Centro de Investigación Científica y de Educación Superior de Ensenada

CODIFICACION DE CANAL PARA LA TRANSMISION DE DATOS ENFOCADA A LOS SISTEMAS CDMA

TESIS
MAESTRIA EN CIENCIAS

RAMON ORLANDO SALAICES SOTELO

ENSENADA, B. C., AGOSTO DEL 2000.

TESIS DEFENDIDA POR
RAMÓN ORLANDO SALAICES SOTELO
Y APROBADA POR EL SIGUIENTE COMITE

Dr. David H. Covarrubias Rosales

Director del Comité

M.C. Jaime Sanchez García

Miembro del Comité

M.C. Jorge E. Preciado Velasco

Miembro del Comité

Dr. Pedro Negrete Regagnon

Miembro del Comité

Dr. José Luis Medina Monroy

Jefe del Departamento de Electrónica y Telecomunicaciones

Dr. Federico Graef Ziehl

Director de Estudios del Posgrado

11 de Agosto del 2000

CENTRO DE INVESTIGACIÓN CIENTÍFICA Y DE
EDUCACIÓN SUPERIOR DE ENSENADA

DIVISIÓN DE FÍSICA APLICADA

DEPARTAMENTO DE
ELECTRÓNICA Y TELECOMUNICACIONES

CODIFICACIÓN DE CANAL PARA LA TRANSMISIÓN DE DATOS ENFOCADA A LOS SISTEMAS CDMA

TESIS

que para cubrir parcialmente los requisitos necesarios para obtener el grado de MAESTRO EN CIENCIAS presenta:

RAMÓN ORLANDO SALAICES SOTELO

Ensenada, Baja California, México. Agosto del 2000.

RESUMEN de la Tesis de ***Ramón Orlando Salaices Sotelo***, presentada como requisito parcial para la obtención del grado de ***MAESTRO EN CIENCIAS*** **en** ***ELECTRÓNICA Y TELECOMUNICACIONES.*** Ensenada, Baja California, México. Agosto del 2000.

CODIFICACIÓN DE CANAL PARA LA TRANSMISIÓN DE DATOS ENFOCADA A LOS SISTEMAS CDMA

Resumen aprobado por:

Dr. David H. Covarrubias Rosales
Director del comité de tesis

El canal radio de comunicaciones presenta características muy particulares con respecto a otros medios de propagación, así para el caso de medios guiados, como por ejemplo, en la transmisión vía fibras ópticas, se está hablando, en transmisión digital, de una probabilidad de error de bit, *BER*, muy baja del orden de 10^{-9}, o inclusive menor aún; es decir, de una transmisión propiamente sin error, conservando además el medio en todo momento sus características de propagación. En cambio el canal radio se caracteriza por ser un medio de propagación fuertemente hostil, con probabilidades de error muy grandes, con variación temporal (canal no estacionario) del *BER* desde 10^{-6} hasta 10^{-2}, con circunstancias especiales por la movilidad del usuario y con problemas fuertes de desvanecimientos y de dispersión.

Por lo mencionado anteriormente, es necesario que la información a transmitir sea protegida contra errores, dando lugar a lo que se conoce como codificación de canal. En la actualidad los sistemas móviles están orientados fundamentalmente al servicio de voz, pero de acuerdo a las expectativas de los sistemas de comunicación móvil, surge la gran necesidad de la transmisión de datos, dando como resultado una arda investigación, dentro de las cuales se encuentra el estudio y análisis de los sistemas de codificación de canal orientada al servicio de datos.

En este trabajo de investigación se plantea una propuesta de los parámetros óptimos del sistema de codificación de canal *CDMA* (códigos bloque). Dichos parámetros mantienen un *Throughput* elevado y constante en todo el margen de variación del *BER* de 10^{-6} hasta 10^{-2} y sobre todo manteniendo una sencillez en el codificador y decodificador.

Palabras clave: *BER*, *Throughput*, *CDMA* y Q_oS

ABSTRACT of the Thesis of ***Ramón Orlando Salaices Sotelo***, presented as a partial requirement to obtain the ***Master In Sciences*** **Degree in Electronic and Telecommunications.** Ensenada, Baja California, Mexico. August 2000.

Codification of Channel For the Data transmission Focused to CDMA Systems

The communications radio channel presents very particular features with respect to other propagation medium, thus for the case of average guidances, like for example, the transmission through optical fibers, in which is being spoken in digital transmission of a very low bit error rate probability (*BER)* the order of the 10^{-9}, or inclusively smaller one still; that is a transmission properly without error, conserving in addition the means at any moment its characteristics to propagation. However the radio channel is characterized being medium of strongly hostile propagation, with very high probabilities of error, temporary variation (nonstationary channel) of *the BER* from 10^{-6} to 10^{-2}, with special circumstances by the mobility of the user and with strong problems of data signal fadings and dispersion.

By the thing previously mentioned, is necessary that the information to data transmit will be protected against errors, giving rise which it is known like channel codification. At the present time the movable systems are oriented fundamentally to the service of voice, but according to the expectations of such systems, the great necessity arises from the data transmission, giving as result one burns research, within which is the study and analysis of the systems of codification of channel oriented to the data service.

In this work of thesis is made a deep study about block codes channel codifications and as a result we proposed the optimal parameters of the codification of channel (block codes) for the CDMA system. These parameters maintain mainly a high and constant Throughput in all the margin of variation of the BER of 10^{-6} up to 10^{-2} and maintaining simplicity in the coder and decoder.

Key words: *BER*, *Throughput*, *CDMA* y Q_oS

Dedicatoria

A mis padres,

Orlando Salaices Piña

Rosalva Sotelo de Salaices

por ser unos padres ejemplares, por sus enseñanzas y brindarme su apoyo incondicional para lograr una de mis metas.

A mi hermano y hermana,

Rommel Aly Salaices Sotelo

Solymar Salaices Sotelo

por su sensibilidad y muestra de cariño y apoyo en todo momento.

A mi abuela,

Josefina Juárez viuda de Sotelo

Por darme su amor y comprensión incondicional en los momentos difíciles.

A mis tíos, tías, primos y primas, por proporcionarme todos sus afectos y confianza incondicional.

Agradecimientos

Primero que nada, doy gracias a *Dios* por permitirme alcanzar otra etapa más en mi vida.

Quiero agradecer a mi amigo y director de tesis *Dr. David H. Covarrubias Rosales*, quien me brindó todo su apoyo y confianza durante el desarrollo de este trabajo.

A los miembros del comité de tesis *M.C. Jorge E. Preciado Velasco, Dr. Pedro Negrete Regagnon y M.C. Jaime Sánchez García*, gracias por sus consejos y aportaciones que realizaron durante el desarrollo de este trabajo de investigación.

A mi compañero y amigo *Nataniel Mendoza Urías,* por el gran trabajo en equipo que desarrollamos durante este periodo de investigación.

A mis *amigos y compañeros de generación* (Telecos 1999-2000) por todas las experiencias que compartimos los dos años de estancia en el Centro de Investigación.

Al *CICESE* por brindarme la oportunidad de llevar a cabo esta etapa de superación.

Al *Consejo Nacional de Ciencia y Tecnología (CONACyT)* por el financiamiento otorgado.

Contenido

Página

Contenido (continuación) Página

Contenido (continuación)

Página

Contenido (continuación)

Página

Lista de Figuras

Página

Lista de Figuras (continuación)

Página

Lista de Tablas

Página

Codificación de canal para la transmisión de datos enfocada a los sistemas CDMA.

I Introducción.

I.1 Antecedentes.

El marco de referencia de este trabajo de investigación radica en las comunicaciones móviles celulares de tercera generación que utilizan como técnica de acceso *CDMA* de secuencia directa, de la cual se estudiará, analizará y se propondrán los parámetros óptimos (*n, k, t*) de un esquema de codificación de canal orientada a la transmisión de datos, esta clase de servicio es tolerable al retardo pero no a la pérdida de información, por lo tanto los parámetros de prestaciones que se esperan obtener estarán en función de la pérdida de información y no del retardo (*Throughput* contra el *BER* del canal).

Uno de los aspectos críticos de comunicaciones de radio móvil celular es la eficiencia de la codificación de los datos para asegurar conconfiabilidad dada la presencia de ruido y desvanecimientos. El canal móvil es caracterizado por la presencia de ruido, desvanecimientos rápidos y desvanecimientos lentos, por lo que es un medio de propagación fuertemente hostil, con probabilidades de errores muy grandes presentando variación temporal del *BER* desde 10^{-6} hasta 10^{-2} (canal no estacionario). Además de lo anterior, con circunstancias especiales por la movilidad de la terminal remota y con problemas fuertes de desvanecimientos y de dispersión.

Siendo la codificación de canal un elemento importante en las prestaciones del sistema de comunicaciones, y tomando en cuenta que no existe un codificador de canal único que satisfaga todos los requerimientos de calidad de servicio, es necesario establecer una fase de especificación del esquema de codificación. Para ello, hay que tomar en cuenta varios factores, por ejemplo las características deseadas para el sistema, en cuanto a retardo

y a *BER* o probabilidad de error del canal, las cuales varían según el tipo de servicio requerido.

La técnica de acceso múltiple por división de código (*CDMA*) es una forma de espectro ensanchado (*SS*) y una técnica avanzada de transmisión digital inalámbrica. La técnica *CDMA* en lugar de emplear frecuencia o ranuras de tiempo, como lo hacen las tecnologías tradicionales, utiliza códigos matemáticos para transmitir y distinguir entre múltiples sesiones inalámbricas. Su ancho de banda es mucho mayor que la requerida para un enlace simple punto a punto a la misma velocidad de datos [Sklar, 1998], puesto que hace uso de portadoras conocidas como "semejantes a ruido" para ensanchar la información de interés, contenida en un ancho de banda mucho mayor. Sin embargo, dado que las sesiones establecidas son distinguibles por medio de códigos digitales, múltiples usuarios pueden compartir el mismo ancho de banda.

Los métodos avanzados aplicados en la tecnología comercial *CDMA* permite una mejora sustancial en: la capacidad del sistema, área de cobertura y calidad de voz. Por estas características *CDMA* ha sido elegido como la técnica de acceso para los sistemas móviles de tercera generación.

I.2 Motivación del trabajo.

La necesidad de este trabajo surge debido a que el ancho de banda en las comunicaciones de radio móvil actuales está limitado, pero el número de usuarios y la velocidad de transmisión están constantemente en aumento. Ello condiciona el diseño del protocolo de transmisión de los datos: si el ancho de banda es limitado es necesario minimizar las retransmisiones. Por otro lado al ser la tasa de error grande es importante realizar transmisiones redundantes de los paquetes, aumentando con ello la probabilidad de recepción correcta de éstos.

Dentro del conjunto de técnicas que pueden alcanzar parcial o totalmente las condiciones anteriores, está la utilización de nuevos esquemas de codificación y decodificación de canal, que optimizan la detección y corrección de errores manteniendo una eficiencia elevada (*caudal eficaz*) y con la capacidad de adaptarse a las condiciones variantes del canal de comunicaciones.

Actualmente los sistemas de comunicación móvil están orientados al servicio de voz, pero de acuerdo a las expectativas de los futuros sistemas celulares surge la necesidad de desarrollar un estudio de análisis de prestaciones de codificación de canal orientada al servicio de datos, siendo este servicio no sensitivo al retardo pero sí lo es a la pérdida de información, como se observa en la *Figura 1*. Los sistemas actuales (*IS-54, IS-95 y GSM*) utilizan codificación de canal no orientados al servicio de datos, cuyo comportamiento sufre un fuerte decaimiento del *Throughput* en la región del *BER* de interés de 10^{-4} hasta 10^{-2}, por lo que estos sistemas se verían forzados a interrumpir la transmisión de los datos y reanudar la transmisión hasta que el *BER* del canal se encuentra en una región favorable *BER* de 10^{-6} hasta 10^{-4}, de aquí el motivo principal de este trabajo de tesis en el cual se buscará que el sistema no interrumpa la transmisión de los datos en todo el margen del *BER* de 10^{-6} hasta 10^{-2}.

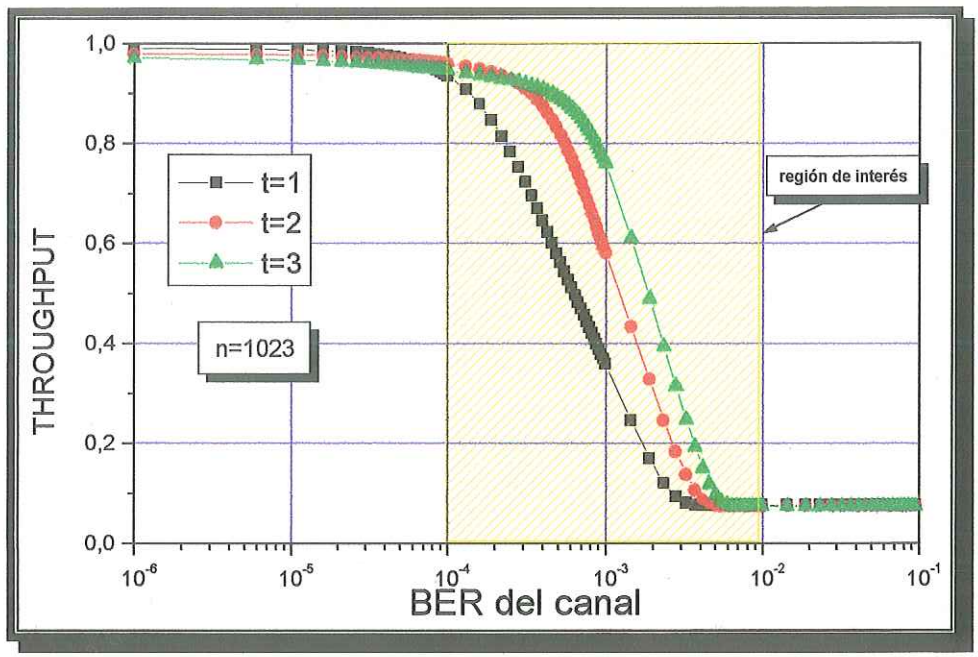

Figura 1: Respuesta obtenida del throuhput mediante un esquema de codificación no orientado al servicio de datos con t capacidad de corrección de error [*Covarrubias, 1999*].

Tomando en consideración que este trabajo de tesis junto con el de Nataniel Mendoza Urías (donde se estudian y analizan los códigos convolucionales), son las primeras investigaciones a un nivel de tesis de maestría realizadas en *CICESE*, donde se aborda el estudio y análisis de la codificación de canal bajo un entorno móvil celular para diferentes tipos de servicios (voz, datos y video), dando como resultado una originalidad de estos trabajos de investigación en *CICESE*, los cuales podrán ser utilizados como referencia para los futuros estudiantes del *CICESE*. En nuestro caso, la trascendencia del trabajo es la propuesta de los parámetros óptimos (*n, k, t*) de la codificación de canal orientada al servicio de datos aterrizado a los sistemas *CDMA*, en la cual se buscará que el *Throughput* del sistema sea lo más alto posible y que no presente la caída tan abrupta en la región del *BER* del canal de 10^{-4} hasta 10^{-2} (*Figura 1*).

I.3 Objetivo.

Por lo mencionado anteriormente el objetivo de este trabajo de tesis es proponer un esquema de codificación eficiente que permita asegurar la confiabilidad en la transmisión de paquetes, bajo la presencia de ruido y desvanecimientos en un entorno de comunicaciones móviles, el cual tiene como principal objetivo mantener un *Throughput* elevado y constante en el margen del *BER* del canal de 10^{-6} hasta 10^{-2}, con ésto se asegura que el sistema no se vea forzado a dejar de transmitir información cuando el ruido del canal empieza a aumentar.

El tipo de codificador depende del tipo de información a manejar (datos, voz, video o imagen), del canal (canal con memoria o sin memoria), las velocidades de transmisión, el retardo tolerable, la calidad o *BER* exigida, tipo de ruido (aleatorio o ráfagas) y del compromiso del decodificador (sencillez en su implementación).

I.4 Metas.

Para la realización de este trabajo se plantearon las siguientes metas:

- Estudio del estado del arte de los sistemas de comunicaciones móviles.
- Estudio de las características del canal radio, para transmisiones en exteriores (micro y pico celdas) y frecuencias de *UHF*.
- Estudio del estado del arte de las características de la interfaz radio *CDMA* con características de transmisión multi códigos.
- Estudio de la teoría de cuerpos finitos o álgebra de *Galois*.
- Estudio de la teoría de codificación de canal.
- Análisis de prestaciones de codificación de canal aplicado al entorno de canales no estacionarios.
- Simulación y validación del esquema de codificación propuesto enfocado a servicios sensitivos a la pérdida de información.

I.5 Infraestructura utilizada.

- Biblioteca *CICESE.*
- Biblioteca del Campus Ensenada, *UABC.*
- Internet.
- Computadora Personal Pentium III (procesador intel, memoria *RAM* de 128 *Mbytes*, 10 *GBytes* en disco duro).
- Lenguaje de programación *MATLAB* 5.3.0 y toolbox de comunicación y estadística.
- Paquetes de computación como Word, Excel, Powerpoint, Netscape, etc.
- Red *CICESE.*

I.6 Organización del trabajo.

A continuación se describirá de forma más detallada el contenido de cada uno de los capítulos que forman parte de este trabajo de tesis.

En el capítulo dos, caracterización del canal radio, se presenta el análisis de la problemática de la transmisión de la información en un entorno de canal radio (canal no estacionario con fuertes desvanecimientos de tipo *Rayleigh*), ya que el código corrector de error que se analizará estará pensado en trabajar en un canal radio no estacionario y fuertemente hostil, también se describen las técnicas que utilizan los sistemas actuales de comunicación para contrarrestar los efectos del canal radio.

En el capítulo tres, acceso múltiple por división de código (*CDMA*), se presentan las características más relevantes de los sistemas *CDMA*, ya que los parámetros óptimos del código corrector de error que se elijan, estarán pensados para que puedan ser utilizados en dichos sistemas, también se lleva a cabo un estudio de los estándares de primera, segunda y tercera generación, así como simulaciones del sistema de concatenación de códigos de los sistemas de tercera generación (*3G*).

En el capítulo cuatro, teoría de cuerpos finitos aplicada a la codificación de canal, se presenta un estudio de la matemática que se encuentra asociada a la codificación de canal, el cual tiene como principal objetivo reducir la complejidad de la codificación y decodificación del mensaje.

Capítulo cinco, codificación de canal, en este capítulo se estudian todos los parámetros que están relacionados a los códigos bloque, para posteriormente determinar cuales de ellos están relacionados con la eficiencia del código.

Capítulo seis, análisis de prestaciones de los códigos bloque binarios (*BCH*) y no binarios (*RS*), en este capítulo radica el peso de todo este trabajo de investigación, ya que aquí se encuentra el análisis de los resultados de las simulaciones realizadas y la recomendación de los parámetros de los códigos bloque que peden ser implementados en los sistemas *CDMA*.

Finalmente en las "conclusiones y trabajos futuros" se presentan las conclusiones que se consideran más importantes de este trabajo de tesis, así como las recomendaciones, y trabajos futuros que se pueden desarrollar a partir de este trabajo.

II Caracterización del canal radio.

II.1 Introducción.

El medio de propagación que conecta al transmisor y el receptor es llamado canal. En general, un canal de comunicación puede consistir de alambre, cable coaxial, cable de fibra óptica, y en el caso de enlaces de radio frecuencia (*RF*), guías de onda, la atmósfera o el espacio.

El estudio del canal radio será de utilidad para el desarrollo de este trabajo de tesis ya que las comunicaciones móviles utilizan como medio de transmisión el canal radio (espacio libre), donde el enlace de comunicación se da en exteriores. Por lo cual es importante tener definida la problemática que involucra la transmisión de información a través del espacio libre y con un enlace donde no existe visión directa entre el móvil y la estación base.

El canal de radio es un medio extremadamente hostil además de ser no estacionario, en el cual es difícil establecer y mantener comunicaciones fiables. Todos los esquemas y mecanismos que se implementan para hacer posible la comunicación en el canal de radio, se agrupan en los procedimientos de la interfaz de radio. En este capítulo se mencionarán los principales procesos que se llevan a cabo en la interfaz de radio.

El objetivo de este capítulo es analizar y comprender los problemas que implica transmitir en un canal no estacionario (se define como aquél en el que el *BER* del canal cambia en función del tiempo) y con fuertes desvanecimientos de tipo multitrayectorias. Así como entender las diferentes técnicas que son implementadas para minimizar los efectos del canal radio, tales como: entrelazado, igualadores de canal y diversidad, las cuales se estudiarán en este capítulo.

II.2 Canal AWGN (Additive White Gaussian Noise Channel).

El ruido blanco Gaussiano básicamente es el ruido generado en el receptor. El ruido tiene una densidad espectral de potencia constante sobre todo el ancho de banda del canal (N_o / 2), y una amplitud de función de densidad de probabilidad Gaussiana.

El ruido térmico se puede describir como un proceso aleatorio Gaussiano con media cero. Un proceso Gaussiano, *n(t)*, es una función aleatoria cuyo valor, *n*, en cualquier tiempo arbitrario, *t*, es caracterizado por la función de densidad de probabilidad Gaussiana, *p(n)* [Proakis y Salehi, 2000]:

$$P(n) = \frac{1}{\sigma\sqrt{2\pi}} e^{-1(n)^2/2\sigma^2} \qquad (1)$$

donde σ^2 es la varianza de *n*.

El canal *AWGN* puede ser descrito en términos de la entrada *x* y la salida *y* dada por: $y=x+n$

donde *n* es una variable aleatoria de ruido Gaussiano, *"y"* la entrada *"x"* puede tener cualquier valor discreto *M*. Expresando en función de la entrada:

$$P(y) = \frac{1}{\sigma\sqrt{2\pi}} e^{-1(y-x)^2/2\sigma^2} \qquad (2)$$

La principal característica espectral del ruido térmico es que su densidad espectral de potencia es la misma para todas las frecuencias de interés en los sistemas de comunicación. Por lo tanto un simple modelo se asume para el ruido térmico, ésto es, la densidad de potencia espectral $G_n(f)$ es ensanchada para todas las frecuencias y es denotada como:

$$\mathrm{Gn(f)} = \frac{N_o}{2} \text{ Watts/hertz} \qquad (3)$$

donde N_o es la densidad espectral del ruido.

El efecto en el proceso de detección de un canal *AWGN* es que el ruido afecta cada símbolo transmitido independientemente, tal canal es llamado un canal sin memoria. De aquí que el ruido térmico está presente en todos los sistemas de comunicación y es la fuente de ruido más prominente para los sistemas de comunicación, las características del ruido térmico o ruido blanco Gaussiano aditivo es más a menudo usado para modelar el ruido en sistemas de comunicación, ya que es el canal más simple de modelar.

II.3 Canal simétrico binario (BSC).

En el canal simétrico binario los bits de salida dependen únicamente de los correspondientes bits de entrada, por lo que el canal es un canal sin memoria. En un canal simétrico binario la probabilidad de transmitir un cero lógico es igual a la probabilidad de transmitir un uno lógico.

Suponiendo que *"x"* son los bits transmitidos, *"y"* los bits recibidos. Sea p la probabilidad de recibir un bit con error y $p-1$ la de recibirlo correctamente, lo cual se puede escribir como.

$$p(y=1|x=0)=p(y=0|x=1)=p \qquad (4)$$

$$p(y=0|x=0)=p(y=1|x=1)=1-p$$

Un canal simétrico binario es representado en la ***Figura 2***.

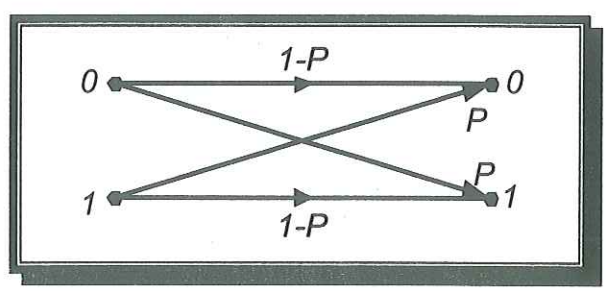

Figura 2: Modelo de canal simétrico binario.

II.4 Propagación en el canal radio.

A diferencia de los canales de comunicación cableados que son estacionarios y predecibles, el canal radio es extremadamente hostil, variante en el tiempo, aleatorio y por lo tanto dá como resultado un complejo canal de propagación multitrayectoria de difícil análisis.

Una señal de radio móvil *r(t)* es caracterizada artificialmente por dos componentes *m(t)* y *r(t)* basada en fenómenos físicos [Lee, 1995], tal como se observa en la *Figura 3*.

$$r(t) = m(t)r(t) \qquad (5)$$

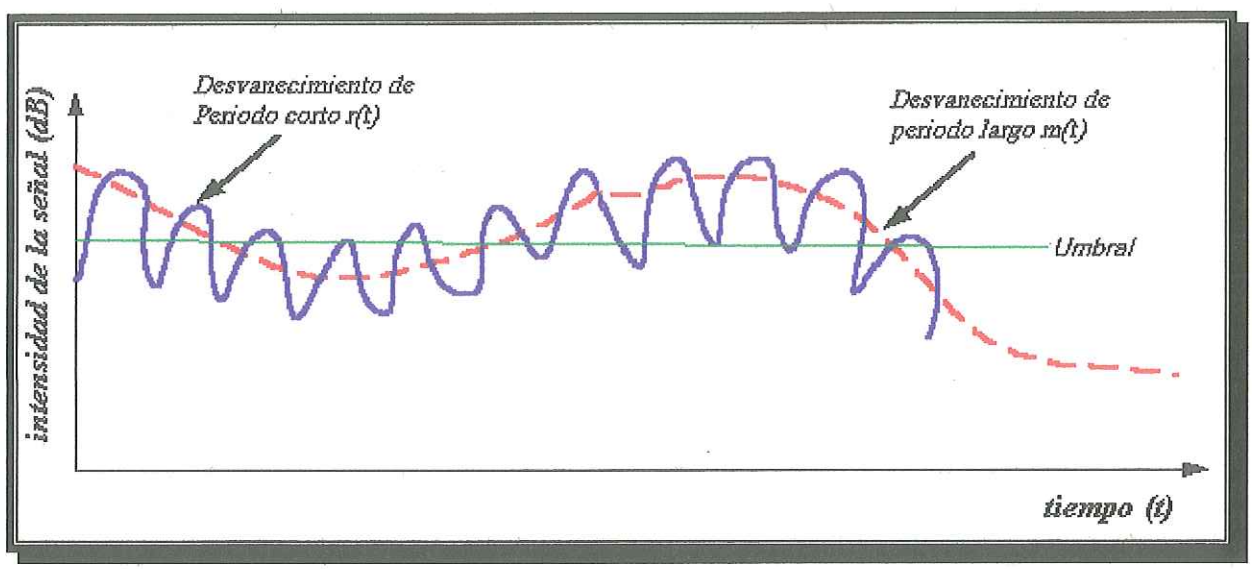

Figura 3: Características de desvanecimiento de una señal radio.

El componente *m(t)* es llamado desvanecimiento de periodo largo o desvanecimiento *log-normal*, esta variación se debe al contorno del terreno entre la estación base y el móvil. El factor *r(t)* es denotado como desvanecimiento multitrayectoria, desvanecimiento de periodo corto o desvanecimiento *Rayleigh*, esta variación es causada por las reflexiones de onda ocasionada por edificios u otras estructuras [Lee, 1995].

La propagación de las ondas electromagnéticas en el canal radio son generalmente atribuídas a tres fenómenos los cuales son [Gibson, 1996]:

- Reflexión.
- Difración.
- Dispersión.

Estos fenómenos se presentan ya que los sistemas de comunicación móvil operan en áreas urbanas donde no existe un camino de visión directa entre el transmisor y el receptor, y donde la presencia de obstáculos altos causan severas pérdidas. Estos mecanismos dan origen a desvanecimientos (*Multipath Fading*) y distorsiones en las señales de *RF*, lo que a su vez se traduce en una reducción de la relación señal a ruido *SNR* en el receptor y un aumento en la tasa de errores *BER*, ya que una señal desvanecida dificulta la tarea del discriminador en el demodulador. A los canales móviles se les conoce como "canales dinámicos o variantes" debido a estas tendencias de variabilidad.

Reflexión: Ocurren cuando la señal de Radio Frecuencia (*RF*) es reflejada sobre una superficie de mayor longitud a su longitud de onda. Por ejemplo la superficie terrestre, paredes y edificios. La cantidad de energía reflejada depende de la naturaleza dieléctrica de la superficie incidente.

Difración: Ocurre cuando la señal de *RF* se flexiona o "dobla" para vencer obstáculos entre el transmisor y el receptor. A través de este efecto es posible que las señales de *RF* viajen sobre la superficie curva de la Tierra.

Dispersión: Ocurre cuando la señal de *RF* incide sobre superficies de tamaño menor que la longitud de onda de la señal. Por ejemplo postes de luz, follaje y anuncios de tránsito.

II.4.1 Propagación en el espacio libre.

El modelado de propagación en el espacio libre es usado para predecir la energía de la señal recibida cuando el transmisor y el receptor están en visión directa. La potencia recibida en el espacio libre por una antena receptora la cuál está separada de una antena transmisora por una distancia *d,* esta dada por [Parson, 1992]:

$$\frac{P_R}{P_T} = \left(\frac{\lambda}{4\pi d}\right)^2 G_T G_R \qquad (6)$$

donde:

P_R Potencia recibida.

P_T Potencia transmitida.

λ Longitud de onda.

d Distancia entre el receptor y el transmisor (metros).

G_T y G_R Ganancia de la antena transmisora y receptora respectivamente.

II.5 Efecto de la movilidad.

Los efectos de la movilidad son principalmente tres:

- Pérdida por propagación de camino.
- Efecto de sombra (*shadowing*).
- Propagación por multitrayectoria.

II.5.1 Pérdida por propagación de camino.

La pérdida por propagación de camino depende de la distancia entre el receptor y el transmisor. Esta pérdida es aleatoria ya que depende de la posición del móvil. Como todos los sistemas son diseñados para ofrecer la misma calidad de servicio independientemente de la distancia entre el móvil y la estación base, éstos requieren de un control de potencia para mantener la calidad del servicio. Por lo que estos tipos de desvanecimientos son

contrarestados por medio del control de potencia. La pérdida de camino en el espacio libre está dada por [Rappaport, 1996]:

$$PL(dB) = -10\log\left[\frac{G_T G_R \lambda^2}{(4\pi d)^2}\right] \qquad (7)$$

II.5.2 Efecto de sombra (Shadowing).

Este tipo de desvanecimiento es lento, en el sentido de que cambia poco bajo regiones bastante grandes. El *shadowing* se dá por que el camino es bloqueado por objetos más grande que el móvil (montañas, edificios, etc.). El *shadowing* y la pérdida de camino, son vistas como una fluctuación lenta de la potencia de la señal cuando el móvil se desplaza, por lo que son desvanecimientos lentos (*log-normal*) o desvanecimientos de periodo largo (*long-term*) y son virtualmente invariantes en la frecuencia.

II.5.3 Propagación multitrayectoria.

La propagación multitrayectoria causa rápidas fluctuaciones en la potencia de la señal recibida cuando el móvil se desplaza. Incluso bajo distancias muy cortas. Por este motivo a la propagación multitrayectoria se le conoce como desvanecimiento rápido (*Rayleigh fading, Rician fading o Nakagami-m*) o desvanecimiento de periodo corto (*short-term*). La propagación multitrayectoria causa principalmente tres fenómenos [Rappaport, 1996]:

- Cambios rápidos en la energía de la señal bajo un corto intervalo de tiempo o cortas distancia de recorrido de la señal.
- Dispersión de tiempo causados por retardos de propagación multitrayectoria.
- Desplazamiento *Doppler* debido a la movilidad del usuario.

Para analizar la naturaleza dispersiva y variante del canal radio basta transmitir un pulso muy estrecho sobre un canal radio móvil, idealmente un impulso. La respuesta al impulso del canal radio móvil es un tren de un cierto número de pulsos con un retardo

respecto al primero y una atenuación diferente para cada uno de ellos tal como se muestra en la ***Figura 4***, por lo que la primera característica del canal radio es la dispersión temporal del canal radio.

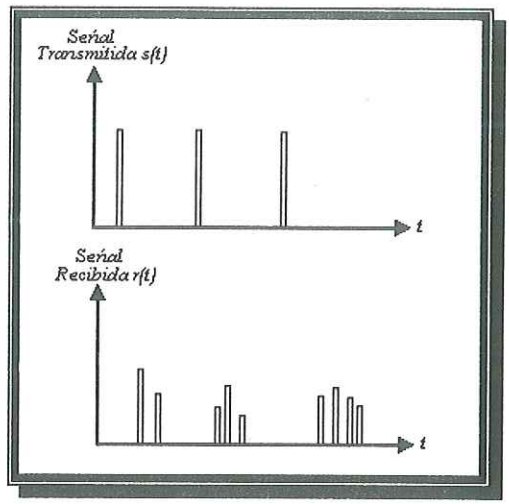

Figura 4: Respuesta al impulso del canal radio.

En la ***Figura 4*** se observa como los retardos relativos de la señal recibida y las atenuaciones de los pulsos así como el número de ellos son diferentes en cada transmisión, dando como resultado la segunda característica del canal radio, la variabilidad [Proakis, 1989].

La respuesta al impulso del canal contiene toda la información necesaria para analizar cualquier tipo de transmisión de radio a través del canal y está en función del tiempo t y del retardo τ, por lo que esta respuesta es usada para predecir y comparar la eficiencia de los sistemas de comunicación móvil. Esto proviene del hecho de que un canal radio móvil puede ser modelado como un filtro lineal con una respuesta al impulso de tiempo variante, donde la variación del tiempo se debe al movimiento del receptor [Rappaport, 1996]. En un sistema digital, la propagación multitrayectoria causa interferencias entre símbolos, lo que obliga el uso de técnicas de transmisión capaces de

combatir la interferencia entre símbolos como lo son los igualadores de canal. La respuesta al impulso de un canal radio móvil variante con el tiempo viene dada por [Proakis, 1989]:

$$h(t;\tau) = \sum_{i=1}^{N} \alpha_i(t) e^{(-j2\pi f_o \tau_i(t))} \delta(\tau - \tau_i(t)) \qquad (8)$$

donde:

$\alpha_i(t)$ Factor de atenuación para la señal recibida.

$\tau_i(t)$ Retardo de propagación.

$2\pi f_o \tau_i(t)$ Representa el desplazamiento de fase debido a la propagación en el espacio libre.

N Número posible de componentes de multitrayectoria.

$\delta(\bullet)$ Función de impulso unitario.

II.5.3.1 Dispersión temporal del canal radio.

Ya que la respuesta al impulso es variante y un proceso aleatorio en *(t)*, su comportamiento estadístico no es estacionario, pero puede llegar a considerarse estacionario en pequeños intervalos de tiempo o cortos intervalos de distancias. En este caso, la función de autocorrelación de $h(t;\tau)$ viene definido por [Proakis, 1989]:

$$R_h(\tau_1, \tau_2; \Delta t) = \frac{1}{2} E\left[h^*(\tau_1; t) h(\tau_2; t + \Delta t)\right] \qquad (9)$$

Como la atenuación y desplazamiento de la fase del canal asociado con el retardo de camino τ_1 es no-correlacionado (*uncorrelated*) con la atenuación y desplazamiento de fase asociado con el camino τ_2, por lo que la atenuación y fase de los distintos caminos son diferentes entre sí. Haciendo esta segunda suposición: propiedad que se conoce como *uncorrelated scattering*. Esta suposición junto con la anterior, se les conoce como suposición *WSSUS* (*Wide Sense Stationary Uncorrelated Scattering*). Aplicando esta suposición en la ecuación 9 se obtiene [Proakis, 1989]:

$$R_h(\tau_1, \tau_2; \Delta t) = R_h(\tau_1; \Delta t) \delta(\tau_1 - \tau_2) \qquad (10)$$

II.5.3.1.1 Power delay profile.

El *power delay profile* representa la potencia media de salida del canal en función del retardo τ. Retomando la ecuación 8 y haciendo Δt=0 se obtiene el *power delay profile,* que está definido por [Rappaport, 1996]:

$$P(\tau) = R_h(\tau;0) = E\left[[h(t;\tau)]^2\right] \qquad (11)$$

II.5.3.1.2 Time delay spread.

El efecto de *time delay spread,* puede ser contemplado como un efecto de desvanecimiento selectivo en frecuencia (*frequency-selective fading*). Es el margen de valores de retardo en el que *power delay profile* es esencialmente no nulo. Este parámetro caracteriza la dispersión temporal del canal y se define como la raíz cuadrada del momento central de segundo orden del *power delay profile* del canal:

$$\tau_d = \left[\frac{\int_0^\infty (\tau - m)^2 p(\tau) d\tau}{\int_0^\infty p(\tau) d\tau}\right]^{1/2} \qquad (12)$$

donde m representa el retardo medio de propagación y se denomina *average mean delay.*

$$m = \frac{\int_0^\infty \tau p(\tau) d\tau}{\int_0^\infty p(\tau) d\tau} \qquad (13)$$

El *time delay spread* causa distorsión en la forma de onda de la señal detectada e impone un límite en la eficiencia de probabilidad de error de los sistemas de transmisión de alta velocidad [Feher, 1987].

II.5.3.1.3 Ancho de banda de coherencia (coherence bandwidth).

Mientras que el *delay spread* es un fenómeno causado por reflexiones y propagación multitrayectoria en el canal radio, el ancho de banda de coherencia, B_c, está relacionado con el *rms delay spread*. El ancho de banda de coherencia es un cálculo estadístico que mide la dispersión mínima entre dos frecuencias que pueden considerarse afectadas de manera diferente por el canal. El ancho de banda de coherencia vienen dado por:

$$B_c = 1/\tau_d \qquad (14)$$

II.5.3.1.4 Efecto de desvanecimiento debido a MDS (multipath delay spread).

Los dos efectos que provocan el *delay spread* son:

- Desvanecimiento no selectivo en frecuencia (Flat fading).
- Desvanecimiento selectivo en frecuencia.

II.5.3.1.4.1 Desvanecimiento no selectivo en frecuencia (Flat fading).

Si el canal radio móvil tiene un ancho de banda de coherencia mucho más grande que el ancho de banda de la señal transmitida ($B_{c>>}B_s$), entonces la señal recibida experimenta este tipo de desvanecimiento. Este tipo de desvanecimiento es el más común. Este canal también es conocido como un canal variante en amplitud o canal de banda estrecha, con lo que los componentes frecuenciales de la señal a transmitir se verán afectados de la misma forma por el canal móvil (baja dispersivilidad en el canal).

La distribución de la ganancia instantánea de este tipo de desvanecimiento es importante para diseño de enlace de radio, y la distribución de amplitud más común es la distribución *Rayleigh*. El modelo de canal con desvanecimientos tipo *Rayleigh* asume que el canal induce una amplitud la cual varia en tiempo acorde a la distribución de *Rayleigh*.

II.5.3.1.4.2 Desvanecimiento selectivo en frecuencia.

Si el canal radio móvil tiene un ancho de banda de coherencia más pequeño que el ancho de banda de la señal transmitida ($B_c<B_s$), cuando ésto ocurre, la señal recibida tiene múltiples versiones de la forma de onda transmitida, la cual es atenuada y retardada en tiempo, por lo que la señal recibida es distorsionada. El desvanecimiento selectivo en frecuencia se debe a la dispersión de tiempo del símbolo transmitido en el canal. Por lo que este tipo de canal induce interferencia entre símbolos (*ISI*). El canal de desvanecimiento selectivo en frecuencia también es conocido como canal de banda ancha. Este tipo de canal es más difícil de modelar, por lo que cada señal de multitrayectoria debe ser modelado.

II.5.3.2 Ensanchado Doppler (Doppler Spread).

Debido al movimiento relativo entre el móvil y la estación base, cada onda de multitrayectoria experimenta un desplazamiento en frecuencia. El desplazamiento en la frecuencia de la señal recibida debido al movimiento es llamado el desplazamiento *Doppler*, y es directamente proporcional a la velocidad y dirección del movimiento del móvil con respecto a la dirección de llegada de la onda de multitrayectoria recibida.

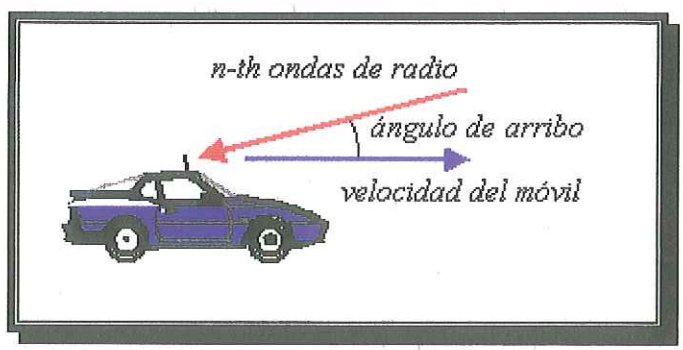

Figura 5: Movimiento del móvil.

El desplazamiento Doppler de onda de la figura anterior viene dado por:

$$\Delta f_n = \frac{v_{eff}}{\lambda}\cos\alpha_n \qquad (15)$$

donde v_{eff} velocidad efectiva del móvil.

El máximo desplazamiento Doppler ocurre cuando la onda viene en dirección opuesta al móvil y está dada por [Parson, 1992]:

$$f_d = \frac{v_{eff} f_c}{c} \qquad (16)$$

donde:

v_{eff} Velocidad efectiva del móvil.

f_c Frecuencia portadora

c Velocidad de la luz ($3x10^8$ m/seg).

El *ensanchado Doppler* (B_D) mide la intensidad de la señal en función del desplazamiento *Doppler*, por lo que $B_D=f_d$.

II.5.3.2.1 Tiempo de coherencia (coherence time).

Es implementado para caracterizar la variación del tiempo de la dispersión de frecuencia del canal en el dominio del tiempo y es inversamente proporcional al *ensanchado Doppler*.

$$T_c = 1/B_D \qquad (17)$$

II.5.3.2.2 Efecto de desvanecimiento debido a Doppler Spread.

Los dos desvanecimientos provocados por el *Doppler spread* son:

- Desvanecimientos rápidos (*fast fading*).
- Desvanecimientos lentos (*slow fading*).

II.5.3.2.2.1 Desvanecimientos rápidos.

Si el ancho de banda de la señal es menor que el ancho de banda *Doppler* ($B_s<B_D$), entonces el canal será clasificado como un canal de desvanecimiento rápido. Este tipo de canal causa la dispersión de frecuencia (también llamado desvanecimiento selectivo en

tiempo) debido al *ensanchamiento Doppler*. El desvanecimiento rápido está relacionado con la relación de cambio del canal debido al movimiento.

II.5.3.2.2.2 Desvanecimientos lentos.

Si el *ensanchado Doppler* del canal es mucho menor que el ancho de banda de la señal ($B_D << B_s$), entonces el canal es del tipo de desvanecimiento lento. Un aspecto muy importante que se tiene que tomar en cuenta es que los desvanecimientos rápidos y lentos están relacionados con la razón de cambio en el canal y la señal transmitida no con los modelos de pérdidas por propagación de camino [Rappaport, 1996].

II.5.3.3 Estadística de la amplitud.

Se ha comprobado que si el móvil se encuentra en movimiento, la estadística que más se ajusta las fluctuaciones de la señal es de tipo *Rayleigh* tanto en entornos interiores como en exteriores. Para en caso en el que el móvil y la estación base se encuentran en reposo, la estadística que más se ajusta es de tipo *Rician*.

II.5.3.3.1 Distribución de desvanecimiento Rayleigh.

En un canal radio móvil, la distribución *Rayleigh* se utiliza para describir la estadística de la variación del tiempo de una señal recibida de un canal de banda estrecha. La función de densidad de probabilidad (*pdf*) de la distribución *Rayleigh* viene dada por:

$$p(r) = \begin{cases} \dfrac{r}{\sigma^2} e^{\left(-\frac{r^2}{2\sigma^2}\right)} & \text{Para } (0 \le r \le \infty) \\ 0 & \text{Para } (r < 0) \end{cases} \qquad (18)$$

donde:

- σ Valor rms del voltaje recibido.
- σ^2 Potencia promedio de tiempo de la señal recibida.

La probabilidad de que la señal recibida no exceda un valor específico R está dado por la función de densidad acumulativa (*cdf*).

$$p(R) = pr(r \le R) = \int_0^R p(r)dr = 1 - \exp\left(-\frac{R^2}{2\sigma^2}\right) \qquad (19)$$

El valor medio r_{mean} de la distribución de Rayleigh está dada por:

$$r_{mean} = E[r] = \int_0^\infty rp(r)dr = \sigma\sqrt{\frac{\pi}{2}} = 1.2533\sigma \qquad (20)$$

y la varianza de ésta está dada por σ_r^2, la cual representa la potencia de la señal.

$$\sigma_r^2 = E[r^2] - E^2[r] = \int_0^\infty r^2 p(r)dr - \frac{\sigma^2\pi}{2} = \sigma^2\left(2 - \frac{\pi}{2}\right) = 0.4292\sigma^2 \qquad (21)$$

El valor medio de r es

$$r_{medio} = 1.177\sigma \qquad (22)$$

II.5.3.3.2 Distribución de desvanecimiento Rician.

Cuando existe una componente de señal estacionaria presente, tal como un camino de propagación de visión directa (*line-of-sight*) se implementa una distribución tipo *Rician*, la cual está dada por:

$$p(r) = \begin{cases} \frac{r}{\sigma^2} e^{-\frac{(r^2+A^2)}{2\sigma^2}} I_0\left(\frac{Ar}{\sigma^2}\right) & \text{para } (A \ge 0, r \ge 0) \\ 0 & \text{Para } (r < 0) \end{cases} \qquad (23)$$

donde:

A Denota el pico de amplitud para la señal dominante.

$I_0(\bullet)$ Es la función de *Bessel* modificada de primera clase y orden cero.

La distribución *Rician* a menudo es descrita en términos del parámetro K el cual es definido como la relación entre la potencia de la señal y la varianza de multitrayectoria, y está dada por:

$$K = A^2/2\sigma^2 \quad \text{y en términos de dB} \qquad K(dB) = 10\log\frac{A^2}{2\sigma^2}dB \qquad (24)$$

II.6 Diversidad.

La diversidad es una poderosa técnica de recepción de comunicación que proporciona mejoras en los enlaces inalámbricos con un costo relativamente bajo. La diversidad explota la naturaleza aleatoria de la propagación de radio. El concepto de diversidad puede ser expresado de una forma sencilla: Si una señal de radio sigue un camino determinada, y alguna otra señal sigue otro camino puede proporcionar una señal con mejor relación señal a ruido. Por lo que existe una trayectoria con mayor señal a ruido a escoger.

Las técnicas de diversidad más conocidas son:

- Diversidad espacial.
- Diversidad de polarización.
- Diversidad de frecuencia.
- Diversidad en tiempo.

Los sistema *CDMA* utilizan un receptor *Rake* para introducir mejoras en el enlace gracias a la diversidad en tiempo. Un receptor *Rake* implementa la técnica de diversidad en tiempo.

II.6.1 Receptor Rake.

Las múltiples trayectorias introducen desvanecimientos indeseados en el canal lo que se traduce un incremento de la *BER*, así como un decremento en la relación señal a ruido de la señal recibida. El receptor *Rake* es esencialmente un receptor de diversidad en tiempo diseñado específicamente para *CDMA*, donde la diversidad es proporcionada por el

hecho de que las componentes multitrayectoria son prácticamente incorreladas una de otra cuando su retardo de propagación relativo exceden un chip de periodo.

Un receptor *Rake* utiliza correladores múltiples para detectar separadamente las M componentes de multitrayectorias con mayor potencia. Las salidas de cada correlador, son ponderadas para proveer una mejor estimación de la señal transmitida, que la que se obtendría procesando una sola trayectoria.

II.6.2 Entrelazado (interleaving).

El entrelazado es utilizado para obtener diversidad en tiempo en un sistema de comunicación digital. El entrelazado ha sido una técnica muy empleada por los sistemas de segunda generación de sistemas celulares. El entrelazado permite aleatorizar los errores tipo a ráfaga y por lo tanto nulificar la memoria de un canal. Con lo que es posible aplicar la mayor parte de la teoría de canal sin memoria, lo cual simplifica el análisis. El entrelazado es utilizado en conjunto con los códigos correctores de error (*FEC*) para mejorar la eficiencia de la corrección de errores. El entrelazado es colocado entre el codificador y el modulador y el desentrelazado es colocado entre el demodulador y el decodificador, tal como se ilustra en la ***Figura 6***.

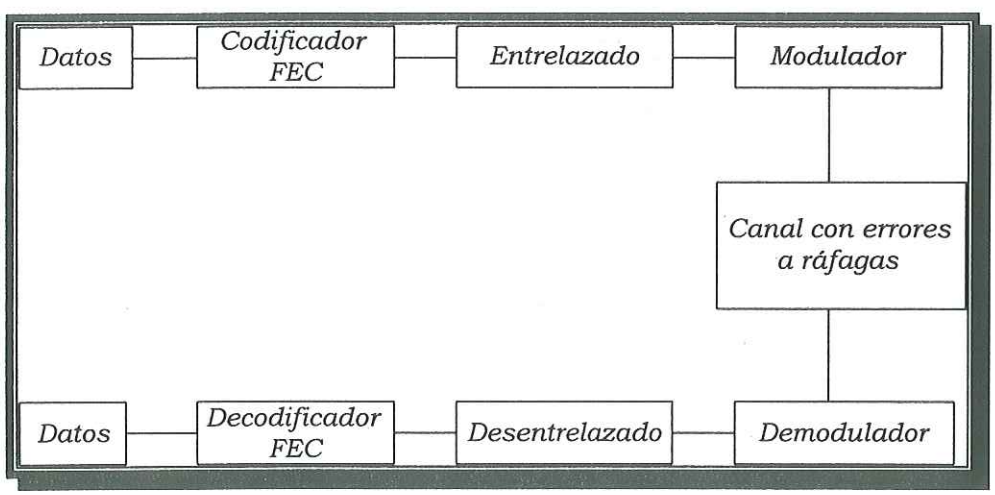

Figura 6: Sistema de comunicación típico con código FEC y entrelazado.

El entrelazado es un proceso de reasignar el orden de una secuencia de bits o de símbolos de una manera determinística. El proceso inverso a este proceso es el desentrelazado (*deinterleaving*) el cual tiene la función de ordenar la secuencias de bits a su orden original. Las técnicas de entrelazado más implementados son [Steele, 1992]:

- Entrelazado diagonal.
- Entrelazado a bloques.
- Entrelazado convolucional.
- Entrelazado inter-bloque.

II.7 Conclusiones.

Como se ha venido mencionando, el canal radio es un canal no estacionario con variaciones del *BER* de 10^{-6} hasta 10^{-2}, por lo que para el desarrollo de esta tesis resulta importante el estudio de canal radio, ya que con ello se tiene una mejor comprensión de la transmisión de la información en el espacio libre, así como los problemas que implica transmitir información en este tipo de canal. Todo lo anterior establece las bases para el desarrollo de esta tesis.

III Acceso múltiple por división de código (CDMA).

III.1 Introducción.

La mayoría de los estudios y desarrollos de sistemas de comunicación digital, se han realizado tratando de emplear el ancho de banda del canal de comunicación disponible en forma óptima y con la menor potencia posible, teniendo en consideración la existencia de calidad para un determinado servicio. Sin embargo otras consideraciones de calidad de comunicación como la inmunidad frente a interferencias o confidencialidad de las comunicaciones han sido menos consideradas. En la actualidad estos dos últimos aspectos han cobrado mucha importancia, los cuales pueden ser alcanzados por medio de la técnica conocida como modulación de espectro ensanchado (*Spread Spectrum Modulation*), por lo que esta técnica aprovecha una capacidad mucho más elevada que las técnicas de acceso múltiples conocidas [Viterbi, 1998].

La base de la tecnología de espectro ensanchado es expresada por la ecuación de Shannon, la cual muestra la relación entre la utilidad de un canal para transmitir información libre de error comparado con la relación señal a ruido existente en el canal, y el ancho de banda usado para transmitir la información [Dixon, 1994].

CDMA provee una eficiencia espectral superior para los servicios de segunda generación, teléfonos inalámbricos y sistemas de comunicaciones personales (*PCS*), minimiza el número de estaciones base requeridas para un excelente grado de cobertura de servicio.

Las principales características de esta técnica son las siguientes:

- La modulación de espectro ensanchado ocupa un ancho de banda mucho mayor que el mínimo requerido para que los datos sean transmitidos.

- El ensanchamiento de la señal transmitida se consigue con la suma binaria de ésta con otra señal pseudo aleatoria que es independiente de la señal a transmitir.
- La recepción se realiza mediante el proceso de desensanchado, el cual consiste en la suma binaria de la señal recibida con una señal local que es la réplica de la señal empleada en la transmisión.

Las ventajas más importantes de los sistemas de modulación de espectro ensanchado son:

- Baja probabilidad de ser interceptadas debido a que el ensanchamiento del espectro hace difícil la captación de las señales transmitidas por parte de un receptor ajeno a la comunicación.
- Alta inmunidad frente a interferencias intencionadas.
- Alta inmunidad frente a interferencias de señales de múltiples caminos.
- Permite implementar múltiples usuarios en un canal común para la transmisión de la información.
- Todo el ancho de banda es ocupado por cada estación base.
- Privacidad en la comunicación.

En la ***Figura*** *7* se pueden observar las últimas dos ventajas mencionadas anteriormente.

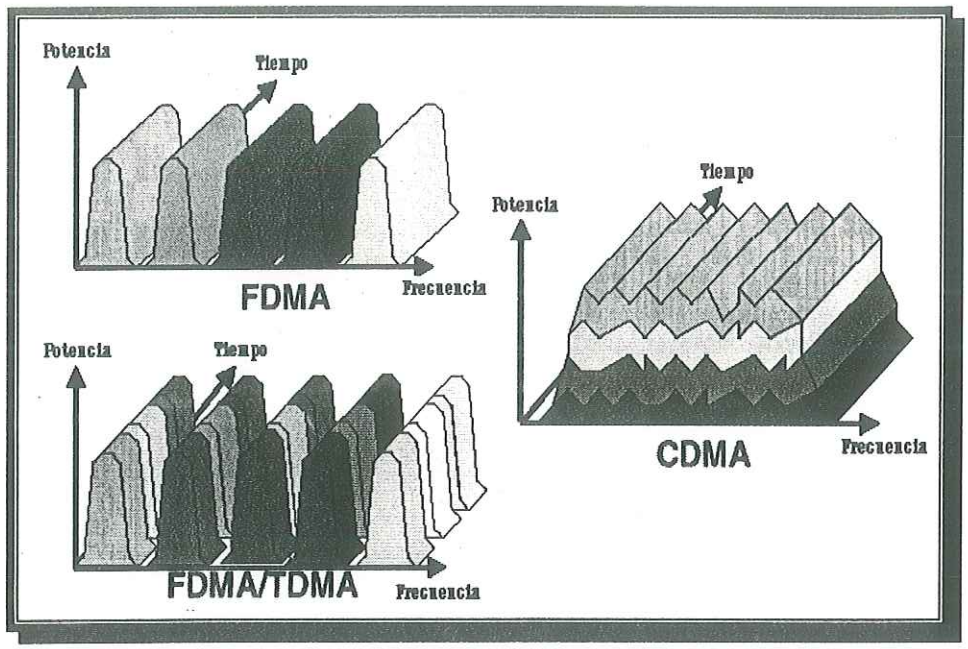

Figura 7: Comparación de los espectros de los sistemas de acceso.

Ya que los parámetros óptimos del código bloque a seleccionar podrá ser utilizado por los sistemas CDMA es importante que esta técnica de acceso sea bien comprendida, tales como sus características espectrales, secuencias ensanchadoras y esquemas de modulación asociados.

III.1.1 Estándares de primera generación.

Los estándares de primera generación fueron diseñados para proveer una cobertura local y nacional. Se caracterizan por ofrecer servicios analógicos de voz, donde el esquema de acceso utilizado es *FDMA* (*Acceso Múltiple por División de Frecuencia*).

El estándar *NTT* japonés fue el primero en operar un sistema celular en el mundo en el año 1979. A finales de 1983 comienza a operar el estándar *AMPS* Norteamericano y su contra parte europea *ETACS* aparece en 1985.

III.1.2 Estándares de segunda generación.

Debido al incremento en la demanda de servicios se introdujeron nuevas capacidades, donde una de ellas es la cobertura entre países. Los estándares de segunda generación se caracterizan por ofrecer servicios digitales de voz y cuentan con capacidad para la transferencia de datos a baja velocidad. Los esquemas de acceso utilizados son *TDMA* (*Acceso Múltiple por División de Tiempo*) y *CDMA* (*Acceso Múltiple por División de Código*).

El estándar europeo *GSM* aparece en 1990 y su contraparte norteamericana *USDC* comienza a operar en 1991; ambos utilizan *TDMA*. *IS-95* se introduce en 1993 como un estándar de telefonía celular digital basado en *CDMA*.

III.1.3 Situación actual de las CM.

Actualmente las comunicaciones móviles ofrecen servicios de telefonía celular digital y analógica, paging (beepers), transferencia de datos, entre otros. Los estándares implementados varían de acuerdo al país, ya sean de primera o segunda generación y es posible que ambos estándares coexistan.

III.1.4 Tendencias y estándares de las CM hacia servicios de Tercera Generación 3G.

A los servicios de tercera generación también se les conoce como *UMTS/IMT-2000* y serán capaces de soportar de manera simultanea múltiples servicios como transmisiones multimedia, transferencia de datos a alta velocidad y voz digital (p.e. navegar por Internet a través de una terminal móvil). La disponibilidad de estos servicios se dará en cualquier momento y en cualquier parte del mundo.

Para ofrecer estos servicios se requieren mayores anchos de banda como el ofrecido por el estándar de *CDMA* de banda ancha (*W-CDMA*). En términos generales *CDMA* ofrece ciertas ventajas sobre *FDMA* y *TDMA* algunas de las cuales son:

1. Traspaso suave (Hand-off).
2. Mejor administración de la potencia.
3. Mayor tolerancia a las interferencias.
4. Mayor rendimiento del ancho de banda.

El estándar de *CDMA* de banda ancha difiere del utilizado por *IS-95* básicamente en la capacidad de ancho de banda, en la tasa de chip de los códigos y en la naturaleza multi-códigos de las secuencias ensanchadoras que le permite dar soporte simultáneo a servicios diferentes. La Tabla I muestra estos servicios y sus requerimientos.

Tabla I: Clases de servicios y sus requerimientos.

	Clase I		Clase II-A	Clase II-B
Ejemplos	voz	vídeo	conexión remota	correo electrónico
Retardo	acotado		sensitivo	tolerable
Velocidad	garantizada		no garantizada	
	0-8 kbps	0-64 kbps	8-128 kbps	
BER	$\leq 10^{-3}$	$\leq 10^{-5}$	$\leq 10^{-7}$	

A pesar de las ventajas que ofrecen los sistemas *CDMA* de banda ancha, no es posible implementar un único estándar de tercera generación que no contemple otros esquemas de acceso como *TDMA* ya que hay muchos intereses económicos y políticos de por medio. La tendencia será flexibilizar los estándares para que puedan coexistir y generar sistemas híbridos.

III.2 Elementos básicos de un sistema de comunicación digital de espectro ensanchado.

En la ***Figura 8*** se muestran los componentes de un sistema básicos de comunicación de espectro ensanchado. La codificación de canal, decodificación de canal, modulación y demodulación son elementos esenciales del sistema. El generador pseudo aleatorio genera secuencias de señales pseudo aleatorias, la cual es multiplicada por la señal de información en el modulador y removida del receptor en la señal recibida. Como se mencionó en el capítulo anterior, cuando los errores en el sistema son del tipo ráfagas es necesario una etapa de entrelazado, con lo cual se logra una dispersión de los errores consecutivos.

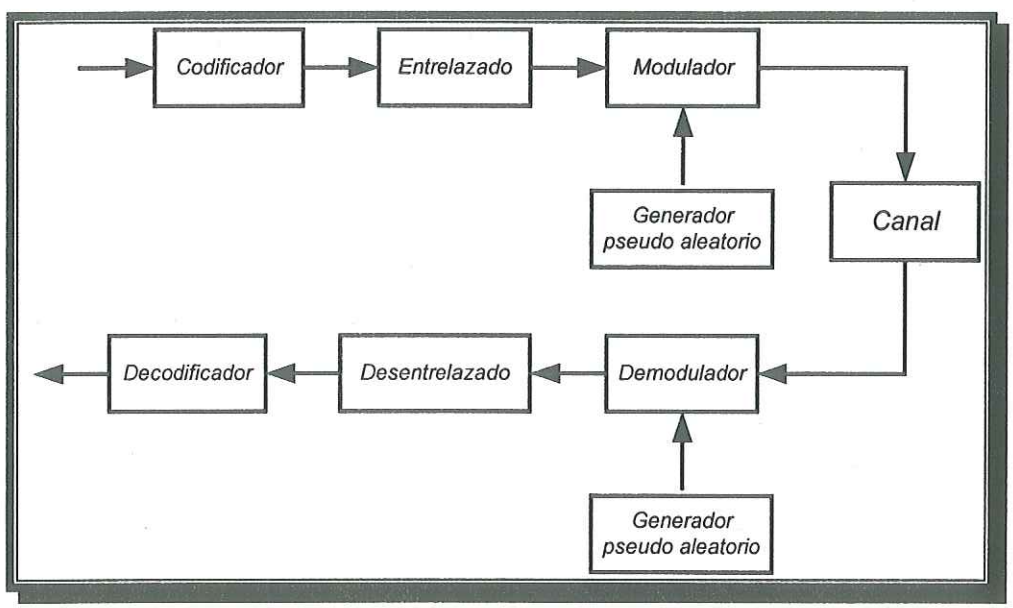

Figura 8: Modelo de un sistema básico de espectro ensanchado.

III.3 Técnicas de espectro ensanchado.

CDMA es implementado en sistemas de espectro ensanchado. Esta es una técnica de transmisión en la cual el espectro de frecuencia de una señal de datos es ensanchada usando

un código, el cual es multiplicado con la señal. Como el código implementado es seleccionado para tener un bajo valor de correlación cruzada, es posible hacer una distinción entre las diferentes señales.

La capacidad de un sistema *CDMA* está limitada por las interferencias, mientras que en los sistemas *FDMA* y *TDMA* el ancho de banda es el que se encuentra limitado. Por lo tanto cualquier reducción en la interferencia causará un incremento lineal en la capacidad de *CDMA* [Rappaport, 1996].

Las técnicas de espectro ensanchado existentes son: secuencia directa (*Direct Sequence DS*), salto en frecuencia (*Frequency Hopping FH*) y salto en el tiempo (*Time Hopping*). Es posible implementar combinaciones de estas técnicas [Dixon, 1994]. De ellas la que tiene especial interés en este trabajo es la de secuencia directa, ya que mediante esta técnica es posible compensar los efectos dispersivos del canal radio. La *Figura 9* muestra la clasificación de CDMA.

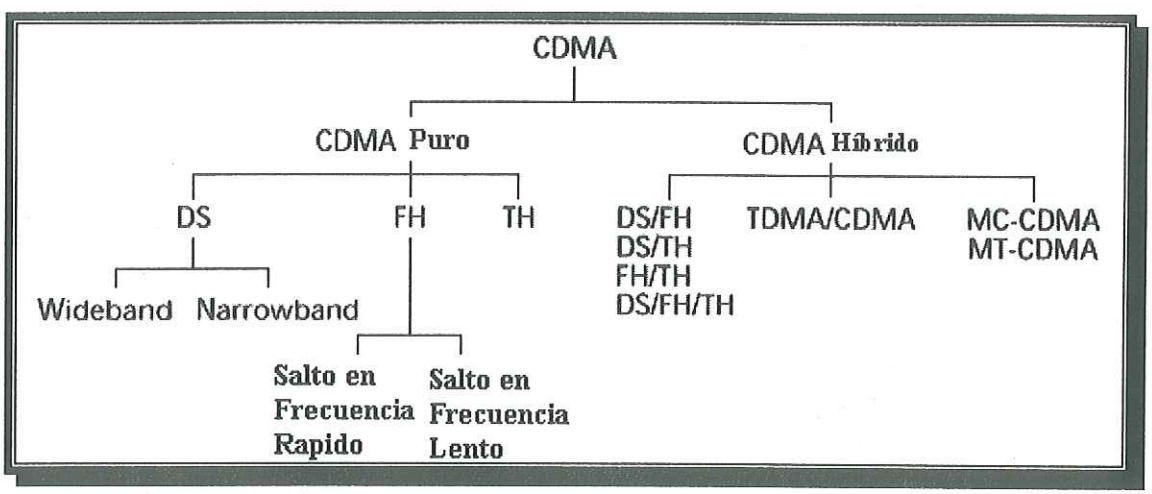

Figura 9: Clasificación de CDMA.

III.3.1 Secuencia directa (Direct Sequence DS).

La secuencia directa (modulación de secuencia de código) es la técnica de espectro ensanchado más popular. En esta modulación la fase de una señal portadora es variada de acuerdo a una señal pseudo aleatoria resultado de la multiplicación de la señal de datos a transmitir con una señal denominada código *PN*. En el receptor toda señal que entra es multiplicada por un código *PN* produciendo un ensanchamiento con lo que se consigue reducir el efecto de las señales interferentes, cuya influencia quedaría disminuida en un factor que es proporcional a la longitud de la señal de código empleada para ensanchar la señal, en cambio la señal ensanchada proveniente del transmisor quedará desensanchada por el efecto de doble multiplicación del mismo código. Este tipo de modulación es usualmente implementada con señal de información *BPSK* [Proakis, 1989].

Para mostrar el efecto de ensanchamiento en el tiempo, se considera a $G(t)$ (***Figura 10***a) como la señal a transmitir, $a(t)$ (***Figura 10***b) como la secuencia PN y $Gss(t)$ (***Figura 10***c) después del ensanchamiento.

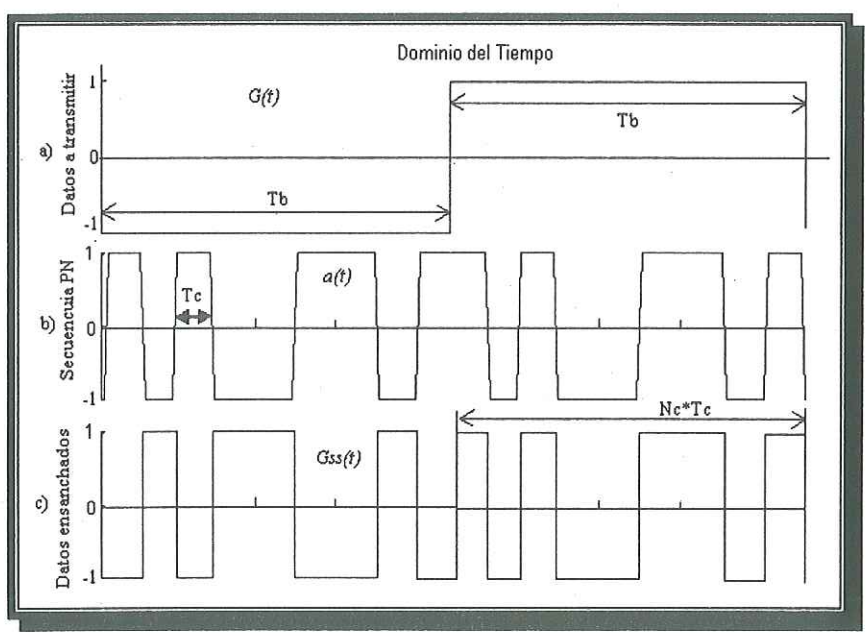

Figura 10: Proceso de ensanchamiento de la señal a transmitir.

En dicha *Figura 10* se puede apreciar como la multiplicación de los datos por la secuencia pseudo aleatoria se lleva a cabo por medio de una suma en módulo 2. Esto es posible ya que las secuencias de pulsos son bipolares +1, -1 y éstas son asignadas en forma binaria 0, 1 respectivamente [Sklar, 1998].

En la *Figura 10* se asume que la velocidad de información es R *(bits/seg)*, por lo que T_b *(1/R)* es la duración de un bit de información a transmitir, T_c define la duración de un pulso del generador de secuencia *PN*. Por lo que el ancho de banda de la señal ensanchada puede ser expresada por medio de la siguiente ecuación:

$$B_c = \frac{T_b}{T_c} = L_c \qquad (25)$$

donde L_c es denotado como el número de chip por bit de información. Esto es, L_c es el número de desplazamientos de fase que ocurren en la señal transmitida durante un bit de información T_b.

Para mostrar la ventaja de la modulación de espectro ensanchado frente a interferencias, sea $G(f)$ (*Figura 11*a) la densidad espectral de potencia de la señal a transmitir antes del proceso de ensanchamiento, N_0 la densidad espectral de potencia del ruido térmico y $Gss(f)$ (*Figura 11*b) como la densidad espectral de potencia después del ensanchamiento. Como resultado del proceso de ensanchamiento se observa que $G(f)$ se ha transformado en $Gss(f)$, mientras que la densidad espectral del ruido blanco (N_o) no es alterado como resultado de ensanchar la señal de W a W_{ss}.

En la *Figura 11* se puede apreciar como la señal a transmitir es ensanchada ocupando un mayor ancho de banda (W_{ss}).

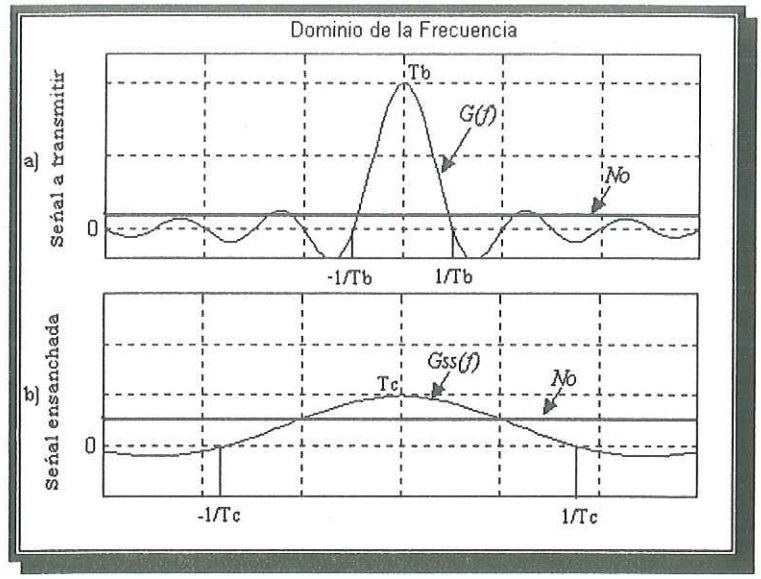

Figura 11: Densidad espectral de la señal a transmitir y de la señal ensanchada.

A continuación se supone que la señal ensanchada es transmitida e interferida en el canal de comunicación por otra señal *H(f)*, como se muestra en la *Figura 12*.

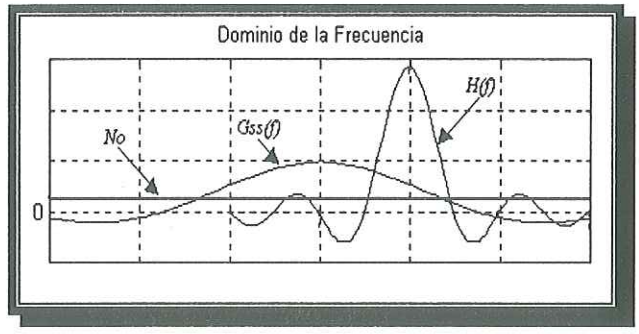

Figura 12: Señal ensanchada y señal interferente.

En el receptor toda señal que entra es multiplicada por el código pseudo aleatorio produciéndose el desensanchamiento para la señal transmitida *Gss(f)* y un ensanchamiento para las señales interferentes *H(f)*, lo que permitirá finalmente recuperar la información contenida en *G(f)* tal como se observa en la *Figura 13*. En el caso de señales de potencia

infinita tales como el ruido blanco, no se producirá ensanchamiento del espectro por lo que la modulación de espectro ensanchado no proporciona ventaja adicional frente al ruido blanco, pero sí frente a interferencias.

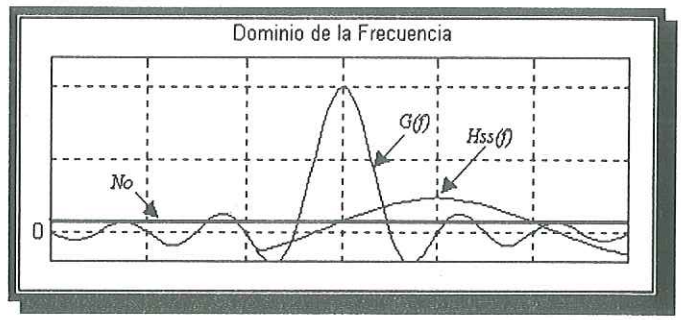

Figura 13: Señal recuperada y señal interferente ensanchada.

Para un sistema *DS/SS-BPSK* la ganancia de procesado viene definida por:

$$G_p = \frac{\left(2/T_b\right)}{\left(2/T_c\right)} = T_b/T_c = N \qquad (26)$$

donde N es la longitud de la secuencia *PN*.

La ganancia de procesado, representa el factor en que son reducidas las interferencias en el receptor, debido al ensanchamiento que sufren éstas cuando son multiplicadas por el código *PN* en el proceso de recepción. Para los sistemas de espectro ensanchado, es una gran ventaja tener una ganancia de procesado tan grande como sea posible.

III.4 Secuencias pseudo aleatorias (secuencias PN).

Los códigos implementados en *CDMA* poseen propiedades periódicas y aleatorias, por lo que se les denomina códigos de pseudo-ruido o secuencias pseudo aleatorias. Sin embargo no todos los códigos poseen las mismas propiedades. Existen diversos tipos de secuencias *PN*, pero la más importante es la secuencia binaria de longitud máxima o secuencia *M*.

Las aplicaciones de las secuencias *PN* incluyen sincronización de señal, navegación, generador de números aleatorios, comunicación de espectro ensanchado, resolución de múltiples caminos e identificación de señal en sistemas de comunicación de acceso múltiple. La correlación entre dos secuencias $\{x(t)\}$ y $\{y(t)\}$ es el producto interno de la primera secuencia con una versión desplazada de la segunda secuencia. La correlación es llamada:

- Una relación de autocorrelación si las dos secuencias son las mismas.
- Una correlación cruzada si ellas son distintas.
- Una correlación periódica si el desplazamiento es un desplazamiento cíclico.
- Una correlación aperiódica si el desplazamiento no es cíclico.
- Una correlación periódica parcial si el producto interno envuelve únicamente un segmento parcial de las dos secuencias.

III.4.1 Secuencias de longitud máxima (secuencias M).

Los códigos de secuencia máxima son por definición los códigos más largos que pueden ser generados por un registro de desplazamiento o un elemento de retardo [Dixon, 1994]. En un registro de desplazamiento binario la secuencia de longitud máxima es de 2^n-1 chips, donde n es el número de estados en el registro de desplazamiento.

La secuencia *M*, es obtenida usando registros de desplazamiento realimentados asociada a una lógica digital conformada por compuestas *XOR*.

Cualquier código puede ser representado por un polinomio característico, donde el código binario es representado por un polinomio característico de la forma:

$$Zx^n + \cdots\cdots + Cx^3 + Bx^2 + Ax + 1 \qquad (27)$$

Donde cada coeficiente (A,B,....Z) es 1 ó 0. Cada término del polinomio característico (excepto por el primero, 1) corresponde a un estado de un registro de desplazamiento binario, y hay *n* estados en el registro.

La conexión de realimentación en el generador de código está definido por el término en el polinomio cuyo coeficiente es uno. Por ejemplo un generador de código cuyo polinomio característico es $x^7+x^5+x^3+1$ tiene siete estados con realimentación tomada de su primero, tercero, quinto y séptimo estado. Tal como se ilustra en la *Figura 14*.

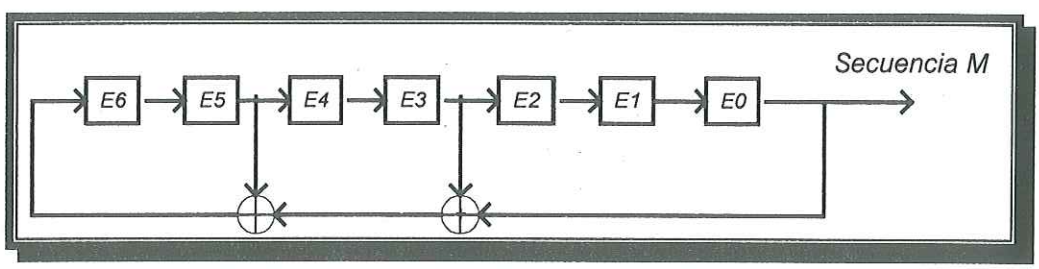

Figura 14: Representación del polinomio característico $x^7+x^5+x^3+1$

Dado que el número de estados posibles en un registro de desplazamiento de *n* etapas es de 2^n, la secuencia de salida deberá ser periódica. Es claro que el estado nulo del registro, con todos los estados de inicio a cero lógico, es un estado degenerado, ya que a la salida siempre se tendrán ceros lógicos. Por lo tanto el máximo periodo posible en un sistema de este tipo es $N = 2^n-1$. Un aspecto que se tiene que tomar en cuenta en este tipo de secuencias es que no todos los polinomios dan lugar a una secuencia de longitud

máxima. La condición necesaria y suficiente para que un registro de desplazamiento linealmente realimentado de lugar a una secuencia de longitud máxima es que su polinomio característico sea primitivo. En [Dixon, 1994 y Lin Shu y Costello, 1983] se representan los diferentes polinomios primitivos. Este tipo de polinomios y polinomios irreducibles se analizarán más detalladamente en el siguiente capítulo.

Las propiedades que son aplicadas a cualquier secuencia *M* más relevantes son las que se mencionan a continuación:

1. Propiedad de desplazamiento: El desplazamiento cíclico de una secuencia *M* es también una secuencia *M*.
2. Propiedad de balance: En cualquier secuencia *M* se tiene un buen balance en donde el número de unos binarios es de 2^{n-1} y el número de ceros binarios es $2^{n-1}-1$.
3. Propiedad Runs: Un run es una secuencia consecutiva de unos y ceros. En una secuencia *M* la mitad de runs tiene longitud uno, un cuarto tiene longitud dos, un octavo tiene longitud tres y así sucesivamente. El total de runs de una secuencia *M* es $(N+1)/2$ donde $N=2^n-1$.
4. Propiedad de la suma: La suma binaria de una secuencia *M* es también una secuencia *M*.
5. La autocorrelación de una secuencia periódica es bivaluada, esto puede ser descrito por.

$$C(K)=\sum_{n=1}^{N} a_n a_{n+k} = \begin{cases} N & \text{K=0, N, 2N, ...} \\ -1 & \text{Cualquier otro caso} \end{cases} \qquad (28)$$

donde $a_{n+N}=a_n$ y N= 2^n-1

La respuesta de la correlación para una secuencia *M* es la que se muestra en la *Figura 15*.

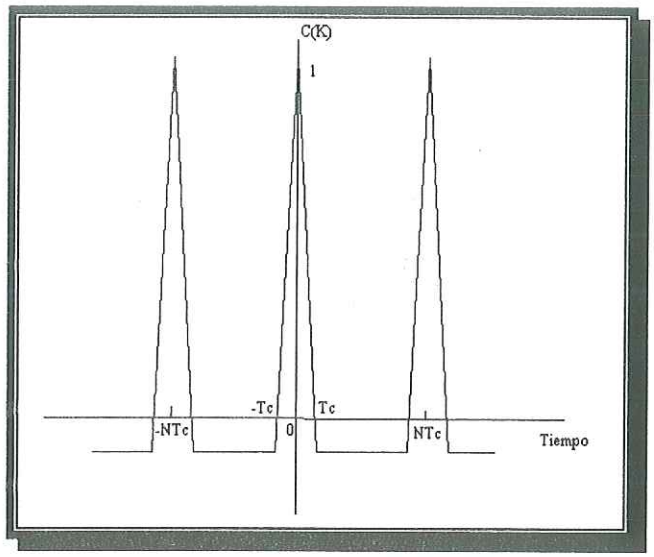

Figura 15: Autocorrelación de una secuencia M.

Las secuencia *M* no son inmunes a los problemas de correlación cruzada, y pueden tener un valor grande de correlación cruzada. Este tipo de secuencias son de más interés en sincronización de sistema celulares. Entonces cada estación base o móvil es identificada por una única secuencia binaria en enlace ascendente (*forward*) y descendente (*reverse*).

En *DS/CDMA*, usualmente se requieren grandes familias de secuencia que, tomadas de dos en dos, presenten baja correlación, es posible combinar en ciertos casos parejas preferidas de secuencias *M* (secuencias cuya correlación periódica es trivaluada) para formar una familia, las cuales son conocidas como familias maximalmente conexionadas y el tamaño de estas familias, para grado n, se denota por M_n. Se obtiene: $M_1=M_2= 0$, ya que sólo existe una secuencia *M* en cada de estos casos de período tan corto. Como no existen parejas preferidas de secuencias cuando *n* es múltiplo de 4, tenemos $M_4=M_8=M_{12}=M_{16}= 0$. Para el resto de valores de n entre 1 y 16, se encuentra:

$$M_3=M_6=M_9=M_{15}= 2$$

$$M_5=M_{10}=M_{14}= 4$$

$M_{11}=M_{13}=6$

$M_7=6$

Por lo que nunca hay más de 6 secuencias *M* en cualquier familia maximalmente conexionadas de periodo inferior a $2^{16}-1=65535$, por lo que estas secuencias solo dan servicio a un número muy reducido de usuarios.

III.5 Secuencias de Gold.

Una secuencia de *Gold* se obtiene a partir de un par de secuencias *M*. La secuencia de *Gold* es apropiada para la multiplexación de códigos, porque el número de direcciones asignables es mayor. Presentan buen comportamiento de correlación cruzada y autocorrelación. El código es generado por una suma en módulo 2 de un par de secuencias lineales máximas tal como se muestra en la *Figura 16*.

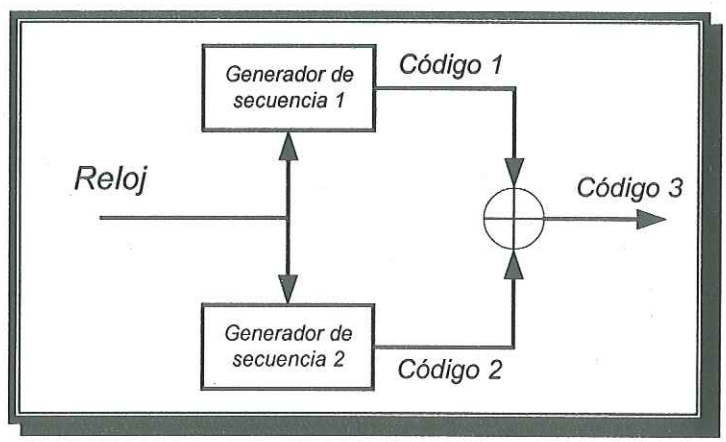

Figura 16: Generador de secuencias de código Gold.

Suponiendo que los registros de desplazamiento descritos por los polinomios característicos *f(x)* y *g(x)* generan las secuencias binarias {*a*} y {*b*}, de periodos N_a y N_b, respectivamente. Cualquier secuencia generada por el registro de desplazamiento descrito por el polinomio característico f(x)• g(x) debe tomar una de estas tres formas:

$$\begin{aligned} &\text{(i)} \quad \{y\} = \{\mathbf{T}^i a\} \\ &\text{(ii)} \quad \{y\} = \{\mathbf{T}^j b\} \\ &\text{(iii)} \quad \{y\} = \{\mathbf{T}^i a\} \oplus \{\mathbf{T}^j b\} \end{aligned} \qquad (29)$$

donde T es el operador de rotación cíclica a la izquierda

Observando que el mínimo período de una secuencia cualquiera, $\{y\}$, del tipo (iii) es el mínimo común múltiplo (*mcm*) de los períodos de {a} y {b}. Es decir $N_y = mcm(N_a,N_b)$. Las secuencias de los tipos (i) y (ii) son simples rotaciones cíclicas de {a} y {b}. Por lo tanto, el número N_s de secuencias diferentes del tipo (iii) es:

$$N_s = N_a N_b / N_y = N_a N_b / mcm(N_a,N_b) = mcd(N_a,N_b) \qquad (30)$$

donde *mcd* es el máximo común divisor. Finalmente, todas y cada una de las N_s diferentes secuencias del tipo (iii) pueden obtenerse mediante la siguiente expresión para algún valor de *k*:

$$\{y\} = \{\mathbf{T}^k a\} \oplus \{b\} \quad \text{Para } 0 \le k \le N_s\text{-}1 \qquad \text{ó} \qquad (31)$$

$$\{y\} = (b,\ a,\ b\oplus a,\ b\oplus \mathbf{T}a,\ b\oplus \mathbf{T}^2 a,\ \ldots\ldots\ldots,\ b\oplus \mathbf{T}^{K-1} a)$$

donde a y b son dos vectores *PN*, y $T^k a$ es el vector a desplazado *k* muestras.

Si $N_a = N_b = N$ por lo tanto $N_s = N$, es decir, que podemos generar una gran familia de *N* nuevas secuencias, de período *N*, a partir de la pareja original (Propiedad para generar los códigos de *Gold*).

La correlación cruzada entre una pareja preferida es trivaluada, donde estos tres valores son *–1, -t(n)* y *t(n)-2,* donde *t(n)* es:

$$t(n)=\begin{cases}1+2^{(n+1)/2} & \text{Para n impar}\\ 1+2^{(n+2)/2} & \text{Para n par}\end{cases} \qquad (32)$$

Existen dos formas de generar las secuencias de código de *Gold*.

- Mediante implementación directa.
- Mediante implementación indirecta.

III.5.1 Calculo de las secuencias de Gold mediante implementación directa.

El polinomio producto $f(x) \cdot g(x)$, tiene grado $2n$, de forma que el correspondiente registro deberá tener $2n$ etapas. Las diferentes $N+2$ secuencias pueden obtenerse cargando inicialmente este registro de desplazamiento con $N+2$ palabras binarias diferentes de $2n$ bits. Para averiguar cuales son estas $N+2$ palabras binarias, se debe determinar previamente cuales son los N bits que conforman la secuencia {a} y los primero $2n$ bits de la secuencia {b}, y aplicar a continuación la expresión 31 para las sucesivas rotaciones de la secuencia {a}.

III.5.2 Calculo de las secuencias de Gold mediante implementación indirecta.

La segunda alternativa, para generar los códigos de Gold, es implementar los dos registros de desplazamiento que generan {a} y {b} y sumarlos en módulo 2 "chip" a "chip", las dos salidas.

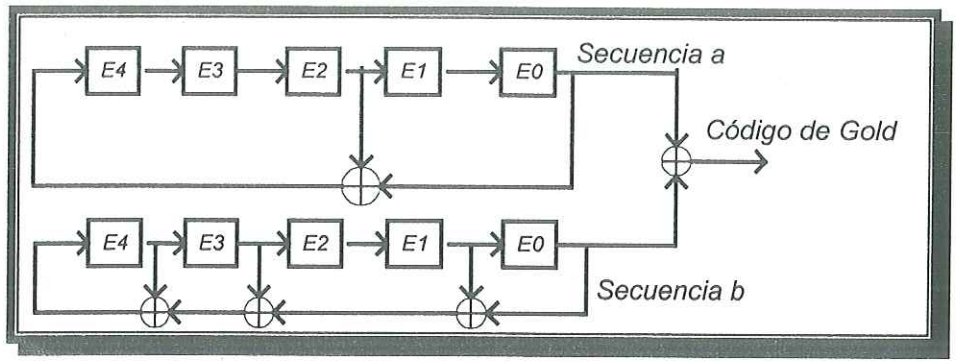

Figura 17: Secuencia de Gold mediante la implementación indirecta.

Una característica de los polinomios a implementar es que tienen que ser polinomios de parejas preferidas. Estos polinomios pueden ser consultados en la referencia [Dixon, 1994].

III.6 Secuencias de Walsh.

Los códigos *Walsh* son los patrones primarios de transmisión utilizados en los sistemas *CDMA* de telefonía móvil. Los códigos *Walsh* sirven para identificar a cada transmisor con la base y a la base con cada transmisor así como para ensanchar el código de la señal original.

Las funciones de *Walsh* son mutuamente ortogonales lo que significa que la correlación cruzada entre funciones *Walsh* es mínima. El efecto de los códigos *Walsh* es hacer a los canales completamente separables en el receptor, al menos con la ausencia del efecto de múltiples caminos. La ortogonalidad de los códigos *Walsh* garantiza que no habrá interferencia entre usuarios dentro de la misma célula.

Los códigos *Walsh* están basados en matrices de *Walsh-Hadamard*. En el canal ascendente (*forward link*) los códigos de *Walsh* garantizan la independencia de los

diferentes canales y en el enlace descendente (*reverse link*) son utilizados como moduladores ortogonales.

Los códigos *Walsh* tienen ciertas desventajas:

- Los códigos no presentan un único pico estrecho de autocorrelación. Como consecuencia la sincronización del código llega a ser difícil.
- El ensanchamiento no se lleva acabo sobre todo el ancho de banda y la energía es esparcida sobre un número discreto de componentes de frecuencia. Esto se puede apreciar en la *Figura 18*.

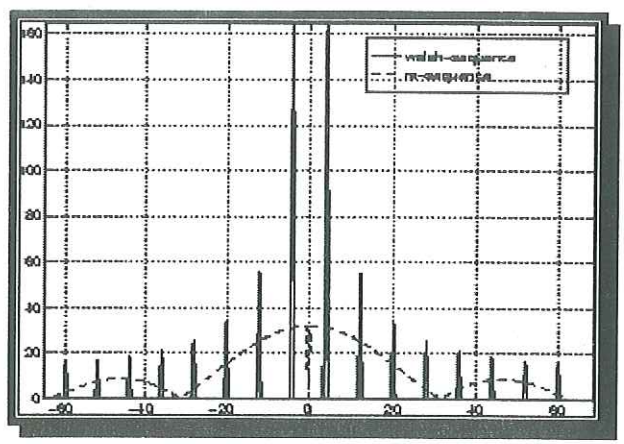

Figura 18: Comparación del espectro de frecuencia de una secuencia M a una de Walsh.

Las secuencias de *Walsh* son implementados en sistemas *CDMA* y en los sistemas celulares *CDMA IS-95*.

III.7 Concatenación de códigos.

Este tipo de arreglo de secuencias surge con la necesidad de poder implementar una variedad de servicios (voz, datos y video), lo cual no se puede llevar a cabo en los sistemas de segunda generación. Estas secuencias son implementadas por los sistemas de tercera

generación los cuales pueden manejar estos tipos de servicios sin ningún problema, por lo que surge lo que se conoce como CDMA2000 y UMT2000,

III.8 IS-95.

Este estándar fue especificado por *TIA* basado en la propuesta por *Qualcomm* para los sistemas celulares de segunda generación. IS-95 está basado en un sistema de espectro ensanchado en secuencia directa (*DS/CDMA*). Implementa una señal de secuencia pseudo aleatoria para ensanchar los datos la cual tiene una velocidad de chip de 1.2288 *MHz*, el ancho de banda de la señal trasmitida es aproximadamente de 1.25 *MHz*. Una combinación de control de potencia en lazo abierto y lazo cerrado habilitan a la estación móvil para operar en un nivel de transmisión de potencia mínima. Esta tecnología opera en la banda de 1.7 a 1.8 *GHz*.

III.9 CDMA de banda ancha (W-CDMA).

Los sistemas de tercera generación implementan este método de acceso, el cual fue estandarizado por *TIA* como el estándar *CDMA2000* (TR45.5) y tiene capacidad para manejar anchos de banda de 1.25, 5, 10, 15 y 20 *MHz*. La velocidad de chip considerada en los sistemas de *3G* es de 1.2288, 3.3728, 11.0593 y 14.7456 *Mcps* para secuencia directa y de (n * 1.2288 *Mcps*) para portadora múltiple.

Los sistemas de *3G* manejan cualquier tipo de servicio (voz, datos y video), esto es posible gracias a la concatenación de códigos que implementan. Se utilizan tres tipos de secuencias *PN* para transmitir los datos: las secuencias de *Walsh* que son utilizadas para identificar el canal de cada usuario con lo que un usuario puede tener múltiples canales para poder transmitir los múltiples servicios, los códigos de *Gold* se utilizan para identificar a los usuarios y las secuencias *M* identifica las estaciones base.

III.10 El sistema CDMA.

En un sistema *DS/CDMA* el control de potencia es una necesidad vital para la operación del sistema. Así como la implementación tanto para transmisión como para recepción de antenas sectorizadas y un diseño de un sistema de codificación de corrección de error muy poderoso.

III.10.1 Control de potencia.

Como en un sistema *CDMA* los móviles están en continuo movimiento se tienen que emplear técnicas de control de potencia ya que los sistemas son sujetos a los efectos de cerca-lejos (*near-far*) en las cuales una estación móvil cerca de la estación base tiene una mucho menor pérdida de trayectoria a la estación base que una que se encuentra lejos de la estación base. Por lo que una combinación de control de potencia, en lazo abierto y lazo cerrado, comandan la estación base para realizar ajustes de potencia, de tal manera que las potencias recibidas provenientes de todos los usuarios deben de ser casi iguales. Estos controles de potencia minimizan la interferencia con otros usuarios, ayuda a dominar los efectos de desvanecimientos (*fading*) y conserva la potencia de la batería del móvil. La potencia transmitida en el móvil debe ser ajustado de una manera inversamente proporcional a la distancia efectiva de la estación base [Gibson, 1996].

El sistema de control de potencia no tiene que compensar únicamente las variaciones de señal debido a la variación de la distancia entre la estación base y el móvil, sino también debe compensar las típicas fluctuaciones de señal de un canal RF. Estas fluctuaciones son debidas a los cambios de propagación del medio ambiente entre la estación base y el móvil. Existen dos grupos principales de fluctuación de canal: lento (*shadowing*) y rápido (*fading*).

III.10.1.1 Control en lazo abierto.

Las pérdidas por propagación entre el móvil y la estación base varían continuamente, de manera que el control de potencia debe llevarse a cabo ininterrumpidamente, ésto se lleva acabo mediante el control de potencia en lazo abierto, este tipo de control de potencia debe basar su acción en la estimación del estado del canal.

El funcionamiento de este tipo de control de potencias es el siguiente. Las estaciones base transmiten una señal piloto a la misma frecuencia, los móviles se encargan de medir, tanto la potencia de la señal piloto de la estación base a la que se encuentra conectado, como la suma de potencias de las señales piloto del resto de las estaciones base del sistema celular. Con la potencia recibida de la estación base el móvil estima las pérdidas de propagación y decide la potencia a trasmitir. El móvil analiza también la potencia recibida del resto de las estaciones base del sistema, ya que se puede dar el caso de que exista una mejor trayectoria de propagación con alguna otra estación base.

Este tipo de control es adecuado para el caso de una fluctuación repentina del canal, tal como es el caso de un móvil que pasa por detras de un obstáculo alto (Desvanecimientos lentos o *lognormal*).

III.10.1.2 Control en lazo cerrado.

El control de lazo cerrado tiene la función de controlar la potencia transmitida por el móvil para que la relación señal a ruido (*SNR*) deseada sea recibida en la célula. Este control de potencia no solo controla la potencia sino que también controla la *SNR*.

Cada estación base lleva a cabo una estimación de la *SRN* recibida de los móviles. Esta estimación se realiza cada 1.25 ms [Gibson, 1996]. La *SRN* recibida es comparada con la mínima SNR fijada por la estación base. Si la *SRN* recibida es demasiado alta, la estación base manda un mensaje al móvil para que el móvil disminuya el nivel de potencia, este mensaje es mandado a una razón de 800 bps [Gibson, 1996]. En caso contrario si la *SRN* es

demasiado pobre, la estación base manda un mensaje al móvil para que aumente el nivel de potencia de transmisión.

Los mensajes de control de potencia que la estación base envía al móvil están contenidos en los bits de control de potencia, los cuales son transmitidos al principio del flujo de datos y no son protegidos contra errores, ya que se desea que el móvil recupere rápidamente los bits de control de potencia. Estos bits de control de potencia indican un aumento o disminución de potencia de 1 *dB* de la potencia nominal.

III.10.2 Capacidad.

Los parámetros principales que determinan la capacidad en un sistema celular *CDMA* son la ganancia de procesado, la relación E_b/N_0, el factor de actividad de la voz, la reutilización de frecuencia, las interferencias de otros usuarios de la misma celda, las interferencias de celdas adyacentes y el número de sectores de la antena en la celda.

Por ejemplo para el sistema *IS-95* (ancho de banda de 1.25 *MHz*, 9600 *bps* velocidad de transmisión del móvil y un E_b/N_0 de 6 *dB*) se tiene que la capacidad objetiva es de 32 usuarios como máximo transmitiendo simultáneamente de acuerdo a la ecuación 33 [Gibson, 1996]. En un sistema *CDMA* esta capacidad es reducida por interferencias e incrementada por otros factores tales como la sectorización de las antenas, reutilización de frecuencias y factor de actividad de la voz.

$$M = \frac{W/R}{E_b/N_0} = \frac{G_p}{E_b/N_0} \qquad (33)$$

En un sistema bidireccional (*full duplex*) el factor de actividad de la voz es aproximadamente un 35%. En los sistemas *FDMA* y *TDMA* es difícil de explotar este factor debido al tiempo de retardo asociado con la reasignación de la fuente del canal durante la pausa del habla. Con los sistemas *CDMA* es posible reducir la velocidad de

transmisión cuando no hay habla, y por lo tanto reducir substancialmente interferencias con otros usuarios.

Las antenas implementadas por los sistemas *CDMA* son sectorizadas, con ésto la capacidad del sistema se incrementa gracias a la sectorización de las antenas. Los sitios son sectorizados usualmente en tres formas. Esto es cada sitio es equipado con tres conjuntos de antenas direccionales, con azimut separada por 120^0.

La capacidad del sistema es afectado por los fenómenos de propagación. Los múltiples caminos se pueden deber a la reflexión o refracción atmosférica, a la reflexión en edificios u otros objetos, como consecuencia de ello tenemos fluctuación del nivel de la señal recibida y en el peor caso un desvanecimiento de la señal. Los diferentes caminos múltiples consisten en caminos de señal con diversas atenuaciones y retardos.

III.10.2.1 Capacidad efectiva.

La capacidad efectiva del sistema puede ser calculada frente a todas las consideraciones mencionadas anteriormente y con la ecuación 33. Obteniendo la ecuación 35. Por lo que para un sistema *IS-95* la capacidad máxima teórica es de 128 usuarios por celda [Gibson, 1996].

Considerando las interferencias, se tiene:

$$I = (M-1)S\upsilon^{-1}F \qquad (34)$$

donde: F = interferencia interceldas.

M = número de usuarios en el sistema.

S = sectorización de las antenas.

υ = factor de actividad de la voz.

$$M_{neta} = \frac{G_p}{(E_b / N_0)\upsilon} SF \qquad (35)$$

III.10.3 Sincronización.

El problema fundamental de recuperar la señal en un sistema *DS/CDMA* reside en tener una replica completamente sincronizada de la señal de código *PN* que se utiliza en el transmisor. A consecuencia de ésto o se manda una señal de sincronismo a los receptores, o se debe de tener un método para realizar el sincronismo de forma local en el receptor, el proceso de sincronismo se realiza generalmente en dos fases: adquisición y seguimiento.

III.10.3.1 Adquisición (ajuste grueso).

En primer lugar se ha de realizar una búsqueda tanto en tiempo como en frecuencia antes de la sincronización de la señal ensanchada recibida con la secuencia ensanchadora generada localmente en recepción. Para ello se deben de resolver ciertos problemas entre los cuales están:

- Incertidumbre entre la distancia transmisor receptor lo que se traduce en una incertidumbre en el retardo de transmisión.
- Incertidumbre entre las velocidades relativas transmisor receptor lo que conlleva a un desconocimiento de la deriva en frecuencia por el efecto *Doppler*.
- Inestabilidad entre los relojes de transmisión y recepción que origina diferencias de fase entre ambas señales.
- Inestabilidades relativas entre los osciladores de transmisión y recepción lo que origina *offsets* de frecuencias entre ambas señales.

Los métodos de adquisición se basan en medir la similitud que existe entre la señal que llega y la generada internamente en el receptor para posteriormente, mediante un comparador decidir si las señales están en sincronismo. Existen diversas maneras de realizar este proceso, los cuales pueden ser mediante estructurado en paralelo, en serie o sistemas mixtos.

III.10.3.1.1 Estructura en paralelo.

Si existe una incertidumbre de tiempo dada entre la transmisión y la recepción, ésta es expresada en función a su equivalencia con N_c chips. Para cubrirla se sitúa una serie de $2N_c$ correladores en paralelo de forma que a cada uno se lo introduce el código ensanchador generado con una diferencia de retardo de medio chip, $T_c/2$. Cada uno de ellos hace la correlación de un chip y posteriormente se comparan las $2N_c$ salidas, de forma que cuando en una de las ramas se tenga un valor por encima de un cierto umbral, se considera que se ha acertado con el retraso. En caso de que en todas ellas las salida se mantenga en un nivel mínimo, se habrá de modificar los retrasos de los correladores, ampliando así el margen de incertidumbre. El valor de L, número de chips que compara cada correlador, hay que fijarlo de acuerdo con un compromiso que se marque entre la probabilidad de elegir una secuencia incorrecta, que decrecerá a medida que aumenta L, y la velocidad de sincronización, que lo contrario crecería según disminuya L.

III.10.3.1.2 Estructura en serie.

La ventaja de este esquema es su menor costo y complejidad, puesto que únicamente se precisa de un solo correlador, aunque la gran desventaja es que no es útil para esquemas de alta velocidad a causa de que el tiempo máximo en el cual se adquiere el sincronismo se incrementa en un factor de $2N_c$. El funcionamiento de un sistema de este tipo es el siguiente: Se compara el código generado con la señal que se recibe durante un periodo de un chip. Si la salida resultante se mantiene en un nivel inferior a un cierto umbral, se incrementa la fase de la señal utilizada en la comparación en dos chip y se procede de nuevo a la correlación hasta que se sobrepase este límite y por lo tanto se considere adquirido el sincronismo.

III.10.3.2 Seguimiento.

Una vez que se tiene sincronizada la señal comienza el proceso de seguimiento o sincronización fina este se realiza mediante lazos de seguimiento que se clasifican habitualmente de dos formas: delay-locked loop (*DLL*) y tau-dither loop (*TDL*).

III.11 Probabilidad de error en BPSK y QPSK.

En *BPSK*, la fase de una portadora de amplitud constante es conmutada entre dos valores acorde a los dos posibles señales m_1 y m_2 correspondiendo a 1 y 0 binario respectivamente, las dos fases son separadas por 180^0. Si la portadora tiene una amplitud A y la energía por bit $E_b = \frac{1}{2}A^2T_b$, Por lo tanto la señal transmitida es:

$$S_{BPSK}(t) = \sqrt{\frac{2E_b}{T_b}}\ Cos(2\pi f_c t + \theta_c) \qquad 0 \le t \le T_b \ \text{(binario 1)}$$

ó

$$S_{BPSK}(t) = \sqrt{\frac{2E_b}{T_b}}\ Cos(2\pi f_c t + \pi + \theta_c)$$

$$= -\sqrt{\frac{2E_b}{T_b}}\ Cos(2\pi f_c t + \theta_c) \qquad 0 \le t \le T_b \ \text{(binario 0)}$$

La probabilidad de error para muchos esquemas de modulación en un canal AWGN es encontrada usando la función Q de la distancia entre los puntos de la señal [Rappaport, 1996]. Por lo que la probabilidad de error en BPSK esta dada por la ecuación 36.

$$Pe_{,BPSK} = Q\left(\sqrt{\frac{2E_b}{N_0}}\right) \qquad (36)$$

En la modulación *QPSK* la fase de la portadora toma de 1 a 4 valores espaciados equitativamente, tales como 0, π/2, π y 3π/2, donde cada valor de fase corresponde a un único par de bits de mensaje. La señal *QPSK* para este conjunto de símbolos de estados es definida por la formula siguiente.

$$S_{QPSK} = \sqrt{\frac{2E_s}{T_s}}\ \cos\left[2\pi f_c t + (i-1)\frac{\pi}{2}\right] \qquad 0 \le t \le T_s \qquad i = 1,2,3,4.....$$

donde T_s es la duración de símbolo y es igual a dos veces el periodo de bit de la señal.

La probabilidad de error para la modulación *QPSK* esta definida por la ecuación 36. Por lo que la modulación *BPSK* y *QPSK* tienen la misma probabilidad de error.

III.12 Simulación de la asignación de códigos en CDMA.

En este apartado se verifican las propiedades de las secuencias *M*, secuencias de *Gold* y secuencias de *Walsh* obtenidas mediante simulación, también se analizará la modulación de *CDMA* y *W-CDMA*.

III.12.1 Secuencias M.

Las secuencias *M* implementadas fueron generadas por medio de los siguientes polinomios primitivos característicos (Estos polinomios serán definidos en el siguiente capítulo de esta tesis) $g(x)=1+x^6+x^7+x^8$ y $h(x)= g(x)=1+x^3+x^3+x^8$. Los resultados de autocorrelación y correlación cruzada se muestran en la ***Figura 19***.

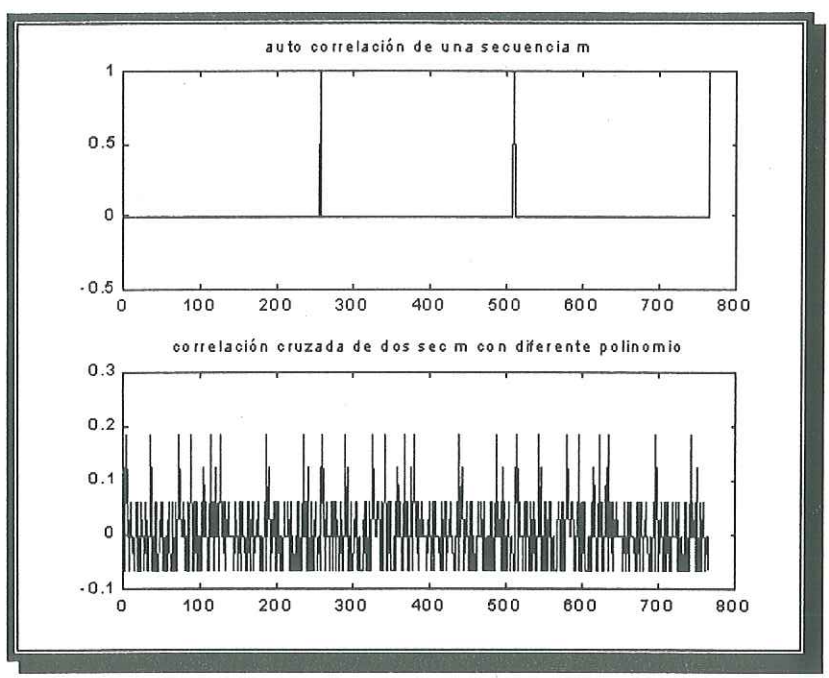

Figura 19: Autocorrelación, y correlación cruzada de una secuencia M.

Los resultados de correlación fueron obtenidos mediante la ecuación 37 [Sklar, 1998].

$$R_x(\tau) = \frac{1}{P}\begin{pmatrix}\text{número de acuerdos menos número de desacuerdos}\\ \text{comparados en un periodo completo de la secuencia}\\ \text{con un desplazamiento } \tau \text{ veces una respecto}\\ \text{a la otra secuencia}\end{pmatrix} \qquad (37)$$

donde P es el periodo de repetición de la secuencia.

$$P=2^n-1 \qquad (38)$$

Comparando los resultados de la ***Figura 19*** con los resultados descritos por Sklar y Dixon, se comprueba como la autocorrelación de una secuencia M es bivaluada. Esto quiere decir que únicamente tiene dos valores. Como se mencionó anteriormente la desventaja principal de las secuencias M es que únicamente se le puede dar servicio a un número reducido de usuarios, por lo que surge la necesidad de emplear otro tipo de secuencias, tales como *Gold o Walsh.*

III.12.2 Secuencias de Gold.

Las secuencias de *Gold* se generaron mediante la siguiente pareja preferida (Condición necesaria).

$$g(x)=1+x^2+x^5++x^6+x^7+x^8 \qquad h(x)=1+x^6+x^7+x^8$$

obteniendo las gráficas de la ***Figura 20***.

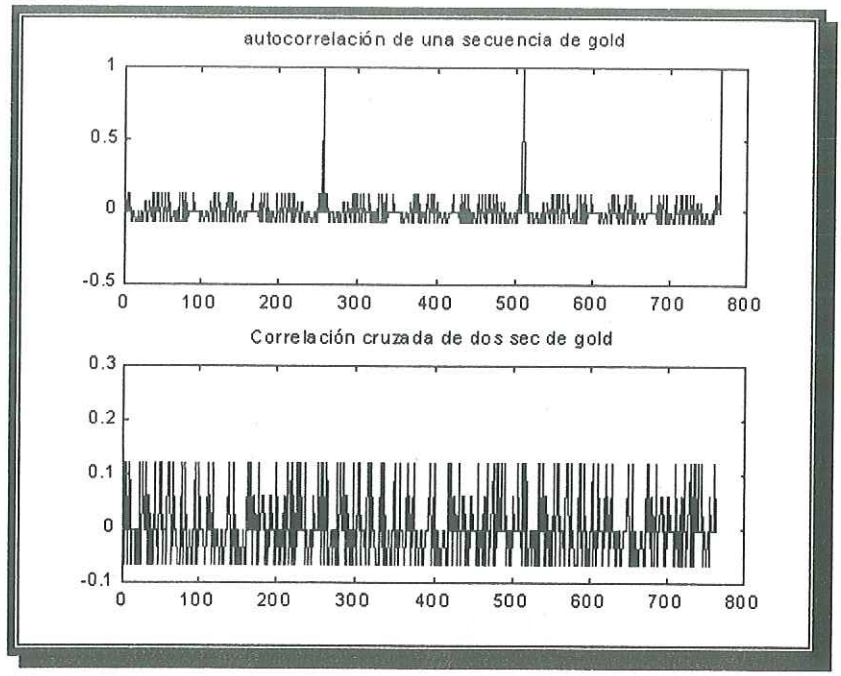

Figura 20: Autocorrelación, y correlación cruzada de una secuencia de Gold

Analizando los resultados obtenidos por las secuencias de *Gold*, en esta figura se observa como la autocorrelación de una secuencia de *Gold* es trivaluada. La principal ventaja de esta secuencia es que para una pareja preferida se pueden asignar un número de usuarios de 2^n-1, por lo que se pude manejar más usuarios por el sistema.

III.12.3 Secuencias de Walsh.

Las secuencias de *Walsh* se obtuvieron por medio de la función *Walsh-Hadamard*, en donde las filas representa un código de *Walsh* diferente. Los resultados obtenidos se muestran en la ***Figura 21***.

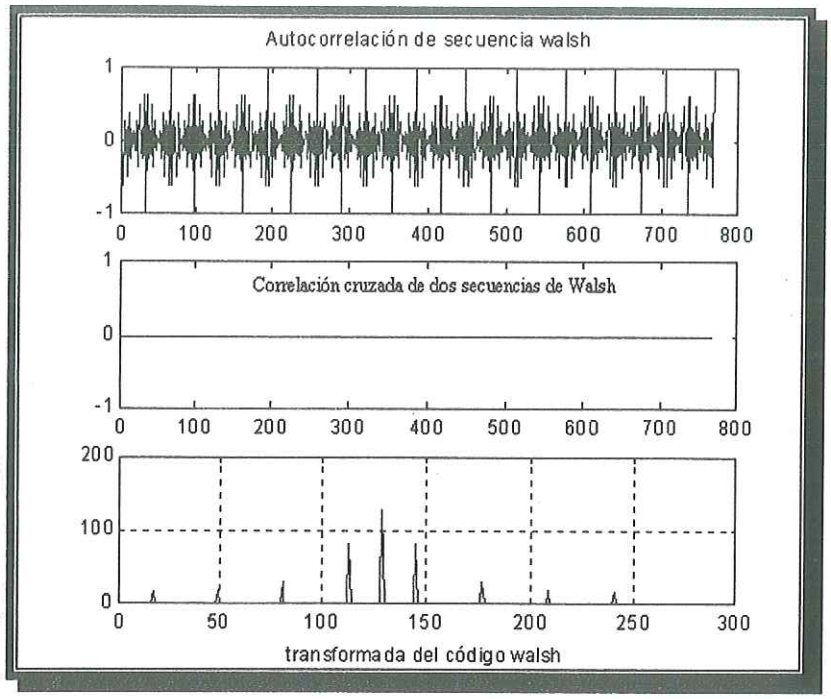

Figura 21: Autocorrelación, correlación cruzada y transformada de un código de Walsh

En estas gráficas se puede observar como la autocorrelación de una secuencia de *Walsh* no presenta un solo pico de autocorrelación, por lo que la sincronización del código puede llegar a ser difícil. También se observa como la correlación cruzada de dos secuencias de *Walsh* es completamente cero (interferencia nula entre usuarios), con lo que se asegura que las secuencias de *Walsh* son completamente ortogonales. Analizando la transformada de la secuencia de *Walsh* se aprecia como la energía se esparce sobre un número discreto de componentes de frecuencia.

III.12.4 Concatenación.

Para verificar que las secuencias concatenadas siguen cumpliendo las propiedades de una secuencia *PN* se realizó la simulación de una secuencia concatenada, obteniendo los siguientes resultados.

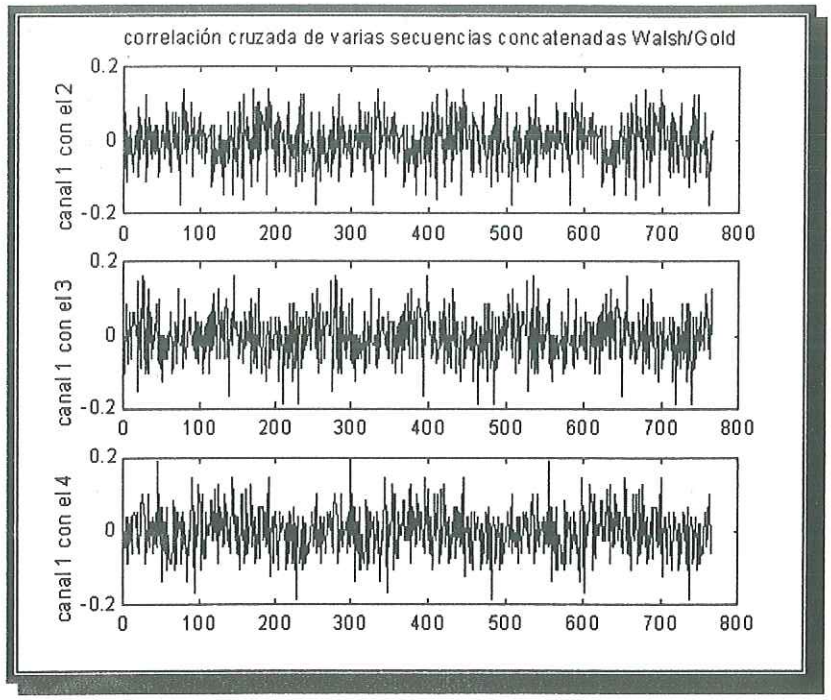

Figura 22: Correlación cruzada de la concatenación de códigos Walsh con Gold.

En la ***Figura 22*** se muestra la correlación cruzada de los canales de transmisión de datos que pertenecen a un solo usuario. El procedimiento consistió en concatenar un código de *Gold* que identifica al usuario con diferentes códigos *Walsh* que identifican a los canales (un canal diferente para cada servicio) y al correlar los valores bajos de correlación cruzada demuestran la independencia de los canales. En la ***Figura 23*** se observa la autocorrelación de cada canal, donde se aprecia el pico de correlación esperado.

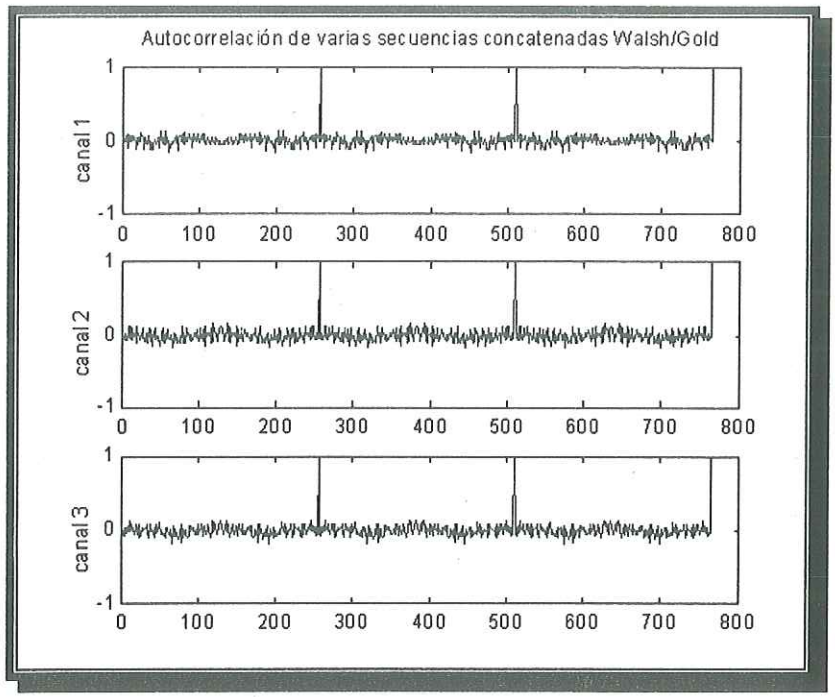

Figura 23: Autocorrelación de códigos concatenados Walsh con Gold.

III.12.5 Modulación en CDMA.

En la ***Figura 24*** se observa el proceso de ensanchamiento de la señal a transmitir, por ejemplo en la primera gráfica se tiene los datos a transmitir, en la segunda gráfica la secuencia ensanchadora (*Gold*) y en la tercera se tiene la multiplicación de la secuencia de *Gold* por cada bit de datos obteniendo los datos ensanchados (datos a transmitir).

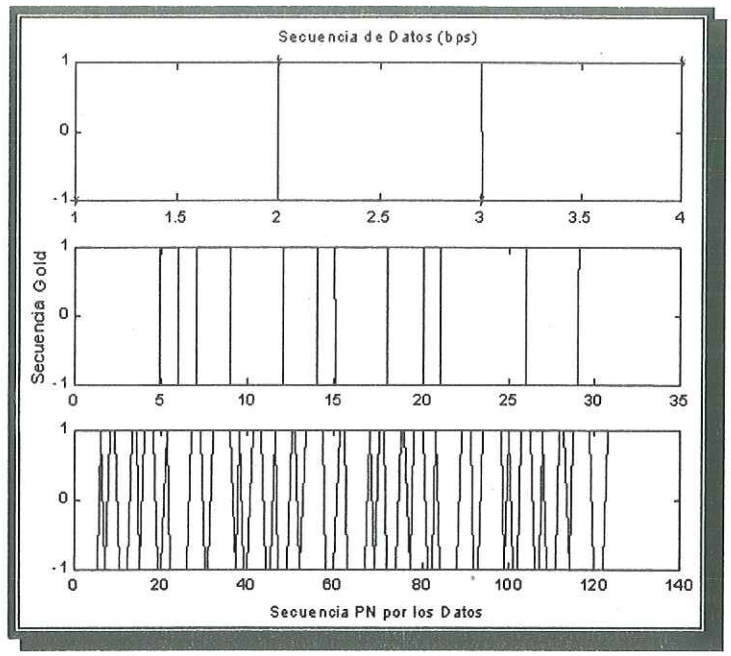

Figura 24: Proceso de ensanchamiento de la señal a transmitir en DS-CDMA.

En la ***Figura 25*** se observa el proceso de simulación, donde en la gráfica tres se aprecia la señal transmitida en *BPSK*.

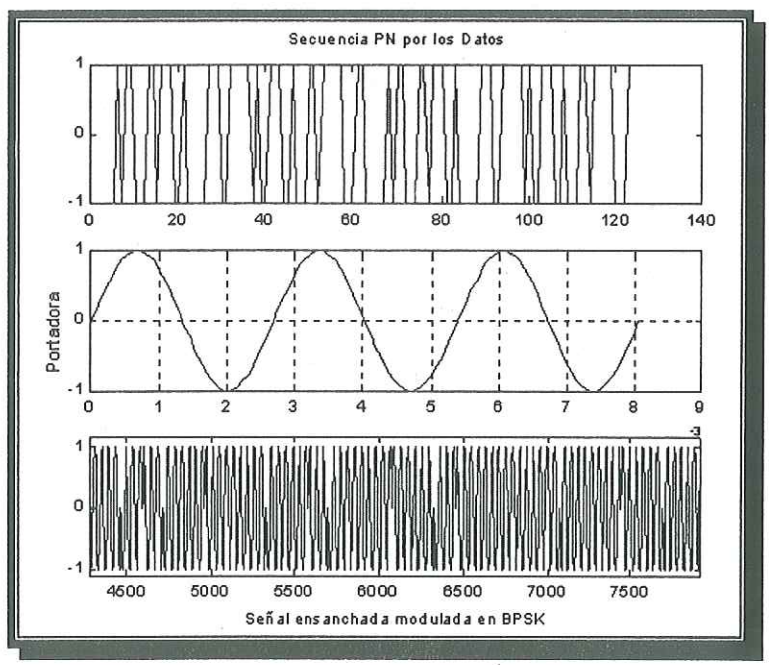

Figura 25: Proceso de modulación BPSK en DS-CDMA.

III.12.6 Modulación en W-CDMA.

En la ***Figura 26*** se observa el proceso de ensanchamiento de *W-CDMA* en donde la gráfica tres se aprecia los datos ensanchados por medio de una secuencias de *Walsh*.

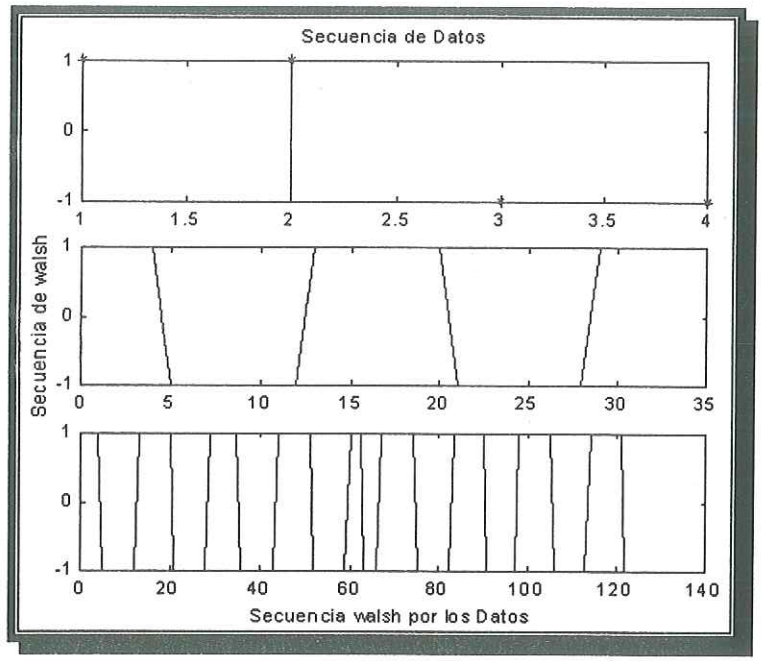

Figura 26: Proceso de ensanchamiento de W-CDMA.

En la ***Figura 27*** se observa como se lleva a cabo el proceso de concatenación de las secuencias de *Walsh* con *Gold*, en donde la gráfica uno muestra la secuencia de *Gold*, en la gráfica dos se aprecia la señal a transmitir ya ensanchada y concatenada y en la gráfica tres se aprecia la señal modulada en *BPSK*.

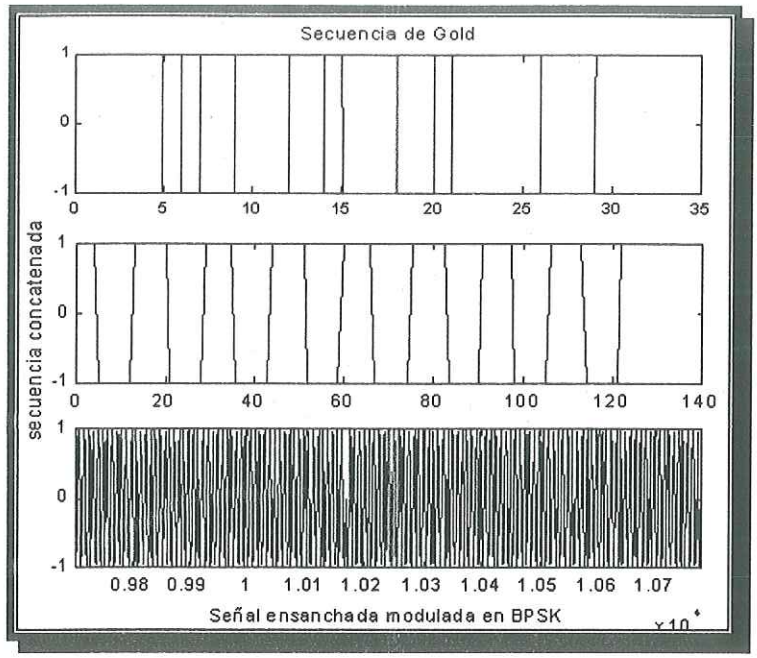

Figura 27: Proceso de modulación de W-DS-CDMA.

III.13 Conclusiones.

Con el estudio de este capítulo se tiene una mejor comprensión de un sistema *DS-CDMA*, como se realiza el ensanchamiento de los datos tanto en tiempo como en la frecuencia. Las consideraciones que se tienen que seguir para que un sistema de este tipo no tenga interferencias entre usuarios.

Un aspecto que se tienen que tomar muy en cuenta cuando se quiere generar secuencias pseudo aleatorias es que los polinomios que generan estas secuencias tienen que ser polinomios primitivos. Este tipo de polinomios se estudiará más detalladamente en el capítulo siguiente el cual trata acerca de la teoría de cuerpos finitos (*Campos de Galois*).

La concatenación de códigos juega un papel muy importante en los sistemas de tercera generación ya que por medio de ésta se pueden transmitir múltiples servicios (voz, datos y video) al mismo tiempo. Los códigos que se implementan en este tipos de sistemas son: secuencias de *Walsh* para identificar el canal, secuencias de *Gold* para identificar a los usuarios y secuencias *M* para identificar las estaciones base.

Como se mencionó anteriormente las interferencias juegan un papel muy importante en los sistemas *CDMA* ya que son éstas las que limitan la capacidad del sistema por lo que tienen que ser minimizadas para que la capacidad del sistema no se demerite. Tal como se analizó en los apartados anteriores donde el sistema *IS-95* tiene una capacidad objetiva de 32 usuarios por celda sin consideraciones y tomando en cuenta las consideraciones que se mencionaron tiene una capacidad neta de 128 usuarios por celda.

Con el desarrollo de las simulaciones realizadas se tiene una mejor comprensión de las propiedades de los códigos analizados, tal como es autocorrelación, correlación cruzada y concatenación de códigos. También se analizaron tanto las ventajas como desventajas de los códigos manejados. Por ejemplo se llego a la conclusión de que una secuencia M

presenta únicamente dos valores de autocorrelación, el número de usuarios que se pueden manejar con un mismo polinomio son muy pocos.

Dado que las secuencias *M* no puede brindar servicio a varios usuarios, es necesario implementar secuencias de *Gold* ya que estas secuencias pueden dar servicio a un número de 2^n-1 usuarios donde n es el grado del polinomio de pareja preferida.

Para las secuencias de *Walsh* se tiene que son perfectamente ortogonales ya que tienen valor de correlación cruzada de cero, pero presenta varios valores de autocorrelación en un mismo periodo de la secuencia.

En el caso de la concatenación de la secuencia *Walsh* con *Gold* se tiene que la secuencia resultante sigue presentando cierta propiedad de ortogonalidad ya que las correlaciones cruzadas no pasaron del valor normalizado de 0.2, se observa también como la autocorrelacion de la secuencia resultante tiene un solo valor máximo con lo que la sincronización del código es mas sencilla que la sincronización de las secuencias de *Walsh.*

IV Teoría de cuerpos finitos aplicada a la codificación de canal.

IV.1 Introducción.

El propósito de este capítulo es analizar los conceptos básicos asociados a la teoría de cuerpos finitos (*álgebra de Galois*) que nos ayudara a entender la parte de teoría de codificación. El *álgebra de Galois* es implementada en la construcción de los códigos que son usados para la codificación de canal, por lo que es importante estudiar este tema, ya que éstas son la bases para la realización del diseño del código corrector de errores, los cuales serán estudiados en el siguiente capítulo.

La teoría de cuerpos finitos es utilizada debido a la naturaleza discreta de la información digital y a su manipulación en bloques de tamaño fijo, los cuales son representados como polinomios pertenecientes a un cuerpo extensivo $GF(2^m)$, donde m es el tamaño en bits de los bloques de datos. Estos polinomios pueden ser operados con las propiedades definidas para dicho cuerpo finito.

IV.2 Definiciones.

A continuación se mencionarán los conceptos más importantes acerca de la teoría de cuerpos finitos.

IV.2.1 Grupo.

Un *grupo* es un sistema de elementos en el cual son definidas una operación matemática y su inversa, tales como suma y resta o multiplicación y división. Sí la operación definida es la suma, el sistema es llamado un grupo aditivo, y sí es la multiplicación, un grupo multiplicativo. Y se definirá a un grupo más formalmente como:

Un grupo está definido por la combinación de un conjunto G y una operación binaria. Una operación binaria * es descrita como una operación la cual toma dos elementos a y b y produce un resultado único $c = a * b$. Un grupo satisface las siguientes condiciones:

(i) La operación binaria * es asociativa.

(ii) G contiene un elemento e (*elemento identidad*) tal que para cualquier a de G:

$$a * e = e * a = a$$

(iii) Para cualquier elemento a de G existe otro elemento a′ (*inversa de a*) de G tal que:

$$a * a' = a' * a = e$$

Un grupo G es conmutativo si la operación binaria * satisface la siguiente condición:

$$a * b = b * a$$

Como ejemplo considérese los dos enteros $G=\{0,1\}$ y una operación binaria denotada por $\oplus$ (suma en módulo-2) en G como sigue:

$$0 \oplus 0 = 0, \quad 0 \oplus 1 = 1, \quad 1 \oplus 0 = 1, \quad 1 \oplus 1 = 0 \qquad (39)$$

Se demuestra que G es un grupo conmutativo sobre la suma en módulo-2. El elemento 0 es el elemento identidad. La inversa de 0 es el mismo y la inversa de 1 es también el mismo. Así G junto con $\oplus$ es un grupo conmutativo.

Al número de elementos en un grupo se le llama el *orden del grupo*, y un grupo puede ser de orden finito o infinito. Pero el grupo de vital importancia para nosotros es el grupo finito.

Se demuestra que para cualquier entero positivo m, el conjunto de enteros $G=\{0,1,2,3,\ldots\ldots,m-1\}$ es un grupo conmutativo y asociativo sobre la suma en módulo m. De igual manera se demuestra que para cualquier número primo p (2,3,5,7,11,.....), el conjunto de enteros $G=\{1,2,3,\ldots\ldots,p-1\}$ es conmutativo y asociativo bajo la multiplicación en módulo p [Lin y Costello, 1983]. Es importante destacar que si p no es primo el conjunto $G=\{1,2,3,\ldots\ldots,p-1\}$ no es un grupo bajo la multiplicación en módulo p.

Tabla II: Suma en módulo 5

⊕	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Tabla III: Multiplicación en módulo 5

*	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Los valores de la *Tabla II* fueron obtenidos de la siguiente manera: $i \oplus j = r$ (Para i y j en G). Donde r es el resultado del residuo de dividir $i + j$ por m. El residuo r es un entero entre 0 y $m-1$, por lo tanto está en G.

Los valores de la *Tabla III* fueron obtenidas de la siguiente manera: $i * j = r$ (Para i y j en G). Donde r es el resultado del residuo de dividir $i * j$ por p y $0 < r < p$, por lo tanto r es un elemento de G.

Un subconjunto S de los elementos en un grupo G es llamado un *subgrupo* de G si el mismo S es un grupo con respecto a la operación definida en G [Michelson, 1985].

IV.2.2 Campo.

Un campo es un conjunto de elementos en los cuales se pueden realizar sumas, restas, multiplicaciones y divisiones sin dejar el conjunto. Y se definirá a un campo más formalmente como:

Sea F un conjunto de elementos en la cual están definidas dos operaciones binarias, suma "+" y multiplicación "*". El conjunto F junto con las dos operaciones binarias forman un campo si las condiciones siguientes se satisfacen:

(i) F es un grupo conmutativo bajo la suma +. El *elemento identidad* con respecto a la suma es el elemento cero o *identidad aditiva* de F y es denotada por 0.

(ii) El conjunto de elementos distinto de cero en F es un grupo conmutativo bajo la multiplicación *. El elemento con respecto a la multiplicación es el *elemento unidad* o *identidad multiplicativa* de F y es denotado por 1.

(iii) La multiplicación es distributiva sobre la suma; esto es, para cualquiera de los tres elementos a, b y c en F:

$$a * (b + c) = a * b + a * c$$

El número de elementos en un campo es llamado el *orden del campo*. Un campo con número finito de elementos se le llama *campo finito*. Un campo finito es llamado un *campo de Galois*[1] y es denotado por *GF(q)*, donde q es el número de elementos en el campo. Un campo finito GF(P^m) existe para cualquier P^m, donde P es un primo y m es un entero. El ejemplo puro de un campo finito es un *campo primo,* GF(p), consiste del conjunto de todos los enteros en módulo p, donde p es cualquier *número primo* más grande que 1 y las operaciones suma y multiplicación son realizadas en módulo p [Michelson, 1985].

[1]Es nombrado *campo de Galois* en honor al matemático francés Evariste Galois (1811-1832).

Para cualquier primo p existe un campo finito de p elementos, para cualquier entero positivo m, éste es posible de extender el campo primo GF(q) a un campo de q^m elementos el cual es llamado un *campo extensión* de GF(q) y es denotado por GF(q^m).

La *característica* de un campo GF(q) es el entero positivo λ que cumple la siguiente condición:

$$\sum_{i-1}^{\lambda} 1 = 0 \qquad (40)$$

Se demuestra que la característica (λ) de un capo finito es un número primo. Y GF(λ) es llamado un *subcampo* de GF(q), por lo tanto cualquier campo finito GF(q) de característica λ contiene un subcampo de λ elementos [Lin y Costello, 1983].

El *orden de un elemento a* del campo es el menor entero positivo n que cumpla con $a^n=1$.

En un campo finito GF(q) un elemento a diferente de cero es *primitivo* si el orden de a es $q-1$ (en un campo finito puede haber más de un elemento primitivo). Por lo tanto la potencia de un elemento primitivo genera todos los elementos diferentes de cero de GF(q).

Como ejemplo considere el campo primo GF(7)={0,1,2,3,4,5,6} y la operación multiplicación en módulo-7. La característica de este campo es 7. Si tomamos el elemento 3 de GF(7), se observa que este elemento tiene orden 6. Y como la potencia es $q-1$ se dice que es un elemento primitivo.

$3^1=3$, $3^2=3\cdot3=2$, $3^3=3\cdot3^2=6$, $3^4=3\cdot3^3=4$, $3^5=3\cdot3^4=5$ $3^6=3\cdot3^5=1$

Un grupo se dice que es *cíclico* si existe un elemento en el grupo cuya potencia constituye el grupo completo.

Teorema 4.1: Sea a un elemento no cero de un campo finito GF(q). Entonces $a^{q-1}=1$.

Teorema 4.2: Sea a un elemento no cero de un campo finito GF(q). sea n el orden del elemento a. Entonces n divide a $q-1$.

Este último teorema nos indica que n debe dividir a $q-1$.

IV.3 Aritmética del campo binario.

En general podemos construir códigos con símbolos de cualquier campo de Galois GF(q), donde q es un primo P o una potencia de p. Sin embargo los códigos con símbolos del campo binario GF(2) o su extensión GF(2^m) son más usados en transmisiones digitales de datos porque la información en estos sistemas es codificada en forma binaria [Lin y Costello, 1983].

Una vez que se conocen todos los elementos del campo, se pueden adoptar varias notaciones para su representación: *notación exponencial*, *notación polinómica* o *notación vectorial*. En la notación exponencial los elementos del campo se representan como las sucesivas potencias del elemento primitivo. En la notación polinómica cada elemento tiene asociado un polinomio y en la notación vectorial , los coeficientes del polinomio de la representación polinómica se ordenan en forma de vector binario.

Los polinomios del campo binario GF(2), son representados de la siguiente forma:

$$f(X) = f_0 + f_1X + f_2X^2 + \cdots\cdots + f_nX^n \qquad (41)$$

Donde $f_i = 0$ ó 1 para $0 \leq i \leq n$. El *grado de un polinomio* es el grado de mayor orden de X con coeficiente diferente de cero. Los polinomios con coeficientes de GF(2)

pueden ser sumados, restados, multiplicados y divididos de la misma forma que los polinomios tradicionales, teniendo en cuenta que las operaciones se realizan en módulo-2.

Por ejemplo para sumar $f(X) = 1+X+X^3+X^5$ y $g(X) = 1+X^2+X^3+X^4+X^7$, se obtiene la siguiente suma:

$$f(X) + g(X) = (1+1) + X + X^2 + (1+1)X^3 + X^4 + X^5 + X^7$$
$$= X + X^2 + X^4 + X^5 + X^7$$

Para multiplicar los polinomios $f(X)$ y $g(X)$ se obtiene de la siguiente forma:

$$f(X) * g(X) = (1 + X + X^3 + X^5) * (1 + X^2 + X^3 + X^4 + X^7)$$
$$= 1+X^2+X^3+X^4+X^7+X+X^3+X^4+X^5+X^8+X^3+X^5+X^6+X^7+X^{10}+X^5+X^7+X^8+X^9+X^{12}$$
$$= 1 + X + X^2 + X^3 + X^5 + X^6 + X^7 + X^9 + X^{10} + X^{12}$$

IV.4 Polinomios con coeficientes de GF(2). Polinomios primitivos.

Cuando un polinomio $f(X)$ es dividido por $g(X)$, si el residuo $r(X)$ es igual a cero $\{r(X)=0\}$, se dice que $f(X)$ es *divisible* por $g(X)$ y $g(X)$ es un factor de $f(X)$.

Un polinomio $f(X)$ bajo GF(2) de grado m se dice que es *irreducible* bajo GF(2) si $f(X)$ no es divisible por cualquier otro polinomio bajo GF(2) o de un grado menor que m pero diferente de cero.

Como ejemplo de los cuatro polinomios de grado 2, X^2, X^2+1 y X^2+X no son irreducibles ya que o son divisibles por X o por $X+1$. Sin embargo, X^2+X+1 no tiene a 0 ni a 1 como raíz y por lo tanto no es divisible por ningún polinomio de grado 1.

Teorema 4.3: Cualquier polinomio irreducible sobre GF(2) o de grado m divide a:

$$X^{2^m-1} + 1$$

Un *polinomio primitivo* de grado n es aquel polinomio irreducible que divide a X^k+1 con $K=2^n-1$, pero no divide a X^m+1 con $m<2^n-1$. Como ejemplo se tiene un polinomio $p(X) = X^4+X+1$ el cual divide a $X^{15}+1$, y no divide a ninguno polinomio del tipo X^n+1 por lo que se habla de un polinomio primitivo.

Un polinomio primitivo debe cumplir con las siguientes condiciones:

(i) Debe tener términos independientes (sino sería divisible por X).

(ii) Debe tener un número impar de coeficientes iguales a 1 (sino sería divisible por $X+1$).

(iii) Debe tener algún termino de grado impar.

(iv) Algún coeficiente debe ser cero.

Para una m dada puede existir más de un polinomio primitivo de grado m [Steele, 1992]. En la *Tabla IV* se muestran los polinomios con el menor número de términos.

Tabla IV: Polinomios primitivos bajo GF(2).

M		M	
3	$1+X+X^3$	14	$1+X+X^6+X^{10}+X^{14}$
4	$1+X+X^4$	15	$1+X+X^{15}$
5	$1+X^2+X^5$	16	$1+X+X^3+X^{12}+X^{16}$
6	$1+X+X^6$	17	$1+X^3+X^{16}$
7	$1+X^3+X^7$	18	$1+X^7+X^{18}$
8	$1+X^2+X^3+X^4+X^8$	19	$1+X+X^2+X^5+X^{19}$
9	$1+X^4+X^9$	20	$1+X^3+X^{20}$
10	$1+X^3+X^{10}$	21	$1+X^2+X^{21}$
11	$1+X^2+X^{11}$	22	$1+X+X^{22}$
12	$1+X+X^4+X^6+X^{12}$	23	$1+X^5+X^{23}$
13	$1+X+X^3+X^4+X^{13}$	24	$1+X+X^2+X^7+X^{24}$

IV.5 Construcción de campos de Galois GF(2).

A continuación presentaremos un método para construir el campo de Galois de 2^m elementos ($m>1$) del campo binario GF(2). Empezaremos con dos elementos 0 y 1, de GF(2) y un nuevo símbolo α y la operación de multiplicación. De esta forma se introduce una secuencia de potencias de α siguiente:

$$0 * 0 = 0$$
$$0 * 1 = 1 * 0 = 0$$
$$1 * 1 = 1$$
$$0 * \alpha = \alpha * 0 = 0$$
$$1 * \alpha = \alpha * 1 = \alpha$$
$$\alpha^2 = \alpha * \alpha$$
$$\alpha^3 = \alpha * \alpha * \alpha$$
$$\vdots$$
$$\alpha^j = \alpha * \alpha * \alpha * \ldots \alpha \quad \text{(j veces)} \qquad (42)$$
$$\vdots$$

A continuación se tiene el siguiente conjunto de elementos en el cual una operación de multiplicación es definida $F = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^j, \ldots\}$ e imponiendo la condición en el elemento α de manera que el conjunto F contiene únicamente 2^m elementos y es cerrado bajo la multiplicación de las ecuaciones 42. Sea $p(X)$ un polinomio primitivo de grado m bajo GF(2). Asumiendo que $p(\alpha) = 0$ y que $p(X)$ divide a $X^{2^m-1}+1$ se obtiene:

$$\alpha^{2^m-1} = 1$$

Por lo tanto bajo la condición de $p(\alpha) = 0$, el conjunto F se convierte en finito y contiene los siguientes elementos:

$$F^* = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{2^m-2}\}$$

Los elementos diferentes de cero de F^* son cerrados bajo la operación de multiplicación.

Como ejemplo de construcción de un campo se presenta el cuerpo con m = 4, $GF(2^4) = GF(16)$ generado por el polinomio primitivo bajo GF(2) $p(X) = 1 + X + X^4$. Como $p(\alpha) = 1 + \alpha + \alpha^4 = 0$, entonces la igualdad $\alpha^4 = 1 + \alpha$ es implementada para construir los elementos de $GF(2^4)$. Por ejemplo:

$$\alpha^5 = \alpha * \alpha^4 = \alpha * (1 + \alpha) = \alpha + \alpha^2$$

$$\alpha^6 = \alpha * \alpha^5 = \alpha * (\alpha + \alpha^2) = \alpha^2 + \alpha^3$$

$$\alpha^7 = \alpha * \alpha^6 = \alpha * (\alpha^2 + \alpha^3) = \alpha^3 + \alpha^4 = \alpha^3 + 1 + \alpha = 1 + \alpha + \alpha^3$$

De esta manera en la *Tabla V* se obtiene la representación de todos los elementos del campo que se presentan, según las diferentes notaciones posibles.

Tabla V: Elementos del campo $GF(2^4)$generado por $P(X)=1+X+X^4$.

Representación Exponencial	Representación Polinómica	Representación Vectorial
0	0	0 0 0 0
1	1	1 0 0 0
α	X	0 1 0 0
α^2	X^2	0 0 1 0
α^3	X^3	0 0 0 1
α^4	1 + X	1 1 0 0
α^5	$X + X^2$	0 1 1 0
α^6	$X^2 + X^3$	0 0 1 1
α^7	$1 + X + X^3$	1 1 0 1
α^8	$1 + X^2$	1 0 1 0
α^9	$X + X^3$	0 1 0 1
α^{10}	$1 + X + X^2$	1 1 1 0
α^{11}	$X + X^2 + X^3$	0 1 1 1
α^{12}	$1 + X + X^2 + X^3$	1 1 1 1
α^{13}	$1 + X^2 + X^3$	1 0 1 1
α^{14}	$1 + X^3$	1 0 0 1

La ventaja de tener diferentes representaciones se hace evidente al realizar operaciones con las diferentes representaciones. La representación exponencial es conveniente para las operaciones de multiplicación y la representación polinómica es conveniente para las operaciones tipo sumas. Por lo tanto para multiplicar dos elementos α^i y α^j simplemente se suman los exponentes teniendo en cuenta que $\alpha^{15}= 1$. Por ejemplo, $\alpha^5 * \alpha^7 = \alpha^{12}$ y $\alpha^{12} * \alpha^7 = \alpha^{19} = \alpha^4$. Para dividir α^j por α^i simplemente multiplicamos α^j por la inversa multiplicativa de α^{15-i} de α^i. Por ejemplo, $\alpha^4/\alpha^{12} = \alpha^4 * \alpha^3 = \alpha^7$. Para sumar α^i y α^j se implementan las representaciones polinómicas de la *Tabla V*. Por ejemplo, $\alpha^5 + \alpha^7 = (X + X^2) + (1 + X + X^3) = 1 + X^2 + X^3 = X^{13}$.

IV.6 Propiedades básicas del campo de Galois GF(2^m).

En la aritmética ordinaria a menudo se observa que un polinomio con coeficientes reales no tiene raíces del campo de los números reales pero tiene raíces del campo de los números complejos, que contiene el campo de los números reales como un subcampo. Esto es igual para polinomios con coeficientes de GF(2). En este caso un polinomio con coeficientes de GF(2) no puede tener raíces de GF(2) pero tiene raíces de un campo extensión de GF(2) [Lin y Costello, 1983].

Por ejemplo: sea $f(X) = X^4 + X^3 + 1$ es irreducible sobre GF(2) y por lo tanto este no tiene raíces de GF(2). Sin embargo este tiene cuatro raíces del campo GF(2^4). Sustituyendo el elemento de GF(2^4) dentro de $f(X)$ se encuentra que α^7, α^{11}, α^{13} y α^{14} son raíces de $f(X)$. Esto se puede verificar sustituyendo las raíces en $f(X)$.

$$f(\alpha^7)=(\alpha^7)^4+(\alpha^7)^3+1=\alpha^{28}+\alpha^{21}+1=(1+\alpha^2+\alpha^3)+(\alpha^2+\alpha^3)+1=0$$ y de igual manera se haría para las raíces restantes. Entonces:

$$(X+\alpha^7)\,(X+\alpha^{11})\,(X+\alpha^{13})\,(X+\alpha^{14}) = X^4 + X^3 + 1$$

Las características de las raíces quedan definidas en las siguientes propiedades:

Teorema 4.4: Sea *f(X)* un polinomio con coeficientes de GF(2) y β un elemento de un campo extensión de GF(2). Si β es una raíz de *f(X)*, entonces para cualquier l≥0, β^{2^l} es también una raíz de *f(X)*

El elemento β^{2^l} es llamado el *conjugado* de β (el conjugado empieza a repetirse a partir de *l>m-1*). El teorema anterior dice que si β es un elemento de GF(2^m), una raíz de un polinomio de *f(X)* sobre GF(2), entonces todos los distintos conjugados de β, también son elementos de GF(2^m), raíces de *f(X)* [Covarrubias y Diaz, 1999].

Ejemplo: sea $f(X) = 1 + X^3 + X^4 + X^5 + X^6$ no tiene raíces de GF(2), pero se puede apreciar que tiene a α^4 un elemento de GF(2^4) como una raíz. Para verificar ésto se sigue el mismo procedimiento del ejemplo anterior.

$$f(\alpha^4)=1+\alpha^{12}+\alpha^{16}+\alpha^{20}+\alpha^{24}=1+\alpha^{12}+\alpha+\alpha^5+\alpha^9$$
$$=1+(1+\alpha+\alpha^2+\alpha^3)+\alpha+(\alpha+\alpha^2)+(\alpha+\alpha^3)=0$$

Los conjugados de α^4 son $(\alpha^4)^2=\alpha^8$, $(\alpha^4)^{2^2}=\alpha^{16}$, $(\alpha^4)^{2^3}=\alpha^{32}=\alpha^2$ se puede ver que α^8, α^{16}y α^2 también son raíces de *f(X)*.

Propiedad 1: Como todo elemento β de GF(2^m) es una raíz del polinomio $X^{2^m}+X$, β puede ser una raíz del polinomio bajo GF(2) con un grado menor que 2^m. Sea $\phi(X)$ el polinomio de grado menor bajo GF(2) tal que $\phi(\beta)=0$. Este polinomio $\phi(X)$ es llamado el *polinomio mínimo* de β.

El polinomio mínimo de β es único, y diferentes elementos de un campo pueden tener el mismo polinomio mínimo. Además, para todo elemento de GF(2^m), el grado del polinomio mínimo sobre GF(2^m) es como máximo m.

Teorema 4.5: sea $f(X)$ un polinomio irreducible bajo GF(2). Sea β un elemento en GF(2^m). Sea $\phi(X)$ el polinomio mínimo de β. Si $f(\beta)=0$, entonces $\phi(X)=f(X)$.

El teorema 4.5 dice que si un polinomio irreducible tiene a β como una raíz. $\phi(X)$ es el polinomio mínimo de β. Y del teorema 4.4 que β y sus conjugados son todas las raíces de $\phi(X)$. sea e el entero más pequeño tal que $\beta^{2^e}=\beta$. Entonces $\beta^2, \beta^{2^2}, \ldots\ldots, \beta^{2^{e-1}}$ son todos los conjugados distintos de β. Por lo que $\beta^{2^m}=\beta$, $e \le m$.

Teorema 4.6: Sea β un elemento de GF(2^m) y e el entero no negativo más pequeño tal que $\beta^{2^e}=\beta$. Entonces

$$f(X)=\prod_{i=0}^{e-1}(X+\beta^{2^i})$$ Es un polinomio irreducible bajo GF(2).

Se puede observar del teorema 4.5 y 4.6 que $f(X)=\phi(X)=\prod_{i=0}^{e-1}(X+\beta^{2^i})$

Ejemplo: Considere el campo de Galois GF(2^4). Sea $\beta=\alpha^3$. Los conjugados de β son:

$$\beta^2=\alpha^6, \qquad \beta^{2^2}=\alpha^{12}, \qquad \beta^{2^3}=\alpha^9$$

el polinomio mínimo de $\beta=\alpha^3$ es entonces

$$\phi(X)=(X+\alpha^3)(X+\alpha^6)(X+\alpha^{12})(X+\alpha^9)$$

Teorema 4.7: Si β es un elemento primitivo de GF(2^m), todos sus conjugados son también elementos primitivos de GF(2^m).

IV.7 Espacio vectorial.

El concepto de espacio vectorial está relacionado con el álgebra lineal y teoría de matrices de las matemáticas. Un espacio vectorial bajo un campo F satisface las siguientes condiciones:

(i) V es un grupo conmutativo bajo la suma.

(ii) Para cualquier elemento a de F y cualquier elemento v en V, $a \bullet v$ es un elemento de V.

(iii) (ley distributiva) para cualquier elemento u y v de V y cualquier elemento a y b de F.

$$a \bullet (u + v) = a \bullet u + a \bullet v$$

$$(a + b) \bullet v = a \bullet v + b \bullet v$$

(iv) (ley asociativa) para cualquier v de V y cualquier a y b de F.

$$(a \bullet b) = a \bullet (b \bullet v)$$

(v) Sea 1 el elemento unidad de F. Entonces, para cualquier v de V, $1 \bullet v = v$

El elemento de V es llamado *vector* y el elemento del campo F es llamado *escalar*. La suma en V es llamada suma vectorial y la multiplicación que combina un escalar de F y un vector de V dentro de un vector de V es referida como una multiplicación escalar (producto).

Una forma muy usada para implementar un espacio vectorial bajo GF(2) es la que se muestra a continuación: $(a_o, a_1, \ldots\ldots, a_{n-1})$, donde cada componente a_i es un elemento del campo binario GF(2) ($a_i = 0$ ó 1). Esta secuencia es generalmente llamada una *n-tuple* bajo GF(2).

Teorema 4.8: Sea S un subcampo no vacío de un espacio vectorial V bajo un campo F. Entonces S es un subespacio si las siguientes condiciones se satisfacen:

(i) Para dos vectores cualesquiera u y v de S, u + v es también un vector de S.

(ii) Para ningún elemento a de F y cualquier vector u de S, a•u es también un vector de S.

Un conjunto de vectores se dice ser parte de un espacio vectorial V si cada vector de V es una combinación lineal del vector del conjunto. En cualquier espacio vectorial o subespacio existe al menos un conjunto B de vectores linealmente independientes. Este conjunto es llamado una base del espacio vectorial. El número de vectores en una base de un espacio vectorial es llamado la dimensión del espacio vectorial.

Sea $u = (u_0, u_1,.....,u_{n-1})$ y $v = (v_0, v_1,.....,v_{n-1})$ dos n-tuples de V_n. Definiendo el producto interno de u y v como:

$$u \bullet v = u_0 \bullet v_0 + u_1 \bullet v_1 + ...+ u_{n-1} \bullet v_{n-1}$$

Donde $u_i \bullet v_i$ y $u_i \bullet v_i + u_{i+1} \bullet v_{i+1}$ son multiplicados y sumados en suma en módulo-2. De aquí el producto interno u•v es un escalar de GF(2). Si u•v = 0, u y v se dicen ser ortogonales.

IV.8 Conclusiones.

Como se mencionó la teoría de cuerpos finitos es una herramienta que se implementa en las operaciones que se realizan cuando la información es codificada y cuando se verifica que la información no tenga ningún error de transmisión, ésto es posible ya que la información a transmitir es digital y es mucho más sencilla la manipulación de las operaciones por medio de la teoría de cuerpos finitos.

Se puede llegar a concluir que hay tres sistemas algebraicos que son fundamentales en la teoría de detección de error y códigos correctores de error: grupos, campo y espacio vectorial. El tipo de grupo que es de central interés para nosotros es el grupo aditivo compuestos de elementos que son palabras códigos.

La principal ventaja de tener diferentes representaciones se hace evidente al realizar operaciones con las diferentes representaciones. Por ejemplo para las operaciones de multiplicación es conveniente implementar la representación exponencial y la representación polinómica para las operaciones tipo sumas.

V Codificación de canal.

V.1 Introducción.

En 1948 *Shannon* demostró la existencia de códigos correctores de error que bajo condiciones apropiadas y a velocidades menores que la capacidad del canal, permitirían la transmisión de la información libre de errores. A partir de ese momento, se ha iniciado la búsqueda de códigos correctores de error eficientes y hasta la fecha el proceso de investigación continua vigente.

Es evidente que la codificación de canal juega un papel muy importante para garantizar la integridad de la información en los sistemas de comunicación, ya que en la actualidad no existe un único codificador de canal, que satisfaga todos los requerimientos de calidad servicio (Q_oS), es necesario pues implementar diferentes tipos de codificación para los diferentes tipos de servicio (datos, voz y multimedia). Para ello, se tienen que tomar en cuenta varios factores, por ejemplo, las características deseadas para el sistema en cuanto a retardo y a *BER* o probabilidad de error del canal, las cuales varían según el tipo de servicio requerido.

El tipo de canal también influye en la elección del tipo de código a utilizar, ya que las características de transmisión y error son diferentes según el tipo de canal. En canales sin memoria, el ruido afecta a cada símbolo transmitido de manera independiente (errores de tipo aleatorios), mientras que en un canal con memoria el ruido no es independiente de una transmisión a otra. Este tipo de canal está la mayor parte del tiempo en un estado en donde la transmisión de errores es poco frecuente, y tan sólo en alguna ocasión, las características del canal cambian y se pasa a un estado donde la probabilidad de error de transmisión es alta. En este caso es cuando se presentan los errores de tipo a ráfagas en la transmisión de los datos. Por lo que es adecuado realizar un estudio y análisis de los diferentes tipos de códigos para definir cual de éstos es el apropiado para cada servicio.

El objetivo de la codificación de canal es aumentar la confiabilidad de los datos recibidos, con una rápida decodificación. Para lo cual es necesario añadir redundancia al mensaje del usuario obteniendo lo que se conoce como palabra código. Al agregar bits de redundancia se trae como consecuencia el incremento del ancho de banda del sistema, pero proporciona excelente eficiencia del *BER* a bajos valores de *SNR*.

Los códigos de canal que son implementados para detectar errores son llamados *códigos detectores de error,* mientras que los códigos que pueden detectar y corregir errores son llamados códigos correctores de error [Rappaport, 1996].

Las funciones de codificación y decodificación envuelven las operaciones aritméticas de la teoría de cuerpos finitos o álgebra de *Galois*, de aquí la importancia del estudio de la teoría de cuerpos finitos, la cual fue estudiada en capítulos anteriores.

Un codificador de canal opera sobre datos digitales para codificar la fuente de información dentro de una secuencia código que es transmitida en el canal. Existen dos tipos principales de código, los códigos bloque y los códigos convolucionales. Como se ha venido mencionando el tipo de código a utilizar depende del tipo de información a manejar (Datos, Voz, Video o Imagen), del canal (canal con memoria o sin memoria), las velocidades de transmisión, el retardo tolerable, la calidad o *BER* exigida, tipo de ruido (aleatorio o ráfagas) y del compromiso del decodificador (sencillez en su implementación). Por lo que para un servicio requerido el tipo de código ya está bastante definido [Covarrubias, 1999].

El objetivo de este capítulo es proporcionar los conocimientos fundamentales que están relacionados con los códigos bloque, tales como propiedades, características, parámetros y aplicaciones más importantes de los códigos bloque. Es importante destacar que durante el tiempo que se ha estado trabajando en este trabajo de tesis, existe otro

trabajo de tesis paralelo a éste, en el cual se está trabajando con códigos convolucionales, por este motivo nosotros no abordaremos el análisis de los códigos convolucionales.

V.2 Esquemas básicos de control de errores.

Para resolver los problemas del canal radio los sistemas actuales implementan protocolos con técnicas de detección y corrección de error en los que el caudal eficaz disminuye o el sistema no es fiable. Las técnicas de control de error que utilizan estos sistemas son:

- *ARQ* (*Automatic Repeat reQuest*)
- *FEC* (*Forward Error Control*)

V.2.1 FEC.

En los sistemas de control de error *FEC* se implementa un código corrector de errores bloque o convolucional para contrarrestar los errores introducidos por el canal. Cuando el receptor detecta la presencia de errores en un vector recibido, éste procura encontrar la localidad de los errores y entonces corregirlos. Si la localización exacta de los errores es encontrada, el vector recibido será decodificado correctamente, si el receptor falla al encontrar la localización de los errores, el vector recibido será decodificado incorrectamente y los datos que se entregarán al usuario final son erróneos. Debido a que el esquema *FEC* no emplea retransmisiones cuando el vector recibido no puede ser decodificado correctamente, el *Throughput* del sistema se mantiene constante, e igual a la velocidad del código, independientemente de la tasa de error del canal. Pero presenta un problema muy critico en la transmisión de datos que es la confiabilidad del sistema, cuando la tasa de error del canal aumenta la confiabilidad disminuye.

V.2.2 ARQ.

En un sistema *ARQ* es utilizado un código con buena capacidad de detección de error. En el receptor, el síndrome del vector recibido es calculado. Si el síndrome es cero, el vector recibido está libre de errores y es aceptado por el receptor. Al mismo tiempo el receptor notifica al transmisor por un enlace de retorno, que el vector código transmitido ha sido recibido correctamente. Si el síndrome es diferente de cero, se detectó un error en el vector recibido. Entonces la transmisión es interrumpida, para retransmitir el mismo vector código, continuando la transmisión hasta que el vector código es recibido correctamente. Por lo que un sistema *ARQ* proporciona una confiabilidad muy elevada pero el *Throughput* depende fuertemente de la calidad del canal, por lo que trae como consecuencia una disminución del *Throughput* cuando aumenta la tasa de error del canal.

A partir de las limitaciones de los sistemas *ARQ* y *FEC*, surge la necesidad de combinar las ventajas de ambos sistemas (confiabilidad y alto *Throughput*), por lo que surgen los sistemas *ARQ híbridos*.

V.2.3 Esquemas Híbridos.

Un sistema *ARQ* híbrido consiste de un subsistema *FEC* contenido dentro del sistema *ARQ*. La función del sistema *FEC* es proporcionar capacidad de corrección de error sin que el sistema se vea en la necesidad de pedir una retransmisión del vector transmitido. Cuando los errores del canal sobrepasan la capacidad de corrección del código *FEC*, el sistema *ARQ* interrumpe la transmisión de los datos y pide una retransmisión del vector transmitido. Con esto el sistema mantiene un *Throughput* elevado y lo principal se asegura la confiabilidad del sistema en la transmisión de los datos.

V.2.3.1 ARQ híbrido tipo I.

El funcionamiento del esquema *ARQ híbrido tipo I* es básicamente el mencionado anteriormente, utiliza un solo código. Cuando una palabra recibida se detecta con error, el receptor primero intenta la corrección de los errores. Si el número de errores está dentro de

la capacidad de corrección del código, los errores serán corregidos y entregados al usuario correctamente. Si los errores encontrados en la palabra recibida sobrepasan la capacidad de corrección del código, el receptor descarta la palabra recibida y solicita la retransmisión de la misma palabra código. Cuando la palabra retransmitida es recibida, el receptor intenta de nuevo la corrección de los errores (sí es que ocurrieron errores durante la retransmisión). Si la decodificación nuevamente no tiene éxito, el receptor vuelve a descartar la palabra recibida y solicita otra retransmisión. Este proceso continua hasta que la palabra código es recibida correctamente

Dado que la corrección de error se basa siempre en el mismo código, este esquema suele denominarse *ARQ híbrido* de velocidad fija. Una velocidad de corrección fija no es útil en un entorno de comunicaciones móviles donde el canal varia fuertemente. Si el canal introduce pocos errores, la redundancia del código resultará excesiva. Por otro lado, si el canal introduce muchos errores, sobrepasará la capacidad de corrección del código y habrá que realizar un gran número de retransmisiones disminuyendo el *Throughput.*

Para resolver el problema mencionado anteriormente se requiere que la velocidad del código corrector sea capaz de adaptarse a las condiciones del canal, dando lugar con ello al código *ARQ híbrido tipo II.*

V.2.3.2 ARQ híbrido tipo II.

Como se mencionó anteriormente, el sistema *ARQ híbrido tipo II* se basa en el concepto de que los dígitos de verificación de paridad para la corrección de error son enviados únicamente cuando son necesitados. En este tipo de esquema se utilizan dos códigos lineales, uno es un código C_0 *(n, k)* de alta velocidad el cual únicamente es diseñado para la detección de error, el otro es un código invertible de media velocidad C_1 *(2k, k)* el cual tiene la función de detectar y corregir errores simultáneamente. Un código se dice ser invertible si, conociendo únicamente los bits de verificación de paridad de un

vector código, los correspondientes bits de información pueden ser determinados por un proceso de inversión.

V.2.3.2.1 Códigos invertibles de media velocidad.

La propiedad de invertible en los códigos facilita el proceso de recuperación de los datos. El proceso de inversión también reduce la frecuencia de retransmisión, mejorando así el *Throughput* del sistema. A continuación se describe el proceso de inversión [Lin y Costello, 1983].

Sea C un código cíclico (n, k) con $n\text{-}k<k$. Sea $g(x)$ el polinomio generador de C con la forma: $g(X)=1+g_1X+g_2X^2+\ldots+g_{n-k-1}X^{n-k-1}+X^{n-k}$, y sea $v(x)$ el polinomio código ($v(X)=v_0+v_1X+v_2X^2+\ldots+v_{n-1}X^{n-1}$). En forma sistemática, los k coeficientes de mayor peso $v_{n-k}, v_{n-k-1}, \ldots, v_{n-1}$ son idénticos a los k bits de información mientras que los $n\text{-}k$ coeficientes de menor peso $v_0, v_1, \ldots, v_{n-k-1}$ son los dígitos de verificación de paridad. Considérese el conjunto de aquellos vectores código en C cuyos $2k–n$ componentes de mayor peso $v_{2(n-k)}, v_{2(n-k)+1}, \ldots, v_{n-1}$ son cero. Existen 2^{n-k} vectores código de este tipo en C. Si los $2n\text{-}k$ componentes de mayor peso de valor cero se eliminan de estos vectores, obteniendo un conjunto de 2^{n-k} vectores de longitud $2(n\text{-}k)$. Estos vectores forman un código $(2n\text{-}2k, n\text{-}k)$ cíclico recortado de media velocidad C_1. Este código cíclico recortado tiene al menos la misma capacidad de corrección de error que C.

Ahora observemos como el código cíclico recortado C_1 tiene la propiedad de invertible. Sea $u(X)=u_0+u_1X+u_2X^2+\ldots+u_{n-k-1}X^{n-k-1}$ el mensaje a codificar. Como se verá más adelante (códigos cíclicos) el polinomio código para $u(X)$ será:

$$w(X)=b(X)+X^{n-k}u(X) \qquad (43)$$

donde $b(X)$ es el polinomio de verificación de paridad. Como en un código cíclico recortado de media velocidad no existen dos vectores código con los mismos bits de

verificación de paridad, el polinomio $b(X)$ es único, lo que implica una correspondencia uno a uno entre el mensaje $u(X)$ y su verificación de paridad $b(X)$.

De la siguiente expresión se ve que el mensaje $u(X)$ es simplemente el residuo de dividir $b(X)X^k$ por el polinomio generador $g(X)$.

$$b(X)X^k = [u(X)h(X) + a(X)X^k]g(X) + u(X) \qquad (44)$$

donde $h(X) = (X^n + 1)/g(X)$.

V.2.4 Códigos concatenados.

La concatenación de códigos es un método especifico para la construcción de códigos largos a partir de códigos más cortos y es en ésto en lo que se fundamentan los sistemas esquemas híbridos.

Un código concatenado simple está formado por dos códigos , un código C_1 (n_1, k_1) binario llamado código interno (*Inner encoder*) y un código C_2 (n_2, k_2) no binario con símbolos pertenecientes a $GF(2^{k_1})$ llamado código externo (*Outer encoder*). Si la distancia mínima del código externo es d_1 y la distancia mínima del código interno es d_2, la distancia mínima del sistema concatenado es de al menos $d_1 d_2$. La codificación se lleva a cabo en dos pasos como se muestra en la *Figura 28*.

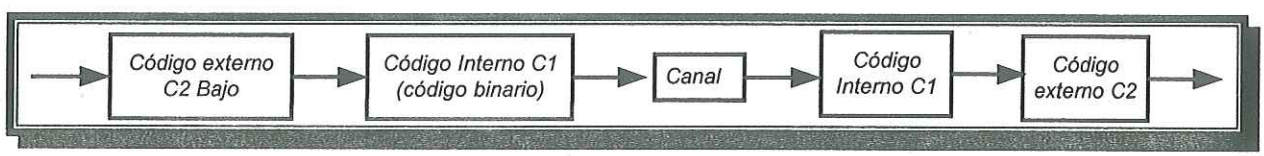

Figura 28: Sistema de comunicación utilizando un código concatenado.

1.- Los dígitos de información binario $k_1 k_2$ son divididos dentro de k_2 símbolos de k_1 dígitos de información cada uno. Estos k_2 símbolos son codificados acorde a las reglas de C_2 para formar un vector código de n_2 símbolos.

2.- Cada k_1 símbolos es codificado dentro de un vector código en C_1, resultando un flujo de n_2 vectores código de C_1, un total de $n_1 n_2$ dígitos. Estos dígitos son entonces transmitidos, en un vector código de C_1 en un tiempo de manera sucesiva. Dando como resultado un código lineal binario $(n_1 n_2, k_1 k_2)$.

Este tipo de codificación se caracteriza por tener una longitud de bloque que puede ser muy grande, la velocidad del código puede ser bastante baja $(R = k_1 k_2 / n_1 n_2)$, la complejidad del decodificador se ve bastante reducida, ya que el decodificador es separado en dos fases.

V.3 Códigos bloque.

Los códigos bloque son códigos *FEC* (*Forward Error Correction*) que detectan y corrigen un número limite de errores sin retransmisión. En este tipo de código, el codificador acepta un mensaje de *k* bits y genera una palabra código de *n* bits. Es decir las palabras código se producen bloque a bloque, siendo $n > k$ ya que se está añadiendo confiabilidad (bits de redundancia) a la transmisión de los datos a transmitir, tal como se muestra en la *Figura 29*.

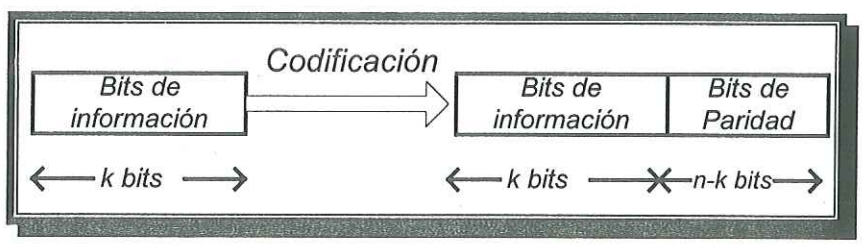

Figura 29: Codificación bloque.

Un mensaje a codificar es representado por la *k*-tupla $u=(u_1,u_2,...,u_k)$ llamada comúnmente como un mensaje. Por lo que existe un total de 2^k posibles mensajes diferentes a codificar. La palabra código es representada por una *n*-tupla $v=(v_1,v_2,...,v_n)$. Por lo tanto, a los correspondientes 2^k posibles mensajes diferentes, existen 2^k posibles diferentes palabras código en la salida del codificador, las 2^k palabras código deben ser distintas. Por lo tanto existe una correspondencia uno a uno entre un mensaje *u* y su palabra código *v*. Este conjunto de 2^k palabras código de longitud *n* son llamadas un *código bloque (n, k)*. La razón $R_c = k/n$ (donde $R_c \leq 1$) es llamada la velocidad del código.

Además del parámetro de velocidad del código R_c, existen otros parámetros importantes, tales como la distancia del código que es la que determina la capacidad correctiva del código y el peso del código. Todos estos parámetros serán definidos en los próximos apartados.

V.3.1 Códigos bloque lineales.

Para un código con 2^k palabras código de longitud *n*, la parte de codificación será demasiado compleja si *k* y *n* son grandes, ya que tiene que almacenar las 2^k palabras código de longitud *n* en una tabla de almacenamiento, por lo tanto, se trabajará con códigos bloque que tengan una *estructura lineal* (*códigos bloque lineales*), los cuales reducen la complejidad de la codificación y decodificación.

A un código bloque de longitud *n* y 2^k palabras código se les conoce como códigos lineales (*n, k*) si y sólo si sus 2^k palabras código forman un subespacio *k*-dimencional del espacio vectorial de las *n*-tuplas sobre el campo *GF(2)*. De hecho, un código bloque es lineal si y sólo si la suma en *módulo 2* de dos palabras código es también una palabra código.

Dado que un código lineal C (n, k) es un subespacio k-dimensional del espacio de vectores v_n de las n-tuplas binarias, es posible encontrar k palabras código linealmente independientes (*base*), $g_0, g_1, ..., g_{k-1}$ en C, de tal forma que cada palabra código v en C es una combinación lineal de esas k palabras código. esta idea da como resultado la siguiente representación matricial:

$$v = u \cdot G \qquad (45)$$

donde u es el mensaje a ser codificado, v la palabra código resultante y G la matriz generadora de dimenciones *Kxn,* que contiene el vector g como filas. Por lo tanto, un código lineal está completamente definido por las k filas de la matriz generadora G. Como consecuencia de esto, el codificador solo tiene que almacenar las k filas de G y formar una combinación lineal de estas k filas basadas en el mensaje de entrada, dando como resultado la siguiente matriz generadora.

$$G = \begin{bmatrix} g_0 \\ g_1 \\ \vdots \\ g_{k-1} \end{bmatrix} = \begin{bmatrix} g_{00} & g_{01} & g_{02} & \cdots & g_{0,n-1} \\ g_{10} & g_{11} & g_{12} & \cdots & g_{1,n-1} \\ \vdots & \vdots & \vdots & \vdots\vdots & \vdots \\ g_{k-1,0} & g_{k-1,1} & g_{k-1,2} & \cdots & g_{k-1,n-1} \end{bmatrix} \qquad (46)$$

V.3.1.1 Forma sistemática.

Otra propiedad que se desea en un código lineal es una estructura sistemática de las palabras código, donde una palabra código se divide en dos partes: la parte del mensaje y la parte de la redundancia como se muestra en la ***Figura 30***.

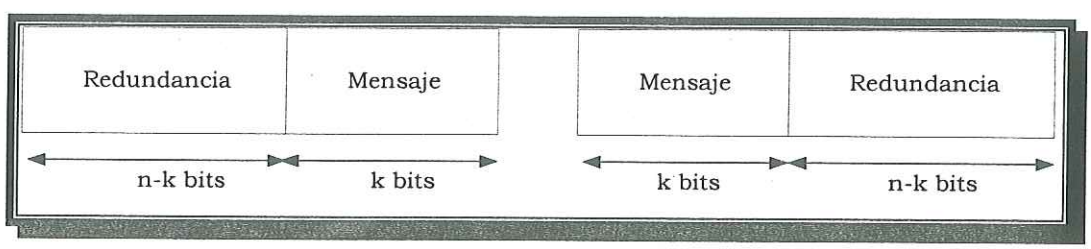

Figura 30: Forma sistemática de una palabra código.

La parte del mensaje consta de *k* bits del mensaje sin ser alterados y la parte de redundancia consiste de *n-k* bits de comprobación de paridad, los cuales son una suma lineales de los bits de información. Por lo que un código lineal sistemático queda completamente definido por la siguiente matriz *G*:

$$G = [p\,; I_k] \qquad (47)$$

donde I_k es la matriz de identidad de dimensiones *kxk* y *P* es la matriz de paridad de dimensiones *kxn* que genera los bits de paridad, por lo que la matriz *G* queda definida de la siguiente forma:

$$G = \begin{bmatrix} b_{00} & b_{01} & b_{02} & \cdots & b_{0,n-k-1} & 1\ 0\ 0\ \ldots\ 0 \\ b_{10} & b_{11} & b_{12} & \cdots & b_{1,n-k-1} & 0\ 1\ 0\ \ldots\ 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \\ b_{k-1,0} & b_{k-1,1} & b_{k-1,2} & \cdots & b_{k-1,n-k-1} & 0\ 0\ 0\ \ldots\ 1 \end{bmatrix} \qquad (48)$$

por lo que al sustituir esta matriz generadora en la ecuación 45 se tiene la siguiente palabra código:

$$v_{n-k+i} = u_i \qquad \text{para } 0 \le i < k$$

$$v_j = u_0 b_{1j} + u_1 b_{1j} + \ldots + u_{k-1} b_{k-1,j} \qquad \text{para } 0 \le j < n-k$$

Esto nos demuestra que los *k* primeros dígitos por la derecha de una palabra código *v* son idénticos a los dígitos de información $u_0, u_1, \ldots, u_{k-1}$ que hay que codificar, y que los *n-k* dígitos de redundancia son sumas lineales de los bits de información.

La matriz *G* está relacionada con el transmisor ya que ésta se usa para codificar los mensajes de usuario. Para poder comprobar si la palabra código recibida está libre de errores introducidos por el canal, se define una nueva matriz llamada *matriz de verificación de paridad H*, la cual está asociada con el receptor.

Para cada matriz *G* de dimensiones *kxn* con *k* filas linealmente independientes, existe una matriz *H* de dimensiones *(n-k)xn* con *n-k* filas linealmente independientes de tal

manera que cada vector en el espacio de las filas de G es ortogonal a las filas de H y todo vector que es ortogonal a las filas de H pertenece al espacio de las filas de G. Esto implica que una n-tupla v es una palabra código en el código generado por G si y sólo si:

$$v \cdot H^T = 0 \qquad (49)$$

Las 2^{n-k} combinaciones lineales de las filas de la matriz H forman un código lineal $C_d(n, n-k)$. Este código es el espacio nulo del código lineal $C(n, k)$ generado por la matriz G. C_d es el código dual de C.

Si la matriz G de un código lineal está en forma sistemática, la matriz H tiene la siguiente forma:

$$H = [I_{n-k}; P^T] \qquad (50)$$

donde P^T es la transpuesta de la matriz de paridad P. De las ecuaciones 47 y 50 se tiene la siguiente relación:

$$G \cdot H^T = 0 \qquad (51)$$

Por lo tanto, un código lineal también queda definido por la matriz de verificación de paridad H.

V.3.1.2 Síndrome.

Consideremos un código lineal (n, k) con su matriz generadora G y su matriz de verificación de paridad H. Sea v una palabra código que se transmite en un canal ruidoso tal como se muestra en la *Figura 31*, y r es el vector recibido a la salida del canal. Debido a que el canal es ruidoso, r puede ser diferente de v.

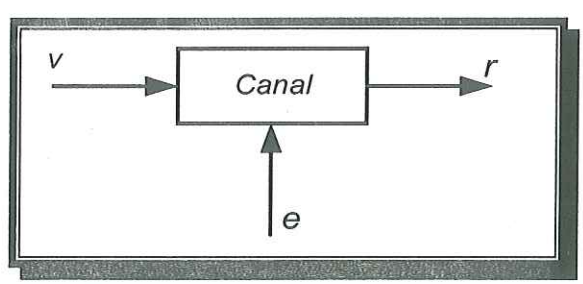

Figura 31: Vector recibido a la entrada del decodificador.

El vector suma de r y v es e $(r = v + e)$, e es una n-tupla tal que $e_i=1$ si r_i es diferente de v_i y $e_i = 0$ si $r_i = v_i$. Esta n-tupla es llamada como vector error.

Cuando el decodificador recibe r calcula la siguiente n-tupla:

$s = r \cdot H^T = (s_0, s_1, ..., s_{n-k-1})$, Esta n-tupla es el síndrome de r.

como $v \cdot H^T = 0$, entonces:

$$s = e \cdot H^T \qquad (52)$$

La expresión 52 nos indica como el síndrome depende solamente del vector error y no del mensaje original que se transmitió.

El principal problema del sistema de decodificación es determinar cual es el verdadero vector de error. Esto se debe a que las n-k ecuaciones lineales de la ecuación 52 no tienen una solución única, si no que tienen 2^k soluciones. En otras palabras, existen 2^k patrones de error que dan el mismo síndrome, y el verdadero error que se ha producido es únicamente uno de ellos. Para minimizar la probabilidad de error, se elige como vector error al patrón de error más probable. Si el canal es un canal simétrico binario (*BSC*), el vector error más probable será el que tiene un peso de *Hamming* mínimo.

$s = 0$ si y sólo si r es una palabra código y s es distinto de 0 si y sólo si r no es una palabra código. Pero es posible que los errores no sean detectables. Esto sucede cuando el vector de error es idéntico a una palabra código no nula. En este caso r es la suma de dos palabras código y por lo tanto el síndrome es igual a cero. Estos errores son errores indetectables. Como hay $2^k - 1$ palabras código no nulas, hay 2^k-1 errores indetectables [Lin y Costello, 1983].

V.3.1.3 Distancia y peso del código.

La distancia de una palabra código es el número de elementos en la cual difieren dos palabras código $u = (u_0, u_1, \ldots, u_{n-1})$ y $v = (v_0, v_1, \ldots, v_{n-1})$, y es denotada por $d(u, v)$. Esto es:

$$d_H(u,v) = \sum_{i=1}^{n} \delta(u_i, v_i) \qquad (53)$$

donde: $\delta(u_i, v_i) = \begin{cases} 0 & u_i = v_i \\ 1 & u_i \neq v_i \end{cases}$

Si las palabras código implementadas son binarias, la distancia es conocida como la *distancia de Hamming.*

El peso de una palabra código está dado por el número de elementos diferentes de cero en la palabra código. Para un código binario, el peso es básicamente los números de unos en la palabra código y es denotado por w.

La distancia de *Hamming* es una función métrica que satisface la desigualdad triangular [17]. Sean x, y y z tres n-tuplas, entonces:

$$d(x,y) + d(y,z) \geq d(x,z) \qquad (54)$$

De todo esto se deduce que la distancia de *Hamming* entre dos n-tuplas x y y, es igual al peso de *Hamming* de la suma de x y y, esto es:

$$d(x,y) = \mathrm{w}(x+y) \qquad (55)$$

Dado un código bloque C, se puede calcular la distancia de *Hamming* entre cualquiera dos palabras código distintas. La distancia mínima de C (d_{min}) se define como:

$$d_{\min} = \min d(v,u) \qquad v, u \text{ Pertenecen a C, } v \text{ distinto de } u \qquad (56)$$

Sea *C* un código lineal, la suma de dos vectores es también un vector código. Por lo tanto, la distancia de *Hamming* entre dos vectores código en *C* es igual al peso de *Hamming* de un tercer vector código en *C*. De esto se obtiene que:

$$d_{\min} = \min d(v,u) = \min \mathrm{w}(x) \qquad x \text{ pertenece a C, } x \text{ distinto de } 0 = \mathrm{w}_{\min} \qquad (57)$$

Por lo que nos indica la ecuación 57 se deduce que la distancia mínima de un código lineal de bloque es igual al peso mínimo de sus palabras distintas de cero.

La distancia mínima de un código es un parámetro que determina la capacidad para la detección y corrección de errores en un código bloque lineal. Específicamente un código es capas de corregir menos de *t* errores en cualquier palabra código recibida si la distancia mínima entre palabras código es $2t+1$, donde *t* es la capacidad correctiva del código.

V.3.2 Propiedades de detección de un código bloque.

Cuando se transmite un vector código *v* por un canal ruidoso, un vector de error *e* con 1 error causa que el vector recibido *r* sea diferente del vector *v* en 1 posición [d(*v*,*r*)=1]. Si la distancia mínima del código *C* es d_{min}, cada pareja de dos vectores de *C* tienen al menos d_{min} posiciones distintas. Por lo tanto, cualquier vector de error con $d_{min}-1$ o menos errores da un vector *r* que no es una palabra código de *C*. Cuando el receptor detecta que el vector recibido no es una palabra código de *C*, el error ha sido detectado.

Por lo tanto un código bloque con distancia mínima d_{min} es capaz de detectar todos los patrones de error de $d_{min}-1$ o menos errores. En realidad un código lineal (*n*, *k*) es capaz de detectar 2^n-2^k patrones de error de longitud *n*, y hay 2^k-1 patrones de error que son indetectables [Lin y Costello, 1983].

Un código bloque con distancia mínima d_{min} garantiza que corrige todos los patrones de error de $t=[(d_{min}-1)/2]$ o menos errores.

V.3.3 Propiedades de corrección de error del código.

Si el vector recibido tiene un síndrome diferente de cero, el decodificador se basa en una matriz (matriz típica) de decodificación para realizar la localización y corrección de la palabra código recibida [Steele, 1992, Lin y Costello, 1983].

Sea *C(n, k)* un código lineal y $v_1, v_2, ..., v_{2^k}$ los vectores código que componen C. Si transmitimos un vector código cualquiera a través de un canal ruidoso, el vector símbolo recibido estará dentro de las *n*-tuplas $(U_1, ..., U_n)$, por lo que en el primer renglón contiene todos los vectores código, empezando con el vector de ceros, y la primera columna contiene todos los patrones de error corregibles. Cada fila consiste de un patrón de error en la primera columna, seguido por el vector código perturbado por el patrón error. La matriz típica para un código *C* es de la siguiente forma:

$$\begin{array}{ccccccc} v_1 & & v_2 & \cdots & v_i & \cdots & v_{2^k} \\ e_2 & e_2 + v_2 & & \cdots & e_2 + v_i & \cdots & e_2 + v_{2^k} \\ \vdots & & & & & & \vdots \\ e_j & e_j + v_2 & & \cdots & e_j + v_i & \cdots & e_j + v_{2^k} \\ \vdots & & & & & & \vdots \\ e_{2^{n-k}} & e_{2^{n-k}} + v_2 & & \cdots & e_{2^{n-k}} + v_i & \cdots & e_{2^{n-k}} + v_{2^k} \end{array} \qquad (58)$$

Se deduce que hay 2^{n-k} filas distintas cada una con 2^k elementos distintos. Estas filas son denominadas conjuntos del código *C* y la primera *n*-tupla de cada conjunto se denomina líder de conjunto.

Supongamos que un vector código v_i es transmitido bajo un canal ruidoso. Si el patrón error causado por el canal es un líder de conjunto, el vector recibido será decodificado correctamente. Si el patrón de error no es líder de conjunto, una decodificación errónea será el resultado.

V.4 Códigos lineales modificados.

En muchas aplicaciones existe la necesidad de modificar la palabra código, por lo que la palabra código puede ser cambiada de las siguientes formas [Wicker, 1995]:

- Perforados: Un código es perforado si se borran bits de la palabra código original. Un código *(n, k)* es cambiado por el código *(n-1, k)*.
- Recortados: Un código es recortado si se borran mensajes del proceso de codificación. Un código *(n, k)* al recortarlo queda como *(n-1, k-1)*.
- Expurgados: Un código es expurgado por borrar algunas de sus palabras código, quedando de la forma *(n, k-1)*.
- Extendidos: Un código es extendido por sumar bits de redundancia a la palabra código original, quedando como *(n, k+1)*.
- Aumentados: Un código es aumentado si se le suman nuevas palabras código dando como resultado un código *(n, k+1)*.
- Alargados: Un código es alargado si se suman mensajes dando un código *(n+1, k+1)*.

V.5 Códigos cíclicos.

Los códigos cíclicos son una subclase importante de los códigos bloque lineales, poseen dos características muy importantes:

- ✓ Son fáciles de implementar usando una circuitería basada en registros de desplazamiento.
- ✓ Tienen una estructura algebraica bien definida, por lo que reducen considerablemente la complejidad del codificador y lo más importante la del decodificador.

El código $C(n, k)$ es cíclico si y sólo si cualquier rotación cíclica de un vector v pertenece a C es también un vector del código C. Para representar los vectores

pertenecientes a los códigos cíclicos se usará la representación *polinomial*. Cada uno de los componentes de un vector código $v=(v_0, v_1, ..., v_{n-1})$ serán los coeficientes del polinomio $v(x)=v_0+v_1x+v_2x^2+...+v_{n-1}x^{n-1}$. A este polinomio se le denomina polinomio código. Por lo tanto a toda palabra código v le corresponde un polinomio código $v(x)$ de grado (n-1) o menor. El desplazamiento cíclico del polinomio código será representado por el siguiente polinomio:

$$v^i(x)=v_{n-i}+v_{n-i+1}x+,...,+v_{n-1}x^{i-1}+v_0x^i \qquad (59)$$

donde i es el número de desplazamientos del polinomio código original. El siguiente teorema muestra la relación algebraica entre $v(x)$ y $v^i(x)$.

Teorema 5.1: El desplazamiento cíclico de un polinomio código está relacionado en la siguiente forma:

$$v^i(x)=x^iv(x) \bmod x^n-1 \qquad (60)$$

Del teorema 5.1 se observa que i desplazamientos del polinomio código ($v(x)$) es el residuo de la división de $x^iv(x)$ por x^n+1.

V.5.1 Algoritmo de codificación de los códigos cíclicos.

Cada polinomio $v(x)\in C$ puede ser expresado como $v(x)=u(x)g(x)$, donde $u(x)$ es un polinomio de grado menor o igual a $k=n-r$ con coeficientes de *GF(q)*. $g(x)$ es un polinomio de grado $r=n-k$ y es factor de grado x^n-1. En otras palabras $g(x)$ es el polinomio primitivo mónico de grado r (Polinomio primitivo de menor elementos) y es llamado el polinomio generador del código cíclico.

Por las razones mencionadas anteriormente nos interesa que la palabra código esté en forma sistemática, por lo que para codificar en forma sistemática se siguen los siguientes pasos:

1. Desplazar el mensaje $u(x)$ hacia la derecha n-k posiciones (multiplicar $u(x)$ por x^{n-k}).
2. Dividir el resultado del paso uno por $g(x)$. Obteniendo el residuo $b(x)$.
3. Combinar $b(x)$ y $x^{n-k}u(x)$, para obtener el siguiente polinomio código:

$$v(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_{n-k-1}x^{n-k-1} + u_0 x^{n-k} + u_1 x^{n-k+1} + \ldots + u_{k-1}x^{n-1} \quad (61)$$

Como se mencionó anteriormente la matriz generadora G en forma sistemática está formada por $G = [P \; ; \; I_k]$, donde P es la matriz de verificación de paridad y está representada por:

$$P = \begin{bmatrix} b_{00} & b_{01} & b_{02} & \ldots & b_{0,n-k-1} \\ b_{10} & b_{11} & b_{12} & \ldots & b_{1,n-k-1} \\ . & . & . & \ldots & . \\ b_{k-1,0} & b_{k-1,1} & b_{k-1,2} & \ldots & b_{k-1,n-k-1} \end{bmatrix} \quad (62)$$

Por lo que para encontrar los componentes de la matriz P se siguen los siguientes procedimientos:

1. Se divide x^{n-k+i} por el polinomio generador $g(x)$ obteniendo el residuo $b_i(x)$ para $0 \le i \le k-1$.

$$b_i(x) = x^{n-k+i} \mod g(x) \quad (63)$$

V.5.2 Algoritmo de decodificación de los códigos cíclicos.

Pare llevar a cabo la decodificación se siguen los siguientes pasos [http://web.syr.edu/~rrosenqu/ecc/main.htm]:

1. Calcular el síndrome del vector recibido $r(x)$:

$$s(x) = r(x) \mod g(x) \quad (64)$$

Si el síndrome $s(x)=0$, quiere decir que no ocurrió un error en la transmisión y el vector recibido $r(x)$ es igual a la palabra código transmitida $v(x)$. Si $s(x)\neq 0$ indica que ocurrió un error en la transmisión, por lo que se pasa al paso 2.

2. Se procede a asociar el síndrome a un patrón error.

En este paso se utiliza la propiedad de desplazamiento del síndrome: si $s(x)$ es el síndrome de un vector recibido $r(x)$, entonces el síndrome $s^i(x)$ de $r^i(x)$ es residuo de dividir $x^i s(x)$ por $g(x)$:

$$s^i(x) = x^i s(x) \mod g(x) \qquad (65)$$

El paso para asociar el síndrome a un patrón error es el siguiente:

Se calcula el desplazamiento del síndrome $s^i(x)$ para cada $i \geq 0$, hasta que un síndrome s^j sea encontrado, el cual $w(s^j) \leq t$ donde t es la capacidad de corrección del código, ya que se encuentra esta relación se asocia el síndrome a un patrón error por medio de la siguiente expresión [http://web.syr.edu/~rrosenqu/ecc/main.htm]:

$$e(x) = x^{n-j} s_j(x) \mod g(x) \qquad (66)$$

Si el síndrome es desplazado más de n veces se dice que la capacidad de corrección del código a sido superada, por lo que el código no puede corregir el error y pide la retransmisión de la palabra código. Todo código cíclico $C(n, k)$ detecta ráfagas de longitud menor o igual a $n-k$. La capacidad de corrección está dada por:

$$t = \frac{d_{\min} - 1}{2} \qquad (67)$$

V.6 Códigos BCH.

Los códigos *Bose, Chaudhuri y Hocquenghem (BCH)* forman una clase fuerte de códigos bloque cíclicos con capacidad elevada de detección y corrección de error múltiples, existen en un amplio intervalo de velocidades de código, tienen una ganancia de

codificación significativa [Rappaport, 1996].Uno de los códigos *BCH* no binarios más importante es el código *Reed Solomon*, el cual es el que nos interesa analizar debido a sus características que se describirán más adelante. Pero primero se estudiarán los códigos *BCH* no binarios para tener bien definidas las bases de los *BCH* no binarios (*Reed Solomon*).

V.6.1 Códigos BCH binarios.

Para cualquier entero positivo m y $t < 2^{m-1}$ existe un código binario *BCH* con los siguientes parámetros:

Longitud del código	$n = 2^m - 1$	
Número de bits de redundancia	$n - k \leq mt$	*(68)*
Distancia mínima	$d_{\min} \geq 2t + 1$	

El código *BCH* es generado por el polinomio generador $g(x)$, el polinomio de menor grado (polinomio mínimo $\phi_i(x)$) sobre *GF*(2) y tiene como raíces a α^i (para $i = 1,...,2t$), donde α es un elemento primitivo de *GF*(2^m) y consecuentemente también son raíces de cada palabra código, entonces el polinomio generador se define como el mínimo común múltiplo (*LCM*) de los polinomios mínimos $\phi_1(x), \phi_2(x),..., \phi_{2t}(x)$, que tiene $2t$ potencias consecutivas de α como raíces, y está representado por la siguiente expresión:

$$g(x) = LCM[\phi_1(x), \phi_2(x),..., \phi_{2t}(x)] \qquad (69)$$

Recordando que en *GF*(2^m), los elementos α y α^2 son conjugados, y tienen el mismo polinomio mínimo, por lo tanto el polinomio generador se puede formar por considerar únicamente las potencias impares del elemento primitivo α, quedando de la siguiente forma:

$$g(x) = LCM[\phi_1(x), \phi_3(x),..., \phi_{2t-1}(x)] \qquad (70)$$

El grado del polinomio generador es de mt o menos, y determina el número de bits de redundancia en una palabra código. El tipo de código definido arriba es el *BCH* primitivo, porque las raíces especificadas son potencias consecutivas de un elemento primitivo de $GF(2^m)$.

V.6.1.1 Algoritmo de codificación para los códigos BCH.

Los pasos para realizar una codificación con códigos *BCH* binarios son los siguientes:

1. Encontrar un polinomio primitivo $p(x)$ de grado m bajo $GF(2)$.
2. Usar el polinomio primitivo $p(x)$ para construir $GF(2^m)$.
3. Encontrar el polinomio mínimo de α^i, para $i = 1,3,...,2t-1$, para obtener el polinomio generador $g(x)$.
4. Desplazar el mensaje $u(x)$ hacia la derecha n-k posiciones (multiplicar $u(x)$ por x^{n-k}).
5. Dividir el resultado del paso cuatro por $g(x)$. Obteniendo el residuo $b(x)$.
6. Combinar $b(x)$ y $x^{n-k}u(x)$, para obtener la palabra código.

Ejemplo: Se desea encontrar el polinomio generador del codificador de canal *BCH(15, 5, 3)*, donde 15 es la longitud de la palabra código (n), 5 la longitud de la palabra código (k) y 3 la capacidad de corrección del código (t).

Para encontrar el polinomio generador $g(x)$ se siguen los pasos mencionados anteriormente:

1.- Se encuentra el polinomio primitivo de grado m=4 (n=2^m-1).

$$p(x) = 1 + x + x^4$$

2.- Se construye los elementos del campo de Galois GF(2^m), los cual se muestra en la *Tabla VI.*

Tabla VI: Elementos del campo GF(16).

Exponencial	*Polinomial*	*Exponencial*	*Polinomial*
0	0	σ^7	$1+x+x^3$
1	1	σ^8	$1+x^2$
σ	x	σ^9	$x+x^3$
σ^2	x^2	σ^{10}	$1+x+x^2$
σ^3	x^3	σ^{11}	$x+x^2+x^3$
σ^4	$1+x$	σ^{12}	$1+x+x^2+x^3$
σ^5	$x+x^2$	σ^{13}	$1+x^2+x^3$
σ^6	x^2+x^3	σ^{14}	$1+x^3$

3.- Se calculan los polinomios mínimos de σ^i, obteniendo la *Tabla VII.*

Tabla VII: Polinomios mínimos en GF(16) generados por $p(x)=1+x+x^4$.

Raíces conjugadas	*Polinomio mínimo*
0	x
1	$1+x$
$\sigma,\sigma^2,\sigma^4,\sigma^8$	x^4+x+1
$\sigma^3,\sigma^6,\sigma^9,\sigma^{12}$	$x^4+x^3+x^2+x+1$
σ^5,σ^{10}	x^2+x+1
$\sigma^7,\sigma^{11},\sigma^{13},\sigma^{14}$	x^4+x^2+1

Una ves que se tienen los polinomios mínimos del código *BCH(15,5,3)* y aplicando la ecuación 70 se tiene *g(x)* es:

$$g(x) = LCM[\phi_1,\phi_3,\phi_5] = (x^4+x+1)(x^4+x^3+x^2+x+1)(x^2+x+1) = 1+x+x^2+x^4+x^5+x^8+x^{10}$$

V.6.1.2 Algoritmo de decodificación para los códigos BCH.

Sea $v(x) = v_0 + v_1x + v_2x^2 + \ldots + v_{n-1}x^{n-1}$ la palabra código transmitida y $r(x) = r_o + r_1x + r_2x^2 + \ldots + r_{n-1}x^{n-1}$ el vector recibido en la entrada del decodificador, sea $e(x)$ el patrón de error, por lo tanto $r(x) = v(x) + e(x)$. Como es usual, el primer paso del

decodificador es calcular el síndrome del vector recibido $r(x)$. Para un código *BCH* primitivo el síndrome es una *2t*-tupla, la cual es obtenida con la ayuda de la siguiente expresión:

$$b_i(x) = r(x) \mod \phi_i(x) \qquad \text{Para } 1 \le i \le 2t \qquad (71)$$

donde el componente del síndrome S_i es obtenida por evaluar $b_i(x)$ con $X = \sigma^i$.

Ejemplo: Consideremos el código *BCH(15, 5, 3)* del ejemplo anterior, sea $v(x) = x^{11} + x^9 + x^6 + x^5 + x^3 + x^2 + x$ la palabra código transmitida y se recibe la el vector $r(x) = x^{13} + x^{11} + x^9 + x^5 + x^3 + x^2 + x$

El síndrome consiste de 6 componentes (*2t*) $S = (s_1, s_2, s_3, s_4, s_5, s_6)$

Los polinomios mínimos para σ, σ^2 y σ^4 son $\phi_1 = \phi_2 = \phi_4 = x^4 + x + 1$, el polinomio mínimo de σ^3 es $\phi_3 = x^4 + x^3 + x^2 + x + 1$ y el de σ^5 es $\phi_5 = x^2 + x + 1$

Dividiendo $r(x)$ por $\phi_1(x)$ y usando *GF(2^4)* dado por la *Tabla VI.*

y sustituyendo α, α^2 y α^4 dentro del residuo $b_1(x)$, obtenemos:

$$s_1 = 1 \qquad s_2 = 1 \qquad s_4 = 1$$

Substituyendo α^3 y α^6 dentro de $b_3(x)$, obtenemos:

$$s_3 = \alpha \qquad s_6 = \alpha^2$$

Substituyendo α^5 dentro de $b_5(x)$, se obtiene:

$$s_5 = \alpha^{10}$$

Teniendo como resultado la *2t*-tupla *S=(1, 1, α, 1, α^{10}, α^2)*, de estos resultados se aprecia como son diferente de cero por lo que se detectaron los errores introducidos por el canal.

Ya que el síndrome depende únicamente del vector error se tiene la siguiente relación:

$$S_i = e(\alpha^i) \qquad \text{Para } 1 \le i \le 2t \qquad (72)$$

Sea v los errores producidos por el canal en el vector error en las posiciones $i_1, i_2, ..., i_v$ y de magnitudes $e_{i_1}, e_{i_2}, ..., e_{i_v}$ (caso binario $e_{i_j} = 1$), por lo tanto el polinomio error se puede expresar como:

$$e(x) = e_{i_1} x^{i_1} + e_{i_2} x^{i_2} + ... + e_{i_v} x^{i_v} \qquad (73)$$

Como incógnitas se tienen las posiciones y las magnitudes de los errores (no binarios), así como v (el número de errores). Una vez conocidas todas estas incógnitas se podrá corregir el vector $r(x)$ recibido. El primer paso, como se mencionó anteriormente, es calcular los componentes del síndrome, definiendo el síndrome como:

$$S_i = e_{i_1} \alpha^{i_1} + e_{i_2} \alpha^{i_2} + ... + e_{i_v} \alpha^{i_v} \qquad (74)$$

Evaluando el polinomio recibido $r(x)$ en las $2t$ raíces del polinomio generador $g(x)$, se obtiene el conjunto de $2t$ ecuaciones no lineales:

$$\begin{aligned} S_1 &= M_1 P_1 + M_2 P_2 + ... + M_v P_v \\ S_2 &= M_1 P_1^2 + M_2 P_2^2 + ... + M_v P_v^2 \\ &\vdots \qquad\qquad\qquad \vdots \\ S_{2t} &= M_1 P_1^{2t} + M_2 P_2^{2t} + ... + M_v P_v^{2t} \end{aligned} \qquad (75)$$

donde para realizar la simplificación de la notación se ha renombrado las posiciones de errores α^{i_x} por P_x y las magnitudes de error e_{i_x} por M_x (si el código no es binario), y cualquier método para resolver estas ecuaciones no lineales es llamado un algoritmo de decodificación para los códigos *BCH,* tales como algoritmo de *Berlekamp*, algoritmo de *Kasami, Peterson-Gorenstein-Zierler..*

V.6.1.2.1 Decodificación según el método de Peterson-Gorenstein-Zierler.

Nosotros utilizaremos el método de Peterson para convertir las ecuaciones no lineales de 75 en ecuaciones lineales de las cuales la posición del error y la magnitud del error pueden ser calculadas, para encontrar las posiciones de los errores se echará mano de un polinomio localizador de error, $\sigma(X)$, como el polinomio con ceros en los inversos de las posiciones de error P_i^{-1} con i=1,2,...,v.

$$\sigma(X) = (1 + P_1 X)(1 + P_2 X)...(1 + P_v X) = 1 + \sigma_1 X + \sigma_2 X^2 + ... + \sigma_v X^v \qquad (76)$$

Los ceros de este polinomio permitirán obtener las posiciones de los errores, pero para ello es necesario conocer los coeficientes del polinomio que se calculan mediante la inversión de una matriz no singular según la siguiente ecuación:

$\vec{\sigma} = \overline{\overline{S}}^{-1} \vec{S}$ y en forma matricial:

$$\begin{bmatrix} \sigma_v \\ \sigma_{v-1} \\ : \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} S_1 & S_2 & ... & S_v \\ S_2 & S_3 & ... & S_{v+1} \\ : & & & : \\ S_v & S_{v+1} & ... & S_{2v-1} \end{bmatrix}^{-1} \begin{bmatrix} S_1 \\ S_2 \\ : \\ S_{2v} \end{bmatrix} \qquad (77)$$

La matriz $\overline{\overline{S}}$ será no singular si su dimensión es vxv pero será singular (y no podrá invertirse) si su dimensión es mayor que v, donde v es el número actual de errores introducidos por el canal.

Una vez obtenida las posiciones de los errores, se procede a calcular las magnitudes de los errores (si el código no es binario), el cual se realiza de manera semejante mediante otra operación con matrices:

$$\begin{bmatrix} M_1 \\ M_2 \\ : \\ M_v \end{bmatrix} = \begin{bmatrix} P_1 & P_2 & \dots & P_v \\ P_1^2 & P_2^2 & \dots & P_v^2 \\ : & & & : \\ P_1^v & P_2^v & \dots & P_v^v \end{bmatrix}^{-1} \begin{bmatrix} S_1 \\ S_2 \\ : \\ S_v \end{bmatrix} \qquad (78)$$

En síntesis, los pasos que se siguen para llevar a cabo la detección, localización y corrección de errores son:

1.- Obtención de la $2t$-tupla del síndrome $S = (s_1, s_2, \dots, s_{2t})$

2.- Determinar el número de errores v, que se han producido. Comenzando por $v=t$, donde t es la máxima capacidad de corrección del código.

3.- Construir la matriz S(vxv) a partir de los síndromes obtenidos y calcular su determinante.

4.- Si det(S)=0 no se puede invertir S (no ocurrieron v errores en la transmisión de la palabra código). Disminuir v en 1 y volver al paso 3. Si det(S)≠0 S se podrá invertir (se detectan v errores en la palabra código transmitida).

5.- Se calculan los coeficientes del polinomio localizador de error $\sigma(X)$ a partir de la ecuación 76.

6.- Encontrar los ceros del polinomio $\sigma(X)$. Para ésto se suele utilizar el método de *Chien* que consiste en ir probando todos los elementos del cuerpo $GF(2^m)$ hasta dar con los ceros.

7.- Si el código es binario las magnitudes de error son 1, pero si el código no es binario se procede a calcular por medio de la ecuación de matriz 78.

V.7 Códigos de Reed-Solomon.

Los códigos *Reed Solomon* son una subclase importante de los códigos *BCH* no binarios. Son códigos con un rango amplio de aplicaciones incluyendo [Wicker y Bhargava,1994]:

- Dispositivos de almacenamiento (incluyendo Compact Disk, *DVD*, etc.)
- Comunicaciones inalámbricas o móviles.

- Comunicación satelital.
- Televisión digital (*DVB*)
- Modems de alta velocidad tales como *ADSL*, *xDSL*, etc.

Un código *Reed Solomon* es especificado como *RS(n, k)* con s-bits de símbolos. Esto significa que el codificador toma *k* símbolos de datos de *s* bits cada uno de los símbolos. Un código *Reed Solomon* con símbolos pertenecientes a $GF(q^m)$ se caracteriza por los siguientes parámetros:

Longitud del bloque	$n = q^m - 1$	
Número de símbolos de verificación de paridad	$n - k = 2t$	*(79)*
Distancia mínima	$d_{\min} = 2t + 1$	

Considerando la construcción de un código *RS* de longitud $q^m - 1$ con símbolos pertenecientes a $GF(q^m)$, y sea α un elemento primitivo donde $\alpha \in GF(q^m)$. Entonces el polinomio generador está dado por:

$$g(x) = LCM[\phi_1(x), \phi_2(x), ..., \phi_{2t}(x)] \qquad (80)$$

donde ahora el polinomio mínimo esta bajo $GF(q^m)$. Pero como el polinomio mínimo bajo $GF(q^m)$ de cualquier $\beta \in GF(q^m)$ es simplemente $\phi_\beta = x - \beta$. Por lo tanto el polinomio generador está dado por:

$$g(x) = (x + \alpha)(x + \alpha^2)...(x + \alpha^{2t}) \qquad (81)$$

Una característica importante de los códigos RS es que tienen la distancia mínima más grande para una *n* y *k* dada.

V.7.1 Algoritmo de codificación.

Los pasos para realizar una codificación con códigos *Reed Solomon* son los siguientes:

1. Encontrar un polinomio primitivo $p(x)$ de grado m bajo $GF(2)$.
2. Usar el polinomio primitivo $p(x)$ para construir $GF(2^m)$.
3. Desplazar el mensaje $u(x)$ hacia la derecha $2t$ posiciones (multiplicar $u(x)$ por x^{2t}).
4. Dividir el resultado del paso tres por $g(x)$. Obteniendo el residuo $b(x)$.
5. Combinar $b(x)$ y $x^{2t}u(x)$, para obtener el polinomio código.

V.7.2 Algoritmo de decodificación.

Pare llevar a cabo la decodificación se siguen los siguientes pasos:

1. Calcular el síndrome del vector recibido $r(x)$:

$$s_i(x) = r(x) \mod (x + \alpha^i) \quad \text{Para } 1 \le i \le 2t \qquad (82)$$

Si el síndrome $s(x) = 0$, quiere decir que no ocurrió un error en la transmisión y el vector recibido $r(x)$ es igual a la palabra código transmitida $v(x)$. Si $s(x) \neq 0$ indica que ocurrió un error en la transmisión, por lo que se pasa al paso 2.

2. Se utiliza el método de Peterson-Gorenstein-Zierler para asociar el síndrome a un patrón de error [Steele, 1992, Wiggert, 1988, http://www.itr.unisa.edu.au/~alex/ECC/].
3. Se calcula la magnitud del vector error con el método de Peterson-Gorenstein-Zierler [Steele, 1992, Wiggert, 1988, http://www.itr.unisa.edu.au/~alex/ECC/].
4. Se corrige el error

V.8 Conclusiones.

En este capítulo se han presentado los resultados del estudio de los parámetros más importantes de los códigos bloque (códigos lineales, códigos cíclicos, códigos BCH binarios y códigos *Reed Solomon*), En nuestro caso en particular se estudiaron los códigos bloque ya que el análisis que se desea hacer es sobre transmisión de datos en exteriores, donde ocurren errores de tipo a ráfagas.

La matemática asociada a los códigos bloque juega un papel muy importante, ya que con la matemática de Galois, tanto la codificación como la decodificación se reduce la complejidad considerablemente de aquí la importancia del estudio de cuerpos finitos o matemática de Galois, la cual fue estudiada anteriormente.

Como se mencionó anteriormente los sistemas de codificación de canal híbridos son una muy buena opción para los sistemas de tercera generación ya que éstos se adaptan a los condiciones variantes del canal radio, dando como resultado un sistema de comunicación con alto *Throughput* y con alta confiabilidad.

Hasta este punto de la tesis ya nos encontramos con las suficientes herramientas para realizar el análisis de prestaciones de los códigos bloque, por lo que en el siguiente capítulo se describirá el programa de simulación desarrollado, así como el análisis de los resultados obtenidos por las simulaciones, las cuales nos llevaran a proponer los parámetros óptimos del código de los canales *RACH* y *TCH* del sistema *CDMA*.

VI Análisis de prestaciones de los códigos bloque binarios (BCH) y no binarios (Reed Solomon).

VI.1 Introducción.

Como se ha venido mencionado en los capítulos anteriores, el canal radio (transmisión en exteriores) presenta desvanecimientos rápidos (*Rayleigh*) debido a las mutitrayectorias, como consecuencia de ésto, la señal recibida presenta una distribución de tipo *Rayleigh*, produciendo con ello errores de tipo a ráfagas en la transmisión del tráfico de datos. Por lo que, el canal radio al que nos enfrentamos es un canal de tipo no estacionario y fuertemente hostil.

En el capítulo anterior se estudiaron los códigos bloque binarios (*BCH*) y los códigos bloque no binarios (*Reed Solomon*) así como sus parámetros más importantes tales como la capacidad de corrección, la distancia mínima, el polinomio generador, la codificación, detección, localización y corrección de errores. Por lo que en este punto de la tesis ya nos encontramos con las bases suficientes para realizar el programa de simulación de los códigos bloque (*BCH* y *RS*) y poder discutir y analizar sobre los resultados que se obtengan en las simulaciones.

Como se mencionó en los apartados anteriores el tipo de información a transmitir son datos (canal de petición de servicio y canal de transmisión de paquetes), el cual es sensitivo a la pérdida de información (*BER* del canal de 10^{-6} a 10^{-2}), Por lo que en este capítulo se analizarán las prestaciones de los códigos *BCH* y *RS*, como códigos *FEC* solamente, y se propondrán los parámetros óptimos del código (n, k y t), tanto para el canal de petición de servicio (*RACH*) como para el canal de transmisión de paquetes (*TCH*).

El principal problema de los sistemas actuales de comunicación que utilizan codificación de canal, es que no está orientado al servicio de datos, con lo que no se compensa la fuerte caída del *Throughput* en la región del *BER* del canal de 10^{-4} a 10^{-2}, dando como resultado que estos sistemas se vean forzados, ya sea a interrumpir la transmisión de los datos y/o a reanudar la transmisión hasta que el *BER* del canal se encuentra en una región favorable (10^{-6} a 10^{-4}) tal como se muestra en la *Figura 32*.

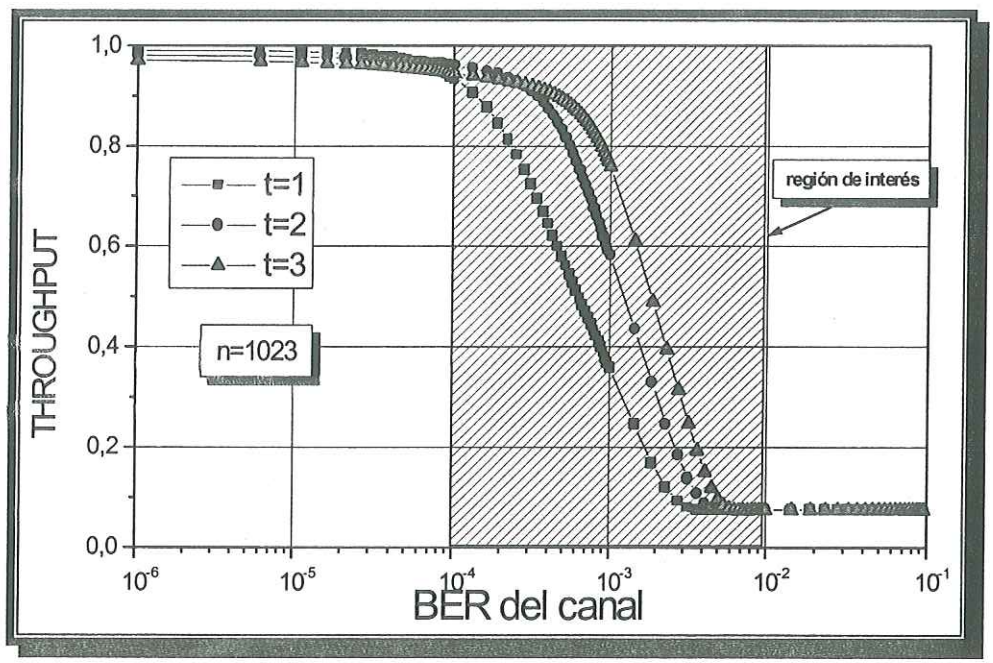

Figura 32: Respuesta obtenida del Throughput mediante un esquema de codificación no orientado al servicio de datos con t capacidad de corrección de error [Covarrubias, 1999].

En esta figura se aprecia que se tiene una región del *BER* del canal (10^{-6} a 10^{-4}) en la cual no se introduce muchos errores, y una región del *BER* del canal (10^{-4} a 10^{-2}) donde el *Throughput* del sistema cae drásticamente, teniendo como consecuencia que el sistema reenvíe los datos hasta que sean entregados en el receptor sin ningún error o en algunos casos interrumpiéndose la transmisión hasta que el *BER* del canal disminuya. Por lo que el principal objetivo de este capítulo es la obtención de los parámetros óptimos del código *BCH* y del Reed Solomon (*RS*), los cuales conserven el *Throughput* del sistema lo más alto

posible en todo el margen de variación del *BER* (10^{-6} a 10^{-2}) del canal radio, lo cual no ocurre en sistemas donde se emplea códigos correctores de error que no están enfocados al servicio de transmisión de datos.

Por las razones mencionadas anteriormente, se obtendrán los parámetros óptimos del código, los cuales en conjunto harán que el sistema no presente una caída brusca en el *Throughput* (en todo el intervalo de 10^{-6} a 10^{-2}) ante la presencia del canal radio con envolvente de tipo *Rayleigh*. Además de lo anterior se buscará que el código de canal seleccionado presente un esquema sencillo de decodificación y que cumpla con las expectativas de un esquema de codificación de canal eficiente para la transmisión de datos bajo un entorno *CDMA*. Dado que los sistemas actuales que implementan *CDMA* utilizan un canal para realizar la petición de servicio (*RACH*) y otro para la transmisión de los paquetes (*TCH*), es necesario que se realicen simulaciones para ambos canales. En un sistema de comunicaciones móviles celulares se establece como inicio de protocolo entre el móvil y la estación base una fase de petición de acceso (*RACH*) o de servicio cuyo paquete *RACH* normalmente es de una longitud corta, en nuestro caso emplearemos una palabra código de 31 y 63 bits, con esto se apreciará la influencia de la longitud de la palabra código. Para la fase de transmisión de datos utilizaremos una longitud de palabra código de 1023 bits, longitud que al pasar por el esquema de codificación bloque resultará en un paquete de longitud similar a una celda *ATM* [McTiffin et al, 1994, David, 1999].

En suma en este capítulo presentaremos todo el proceso de simulación seguido para la caracterización de los parámetros de los códigos bloque binarios (*BCH*) y no binarios (*RS*). Se obtiene también los parámetros óptimos del código *RS* propuesto para los sistemas móviles de tercera generación.

VI.2 Programa de simulación utilizado.

Para llevar a cabo el proceso de simulación se diseño un programa en *MATLAB* versión 5.3.0, utilizando además el *toolbox* de comunicación. Esta plataforma de simulación fue elegida, por contar con varias herramientas que nos permitieron reducir principalmente el tiempo de simulación. En la *Figura 33* se muestra un diagrama a bloques de la secuencia de programación, dicha secuencia se puede dividir en tres partes principales:

- Transmisor.
- Canal.
- Receptor.

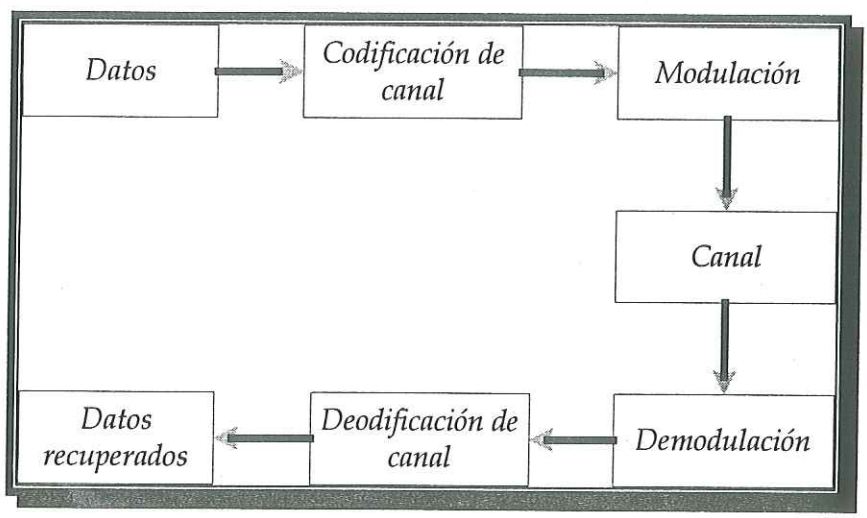

Figura 33: Diagrama a bloques de la secuencia de simulación.

VI.2.1 Transmisor.

La etapa del transmisor se puede dividir en tres partes: fuente de datos, codificación de canal y modulación.

La fuente de datos es generada por un proceso de *Bernoulli*, esto es por que el tráfico de tipo datos es a ráfagas y discontinuo. Se asume que los datos son previamente pasados por una etapa de codificación fuente, por lo que los datos que recibe el codificador de canal son digitales (0 ó 1) y aleatorios, los cuales son generados a una velocidad de transmisión de R *bps* (bits por segundo).

En la etapa de codificación de canal se utiliza el código bloque *BCH* y el *RS*, los cuales reciben los bits de entrada (k bits) y los transforman en una palabra código (n bits ó símbolos), modificando la velocidad de transmisión por un factor de n/k, por lo que la velocidad de transmisión a la salida del codificador es $R(n/k)$ *símbolos por segundo.*

En la etapa de modulación se utiliza una modulación *BPSK* coherente, ya que es una de las técnicas de modulación que más reduce el E_b/N_o y además es la más utilizada por los sistemas *CDMA*.

VI.2.2 Canal.

Los tipos de canal utilizados en estas simulaciones son tanto un canal *AWGN* como el canal *Rayleigh*. El canal *AWGN* fue utilizado para realizar la validación del modelo, ya que este tipo de canal es el más sencillo de analizar y de implementar en los sistemas de comunicación.

El canal *AWGN* añade a los datos modulados un componente de ruido blanco *gaussiano* con densidad espectral de potencia de $N_o/2$. En cambio, el canal *Rayleigh* afecta a los datos tanto en amplitud como en fase.

VI.2.3 Parámetros de simulación y resultados a obtener.

Los parámetros de simulación que se tomaron en cuenta para todas las simulaciones son:

- Tipo de servicio datos.
- Proceso de generación de datos: *Bernoulli*.
- Los códigos correctores de error que se utilizaron son: *BCH* y *RS*.
- Tipo de canal: *AWGN* y *Rayleigh*.
- Modulación y demodulación *BPSK*.
- Longitudes de paquetes de datos: 31, 63 y 1023 bits para *BCH* y 15 y 127 símbolos para *RS*.
- La varianza del canal tanto *AWGN* como *Rayleigh* es determinada por la siguiente formula [Proakis y Salehi, 2000]:

$$E_s / N_o = 1/2\sigma^2 \qquad (83)$$

donde:

$$E_s / N_o = \left(\frac{k}{n}\right)\left(\frac{E_b}{N_o}\right)$$

E_b / N_o Energía de bit entre la densidad espectral de potencia del ruido.

E_s / N_o Energía de símbolo entre la densidad espectral de potencia.

σ^2 Varianza del canal.

- Región de interés del *BER* del canal: 10^{-4} a 10^{-2}.
- Intervalo de variación del parámetro E_b / N_o de 2 a 14 dB.
- El parámetro de evaluación de eficiencia en las simulaciones es la probabilidad de error de bit.

Las estadísticas obtenidas mediante el proceso de simulación son comportamiento del *BER* versus E_b / N_o, del cual obtendremos el parámetro de ganancia de codificación y el más importante: *Throughput* versus *BER* del canal. Como compromiso se buscará que el

Throughput del sistema sea lo más alto posible pero que al mismo tiempo no presente una caída abrupta en la región del *BER* del canal comprendida entre 10^{-4} y 10^{-2}.

VI.3 Validación del modelo.

En cualquier sistema de simulación es importante que se lleve a cabo una etapa de validación del modelo, ya que es por medio de éste que se le da credibilidad a los resultados obtenidos por la simulación. Para validación del modelo se compararon los resultados que se obtuvieron de las simulaciones con los resultados teóricos basados en las siguientes expresiones matemáticas.

Para la probabilidad de error de bit consideramos dos escenarios:

a) Sin codificación de canal; cuya expresión matemática, para el esquema de modulación *BPSK*, viene dada por:

$$p_{uB(BPSK)} = Q(\sqrt{2E_b / N_o}) \qquad (84)$$

donde:

E_b / N_o Energía de bit entre la densidad espectral de potencia del ruido.

$p_{uB(BPSK)}$ Probabilidad de error de bit sin codificación de canal.

Q Función de error complementaria de la estadística Gaussiana.

b) Con codificación de canal; cuya expresión matemática se deriva a partir de:

$$p_{c(BPSK)} = Q(\sqrt{2E_s / N_o}) \qquad (85)$$

donde:

$$E_s / N_o = \left(\frac{k}{n}\right)\left(\frac{E_b}{N_o}\right)$$

$$\text{finalmente } p_{cB} \cong \left(\frac{1}{n}\right)\sum_{j=t+1}^{n} j\binom{n}{j} p_c{}^{j}(1-p_c)^{n-j} \qquad (86)$$

donde:

(k/n) Velocidad de codificación del código.

E_s / N_o Energía de símbolo entre la densidad espectral de potencia.

$p_{c(BPSK)}$ Probabilidad de error de símbolo del canal.

t Capacidad de corrección del código.

p_{cB} Probabilidad de error de bit con codificación de canal.

Es importante destacar que las expresiones matemáticas descritas anteriormente son aplicables solamente a una modulación *BPSK* y bajo un canal de transmisión del tipo *AWGN*, ya que es el canal de comunicación más sencillo de analizar y de modelar en un sistema de comunicación. Los resultados obtenidos por las expresiones matemáticas descritas anteriormente, son representados en la *Figura 34*, Estos resultados son obtenidos, utilizando un código *BHC* (31,*k*,*t*), en donde los parámetros *k* (longitud del bloque de bits a codificar) y *t* (capacidad de corrección de error) se varían para establecer su comportamiento en términos de la mejor combinación de parámetros *n*, *k* y *t*.

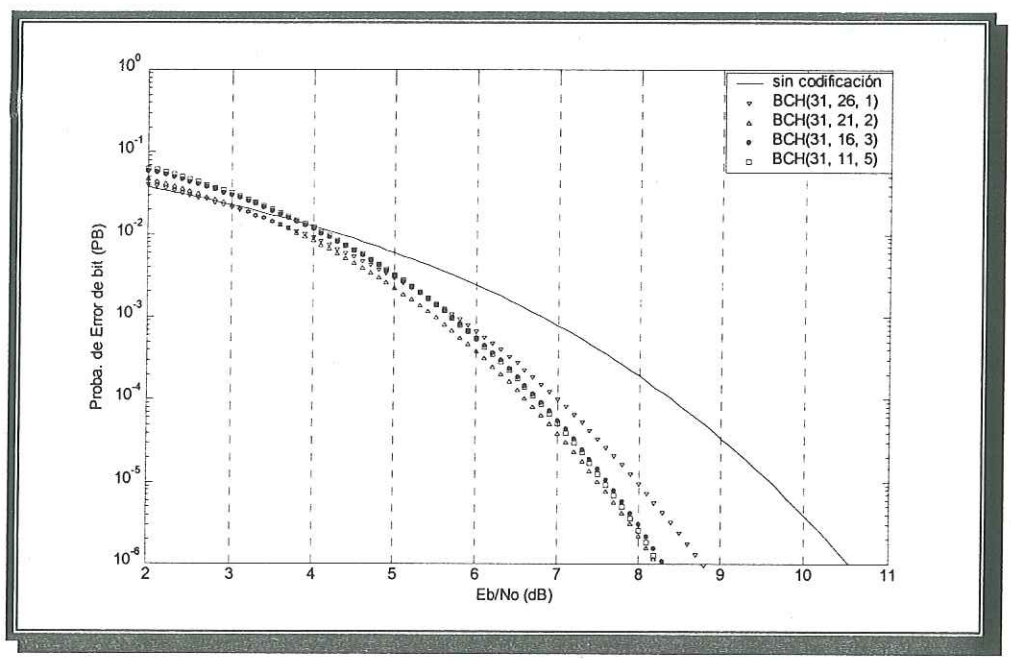

Figura 34; Respuesta teórica de la probabilidad de error de bit versus E_b/N_o, para el código BCH (n = 31) con una modulación BPSK y bajo un canal AWGN.

En la figura anterior se observa como al ir aumentando la capacidad de corrección se tiene una cierta ganancia de codificación, la cual se ve reflejada en un menor valor de E_b / N_o requerido para alcanzar una probabilidad de error. La ganancia de codificación será especificada posteriormente con más detalle.

Una vez obtenido el comportamiento teórico, se realizaron simulaciones, empleando un código *BCH*(31,*k*,*t*) como codificación de canal y la transmisión de los datos se realizó empleando, en primer caso, un canal *AWGN*, obteniendo los resultados que se muestran en la *Figura 35*, en la cual la nomenclatura empleada se refiere a 31 la longitud de la palabra código (*n*), el segundo campo (*k*) que varía desde 11 hasta 26 se refiere a la longitud de la palabra a codificar y el tercer campo (*t*) que varia desde 1 hasta 5 se refiere a la capacidad de corrección del código.

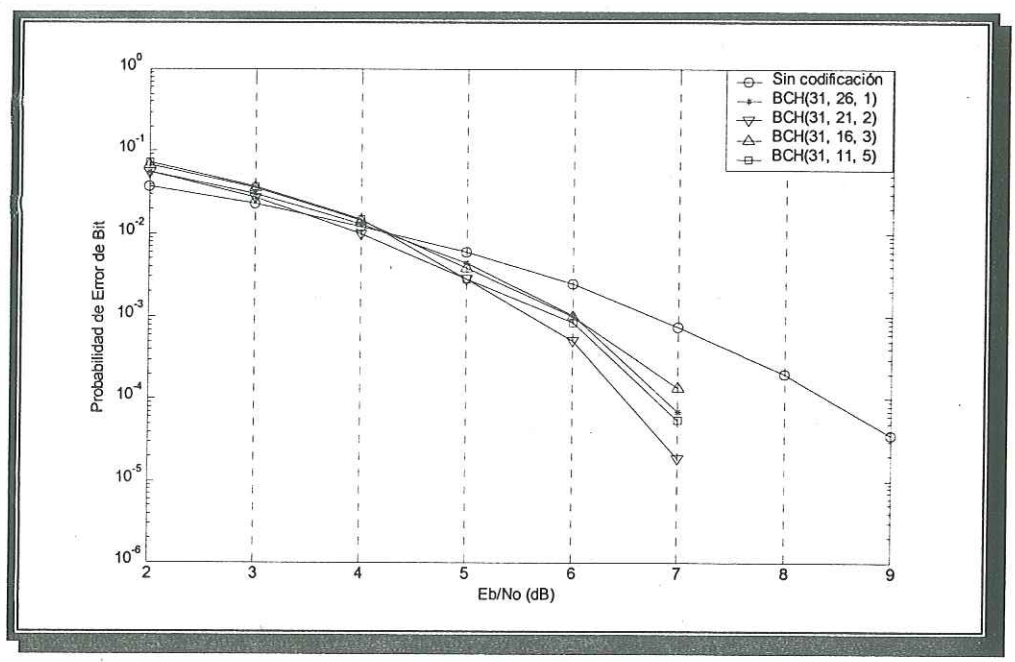

Figura 35: Probabilidad de error de bit versus E_b/N_o, para el código BCH (n=31) con una modulación BPSK y bajo un canal AWGN, obtenida mediante simulación.

En la figura anterior se puede observar como el código trabaja adecuadamente en la región del *BER* de interés (10^{-4} a 10^{-2}) presentando cierta ganancia de codificación, y cómo el código no tiene ninguna influencia en la región más desfavorable de 10^{-1}, ésto es entendible ya que el código no está diseñado para trabajar en dicha *BER*. En esta figura se puede apreciar también como para una misma capacidad de corrección de error, la ganancia de codificación es inversamente proporcional a la disminución de la probabilidad de error de bit.

Los resultados de la figura anterior al compararlos con los resultados obtenidos en la *Figura 34*, permite apreciar como los resultados obtenidos mediante la simulación son muy semejantes a los resultados teóricos, con lo que se comprueba que el sistema (codificación de canal y modulación) simulado está trabajando correctamente.

Un parámetro importante de medida en las prestaciones de los códigos correctores de error es la ***ganancia de codificación*** (*G*), la cual se puede explicar como la reducción del E_b / N_o (en dB) que se obtiene al aplicar codificación de canal, la ganancia de codificación está en función de la probabilidad de error y del tipo de modulación implementada en el sistema [Gibson, 1996], este parámetro es obtenido mediante la siguiente expresión:

$$G = (E_b / N_o)_{\text{sin codificación}} - (E_b / N_o)_{\text{con codificación}} \qquad (87)$$

donde:

E_b Energía de bit.

N_o Densidad espectral de potencia.

A manera de ejemplo la ganancia de codificación será tomada en el valor de probabilidad de error de 10^{-4}. En la *Figura 36* se observa la ganancia de codificación para este caso. Cuyos resultados son obtenidos por medio de la ecuación anterior y con ayuda de los resultados de las simulaciones de la *Figura 35*.

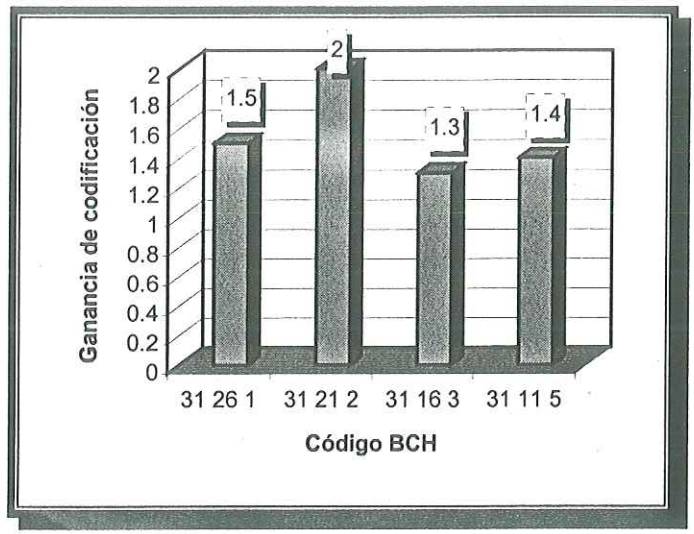

Figura 36: Ganancia de codificación del código BCH (n=31) con una modulación BPSK y en un canal AWGN a una BER de 10^{-4}.

En esta figura podemos apreciar que si bien al incrementar la capacidad de corrección del código, se obtiene una mayor ganancia de codificación, con lo cual se reduce el E_b / N_o requerido a un *BER* específico, también se observa como para una capacidad de corrección de t=3 la ganancia de codificación disminuye (1.3 *dB*). Lo anterior nos proporciona un primer criterio de decisión para definir la capacidad de corrección del código con respecto a la relación de E_b / N_o, ya que si aumentamos demasiado la capacidad de corrección del código se tendrá una disminución en la ganancia de codificación, y el principal problema que se tendrá es que se requerirá de un decodificador más complejo.

A partir de lo anterior podemos concluir que ***no necesariamente una gran capacidad de corrección de error del código bloque nos lleva a la condición óptima del mismo.***

Como se mencionó anteriormente el canal radio es un canal con una envolvente predominante que sigue una estadística tipo *Rayleigh*, por lo que es necesario que la transmisión de los datos se lleve a cabo en un canal de este tipo. En la *Figura 37* se observa como el canal *Rayleigh* simulado sigue una envolvente con esta estadística.

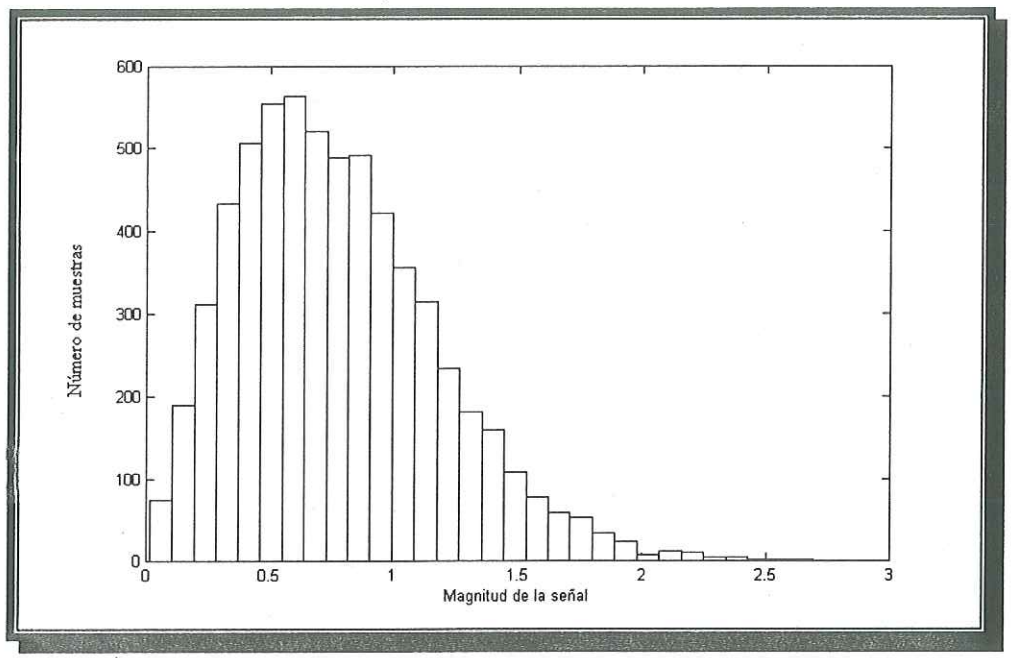

Figura 37: Histograma del canal Rayleigh simulado.

En la Figura 38 se observa el comportamiento espectral de una de las simulaciones de una señal típica con una envolvente de desvanecimiento tipo *Rayleigh*. En esta figura se aprecia como la señal transmitida por un canal *Rayleigh* sufre fuertes fluctuaciones causadas por las multitrayectorias, por lo que la señal recibida es afectada tanto en amplitud como en fase. La simulación del canal *Rayleigh* está basado en el modelo de Clark [Steele, 1992, Rappaport, 1996].

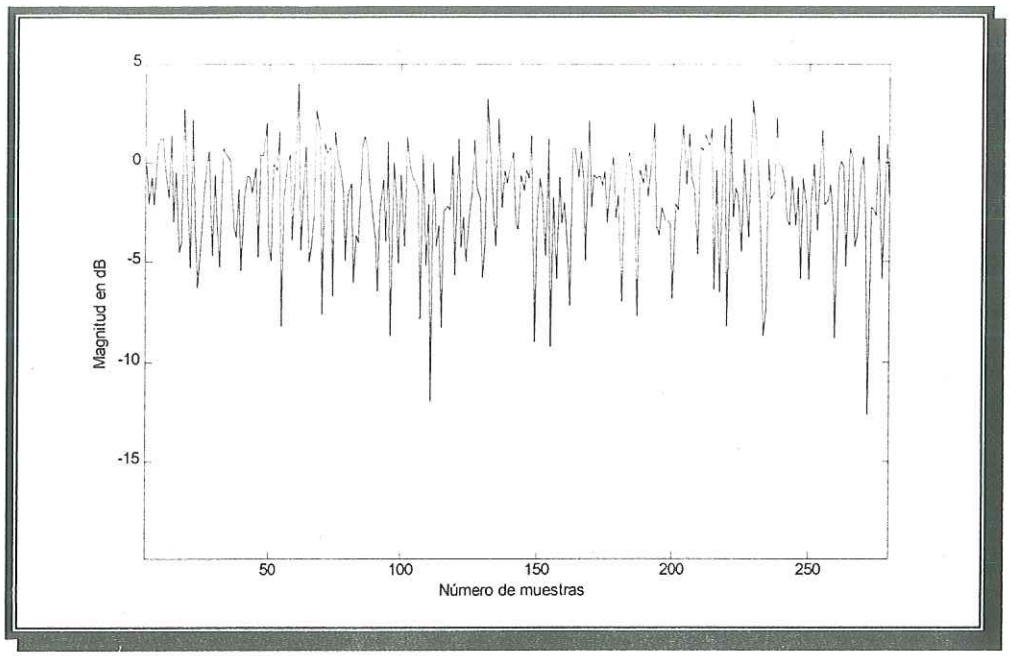

Figura 38: Envolvente de desvanecimiento tipo Rayleigh.

Con los resultados mostrados en las dos últimas figuras, se observa como el canal simulado sigue una distribución de tipo *Rayleigh.*

VI.4 Análisis de prestaciones considerando la ganancia de codificación.

Como se mencionó anteriormente, la ganancia de codificación es un parámetro que caracteriza las prestaciones de los códigos correctores de error tomando en cuenta el parámetro de E_b / N_o. Recordando lo que se mencionó en capítulos anteriores en relación a que la capacidad (M) en usuarios de un sistema *CDMA* está asociado con el parámetro de E_b / N_o por medio de:

$$M = \frac{G_p}{E_b / N_0} \qquad (88)$$

donde:

G_p Ganancia de procesado.

M Capacidad del sistema en número de usuarios.

E_b / N_o Energía de bit entre la densidad espectral de potencia del ruido.

En la expresión anterior se aprecia como al tener un valor más pequeño de E_b / N_o se tiene una mayor capacidad de usuarios en el sistema por lo que se desea tener un valor bajo de E_b / N_o. Con esta reducción de E_b / N_o se logra una disminución en la potencia de transmisión para mantener un mismo valor de probabilidad de error, reduciendo con ello las interferencias en el sistema.

Por lo mencionado anteriormente el primer parámetro a considerar en las prestaciones de los códigos bloque a analizar será la ganancia de codificación, la cual se analizará para el tamaño de paquete utilizado tanto en el *RACH* como en el *TCH*.

VI.4.1 Resultados del comportamiento del BER para el paquete utilizado en el canal RACH.

En el caso de los códigos *BCH* se consideró una longitud de palabra código de 31 y 63 bits para el canal *RACH*, mientras que en el código Reed Solomon (*RS*) se realizó una simulación para el canal *RACH*, el cual consta de una longitud de palabra código de n=15 símbolos, donde cada símbolo consta de 4 bits (n=60 bits), por lo que esta palabra código se puede comparar al del código *BCH* con n=63 bits.

VI.4.1.1 Prestaciones del código BCH.

La *Figura 39* muestra los resultados obtenidos de las simulaciones con un código *BCH* como codificación de canal y con una modulación *BPSK* considerando un canal *Rayleigh*. Al igual que en los casos anteriores se varían los parámetros k y t del código bloque.

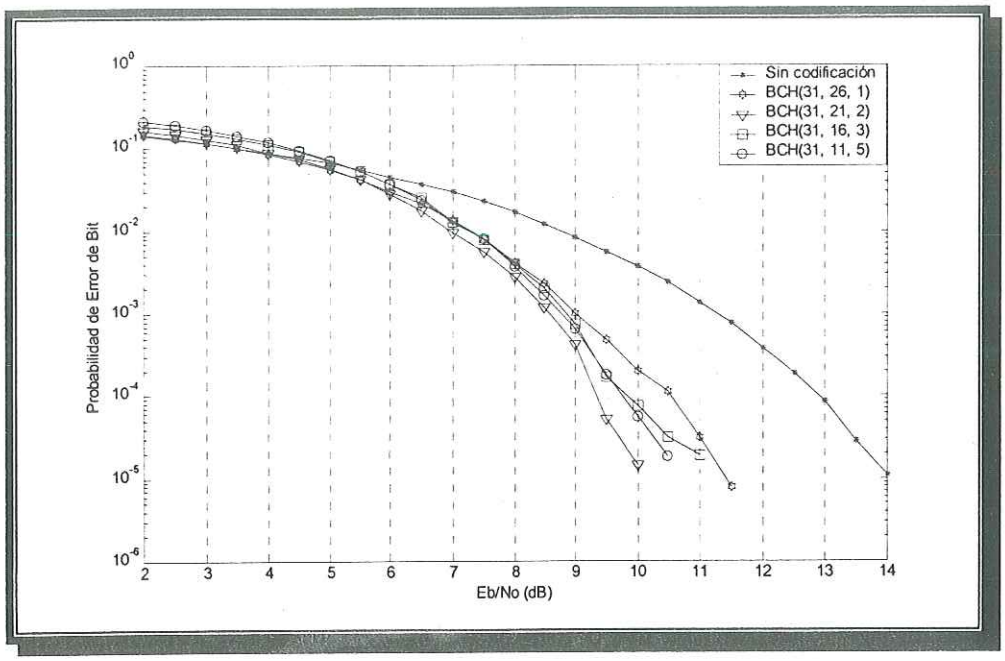

Figura 39: Probabilidad de error de bit versus E_b/N_o, para el código BCH (n=31) con una modulación BPSK y bajo un canal Rayleigh.

De acuerdo a la figura anterior y comparándola con la *Figura 35*, se puede observar como al transmitir información en un canal *Rayleigh* se requiere de un mayor E_b / N_o para obtener la misma probabilidad de error, lo anterior confirma que en un canal tipo *Rayleigh* existe una mayor probabilidad de error cuando se realiza la transmisión de los datos. Por ejemplo tomemos una capacidad de corrección de t=2 de ambas figuras, para poder obtener una probabilidad de error de 10^{-2} se requiere un E_b / N_o de 4 *dB* cuando se transmite en un canal *AWGN*, mientras que cuando se transmite en un canal *Rayleigh* se requiere un E_b / N_o de 7.2 *dB*.

La *Figura 40* muestra la ganancia de codificación que se obtiene para este caso, estos resultados son obtenidos de la figura anterior y aplicando la formula de ganancia de codificación.

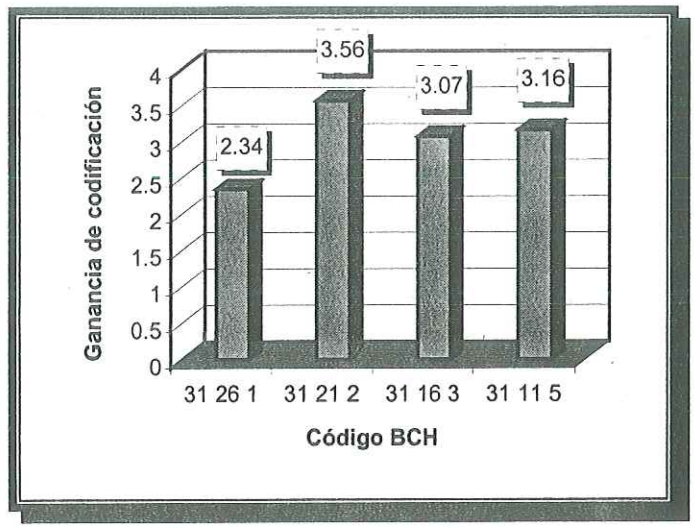

Figura 40: Ganancia de codificación del código BCH (n=31) con una modulación BPSK y en un canal Rayleigh a una BER de 10^{-4}.

En esta figura se aprecia como en un canal *Rayleigh* y para una capacidad de corrección de error de t=2 se obtiene una mayor ganancia de codificación (G=3.56 *dB*) que cuando se transmite en un canal *AWGN* (G=2 *dB* para t=2 de la *Figura 36*), pero al igual que en el canal *AWGN*, si aumentamos demasiado la capacidad correctora del código se tiene un decremento en E_b / N_o.

Para darnos una idea de la influencia de la longitud de la palabra código del canal *RACH*, se realizaron simulaciones con una longitud de palabra código de 63 bits, obteniendo los resultados de la *Figura 41*.

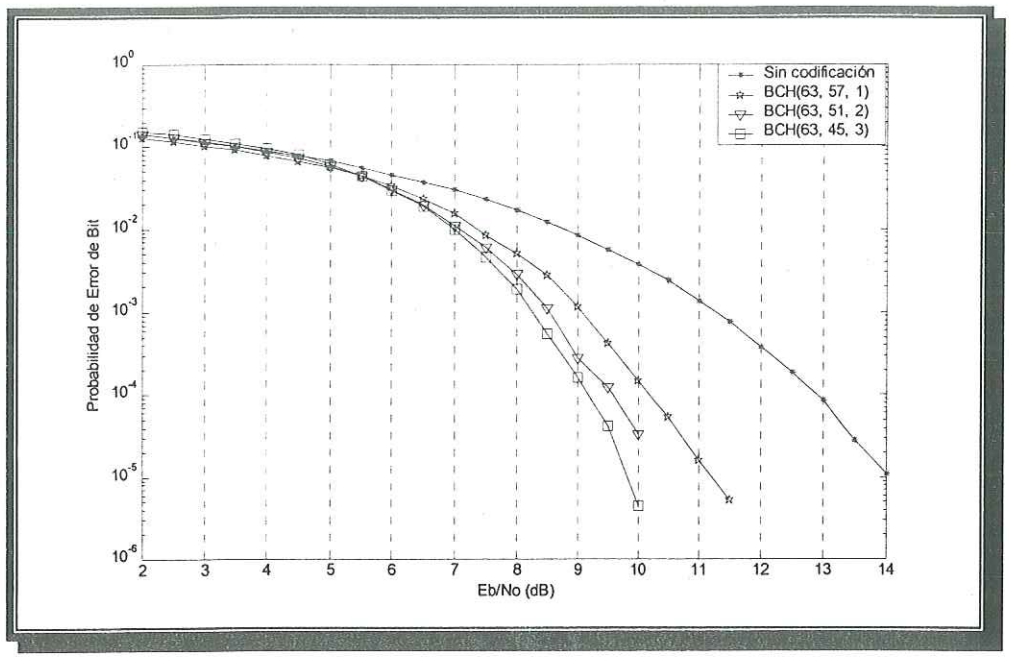

Figura 41: Probabilidad de error de bit versus E_b/N_o, para el código BCH (n=63) con una modulación BPSK y bajo un canal Rayleigh.

En esta figura se observa como los resultados obtenidos siguen el mismo comportamiento, por lo que se compararán con los resultados de la *Figura 39*, en donde se observa como al aumentar la longitud de la palabra código de 31 a 63 bits el código presenta una mejor respuesta hasta la región de 10^{-1}. Por ejemplo tomemos de ambas figuras una t=2, por lo tanto se aprecia que para n=31 la curva está por encima de la línea sin codificación hasta $E_b / N_0 = 5$, mientras que para n=63 se encuentran sobrepuestas. De lo mencionado anteriormente se puede concluir como al aumentar la longitud de la palabra código se mejoran las prestaciones del código inclusive hasta la región de 10^{-1}.

En la *Figura 42* se muestra la ganancia de codificación obtenida de la figura anterior, en esta figura se aprecia como para una mayor longitud de palabra código (n=63) se tiene una mayor ganancia de codificación a la misma capacidad correctiva del código.

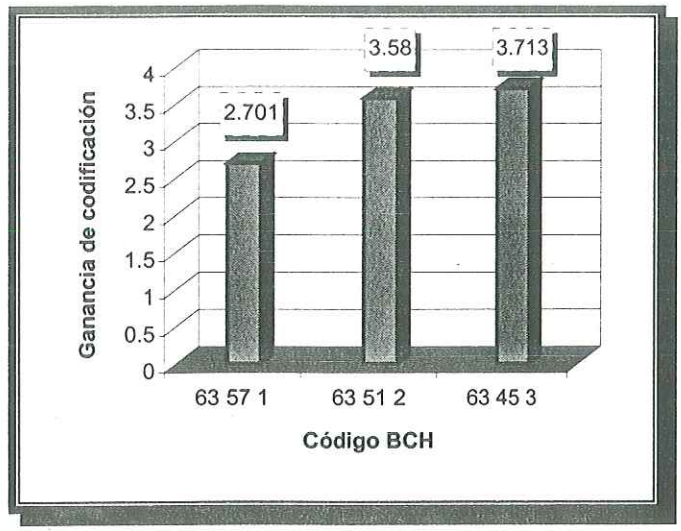

Figura 42: Ganancia de codificación del código BCH (n=63) con una modulación BPSK y en un canal Rayleigh a una BER de 10^{-4}.

En la figura anterior se observa como los resultados de ganancia de codificación siguen un comportamiento creciente, pero al igual que la *Figura 40* si aumentamos demasiado la capacidad de corrección del código la ganancia de codificación empieza a disminuir. Recordemos que el objetivo de este trabajo de tesis no es en sí encontrar el valor máximo de ganancia de codificación, sino mantener un *Throughput* elevado y constante en el margen del *BER* del canal de 10^{-6} a 10^{-2}. Con ésto se asegura que el sistema no se vea forzado a dejar de transmitir la información cuando el ruido del canal empieza a aumentar. Recordemos también que tenemos un compromiso en cuanto a complejidad del decodificador, ya que si aumentamos la capacidad de corrección de error la complejidad del decodificador también aumenta.

VI.4.1.2 Prestaciones del código RS.

La *Figura 43* muestra los resultados de las simulaciones del código *RS*, para el canal *RACH* (ideal) considerando una longitud de palabra código de n=15 símbolos, donde cada símbolo consta de 4 bits.

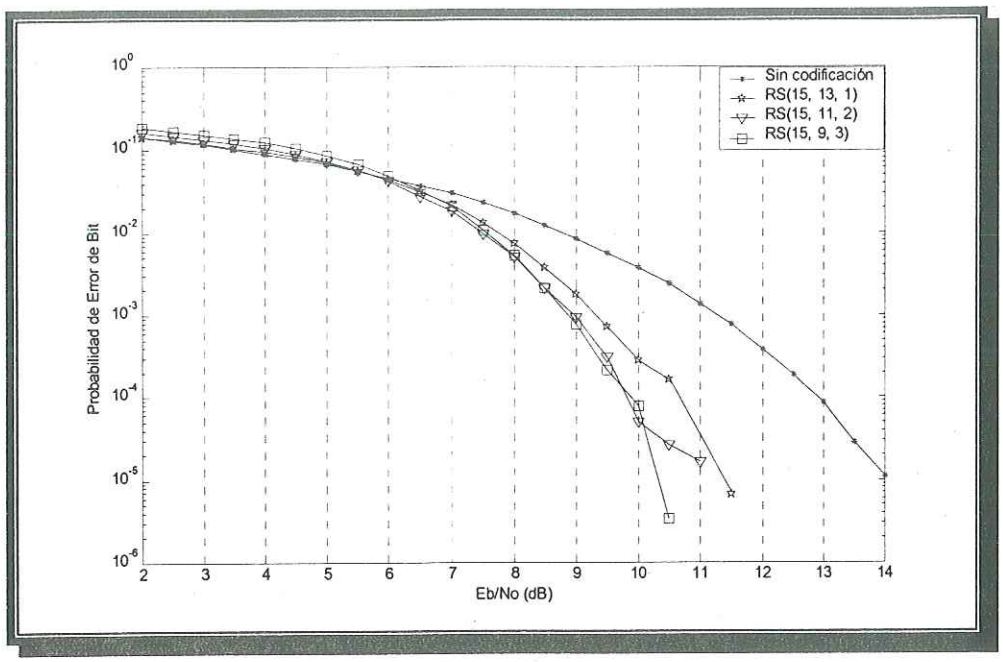

Figura 43: Probabilidad de error de bit versus E_b/N_o, para el código RS (n=15) con una modulación BPSK y bajo un canal Rayleigh.

Comparando esta figura con la *Figura 41* se observa como el código *BCH* tiene una relación de E_b / N_o menor que el código *RS* en el la zona de probabilidad de error más crítico (10^{-2}), donde además el código *BCH* presenta una mayor ganancia de codificación en el valor de probabilidad de error de 10^{-4} (*Figura 44*), por lo que se puede decir que las prestaciones del código *BCH* son mejores que las del código *RS*, tomando como referencia el parámetro de E_b / N_o como medida de eficiencia para el canal *RACH* (ideal).

La *Figura 44* muestra la ganancia de codificación para el código *RS* con una longitud de palabra de 15 símbolos, con una modulación *BPSK* y bajo la influencia de un canal Rayleigh.

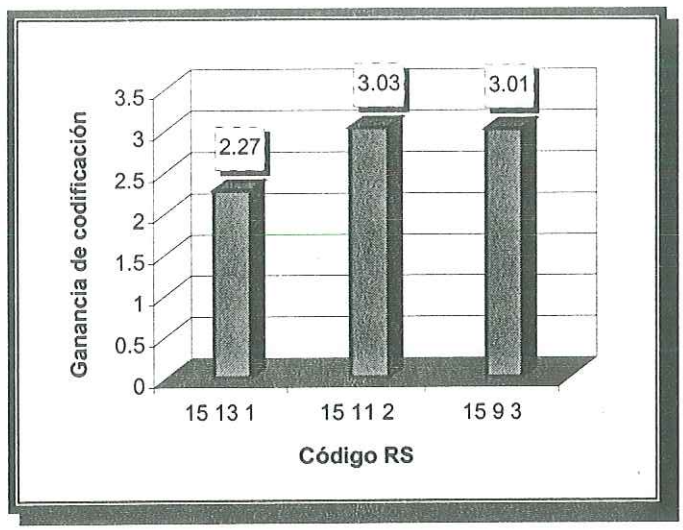

Figura 44: Ganancia de codificación del código RS (n=15) con una modulación BPSK y en un canal Rayleigh a una BER de 10^{-4}.

En esta figura se aprecia como para el canal *RACH* el código *RS* presenta una menor ganancia de codificación que el código *BCH* (3.03<3.56 con t=2 de la *Figura 40*), también se observa como al aumentar la capacidad correctiva de 2 a 3 se tiene una disminución en la ganancia de codificación, por lo que se reitera, que no necesariamente una mayor capacidad correctiva nos lleva a los parámetros óptimos del código.

VI.4.2 Comportamiento del BER del canal para el canal de transmisión (TCH).

Para el caso de los códigos *BCH* se consideró una longitud de palabra código 1023 bits para el canal *TCH*, mientras que en el código Reed Solomon (*RS*) se utilizó una longitud de palabra código de 127 símbolos que proviene de un código *RS* recortado (*RS* de 255 símbolos, donde cada símbolo consta de 8 bits), dando un total de 1016 bits, los cuales pueden ser comparados con 1023 bits que se utilizó en el código *BCH* para la simulación del canal *TCH*.

VI.4.2.1 Resultados del código BCH.

En la *Figura 45* se presentan los resultados obtenidos en las simulaciones para la transmisión del canal *TCH* (ideal), implementando un código *BCH* con una modulación *BPSK*, y bajo un canal tipo *Rayleigh*.

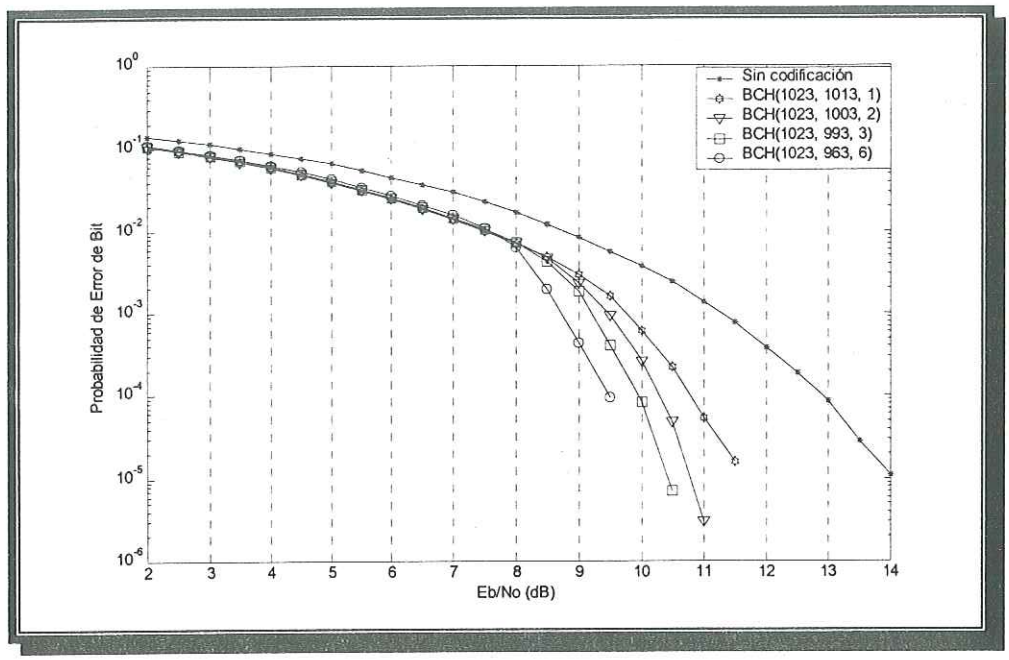

Figura 45: Probabilidad de error de bit versus E_b/N_o, para el código BCH (n=1023) con una modulación BPSK y bajo un canal Rayleigh.

En la figura anterior se aprecia como al aumentar *n* a 1023 bits, el código corrector de error trabaja eficientemente para todos los valores de E_b / N_0, no como en el caso de *n*=31 (*Figura 39*), en donde el código empieza a trabajar adecuadamente a partir de 4 a 5 *dB*, o como en el caso de n=63 (*Figura 41*) en donde la respuesta del código se encuentra sobrepuesta con el resultado sin codificación de canal en el margen de 2 a 4 *dB*. Con ésto se reitera lo que se mencionó anteriormente entre mayor es la longitud de la palabra código, se tiene una mejor respuesta del código en el extremo de la región más desfavorable de 10^{-4} a 10^{-2}.

La *Figura 46* muestra la ganancia de codificación para una n=1023 y diferentes capacidades de corrección del código.

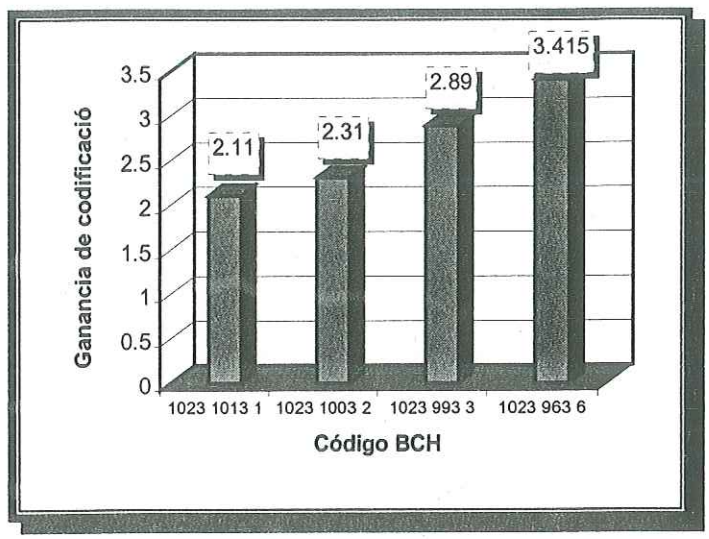

Figura 46: Ganancia de codificación del código BCH (n=1023) con una modulación BPSK y en un canal Rayleigh a un BER de 10^{-4}.

Comparando esta figura con las *figuras 40* y *42* de ganancia de codificación, se aprecia como la ganancia de codificación para n=1023 (G=2.31 para t=2), disminuye para una misma capacidad de corrección del código para una n=63 (G=3.58 para t=2) y n=31 (G=3.56 para t=2), por lo que no siempre se cumple de que a mayor longitud de palabra código (n) mayor ganancia de codificación (G), pero existen excepciones, tal como es el caso de n=63 que tiene una mayor ganancia de codificación sobre n=31. El comportamiento de esta figura, al igual que las anteriores es creciente conforme aumentemos la capacidad de corrección del código, pero recordemos que llega un valor de t donde la ganancia de codificación empieza a disminuir. Otro aspecto importante a mencionar es que está muy relacionada la capacidad de corrección de error con la longitud de palabra código. A mayor longitud de palabra código se requiere una mayor capacidad correctiva de error del decodificador y por lo tanto se presenta una mayor complejidad del decodificador.

VI.4.2.2 Resultados del código RS.

La *Figura 47* muestra los resultados de las simulaciones del código *RS*.

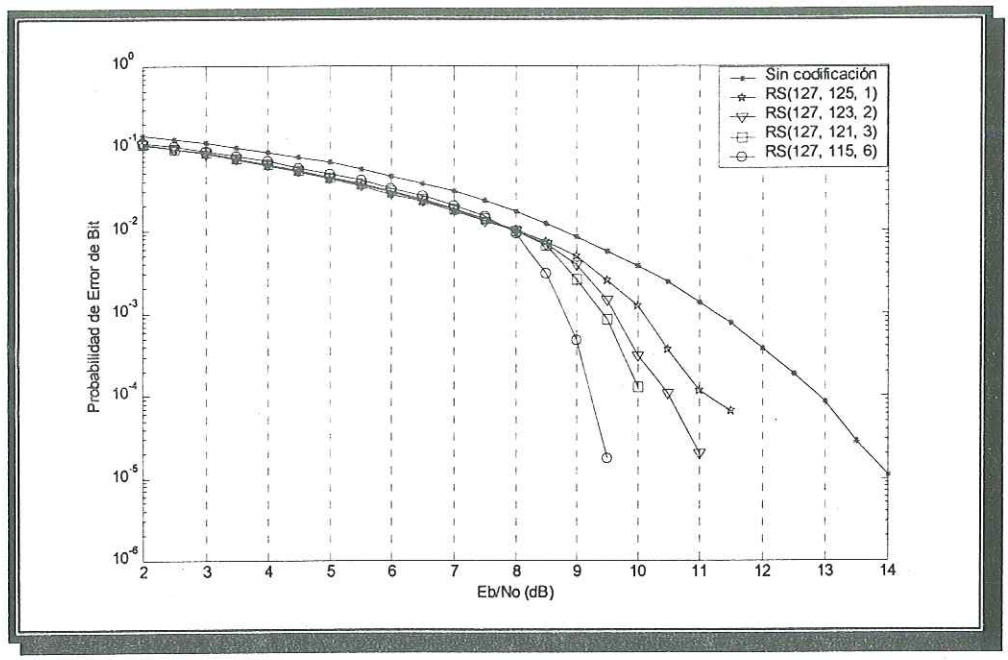

Figura 47: Probabilidad de error de bit versus E_b/N_o, para el código RS (n=127) con una modulación BPSK y bajo un canal Rayleigh.

De dicha figura, al igual que el código *BCH*, a mayor longitud de palabra código mejor es la respuesta de la probabilidad de error (los resultados de las simulaciones están por debajo de la curva sin codificación de canal). Comparando la *Figura 45* y la *Figura 47* se aprecia como el código *BCH* ocupa menos E_b / N_o (7 *dB*) que el código *RS* (8 *dB*) para alcanzar una probabilidad de error de 10^{-2}, por lo que en este punto de probabilidad de error el código tiene mejores prestaciones en cuanto a E_b / N_o, pero no podemos decir todavía si el *BCH* es mejor que el *RS* en cuanto a reducción de E_b / N_o ésto se podrá asegurar hasta que analicemos la ganancia de codificación en el valor del *BER* de 10^{-4}.

La *Figura 48* representa la ganancia de codificación que se obtuvo de las simulaciones de la figura anterior.

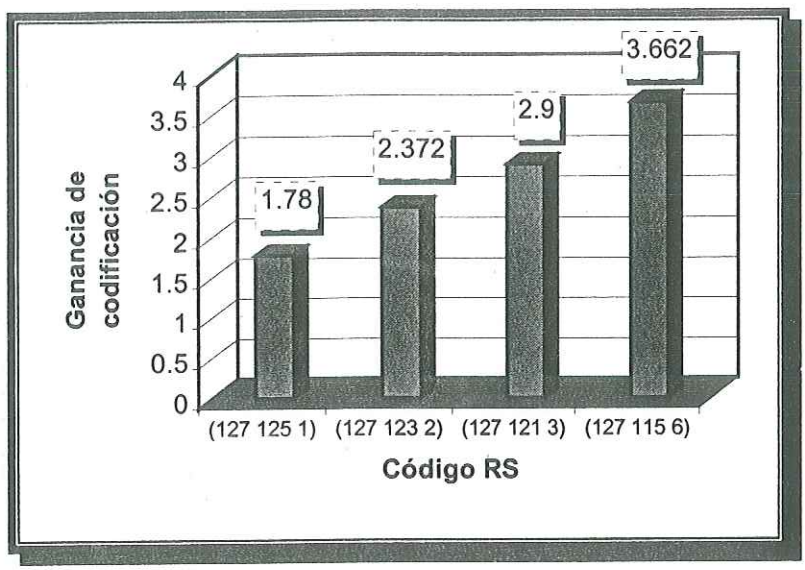

Figura 48: Ganancia de codificación del código RS (n=127) con una modulación BPSK y en un canal Rayleigh a un BER de 10^{-4}.

Esta figura nos muestra como para una $t>1$, el código *RS* tiene una mayor ganancia de codificación que el *BCH* en el valor del *BER* de 10^{-4}. por lo que se puede concluir que para una $t>1$ el código *RS* tiene mejores prestaciones para el canal *TCH* en cuanto a reducción de E_b / N_o que el *BCH*.

Otro parámetro que está fuertemente relacionado con la eficiencia de los códigos correctores de error es el *Throughput*. Como se mencionó anteriormente es este parámetro el que nos interesa analizar, ya que nuestro propósito es mantener un *Throughput* elevado y constante en la región de interés de *BER* del canal de 10^{-4} a 10^{-2}.

VI.5 Análisis del Throughput.

El *Throughput* (caudal eficaz) es el parámetro de interés en este trabajo, el cual está definido como el número medio de bits de información aceptados por el receptor por símbolos transmitidos al canal y es calculado por la siguiente expresión [Covarrubias, 1999]:

$$S = \frac{k}{R} \qquad (89)$$

donde k representa la longitud de la parte de información en una trama de información (k bits) y donde R es el número medio de bits totales transmitidos para que el receptor reciba o decodifique una trama correctamente.

R a su vez esta definida como:

$$R = [n + k(t)] \cdot [1 + \sum_{i=1}^{t} (p'_t)^t] \qquad (90)$$

$p'_t = 1 - p_t$, donde p_t es la probabilidad de que el receptor reciba la trama de información con t o menos errores, siendo:

$$p_t = \sum_{i=0}^{t} \binom{n}{i} p^i (1-p)^{n-i} \qquad (91)$$

donde p es la probabilidad de error del canal (*BER*).

Sea n la longitud de las tramas de paridad y p_a la probabilidad de que la trama de paridad A_i sea errónea. Por lo tanto:

$$p_a = 1 - (1-p)^n \qquad (92)$$

De esta forma, *K(t)* se puede expresar como:

$$k(t) = n \cdot \sum_{i=1}^{t} \frac{p(i)}{(1-p_a)} \qquad (93)$$

donde $p(i)$ es la probabilidad de que la trama de información contenga exactamente i errores.

$$p(i) = \binom{n}{i} p^i (1-p)^{n-i} \qquad (94)$$

VI.5.1 Resultados del Throughput del canal RACH ideal.

Al igual como se realizó en los resultados de análisis del *BER*, para el análisis del *Throughput* se analizarán primero una longitud de palabra código de 31 y 63 bits aplicables a un código corrector de error *BCH* y una longitud de palabra código de 15 símbolos, donde cada símbolo consta de 4 bits para el código *RS*.

VI.5.1.1 Throughput del canal RACH ideal empleando un código BCH.

En la *Figura 49* se presenta el comportamiento del *Throughput* versus *BER* del canal para un código corrector de error *BCH* con una longitud de palabra código de n=31 y diferentes capacidades de corrección de error (t).

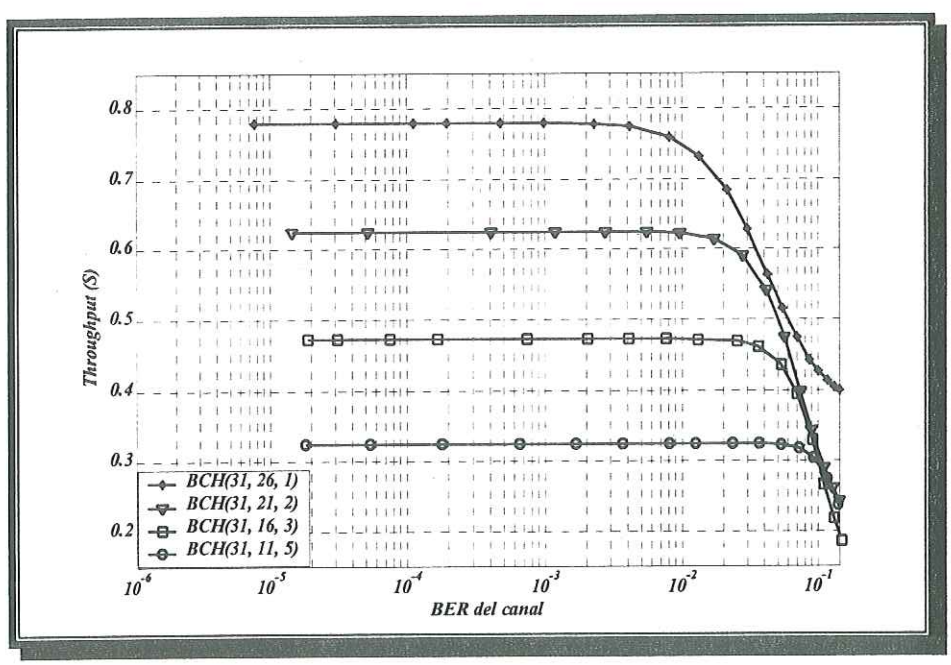

Figura 49: Throughput en función del BER del canal para códigos BCH binarios de longitud n=31 con capacidades de corrección t=1,2,3 y 5.

En la figura anterior se puede observar como al ir aumentando la capacidad de corrección del código el *Throughput* empieza a disminuir (0.78 para t=1 a 0.324 para t=5, a un *BER* de 10^{-4}), por lo que se llega a establecer un criterio de decisión en cuanto al *Throughput* del sistema contra la capacidad correctiva del código (t). De dicha figura se aprecia como para una capacidad correctiva de t=1 se tiene el *Throughput* más elevado cuando el canal no introduce muchos errores, sin embargo cuando el canal es más ruidoso el mejor comportamiento pasa primero para t=2, después al de t=3 y por último al de t=5. Esto es entendible ya que si se aumenta el *BER* del canal, el canal introduce más errores, por lo tanto existe un mejor comportamiento del código con una mayor capacidad correctiva. Recordemos que al utilizar una mayor capacidad de corrección, la ganancia de codificación puede disminuir, tal como se mostró en la *Figura 40* donde la ganancia de decodificación empieza a disminuir a partir de t=3, y trayendo como consecuencia un decodificador mucho más complejo. Por lo que la mejor elección del código no es siempre el de mayor capacidad de corrección de error. En esta figura también se observa que para una capacidad de corrección de 3 y 5 se tienen valores bajos de *Throughput* de 0.472 y 0.324 respectivamente. Esto se debe a que se están añadiendo más de la mitad de bits de redundancia y recordemos que el *Throughput* es el número neto de bits recibidos correctamente sin retransmisión entre el número de bits de información transmitidos, dando como resultado un *Throughput* demasiado bajo.

En la *Figura 50* se presenta la gráfica del *Throughput* versus *BER* del canal, para una n=63 bits y diferentes capacidades de corrección de error (t).

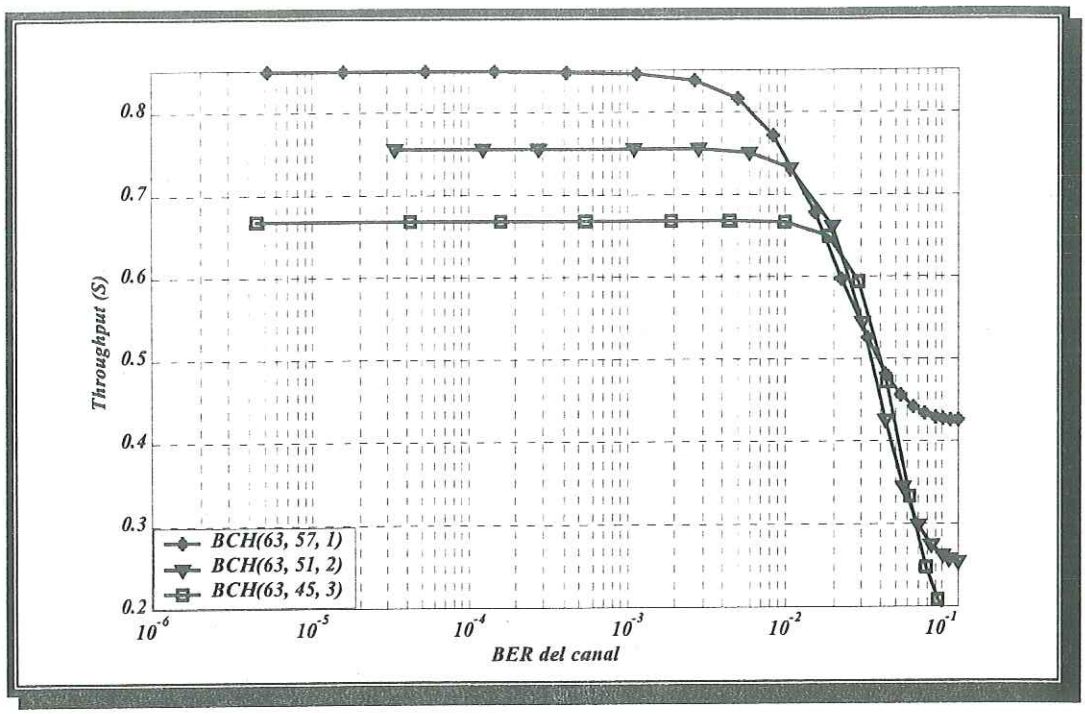

Figura 50: Throughput en función del BER del canal para códigos BCH binarios de longitud n=63 con capacidades de corrección t=1,2 y 3.

Comparando esta figura con la figura anterior, se aprecia como al aumentar la longitud de la palabra código de n=31 a n=63, el *Throughput* aumenta, pero tiene una caída más rápida en la región del *BER* del canal de 10^{-4} a 10^{-2}. Por ejemplo tomemos de ambas figuras las curvas para t=2. Para n=31 se tiene un *Throughput* (S=0.625) constante en todo el margen del *BER* del canal de 10^{-6} a 10^{-2}, mientras que para n=63 se tiene un *Throughput* (S=0.7555) constante en el margen del *BER* del canal de 10^{-6} a 10^{-3}, y una disminución del *Throughput* del 2.8458% en el margen del *BER* del canal de 10^{-3} a 10^{-2}.

VI.5.1.2 Resultados del Throughput considerando un código RS.

La *Figura 51* muestra los resultados del *Throughput* contra el *BER* del canal del código *RS*, para una longitud de palabra código de 15 símbolos (60 bits).

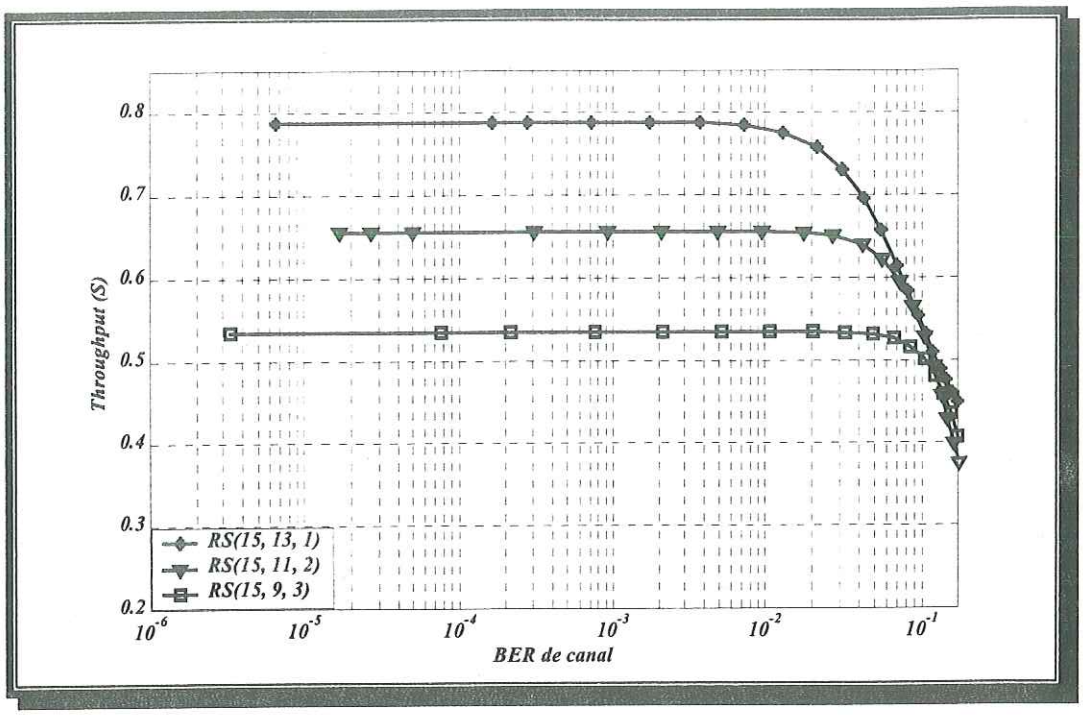

Figura 51: Throughput en función del BER del canal para códigos RS de longitud n=15 con capacidades de corrección t=1,2 y 3.

Comparando esta figura con la *Figura 50*, se observa como el código *BCH* tiene un mayor *Throughput* para el mismo valor de capacidad de corrección de error del código, pero la caída del *Throughput* se presenta primero al utilizar un código *BCH*. Por ejemplo, para t=2 se tiene que para el código *BCH* se tiene un decremento del *Throughput* del 2.8458% en el margen del *BER* de 10^{-4} a 10^{-2}, mientras que para el mismo valor de t en el código *RS* el *Throughput* tiene una caída de 0.0763 en el margen del BER de 10^{-4} a 10^{-2}, pero con un valor menor del *Throughput.*

VI.5.2 Resultados del Throughput para el canal de transmisión (TCH ideal).

A continuación se muestran los resultados del *Throughput* para el canal *TCH*, para el caso de los códigos *BCH* se consideró una longitud de palabra código 1023 bits para el canal *TCH*, mientras que en el código *Reed Solomon* (*RS*) se utilizó una longitud de palabra

código de 127 símbolos, donde cada símbolo consta de 8 bits dando un total de 1016 bits, los cuales pueden ser comparados con 1023 bits que se utilizó en el código *BCH* para la simulación del canal *TCH*.

VI.5.2.1 Resultados del código BCH.

La *Figura 52* muestra los resultados del *Throughput* contra el *BER* del canal.

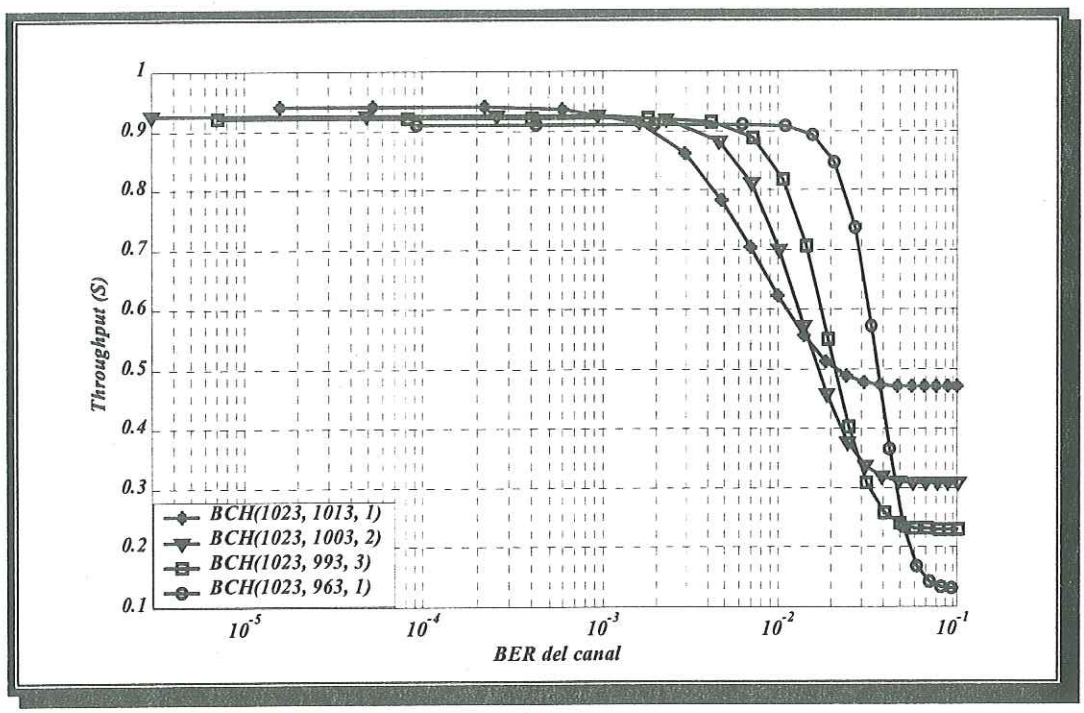

Figura 52: Throughput en función del BER del canal para códigos BCH binarios de longitud n=1023 con capacidades de corrección t=1,2,3 y 6.

En esta figura se puede observar como al aumentar la longitud de la palabra código a 1023, se tiene un *Throughput* más elevado ($S \cong 1$), pero se tiene una caída del *Throughput* más rápida en la región del *BER* del canal de interés, por ejemplo para $t=1$ se tiene una caída del 34.13%, para $t=2$ se presenta una caída del 23.22%, para $t=3$ se presenta un decremento de 9.82%.

VI.5.2.2 Resultados del código RS.

En la *Figura 53* se representa el *Throughput* contra el BER del canal.

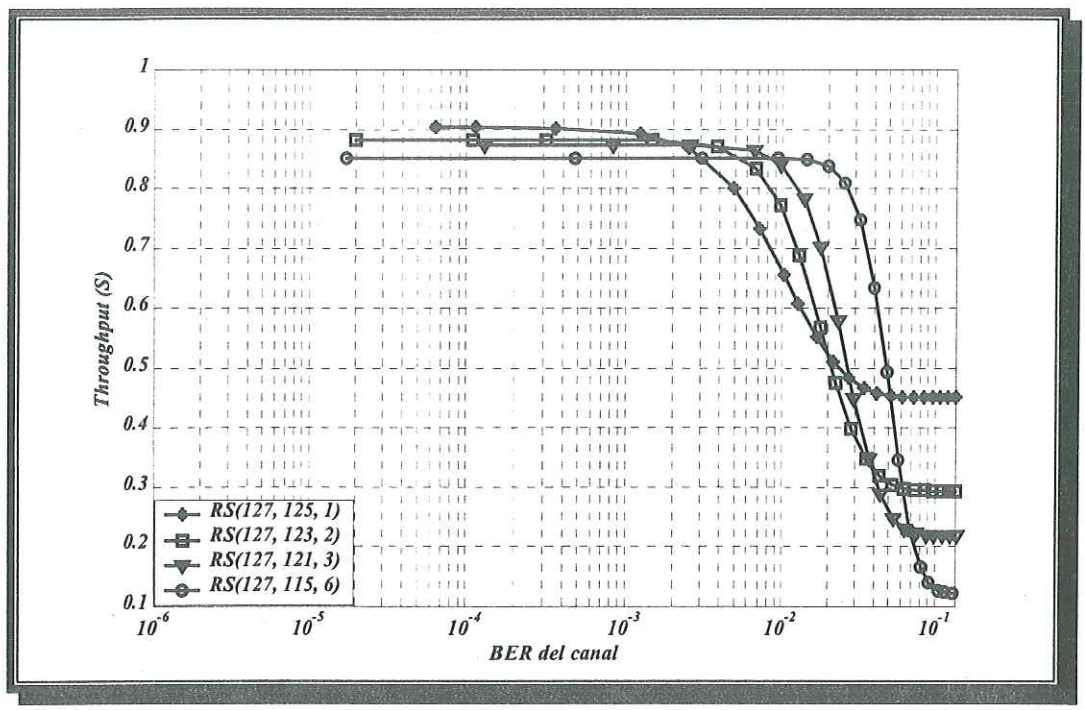

Figura 53: Throughput en función del BER del canal para códigos RS de longitud n=127 con capacidades de corrección t=1,2,3 y 6.

Comparando esta figura con la *Figura 52*, se observa que para el código *BCH* se tiene el *Throughput* más elevado, pero la caída del *Throughput* se presenta más prematuramente que cuando se utiliza el código *RS*. Por ejemplo tomemos las curvas de la capacidad de corrección igual a 3 de ambas figuras, el código *BCH* presenta un *Throughput* constante de 0.9203 en la región del *BER* del canal de 10^{-6} a 10^{-3} y presenta una caída del *Throughput* de 9.82% en la región del *BER* del canal de 10^{-3} a 10^{-2}, En cambio para el código *RS* se tiene un *Throughput* de 0.8726, el cual es constante en la región del *BER* del canal de 10^{-6} a 10^{-3} y presenta una caída del 4.034%.

VI.6 Parámetros óptimos para el canal ideal RACH.

Para encontrar los parámetros óptimos de los códigos *BCH* y *RS* del canal *RACH* nos basaremos en la *Tabla VIII* que es una síntesis de los resultados representados se obtuvieron anteriormente, donde el campo *n* se refiere a la longitud de la palabra código, *k* al bloque de bits o símbolos a codificar, *t* la capacidad de corrección del código, E_b / N_o en *BER* 10^{-2} se refiere al valor de E_b / N_o para lograr una probabilidad de error de 10^{-2}, *G* en *BER* 10^{-4} se refiere a la ganancia de codificación en el valor de referencia del *BER* de 10^{-4}, R_c a la velocidad del código, *n/k* al incremento del ancho de banda del sistema, *S* es el máximo valor del *Throughput* y por ultimo Caída del *S* en *BER* 10^{-4} a 10^{-2} se refiere a la caída que sufre el *Throughput* en la región de interés.

Tabla VIII: Resultado de los códigos BCH y RS para el canal RACH.

Código	*n*	*k*	*t*	E_b/N_o en *BER* 10^{-2}	*G* en *BER* 10^{-4}	R_c	*n/k*	*S*	Caída del S en *BER* 10^{-4} a 10^{-2}
BCH	31	26	1	7.29 dB	2.34 dB	0.8387	1.1923	0.78	4.1025 %
BCH	31	21	2	7 dB	3.56 dB	0.6774	1.4761	0.625	0 %
BCH	31	16	3	7.25 dB	3.07 dB	0.5161	1.9375	0.4722	0 %
BCH	31	11	5	7.26 dB	3.16 dB	0.3548	2.8181	0.3242	0 %
BCH	63	57	1	7.37 dB	2.701 dB	0.9047	1.1052	0.848	12.2614 %
BCH	63	51	2	7.07 dB	3.58 dB	0.8095	1.2352	0.7555	2.8458 %
BCH	63	45	3	7 dB	3.713 dB	0.7142	1.4	0.668	0.2994 %
RS	15	13	1	7.724 dB	2.27 dB	0.8666	1.1538	0.7869	1.0802 %
RS	15	11	2	7.474 dB	3.03 dB	0.7333	1.3636	0.655	0.0763 %
RS	15	9	3	7.55 dB	3.01 dB	0.6	1.6666	0.534	0 %

Como se ha mencionado anteriormente el principal parámetro de medida de eficiencia para nuestro sistema es el *Throughput* ya que se desea mantener un *Throughput* elevado y constante en todo el margen del *BER* de 10^{-6} a 10^{-2}, por lo que será el primer parámetro en el que buscaremos los parámetros óptimos del código corrector de error, por lo mencionado anteriormente los parámetros de los códigos que cumplen esta condición son los que se muestran en la *Figura 54*.

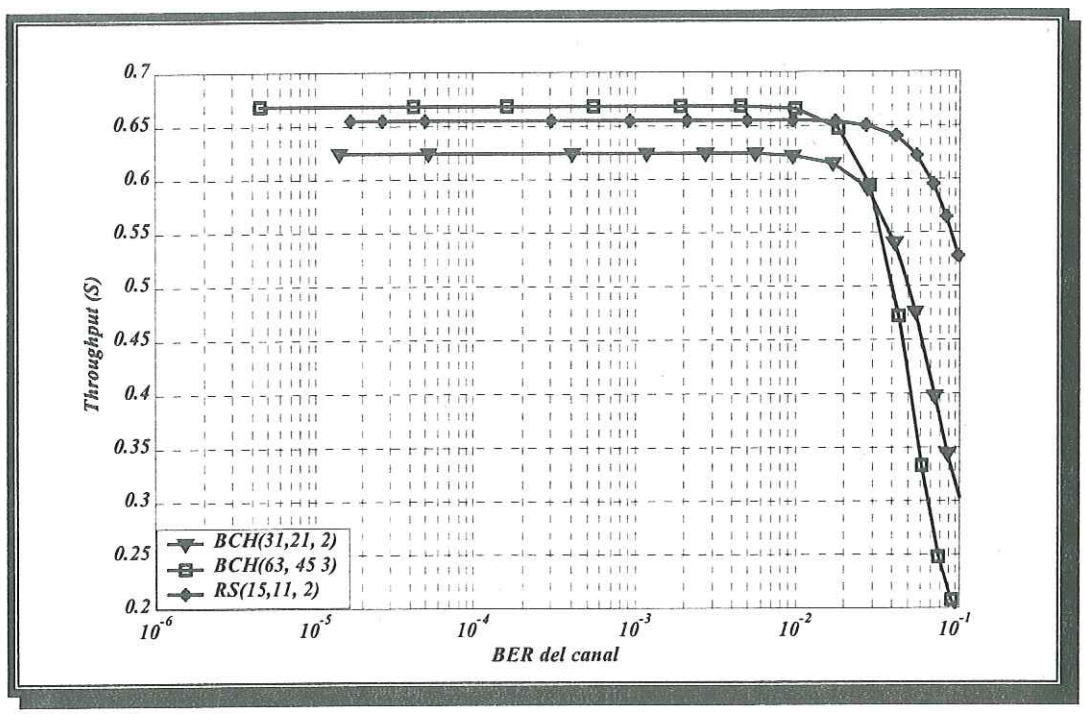

Figura 54: Parámetros óptimos (n, k, t) de los códigos BCH y RS para el canal RACH ideal.

De esta gráfica se aprecia como el código *RS* (n=15) tiene la caída del *Throughput* menos abrupta por lo que uno pude pensar que es el más apropiado para el canal *RACH*, pero analicemos para estos mismos parámetros de códigos los demás resultados de la *Tabla VIII*, dando como resultado que el código *RS* tiene la mínima ganancia de codificación, por lo que si fuera escogido como el código corrector de error para el canal *RACH*, el sistema *CDMA* tendría una capacidad menor que si se utilizarán los códigos *BCH*. Ahora bien ¿cual

de los dos posibles códigos *BCH* es el apropiado para el canal *RACH*?. Para responder lo anterior hay que mencionar que otro compromiso del sistema es que el decodificador sea lo más sencillo posible, **por lo que los parámetros óptimos para el canal *RACH* propuestos son los del código *BCH*(31, 21, 2)**, ya que además de ser óptimo implica una etapa de decodificación siempre al considerar una capacidad de corrección de error de 2 suficiente para la mejor prestación del sistema.

VI.7 Parámetros óptimos para el canal ideal TCH.

Para encontrar los parámetros óptimos de los códigos *BCH* y *RS* para el canal *TCH* nos basaremos en la *Tabla IX*.

Tabla IX: Resultado de los códigos BCH y RS para el canal TCH.

Código	n	k	t	E_b/N_o en *BER* 10^{-2}	G en *BER* 10^{-4}	R_c	n/k	S	Caída del S en *BER* 10^{-4} a 10^{-2}
BCH	1023	1013	1	7.4898 dB	2.11 dB	0.99	1.0098	0.9413	34.13 %
BCH	1023	1003	2	7.5398 dB	3.31 dB	0.98	1.0199	0.9248	23.22 %
BCH	1023	993	3	7.5898 dB	3.89 dB	0.97	1.30	0.9203	9.82 %
BCH	1023	963	6	7.5898 dB	3.415 dB	0.94	1.062	0.9103	0 %
RS	127	125	1	7.951 dB	1.78 dB	0.98	1.016	0.9029	26.90 %
RS	127	123	2	7.921 dB	2.372 dB	0.96	1.0325	0.8824	13.45 %
RS	127	121	3	7.981 dB	2.9 dB	0.95	1.0496	0.8726	4.034 %
RS	127	115	6	8.041 dB	3.662 dB	0.9	1.1043	0.85	0 %

Siguiendo el mismo criterio que en el canal *RACH* para decidir cuales parámetros (n, k , t) del código son los apropiados para el canal *TCH*, se llega a la conclusión que el

código *BCH* y *RS* más apropiado para la transmisión del canal *TCH* son los parámetros de los códigos que se muestra en la *Figura 55*.

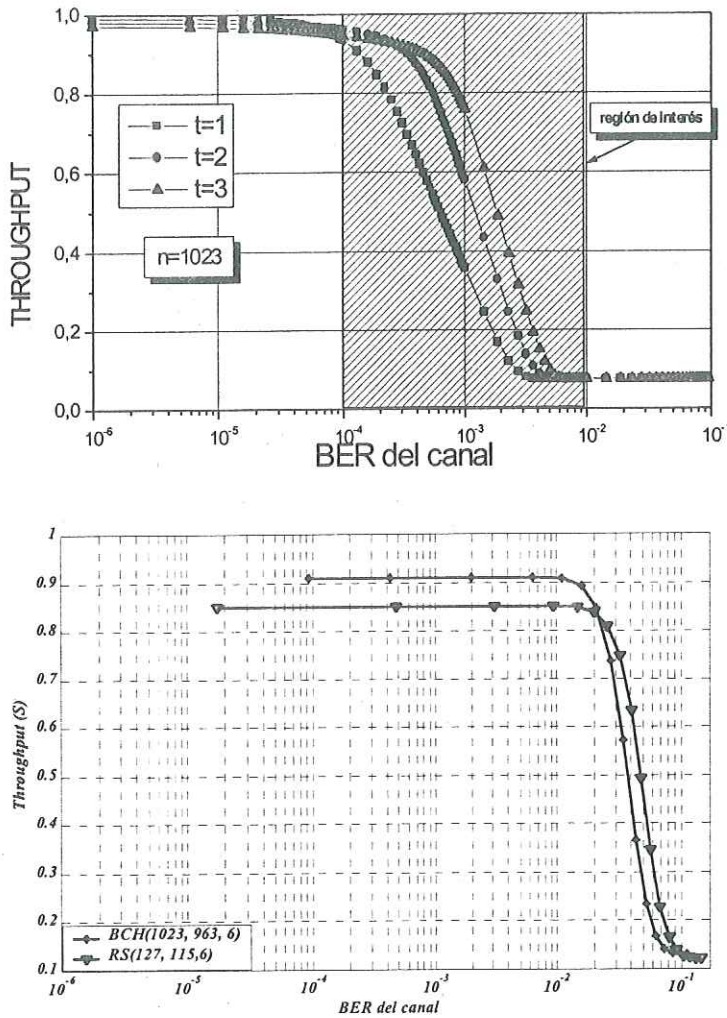

Figura 55: Parámetros óptimos (n, k, t) de los códigos BCH y RS para el canal TCH.

De esta figura se observa como el código *BCH* tiene un *Throughput* más elevado en la región del *BER* de 10^{-6} a 10^{-2}, cumpliendo con el objetivo que se había propuesto desde un principio, y de la tabla se aprecia como el código *BCH* tiene una mejor respuesta del *BER* en el valor de 10^{-2}, por lo que es más eficiente cuando el canal se torna más ruidoso, **por lo que los parámetros óptimos para el canal *TCH* propuestos son los del código *BCH*(1023, 963, 6)**.

VI.8 Conclusiones.

En este capítulo *VI* se demostró que los códigos *BCH* y *RS* son apropiados para la transmisión de datos bajo canales de transmisión ruidosos como lo es el canal radio, ya que logran mantener un *Throughput* constante y elevado en todo el margen del *BER* de 10^{-6} a 10^{-2}.

Como se mencionó anteriormente el código *BCH* mantiene un *Throughput* constante pero la caída del mismo se da más rápido que el del código *RS*, por lo que cuando se quiere elegir los parámetros óptimos se tiene que establecer un compromiso en cuanto a *Throughput* y *BER* del canal, en nuestro caso tanto para el canal de petición de servicio (*RACH*) como para el canal de transmisión de los datos (*TCH*), se busca mantener un *Throughput* elevado y constante en todo el margen del *BER* de 10^{-6} a 10^{-2}, lo cual se cumplió tanto para el canal *RACH* ideal como para el canal *TCH* ideal.

Como fue mencionado en este capítulo se debe de tener cuidado cuando se elijan los parámetros (*n, k, t*) del código, ya que si aumentamos demasiado la capacidad correctiva del código se tendrá una disminución en la ganancia de codificación trayendo como consecuencia una reducción en la capacidad del sistema, un mayor aumento en el ancho de banda, teniéndose además un decodificador más complejo.

El código que se recomienda para el canal *RACH* ideal es el *BCH*(31, 21, 2), ya que éste mantiene un *Throughput* constante en la región del *BER* de interés, tiene una mejor ganancia de codificación lo cual influye en la capacidad del sistema y el decodificador es menos complejo.

A partir de los resultados obtenidos y comparándolos con el código bloque utilizado por la plataforma europea de los sistemas *3G UMTS-2000*, donde sita que el código *RS*

utilizado para el canal *TCH* en los sistemas de *3G*, es un código externo con una velocidad de aproximadamente *4/5*, comparando esto con los resultados de los parámetros óptimos del código *RS* en el canal *TCH*, nos damos cuenta que el código *RS* propuesto tiene una velocidad de código de 0.9055, la cual es muy elevada. Esto se puede justificar, supongamos que los parámetros (*n, k, t*) del código *RS* propuesto son (127, 103, 12), con lo cual tenemos una velocidad de código de 0.8110 y una capacidad de corrección de 12 símbolos, pero recordemos que al aumentar la capacidad de corrección del código el *Throughput* del sistema se ve afectado considerablemente, por lo que para mantener un *Throughput* elevado los sistemas *3G* echan mano de los sistemas *ARQ híbrido tipo II*, con esto se tiene un *Throughput* elevado y una mayor capacidad correctiva del sistema.

VII Conclusiones y recomendaciones.

VII.1 Conclusiones.

Recordando que el objetivo de este trabajo de tesis fue proponer un esquema de codificación eficiente que permitiera asegurar la confiabilidad en la transmisión de paquetes, bajo la presencia de ruido y desvanecimientos en un entorno de comunicaciones móviles celulares, y como consecuencia mantener un *Throughput* elevado y constante en el margen del *BER* del canal de 10^{-6} hasta 10^{-2}, pero sobre todo manteniendo la idea de plantear un codificador y decodificador sencillo.

Para lograr los objetivos mencionados anteriormente fue necesario un extenso estudio de los siguientes temas:

- ✓ Caracterización del canal radio.
- ✓ Estudio y análisis del sistema *CDMA*.
- ✓ Teoría de cuerpos finitos o álgebra de *Galois*.
- ✓ Técnicas de corrección de error.
- ✓ Codificación de canal.

En este trabajo de investigación se estudió y analizó la codificación de canal (códigos bloque) enfocada al servicio de datos, la cual nos llevo a proponer los parámetros óptimos (*n, k, t*) del código bloque para el canal *RACH* ideal y el canal *TCH* ideal, el cual podría llegar a ser usado por los sistemas *CDMA*. A partir de todo el estudio y análisis realizado anteriormente se puede concluir lo siguiente:

- 🕮 Se ha demostrado y simulado que *DS-CDMA* es capáz de transmitir múltiples servicios sin aumentar el ancho de banda del sistema, ésto es posible gracias a la concatenación de códigos pseudo aleatorios que no permiten la interferencia entre los diferentes servicios de un mismo usuario y diferentes usuarios, lo cual es muy importante ya que los sistemas *CDMA* están fuertemente limitados por las

interferencias, por lo que se busca a toda costa reducir estas interferencias para aumentar la capacidad del sistema. Por tal motivo las secuencias pseudo aleatorias son un tema importante de investigación, tanto que ha merecido en este centro de investigación se haya desarrollado un trabajo de tesis en donde se utilizaron secuencias caóticas para ensanchar los datos de un sistema *CDMA*.

- Como se mencionó anteriormente, la codificación de canal es uno de los pilares principales de los sistemas de comunicación actuales, ya que con ésta se pueden contrarestar los errores introducidos por el canal radio, de aquí que en la actualidad se continúe con la búsqueda de nuevos códigos correctores de error que permitan que el sistema sea más eficiente bajo un canal no estacionario y fuertemente hostil.

- En los resultados de las simulaciones que se realizaron, se apreció como al aumentar la longitud del tamaño del paquete para el canal *RACH* se tiene un mayor aumento del *Throughput* pero con una caída más rápida del mismo. También se encontró como no siempre la mayor capacidad de corrección del código nos lleva a una mejor eficiencia del sistema, ya que si aumentamos demasiado la capacidad correctiva del código se puede llegar a tener un decremento en la ganancia de codificación y una disminución del *Throughput,* trayendo como consecuencia un decremento en la capacidad del sistema y codificador-decodificador más complejo.

- En este trabajo de tesis se encontró que los códigos *BCH* presentan un *Throughput* más elevado que los códigos *RS* pero estos presentan la caída del *Throughput* más prematura entre 10^{-4} y 10^{-2}, dando como resultado que los códigos *RS* suavicen la caída del *Throughput* pero con un valor más bajo del *Throughput.*

VII.2 Aportaciones.

Tomando en consideración que este trabajo de tesis junto con el de Nataniel Mendoza Urías, son las primeras investigaciones a nivel de maestría realizadas en *CICESE*, que se estudia y analiza la codificación de canal en un entorno de desvanecimiento tipo *Rayleigh*, por lo que las aportaciones en esta área son las siguientes:

- Estudio y Análisis de resultados de simulaciones de la concatenación de códigos que son utilizados en los sistemas *DS-CDMA* de tercera generación.

- Desarrollo de circuitos generadores de secuencias pseudo aleatorias, los cuales fueron aprovechados en los cursos de comunicaciones digitales.

- Elaboración de un informe técnico el cual puede servir como consulta teórica, de toda la matemática que está involucrada en la codificación de canal y más específicamente códigos bloque.

- Definición del conjunto de parámetros *(n, k, t)* óptimos del código bloque que pueden ser usados por los sistemas *CDMA* en el canal *RACH* y el canal *TCH*.

- Comparación y análisis (bajo condiciones ideales) de los parámetros óptimos obtenidos por las simulaciones de un sistema *FEC,* con los parámetros del código *RS* utilizado por los sistemas de tercera generación (*3G*) que especifica *UMTS-2000*.

VII.3 Recomendaciones.

Como se ha venido mencionando el código corrector de error a utilizar depende de varios factores, tales como: el tipo de información a cursar por el canal, el tipo de canal, la calidad de servicio requerida, etc. Por tal motivo antes de decidir que codificador de canal utilizar en un sistema de comunicación, se deben de tener bien definidos los puntos mencionados anteriormente, para posteriormente inclinarnos por un código corrector de error especifico.

Una vez que se tiene bien definido el tipo de código corrector de error a utilizar, es recomendado definir los parámetros que regirán las prestaciones del sistema y realizar un análisis de prestaciones del código corrector de error a utilizar, ya que como se vió en este trabajo de tesis no siempre la máxima capacidad de corrección de error nos lleva a los parámetros óptimos del código corrector de error que maximice la eficiencia del sistema.

VII.4 Trabajos futuros.

Como se mencionó anteriormente, este trabajo de tesis junto con el trabajo de Mendoza son las primeras investigaciones en el área, las cuales están involucradas con la codificación de canal, por lo que el trabajo futuro es bastante amplio. Las tareas a seguir pueden ser las siguientes:

- La continuación de este trabajo inmediato sería, buscar entre las técnicas de entrelazado existentes la que decremente lo más que se pueda la relación E_b / N_0, ya que con este decremento se alcanzará reducir más las interferencias del sistema y por lo tanto se tendrá un aumento en la capacidad del sistema.

- La unión de este trabajo (códigos bloque) con el de Mendoza (códigos convolucionales), para formar un sistema *ARQ híbrido tipo II* que pueda ser utilizado por los sistemas de tercera generación, en la cual ya se incluya la etapa de

entrelazado y desentrelazado (interno y externo) del sistema de codificación de canal.

- Un trabajo de investigación donde se analice las prestaciones del sistema *ARQ híbrido tipo II* con las prestaciones de los turbo códigos (estado del arte de codificación de canal), para llegar a recomendar uno de los dos para los diferentes servicios que brindan los sistemas de tercera generación.

Literatura citada.

Anderson John B. "Digital transmission engineering", Prentice-Hall, USA, 1999, 369 pp.

Covarrubias, David y Díaz, Pilar. "Algebra, Teoría de Cuerpos Finitos", publicaciones académicas, CICESE, 1999.

Covarrubias, David. "Control de errores en codificación de canal", publicaciones académicas, CICESE, 1999.

Covarrubias, David. "Técnicas de asignación dinámica y estabilización de MAC aplicables a sistemas móviles de tercera generación", Tesis de doctorado, UPC, 1999.

Dixon Robert C. "Spread Spectrum System", Tercera edición, Wiley-Interscience, 1994, 573 pp.

Durazo Acevedo Salvador. "Análisis de la técnica de espectro extendido (CDMA) en aplicaciones de comunicaciones satelitales con tráfico variable", CICESE, División de Física Aplicada.

Feher Kamiro, "Advanced digital communications systems and signal processing techniques", Prentice-Hall, USA, 1987, 726 pp.

Garg Vijay K. Wlkes Joseph E. "Wireless and personal communications systems", Prentice-Hall, USA, 1996, 445 pp.

Gibson, Jerry D. "The Mobile Communications Handbook", Segunda edición, CRC Prs., USA, 1996, 577 pp.

IEEE, "Communications magazine wideband CDMA", September 1998, Vol. 36 Número 9, 48-54 pp.

Lee William, "Mobile cellular telecommunications: analog and digital systems", segunda edición, McGraw-Hill, USA, 1995, 664 pp.

Lin Shu and Costello Daniel J. Jr., "Error Control Codig: Fundamentals and Applications ", Prentice-Hall, USA, 1983, 605 pp.

McTiffin M. J.. et al. 1994 "Mobile Access to an ATM Network Using a CDMA Air Interface" IEEE JSAC, Vol 12, N_o 5, 900-908 pp.

Michelson, Arnold M. and Levesque, Allen H. "Error-Control techniques for digital communication", Wiley-interscience publication, USA, 1985, 463 pp.

Parsons David, "The Mobile Radio Propagation Channel", Pentech Press Limited, Great Britain, 1992, 316 pp.

Peebles, Peyton Jr. "Digital Communications Systems", Prentice Hall, USA, 1987, 432 pp.

Pretzel, Oliver. 1992, "Error Correcting Codes and Finite Fields", Oxford University Press, 398 pp.

Proakis, G. John 1989, "Digital Communications", McGraw-Hill, Segunda edición, 905 pp.

Proakis, G. John and Salehi Masoud, "Contemporary Communications Systems Using MATLAB", Books/Cole, 2000, 428 pp.

Rappaport Theodore S. " Wireless Communicatios: Principles and Practice", Prentice-Hall, 641 pp, 1996.

Schneiderman, Ron. Future Talk, the changing wireless game, Segunda edición, IEEE Press, USA, 1997, 259 pp.

Steele Raymond. "Mobile Radio Communications",
Pentech Press Publishers Limited, Londres, 1992, 779 pp.

Sklar, Bernard. "Digital communications: Fundamentals and applications", Prentice-Hall, USA, 1988, 776 pp.

Viterbi, Andrew J. "Principles of Spread Spectrum Communication", Addison-Wesley, 1998, 245 pp.

Wicker Stephen and Bhargava, Vijay. "Reed-Solomon Codes and their Applications", IEEE Press, USA, 1994, 321 pp.

Wicker Stephen B. "Error Control Systems for digital communication and storage", Prentice-Hall, USA, 1995, 512 pp.

Wiggert, Djimitri. "Codes for Error Control and Synchronization,", Artech House, USA, 1988, 203 pp.

http://www.itr.unisa.edu.au/~alex/ECC/

http://web.syr.edu/~rrosenqu/ecc/main.htm

Glosario de términos.

AMPS	Advanced Mobile Phone System
ARQ	Automatic Repeat reQuest
ATM	Asynchronous Transfer Mode
AWGN	Additive white gaussian noise
BCH	Bose-Chaudhuri-Hocquenhem
BER	Bit Error Rate
BPSK	Binary phase shift keying
BSC	Binary symmetric channel
CDMA	Code Division Multiple Access
DLL	Delay locked loop
ETACS	European Total Access Cellular System
ETSI	European Telecommunications Standards Institute
FDMA	Frequency Division Multiple Access
FEC	Forward Error Correction
GSM	Global System for Mobile
IEEE	Institute of Electrical and Electronic Engineers
IMT-2000	International Mobile Telecommunications 2000
ISI	Intersymbol interference
IS-95	Interim Standard 95
ITU	International Telecommunications Union
NTT	Nippon Telephone and Telegraph company
PCS	Personal communications system
QoS	Quality of Service
QPSK	Quaternary Phase Shift Keying
RACH	Random access channel
RF	Radio Frequency
RS	Reed Solomon
S	Throughput
SNR	Signal to noise ratio
S-ALOHA	Slotted ALOHA
TCH	Traffic channel
TDL	Tau dither loop
TDMA	Time Division Multiple Access
TIA	Telecommunications industry association
USDC	United State Digital Cellular
UMTS	Universal Mobile Telecommunications Systems