia ("Single Frequency Networks", SFNs), de modo que se elimina el costoso proceso de planificación frecuencial necesario en redes celulares basadas en FDMA o TDMA.

3. Capacidad de promediado de la calidad de los distintos usuarios. Puesto que todos los usuarios usan todo el ancho de banda del canal durante todo el tiempo, no existe el peligro de que la calidad de un usuario se vea degradada por utilizar un recurso (ranura temporal o frecuencial) que presente peores características: en promedio la calidad experimentada por todos los usuarios es la misma.

Por último, los sistemas de comunicaciones caóticas presentan una serie de ventajas potenciales adicionales con respecto a los sistemas convencionales de espectro ensanchado que justifican el reciente interés por los mismos [Kenne1996, Kenne1998, Lau2003]:

1. La mejora en la seguridad respecto a los sistemas de ensanchado convencionales, debido a la aperiodicidad de las señales caóticas y a su sensibilidad a las condiciones iniciales, que dificulta enormemente su estimación por parte de un usuario no deseado ("eavesdropper") en condiciones de baja relación señal a ruido, tal y como se ha visto en los capítulos 3–6.

2. La capacidad de generación de un gran número de formas de onda diferentes de manera muy sencilla a partir de un único sistema caótico gracias a la sensibilidad a las condiciones iniciales.

3. La posibilidad de integración de las funciones de modulación y ensanchamiento espectral, así como la facilidad de generación de las señales caóticas utilizando circuitos de bajo coste y consumo.

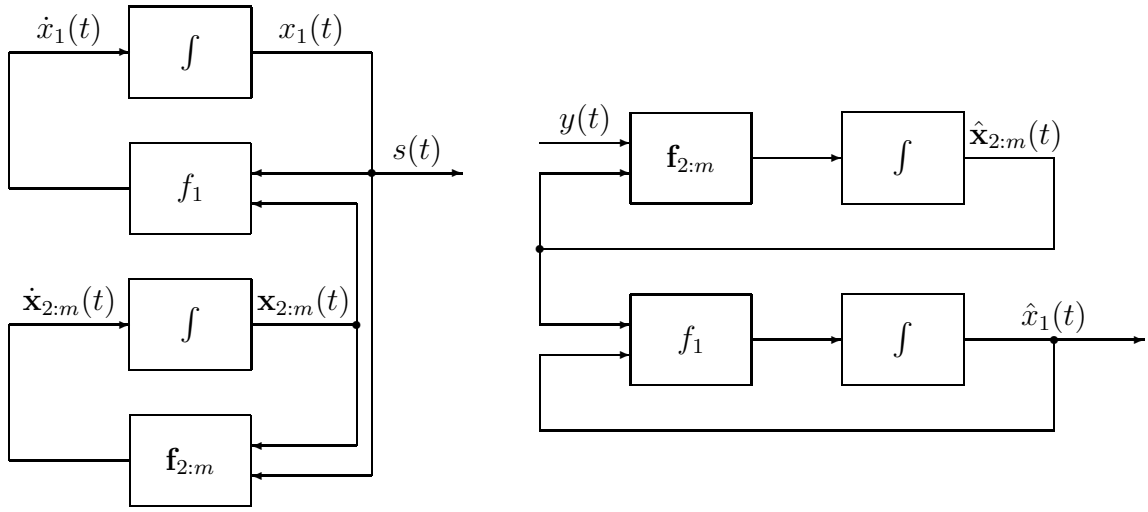
7.2.1.2. Desafíos y Problemas a Resolver

Desafortunadamente, del mismo modo que los sistemas de comunicaciones caóticas presentan una serie de importantes ventajas prácticas, también existen numerosos problemas e inconvenientes que deben analizarse cuidadosamente. Probablemente el reto más importante a la hora de conseguir sistemas de comunicaciones caóticas competitivos y robustos sea la *sincronización*. Al igual que en el caso de los sistemas de comunicaciones convencionales, los receptores óptimos para los distintos sistemas de comunicaciones caóticas (receptores coherentes) requieren una copia exacta de las posibles formas de onda transmitidas (funciones base). Debido a la aperiodicidad de las señales caóticas no es posible disponer de un conjunto de muestras de dichas formas de onda almacenado en el receptor con el que correlar la señal recibida convenientemente muestreada. Asimismo, la extrema sensibilidad característica de los sistemas caóticos desaconseja tratar de regenerar las señales caóticas en el receptor de manera autónoma. En consecuencia, las únicas alternativas viables en un sistema práctico parecen ser utilizar receptores subóptimos (receptores no coherentes) o recurrir a lo que se conoce como *sincronización caótica*.

El hecho (sorprendente a priori) de que dos sistemas caóticos independientes sean capaces de sincronizarse fue descubierto por Pecora y Carroll utilizando los sistemas caóticos de Lorenz y Rössler [Lorenz1963a, Rossle1976] a principios de los años 90 [Pecora1990, Carrol1991]. Este tipo de sincronización, conocida como "master-slave" o "drive-response", se basa en descomponer el sistema original ("drive" o "master") en dos subsistemas, transmitir la salida del primero de ellos, y utilizar dicha variable para reconstruir (estimar) el estado del transmisor en el receptor ("response" o "slave"). Esta división en el transmisor se muestra en la Figura 7.1(a), donde la ecuación de estado del sistema m-dimensional, $\dot{\mathbf{x}}(t) = \mathbf{f}(\mathbf{x}(t))$, se ha fraccionado en otras dos,

$$\begin{aligned} \dot{x}_1(t) &= f_1(x_1(t), \mathbf{x}_{2:m}(t)), \\ \dot{\mathbf{x}}_{2:m}(t) &= \mathbf{f}_{2:m}(x_1(t), \mathbf{x}_{2:m}(t)). \end{aligned}$$

La señal transmitida es $s(t) = x_1(t)$. Al receptor llega la señal $y(t) = x_1(t) * h(t) + w(t)$,



(a) (b)

Figura 7.1: Transmisor y receptor para un sistema de sincronización del tipo "master-slave" o "drive-response". (a) Esquema del transmisor ("drive" o "master"). (b) Esquema del receptor ("response" o "slave").

donde $h(t)$ es la respuesta al impulso combinada del filtro del transmisor, el canal y el filtro del receptor, y $w(t)$ es el ruido del enlace de comunicaciones. Esta señal se usa para alimentar el subsistema 2 en el receptor,

$$\dot{\hat{\mathbf{x}}}_{2:m}(t) = \mathbf{f}_{2:m}(y(t), \hat{\mathbf{x}}_{2:m}(t)),$$

obteniéndose de este modo una estima de $\mathbf{x}_{2:m}(t)$, $\hat{\mathbf{x}}_{2:m}(t)$, que a su vez se usa para intentar reconstruir $x_1(t)$ mediante una réplica del subsistema 1,

$$\dot{\hat{x}}_1(t) = f_1(\hat{x}_1(t), \hat{\mathbf{x}}_{2:m}(t)),$$

tal y como se muestra en la Figura 7.1(b). Esta separación se puede llevar a cabo para cualquier sistema caótico, pero lo que no resulta evidente es que a partir de $y(t)$ sea posible recuperar de forma aproximada el estado del transmisor sin importar cual sea el estado de partida del receptor. Pecora y Carroll demostraron, para los sistemas caóticos de Lorenz y Rössler, que, en ausencia de ruido ($w(t) = 0$) y para un canal ideal ($h(t) = \delta(t)$), el transmisor y el receptor se sincronizan independientemente de cuales sean sus condiciones iniciales [Pecora1990]. Es decir, que

$$\lim_{t\to\infty} \|\hat{\mathbf{x}}(t) - \mathbf{x}(t)\| = 0.$$

Inmediatamente se demostró la generalidad esta clase de sincronización, extendiéndose rápidamente a numerosos sistemas caóticos tanto continuos (sistema de Chua

[Kocar1992], un sistema no autónomo basado en el oscilador de Duffing [Carrol1993], sistemas tetradimensionales [Carrol1998a, Carrol1999]) como discretos (fundamentalmente mapas PWL [Itoh1995, Hasler1997b]). Asimismo han aparecido diversas variantes de la sincronización de Pecora y Carroll, entre las cuales merece la pena destacar la conocida como *sincronización del sistema inverso* [Dedieu1993, Hasler1995]. En este caso no se divide el sistema caótico en dos subsistemas, sino que en el receptor se intenta construir directamente el sistema inverso del transmisor, de tal modo que, independientemente de sus condiciones iniciales, la señal recuperada se sincronice con la señal transmitida.

Otra técnica de sincronización caótica completamente diferente a la de Pecora y Carroll es la que se conoce como *sincronización por realimentación del error* ("error-feedback") o *basada en observadores no lineales* ("observer-based"). Esta clase de sincronización tiene su origen en la teoría de control y en concreto en el campo del *control del caos* [Chen1992, Chen1993c]. La idea básica consiste en generar una señal de error observando el estado del sistema en el receptor, realimentándolo a través de una función adecuada, y restándoselo a la señal recibida [Morgul1996, Nijmei1997, Grassi1997]. Este error se introduce luego en la dinámica del receptor, tratando de corregir su estado con el fin de que se sincronice con el del transmisor. En la Figura 7.2(a) se muestra la forma genérica del transmisor, cuyas ecuaciones de estado son

$$\begin{aligned} \dot{\mathbf{x}}(t) &= \mathbf{f}(\mathbf{x}(t)), \\ s(t) &= h(\mathbf{x}(t)), \end{aligned}$$

mientras que en la Figura 7.2(b) se muestra el receptor, cuyo comportamiento dinámico se rige por

$$\begin{aligned} \varepsilon(t) &= y(t) - h(\hat{\mathbf{x}}(t)) = y(t) - \hat{s}(t), \\ \dot{\hat{\mathbf{x}}}(t) &= \mathbf{f}(\hat{\mathbf{x}}(t)) + \mathbf{g}(\varepsilon(t)). \end{aligned}$$

Una variante de este método introducida muy recientemente consiste en utilizar como entrada al receptor la integral de la señal recibida, $y(t)$, en lugar de la propia señal, consiguiendo de este modo un mejor rendimiento gracias al efecto de filtrado paso bajo propio de la integración [Jiang2006].

Desafortunadamente se ha mostrado mediante simulaciones que la sincronización de Pecora y Carroll es poco robusta frente a los efectos del ruido en el canal, requiriendo al menos 30 dB de SNR para su correcto funcionamiento. Otro tanto ocurre con los sistemas inversos, que son extremadamente sensibles a los efectos del ruido, necesitándose una SNR superior a 40 dB para mantener la sincronización [Kolum1996, Kenne1997]. Por el contrario, la sincronización basada en observadores no lineales puede operar en condiciones de SNR sensiblemente inferiores a las otras dos técnicas (SNR $<$ 20 dB), de modo que es la técnica más estudiada en la actualidad. No obstante, aún está por ver si es suficientemente resistente frente a otros efectos nocivos presentes en canales reales tales como limitaciones severas del ancho de banda (filtrado) o distorsión multicamino.

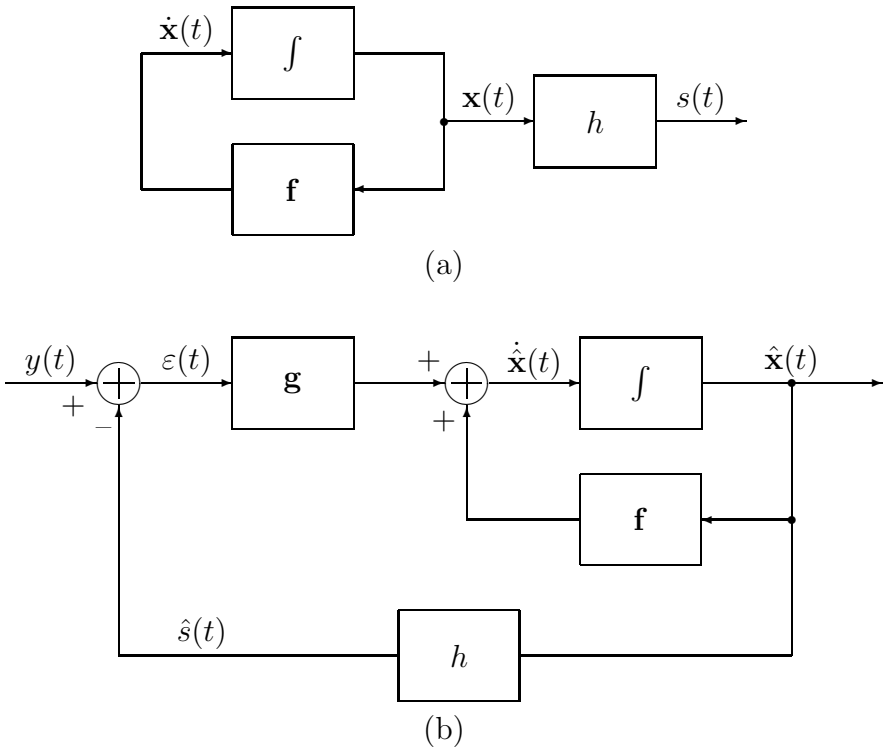


Figura 7.2: Transmisor y receptor para un sistema de sincronización del tipo "error-feedback" u "observer-based". (a) Esquema del transmisor. (b) Esquema del receptor.

Por último, aunque el desarrollo de mecanismos de sincronización robustos sea el principal desafío para la implementación de sistemas de comunicaciones competitivos, a continuación se enumeran otra serie de problemas que se deben solucionar [Lau2003]:

1. La necesidad de conocer/estimar el ancho de banda de las señales caóticas transmitidas, para lo cual no existen herramientas formales y debe recurrirse a simulaciones en la mayor parte de los casos.

2. El planteamiento de esquemas de comunicación que admitan detectores no coherentes y el desarrollo de los mismos para permitir la transmisión en condiciones de baja SNR en las que las técnicas de sincronización no sean aplicables.

3. La investigación del rendimiento de los diferentes esquemas propuestos hasta la fecha en condiciones más realistas de canal (esto es, canales con desvanecimiento selectivo en frecuencia por ejemplo, y no sólo con AWGN), para las que aún no existen suficientes estudios.

4. La dificultad a la hora de encontrar la señal caótica más adecuada (es decir, el sistema caótico y sus parámetros), ya que cada señal caótica es diferente y su elección puede afectar a la BER obtenida.

7.2.2. Revisión de Esquemas de Comunicaciones Caóticas

7.2.2.1. Enmascaramiento Caótico

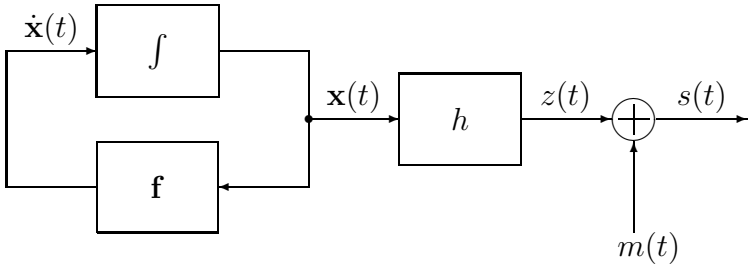
Una de las primeras técnicas de comunicación usando señales caóticas propuesta fue la del enmascaramiento caótico ("chaotic masking", CM) [Oppen1992, Kocar1992]. Los sistemas de CM se basan en utilizar la señal caótica, de banda ancha y aspecto similar al ruido, para enmascarar la señal de información real que se desea transmitir, que puede ser analógica o digital (modulada usando algún código de línea por ejemplo).

La forma más sencilla de construir un sistema de CM consiste en sumar la señal de información a la señal caótica generada mediante un sistema caótico autónomo como el de Lorenz [Oppen1992, Cuomo1993a, Cuomo1993b] o el de Chua [Kocar1992], tal y como se muestra en la Figura 7.3(a). La señal transmitida en este caso es

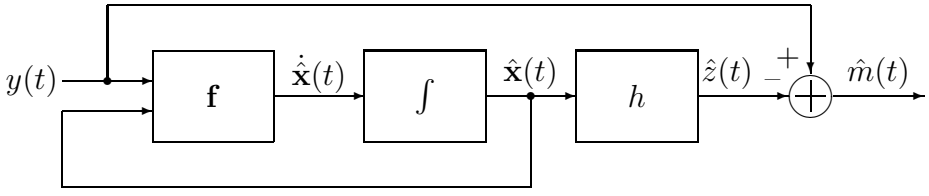
$$s(t) = z(t) + m(t) = h(\mathbf{x}(t)) + m(t),$$

siendo $m(t)$ la señal de información que se desea transmitir (mensaje) y $\dot{\mathbf{x}}(t) = \mathbf{f}(\mathbf{x}(t))$ la ecuación de estado del sistema caótico. En el receptor, mostrado en la Figura 7.3(b), se dispone de un sistema caótico que se sincroniza con el del transmisor, lo que permite sustraer la señal caótica y recuperar la señal de información de manera aproximada,

$$\hat{m}(t) = y(t) - \hat{z}(t) = y(t) - h(\hat{\mathbf{x}}(t)) = m(t) + \tilde{w}(t).$$



(a)



(b)

Figura 7.3: Transmisor y receptor para un sistema de enmascaramiento caótico (CM). (a) Esquema del transmisor. (b) Esquema del receptor.

Una alternativa de CM más sofisticada se basa en incorporar la señal de información a la dinámica del sistema caótico, de modo que su salida dependa de la información

a transmitir. En el receptor se construye el sistema inverso del original sin modificar, detectándose los cambios en la salida, y en consecuencia la señal de información transmitida. Este esquema, también conocido como aproximación basada en el *sistema inverso* ("inverse system approach"), se ha implementado usando tanto sistemas continuos como el de Chua [Halle1993], como mapas PWL discretos [Itoh1993, Itoh1995].

El principal problema de esta clase de técnicas es su falta de robustez frente a los efectos del ruido y la distorsión del canal. Por ejemplo, en la primera aproximación la señal de información debe tener una amplitud mucho menor que la señal caótica para no impedir su sincronización en el receptor, lo que provoca que la señal de información sea muy sensible al ruido en el canal. Respecto al segundo esquema, los sistemas inversos muestran una gran sensibilidad tanto frente al ruido como frente a desajustes en los parámetros del sistema ("parameter mismatch") en general, lo que dificulta enormemente su implementación práctica.

En consecuencia, su nicho de aplicación parece encontrarse en entornos en los que se disponga de un canal relativamente exento de ruido y distorsión, como en las comunicaciones ópticas. En este sentido, la utilización de señales caóticas para la transmisión de información a través de redes de fibra óptica, usando técnicas de enmascaramiento y conmutación caótica fundamentalmente, se comenzó a considerar mediante simulaciones a mediados de los años 90 [Colet1994, Celka1995b, Miras1996]. Posteriormente se llevaron a cabo diversas transmisiones experimentales en condiciones de laboratorio, destacando las pruebas realizadas dentro del proyecto OCCULT ("Optical Chaotic Communications Using Laser Transmitters") en las que se llevaron a cabo comunicaciones caóticas a distancias de aproximadamente 100 km. y velocidades cercanas a 1 Gbps con probabilidad de error inferior a 10^{-7} [Occult]. Por último, recientemente se ha conseguido completar una transmisión usando señales caóticas a través de una red comercial de fibra óptica situada bajo la ciudad de Atenas con prestaciones similares a las de los experimentos de laboratorio [Argyri2005, Syvri2006].

7.2.2.2. Conmutación Caótica y CSK

Otra técnica de comunicaciones caóticas desarrollada en paralelo al enmascaramiento caótico es la conmutación caótica ("Chaotic Switching", CS), también denominada en ocasiones modulación caótica ("Chaotic Modulation") [Oppen1992, Parlit1992]. La idea fundamental de los sistemas de CS consiste en utilizar directamente la señal de información para modificar la señal caótica transmitida. En el caso de los sistemas de CS digitales, conocidos también como sistemas CSK ("Chaos Shift Keying") [Dedieu1993], existen tres formas de transmitir K símbolos diferentes [Hasler1995]:

1. Utilizando K sistemas caóticos independientes distintos y conmutando entre sus salidas en función del símbolo a transmitir [Oppen1992, Dedieu1993].

2. Utilizando un único sistema caótico con K conjuntos de parámetros diferentes entre los que se conmuta según el símbolo que se desee enviar [Parlit1992, Heida1992a, Cuomo1993a].

3. Escalando las señales de salida de P sistemas caóticos (habitualmente $P = 1$ o $P = 2$), que actúan como funciones base, de acuerdo con un conjunto K amplitudes distintas [Kolum1998b, Kolum2000a].

El esquema básico del transmisor para las tres alternativas se muestra en la Figura 7.4 para el caso binario ($K = 2$): en el primer esquema la secuencia de bits de información se usa para seleccionar la salida de uno de los dos sistemas caóticos, en el segundo para seleccionar uno de los dos vectores de parámetros, y en el tercero para seleccionar uno de los dos posibles factores de amplificación. En el caso de los sistemas de CS analógicos, mucho menos estudiados, la única opción posible consiste en modular algún parámetro o conjunto de parámetros del sistema caótico en función de la señal de información a transmitir [Heida1992a, Elmir1994a].

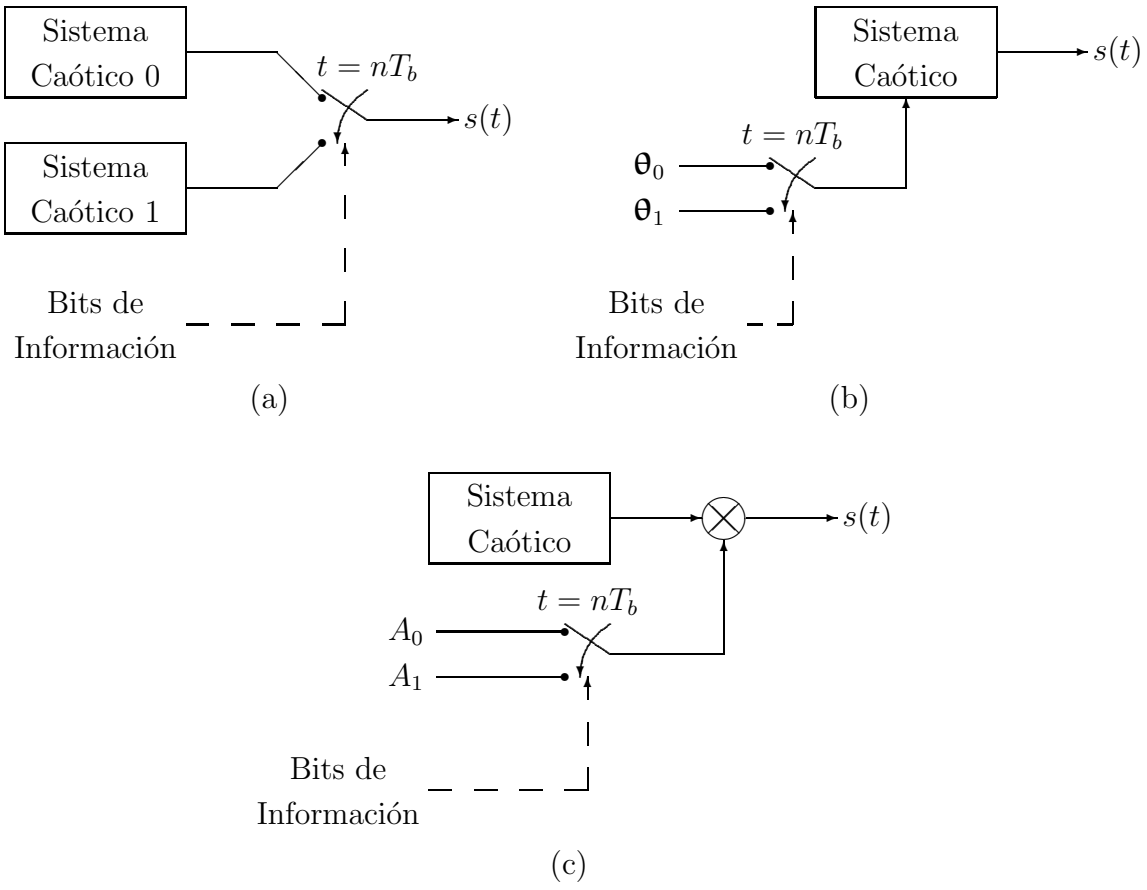


Figura 7.4: Diagrama de bloques del transmisor para diversos sistemas de conmutación caótica binarios. (a) Esquema que conmuta entre la salida de dos mapas caóticos distintos. (b) Esquema con un único mapa caótico que conmuta entre dos posibles vectores de parámetros. (c) Esquema con un único mapa caótico que utiliza amplitudes diferentes para cada símbolo.

En el receptor se trata de estimar la señal de información con la que se corresponde la forma de onda recibida haciendo uso del sistema inverso. Para un sistema de CS analógico esto equivale a estimar los parámetros del sistema caótico original a partir de la señal ruidosa recibida. Para un sistema de CS digital binario el receptor óptimo se basa en la sincronización con el sistema caótico del transmisor, existiendo de nuevo dos posibilidades:

1. Disponer de dos sistemas caóticos, cada uno ajustado a uno de los dos posibles sistemas del transmisor, decidiéndose como símbolo transmitido aquel que mejor se ajuste a las observaciones.

2. Disponer de un único sistema en el receptor y decidir el símbolo transmitido en función de si se sincroniza o no con la señal recibida.

No obstante, debido a la falta de robustez frente a la distorsión de las técnicas actuales de sincronización, alternativamente los sistemas de CS utilizan con frecuencia receptores no coherentes basados generalmente en la energía de la señal recibida.

Dentro de los múltiples esquemas de CSK propuestos, los más interesantes son aquellos que consideran un conjunto de funciones base caóticas ortonormales cuyas amplitudes vienen determinadas por el símbolo a transmitir. Esta formulación fue desarrollada por Kolumbán et al. [Kolum2000a, Kolum2002], y permite enmarcar los sistemas CSK dentro del contexto usual de espacio de señal y funciones base manejado en comunicaciones digitales. Utilizando este marco teórico se han propuesto numerosos esquemas CSK, siendo los principales los que se enumeran a continuación:

1. **COOK ("Chaotic On/Off Keying"):** Esquema de CS más sencillo posible, aunque no fue el primero propuesto, con funcionamiento idéntico al de un sistema OOK convencional: la presencia de señal transmitida (caótica en este caso) indica el envío de un uno, y su ausencia un cero [Kolum1997a].

2. **CSK ("Chaos Shift Keying"):** Consiste en enviar dos señales caóticas distintas para representar el cero y el uno. Se pueden distinguir dos versiones de CSK, unipodal y antipodal, en función de si la salida del detector óptimo en ausencia de ruido puede tomar sólo valores positivos o también negativos. En el primer caso, *CSK unipodal*, puede plantearse un detector coherente basado en la energía de la señal caótica recibida, típicamente distinta para el cero y el uno. En el segundo caso, *CSK antipodal*, esto no es posible, ya que habitualmente las formas de onda asociadas al cero y al uno sólo se diferencian en el signo [Kolum2000a, Kolum2002]. Nótese que COOK puede verse como un caso particular de CSK unipodal. De hecho se trata del esquema unipodal óptimo, ya que presenta la máxima separación posible entre los símbolos de la constelación para una energía media por bit dada.

3. **DCSK ("Differential" CSK):** Propuesta en 1996 por Kolumbán et al. con el propósito de facilitar la realización de un detector no coherente. La idea consiste

en transmitir una señal de referencia, $s(t)$, durante $T_b/2$, seguida de la misma señal entre $T_b/2$ y T_b modulada como en CSK antipodal [Kolum1996]: $s(t)$ para transmitir un uno, y $-s(t)$ para un cero. En el receptor se puede realizar una detección no coherente de un modo similar a DBPSK: correlando la señal de información, $\pm s(t)$, con la señal de referencia, $s(t-T_b/2)$, e integrando entre $T_b/2$ y T_b. DCSK es un esquema más robusto frente a ruido e interferencias que COOK y CSK, y evita la dependencia del umbral de detección óptimo con la varianza del ruido que aparece en COOK y CSK unipodal [Kolum2000a, Kolum2002]. Su principal problema es que se trata de un *esquema de referencia transmitida*: puesto que la señal caótica varía bit a bit y las técnicas de sincronización caótica no son suficientemente robustas, es necesario transmitir la señal de referencia de cada bit para poder correlar en el receptor. Esto supone que únicamente se envía información durante la mitad del periodo de bit, reduciéndose la tasa binaria.

4. **FM-DCSK ("Frequency Modulated" CSK):** Consiste en aplicar la señal caótica a un modulador de FM, y a continuación modular su salida utilizando el mismo esquema que DCSK [Kolum1997c, Kolum1998a]. De este modo se consigue que la energía media por bit permanezca constante (en los esquemas anteriores la energía de la señal caótica podía variar mucho de un bit a otro) y se puede usar exactamente el mismo detector que en DCSK.

5. **CDSK ("Correlation Delay Shift Keying"):** Se trata de una variante de DCSK en la que, en lugar de conmutar entre la señal de referencia, $s(t)$, y la de información, $m(t)$, se transmite la suma de ambas [Sushch2000b, Sushch2000c]. Al igual que en DCSK, la señal de información se genera retardando $s(t)$ y cambiándola el signo o no en función del bit a transmitir, $m(t) = \pm s(t - T_d)$. La diferencia con DCSK es que T_d puede tomar cualquier valor, no necesariamente $T_b/2$. Las ventajas de CDSK con respecto a DCSK son que, al eliminar la conmutación presente en DCSK, CDSK permite que el transmisor y el receptor funcionen en modo continuo, y además aumenta la seguridad, ya que la señal caótica transmitida nunca se repite. El principal problema de CDSK es que, debido a la correlación no nula entre distintos segmentos de la señal caótica, su probabilidad de error empeora con respecto a DCSK y FM-DCSK. No obstante, recientemente ha aparecido una generalización de CDSK, GCDSK, en la que la salida se construye sumando varias versiones de $s(t)$ con distintos retardos [Tam2006], que permite llevar a cabo una modulación multinivel, y puede conseguir una mejor BER que CDSK e incluso DCSK.

6. **SCSK ("Symmetric" CSK):** Se trata de una alternativa sencilla a DCSK y CDSK. La idea consiste en transmitir la primera componente de un sistema caótico d-dimensional modulada por la señal de información como en CSK antipodal [Sushch2000b, Sushch2000c]. En el receptor se usa un sistema inverso para reconstruir el estado del transmisor y correlar su primera componente con la señal recibida. Las ventajas de SCSK son su simplicidad, su mayor seguridad con res-

pecto a DCSK, y su BER (mucho mejor que la de CDSK, aunque peor que la de DCSK). Su principal problema es la limitación en la elección del sistema caótico.

7. **ECSK ("Ergodic" CSK):** Variante de CSK propuesta por Hasler en la que, para un mapa caótico dado, se modifican el transmisor y el receptor haciendo uso de las propiedades ergódicas de los sistemas caóticos con el fin de conseguir una menor tasa de errores para factores de ensanche altos [Hasler2001]. Su gran ventaja con respecto al resto de esquemas de CSK reside en que su rendimiento siempre mejora al aumentar el factor de ensanche, N, mientras que para el resto existe un valor de N (que depende de la E_b/N_0) a partir del cual la BER apenas mejora e incluso empeora [Abel2002].

8. **QDCSK ("Quadrature" DCSK):** Versión multinivel de DCSK propuesta por Galias y Maggio [Galias2001a, Galias2001b]. Guarda la misma relación con DCSK que QPSK con BPSK. Aunque previamente se habían propuesto otras versiones multinivel de DCSK basadas en escalar la parte de información (y posiblemente también la de referencia) o en usar dos señales caóticas distintas como funciones base aproximadamente ortogonales [Kolum1997a, Kenne1998], su rendimiento empeora con respecto al de DCSK. QDCSK consigue la misma tasa de errores que DCSK utilizando una señal caótica cualquiera como función base para la parte en fase, y construyendo una segunda función base para la parte en cuadratura estrictamente ortogonal con la primera mediante la transformada de Hilbert [Oppen1989]. En el receptor se usa la señal ruidosa para reconstruir las funciones base e implementar dos correladores a partir de cuyas salidas se decide el símbolo transmitido. Nótese que, utilizando las amplitudes apropiadas para las partes en fase y cuadratura, es posible conseguir cualquier constelación deseada, por lo que este esquema permite implementar el equivalente caótico de la modulación QAM.

7.2.2.3. Codificación Simbólica

Una tercera posibilidad para modular información digital utilizando señales caóticas son el conjunto de técnicas que se van a agrupar bajo el nombre de *codificación simbólica* o *caótica* (CC). La idea fundamental de todas estas técnicas consiste en explotar la secuencia simbólica asociada a la trayectoria de una señal caótica para codificar la señal digital que se desea transmitir.

Hayes, Grebogi y Ott fueron los primeros en proponer de manera teórica un esquema de comunicaciones basado en la codificación simbólica [Hayes1993], demostrando posteriormente su funcionamiento experimental usando los circuitos de Chua [Hayes1994] y de Lorenz [Hayes1996]. La idea fundamental consiste en construir una secuencia simbólica a partir de la señal generada por un sistema caótico continuo asociando distintas regiones de su atractor al cero y al uno, y a continuación aplicar técnicas de

control del caos para generar una señal de salida cuya secuencia simbólica coincida con los bits de información a transmitir. Esta misma idea fue estudiada con mayor profundidad y generalizada posteriormente por Schweizer y Kennedy bajo el nombre de *control predictivo de Poincaré* ("Predictive Poincaré Control", PPC) [Schwei1995].

Recientemente se han propuesto otros dos esquemas de comunicaciones alternativos que aprovechan la dinámica simbólica para transmitir información digital, aunque usando sistemas discretos en esta ocasión. En primer lugar, Ciftci y Williams han propuesto un esquema que se basa en construir una secuencia simbólica, $\mathbf{s}$, directamente a partir de los bits de información, encontrar la relación entre el itinerario y las muestras de la secuencia caótica, $x[n] = \sigma(\mathbf{s})$ con $0 \leq n \leq N$, y usarla para generar la señal transmitida, $\mathbf{x}$ [Ciftci2001a, Ciftci2001b]. En el receptor se utiliza el algoritmo de Viterbi para recuperar la información transmitida a partir de las observaciones ruidosas. Este esquema permite usar diversos mapas caóticos (básicamente cualquier mapa para el que se pueda encontrar $\sigma(\mathbf{s})$) y presenta un buen rendimiento, aunque requiere un truncamiento de la secuencia simbólica, incrementándose su coste computacional exponencialmente con la precisión utilizada.

Por otro lado, Maggio et al. propusieron un esquema basado en aproximar la dinámica simbólica del BSM usando un registro de desplazamiento con K posiciones [Maggio2001a, Maggio2001b]: cada nuevo bit de información es introducido en el bit menos significativo (LSB) del registro, desplazándose el resto a la izquierda y descartándose el bit más significativo (MSB). A continuación se emplea el valor analógico correspondiente al contenido del registro como condición inicial para generar, usando el BSM, $N + 1 \leq K$ muestras de una señal caótica cuyo itinerario contiene la información a transmitir. Este esquema permite la aplicación de una transformación invertible para generar la señal caótica de acuerdo con la dinámica de otros mapas caóticos (por ejemplo el TM con $\beta = 2$), así como su combinación con un esquema de modulación por la posición de los pulsos (PPM) para conseguir una codificación PPM caótica (CPPM). Además, el detector puede implementarse mediante el VA con una complejidad reducida.

7.2.2.4. Secuencias de Ensanche Caóticas

Las tres alternativas de comunicaciones caóticas descritas anteriormente se basan en sustituir las formas de onda usadas tradicionalmente (pulsos para transmisión en banda base o una combinación de sinusoides para transmisión paso banda) por señales caóticas. En esta sección se considera una idea completamente distinta: utilizar secuencias generadas por mapas caóticos como secuencias de ensanche para un sistema de SS convencional en lugar de las habituales secuencias PN.

Esta idea fue propuesta inicialmente por Heidari-Bateni y McGillem [Heida1992b, Heida1994], que desarrollaron un sistema de espectro ensanchado por secuencia directa (DS-SS) caótico en el que la secuencia PN de ensanche (binaria) era simplemente reemplazada por una secuencia caótica (analógica) generada utilizando un sencillo sistema caótico discreto unidimensional: el mapa logístico. Este primer esquema no

consideraba ningún tipo de acceso multiusuario. Los primeros en plantear un sistema de acceso múltiple por división en el código (CDMA) caótico fueron Parlitz y Ergezinger, usando de nuevo secuencias de ensanche analógicas generadas iterando el mapa logístico con diferentes condiciones iniciales para los distintos usuarios [Parlit1994]. Desde entonces, numerosos autores han estudiado esta clase de esquemas con mayor profundidad, utilizando tanto mapas caóticos discretos como sistemas continuos [Lipton1996, Yang1997, Itoh1999].

Estos primeros esquemas, basados en el uso de señales caóticas analógicas, no son suficientemente robustos frente a la distorsión introducida por canales reales. Para tratar de paliar este problema, Mazzini et al. propusieron utilizar como códigos de ensanche señales discretas obtenidas cuantificando y repitiendo una porción de una secuencia caótica generada iterando un mapa discreto [Mazzi1997, Rovat1998a]. Seleccionando cuidadosamente el mapa caótico, el mecanismo de cuantificación y el conjunto de secuencias generadas, esta clase de sistemas presentan ventajas con respecto a los sistemas CDMA convencionales desde el punto de vista de la capacidad e interferencia cocanal [Rovat1998b, Rovat1998c, Mazzi1999].

Para finalizar, nótese que todos los esquemas mencionados anteriormente son sistemas DS-SS. No obstante, de manera más reciente también se han comenzado a considerar esquemas caóticos con ensanche por salto en frecuencia (FH-SS) [Cong1998, Cong2001] y especialmente por salto en el tiempo (TH-SS), dado el creciente interés existente por los sistemas de banda ultra-ancha (sistemas UWB) [Sushch2000a, Laney2002, Dmitri2003, Leung2006].

7.3. Comunicaciones Digitales de Espectro Ensanchado Caóticas

En esta sección se estudia el rendimiento de dos esquemas de comunicaciones digitales de espectro ensanchado distintos que utilizan secuencias caóticas. El primero de ellos, más sencillo, se basa en la conmutación del parámetro de bifurcación de un mapa caótico unidimensional (sistema CS), y se describe en la Sección 7.3.1. El segundo de ellos, novedoso y más sofisticado, se basa en transmitir la información usando la secuencia simbólica asociada a una señal caótica generada iterando hacia atrás un mapa caótico unidimensional (sistema CC), y se describe en la Sección 7.3.2.

En ambos casos se considera un canal Gaussiano (AWGC), que únicamente introduce AWGN como distorsión sobre la señal transmitida, aplicándose los estimadores subóptimos apropiados desarrollados en los capítulos anteriores para recuperar la información transmitida. Además, en la Sección 7.3.2.4 se estudia la combinación del sistema CC con OFDM para conseguir un cierto grado de inmunidad frente a la distorsión multicamino introducida por canales reales. En todos los casos la medida de calidad utilizada es la tasa de errores (BER), obtenida mediante simulaciones de Monte Carlo.

7.3.1. Sistema Basado en la Conmutación del Parámetro de Bifurcación de un Mapa Caótico Unidimensional

7.3.1.1. Esquema del Transmisor

En esta sección se consideran dos diagramas de bloques distintos para un transmisor CS que permiten representar las tres alternativas existentes para realizar un sistema CSK. El primer esquema considerado es esencialmente el siguiente. Se dispone de $K = 2^k$ mapas caóticos unidimensionales funcionando en paralelo de manera independiente. En primer lugar, la secuencia de bits de información que se desean transmitir se agrupa en bloques de K bits (símbolos), que se usan a continuación para seleccionar la secuencia de $N + 1$ muestras correspondientes a la salida de uno de los K mapas caóticos. Esta señal caótica discreta se convierte en analógica utilizando un conversor digital/analógico (DAC) con periodo/frecuencia de muestreo dados por

$$T_s = \frac{T_b \log_2 K}{N+1} \quad \Rightarrow \quad f_s = \frac{(N+1)R_b}{\log_2 K}, \tag{7.1}$$

siendo R_b la tasa binaria a la que se desea transmitir y T_b la duración de un bit (periodo binario), $T_b = 1/R_b$. Por último, en el caso de sistemas de transmisión paso banda la señal caótica analógica paso bajo se debería aplicar a un mezclador de RF con frecuencia central f_c que traslada la señal caótica a la banda frecuencial deseada. El diagrama de bloques del transmisor se muestra en la Figura 7.5, donde el bloque $\uparrow N{+}1$ representa la interpolación por un factor $N{+}1$ con un interpolador de orden cero ("zero-order hold") [Oppen1989] necesaria para adecuar la tasa binaria a la velocidad de funcionamiento de los mapas caóticos, $N + 1$ veces superior.

Las ecuaciones del transmisor son las siguientes. En primer lugar, la evolución de las secuencias generadas por los dos mapas caóticos viene descrita por

$$\begin{aligned} x_0[n] &= f_0(x_0[n-1]; \boldsymbol{\theta}_0), \\ x_1[n] &= f_1(x_1[n-1]; \boldsymbol{\theta}_1), \end{aligned}$$

donde $\boldsymbol{\theta}_0$ y $\boldsymbol{\theta}_1$ denotan los vectores de parámetros de bifurcación de los dos mapas caóticos, y se ha usado f_0 y f_1 para indicar que se puede tratar de dos mapas caóticos diferentes. La secuencia de bits de información interpolada es

$$b_i[n] = b[\lfloor n/(N+1) \rfloor] = \sum_{m=0}^{N_b-1} \sum_{k=0}^{N} b[m]\delta[n - m(N+1) - k], \tag{7.2}$$

donde $\lfloor \cdot \rfloor$ denota la parte entera aproximada por abajo, y N_b es el número de bits a transmitir. Las dos secuencias caóticas moduladas por $b_i[n]$ son

$$\begin{aligned} \tilde{x}_0[n] &= x_0[n](1 - b_i[n]), \\ \tilde{x}_1[n] &= x_1[n]b_i[n], \end{aligned}$$

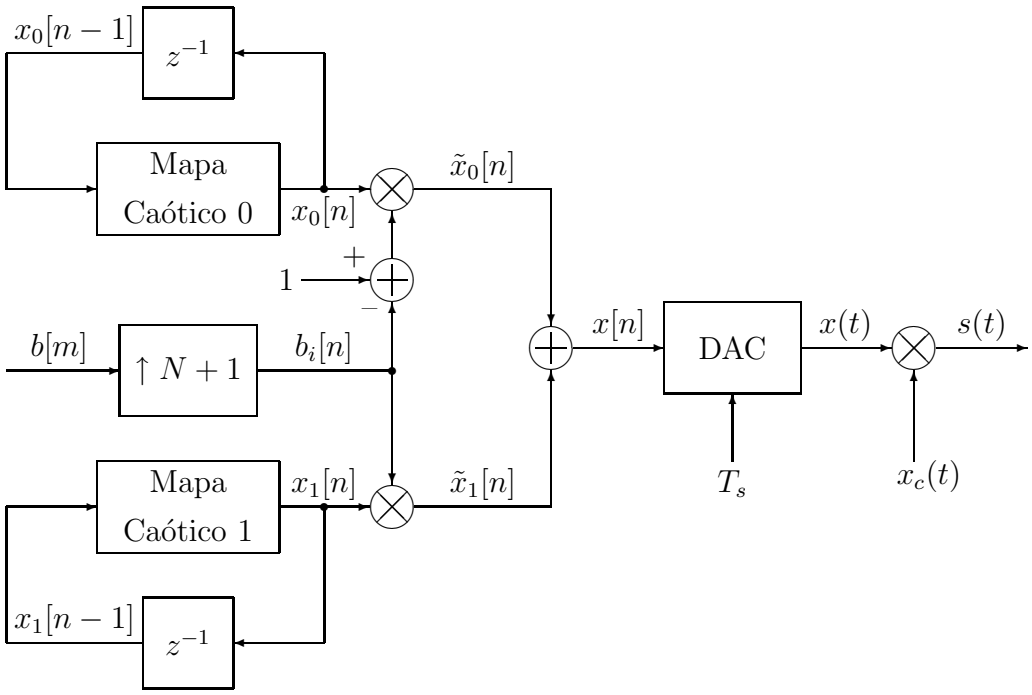


Figura 7.5: Diagrama de bloques del transmisor para un sistema de conmutación caótica binario basado en dos mapas unidimensionales.

y la secuencia caótica discreta resultante es finalmente

$$x[n] = \tilde{x}_0[n] + \tilde{x}_1[n] = \begin{cases} x_0[n], & b_i[n] = 0; \\ x_1[n], & b_i[n] = 1. \end{cases} \tag{7.3}$$

Nótese que, juntando (7.2) y (7.3), $x[n]$ se puede expresar como

$$\begin{aligned} x[n] &= \sum_{m=0}^{N_b-1} \sum_{k=0}^{N} x_{b[m]}[m(N+1)+k]\delta[n-m(N+1)-k] \\ &= \sum_{m=0}^{N_b-1} \sum_{k=0}^{N} f_{b[m]}(x_{b[m]}[m(N+1)+k-1])\delta[n-m(N+1)-k], \end{aligned} \tag{7.4}$$

para $1 \leq n \leq N_b(N+1)-1$, y siendo $x[0] = x_{b[0]}[0]$ la condición inicial del mapa correspondiente a $b[0]$. Las simulaciones se van a llevar a cabo utilizando el equivalente discreto paso bajo del sistema sin tener en cuenta los efectos del DAC ni del mezclador, que se suponen ideales tal y como es habitual a la hora de simular sistemas de comunicaciones digitales, de modo que no es necesario considerar $x(t)$ y $s(t)$.

El esquema de la Figura 7.5 utiliza dos señales caóticas discretas diferentes, obtenidas bien a partir de dos mapas distintos, bien a partir del mismo mapa con dos vectores de parámetros diferentes. Alternativamente, se puede construir un sistema CSK binario

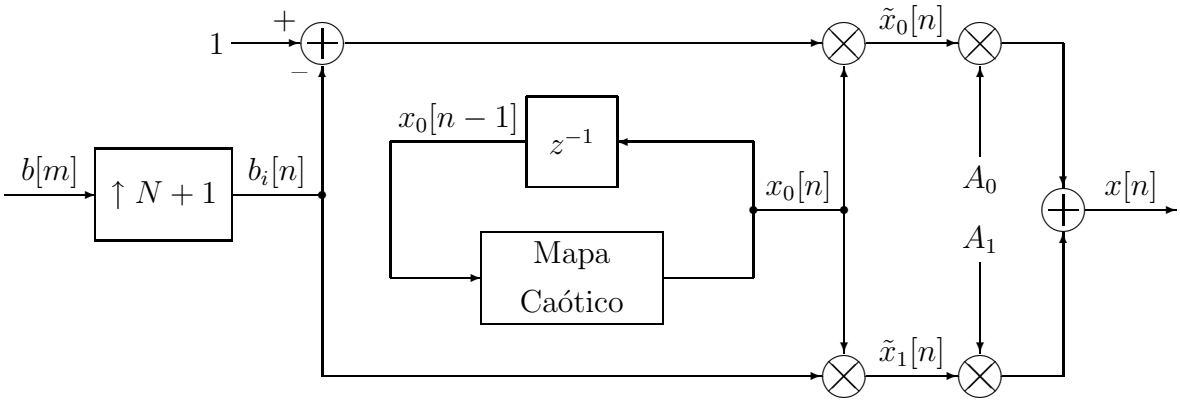


Figura 7.6: Diagrama de bloques del transmisor para un sistema de conmutación caótica binario basado en un único mapa unidimensional.

mediante un único mapa caótico diferenciando las amplitudes correspondientes al cero y al uno, como se muestra en la Figura 7.6.

Nótese que en la Figura 7.6 se ha omitido la parte analógica del transmisor (DAC y mezclador de RF), ya que las simulaciones se realizan usando de nuevo el equivalente discreto paso bajo, y además es idéntica a la de la Figura 7.5. La señal caótica discreta en banda base a la salida de este sistema presenta una expresión similar a (7.4),

$$\begin{aligned} x[n] &= \sum_{m=0}^{N_b-1}\sum_{k=0}^{N} A_{b[m]}x_0[m(N+1)+k]\delta[n-m(N+1)-k] \\ &= \sum_{m=0}^{N_b-1}\sum_{k=0}^{N} A_{b[m]}f(x_0[m(N+1)+k-1])\delta[n-m(N+1)-k], \end{aligned} \tag{7.5}$$

para $1 \leq n \leq N_b(N+1)-1$, con $x[0] = A_{b[0]}x_0[0]$. La principal diferencia entre (7.4) y (7.5) es que ahora $b[m]$ no se usa para conmutar entre dos señales caóticas, sino entre dos factores de escala posibles para la única señal caótica disponible. Seleccionando de manera adecuada los valores de A_0 y A_1, pueden implementarse diversos esquemas de CSK, como COOK ($A_0 = 0$ y $A_1 = 1$) y CSK antipodal ($A_0 = -1$ y $A_1 = 1$).

7.3.1.2. Esquema del Receptor

El diagrama de bloques genérico del canal y el receptor se muestra en la Figura 7.7. Para este esquema de comunicaciones únicamente se considera un canal Gaussiano, $h(t) = \delta(t)$ y $w(t) \sim \mathcal{N}(0, \sigma^2)$ con función de autocorrelación $R_{ww}(\tau) = \sigma^2\delta(t)$, que puede verse como una aproximación de un canal de comunicaciones real cuya respuesta al impulso tiene una duración mucho menor que T_s (esto es, cuyo ancho de banda es mucho mayor que f_s).

En el receptor en primer lugar se deshacen las últimas operaciones realizadas en el transmisor: se mezcla la señal de RF recibida, se le aplica un filtro paso bajo (LPF)

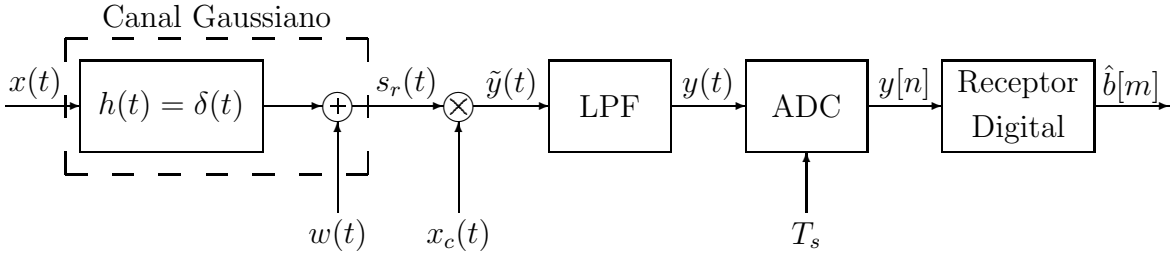


Figura 7.7: Diagrama de bloques del canal y del receptor para un sistema de conmutación caótica cualquiera.

para recuperar la señal en banda base con ruido, $y(t) \approx x(t) + w_{lp}(t)$, y se digitaliza usando de nuevo un periodo de muestreo T_s. La secuencia discreta resultante, $y[n] \approx x[n] + w[n]$ con $w[n] \sim \mathcal{N}(0, \sigma^2)$ y $R_{ww}[m] = \sigma^2\delta[m]$, es la que se va a utilizar para estimar la secuencia de bits transmitidos en el bloque denominado "receptor digital". Para un canal arbitrario este detector digital óptimo constaría de un filtro adaptado a la forma de onda de la secuencia transmitida, seguido por una búsqueda de la secuencia binaria más verosímil de las 2^{N_b} posibles secuencias transmitidas (MLSE), que se puede implementar de manera eficiente mediante el algoritmo de Viterbi. Desafortunadamente este esquema es irrealizable en la práctica, ya que para un sistema de comunicaciones caóticas la señal transmitida es siempre diferente. Esto excluye la posibilidad de disponer de un filtro adaptado almacenado en el receptor, y, debido a la sensibilidad característica de las señales caóticas, las técnicas de regeneración de la señal transmitida en el receptor no son suficientemente robustas, como se ha discutido en la Sección 7.2.1.2.

Por lo tanto se debe recurrir a esquemas de detección subóptimos. A la hora de plantear dichos detectores, nótese que para el canal Gaussiano puede suponerse que las observaciones correspondientes a cada bit son independientes. Esto no es estrictamente cierto debido al mecanismo determinista usado para generar las señales caóticas, pero se trata de una aproximación razonable, puesto que la función de autocorrelación de una señal caótica presenta típicamente una caída exponencial [Sakai1980, Beck1993]. En consecuencia, como receptor práctico se va a considerar el detector óptimo bit a bit: el GLRT con sólo dos hipótesis para cada caso ($2N_b$ hipótesis totales frente a las 2^{N_b} del MLSE), estimando la señal caótica transmitida a partir de las observaciones ya que no se dispone del filtro adaptado.

Considerando el esquema del transmisor de la Figura 7.4 y despreciando los efectos de la parte analógica (DAC, mezcladores, LPF y ADC) para el canal Gaussiano resulta evidente que la FDP de las observaciones condicionadas por cada una de las dos posibles secuencias transmitidas para el bit m-ésimo es una Gaussiana $(N+1)$-dimensional,

$$p(\mathbf{y}_m; \mathbf{x}_i^m) = (2\pi\sigma^2)^{-(N+1)/2} \exp(-J(\mathbf{y}_m; \mathbf{x}_i^m)/2\sigma^2), \tag{7.6}$$

siendo

$$\begin{aligned} J(\mathbf{y}_m;\mathbf{x}_i^m) &= (\mathbf{y}_m-\mathbf{x}_i^m)^T(\mathbf{y}_m-\mathbf{x}_i^m) \\ &= \sum_{k=0}^{N}(y[m(N+1)+k]-x_i[m(N+1)+k])^2 \\ &= \sum_{k=0}^{N}(y[m(N+1)+k]-f_i^{k-n}(x_i[m(N+1)+n];\boldsymbol{\theta}_i))^2 \\ &= J(\mathbf{y}_m;x_i[m(N+1)+n],\mathbf{s}_i,\boldsymbol{\theta}_i), \end{aligned} \tag{7.7}$$

la función de coste habitual,

$$\begin{aligned} \mathbf{y}_m &= [y[m(N+1)],\ y[m(N+1)+1],\ \ldots,\ y[m(N+1)+N]]^T, \\ \mathbf{x}_i^m &= [x_i[m(N+1)],\ x_i[m(N+1)+1],\ \ldots,\ x_i[m(N+1)+N]]^T, \end{aligned}$$

e $i\in\{1,2\}$. En consecuencia, la estima ML del bit m-ésimo se puede encontrar a partir de (7.7) mediante un cociente de verosimilitud. En un caso práctico $\mathbf{x}_i$ es desconocida, de modo que dicho cociente se plantea a partir de la estima de la secuencia obtenida en el receptor:

$$\hat{b}[m]=\begin{cases}0, & J(\mathbf{y}_m;\hat{x}_0[m(N+1)+n],\hat{\mathbf{s}}_0,\boldsymbol{\theta}_0)\le J(\mathbf{y}_m;\hat{x}_1[m(N+1)+n],\hat{\mathbf{s}}_1,\boldsymbol{\theta}_1);\\ 1, & J(\mathbf{y}_m;\hat{x}_0[m(N+1)+n],\hat{\mathbf{s}}_0,\boldsymbol{\theta}_0)> J(\mathbf{y}_m;\hat{x}_1[m(N+1)+n],\hat{\mathbf{s}}_1,\boldsymbol{\theta}_1).\end{cases}$$

Es decir, en un caso práctico el detector se reduce a la resolución de dos problemas de estimación de la secuencia caótica (uno para f_0 y $\boldsymbol{\theta}_0$, y otro para f_1 y $\boldsymbol{\theta}_1$), y la selección de la estima que proporcione un menor error cuadrático medio.

La situación para el segundo esquema de transmisión mostrado en la Figura 7.5 es similar: $p(\mathbf{y}_m;\mathbf{x}_i^m)$ es de nuevo una Gaussiana $(N+1)$-dimensional dada por (7.6), pero cuya función de coste es ahora

$$\begin{aligned} \tilde{J}(\mathbf{y}_m;\mathbf{x}_i) &= (\mathbf{y}_m-\mathbf{x}_i^m)^T(\mathbf{y}_m-\mathbf{x}_i^m) \\ &= \sum_{k=0}^{N}(y[m(N+1)+k]-A_i x_0[m(N+1)+k])^2 \\ &= \sum_{k=0}^{N}(y[m(N+1)+k]-A_i f_{\mathbf{s}}^{k-n}(x_0[m(N+1)+n]))^2 \\ &= \tilde{J}(\mathbf{y}_m;x_0[m(N+1)+n],\mathbf{s}_i,A_i). \end{aligned} \tag{7.8}$$

Y el detector óptimo se plantea exactamente igual que en el caso anterior, haciendo uso de (7.8) en lugar de (7.7):

$$\hat{b}[m]=\begin{cases}0, & \tilde{J}(\mathbf{y}_m;\hat{x}_0^0[m(N+1)+n],\hat{\mathbf{s}}_0,A_0)\le \tilde{J}(\mathbf{y}_m;\hat{x}_0^1[m(N+1)+n],\hat{\mathbf{s}}_1,A_1);\\ 1, & \tilde{J}(\mathbf{y}_m;\hat{x}_0^0[m(N+1)+n],\hat{\mathbf{s}}_0,A_0)> \tilde{J}(\mathbf{y}_m;\hat{x}_0^1[m(N+1)+n],\hat{\mathbf{s}}_1,A_1);\end{cases}$$

donde $\hat{x}_0^i[m(N+1)+n]$ y $\hat{\mathbf{s}}_i$ representan la estima ML de la muestra de referencia y del itinerario del bloque m-ésimo suponiendo que $b[m] = i$ ($i \in \{0,1\}$) respectivamente.

Como alternativa sencilla se va a considerar también otro detector subóptimo basado en la estimación del vector de parámetros de bifurcación. En el caso binario la idea consiste simplemente en obtener una estima de $\boldsymbol{\theta}$, $\hat{\boldsymbol{\theta}}$, mediante alguno de los métodos propuestos en el Capítulo 6, y, para el primer esquema estudiado, decidir el bit transmitido de acuerdo con

$$\hat{b}[m] = \begin{cases} 0, & J_{\mathrm{LS}}(\hat{\boldsymbol{\theta}}_0^m) \leq J_{\mathrm{LS}}(\hat{\boldsymbol{\theta}}_1^m); \\ 1, & J_{\mathrm{LS}}(\hat{\boldsymbol{\theta}}_0^m) > J_{\mathrm{LS}}(\hat{\boldsymbol{\theta}}_1^m); \end{cases}$$

siendo $\hat{\boldsymbol{\theta}}_i^m = h_i(\mathbf{y}_m)$ el estimador de $\boldsymbol{\theta}$ para el bloque de observaciones correspondiente al bit transmitido m-ésimo, con $0 \leq m \leq N_b - 1$, y $J_{\mathrm{LS}}(\boldsymbol{\theta})$ la función de coste de mínimos cuadrados, dada por (6.30), que únicamente considera el error de predicción entre muestras consecutivas:

$$J_{\mathrm{LS}}(\boldsymbol{\theta}) = \sum_{k=1}^{N} (y[k] - f(y[k-1]; \boldsymbol{\theta}))^2,$$

Para el segundo esquema la idea es la misma, pero de nuevo debe modificarse la función de coste,

$$\tilde{J}_{\mathrm{LS}}(A_i, \boldsymbol{\theta}) = \sum_{k=1}^{N} (y[k] - A_i f(y[k-1]; \boldsymbol{\theta}))^2,$$

de modo que finalmente el detector resulta

$$\hat{b}[m] = \begin{cases} 0, & \tilde{J}_{\mathrm{LS}}(A_0, \hat{\boldsymbol{\theta}}_m) \leq \tilde{J}_{\mathrm{LS}}(A_1, \hat{\boldsymbol{\theta}}_m); \\ 1, & \tilde{J}_{\mathrm{LS}}(A_0, \hat{\boldsymbol{\theta}}_m) > \tilde{J}_{\mathrm{LS}}(A_1, \hat{\boldsymbol{\theta}}_m); \end{cases}$$

siendo $\hat{\boldsymbol{\theta}}_m$ el estimador de $\boldsymbol{\theta}$ para el único vector de parámetros existente en este caso.

7.3.1.3. Rendimiento para Canal Gaussiano

En esta sección se analizan brevemente dos posibles esquemas de conmutación caótica. El mapa utilizado en ambos casos para generar la secuencia caótica ha sido el BSK-TM, debido a que proporciona señales bipolares cuya energía media se mantiene constante con independencia del valor de su parámetro de bifurcación. En [Luengo2000b] puede verse otro ejemplo en el que se utiliza el TM con $\beta = 1{,}5$ y $\beta = 1{,}9$ para generar las señales caóticas.

En primer lugar, en la Figura 7.8 se muestra la tasa de errores en función de la relación E_b/N_0 para el esquema de CS unipodal de la Figura 7.5 con $K = 2$ y cuatro longitudes de la secuencia caótica (factores de ensanche) distintos. Puede apreciarse cómo el detector óptimo (basado en el filtro adaptado y en consecuencia irrelizable) consigue una BER muy cercana a la de la modulación no caótica equivalente, OOK.

En cuanto al resto de los detectores, para $N \leq 8$ todos presentan una BER bastante mala, siendo necesario $N \geq 16$ para conseguir una buena tasa de aciertos, aunque aún alejada de la del detector óptimo. En general se observa que los detectores basados en el VA son los que mejor funcionan, mientras que el basado en el estimador HC-ML es el que proporciona una BER más elevada. El detector alternativo basado en estimar el valor del parámetro de bifurcación mediante el estimador HCLS funciona muy mal para valores de N bajos, pero conforme N aumenta mejora su rendimiento, siendo similar al del VA para $N = 32$ y $N = 64$. Nótese además que en este caso no es posible recurrir a detectores basados en la energía de la señal recibida como en otros esquemas de conmutación.

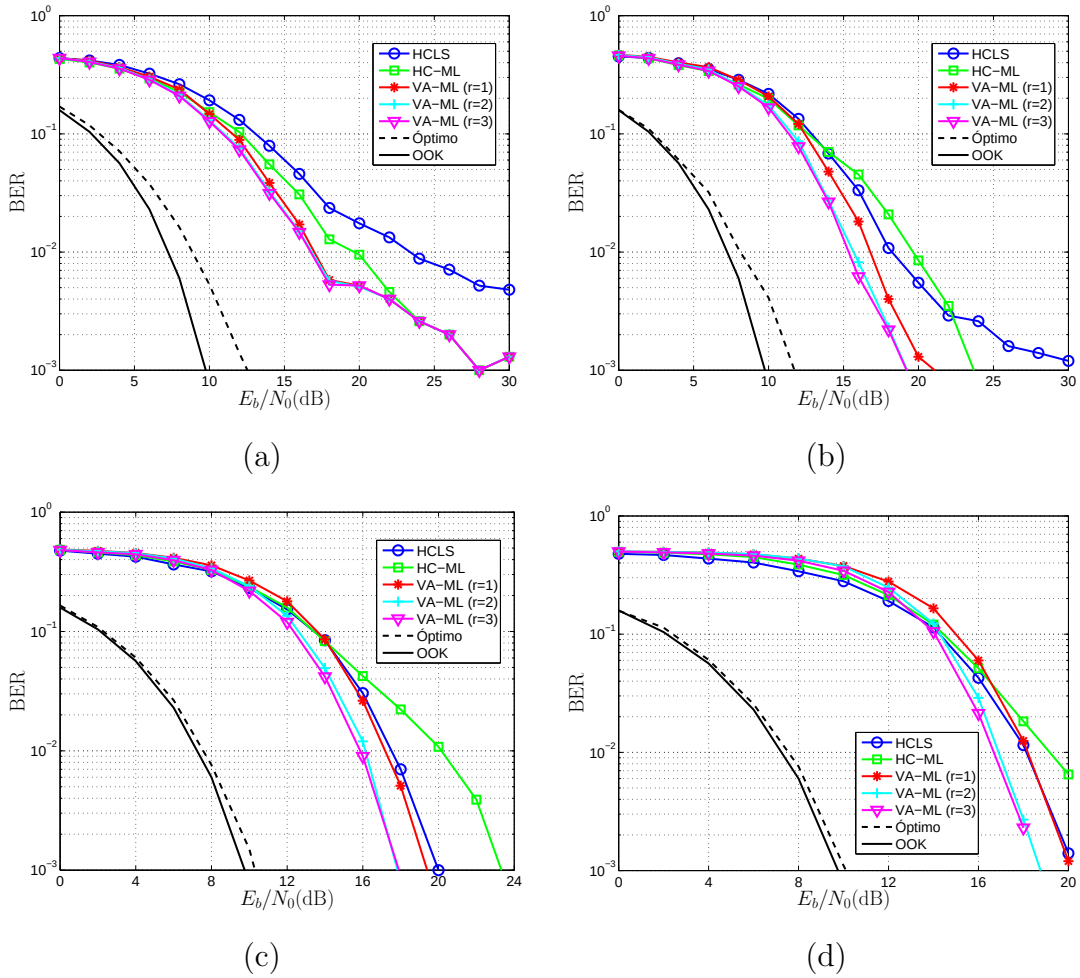


Figura 7.8: BER para el esquema de conmutación caótica unipodal con $K = 2$ en el que se usa el BSK-TM con dos parámetros de bifurcación distintos ($c_0 = -0{,}1$ y $c_1 = 0{,}1$). (a) $N = 8$. (b) $N = 16$. (c) $N = 32$. (d) $N = 64$.

A continuación, en la Figura 7.9 se muestra la tasa de errores para el esquema de conmutación antipodal de la Figura 7.6, en el que se usa una sola función base

caótica generada mediante el BSK-TM con $c = 0{,}1$. Los resultados y las conclusiones son similares al caso anterior: el detector óptimo consigue un rendimiento similar al del esquema no caótico correspondiente (PSK en este caso) y los mejores detectores subóptimos son los basados en el VA. Sin embargo, a diferencia del sistema unipodal, el peor detector en esta ocasión es el basado en el HCLS, mientras que el basado en el HC-ML presenta un rendimiento más cercano al del VA con $r = 1$. Nótese que de nuevo no es posible plantear un detector basado en la energía, y que la ganancia del esquema antipodal frente al unipodal disminuye conforme aumenta N para los detectores subóptimos. Por ejemplo, usando el VA con $r = 3$ para $N = 16$ se alcanza una probabilidad de error de 10^{-3} con un valor de E_b/N_0 casi 3 dB inferior en el caso del esquema antipodal, mientras que para $N = 32$ esta ganancia se ha reducido a aproximadamente 1 dB, y para $N = 64$ es todavía menor.

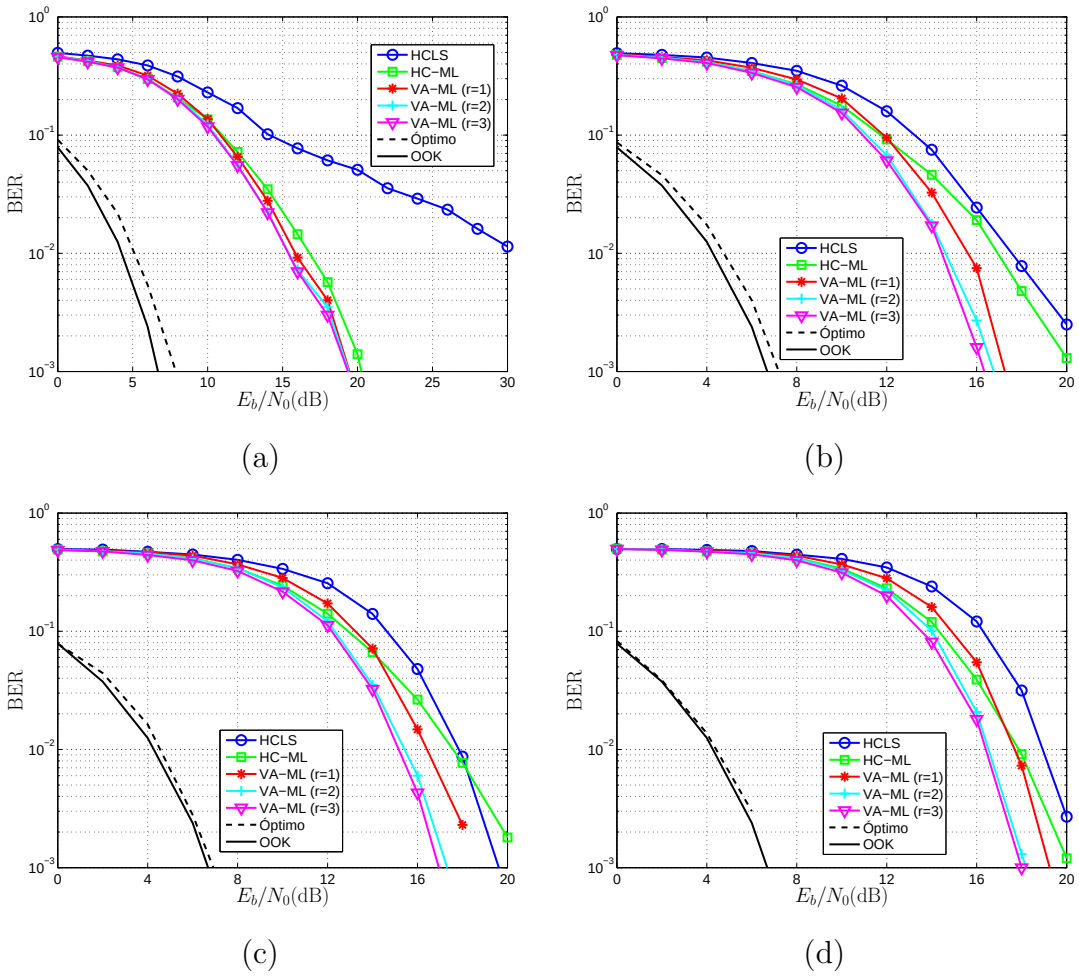


Figura 7.9: BER para el esquema de conmutación caótica antipodal con $K = 1$ en el que se usa el BSK-TM con un único parámetro de bifurcación: $c = 0{,}1$. (a) $N = 8$. (b) $N = 16$. (c) $N = 32$. (d) $N = 64$.

7.3.2. Esquema Basado en la Secuencia Simbólica y la Iteración Hacia Atrás

7.3.2.1. Esquema del Transmisor

En esta sección se propone un esquema de comunicaciones caóticas novedoso basado en la generación de las secuencias caóticas mediante iteración hacia atrás. Como ya se vio en la Sección 2.4.2, para un mapa caótico unidimensional la iteración hacia atrás requiere el conocimiento a priori de la secuencia simbólica. Esta secuencia es la que permite seleccionar una única señal caótica de entre el conjunto de todas las que se pueden generar mediante iteración hacia atrás, ya que los mapas caóticos unidimensionales nunca son invertibles, pero cada punto dispone siempre de un número finito de preimágenes.

La idea básica del modulador consiste en aprovechar la relación conocida entre una señal caótica y su itinerario para transmitir la información deseada embebida en la secuencia simbólica de la propia señal caótica. Es decir, para un mapa caótico con $K \leq M$ intervalos "útiles" (esto es, que se utilizan para codificar), el modulador asocia cada bloque de $k = \lfloor \log_2 K \rfloor$ bits de información (símbolos digitales) con un símbolo del itinerario del mapa caótico, que se utiliza para generar la secuencia caótica transmitida mediante iteración hacia atrás. El esquema del transmisor se muestra en la Figura 7.10, donde se utiliza el índice m para la secuencia de bits de información, $b[m]$, indicando que la tasa binaria puede ser distinta de la tasa de la señal caótica, $f_s = 1/T_s$, que viene dada por (7.1), suponiendo que $K = 2^k$ y se transmite un bloque de $N + 1$ muestras de la señal caótica por bit.

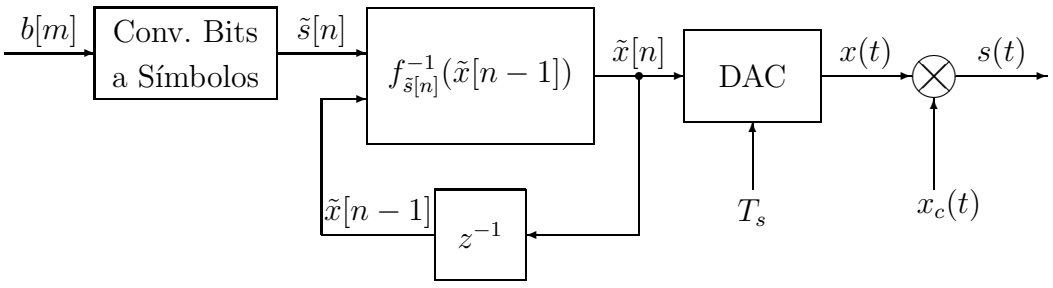


Figura 7.10: Diagrama de bloques del transmisor para el sistema de codificación simbólica propuesto.

Suponiendo que $K = 2$ y que únicamente se transmite una muestra de la señal caótica por bit (único caso considerado en lo sucesivo), el equivalente discreto en banda base de la señal caótica transmitida para el esquema de la Figura 7.10 es

$$\tilde{x}[n] = x[N_b - (n+1)] = f^{-1}_{\tilde{s}[n]}(\tilde{x}[n-1]; \boldsymbol{\theta}) = f^{-1}_{s[N_b-n]}(x[N_b - n]; \boldsymbol{\theta}),$$

para $0 \leq n \leq N_b - 1$, donde N_b es el número de bits que se desean transmitir. El estado inicial del sistema, $\tilde{x}[-1] = x[N_b]$, puede ser aleatorio o fijado a priori, ya que para

secuencias suficientemente largas es irrelevante, y la secuencia caótica transmitida es

$$\begin{aligned}\tilde{\mathbf{x}} &= [\tilde{x}[0],\ \tilde{x}[1],\ \ldots,\ \tilde{x}[N_b-2],\ \tilde{x}[N_b-1]]^T \\ &= [x[N_b-1],\ x[N_b-2],\ \ldots,\ x[1],\ x[0]]^T.\end{aligned}$$

La relación entre $\tilde{s}[n]$ y $b[n]$ y el rendimiento de este sistema se encuentran íntimamente ligados al mapa caótico utilizado. En [Luengo2005c] se analizó el rendimiento de este esquema para varios de los mapas caóticos utilizados a lo largo de la Tesis (BSM, SK-TM y BSK-TM). Sin embargo, en [Luengo2005a] se ha propuesto un mapa específico más adecuado para este sistema:

$$f(x) = \begin{cases} \frac{2x+(1+c)}{1-c}, & -1 \leq x \leq -c; \\ \phi(x;c), & -c < x < c; \\ \frac{2x-(1+c)}{1-c}, & c \leq x \leq 1. \end{cases} \tag{7.9}$$

La idea de este mapa es que el intervalo central actúe como *intervalo de guarda* que garantice una separación mínima entre las muestras de la señal caótica, facilitando su posterior detección. En este caso, la relación entre los símbolos del itinerario y los bits de información viene dada por

$$\tilde{s}[n] = s[N_b - (n+1)] = 1 + 2b[n], \tag{7.10}$$

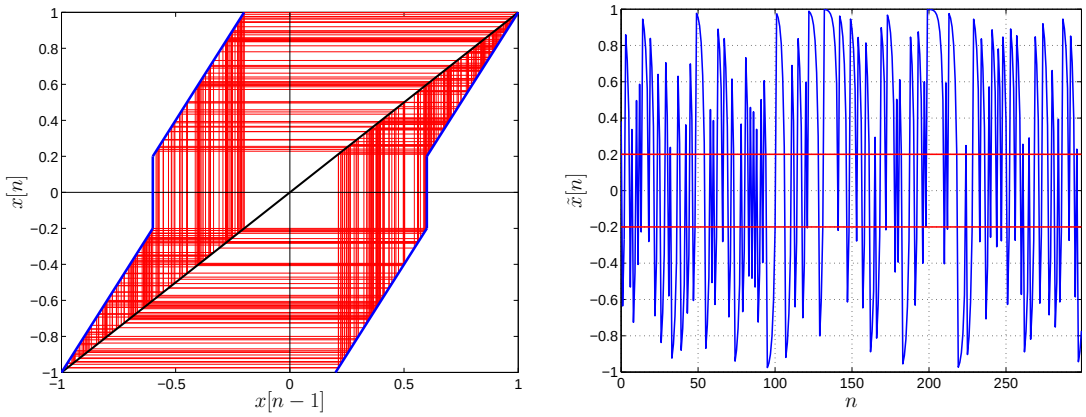
con $0 \leq n \leq N_b - 1$. Nótese que $x[n]$ nunca va a pertenecer a $E_2 = (-c, c)$, ya que $s[n] \neq 2$ siempre, de modo que en dicho intervalo $f(x)$ puede tomar una forma arbitraria cualquiera que se representa por $\phi(x;c)$ (en [Luengo2005a] se utilizó $\phi(x;c) = x/c$, de modo que $f(x)$ fuera un mapa de Bernouilli). El mapa inverso de (7.9), que es el que realmente se utiliza en la codificación, resulta [Luengo2005a]

$$f_s^{-1}(x) = \begin{cases} \frac{(1-c)x-(1+c)}{2}, & s = 1; \\ \phi^{-1}(x;c), & s = 2; \\ \frac{(1-c)x+(1+c)}{2}, & s = 3. \end{cases} \tag{7.11}$$

En la Figura 7.12(a) se muestra la forma del mapa en los dos intervalos de interés. Y en la Figura 7.11 se presenta un ejemplo de la iteración gráfica hacia atrás del mapa usando (7.11) con $s[n] \in \{1, 3\}$, junto con la señal caótica obtenida, constatándose que efectivamente $x[n]$ nunca pertenece a E_2.

Aunque el mapa caótico dado por (7.9) proporciona un buen rendimiento en términos de BER, como se muestra en la Sección 7.3.2.3, presenta dos problemas importantes [Luengo2006]:

1. El mapa tiene exactamente la misma forma en los dos intervalos de interés, E_1 y E_3. Esto facilita la detección de la información transmitida, ya que, como se ha visto a lo largo de la Tesis, los mapas PWL con la misma pendiente en sus intervalos son en general más sencillos de estimar (véase por ejemplo el BSM), pero compromete la seguridad del esquema de comunicaciones.



(a) (b)

Figura 7.11: Ejemplo de señal caótica generada mediante iteración hacia atrás usando (7.11) con $c = 0{,}2$, $N_b = 299$ y $\tilde{s}[n] \in \{1, 3\}$. (a) Iteración gráfica. (b) Secuencia caótica obtenida, $\tilde{x}[n]$.

2. Al dejar el intervalo central como intervalo de guarda sin usar se está limitando mucho el rango de $\tilde{x}[n]$, ya que las sucesivas muestras de la secuencia caótica tampoco podrán pertenecer a aquellas regiones del espacio de fases que se mapeen en E_2 bajo una, dos, y hasta N_b iteraciones. Por ejemplo, teniendo en cuenta que $\tilde{x}[-1] \in \{[-1, -c] \cup [c, 1]\}$ y que $f(\tilde{x}[0])$ no puede pertenecer a E_2, se concluye que $\tilde{x}[0] \notin \{-R_E^1 \cup E_2 \cup R_E^1\}$, siendo

$$R_E^1 = \left(\frac{1+c}{2} - \frac{c(1-c)}{2},\ \frac{1+c}{2} + \frac{c(1+c)}{2} \right)$$

la *región de exclusión* para la primera iteración hacia atrás, cuyo tamaño aumenta en gran medida conforme se incrementa c. Así por ejemplo, para $c = 0{,}1$, $R_E^1 = (0{,}505,\ 0{,}595)$, habiéndose perdido un 10 % del espacio de fases total disponible, mientras que para $c = 0{,}5$, $R_E^1 = (0{,}625,\ 0{,}875)$, descartándose ya un 50 % del conjunto de valores que debería poder tomar $\tilde{x}[0]$. Además, este problema se agrava conforme se itera hacia atrás, ya que hay que considerar $R_E^2,\ R_E^3,\ \ldots,\ R_E^{N_b}$. Esto implica que para valores altos de N_b el conjunto de valores que pueden tomar las últimas muestras de la secuencia transmitida es muy limitado, lo que puede causar la pérdida de parte de las características interesantes de la señal caótica y de nuevo reduce la seguridad del esquema de comunicación propuesto.

Afortunadamente, estos dos problemas se pueden resolver utilizando otros mapas PWL similares a (7.9), aunque con ligeras modificaciones, cuyos parámetros (pendiente y "offset" en cada intervalo, excepto el de guarda) se muestran en la Tabla 7.1, y cuya forma se presenta en la Figura 7.12.

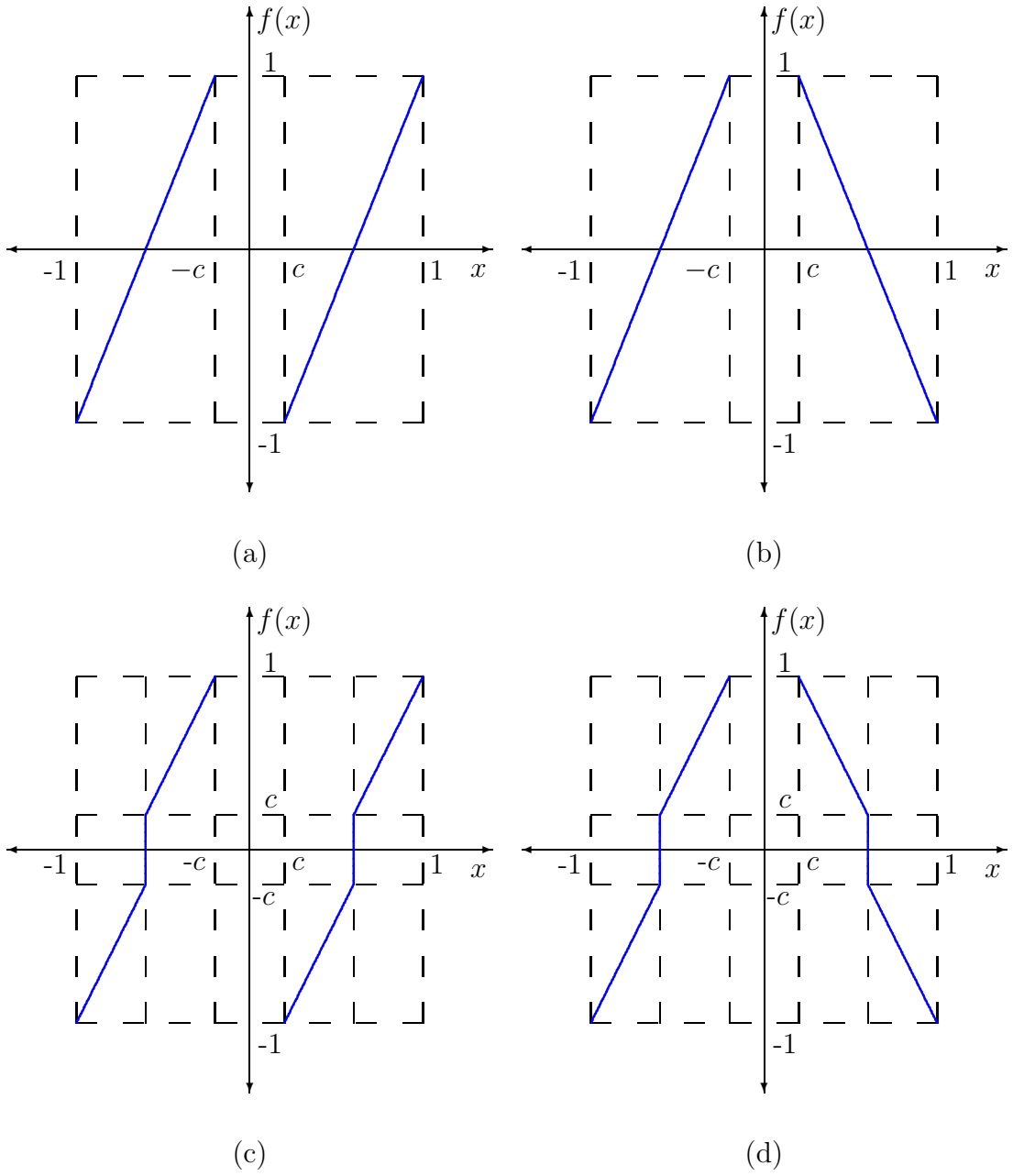


Figura 7.12: Mapas caóticos considerados para el esquema de codificación simbólica propuesto. (a) Mapa de [Luengo2005a]. (b) Mapa de [Luengo2005a] con inversión de la pendiente en E_3. (c) Mapa de [Luengo2005a] con división de E_1 y E_3 en dos subintervalos de tal modo que $f(x) \notin (-c, c)$. (d) Mapa de [Luengo2005a] con división de E_1 y E_3 en dos subintervalos como en (c) e inversión de la pendiente para $x > 0$.

Como se puede apreciar, una primera posibilidad para tratar de mejorar la seguridad del sistema es sustituir (7.9) (que degenera en un BSM bipolar con rango $[-1, 1]$ cuando

$c = 0$) por un mapa del tipo tienda de campaña que tenga pendiente negativa en E_3 como el mostrado en la Figura 7.12(b) (este mapa degenera en el S-TM con $\beta = 2$ cuando $c = 0$). Sin embargo, sigue apareciendo el segundo problema mencionado anteriormente: la existencia de regiones de exclusión. Para evitarlo se proponen los dos mapas PWL con cinco regiones de las figuras 7.12(c) y (d), construidos de tal modo que $f(x)$ nunca se mapee en el intervalo de guarda para ninguna de las cuatro regiones útiles ($E_1,\ E_2,\ E_4,\ E_5$).

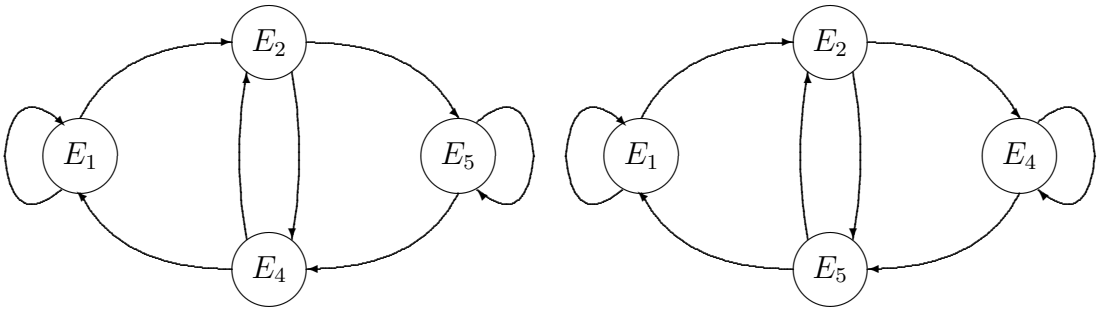
Nótese que ahora $b[n] = 0$ se representa haciendo que $\tilde{x}[n]$ pertenezca a E_1 o E_2, y $b[n] = 1$ se representa con $\tilde{x}[n]$ dentro de E_4 o E_5. No obstante, nunca existe confusión a la hora de elegir el intervalo, ya que para cualquier valor de $x[n]$, al iterar hacia atrás únicamente se puede llegar exactamente a uno de los dos intervalos asociados al cero y a uno de los dos intervalos asociados al uno. Esto se puede apreciar claramente en los diagramas de estados correspondientes a los mapas de las figuras 7.12(c) y (d) (idénticos excepto por el hecho de encontrarse los estados E_4 y E_5 intercambiados), mostrados en la Figura 7.13, en los que se observa que a cada estado llega solamente una transición correspondiente a $\tilde{s}[n] = 0$ y otra debida a $\tilde{s}[n] = 1$.

Mapa	E_i	$a_i,\ b_i$
Mapa 1 [Luengo2005a]	$E_1 = [-1, -c]$ $E_3 = [c, 1]$	$a_1 = 2/(1-c),\ b_1 = (1+c)/(1-c)$ $a_3 = 2/(1-c),\ b_3 = -(1+c)/(1-c)$
Mapa 2	$E_1 = [-1, -c]$ $E_3 = [c, 1]$	$a_1 = 2/(1-c),\ b_1 = (1+c)/(1-c)$ $a_3 = -2/(1-c),\ b_3 = (1+c)/(1-c)$
Mapa 3	$E_1 = [-1, -(1+c)/2]$ $E_2 = [-(1+c)/2, -c]$ $E_4 = [c, (1+c)/2]$ $E_5 = [(1+c)/2, 1]$	$a_1 = 2,\ b_1 = 1$ $a_2 = 2,\ b_2 = 1 + 2c$ $a_4 = 2,\ b_1 = -(1+2c)$ $a_5 = 2,\ b_1 = -1$
Mapa 4	$E_1 = [-1, -(1+c)/2]$ $E_2 = [-(1+c)/2, -c]$ $E_4 = [c, (1+c)/2]$ $E_5 = [(1+c)/2, 1]$	$a_1 = 2,\ b_1 = 1$ $a_2 = 2,\ b_2 = 1 + 2c$ $a_4 = -2,\ b_1 = 1 + 2c$ $a_5 = -2,\ b_1 = 1$

Tabla 7.1: Parámetros (pendiente y "offset") de los cuatro mapas propuestos para el esquema de codificación de la Figura 7.10 en los intervalos útiles.

Para corroborar la mejora introducida por los mapas de las figuras 7.12(c) y (d) con respecto a los de las figuras 7.12(a) y (b), en la Figura 7.14 se muestra el diagrama de "scattering", obtenido simplemente dibujando $x[n]$ frente a $x[n-1]$, para una secuencia típica generada con cada uno de los cuatro mapas. Puede apreciarse claramente como aparecen huecos en el diagrama para los mapas de las figuras 7.12(a) y (b), que se corresponden con las regiones de exclusión (en realidad cuando $n \to \infty$ el conjunto de muestras válidas para ambos mapas forma un conjunto de Cantor), mientras que para las figuras 7.12(c) y (d) reproducen fielmente la forma de los mapas generadores.

Para finalizar esta sección, nótese que, puesto que el sistema propuesto transmite la información haciendo uso de la secuencia simbólica (sistemas CC), se puede incluir



(a) (b)

Figura 7.13: Diagramas de estados para los dos mapas caóticos con 5 intervalos considerados. (a) Diagrama de estados para el mapa de la Figura 7.12(c). (b) Diagrama de estados para el mapa de la Figura 7.12(d).

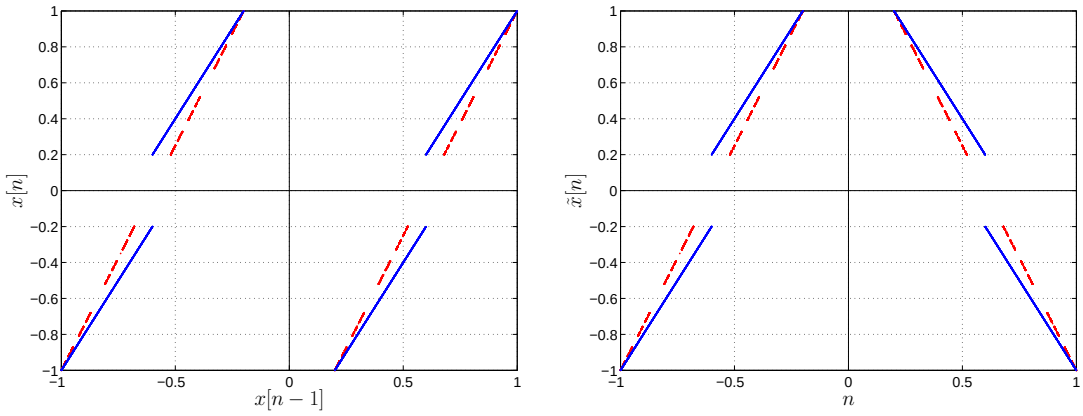
dentro de los esquemas de codificación caótica o simbólica, siendo en este sentido similar a los propuestos por Maggio et al. [Maggio2001a, Maggio2001b] o Ciftci y Williams [Ciftci2001a, Ciftci2001b], descritos brevemente en la Sección 7.2.2.3. Sin embargo, en ambos casos la señal caótica se genera mediante iteración hacia delante, mientras que nuestro sistema recurre a la iteración hacia atrás. Esto proporciona al esquema de la Figura 7.10 una serie de ventajas que la diferencian de los métodos propuestos anteriormente:

1. Tanto el modulador como el demodulador son mucho más simples que los de los esquemas previos.

2. Este esquema admite la utilización de cualquier mapa caótico. Esto no resulta evidente en el caso del esquema de Ciftci y Williams, que se basa en la obtención de la relación entre la dinámica simbólica y la señal caótica, algo que de momento los autores sólo han podido obtener para el BSM y el TM. En cuanto al esquema de Maggio et al., se basa en el BSM, y, aunque permite llevar a cabo una transformación para generar las señales de acuerdo con la dinámica de otros mapas, estos deben ser topológicamente conjugados con el BSM, lo que limita mucho el conjunto de mapas utilizables.

3. El esquema propuesto no realiza ninguna aproximación a la hora de generar las secuencias caóticas, mientras que los otros dos esquemas sí: el de Maggio utiliza una condición inicial representada únicamente por K bits, y el de Ciftci y Williams lleva a cabo un truncamiento en la longitud del filtro lineal que genera las señales caóticas a partir de la secuencia simbólica.

4. Las señales generadas por nuestro método son realmente caóticas, y por lo tanto poseen todas las características interesantes de las mismas, tales como la aperiodicidad. Como consecuencia de las aproximaciones realizadas las señales generadas



(a) (b)

Figura 7.14: Diagramas de "scattering" para los cuatro mapas de la Figura 7.12. (a) Mapas de la Figura 7.12(a) (en rojo) y (c) (en azul). (b) Mapas de la Figura 7.12(b) (en rojo) y (d) (en azul).

por el resto de métodos son *pseudocaóticas*, pudiendo perder parte de las características interesantes de las señales caóticas y apareciendo segmentos de señal repetidos, lo que compromete la seguridad de la señal transmitida.

5. Aunque en los tres casos se utiliza el algoritmo de Viterbi para decodificar, en los esquemas anteriores el número de estados crece exponencialmente con la precisión usada, mientras que en nuestro caso no depende en absoluto de la precisión, pudiéndose utilizar un VA con tan sólo 2 estados con muy buenos resultados.

7.3.2.2. Esquema del Receptor

El diagrama de bloques genérico del canal y el receptor es idéntico al del sistema de CC mostrado en la Figura 7.7. La única diferencia entre ambos se halla en el bloque denominado "receptor digital". Para el esquema de la Sección 7.3.1.1 se buscaba la señal caótica que minimizase el error cuadrático medio de entre un conjunto finito de señales posibles (dos en el caso binario). En esta ocasión, puesto que la información se halla contenida en los símbolos del itinerario, se trata de resolver un problema de estimación de la secuencia simbólica, cuyo estimador ML viene dado por

$$\begin{aligned}\hat{\mathbf{s}}_{\mathrm{ML}} &= \arg\min_{\mathbf{s}} J(\mathbf{y}; x[N_b], \mathbf{s}, \boldsymbol{\theta}) \\ &= \arg\min_{\mathbf{s}} \sum_{k=0}^{N_b-1} \left(y[k] - f^{-(N_b-k)}_{s[k],\ldots,s[N_b-1]}(x[N_b]; \boldsymbol{\theta}) \right)^2.\end{aligned}$$

La relación entre la estima ML de la secuencia simbólica y la estima ML de los bits de información depende del mapa caótico utilizado, pero es siempre unívoca. Por ejemplo,

si esta relación viene dada por (7.10), entonces

$$\hat{\mathbf{b}}_{\mathrm{ML}} = \frac{\hat{\tilde{\mathbf{s}}}_{\mathrm{ML}} - 1}{2} = \frac{\hat{\mathbf{s}}_{\mathrm{ML}}(N_b : -1 : 1) - 1}{2}.$$

Por desgracia, $J(\mathbf{y}; x[N_b], \mathbf{s}, \boldsymbol{\theta})$ es una función discontinua del itinerario, de modo que no se puede tomar su derivada e igualar a cero para obtener $\hat{\mathbf{s}}_{\mathrm{ML}}$. Sin embargo, para un número de bits transmitidos igual a N_b el número de posibles secuencias simbólicas es finito (2^{N_b} como mucho para el caso binario). En consecuencia este problema se puede resolver mediante una aproximación de "fuerza bruta" como la mostrada en el Capítulo 3: probar todos los itinerarios válidos y seleccionar aquel que minimice $J(\mathbf{y}; x[N_b], \mathbf{s}, \boldsymbol{\theta})$. De hecho, en el Capítulo 3 se obtenía dicho itinerario óptimo como paso previo indispensable para encontrar $\hat{\mathbf{x}}_{\mathrm{ML}}$. Idéntico procedimiento se puede seguir para hallar las estimas MAP y MS de la secuencia simbólica.

Desafortunadamente, su elevado coste computacional hace que estos algoritmos de "búsqueda exhaustiva" sean irrealizables para valores de N_b medios/altos. No obstante, en el Capítulo 5 se han propuesto diversos algoritmos computacionalmente eficientes para obtener $\hat{\mathbf{x}}_{\mathrm{ML}}$, todos los cuales se concentraban en obtener una buena estima del itinerario con un coste reducido. En esta sección se propone utilizar uno de dichos algoritmos para obtener $\hat{\mathbf{s}}_{\mathrm{ML}}$: el algoritmo de Viterbi.

7.3.2.3. Rendimiento para Canal Gaussiano

En esta sección se analiza el comportamiento del esquema de codificación simbólica desarrollado cuando la única distorsión introducida por el canal es ruido aditivo blanco y Gaussiano. En primer lugar, en la Figura 7.15 se compara la tasa de errores para los mapas 3 y 4.

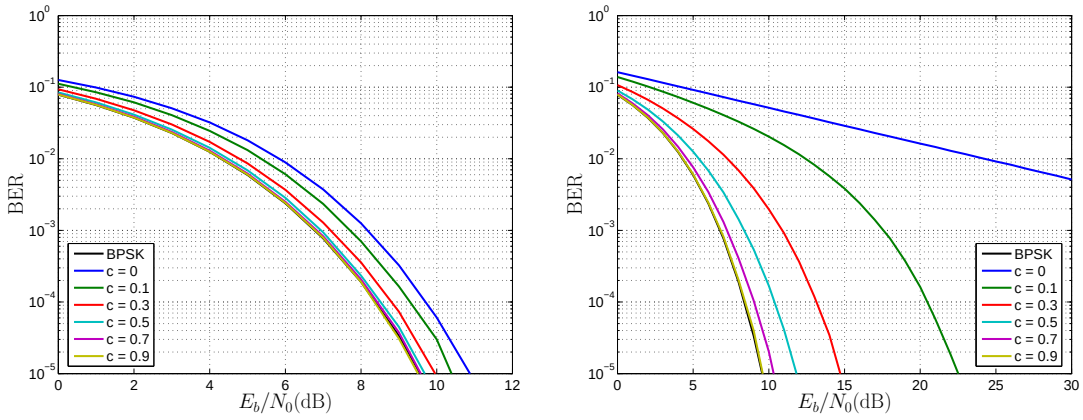


Figura 7.15: BER para el esquema de codificación caótica usando los cuatro mapas de la Figura 7.12. (a) Mapa 3 (Figura 7.12(c)). (b) Mapa 4 (Figura 7.12(d)).

Como puede verse, en ambos casos cuanto mayor es el valor de c menor es la BER (aunque también es menor la "caoticidad" de las señales generadas, y por lo tanto la seguridad del esquema de transmisión), consiguiéndose prácticamente el mismo rendimiento que BPSK para $c = 0{,}9$. Nótese que el mapa 4 resulta más difícil de estimar que el 3, lo que se traduce en una BER mucho peor para valores de c bajos, algo que presumiblemente se verá compensado por un incremento en el grado de seguridad del esquema. En este sentido, las primeras pruebas realizadas parecen indicar la existencia de un compromiso entre rendimiento y seguridad [Luengo2005c], aunque este aspecto debe estudiarse de un modo más riguroso. Para finalizar, como era de esperar al eliminar las zonas de exclusión se consigue una mejora marginal de la BER, tal y como se muestra en la Figura 7.16 para los mapas 2 y 4 [Luengo2006].

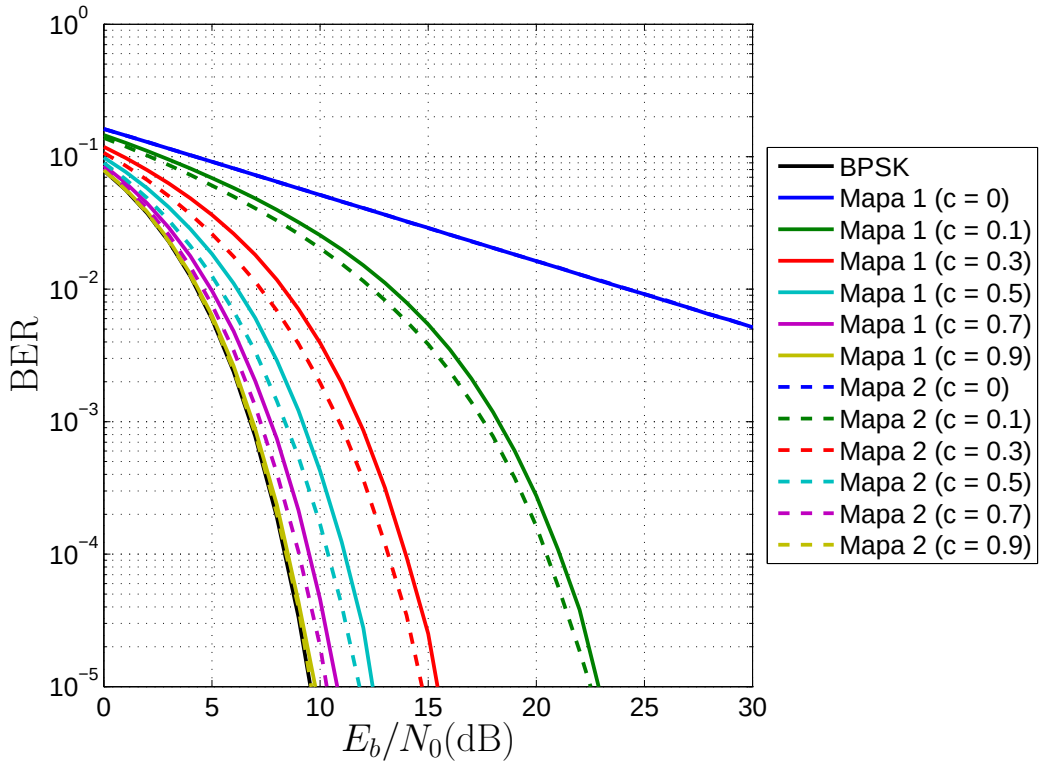


Figura 7.16: Comparación del rendimiento de los mapas 2 y 4 de la Figura 7.12.

7.3.2.4. Combinación con OFDM para Canales Multitrayecto

Hasta ahora se ha considerado únicamente un canal aditivo Gaussiano, y se ha mostrado mediante simulaciones el buen funcionamiento del esquema propuesto para el mismo. Sin embargo, para canales reales sujetos a propagación multitrayecto, variación temporal y/o desvanecimiento selectivo en frecuencia, las prestaciones del esquema de comunicaciones de la Figura 7.10 se van a degradar notablemente, al igual

que ocurre con cualquier sistema convencional de comunicaciones digitales de banda estrecha. Para evitar esta distorsión, en esta sección se propone combinar la codificación caótica descrita en la Sección 7.3.2.1 con un esquema de modulación convencional de banda ancha que es capaz de proporcionar cierta robustez frente a los efectos nocivos del canal: la modulación por división en portadoras ortogonales (OFDM).

La idea básica es la siguiente: construir un sistema OFDM convencional en el que las señales de cada subportadora estén moduladas de acuerdo con la modulación caótica de la Sección 7.3.2.1 en lugar de los tradicionales M-PSK o M-QAM. El diagrama de bloques del transmisor se muestra en la Figura 7.17 junto con el equivalente discreto paso bajo del canal de comunicaciones. En primer lugar, los bits de información se usan para obtener la codificación caótica de acuerdo con el mecanismo descrito en la Sección 7.3.2.1. A continuación, se realiza una conversión serie/paralelo (bloque S/P en la Figura 7.17), que agrupa las muestras caóticas en bloques de tamaño N_c. Esta información, junto con ceros de guarda y portadoras piloto, se le pasa al bloque IFFT ("Inverse Fast Fourier Transform"), que es simplemente el algoritmo que implementa de un modo eficiente de la DFT inversa (IDFT) en la que se basa el esquema de modulación OFDM. Por último, se añade un prefijo cíclico de $k \cdot N$ muestras ($N = N_c + N_p + N_z$ es la longitud de la IFFT) para evitar interferencia entre símbolos (ISI) y entre portadoras (ICI), y se transmite la señal por el canal.

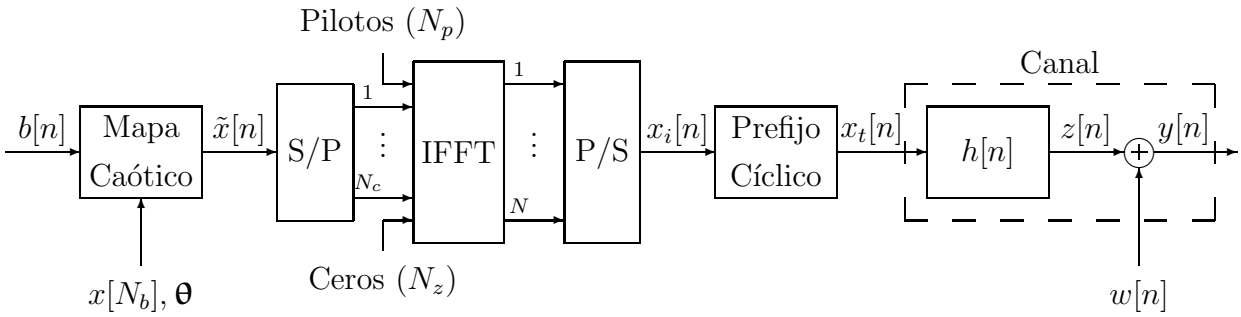


Figura 7.17: Diagrama de bloques del esquema de comunicación basado en OFDM con codificación caótica de las subportadoras: transmisor y canal.

El receptor es simplemente el dual del transmisor, tal y como se muestra en la Figura 7.18. En primer lugar se elimina el prefijo cíclico, y a continuación se lleva a cabo una FFT de $N = N_c + N_p + N_z$ muestras. De la señal resultante se descartan los ceros de guarda y se utilizan las portadoras piloto para estimar la respuesta en frecuencia del canal, lo que permite realizar a continuación una igualación en frecuencia de las N_c portadoras de información. Finalmente, se lleva a cabo una conversión paralelo/serie de la señal recibida (bloque P/S) y se le pasa dicha información al demodulador caótico basado en el VA.

Para realizar las simulaciones de este sistema, se han utilizado los parámetros básicos del estándar HIPERLAN2 [Hiper2, Khun2002]: IFFT de tamaño $N = 64$, con $N_c = 48$ portadoras que transportan información, $N_p = 4$ pilotos, y $N_z = 6$ símbolos

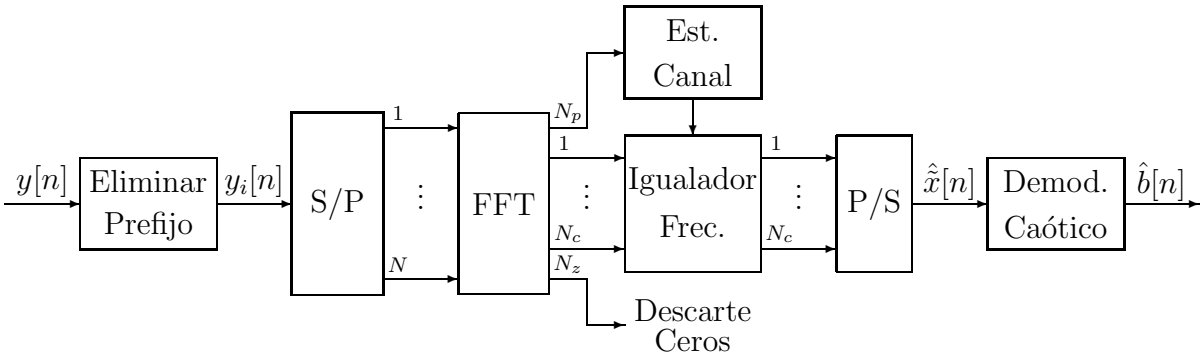


Figura 7.18: Diagrama de bloques del receptor del esquema de comunicación basado en OFDM con codificación caótica de las subportadoras.

de guarda (ceros) repartidos equitativamente en los extremos superior e inferior de la banda frecuencial, y un prefijo cíclico de 8 muestras. Respecto a los canales considerados, han sido cuatro:

1. Canal blanco Gaussiano (AWGC): $h_0[n] = \delta[n]$.

2. Canal muy sencillo de fase mínima con sólo dos rayos en el que la máxima amplitud corresponde al rayo directo:

$$h_1[n] = \delta[n] - 0{,}5\delta[n-1] \qquad \Rightarrow \qquad H_1(z) = \frac{z - 1/2}{z}.$$

3. Canal de fase no mínima de longitud cinco y en el que no existe rayo directo:

$$\begin{aligned} h_2[n] &= -0{,}3\delta[n-1] + 0{,}7\delta[n-2] + 0{,}4\delta[n-3] + 0{,}1\delta[n-4], \\ H_2(z) &= -0{,}3\frac{(z-z_1)(z-z_2)(z-z_2^*)}{z^4}, \end{aligned}$$

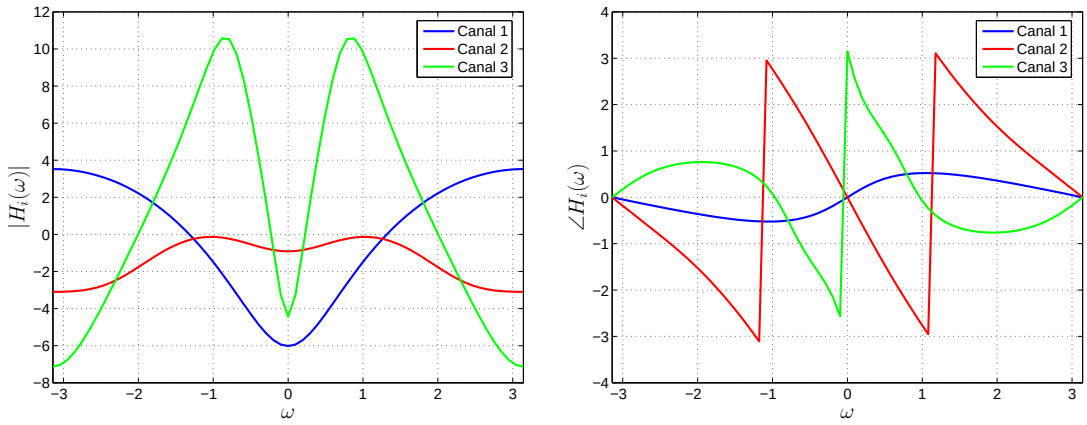
   con $z_1 = 3179/1118 \simeq 2{,}8435$ y $z_2 = -390/1529 + j\ 193/845 \simeq -0{,}2551 + j\ 0{,}2284$.

4. Canal con memoria infinita de fase no mínima:

$$H_3(z) = \frac{(z + 1/2)(z - 6/5)}{(z - z_1)(z - z_1^*)},$$

   con $z_1 = (1 + j)/2$.

En la Figura 7.19 se muestra la respuesta en frecuencia de los cuatro canales utilizados. Aunque ninguno de ellos se corresponda con un canal real, permiten analizar la viabilidad del esquema propuesto, y comprobar su buen funcionamiento en un entorno con interferencia multitrayecto.



(a) (b)

Figura 7.19: Respuesta en frecuencia de los distintos canales utilizados. (a) Módulo, $|H_i(\omega)|$. (b) Fase, $\angle H_i(\omega)$.

Los resultados de las simulaciones se muestran en la Figura 7.20. En todos los casos se asume que se conoce perfectamente la respuesta en frecuencia del canal y la varianza del ruido, de modo que se puede aplicar el estimador MSE para encontrar el símbolo transmitido por cada subcanal. La detección se lleva a cabo siempre sobre cada símbolo OFDM (es decir, se detectan bloques de $N_c = 48$ bits) mediante el VA. Como se puede apreciar en la figura, en ambos casos el rendimiento del sistema se degrada levemente y de una manera similar a lo que ocurre con el sistema basado en BPSK, mostrado como referencia.

7.4. Discusión

En este capítulo se ha considerado una posible aplicación práctica de las técnicas de estimación desarrolladas en los capítulos precedentes: el diseño de sistemas de comunicaciones de espectro ensanchado usando señales caóticas. Se han mostrado las características de las señales y sistemas caóticos que resultan potencialmente interesantes en comunicaciones, se han revisado los principales esquemas propuestos hasta la fecha agrupados en cuatro grandes categorías (enmascaramiento caótico, conmutación caótica, codificación simbólica, y sistemas basados en secuencias de ensanche caóticas). Se ha analizado el rendimiento de diversos sistemas de conmutación caótica haciendo uso de los estimadores subóptimos desarrollados en los capítulos 6 y 5, ya que el estimador óptimo es irrealizable. Por último, se ha propuesto un esquema novedoso basado en la codificación de la información a transmitir en el itinerario de la señal caótica. Las principales conclusiones de este capítulo son las siguientes:

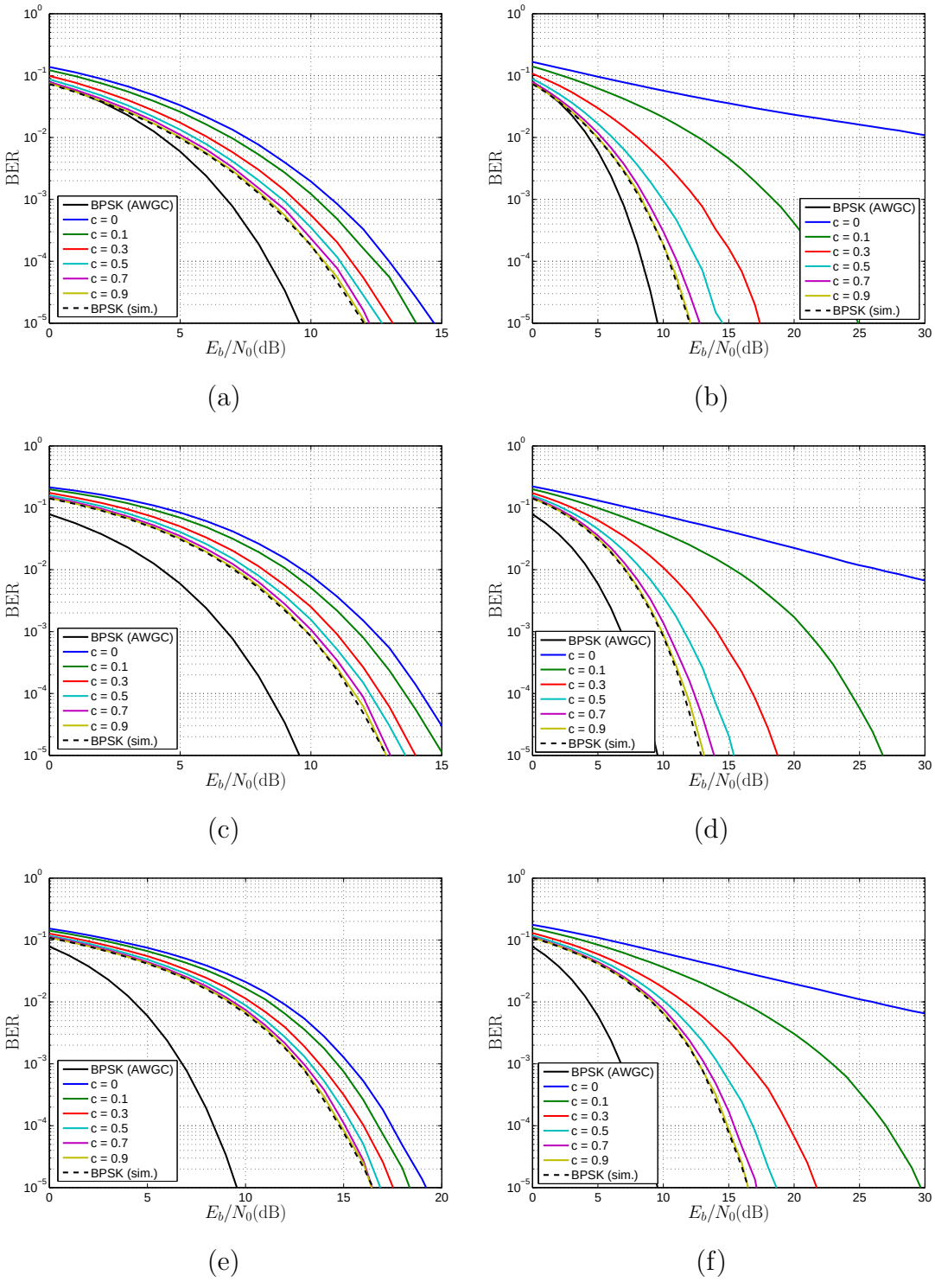


Figura 7.20: Comparación del rendimiento del sistema OFDM con codificación caótica para el canal Gaussiano y tres canales multitrayecto. (a) Mapa 3, canal $h_1[n]$. (b) Mapa 4, canal $h_1[n]$. (c) Mapa 3, canal $h_2[n]$. (d) Mapa 4, canal $h_2[n]$. (e) Mapa 3, canal $h_3[n]$. (f) Mapa 4, canal $h_3[n]$.

1. Los sistemas de comunicaciones caóticas aún no son suficientemente maduros para competir con los sistemas de comunicaciones convencionales. Aunque pueden ofrecer ventajas desde el punto de vista de la seguridad o la simplicidad de implementación, parece difícil que puedan llegar a competir con aquellos desde el punto de vista de BER. En consecuencia, su nicho de aplicación puede quedar reducido a aplicaciones específicas donde resulte aceptable intercambiar BER por un incremento en la seguridad o un menor consumo por ejemplo.

2. Es posible mejorar el rendimiento de los esquemas de conmutación caótica recurriendo a detectores basados en el principio de máxima verosimilitud. A pesar de que el detector ML óptimo sea irrealizable debido a su elevado coste computacional, se ha demostrado que mediante la aplicación del VA es posible conseguir un buen rendimiento, aunque alejado aún del de los sistemas de comunicaciones convencionales.

3. Se ha propuesto un esquema de codificación simbólica basado en la generación de las señales caóticas mediante iteración hacia atrás utilizando su itinerario para transmitir los bits de información deseados. Este esquema ha mostrado un excelente rendimiento, presentando numerosas ventajas frente a otros esquemas similares propuestos con anterioridad.

4. Se ha considerado la combinación del esquema de codificación anterior con OFDM para proporcionar cierto grado de robustez frente a la distorsión introducida por los canales reales. Mediante simulaciones se ha comprobado la viabilidad de esta combinación, así como su buen rendimiento.

5. Se ha constatado que la elección del mapa caótico resulta fundamental para conseguir un buen rendimiento en el caso del esquema de codificación simbólica, así como para garantizar su seguridad.

Sin embargo, todavía quedan múltiples líneas de investigación abiertas. Seguramente la más importante es la búsqueda del mapa idóneo que proporcione el mejor compromiso posible enre BER y seguridad para el esquema de codificación simbólica propuesto. En este sentido, es necesario llevar a cabo un estudio riguroso de la seguridad (probabilidad de detección e intercepción) del esquema CC con los diferentes mapas propuestos, analizando entre otros aspectos la robustez de la clave de codificación, que probablemente deberá ser el parámetro de bifurcación del mapa, ya que resulta mucho más difícil de estimar que la condición final. Además, debe estudiarse con mayor profundidad el rendimiento del esquema OFDM con codificación caótica propuesto, considerando canales más realistas y condiciones menos ideales para el receptor: estimación del canal, sincronización, igualación temporal previa a la frecuencial, etc. Por último, nótese que de nuevo puede resultar muy interesante el uso de mapas d-dimensionales, ya que es previsible que ayuden a mejorar el grado de seguridad del esquema propuesto.