1. INTRODUCCIÓN

1.1 Historia

La historia de los códigos correctores empieza en 1948 con la publicación del artículo de Shannon:"A Mathematical Theory of Communication", en el que describe el esquema general de un sistema de comunicaciones formado por una fuente, un transmisor, un canal de comunicaciones, un receptor y un destino de la información. Estas ideas son ampliadas en 1963 en un libro junto a Warren Weaver (The Mathematical Theory of Communication).

Aunque podemos considerar a este acontecimiento como el nacimiento de los códigos correctores, merece la pena destacar grandes hitos en la historia de los códigos correctores. A continuación presentamos algunos de ellos.

En los años 40, Hamming trabajaba en la computadora del modelo V de los laboratorios BEll. Esta computadora se alimentaba con tarjetas perforadas y con frecuencia se producían errores que eran indicados con luces de destellos para que los operadores pudieran corregirlos. Hamming se sentía frustrado cada vez que tenia que recomenzar sus programas por un fallo en la lectura de la tarjeta por la pobre fiabilidad del lector por lo que decidió ponerle remedio. Dedicó los siguientes años al estudio de la corrección de errores desarrollando numerosos algoritmos cada vez más eficaces. Finalmente, en 1950, creó los Códigos Hamming, que permitían la detección y corrección de errores de un bit (para detectar errores dobles aunque sin corregirlos se emplean los códigos Hamming Extendidos).

Antes de la aparición de los códigos Hamming se usaban otros sistemas como pueden ser los bits de paridad o los sistemas de repetición. Ademas de los códifos, Hamming introdujo también una nomenclatura para designarlos. P.e.: Un código (8,7) es aquel con palabras de 8 bits de las cuales 7 son información y 1 bit corresponde a redundancia.

En 1954 Reed y Muller presentan los códigos Reed-Muller y sus decodificadores, basados en lógica mayoritaria.

En 1955 Elias introdujo los códigos convolucionales, en los que cada símbolo de m bits se convierte en otro de n bits una vez codificado donde m/n es la tasa del código, con $(n \geq m)$, y la transformación es función de los k símbolos anteriores, siendo k la longitud

de código.

En 1957 Prange introduce los códigos cíclicos y en 1960 R.C. Bose y D.K. Chaudhuri propusieron una clase de correctores de errores múltiples (descubiertos de forma independiente por A. Hocqenghem en 1959) conocidos como códigos BCH. También en este año Reed y Solomon presentaron un esquema de codificación que usaba todo el potencial de los códigos de bloque, los códigos Reed-Solomon.

Los inicios de los 60 están marcados por los resultados de Berlekamp sobre algoritmos de decodificación algebraica de los códigos BCH.

En 1966 Forney discutió la posibilidad de usar códigos concatenados para incrementar la eficiencia evitando el aumento de complejidad de los componentes y en 1971 Viterbi introduce el algoritmo para la decodificación de máxima probabilidad de los códigos convolucionales.

Todas estas investigaciones sobre los códigos correctores superaban las posibilidades técnicas de la época y no fue posible una aplicación práctica inmediata. El desarrollo de los dispositivos para la corrección de errores no se dio hasta mediados de los 70.

En 1974, Blokh, Zyablov y Zinovév introdujeron una clase de códigos concatenados capaces de corregir tanto errores aleatorios como ráfagas.

La introducción por Goppa en los años 70 de una nueva construcción de códigos lineales a partir de curvas algebraicas lisas (códigos álgebro-geométricos) cambió por completo el panorama de investigación en el terreno de la teoría de códigos correctores. La codificación parecía sencilla y los parámetros eran fácilmente controlables a partir de fórmulas clásicas de la geometría algebraica pero no pudieron encontrarse algoritmos eficientes para su decodificación hasta finales de los 80 gracias a los trabajos de Justesen et al., Skorobogatov y Vladut, y Porter. Apenas han sido implementados en la práctica debido a la profundidad matemática de sus ideas subyacentes. Por otra parte, aunque los parámetros de estos códigos son mucho mejores que los de los códigos clásicos en un sentido asintótico (para códigos de longitud arbitrariamente grande), las aplicaciones técnicas no se han visto en la necesidad práctica de sustituir los códigos actuales por otros de mayor longitud sin que se dispare simultaneamente el coste y la tasa de error, además de que los códigos clásicos tienen una decodificación bastante más rápida y efectiva.

Hasta mediados de los 90 se podía considerar a los códigos concatenados como la mejor opción para la corrección de errores, pero estos fueron mejorados con la inclusión de los llamados turbo códigos. Conceptualmente, los turbocódigos, son dos códigos concatenados juntos, y nos aproximan a alcanzar las máximas tasas de transmisión derivadas de la teoría de Shannon. Fueron originados por Claude Berrou y Alain Glavieux y la primera

descripción presentando argumentos probabilísticos fue presentada en 1993. Estos códigos se emplean actualmente en canales de comunicación digital y en telefonía de tercera generación.

Recientemente David J.C. Mackay y R. M. Neal han redescubierto unos códigos inventados por Robert Gallager en 1960, los códigos LDPC (Low-Density Parity Check), y que superan notablemente a los turbo códigos presentados anteriormente. Estos códigos se están incorporando a los nuevos satélites de telecomunicaciones y se espera que se incluyan en un futuro a la telefonía móvil de cuarta generación. También se están realizando estudios sobre la aplicación de técnicas heurísticas para la corrección de errores (Recocido Simulado, los Algoritmos Genéticos...), debido a que el problema de encontrar un código óptimo es NP-Completo, y las técnicas exactas son útiles únicamente para pequeñas instancias.

Este último acontecimiento es, de hecho, el origen del presente proyecto, que se centrará en sus algoritmos de decodificación.

1.2 Códigos de Paridad en un Sistema de Comunicaciones

La codificación para la corrección de errores es el medio por el cual los errores introducidos por el canal de transmisión en los datos digitales pueden ser corregidos basándose en la información recibida. La codificación para la corrección de errores y la codificación para la detección de errores son denominadas en conjunto codificación para el control de errores.

Podemos encontrar ejemplos de codificación para el control de errorres no solo en todos los sistemas de comunicación modernos sino incluso en ámbitos cotidianos: DVDs, HDD, llamadas telefónicas digitales, paquetes de datos a través de internet, ISBN de los libros, cuentas bancarias...

Sin embargo, a pesar de que influyen en la vida diaria de todo el mundo, para apreciar las contribuciones de la codificación y comprender sus limitaciones se requieren ciertos conocimientos de la teoría de la información y cómo sus teoremas más importantes limitan las posibilidades de un sistema de comunicaciones.

De hecho, la teoría de la información es realmente relevante para la teoría de la codificación, ya que con recientes avances en la teoría de la comunicación ahora es posible conseguir los límites de la teoría de la codificación. Parte de este éxito se debe a que nos ha permitido situar el problema de la codificación en su contexto de la comunicación, uniendo más cercanamente el problema de la codificación con el problema de la detección, en lugar

de tratarlos de forma independientemente.

En la figura 1.1 podemos ver un esquema general de un sistema de comunicaciones. En este enlace, los datos digitales de la fuente son codificados y modulados para establecer la comunicación sobre el canal. En el otro extremo, los datos son demodulados, decodificados, y enviados al destino. Estos elementos tienen descripciones matemáticas y teoremas de la teoría de la información que gobiernan su comportamiento, dos de los más importantes están señalados en el esquema:

- **La fuente** representa los datos a ser comunicados. Las fuentes se modelan como flujos de números gobernados por alguna función de distribución de probabilidad. Cada fuente tiene una medida de la información que representa, que puede ser cuantificada en términos de la entropía.

- **El codificador de fuente** comprime los datos eliminando la redundancia. La cantidad que una fuente de datos puede ser comprimida sin pérdida de información está gobernada teóricamente por el *teorema de codificación de fuente* que establece que una fuente de información puede ser representada sin pérdida de información de manera que la cantidad de bits requeridos es igual a la cantidad de información contenida (la entropía) en bits. Para alcanzar este límite puede ser necesario que bloques largos de datos sean codificados juntos.

- **El encriptador** esconde o altera la información para que posibles espías en la comunicación no puedan interpretar su contenido. Los códigos usados para la encriptación son generalmente diferentes de los códigos usados para la corrección de errores. Este bloque puede no encontrarse en un sistema de comunicaciones.

- **El codificador de canal** es el primer paso en el proceso de corrección o detección de errores. Añade información redundante al flujo de datos de entrada de manera que permite que los errores introducidos en el canal sean corregidos. Tratar los problemas de la compresión de los datos y la corrección de errores de forma independiente frente a un tratamiento conjunto es asintóticamente óptimo (al hacerse el tamaño de los bloques de datos mayor). Este hecho es denominado el *teorema de la separación fuente-canal*.

  Debido a la redundancia introducida debe haber más símbolos a la salida del codificador que a la entrada. Normalmente el codificador de canal funciona captando bloques de k símbolos de entrada y generando a la salida bloques de n símbolos, con

$n \geq k$. La tasa de este canal será entonces:

$$R = k/n$$

con $R < 1$

- **El modulador** convierte las secuencias de símbolos del codificador del canal en señales apropiadas para la transmisión. Muchos canales requieren que las señales se transmitan como un voltaje continuo en el tiempo o en una banda de frecuencia específica, esto lo consigue el modulador. Como se ve en la figura, la codificación de canal y la modulación puede combinarse.

- **El canal** es el medio sobre el que se transmiten las señales. Algunos canales son las líneas telefónicas, lineas de fibra óptica, canales radioeléctricos... Los canales se suelen caracterizar por modelos matemáticos que se suponen suficientemente precisos al representar los atributos del canal y que son suficientemente abstractos para ser tratables matemáticamente. Normalmente se suele trabajar con dos modelos de canales ideales, los canales binarios simétricos (BSC) y los canales de ruido gaussiano blanco (AWGN). Los canales tienen distintas capacidades de transmisión de la información, como la capacidad C, que representa la cantidad de información que puede ser transmitida de forma fiable. El teorema que gobierna la capacidad es el *teorema de codificación de canal* de Shannon que establece: *Para una tasa de transmisión R, menor que la capacidad C, existe un código tal que la probabilidad de error puede hacerse arbitrariamente pequeña.*

- **El demodulador/ecualizador** recibe la señal del canal y la convierte en una secuencia de símbolos realizando las estimaciones oportunas.

- **El decodificador de canal** se aprovecha de la redundancia introducida por el codificador de canal. Al igual que en el modulador, la demodulación y decodificación de canal pueden combinarse.

- **El desencriptador** elimina la encriptación.

- **El decodificador de fuente** descomprime los datos.

- **El destino** es el receptor final de la información.

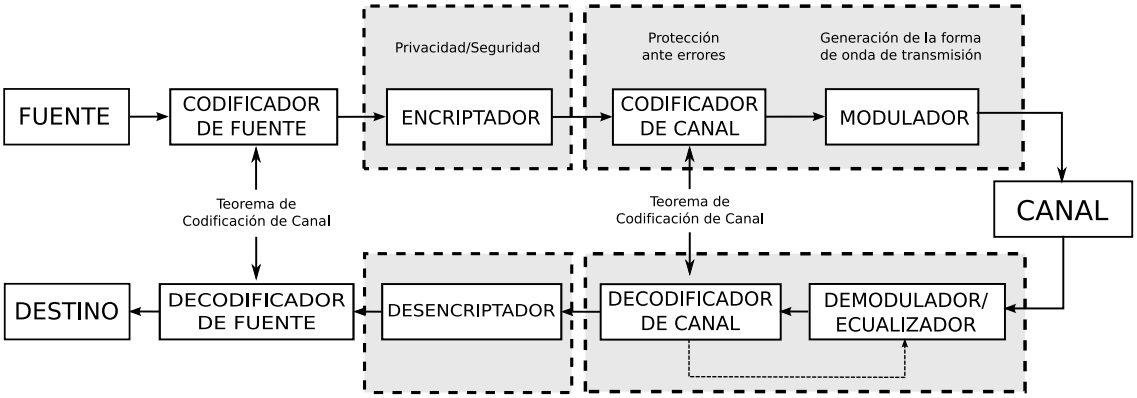

Figura 1.1: Diagrama de bloques de un sistema de comunicaciones

1.3 Por qué Códigos de Paridad

En este apartado vamos a estudiar mediante un ejemplo las ventajas que nos aporta el uso de codificación de canal al transmitir información por un canal ruidoso.

En primer lugar debemos tener en cuenta ciertas consideraciones. En la codificación de canal, k bits de entrada generan n bits a la salida con $n > k$, denotando $R = k/n$ como la tasa del código. Entonces la energía de bit de los bits sin codificar, E_b, se repartirá entre el nuevo número de bits, con lo que será menor, E_c.

Entonces:

$$E_c = RE_b$$

denota la energía de bit codificado. Si nos fijamos en el esquema de modulación BPSK de la figura 1.2, la probabilidad de error en el punto b se calculará como:

$$P_{b,coded} = Q\left(\sqrt{\frac{2E_c}{N_0}}\right)$$

Como $E_c < E_b$, estamos obteniendo peores resultados que con un esquema BPSK sin codificación. En la figura 1.3 podemos ver una comparación entre la BER usando codificación con dos tasas distintas y sin codificación, antes de la corrección. Podemos ver que cuanta más redundancia introducimos, mayor es la probabilidad de error de bit (antes de la corrección).

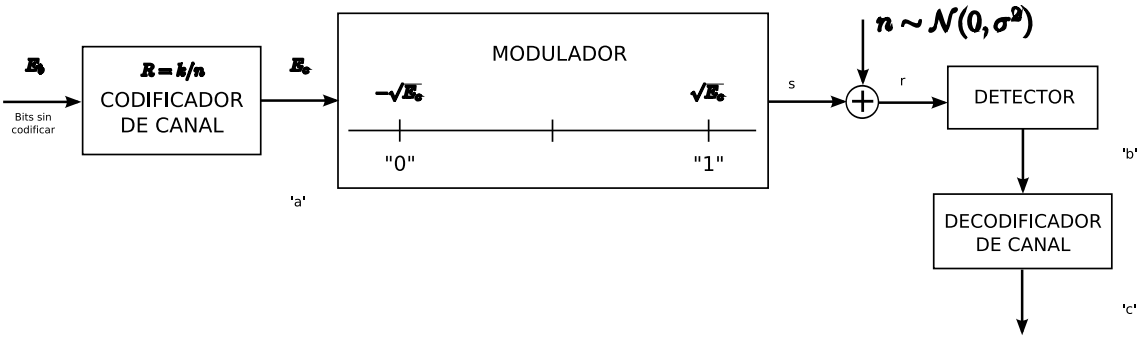

Figura 1.2: Energía de una señal codificada

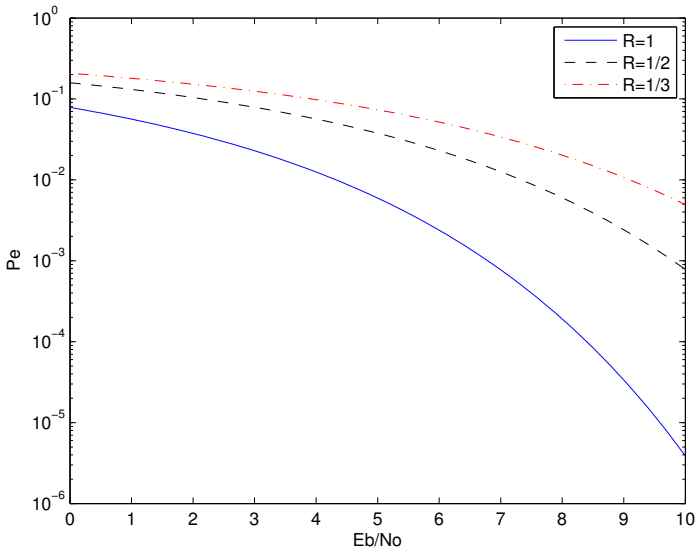

Figura 1.3: Probabilidad de error con y sin codificación

Vamos a estudiar a continuación un caso trivial, los códigos de repetición. Un código de repetición (n,1) es aquel que para un bit de entrada genera n bits iguales a él (con n impar). Por lo tanto tendrá una tasa $R = 1/n$. En forma matricial, la matriz generadora vendrá dada por:

$$G = [\ 1 \quad 1 \quad \cdots \quad 1\ ]$$

Si denotamos por m a los datos a transmitir, la palabra codificada será:

$$c = mG = [\ m \quad m \quad \cdots \quad m\ ]$$

Si consideremos la decodificación de este código cuando se transmite por un canal BSC con probabilidad cruzada $p < 1/2$, denotando la salida por

$$r = c + n$$

donde la suma se realiza en módulo 2 y n es un vector binario de longitud ñ'con unos en las posiciones en en las que ocurre el error.

Asumiendo que las palabras de código son seleccionadas con igual probabilidad, podemos usar la regla de la máxima probabilidad para decodificar. Según esta regla, se selecciona la palabra C que está más cerca del vector recibido r en distancia Hamming. Para el código de repetición, esta regla se reduce a una regla de decodificación por mayoría. Por ejemplo, para un código (7,1), si $m = 1$, entonces, la palabra de código será

$$c = [\ 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1\ ]$$

Suponiendo que el vector recibido sea el siguiente:

$$r = [\ 1 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1 \quad 1\ ]$$

Como 5 de 7 bits son 1, el valor decodificado será

$$\hat{m} = 1$$

Las palabras de un código C pueden verse como puntos en un espacio n-dimensional. En este escenario geométrico, se usa la distancia Hamming para medir las distancias entre

puntos.

La distancia mínima d_{min} de un código C es la mínima distancia Hamming entre dos palabras del código:

$$d_{min} = \min_{c_i, c_j \epsilon C, c_i \neq c_j} d_H(c_i, c_j)$$

Las dos palabras del código de repetición (n,1), claramente tienen una distancia Hamming n. El algoritmo de decodificación ML se reduce a elegir la palabra $\hat{c}$ más cercana al vector r:

$$\hat{c} = arg \min_{c \epsilon C} d_H(r, c)$$

Las capacidades detectoras y correctoras del código son:

- Capacidad correctora: $t = \lfloor (d_{min} - 1)/2 \rfloor$

- Capacidad detectora: $d_{min} - 1$

Habiendo definido el código de repetición e introducido los conceptos básicos para su estudio, estamos en posición de caracterizar la probabilidad de error en función de la probabilidad cruzada del BSC, p.

Para el código (n,1), $d_{min} = n$ y $t = (n-1)/2$. Si suponemos $n = 3$ ($t = 1$), entonces el decodificador cometerá un error si el canal causa 2 o 3 bits erróneos.

Denotando por P_e^n la probabilidad de que se produzca un error de decodificación para un código de longitud n tenemos (para un $n = 3$):

$$P_e^3 = Prob(2\ errores) + Prob(3\ errores) = 3p^2(1-p) + p^3 = 3p^2 - 2p^3$$

Si $p < \frac{1}{2}$ entonces $P_e^3 < p$, el decodificador cometerá menos errores que si no usase codificación.

En general, para un código de longitud n el error será:

$$P_e^n = \sum_{i=t+1}^{n} Prob(i\,errores) \tag{1.1}$$

$$= \sum_{i=t+1}^{n} \binom{n}{i} p^i (1-p)^{n-i} \tag{1.2}$$

$$= \binom{n}{t+1} (1-p)^n \left(\frac{p}{1-p}\right)^{t+1} + \text{términos de orden mayor} \tag{1.3}$$

Que indica que al incrementar n (y por lo tanto t) la probabilidad de error decrece, por lo tanto es posible conseguir una probabilidad de error arbitrariamente pequeña a costa de una tasa muy pequeña: $n \uparrow \Rightarrow P_e^n \downarrow \Rightarrow R \downarrow = 1/n$.

Consideremos ahora el uso de este código en un canal AWGN. Si suponemos que disponemos de 1W de potencia disponible y queremos transmitir 1bit/s, dispondremos de $E_b = 1J$ de energía por bit. Si lo codificamos con un código (n,1), tendremos que transmitir a una tasa nbit/s, repartiéndose la energía disponible por bit como $E_c = E_b/n$. La probabilidad de error para un canal AWGN será

$$p = Q(\sqrt{2E_c/N_0}) = Q(\sqrt{2E_b/nN_0})$$

Como se ve, la probabilidad de error es mayor al usar el código. Aunque se esperaría que la capacidad correctora del código haga que el error sea menor, para el código de repetición, no se consigue, como puede verse en la figura 1.4

Si en lugar de un decodificador tipo hard-decision empleamos un *soft-decision* conseguimos un mejor comportamiento. La función de verosimilitud será

$$p(\boldsymbol{r}|\boldsymbol{c}) = \prod_{i=1}^{n} p(r_i|c_i)$$

Si trabajamos en escala logarítmica y definimos la relación de verosimilitud logarítmica como:

$$\Lambda(\boldsymbol{r}) = log\frac{p(\boldsymbol{r}|m=1)}{p(\boldsymbol{r}|m=0)} = \frac{2\sqrt{E_b}}{\sigma^2} \sum_{i=1}^{n} r_i = L_c \sum_{i=1}^{n} r_i$$

El decodificador decide entonces $\hat{m} = 1$ si $\Lambda(\boldsymbol{r}) > 0$ o $\hat{m} = 0$ si $\Lambda(\boldsymbol{r}) < 0$.

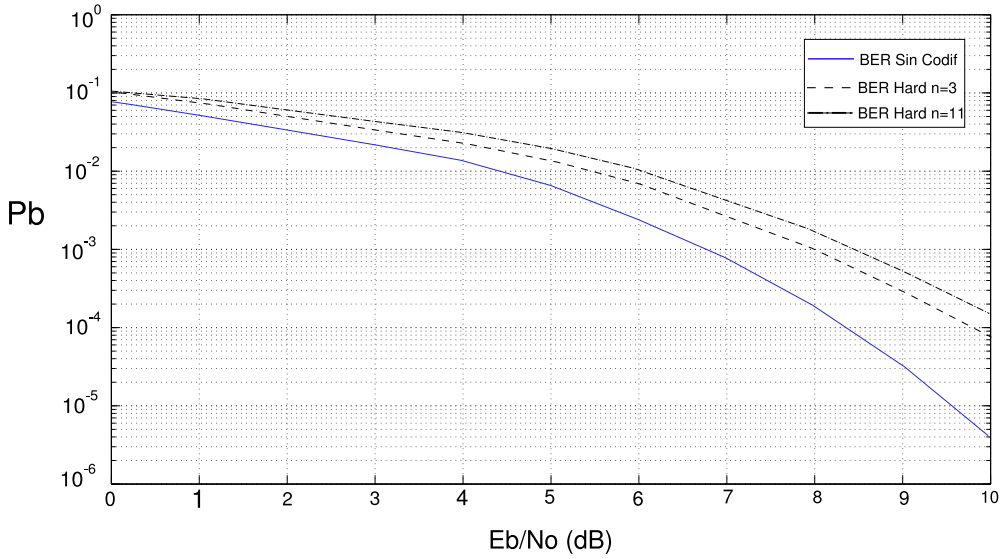

Figura 1.4: Probabilidad de error del código de repetición en un canal BSC

Como la media vale 0 y L_c es positivo:

$$\hat{m} = \begin{cases} 1 & \text{si } \sum_{i=1}^{n} r_i > 0 \\ 0 & \text{si } \sum_{i=1}^{n} r_i < 0 \end{cases}$$

Puede demostrarse que la probabilidad de error para un código de repetición (n,1) con un decodificador soft-decision es

$$P_b = Q(\sqrt{2E_b/N_0})$$

que coincide con la del código sin codificar. Sigue sin ser un código efectivo, pero resulta mejor que el decodificador *hard-decision*.

Como hemos visto, los códigos de paridad nos permiten proteger ante errores los datos transmitidos, pero no cualquier código de paridad es provechoso, ya que el hecho de introducir redundancia, disminuye la potencia disponible para los datos útiles. En la figura 1.5 podemos ver la ganancia conseguida usando un código Hamming (7,4) frente al código sin codificar.

Con esto hemos demostrado la utilidad de un buen código de corrección de errores (pero no cualquier código) en un sistema de comunicaciones ruidoso.

Como decíamos antes, en el resto de este estudio nos centraremos en los LDPC (Low-

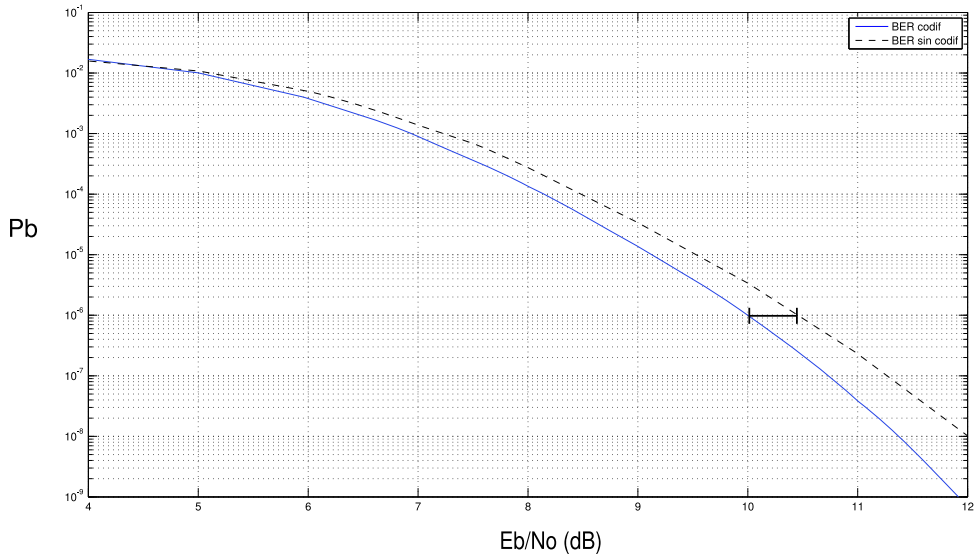

Figura 1.5: Probabilidad de error de un código Hamming en un canal AWGN

Density Parity Check), un tipo de códigos lineales de bloque que han demostrado permitir alcanzar tasas de transmisión de datos cercanas al límite teórico, el límite de Shannon.

1.4 Objetivos

Los objetivos de este proyecto son adquirir los conocimientos necesarios para entender el funcionamiento de los códigos LDPC y realizar un estudio de las principales implementaciones de los algoritmos de decodificación mediante simulaciones usando MATLAB® y establecer una comparativa entre ellas.

Los algoritmos a analizar se basan exclusivamente en simplificaciones de las ecuaciones de los nodos de chequeo de los LDPC y a la hora de su valoración se tendrán en cuenta la complejidad computacional, la facilidad de implementación y el rendimiento obtenido.

No se pretende conseguir una gran precisión cuantitativa en la comparación de las probabilidades de error obtenidas sino una comparación cualitativa, por lo que los resultados numéricos de las BER tendrán cierta incertidumbre. Nos centraremos en un campo de aplicación concreto de los LDPC, el estándar DVBS-2, en el que se emplea en conjunción con códigos BCH (figura 1.6), por lo que para la comparativa usaremos su matriz, para datagramas de una longitud igual a 64800bits con coding rates 1/4, 1/2 y 3/4.

El proyecto está estructurado de la siguiente manera:

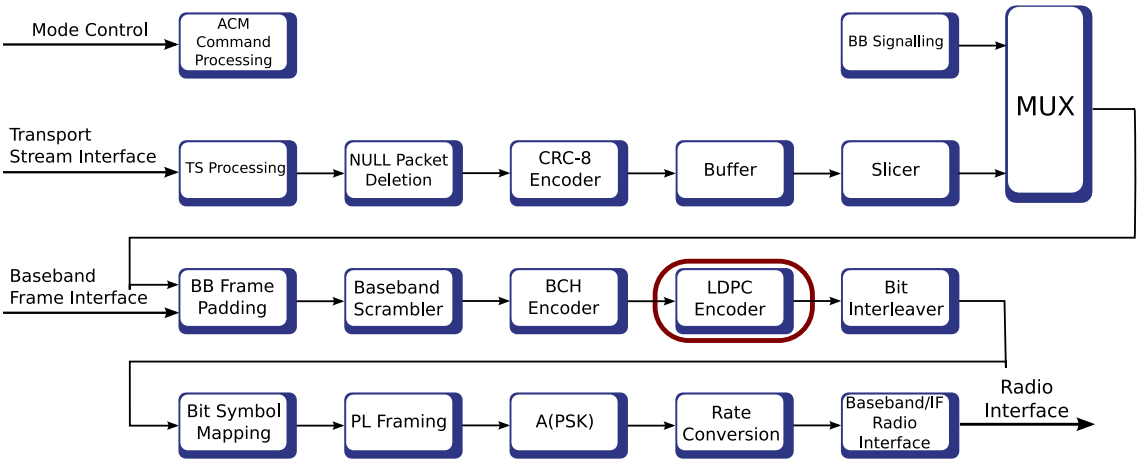

Figura 1.6: Modulador de un sistema DVB-S2

- Definición de los códigos LDPC y presentación de las ecuaciones matemáticas que los describen, así como sus algoritmos.
- Propuesta de posibles simplificaciones de los algoritmos ideales y los resultados obtenidos en las simulaciones.
- Comparativa de las simplificaciones propuestas y discusión sobre los más idóneos
- Conclusiones