Universidad del Norte

División de Ciencias Básicas

Departamento de Matemáticas

Dos funciones de probabilidad de error para distancias de decodificación acotadas

Harry Loyder Charris Polo

Trabajo presentado como requisito parcial para optar al título de Magíster en Matemáticas

Directores: Prof. Dr. Ismael Gutiérrez García
M.Sc. Jorge Robinson Evilla

Barranquilla, 8 de Octubre de 2012

Dedicatoria

A mi esposa, Heidi Navarro Archbold, quien me brindó su amor, su estímulo y su apoyo constante. Su cariño, comprensión y paciente espera para que pudiera terminar mis estudios de maestría son evidencia de su gran amor. ¡Gracias!

A mis adoradas hijas Michelle, Nicolle e Isabella quienes me prestaron el tiempo que les pertenecía para terminar y por que con la presencia de cada una siempre me motivaron e hicieron que continuara. ¡Gracias, mis mágicas princesas!

Agradecimientos

El presente trabajo de tesis primeramente me gustaría agradecerte a ti Dios por bendecirme para llegar hasta donde he llegado, porque hiciste realidad este sueño anhelado.

A la UNIVERSIDAD DEL NORTE por darme la oportunidad de estudiar y mejorar mi formación profesional.

A mis directores de tesis, Dr. Ismael Gutierrez y M.Sc. Jorge Robinson por sus esfuerzos y dedicación, quienes con sus conocimientos y sus experiencias han logrado en mí que pueda terminar mis estudios con éxito.

También me gustaría agradecer a mis profesores durante toda la maestría porque todos han aportado con un granito de arena a mi formación.

Son muchas las personas que han formado parte de mi vida profesional a las que me encantaría agradecerles su amistad, consejos, apoyo, ánimo y compañía en los momentos más difíciles de mi vida. Algunas están aquí conmigo y otras en mis recuerdos y en mi corazón, sin importar en donde estén quiero darles las gracias por formar parte de mí, por todo lo que me han brindado y por todas sus bendiciones.

Introducción

La calidad de un código de corrección de errores cuando se utiliza para transmisiones de datos depende en gran medida de la velocidad de algoritmos de codificación y decodificación y, por supuesto de la probabilidad de que hallan errores en la decodificación. En este trabajo nos interesa la última cuestión, es decir, la probabilidad de que la palabra decodificada no es la transmitida. Esta probabilidad depende de las propiedades del canal y la estrategia de decodificación.

El trabajo está dividido en cinco capítulos. En el primer capítulo estudiamos algunos preliminares necesarios para el estudio de la presente temática.

En el capitulo siguiente introducimos las definiciones referentes a las dos funciones de probabilidad P_{ue} y P_{fd} y algunos resultados que relacionan a dichas funciones entre sí.

En el tercer capítulo estudiamos el comportamiento de la probabilidad P_{ue} para dos códigos lineales, llegaremos a algunos resultados donde los polinomios enumeradores de pesos juegan un papel fundamental.

En el cuarto capítulo veremos algunas propiedades complementarias de las dos funciones de probabilidad que se estudian en el presente trabajo.

Por último el capítulo cinco es un anexo de la teoría básica de estadística y probabilidad necesarios para el estudio de los temas tratados.

Índice general

Capítulo 1

Preliminares

A continuación presentaremos algunas definiciones y teoremas necesarios para el desarrollo de la teoría sobre funciones de probabilidad de error para distancias de decodificación acotada.

1.1. Primeras definiciones

1.1.1 Definición. Sea K un alfabeto con q elementos y $n \in \mathbb{N}$. Un subconjunto no vacío C de K^n se denomina un código de bloque o simplemente un código, de longitud n sobre el alfabeto K. Los elementos de C se denominarán codewords. Si $q = 2$ o $q = 3$, entonces llamaremos a C un código binario o ternario respectivamente.
K^n es el producto cartesiano de n copias de K. Es decir,

$$K^n = \{(a_1, ..., a_n) | a_j \in K\}.$$

1.1.2 Observación. Como no se exige que K sea un cuerpo entonces no podemos afirmar que K^n es un espacio vectorial.
A partir de ahora, cada código que utilicemos en este trabajo serán lineales, esto es, subespacios vectoriales de K^n donde K es un cuerpo finito.

1.1.3 Definición. Distancia de Hamming:
Sean K un cuerpo finito, digamos $|K| = q$, $n \in \mathbb{N}$. Para $u = (u_1, ..., u_n), v = (v_1, ..., v_n) \in K^n$ definimos la distancia de Hamming entre u y v, denotada con $d(u, v)$, así:

$$d(u, v) := |\{j | u_j \neq v_j, j = 1, ...n\}|.$$

1.1.4 Teorema. Sea K un cuerpo finito. Entonces la distancia de Hamming d es una métrica sobre K^n. Es decir, para todo $u, v, w \in K^n$ se verifican

1. $d(u, v) \geqslant 0$
2. $d(u, v) = 0$ si y sólo si $u = v$
3. $d(u, v) = d(v, u)$ (Simetría)
4. $d(u, v) \leqslant d(u, w) + d(w, v)$. (Desigualdad triangular)

Además d es invariante bajo traslaciones. Es decir, para todo $u, v, w \in K^n$ se verifica que

$$d(u + w, v + w) = d(u, v)$$

Demostración. La no negatividad y la simetría son inmediatas.
Sean $u = (u_1, ..., u_n), v = (v_1, ..., v_n), w = (w_1, ..., w_n) \in K^n$. Para la desigualdad triangular, note que, si $u_j \neq v_j$, entonces $u_j \neq w_j$ o $v_j \neq w_j$. Con lo cual se sigue la afirmación.
Por otro lado,

$$\begin{aligned} d(u, v) &= |\{j | u_j \neq v_j, j = 1, ..., n\}| \\ &= |\{j | u_j + w_j \neq v_j + w_j, j = 1, ..., n\}| \\ &= d(u + w, v + w). \end{aligned}$$

1.1.5 Definición. Distancia mínima
Sea $C \leqslant K^n$ un código de longitud n, donde K es un cuerpo finito.

1. Si $|C| > 1$ entonces la distancia mínima de C con respecto a la distancia de Hamming se define de la siguiente manera:

$$d(C) := \text{mín}\{d(c, c') | c, c' \in C, c' \neq c\}$$

2. Si $|C| = 1$ entonces definimos $d(C) := 0$

Si $C \leqslant K^n$ es un código lineal de dimensión k entonces diremos que C es un $[n, k, d]$-código.

1.1.6 Definición. Sea K un cuerpo finito, $r \in \mathbb{N}_0$. Para $v \in K^n$ definimos

$$B_r(v) := \{u | u \in K^n, d(u, v) \leq r\}$$

y la llamamos esfera con centro en v y radio r.

1.1.7 Lema. Si K es un cuerpo finito con $|K| = q, u \in K^n$ y $r \in \mathbb{N}_0$, entonces

$$|B_r(u)| = \sum_{j=0}^{r} \binom{n}{j} (q-1)^j.$$

Es decir, para todo $u \in K^n$ la esfera $B_r(a)$ tiene el mismo número de elementos.

Demostración. Note que para todo $j = 0, 1, ..., r$ se verifica que

$$|\{v | v \in K^n, d(u,v) = j| = \binom{n}{j} (q-1)^j.$$

Por lo tanto

$$|B_r(u)| = \sum_{j=0}^{r} \binom{n}{j} (q-1)^j.$$

En consecuencia, el número de elementos de la esfera $B_r(u)$ es independiente del centro.

1.2. La decodificación de máxima verosimilitud.

A través de un canal de comunicación ruidoso un emisor desea transmitir un mensaje x a un receptor. Las características del canal dependen de la naturaleza del mensaje que se desea enviar, por ejemplo, datos, sonido o imágenes. Como ejemplos de canales podemos considerar una linea telefónica, la atmósfera, un CD, un DVD, una banda magnética o un enlace de comunicación satelital entre otros.
En el proceso de transmisión, accidentalmente, pueden generarse alteraciones del mensaje original, por ejemplo, el ruido atmosférico, las interferencias, cambios en la magnetización de la banda o una incisión sobre el CD. El mensaje original, cuyos caracteres pertenecen a un determinado alfabeto, es transformado por lo general en forma digital, obteniendo así una palabra de código o codeword c. Este proceso se conoce como codificación. Posteriormente el mensaje pasa por el canal y después de decodificado el receptor obtiene el mensaje y en algunos casos puede suceder que $y \neq x$.
El proceso descrito anteriormente puede ilustrarse de la siguiente manera:

$$\boxed{\text{Fuente}} \overrightarrow{x} \boxed{\text{Codificador}} \overrightarrow{c} \boxed{\text{Canal}} \overrightarrow{c'} \boxed{\text{Decodificador}} \overrightarrow{y} \boxed{\text{Receptor}}$$

La tarea principal de la teoría de códigos es codificar y decodificar un mensaje, además de proteger dicho mensaje contra posibles errores presentados en

el proceso de transmisión. Un procedimiento sencillo que podría utilizarse es agregar información al mensaje original, por ejemplo repetir n veces el mensaje enviado. A esto usualmente se le conoce con el nombre de redundancia.

Lo mínimo que debemos garantizar en el canal para aspirar a una buena transmisión es:

1. Todo símbolo $a \in K$ tiene la misma probabilidad (Ver Capitulo 5)

$$p < \frac{q-1}{q}$$

de ser recibido con error.

2. Si un símbolo es recibido con error, entonces cada uno de los $q-1$ errores posibles son igualmente probable.

1.2.1 Observaciones.

1. La condición (1) establece que la probabilidad de transmitir un símbolo sin error es $1-p > \frac{1}{q}$ (pues $p < \frac{q-1}{q}$).

2. De la condición (2) se sigue que la probabilidad de adulteración en otro símbolo dado es $\frac{p}{q-1} < \frac{1}{q}$.

3. De la condición (1) se sigue que

$$\frac{p}{(q-1)(1-p)} < 1.$$

El método de la decodificación de máxima verosimilitud (ML) suele llamarse también decodificación ML, por su nombre en ingles **Maximum Likelihood Decoding**.
Sea K un cuerpo finito con q elementos y $C \leqslant K^n$. Para $c \in C$ y $v \in K^n$ notamos con $P(v|c)$ la probabilidad condicional de que sea recibido el vector v, dado que fue enviado el codeword c. Una decodificación de máxima verosimilitud o simplemente una ML-decodificación, decodifica el vector $v \in K^n$ mediante un codeword $c \in C$, para el cual se verifica que

$$P(v|c) = \text{máx}_{c' \in C} P(v|c').$$

Es decir, mediante el codeword con mayor probabilidad de haber sido enviado. Si existe más de un codeword que alcanza dicho máximo, entonces se elige uno aleatoriamente.

1.2.2 Teorema. Sean K un cuerpo finito, $C \leqslant K^n$ un código y $c \in C$, entonces para cualquier $v \in K^n$ bajo las condiciones impuestas al canal se tiene que

$$P(v|c') = (\tfrac{p}{q-1})^j (1-p)^{n-j} \text{ con } d(v,c') = j.$$

Demostración.

Para $v = (v_1, ..., v_n) \in K^n$ y $c' = (c'_1, ..., c'_n) \in C$ las probabilidades condicionales $P(v_i|c'_i)$ de que en el vector recibido v la i-ésima posición sea v_i dado que en el codeword enviado c su i-ésima posición es c_i, son probabilidades que corresponden a eventos independientes para cada $i = 1, ..., n$, por lo tanto:

$$\begin{aligned} P(v|c) &= P((v_1, ..., v_n)|(c'_1, ..., c'_n) \\ &= P(v_1|c'_1)P(v_2|c'_2) \cdots P(v_n|c'_n) \\ &= \prod_{i=1}^{n} P(v_i|c'_i) \end{aligned}$$

Si $d(v,c') = j$, entonces j posiciones son diferentes, supongamos que i es una de esas j posiciones, se tiene que

$$P(v_i|c_i) = \frac{p}{q-1}$$

La cual es la probabilidad de adulteración en otro símbolo. Por otra parte supongamos que r es una de las $n-i$ posiciones donde $v_r = c'_r$, para cada una de ellas se tiene que

$$P(v_r|c'_r) = 1-p,$$

la cual es la probabilidad de que un símbolo llegue sin error.
De lo anterior se tiene

$$\begin{aligned} P(v|c) &= P(v_1|c'_1)P(v_2|c'_2) \cdots P(v_n|c'_n) \\ &= \underbrace{\frac{p}{q-1} \cdots \frac{p}{q-1}}_{j-veces} \underbrace{(1-p) \cdots (1-p)}_{(n-j)-veces} \end{aligned}$$

Por lo tanto:

$$P(v|c) = (\frac{p}{q-1})^j (1-p)^{n-j}.$$

1.2.3 Observación. Como la función

$$P(v|c') = (\frac{p}{(q-1)(1-p)})^j(1-p)^n$$

tiene la forma

$$f(j) = ak^j$$

con $a > 0$ y $0 < k < 1$ (ver observaciones 1.2.1). La función es decreciente. Con este análisis se observa que la decodificación de máxima verosimilitud se obtiene cuando j es mínimo. Por lo tanto con la decodificación de máxima verosimilitud se obtiene el mismo codeword que con la decodificación del vecino más próximo.

1.3. Los códigos perfectos

1.3.1 Definición. Sean C un código sobre un cuerpo finito K, con distancia mínima d y $t \in \mathbb{N}_0$.

1. C se denomina un código detector de hasta t errores o simplemente un código t-detector, si y sólo si $d \geqslant t+1$.

2. C se llama un código corrector de hasta t errores o simplemente un código t-corrector, si y sólo si $d \geqslant 2t+1$.

1.3.2 Teorema. Sea C un código sobre un cuerpo finito K, con distancia mínima d y $t \in \mathbb{N}_0$.

1. Si C es un código t-detector, entonces para todo $c \in C$ se verifica que $B_t(c)$ no contiene codewords distintos de c.

2. Si C es un código t-corrector, entonces para todo $c, c' \in C$ con $c' \neq c$ se verifica que $B_t(c) \cap B_t(c') = \emptyset$

Demostración.
Sea C un código sobre K con distancia mínima d y $t \in \mathbb{N}_0$.

1. Si $d \geqslant t+1$ y en la transmisión de $c \in C$ ocurrieron a lo más t errores, entonces para el vector recibido $v \in K^n$ se verifica que

   $$d(c,v) \leqslant t \leqslant d-1 < d.$$

   Por lo tanto $v \in B_t(c)$ y no puede ser un codeword.

2. Si $d \geqslant 2t+1$ y en el canal ocurrieron a lo más t errores durante la transmisión de $c \in C$, entonces nuevamente el vector recibido v satisface $v \in B_t(c)$. Supongamos que existe $x \in B_t(c) \cap B_t(c')$. Entonces se verifica que

$$d(x,c) \leqslant t \text{ y } d(x,c') \leqslant t.$$

Por lo tanto usando la hipótesis se tiene que

$$d(c,c') \leqslant d(c,x) + d(x,c') \leqslant 2t \leqslant d-1 < d,$$

lo cual es una contradicción. Entonces nuestro supuesto inicial es falso y se sigue que

$$B_t(c) \cap B_t(c') = \emptyset.$$

Si C es un código de longitud n sobre K y distancia mínima d, entonces las esferas centradas en codewords y con radio $\lfloor \frac{d-1}{2} \rfloor$ son disyuntas. Si todo elemento de K^n pertenece a alguna de tales esferas, entonces la ML-decodificación hace corresponder a cualquier vector recibido un único codeword. Por lo tanto la decodificación sería siempre correcta. Entonces resultaría muy conveniente para la decodificación, si el espacio K^n puede ser recubierto por esferas disyuntas con radio fijo t y centro en codewords.

1.3.3 Definición. Sea C un código de longitud n sobre un cuerpo finito K. Diremos que C es perfecto, si existe $t \in \mathbb{N}_0$ tal que

$$K^n = \bigcup_{c \in C} B_t(c)$$

es la unión disyunta de las esferas $B_t(c)$.

1.3.4 Teorema. Si C es un código perfecto sobre un cuerpo finito K con $|C| > 1$ y t como en la definición 1.3.3, entonces $d(C) = 2t+1$. Es decir, los códigos perfectos tienen distancia mínima impar.

Demostración. Dado que $|C| > 1$, se tiene que $d(C) > t$.

1. Sean $c, c' \in C$, con $c \neq c'$. Estos existen ya que $|C| > 1$. Supongamos que $d(c,c') \leqslant 2t$. Entonces

$$t < d(C) \leqslant d(c,c') \leqslant 2t.$$

Sea $y \in K^n$ el vector construido de la siguiente manera: cámbiese t posiciones del codeword c en las que difiere con c', de tal manera que las correspondientes entradas coincidan después con las de c'. Entonces $d(c', y) = t$. Dado que $d(c, c') \leqslant 2t$, de la construcción de y se sigue que $d(c', y) \leqslant t$. Entonces $y \in B_t(c) \cap B_t(c')$, lo cual es una contradicción ya que C es un código perfecto. En consecuencia $d(C) \geqslant 2t + 1$.

2. Sean $c \in C$ y $z \in K^n$ el vector construido a partir de c, cambiando $t + 1$ posiciones de este. Entonces $d(c, z) = t + 1$ y se verifica que $z \notin B_t(c)$.

   Dado que C es perfecto, se tiene que existe $c' \in C$ con $c' \neq c$ y $z \in B_t(c')$. Es decir, $d(z, c') \leqslant t$. por lo tanto

$$d(C) \leqslant d(c, c') \leqslant d(c, z) + d(z, c') \leqslant (t + 1) + t = 2t + 1.$$

   En conclusión: $d(C) = 2t + 1$.

1.3.5 Ejemplos. Sea K un cuerpo finito y $n \in \mathbb{N}$.

1. $C = K^n$. Es suficiente hacer centro en cualquier vector y tomar $t = 0$.

2. $C = \{0\}$. Se toma como radio la mayor distancia posible entre elementos de K^n.

3. Código binario de repetición de longitud $n = 2t+1$, con $t \in \mathbb{N}$. En efecto, este código cantiene solamente los codewords $u = (0, ..., 0)$ y $v = (1, ..., 1)$ y se puede cubrir el espacio K^n tomando las dos esferas con centro en u y v y radio t.

Presentamos a continuación un código perfecto no trivial.

1.3.6 Ejemplo. Sea $K = \mathbb{F}_2$ y definamos

$$C := \left\{(c_1, ..., c_7) | c_j \in K, \begin{array}{r} c_1 + c_4 + c_6 + c_7 = 0 \\ c_2 + c_4 + c_5 + c_7 = 0 \\ c_3 + c_5 + c_6 + c_7 = 0 \end{array}\right\}.$$

Entonces

$$\begin{aligned} c_1 &= c_4 + c_6 + c_7 \\ c_2 &= c_4 + c_5 + c_7 \\ c_3 &= c_5 + c_6 + c_7 \end{aligned}$$

y se tiene que

$$C = \{(c_4 + c_6 + c_7, c_4 + c_5 + c_7, c_5 + c_6 + c_7, c_4, c_5, c_6, c_7) | c_j \in \mathbb{F}_2\}.$$

Si definimos

$$\begin{aligned} v_4 &= (1,1,0,1,0,0,0) \\ v_5 &= (0,1,1,0,1,0,0) \\ v_6 &= (1,0,1,0,0,1,0) \\ v_7 &= (1,1,1,0,0,0,1), \end{aligned}$$

entonces

$$C = \{c_4 v_4 + c_5 v_5 + c_6 v_6 + c_7 v_7 | c_j \in \mathbb{F}_2\}.$$

Se verifica que C es un espacio vectorial sobre K y que $B = (v_1, v_2, v_3, v_4)$ es una base para C. Por lo tanto $\dim_k C = 4$ y así $|C| = 2^4$.
Listamos a continuación todos los elementos de C.

0000000	0001101	1111111	1110010
1101000	1000110	0010111	0111001
0110100	0100011	1001011	1011100
0011010	1010001	1100101	0101110

Dado que C es un grupo abeliano, de la invariancia bajo traslaciones de la distancia de Hamming se sigue que

$$d(C) = \text{mín}\{d(c,0) | 0 \neq c \in C\}.$$

Todo codeword no nulo que sea solución del sistema de ecuaciones lineales debe tener por lo menos tres entradas iguales a uno.
dado que $0001110 \in C$, se verifica que $d(C) = 3$. Entonces C es un $[7,4,3]$-código binario, además perfecto. En efecto,

$$\frac{2^7}{\sum_{j=0}^{1} \binom{7}{j}} = \frac{2^7}{1+7} = \frac{2^7}{2^3} = 2^4 = |C|.$$

Este código pertenece a la familia de los denominados códigos de Hamming ($\text{Ham}_q(k)$), los cuales están definidos sobre un cuerpo K, con $|K| = q$ y tienen parámetros

$$[\frac{q^k - 1}{q-1}, n-k, 3].$$

Además de los códigos de Hamming existen otros dos códigos perfectos, el G_{23} y el G_{11}, descubiertos en 1949 por M.J.E.Golay. estos son denominados el $[23,12,7]$-código binario de Golay y el $[11,6,5]$-código ternario de Golay respectivamente.

1.4. El código dual

Similar como en los espacios vectoriales euclidianos se describe el código dual con base en una forma bilineal no degenerada, la cual se construye exactamente igual al producto escalar euclidiano. Para ello, sean K un cuerpo finito, $n \in \mathbb{N}$ y definimos

$$(\cdot \mid \cdot) : K^n \times K^n \longrightarrow K$$

mediante

$$(u \mid v) := \sum_{j=1}^{n} u_j v_j,$$

donde $u = (u_1, ..., u_n)$ y $v = (v_1, ...v_n)$.
Por ejemplo, si $u = (1, 0, 1, 1, 0)$, $v = (0, 1, 0, 1, 1) \in \mathbb{F}_2^5$, entonces $(u \mid v) = 1$. Contrario a lo que sucede en los espacios vectoriales euclidianos, es posible que un vector no nulo v sea ortogonal a si mismo. Por ejemplo, sea $v = (1, 1, 0, 1, 1) \in \mathbb{F}_2^5$. Note que $(v \mid v) = 0$.

1.4.1 Lema. Sean $u, v, w \in K^n$ y $a, b \in K$. Entonces

1. $(u + v \mid w) = (u \mid w) + (v \mid w)$
2. $(au \mid v) = a(u \mid v)$
3. $(u \mid v) = (v \mid u)$.
   Es decir, $(\cdot \mid \cdot)$ es una **forma bilineal simétrica.**
4. $(0 \mid v) = (v \mid 0) = 0$
5. Si $(u \mid v) = 0$, para todo $v \in k^n$, entonces $u = 0$.
   Es decir, $(\cdot \mid \cdot)$ es una forma bilineal simétrica **no degenerada**.

Demostración. Las demostraciones de las afirmaciones 1-4 son inmediatas. Para demostrar 5, sea e_j el j-ésimo vector de la base canónica de K^n. Entonces

$$0 = (u \mid e_j) = u_j.$$

Por lo tanto $u = 0$.

1.4.2 Definición. Sea C un $[n, k, d]$-código sobre un cuerpo finito K.

1. El **código dual** de C, notado con $C^{\perp}$, se define de la siguiente manera:

$$C^{\perp} := \{u \in K^n \mid (u \mid c) = 0, \forall c \in C\}.$$

2. C se denomina **auto-ortogonal**, si $C \subseteq C^{\perp}$.

3. C se denomina **auto-dual**, si $C = C^{\perp}$.

Puede verificarse sin dificultades que $C^{\perp}$ es siempre un subespacio vectorial de K^n aun cuando C sea simplemente un subconjunto de K^n. En particular, un código auto-dual es siempre lineal.

1.4.3 Ejemplos.

1. Sea C un $[4, 2, 2]$-código binario dado por

$$C = \{(0,0,0,0), (1,1,0,0), (0,0,1,1), (1,1,1,1)\}.$$

   Entonces $C^{\perp} = C$. Es decir, C es auto-dual.

2. Sea C un $[3, 2, 2]$-código binario dado por

$$C = \{(0,0,0), (1,1,0), (0,1,1), (1,0,1)\}.$$

   Entonces

$$C^{\perp} = \{(0,0,0), (1,1,1)\}.$$

1.5. Matriz generadora y polinomios enumeradores de peso de un código lineal

1.5.1 Definición. sea C un $[n, k, d]$-código sobre un cuerpo finito K y sean $g_1 = (g_{11}, ..., g_{1n}), ..., g_k = (g_{k1}, ...g_{kn}) \in K^n$. Si $B = (g_1, ..., g_n)$ es una base para C, entonces diremos que

$$G = \begin{pmatrix} g_1 \\ . \\ . \\ . \\ g_k \end{pmatrix} = \begin{pmatrix} g_{11} & . & . & . & g_{1n} \\ . & & & & . \\ . & & & & . \\ . & & & & . \\ g_{k1} & . & . & . & g_{kn} \end{pmatrix} \in Mat(k \times n, K)$$

es una matriz generadora de C.

1.5.2 Teorema. Sea C un $[n, k, d]$-código sobre un cuerpo finito K. Entonces $G \in Mat(k \times n, K)$ es una matriz generadora de C, si y sólo si

$$C = \{uG \mid u \in K^k\}.$$

Demostración. Supongamos que

$$G = \begin{pmatrix} g_1 \\ . \\ . \\ . \\ g_k \end{pmatrix} = \begin{pmatrix} g_{11} & . & . & . & g_{1n} \\ . & & & & . \\ . & & & & . \\ . & & & & . \\ g_{k1} & . & . & . & g_{kn} \end{pmatrix} \in Mat(k \times n, K)$$

es una matriz generadora de C. Si $(u_1, ..., u_k) \in K^k$, entonces

$$\begin{aligned} uG &= (u_1 g_{11} + \cdots + u_k g_{k1}, \cdots, u_1 g_{1n} + \cdots + u_k g_{kn}) \\ &= u_1 g_1 + \cdots u_k g_k \in C. \end{aligned}$$

esto demuestra que $\{uG | u \in K^k\} \subseteq C$. $C \subseteq \{uG | u \in K^k\}$ es inmediata por que las filas de G forman una base para C.

Recíprocamente, supongamos que $C = \{uG | u \in K^k\}$ y notemos con e_j, $j = 1, ..., k$ los vectores de la base canónica de K^k. Entonces

$$\begin{aligned} e_1 G &= g_1 \\ &\vdots \\ e_k G &= g_k. \end{aligned}$$

Se tiene que las filas de G pertenecen a C. Por lo tanto

$$C = \{u_1 g_1 + \cdots u_k g_k | u_j \in K\} = \langle g_1, ..., g_k \rangle.$$

Dado que $\dim_K C = k$, se sigue que $B = (g_1, ..., g_k)$ es una base para C y se tiene que G es una matriz generadora para C.

1.5.3 Definición. Sea C un $[n, k, d]$-código sobre un cuerpo finito K, con $k < n$. Diremos que $H \in Mat(n - k \times n, k)$ es una **matriz de control** para C, si

$$C = \{u \in K^n \mid Hu^t = 0\}.$$

1.5.4 Observación. Se puede demostrar que H es una matriz de control de C si y solo si H es una matriz generadora de $C^\perp$.

1.5.5 Ejemplo. En el ejemplo 1.3.6 vimos el $[7, 4, 3]$-código binario de Hamming, una matriz generadora para este código es

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Entonces una matriz generadora para el correspondiente código dual es

$$G' = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Listamos a continuación los codewords del código dual.

0000000	1001011
0101101	0010111
1100110	1011100
0111010	1110001

En general, el código dual del código de Hamming se denomina **código simplex**. Lo denotaremos con $\mathrm{Sim}_q(k)$.

1.5.6 Lema. Sea K un cuerpo finito, con $\mid K \mid = q$.

1. Si $0 \neq c \in \mathrm{Sim}_q(k)$, entonces $d(c, 0) = q^{k-1}$.
2. $\mathrm{Sim}_q(k)$ es un $\left[\frac{q^k-1}{q-1}, k, q^{k-1}\right]$-código sobre K.

Demostración. Sea H una matriz de control de $\mathrm{Ham}_q(k)$, con filas $f_1, ..., f_k$. Sea además $0 \neq c = (c_1, ..., c_n) \in \mathrm{Sim}_q(k)$. Dado que H es una matriz generadora de $\mathrm{Sim}_q(k)$ se tiene que $B = (f_1, ...f_k)$ es una base para $\mathrm{Sim}_q(k)$. Por lo tanto

$$c = \sum_{j=1}^{k} a_j f_j = \sum_{j=1}^{k} a_j (f_{j1}, ..., f_{jn}), a_j \in K.$$

Sea $h_i := (f_{1i}, ..., f_{ki})^t$ la i-ésima columna de H y sea $a := (a_1, ..., a_k) \in K^k$. Definamos el conjunto $U(a)$ de la siguiente manera:

$$U(a) := \{(b_1, ..., b_k)^t \mid b_j \in K, \sum_{j=1}^{k} a_j b_j = 0\} \subseteq K^k.$$

Se verifica inmediatamente que $U(a) = \langle a \rangle^{\perp}$. Por tanto

$$\dim_k U(a) = \dim_k \langle a \rangle^{\perp} = k - \dim_k \langle a \rangle^{\perp} = k - 1.$$

En consecuencia $U(a)$ tiene $\frac{q^{k-1}-1}{q-1}$ columnas h_i de H.
Note que

$$c_i = 0 \Leftrightarrow \sum_{j=1}^{k} a_j f_{ji} = 0 \Leftrightarrow (f_{1i}, ..., f_{ki})^t \in U(a).$$

Esto demuestra que en c hay exactamente $\frac{q^{k-1}-1}{q-1}$ ceros. Entonces

$$d(c,0) = n - \frac{q^{k-1}-1}{q-1} = \frac{q^k-1}{q-1} - \frac{q^{k-1}-1}{q-1} = q^{k-1}.$$

El resto de la demostración es inmediata.

1.5.7 Definición. Sean K un cuerpo finito, $n \in \mathbb{N}$ y $C \subseteq K^n$. Para $x = (x_1, ..., x_n) \in K^n$ definimos

$$\text{wt}(x) := d(x,0) = |\{j \mid x_j \neq 0\}|$$

y lo llamaremos el **peso** de x. La función $wt : K^n \longrightarrow \mathbb{N}_0$ se denomina **función peso** sobre K^n

1.5.8 Definición. Sea C un código de longitud n sobre un cuerpo finito K. Para $0 \leqslant j \leqslant n$, denotamos con A_j el número de codewords con peso j. Esto es,

$$A_j := |\{c \in C | \text{wt}(c) = j\}|.$$

Entonces, el polinomio definido por

$$\sum_{j=0}^{n} A_j x^j \in \mathbb{Z}[x]$$

se denomina **polinomio enumerador de pesos de** C y el vector $(A_0, A_1, ..., A_n)$ se denomina la distribución de pesos de C.

1.5.9 Observaciones.

1. Claramente $A_0 = 1$, dado que el código tiene un único codeword con peso cero, este es el vector nulo.

2. Por la forma como está definida la distribución de pesos para un código C de longitud n se tiene
$$\sum_{j=0}^{n} A_j = |C|.$$

1.5.10 Ejemplo. En el ejemplo 1.3.6 el polinomio enumerador de pesos de C es

$$A = 1 + 7x^3 + 7x^4 + x^7.$$

y

$$|C| = 1 + 7 + 7 + 1 = 16.$$

Capítulo 2

Las funciones P_{ue} y P_{fd}

2.1. La función P_{ue}

2.1.1 Definición. Sea $\mathbb{F}_q$ un cuerpo finito, $C \leqslant \mathbb{F}_q^n$ un $[n,k,d]$-código. Si $t \leq \frac{d-1}{2}$ y $p < \frac{q-1}{q}$ es la probabilidad de que cuando se envía un codeword c cada bit sea recibido con error. Se define $P_{ue}(C,t,p)$ como la probabilidad de que una palabra w con $d(w,c') \leqslant t$ para algún codeword $c' \in C\backslash\{c\}$ se reciba si $c \in C$ es transmitido. Es decir,

$$P_{ue}(C,t,p) = P(Y \in \bigcup_{c \neq c' \in C} B_t(c') \mid X = c)$$

donde X e Y denotan, respectivamente, las variables aleatorias para "enviar un codeword $c \in C$ y recibir un vector $w \in \mathbb{F}_q^n$".

2.1.2 Observación. Se puede notar que la probabilidad $P_{ue}(C,t,p)$ no dependerá de la palabra transmitida, así también tenemos

$$P_{ue}(C,t,p) = P(Y \in \bigcup_{0 \neq c \in C} B_t(c) \mid X = 0)$$

2.1.3 Teorema. Con las condiciones de la definición anterior tenemos:

$$P_{ue}(C,t,p) = (|C| - 1)P(Y \in B_t(0) | X \in C \setminus \{0\}).$$

Demostración.
Con la observación anterior

$$\begin{aligned} P_{ue}(C,t,p) &= P(Y \in \bigcup_{0\neq c\in C} B_t(c)|X=0) \\ &= \sum_{0\neq c\in C}\sum_{v\in B_t(c)} P(Y=v|X=0). \end{aligned}$$

Dado que

$$P(Y=v|X=0) = (\frac{p}{q-1})^{d(v,0)}(1-p)^{n-d(v,0)}$$

y d es invariante bajo traslaciones tenemos que

$$\begin{aligned} P(Y=v|X=0) &= (\frac{p}{q-1})^{d(v-c,-c)}\cdot(1-p)^{n-d(v-c,-c)} \\ &= P(Y=-c+v|X=-c). \end{aligned}$$

Con lo anterior:

$$\begin{aligned} P_{ue}(C,t,p) &= \sum_{0\neq c\in C}\sum_{v\in B_t(c)} P(Y=-c+v|X=-c) \\ &= \sum_{0\neq c\in C}\sum_{w\in B_t(0)} P(Y=w|X=-c). \end{aligned}$$

Pues $v \in B_t(c)$, si y sólo si, $w = -c+v \in B_t(0)$.

2.1.4 Teorema. Con las condiciones de la definición 2.1.1. Si A_i denota el número de codewords con peso i, entonces

$$P_{ue}(C,0,p) = (1-p)^n \sum_{i=1}^{n} A_i \left(\frac{p}{(q-1)(1-p)}\right)^i$$

Demostración.
Por el teorema 1.2.2 tenemos:

$$P(Y=c|X=0) = (\frac{p}{q-1})^i(1-p)^{n-i},$$

donde $i = d(c,0)$.

Si $C_i = \{c \in C | wt(c) = i\}$, entonces Para los A_i codewords de peso i, tenemos:

$$P(Y \in C_i|X=0) = A_i(\frac{p}{q-1})^i(1-p)^{n-i}.$$

Con lo cual:

$$\begin{aligned} P_{ue}(C,0,p) &= P(Y \in C\backslash\{0\}|X=0) \\ &= P(Y \in \bigcup_{i=1}^{n} C_i|X=0) \\ &= \sum_{i=1}^{n} A_i(\frac{p}{q-1})^i(1-p)^{n-i} \\ &= (1-p)^n \sum_{i=1}^{n} A_i \left(\frac{p}{(q-1)(1-p)}\right)^i. \end{aligned}$$

2.1.5 Observación. A la función $P_{ue}(C,0,p)$ se le denomina probabilidad de error no detectado.

2.2. La función P_{fd}

2.2.1 Definición. Sean $\mathbb{F}_q$ un cuerpo finito y $C \leqslant \mathbb{F}_q^n$ un $[n,k,d]$-código. Si $t \leq \frac{d-1}{2}$ y $p < \frac{q-1}{q}$, se define $P_{fd}(C,t,p)$ como la probabilidad de que se halla enviado $c' \in C\backslash\{c\}$ dado que se recibió w con $d(w,c) \leq t \leq \frac{d-1}{2}$. Esto es,

$$P_{fd}(C,t,p) = P(X \in C\backslash\{c\}|Y \in B_t(c)).$$

2.2.2 Observación. Por las condiciones impuestas al canal (equiprobabilidad) tenemos

$$P_{fd}(C,t,p) = P(X \in C\backslash\{0\}|Y \in B_t(0))$$

2.2.3 Teorema. Sean $\mathbb{F}_q$ es un cuerpo finito y $C \leqslant \mathbb{F}_q^n$ un $[n,k,d]$-código. Si $t \leq \frac{d-1}{2}$ y $p < \frac{q-1}{q}$, entonces

$$P(Y \in B_t(0))\cdot P_{fd}(C,t,p) = \frac{1}{|C|}P_{ue}(C,t,p).$$

Demostración.

$$\begin{aligned} P(Y \in B_t(0))\cdot P_{fd}(C,t,p) &= P(X \in C\backslash\{0\}, Y \in B_t(0)) \\ &= \sum_{0\neq c\in C} \sum_{w\in B_t(0)} P(X=c, Y=w) \\ &= \sum_{0\neq c\in C} \sum_{w\in B_t(0)} P(Y=w|X=c)\cdot P(X=c) \\ &= \frac{1}{|C|}P_{ue}(C,t,p). \end{aligned}$$

Esta última igualdad se debe a las condiciones impuestas al canal, esto es, $P(X = c) = \frac{1}{|C|}$.

2.3. Relación entre las funciones P_{fd} y P_{ue}

A continuación veremos que si C es un $[n, k, d]$-código sobre un cuerpo finito K, entonces las funciones $P_{fd}(C, t, p)$ y $P_{ue}(C, t, p)$ solo difieren en términos que no tienen que ver con el código en si, sino con los parámetro t y p

2.3.1 Teorema. Sea C un $[n, k, d]$-código sobre un cuerpo finito K y sea $t \leq \frac{d-1}{2}$ entonces:

$$P_{fd}(C,t,p) = \frac{P_{ue}(C,t,p)}{P_{ue}(C,t,p) + \sum_{i=0}^{t} \binom{n}{i} p^i (1-p)^{n-i}}$$
$$= 1 - \frac{\sum_{i=0}^{t} \binom{n}{i} p^i (1-p)^{n-i}}{P_{ue}(C,t,p) + \sum_{i=0}^{t} \binom{n}{i} p^i (1-p)^{n-i}}.$$

Demostración. De acuerdo con lo visto en el teorema 2.2.3 tenemos

$$\begin{aligned}
\frac{P_{ue}(C,t,p)}{P_{fd}(C,t,p)} &= |C| \cdot P(Y \in B_t(0)) \\
&= |C| \cdot \sum_{c \in C} P(Y \in B_t(0), X = c) \\
&= |C| \cdot \sum_{c \in C} P(Y \in B_t(0) | X = c) P(X = c) \\
&= |C| \cdot P(X = c) \sum_{c \in C} P(Y \in B_t(0) | X = c) \\
&= |C| \cdot \frac{1}{|C|} \sum_{c \in C} P(Y \in B_t(0) | X = c) \\
&= P(Y \in B_t(0) | X = 0) + \sum_{0 \neq c \in C} P(Y \in B_t(0) | X = c) \\
&= \sum_{i=0}^{t} \binom{n}{i} p^i (1-p)^{n-i} + P_{ue}(C,t,p).
\end{aligned}$$

Dado que $P(Y \in B_t(0)|X = 0) = \sum_{i=0}^{t} \binom{n}{i} p^i (1-p)^{n-i}$.

Entonces

$$P_{fd}(C,t,p) = \frac{P_{ue}(C,t,p)}{P_{ue}(C,t,p) + \sum_{i=0}^{t} \binom{n}{i} p^i (1-p)^{n-i}}.$$

Observe que:

$$|C| \cdot P(Y \in B_t(0)) = \sum_{c \in C} P(Y \in B_t(c))$$

(Ver condiciones impuestas al canal en la sección 1.2)
es la probabilidad de decodificar hasta t errores. Como consecuencia de ello tenemos.

2.3.2 Corolario Sea C un $[n,k,d]$-Código y $t \leq \frac{d-1}{2}$. Entonces:

1. $P_{ue}(C,t,p) \leq P_{fd}(C,t,p)$.
2. $P_{ue}(C,t,p) = P_{fd}(C,t,p)$, si y sólo si, C es perfecto y $t = \frac{d-1}{2}$.

Demostración.

1. Por el teorema 2.2.3 tenemos

$$\frac{P_{ue}(C,t,p)}{P_{fd}(C,t,p)} = |C| \cdot P(Y \in B_t(0)) = \sum_{c \in C} P(Y \in B_t(c)) \leq 1.$$

   Entonces $P_{ue}(C,t,p) \leq P_{fd}(C,t,p)$.

2. C es perfecto, si y sólo si, se detectan y corrigen todos los errores, por lo tanto

$$\sum_{c \in C} P(Y \in B_t(c)) = 1$$

   con lo cual

$$\frac{P_{ue}(C,t,p)}{P_{fd}(C,t,p)} = \sum_{c \in C} P(Y \in B_t(c)) = 1.$$

   Es decir,

$$P_{ue}(C,t,p) = P_{fd}(C,t,p).$$

2.3.3 Corolario Si C es un código de longitud n. Entonces

$$\begin{aligned} P_{fd}(C,0,p) &= 1 - \frac{(1-p)^n}{P_{ue}(C,0,p)+(1-p)^n} \\ &= 1 - \frac{(1-p)^n}{\sum_{i=0}^{n} A_i(\frac{p}{q-1})^i(1-p)^{n-i}} \\ &= 1 - \frac{1}{\sum_{i=0}^{n} A_i(\frac{p}{(q-1)(1-p)})^i}. \end{aligned}$$

Demostración.
Por el teorema 2.3.1 tenemos que

$$P_{fd}(C,t,p) = 1 - \frac{\sum_{i=0}^{t}\binom{n}{i}p^i(1-p)^{n-i}}{P_{ue}(C,t,p)+\sum_{i=0}^{t}\binom{n}{i}p^i(1-p)^{n-i}}.$$

En particular cuando $t=0$ se tiene lo siguiente:

$$P_{fd}(C,0,p) = 1 - \frac{\sum_{i=0}^{0}\binom{n}{i}p^i(1-p)^{n-i}}{P_{ue}(C,0,p)+\sum_{i=0}^{t}\binom{n}{i}p^i(1-p)^{n-i}}.$$

Dado que

$$P_{ue}(C,0,p) = \sum_{i=1}^{n} A_i(\frac{p}{q-1})^i(1-p)^{n-i},$$

se tiene la demostración del teorema.

2.3.4 Corolario Sean C y C' $[n,k,d]$ y $[n,k,d']$ Códigos respectivamente, para cualquier probabilidad de error en el símbolo $0 < p < \frac{q-1}{q}$ y cualquier $t \leq min\{\frac{d-1}{2}, \frac{d'-1}{2}\}$ las siguientes expresiones son equivalentes.

1. $P_{fd}(C,t,p) < P_{fd}(C',t,p)$.
2. $P_{ue}(C,t,p) < P_{ue}(C',t,p)$.

Demostración.
$1 \to 2$
Sea $k = \sum_{i=0}^{t}\binom{n}{i}p^i(1-p)^{n-i}$.

Por hipótesis tenemos

$$P_{fd}(C,t,p) = \frac{P_{ue}(C,t,p)}{P_{ue}(C,t,p)+k} < \frac{P_{ue}(C',t,p)}{P_{ue}(C',t,p)+k} = P_{fd}(C',t,p).$$

Con lo cual

$$P_{ue}(C,t,p)\cdot P_{ue}(C',t,p)+kP_{ue}(C,t,p) < P_{ue}(C,t,p)\cdot P_{ue}(C',t,p)+kP_{ue}(C',t,p).$$

Es decir

$$kP_{ue}(C,t,p) < kP_{ue}(C',t,p).$$

Por consiguiente

$$P_{ue}(C,t,p) < P_{ue}(C',t,p).$$

$2 \rightarrow 1$
Si $P_{ue}(C,t,p) < P_{ue}(C',t,p)$, entonces se tiene trivialmente que como la función $f(x) = \frac{x}{x+k}$ con $k > 0$ constante es creciente se tiene que

$$P_{fd}(C,t,p) = \frac{P_{ue}(C,t,p)}{P_{ue}(C,t,p)+k} < \frac{P_{ue}(C',t,p)}{P_{ue}(C',t,p)+k} = P_{fd}(C',t,p).$$

Lo cual demuestra el corolario.

Capítulo 3

La probabilidad $P_{ue}(C, t, p)$

3.1. Relación entre la función P_{ue} y el polinomio enumerador de pesos

En esta sección veremos como el conocimiento del polinomio enumerador de pesos de un código es útil para describir la función $P_{ue}(C, t, p)$ y comparar dicha función para dos códigos con una cota adecuada para p.

3.1.1 Teorema. Sea C un $[n, k, d]_q$-código, si $t \leqslant \frac{d-1}{2}$, $p < \frac{q-1}{q}$ y $A(x) = \sum_{i=0}^{n} A_i x^i$ es el polinomio enumerador de pesos de C, entonces

$$P_{ue}(C, t, p) = \sum_{i=1}^{n} A_i \sum_{j=0}^{t} \sum_{s=0}^{j} [\binom{i}{s} (\frac{p}{q-1})^{i-s} (1 - \frac{p}{q-1})^{s} \cdot \binom{n-i}{j-s} p^{j-s} (1-p)^{n-i-j+s}]$$

Demostración.
Sean $c \in C$, $i \in \{1, ..., n\}$ y $\mathrm{wt}(c) = i$. Si $v \in F_q^n$ y $r \in sop(c) \bigcap sop(v)^C$, entonces la probabilidad de que al ser enviado el vector 0 y recibir al vector v su r-ésima componente sea v_r es

$$P(v_r|0_r) = 1 - \frac{p}{q-1},$$

la cual es la probabilidad de que el símbolo v_r de la palabra v no sea adulterado en otro símbolo.

Si $k \in sop(c) \bigcap sop(v)$ entonces

$$P(v_k|0_k) = \frac{p}{q-1},$$

la cual es la probabilidad de adulteración en otro símbolo.

Si $sop(c) = \{m_1, ..., m_i\}$ y $|sop(c) \bigcap sop(v)^C| = s$ se tiene que

$$\begin{aligned} P(v_{m_1} \cdots v_{m_i}|0_1 \cdots 0_i) &= \underbrace{P(v_r|0_r) \cdots (v_r|0_r)}_{s-veces} \underbrace{P(v_k|0_k) \cdots P(v_k|0_k)}_{(i-s)-veces} \\ &= \underbrace{(1 - \frac{p}{q-1}) \cdots (1 - \frac{p}{q-1})}_{s-veces} \underbrace{(\frac{p}{q-1}) \cdots (\frac{p}{q-1})}_{(i-s)-veces} \\ &= (\frac{p}{q-1})^{i-s}(1 - \frac{p}{q-1})^s. \end{aligned}$$

Por lo tanto si $H = \{v \in F_q^n \mid |sop(c) \bigcap sop(v)^C| = s \wedge d(v, c) = j\}$ y $H_1 = \{h_{m_1}, ..., h_{m_i} \mid h \in H\}$, entonces

$$P(Y \in H_1|X = 0_{F_q^i}) = \binom{i}{s} (\frac{p}{q-1})^{i-s}(1 - \frac{p}{q-1})^s.$$

Dado que $|H_1| = \binom{i}{s}$.

Por otra parte si $f \in sop(c)^C \bigcap sop(v)$, entonces

$$P(v_f|0_f) = p,$$

pues es la probabilidad de que el símbolo llegue con error.

Si $l \in sop(c)^C \bigcap sop(v)^C$, entonces

$$P(v_l|0_l) = 1 - p,$$

la cual es la probabilidad que el símbolo llegue sin error.

Claramente si $v \in H$, entonces $|sop(c)^C \bigcap sop(v)| = j - s$. Por lo tanto si $sop(c)^C = \{m_{i+1}, ..., m_n\}$, se tiene que

$$\begin{aligned} P(v_{m_{i+1}}...v_{m_n}|0_{m_{i+1}}..,0_{m_n}) &= \underbrace{P(v_f|0_f) \cdots P(v_f|0_f)}_{(j-s)-veces} \cdot \underbrace{P(v_l|0_l) \cdots P(v_l|0_l)}_{(n-i)-(j-s)-veces} \\ &= (P(v_f|0_f))^{j-s} \cdot (P(v_l|0_l)^{n-i-(j-s)} \\ &= p^{j-s} \cdot (1-p)^{n-i-(j-s)}. \end{aligned}$$

Por lo tanto si

$$H_2 = \{v_{m_{i+1}}...v_{m_n} \mid v \in H\},$$

entonces

$$\begin{aligned} P(Y \in H_2 | X = 0_{F_q^{n-i}}) &= \binom{n-i}{j-s} \underbrace{P(v_f|0_f) \cdots P(v_f|0_l)}_{(j-s)-veces} \cdot \underbrace{P(v_l|0_l) \cdots P(v_l|0_l)}_{(n-i)-(j-s)-veces} \\ &= \binom{n-i}{j-s} (P(v_f|0_f))^{j-s} \cdot (P(v_l|0_l)^{n-i-(j-s)} \\ &= \binom{n-i}{j-s} p^{j-s} \cdot (1-p)^{n-i-(j-s)}. \end{aligned}$$

Dado que $|H_2| = \binom{n-i}{j-s}$.

Como

$$P(Y \in H \mid X = 0) = P(Y_1 \in H_1 \mid X = 0_{F_q^i}) \cdot P(Y_2 \in H_2 \mid X = 0_{F_q^{n-i}}),$$

se tiene que

$$\begin{aligned} P(Y \in H | X = 0) = \binom{i}{s} (\frac{p}{q-1})^{i-s} (1 - \frac{p}{q-1})^s \\ \cdot \binom{n-i}{j-s} p^{j-s} (1-p)^{n-i-(j-s)}. \end{aligned}$$

Con lo cual

$$\begin{aligned} P(Y \in \{v \in F_q^n | d(v,c) = j\} | X = 0) = \sum_{s=0}^{j} \binom{i}{s} (\frac{p}{q-1})^{i-s} (1 - \frac{p}{q-1})^s \cdot \\ \binom{n-i}{j-s} p^{j-s} \cdot (1-p)^{n-i-(j-s)}. \end{aligned}$$

En virtud de lo anterior tenemos

$$\begin{aligned} P(Y \in B_t(c) | X = 0) = \sum_{j=0}^{t} \sum_{s=0}^{j} [\binom{i}{s} (\frac{p}{q-1})^{i-s} (1 - \frac{p}{q-1})^s \\ \binom{n-i}{j-s} p^{j-s} (1-p)^{n-i-j+s}]. \end{aligned}$$

Por lo tanto si C es un $[n,k,d]$-código, $A(x)=\sum_{i=0}^{n}A_ix^i$ es su polinomio enumerador de pesos y $t\leqslant\frac{d-1}{2}$, entonces

$$\begin{aligned}P_{ue}(C,t,p) &= P(Y\in\cup_{0\neq c\in C}B_t(c)|X=0)\\ &= \sum_{i=1}^{n}A_i\sum_{j=0}^{t}\sum_{s=0}^{j}[\binom{i}{s}(\frac{p}{q-1})^{i-s}(1-\frac{p}{q-1})^s\\ &\cdot\binom{n-i}{j-s}p^{j-s}(1-p)^{n-i-j+s}].\end{aligned}$$

Observe que $\binom{n-i}{j-s}=0$ cuando $j-s>n-i$.
Cabe destacar que esta probabilidad tiene el mismo valor para todas las A_i palabras de peso i.

3.1.2 Corolario Con las hipótesis del teorema 3.1.1. Para un código $1-$corrector C, se tiene

$$\begin{aligned}P_{ue}(C,1,p) = &\sum_{i=1}^{n-1}A_i(\frac{1}{q-1})^ip^i(1-p)^{n-i-1}[i(q-1)+(1+qi)p\\ &+(n-1)p^2+A_n(\frac{1}{q-1})^np^{n-1}[n(q-1)-p(n-1)].\end{aligned}$$

Demostración.

$$
\begin{aligned}
P_{ue}(C,1,p) &= \sum_{i=1}^{n} A_i \sum_{j=0}^{1}\sum_{s=0}^{j}[\binom{i}{s}(\frac{p}{q-1})^{i-s}(1-\frac{p}{q-1})^{s} \\
&\cdot \binom{n-i}{j-s} p^{j-s}(1-p)^{n-i-j+s}] \\
&= \sum_{i=1}^{n} A_i[(\frac{p}{q-1})^{i}(1-p)^{n-i} + (\frac{p}{q-1})^{i}(n-i)p(1-p)^{n-i-1} \\
&+ i(\frac{p}{q-1})^{i-1}(1-\frac{p}{q-1})(1-p)^{n-1}] \\
&= \sum_{i=1}^{n} A_i(\frac{p}{q-1})^{i}(1-p)^{n-i}[1+(n-i)p(1-p)^{-1} \\
&+ i(\frac{p}{q-1})^{-1}(1-\frac{p}{q-1})] \\
&= \sum_{i=1}^{n-1} A_i(\frac{p}{q-1})^{i}(1-p)^{n-i}[1+\frac{np-ip}{1-p}+\frac{iq-i}{p}-i] \\
&+ A_n(\frac{p}{q-1})^{n}[1+n(\frac{q-1}{p})(1-\frac{p}{q-1})] \\
&= \sum_{i=1}^{n-1} A_i(\frac{p}{q-1})^{i}(1-p)^{n-i}[\frac{p-p^2+np^2-ip^2+iq-i-iqp+ip-ip+ip^2}{(1-p)p}] \\
&+ A_n(\frac{p}{q-1})^{n}[1+\frac{nq-n}{p}-n] \\
&= \sum_{i=1}^{n-1} A_i(\frac{1}{q-1})^{i}p^{i-1}(1-p)^{n-i-1}[i(q-1)+(1-qi)p(n-1)p^2] \\
&+ A_n(\frac{p}{q-1})^{n}p^{-1}(p+nq-n-np) \\
&= \sum_{i=1}^{n-1} A_i(\frac{1}{q-1})^{i}p^{i}(1-p)^{n-i-1}[i(q-1)+(1+qi)p+(n-1)p^2 \\
&+ A_n(\frac{1}{q-1})^{n}p^{n-1}[n(q-1)-p(n-1)]
\end{aligned}
$$

3.2. Comparando P_{ue} en dos códigos con p acotado

Con el fin de comparar P_{ue} para dos $[n,k,d]$-códigos, supongamos que en C y C', se pueden calcular los valores del teorema 3.1.1, para un error de símbolo de probabilidad p suficientemente pequeño, hay una manera fácil la cual se describe a continuación.

3.2.1 Definición. Sea $f(x)=\sum_{i=0}^{n} a_i x^i$ y $g(x)=\sum_{i=0}^{n} b_i x^i$ polinomios con coeficientes no negativos $a_i, b_i \in \mathbb{R}$, se tiene que $f(x) \prec g(x)$, si y sólo si, $(a_0,...,a_n) \prec (b_0,...,b_n)$ en orden lexicográfico, esto es, existe $l \in \{0,1,...,n\}$ de tal manera que $a_i = b_i$ para todos los $i < l$ pero $a_l < b_l$. Claramente $f(x) \preceq g(x)$ significa que $f(x) \prec g(x)$ o $f(x) = g(x)$.

3.2.2 Teorema. Sean C y C' $[n,k,d]$ y $[n,k,d']$-códigos con polinomios enumeradores de peso $A(x)$ y $A'(x)$ respectivamente. Supongamos que $t \leq min\{\frac{d-1}{2}, \frac{d'-1}{2}\}$. Para algún p adecuado las siguientes condiciones son equivalentes.

1. $P_{fd}(C,t,p) \leq P_{fd}(C',t,p)$
2. $P_{ue}(C,t,p) \leq P_{ue}(C',t,p)$
3. $A(x) \preceq A'(x)$.

Demostración.
La equivalencia de 1. y 2. se debe al corolario 2.3.4 Por lo tanto, es suficiente demostrar que 2. y 3. son equivalentes. Podemos suponer que $A(x) \neq A'(x)$ y que l, es la menor posición en la que los pesos de C y C' son diferentes. Ahora consideremos la función $f : [0,1] \longrightarrow \mathbb{R}$, definida por:

$$f(p) = P_{ue}(C',t,p) - P_{ue}(C,t,p) = \sum_{i=l}^{n} (A'_i - A_i) f_i(p),$$

donde

$$f_i(p) = \sum_{j=0}^{t} \sum_{s=0}^{j} \Big[\binom{i}{s} (\frac{p}{q-1})^{i-s} (1 - \frac{p}{q-1})^{s} \binom{n-i}{j-s} \cdot p^{j-s} (1-p)^{n-i-j+s} \Big]$$

(ver teorema 3.1.1).
Para demostrar este teorema veremos que para un valor de p adecuado la función $f(p) > 0$, si y sólo si, $A'_i - A_i > 0$, veamos.

Como $0 \leq j \leq t < l$ dado que $l \geqslant min(d, d') > t$, se tiene que para $i \geqslant l$ la función $f_i(p)$ es un polinomio que toma la siguiente forma:

$$\begin{aligned}
f_i(p) = & \underbrace{\binom{i}{t}(\frac{p}{q-1})^{i-t}(1-\frac{p}{q-1})^{t}(1-p)^{n-i}}_{s=t} \\
& + \underbrace{\binom{i}{t-1}(\frac{p}{q-1})^{i-t+1}(1-\frac{p}{q-1})^{t-1}(1-p)^{n-i}}_{s=j=t-1} \\
& + \cdots + \underbrace{(\frac{p}{q-1})^{i}(1-p)^{n-i}}_{s=j=0} \\
& = \binom{i}{t}(\frac{p}{q-1})^{i-t}[1-\sum_{k=1}^{t}\frac{t!}{k!(t-k)!}(-\frac{p}{q-1})^{k}] \\
& \cdot [1-\sum_{m=1}^{n-i}\frac{(n-i)!}{m!(n-i-m)!}(-p)^{m}] + \binom{i}{t-1}(\frac{p}{q-1})^{i-t+1} \\
& \cdot [1+\sum_{k=1}^{t-1}\frac{(t-1)!}{k!((t-1)-k)!}(-\frac{p}{q-1})^{k}][1+\sum_{m=1}^{n-i}(-p)^{m}] \\
& + \cdots + (\frac{p}{q-1})^{i}[1-\sum_{f=1}^{n-i}\frac{(n-i)!}{f!(n-i-f)!}(-p)^{f}]
\end{aligned}$$

Por lo tanto $f_i(p)$ es un polinomio de la forma:

$$f_i(p) = \binom{i}{t}(\frac{1}{q-1})^{i-t}p^{i-t} + \sum_{k=r}^{n}a_k p^k$$

donde $r > i - t$. Por lo tanto $f(p)$ es un polinomio de la forma

$$f(p) = (A'_l - A_l)\binom{l}{t}(\frac{1}{q-1})^{l-t}p^{l-t} + \sum_{k=r}^{n}a_k p^k .....(1)$$

donde $r > l - t$. En particular para p lo suficientemente pequeño tenemos $f(p) > 0$, si y sólo si, $A_l < A'_l$. Así, cuando p es sufientemente pequeño, se tiene que $P_{ue}(C, t, p) < P_{ue}(C', t, p)$, si y sólo si, $A(x) \prec A'(x)$.

3.2.3 Teorema. Sean C y C' $[n, k, d]_q$ y $[n, k, d']_q$-códigos con polinomios enumeradores de peso $A(x)$ y $A'(x)$ respectivamente y sea $t \leq min\{\frac{d-1}{2}, \frac{d'-1}{2}\}$.

Supongamos que $A(x) \neq A'(x)$ y que l es la menor posición en las que las distribuciones de peso de C y C' difieren. Si $A(x) \preceq A'(x)$ entonces

$$P_{ue}(C,t,p) \leq P_{ue}(C',t,p)$$

para todos los p con

$$p \leq \gamma = \frac{(A'_l - A_l)\binom{l}{t}(q-1)}{(\sum_{i=l}^{n} A_i)(\sum_{j=0}^{t}\binom{n}{j}(q-1)^j) + (A'_l - A_l)\binom{l}{t}(q-1)}.$$

Demostración.
Claramente

$$\begin{aligned} P_{ue}(C,t,p) &= P(Y \in \bigcup_{0\neq c\in C} B_t(c) | X = 0) \\ &= \sum_{r=1}^{n} |\{v \in \bigcup_{0\neq c\in C} B_t(c) | wt(v) = r\}| (\frac{p}{q-1})^r (1-p)^{n-r}. \end{aligned}$$

Definamos:

$$\eta_r := |\{v \in \bigcup_{c\in C, wt(c)\geq l} B_t(c) | wt(v) = r\}|$$

y

$$\eta'_r := |\{v' \in \bigcup_{c'\in C', wt(c')\geq l} B_t(c') | wt(v') = r\}|.$$

Si tomamos $m = l - t$ entonces $\eta_r = \eta'_r$ para cualquier $r < m$ y $\eta'_m - \eta_m = (A'_l - A_l)\binom{l}{t}$ (ver ecuación (1) del Teorema 3.2.2). Por lo tanto

$$\begin{aligned} f(p) &= P_{ue}(C',t,p) - P_{ue}(C,t,p) \\ &= \sum_{r=m}^{n} (\eta'_r - \eta_r)(\frac{p}{q-1})^r (1-p)^{n-r} \\ &= (1-p)^n \sum_{r=m}^{n} (\eta'_r - \eta_r)(\frac{p}{(q-1)(1-p)})^r \\ &= (1-p)^n \sum_{r=m}^{n} (n'_r - n_r) x^r \end{aligned}$$

donde $x = \frac{p}{(q-1)(1-p)}$. En las observaciones 1.2.1 vimos que $x \in [0,1]$. Por consiguiente.

$$\begin{aligned} g(x) = f(p) &= (1-p)^n((A'_l - A_l)\binom{l}{t}x^m + \sum_{r=m+1}^{n}(\eta'_r - \eta_r)x^r) \\ &\geq (1-p)^n((A'_l - A_l)\binom{l}{t}x^m - \sum_{r=m+1}^{n}\eta_r x^r) \\ &\geq (1-p)^n x^m((A' - A_l)\binom{l}{t} - x\sum_{r=m+1}^{n}\eta_r). \end{aligned}$$

Ahora definamos

$$a(C,l) := \sum_{i=l}^{n} A_i$$

y

$$b(q,t) := |B_t(0)| = \sum_{j=0}^{t}\binom{n}{j}(q-1)^j,$$

dado que

$$p \leq \gamma = \frac{(A'_l - A_l)\binom{l}{t}(q-1)}{(\sum_{i=l}^{n} A_i)(\sum_{j=0}^{t}\binom{n}{j}(q-1)^j) + (A'_l - A_l)\binom{l}{t}(q-1)},$$

entonces

$$\frac{p}{(q-1)(1-p)} \leqslant \frac{(A'_l - A_l)\binom{l}{t}}{a(C,l)b(q,t)}.$$

Por otra parte

$$\sum_{r=m+1}^{n}\eta_r \leq a(C,l)b(q,t).$$

Así

$$g(x) \geq (1-p)^n x^m((A'_l - A_l)\binom{l}{t} - xa(C,l)b(q,t))$$

el lado derecho es ≥ 0 por definición de γ

3.2.4 Observación. El factor γ en el teorema anterior aumenta si $(A'_l - A_l)\binom{l}{t}$ aumenta. Además si $A'_l - A_l \geq q-1$, podemos sustituir γ en el Teorema 3.2.3 por

$$\overline{\gamma} = \frac{\binom{d}{t}(q-1)^2}{(q^k-1)(\sum_{j=0}^{t}\binom{n}{j}(q-1)^j) + \binom{d}{t}(q-1)^2},$$

dado que $\sum_{i=l}^{n} A_i \leqslant q^k - 1$. Podemos observar que $\overline{\gamma}$ solo depende de los parámetros $[n,k,d]_q$ y t.

3.2.5 Corolario Sea C un $[n,k,d]_q$-código, si $t \leqslant \frac{d-1}{2}$, $p < \frac{q-1}{q}$ y $A(x) = \sum_{i=0}^{n} A_i x^i$ es el polinomio enumerador de pesos de C, entonces

1. $P_{ue}(C,t,p) \geq A_d\binom{d}{t}(\frac{p}{(q-1)(1-p)})^{d-t}(1-p)^n$.

2. $\lim_{p\to 0}\frac{P_{ue}(C,t,p)}{p^{d-t}} = A_d\binom{d}{t}(\frac{1}{q-1})^{d-t}$.

Demostración.

1. Del Teorema 3.1.1 se tiene

$$P_{ue}(C,t,p) = \sum_{i=1}^{n} A_i \sum_{j=0}^{t}\sum_{s=0}^{j}[\binom{i}{s}(\frac{p}{q-1})^{i-s}(1-\frac{p}{q-1})^s \cdot \binom{n-i}{j-s}p^{j-s}(1-p)^{n-i-j+s}]$$

Donde cada sumando es no negativo. Teniendo $i = d$ y $j = s = t$, obtenemos:

$$\begin{aligned} P_{ue}(C,t,p) &\geq A_d\binom{d}{t}(\frac{p}{q-1})^{d-t}(1-\frac{p}{q-1})^t(1-p)^{n-d} \\ &\geq A_d\binom{d}{t}(\frac{p}{q-1})^{d-t}(1-p)^{n-d+t}. \end{aligned}$$

2. Por el Teorema 3.1.1 se tiene claramente que

$$P_{ue}(C,t,p) = A_d\binom{d}{t}(\frac{1}{q-1})^{d-t}p^{d-t} + \sum_{k=r}^{n} a_k p^k,$$

donde $r > d-t$, obteniendo así la afirmación.

3.2.6 Ejemplo. Sea $K = \mathbb{F}_2$ y definamos

$$C := \{(c_1, ..., c_7) | c_j \in K, \begin{matrix} c_1 + c_4 + c_6 + c_7 = 0 \\ c_2 + c_4 + c_5 + c_7 = 0 \\ c_3 + c_5 + c_6 + c_7 = 0 \end{matrix}\}.$$

En el ejemplo 1.3.6 vimos que C es un $[7, 4, 3]$-código y por 1.5.10 el polinomio enumerador de pesos de C es $A = 1 + 7x^3 + 7x^4 + x^7$. Entonces por el corolario 3.2.5 se tiene que

$$P_{ue}(C, t, p) \geqslant 7 \binom{3}{t} \left(\frac{p}{1-p}\right)^{3-t} (1-p)^7.$$

Si $t = 1$ y $p = \frac{1}{3}$, entonces

$$P_{ue}(C, 1, \frac{1}{3}) \geqslant 7 \binom{3}{1} \left(\frac{1}{2}\right)^2 (\frac{2}{3})^7 \approx 0{,}307270233.$$

3.2.7 Ejemplo. Considere códigos binarios C y C' con parámetros $[15, 6, 4]$ generados por $(I_6 A)$ y $(I_6 A')$ respectivamente donde I_6 denota la matriz identidad de orden 6 y

$$A = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

$$A' = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

C y C' tienen polinomios enumeradores de pesos $A(x) = 1 + 8x^4 + 16x^6 + 21x^8 + 16x^{10} + 2x^{12}$ y $A'(x) = 1 + 9x^4 + 51x^8 + 3x^{12}$ respectivamente.

1. Demostremos que $P_{ue}(C, 0, p) < P_{ue}(C', 0, p)$, si y sólo si, $A(\frac{p}{1-p}) < A'(\frac{p}{1-p})$.
   Dado que

$$P_{ue}(C, 0, p) = P(Y \in \bigcup_{c \neq c' \in C} B_0(c') | X = c) = P(Y \in C \setminus \{0\} | X = 0)$$

Entonces:

$$P_{ue}(C,0,p) = \sum_{i=1}^{n} A_i(\frac{p}{q-1})^i(1-p)^{n-i} = (1-p)^n \sum_{i=1}^{n} A_i(\frac{1}{q-1})^i(\frac{p}{1-p})^i.$$

Por lo tanto
$P_{ue}(C,0,p) < P_{ue}(C',0,p)$, si y sólo si,
$(1-p)^n \sum_{i=1}^{n} A_i(\frac{1}{q-1})^i(\frac{p}{1-p})^i < (1-p)^n \sum_{i=1}^{n} A'_i(\frac{1}{q-1})^i(\frac{p}{1-p})^i$
Con lo anterior tenemos que:

$P_{ue}(C,0,p) < P_{ue}(C',0,p)$, si y sólo si, $A(\frac{p}{1-p}) < A'(\frac{p}{1-p})$ que es lo que se quería demostrar.
Ahora consideremos la siguiente función:

$$\begin{aligned} f(p) &= \sum_{i=4}^{15}(A'_i - A_i)(\frac{p}{1-p})^i \\ &= (\frac{p}{1-p})^4 - 16(\frac{p}{1-p})^6 + 30(\frac{p}{1-p})^8 - 16(\frac{p}{1-p})^{10} + (\frac{p}{1-p})^{12}. \end{aligned}$$

Note que $f(p) > 0$ para p lo suficientemente pequeño, por ejemplo si $p \leq \gamma = \frac{1}{64} \sim 0{,}0156$ por el Teorema 3.2.3. En realidad $f(p) > 0$ para $0 < p \leq 0{,}2113...$, pero $f(p) < 0$ en el resto del intervalo $(0, \frac{1}{2})$. Por lo tanto, sólo para la probabilidad de error p pequeña el código C tiene la menor probabilidad de detección de error, P_{ue}.

2. Si usamos C y C' para un código 1-corrector, i.e. $t = 1$ entonces, por el Corolario 3.1.2 se tiene claramente $P_{ue}(C,1,p) < P_{ue}(C',1,p)$ exactamente para $0 < p \leq 0{,}1383$, pero el valor de γ según el Teorema 3.2.3 resulta ser igual a $\frac{4}{1012} = 0{,}0039525$, por lo tanto el valor γ no es suficientemente bueno para acotar p en el caso $t = 1$ del presente ejemplo.

El cálculo para la cota de p utilizando el Teorema 3.2.2 suele ser difícil de determinar dependiendo de la distribución del peso. Sin embargo, en algunas ocasiones las condiciones adicionales son fácilmente comparables para la decodificación utilizando la probabilidad P_{ue} de dos códigos para todo $0 < p < \frac{q-1}{q}$.

3.2.8 Teorema. Sean C y C' $[n,k,d]_q$ y $[n,k,d']_q$-códigos con distribuciones de peso $(A_0,...,A_n)$ y $(A'_0,...,A'_n)$ respectivamente. Supongamos que $\sum_{i=0}^{j} A_i \leq \sum_{i=0}^{j} A'_i$ para todo $j = 0,...,n$ con desigualdad estricta para al menos un j. Entonces:

$$P_{ue}(C,t,p) < P_{ue}(C',t,p)$$

para todo p con $0 < p < \frac{q-1}{q}$ y para todo $t \leq min\{\frac{d-1}{2}, \frac{d'-1}{2}\}$.

Demostración.
Para probar que $P_{ue}(C,t,p) < P_{ue}(C',t,p)$ tenemos que demostrar que

$$\sum_{i=0}^{n} A_i f_i(p) < \sum_{i=0}^{n} A'_i f_i(p).$$

donde

$$f_i(p) = \sum_{j=0}^{t}\sum_{s=0}^{j}[\binom{i}{s}\binom{p}{q-1}^{i-s}(1-\tfrac{p}{q-1})^s\binom{n-i}{j-s}\cdot p^{j-s}(1-p)^{n-i-j+s}]$$

(ver Teorema 3.1.1).
Supongamos que se ha probado que $f_{i+1}(p) < f_i(p)$ para $i = 0, ..., n$ donde $f_{n+1}(p) = 0$. Entonces

$$\begin{aligned} f(p) &= \sum_{i=0}^{n}(A'_i - A_i)f_i(p) \\ &= \sum_{j=0}^{n}(f_j(p) - f_{j+1}(p))\sum_{i=0}^{j}(A'_i - A_i) \end{aligned}$$

puesto que $f_j(p) - f_{j+1}(p) > 0$ para todos los j supuestos en el teorema implica que $f(p) > 0$ para $0 < p < \frac{1}{2}$ y la prueba está completa, por lo tanto queda por demostrar que $f_{i+1}(p) < f_i(p)$ para todo i y cualquier t.

Recordemos que $f_i(p) = P(Y \in B_t(c)|X = 0)$ donde c es una palabra tal que $d(c,0) = i$. note que la probabilidad $f_i(p)$ depende solo del peso de c y no del codeword c. Claramente $f_n(p) > f_{n+1}(p) = 0$. Por lo tanto podemos suponer que si $i < n$ y sin pérdida de generalidad, podemos tomar

$$f_i(p) = \sum_{w \in B_t(c)} P(Y = w|X = 0)$$

y

$$f_{i+1}(p) = \sum_{v \in B_t(\overline{c})} P(Y = v|X = 0).$$

Observe que para cualquier $w \in B_t(c)$, tenemos

$$d(w,\overline{c}) \leq d(w,c) + d(c,\overline{c}) \leq t + 1.$$

Por lo tanto, si $w \in B_t(c) \setminus B_t(\overline{c})$ entonces $d(w,c) = t$ y $d(w,\overline{c}) = t+1$. Esto significa que el último dígito de w es 0 (cero).
Consideremos la siguiente biyección

$$\rho : B_t(c) \longrightarrow B_t(\overline{c}).$$

Propuesta por:

$$\rho(w) = w \text{ si } w \in B_t(c) \bigcap B_t(\overline{c})$$
$$\rho(w) = w + c \text{ si } w \in B_t(c) \setminus B_t(\overline{c}).$$

Es fácil observar que $d(w,0) \leq d(\rho(w),0)$ para cualquier $w \in B_t(c)$ por otra parte ya que $p < \frac{q-1}{q}$ tenemos

$$P(Y = w|X = 0) \geq P(Y = \rho(w)|X = 0)$$

con desigualdad estricta para $w \in B_t(c) \setminus B_t(\overline{c}) \neq \phi$.
Finalmente

$$\begin{aligned} f_i(p) &= \sum_{w \in B_t(c)} P(Y = w|X = 0) \\ &> \sum_{w \in B_t(c)} P(Y = \rho(w)|X = 0) \\ &= \sum_{v \in B_t(\overline{c})} P(Y = v|X = 0) = f_{i+1}(p). \end{aligned}$$

Lo que demuestra la proposición.

Ejemplo.
Sea C el $[n = 2^k - 1, k, 2^{k-1}]$ código binario Simplex. Claramente C tiene la siguiente distribución de pesos:

$$A_0 = 1, A_{2^{k-1}} = 2^k - 1 = n \text{ y todos los demás } A_i = 0.$$

Sea C' el $[n,k]$ código generado por $e + c$ donde c corre a través de una base de C y $e = (1,..,1)$ denota el vector lleno de 1. Fácilmente se tiene que C' tiene una distribución de pesos dada por:

$$A'_0 = 1, A'_{2^{k-1}-1} = 2^{k-1}, A'_{2^{k-1}} = 2^{k-1} - 1 \text{ y todos los demás } A_i = 0.$$

Aplicando 3.2.8 se tiene que

$$P_{ue}(C,t,p) < P_{ue}(C',t,p)$$

para todo $0 < p < \frac{1}{2}$. Note que C' es un $[2^k - 2, k, 2^{k-1} - 1]$ código. Esto no es sorprendente como veremos a continuación.

Con el fin de tener el siguiente teorema se define el soporte de un código C de longitud n como:

$$Supp(C) = \{i| \text{ existe } (x_1, ..., x_n) \in C, x_i \neq 0\}$$

3.2.9 Teorema. Sean C y C' $[n, k]-$ códigos sobre un mismo cuerpo F_q, con distribuciones de pesos $(A_0, ..., A_n)$ y $(A'_0, ..., A'_n)$ respectivamente. Suponga que:

$$\sum_{i=0}^{j} A_i \leq \sum_{i=0}^{j} A'_i \text{ para todo } j = 0, ..., n.$$

Si $|Supp(C)| = |Supp(C')|$ entonces $A_i = A'_i$ para todo $i = 0, ..., n$, esto es, C y C' son formalmente equivalentes.

Demostración.
Sea $r_i = A'_i - A_i$ para $i = 0, ..., n$. Por ([11], 4.5.1), tenemos:

$$\sum_{c \in C} wt(c) = |Supp(C)|(q-1)q^{k-1}.$$

En particular,

$$\begin{aligned} \sum_{i=0}^{n} iA_i = \sum_{c \in C} wt(c) &= |Supp(C)|(q-1)q^{k-1} \\ &= |Supp(C')|(q-1)q^{k-1} \\ &= \sum_{c' \in C'} wt(c') \\ &= \sum_{i=0}^{n} iA'_i. \end{aligned}$$

Por lo tanto $\sum_{i=0}^{n} ir_i = 0 = \sum_{i=1}^{n} ir_i$. Se debe tener en cuenta que $r_1 + r_2 + ... + r_n = 0$ cuando $|C| = |C'|$.
De esto se deduce que:

$$\begin{aligned} 0 = \sum_{i=1}^{n} ir_i &= r_1 + 2r_2 + ... + nr_n \\ &= (r_1 + ... + r_n) + (r_2 + ... + r_n) + ... + (r_{n-1} + r_n) + r_n \\ &= n(r_1 + ... + r_n) - [r_1 + (r_1 + r_2) + ... + (r_1 + ... + r_{n-1})] \\ &= -[r_1 + (r_1 + r_2) + ... + (r_1 + ... + r_{n-1})]. \end{aligned}$$

Puesto que $\sum_{i=0}^{j} r_i = \sum_{i=1}^{j} r_i \geq 0$ obtenemos que $\sum_{i=1}^{j} r_i = 0$ para todo $j = 1, ...n$. Esto demuestra que $r_i = 0$ para $i = 1, ...n$. Por lo tanto $A_i = A'_i$ para $i = 1, ...n$ lo que prueba el teorema ya que, obviamente $A_0 = A'_0$.

Por la dualidad de MacWilliams la distribución de un código dual $C^{\perp}$ esta determinado de manera única por C. Por lo tanto de acuerdo con P_{ue} o P_{fd}, un código C y su dual están relacionados ya que ambas probabilidades sólo dependen de la distribución de los pesos. Sin embargo, la conexión parece ser bastante complicada como se muestra en los siguientes ejemplos.

3.2.10 Ejemplos. Por [3], los dos mejores $[15, 3, 7]$ códigos binarios tienen polinomios enumeradores de pesos

$$A(x) = 1 + x^7 + 2x^8 + 3x^9 + x^{10}$$

$$A'(x) = 1 + x^7 + 3x^8 + 2x^9 + x^{11}.$$

Por MacWilliams fácilmente se pueden calcular los polinomios enumeradores de pesos de los códigos duales, estos están dados por:
$A^{\perp} = 1 + 10x^2 + 66x^3 + 173x^4 + 358x^5 + 630x^6 + 820x^7 + 795x^8 + 620x^9 + 382x^{10}170x^{11} + 55x^{12} + 14x^{13} + 2x^{14}$ y $A'^{\perp} = 1 + 11x^2 + 62x^3 + 175x^4 + 370x^5 + 613x^6 + 812x^7 + 823x^8 + 612x^9 + 365x^{10} + 182x^{11} + 57x^{12} + 10x^{13} + 3x^{14}$ respectivamente. En particular $A(x) \prec A'(x)$ y $A^{\perp} \prec A'^{\perp}$.

b) Sea C el código binario con matriz generadora

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Es fácil comprobar que C es un $[6, 3, 2]$ código con polinomio enumerador de peso

$$A(x) = 1 + x^2 + 4x^3 + x^4 + x^6.$$

El código dual $C' = C^{\perp}$ de C es generado por la matriz

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$C^{\perp}$ es también un $[6, 3, 2]$ código con polinomio enumerador de pesos

$$A'(x) = 1 + 2x^2 + 5x^4.$$

Se tiene que $A(x) \prec A'(x)$, pero $A'^{\perp}(x) = A(x) \prec A'(x) = A^{\perp}(x)$

Capítulo 4

Propiedades de las funciones P_{fd} y P_{ue}

En el capitulo 3 hemos demostrado que P_{fd} y P_{ue} son igualmente buenos cuando se usa para encontrar un código óptimo con respecto a la probabilidad de decodificación de distancia limitada. La función P_{fd} lleva una bonita propiedad, es decir, aumenta monótonamente si la probabilidad en el error del símbolo p aumenta monótonamente esto se aplica a P_{ue} incluso si se utiliza el código sólo para la detección de errores, es decir, $t = 0$. Así, en contraste con P_{ue} la probabilidad de error en la decodificación P_{fd} siempre refleja el hecho de que canales menos fiables provocan más errores en las transmisiones lo que debería llevar a más errores en el proceso de decodificación.

4.0.11 Teorema. Sea C un $[n, k, d]_q$-código y sea $t \leq \frac{d-1}{2}$, entonces la probabilidad de error en la decodificación $P_{fd}(C, t, p)$ es una función monótona creciente en p en el intervalo $[0, \frac{q-1}{q}]$.

Demostración. Definamos:

$$\eta_r := |\{v \in \cup_{c \in C} B_t(c) | wt(v) = r\}|.$$

Note que $\eta_r = \binom{n}{r} (q-1)^r$ para $r \leq t$. Con esta notación tenemos

$$P_{ue}(C, t, p) = \sum_{r=t+1}^{n} \eta_r (\frac{p}{q-1})^r (1-p)^{n-r} = (1-p)^n \sum_{r=t+1}^{n} \eta_r \big(\frac{p}{(q-1)(1-p)}\big)^r$$

y

$$P_{fd}(C,t,p) = \frac{P_{ue}(C,t,p)}{P_{ue}(C,t,p) + \sum_{h=0}^{t} \eta_h (\frac{p}{q-1})^h (1-p)^{n-h}}$$
$$= \frac{(1-p)^n \sum_{r=t+1}^{n} \eta_r \big(\frac{p}{(q-1)(1-p)}\big)^r}{(1-p)^n \sum_{r=t+1}^{n} \eta_r \big(\frac{p}{(q-1)(1-p)}\big)^r + (1-p)^n \sum_{h=0}^{t} \eta_h \big(\frac{p}{(q-1)(1-p)}\big)^h}.$$

Si definimos $\chi = \frac{p}{(q-1)(1-p)}$ obtenemos

$$P_{fd}(C,t,p) = \frac{\sum_{r=t+1}^{n} \eta_r \chi^r}{\sum_{r=t+1}^{n} \eta_r \chi^r + \sum_{h=0}^{t} \eta_h \chi^h} = f(\chi).$$

Observe que χ es una función monótonamente creciente en p en el intervalo $[0, \frac{q-1}{q}]$. Por lo tanto, al tomar la derivada de $f(\chi)$, es fácil comprobar que $P_{fd}(C,t,p)$ es una función monótonamente creciente en p en el intervalo $[0, \frac{q-1}{q}]$ si y sólo si

$$\sum_{r=t+1}^{n} \sum_{h=0}^{t} (r-h) \eta_r \eta_h \chi^{r+h-1} \geq 0.$$

Para $\chi \in (0,1]$. Esto es evidente dado que $r > h$ y $\eta_r, \eta_h \geq 0$.
El aumento del número de errores corregibles debe dar lugar a un aumento de la probabilidad de error de decodificación. Este hecho se refleja en ambas funciones. sin embargo la prueba de P_{fd} resulta ser mucho más complicada.

4.0.12 Teorema. Si C es un $[n,k,d]_q$-código y $0 \leq t \leq t' \leq \frac{d-1}{2}$, entonces:

1. $P_{ue}(C,t,p) < P_{ue}(C,t',p)$
2. $P_{fd}(C,t,p) < P_{fd}(C,t',p)$

para todo $p \in (0, \frac{q-1}{q})$.

Demostración.

1. De acuerdo a 3.1.1 tenemos
   $P_{ue}(C,t',p) = P_{ue}(C,t,p) + \sum_{i=1}^{n} A_i \sum_{j=t+1}^{t'} \sum_{s=0}^{j} \big[\binom{i}{s} (\frac{p}{q-1})^{i-s} (1 - \frac{p}{q-1})^s \binom{n-i}{j-s} p^{j-s} (1-p)^{n-i-j+s} \big]$ donde la suma triple es positiva para $p \neq 0$.

2. Para probar la afirmación en 2), podemos suponer que $t' = t+1$. Teniendo en cuenta que para números reales positivos a, b, c, d la desigualdad $\frac{a}{a+b} < \frac{c}{c+d}$ es equivalente a $\frac{a}{b} < \frac{c}{d}$ la afirmación puede ser reformulada de acuerdo con 2.3.1

$$\frac{P_{ue}(C,t,p)}{P(Y \in B_t(0)|X=0)} < \frac{P_{ue}(C,t+1,p)}{P(Y \in B_{t+1}(0)|X=0)}$$

De acuerdo con 3.1.1 esto es equivalente a

$$\frac{\sum_{i=d}^{n} A_i \sum_{j=0}^{t} \alpha(i,j)}{P(Y \in B_t(0)|X=0)} < \frac{\sum_{i=d}^{n} A_i \sum_{j=0}^{t+1} \alpha(i,j)}{P(Y \in B_{t+1}(0)|X=0)}$$

donde $\alpha(i,j) = \sum_{s=0}^{j} \left[\binom{i}{s} (\frac{p}{q-1})^{i-s} (1-\frac{p}{q-1})^{s} \binom{n-i}{j-s} p^{j-s} (1-p)^{n-i-j+s} \right]$. Por lo tanto, es suficiente para demostrar para cada $i \in \{d, ..., n\}$ que

$$\frac{\sum_{j=0}^{t} \alpha(i,j)}{P(Y \in B_t(0)|X=0)} < \frac{\sum_{j=0}^{t+1} \alpha(i,j)}{P(Y \in B_{t+1}(0)|X=0)},$$

lo que significa que

$$\frac{P(Y \in B_{t+1}(0)|X=0)}{P(Y \in B_t(0)|X=0)} < \frac{\sum_{j=0}^{t+1} \alpha(i,j)}{\sum_{j=0}^{t} \alpha(i,j)}. (1)$$

Ahora definamos $D_j(c) = \{w \in F_q^n | d(c,w) = j\}$ para $j = 0, 1, ..., n$ y $c \in F_q^n$. A continuación (1) puede escribirse como

$$1 + \frac{P(Y \in D_{t+1}(0)|X=0)}{\sum_{j=0}^{t} P(Y \in D_j(0)|X=0)} < 1 + \frac{\alpha(i,t+1)}{\sum_{j=0}^{t} \alpha(i,j)}$$

para $d \leq i \leq n$. Dado que para números reales positivos a, b, a_j, b_j obviamente $\frac{a}{a_j} < \frac{b}{b_j}$ implica $\frac{a}{\sum a_j} < \frac{b}{\sum b_j}$ la desigualdad (1) es verdadera si para i, j con $d \leq i \leq n$ y $o \leq j \leq t$, tenemos:

$$\frac{P(Y \in D_{t+1}(0)|X=0)}{P(Y \in D_j(0)|X=0)} < \frac{\alpha(i,t+1)}{\alpha(i,j)}. (2)$$

Por otra parte, ya que para números reales positivos a_j, b_j las desigualdades $\frac{a_{j+1}}{a_j} < \frac{b_{j+1}}{b_j}$ $(j = 0, ..., t)$ implica $\frac{a_{t+1}}{a_j} < \frac{b_{t+1}}{b_j}$ es suficiente demostrar para $j = t$ para probar (2). Ahora fijamos $i \in \{d, ..., n\}$ y tomamos $c \in F_q^n$

con $d(c,0)=i$. Observe que $\alpha(i,j)=P(Y\in D_j(c)|X=0)$. Así que nos queda demostrar que

$$\frac{P(Y\in D_{t+1}(0)|X=0)}{P(Y\in D_t(0)|X=0)}<\frac{P(Y\in D_{t+1}(c)|X=0)}{P(Y\in D_t(c)|X=0)}. \quad (3)$$

hemos

$$\begin{aligned}\frac{P(Y\in D_{t+1}(0)|X=0)}{P(Y\in D_t(0)|X=0)} &= \frac{\sum_{w\in D_{t+1}(0)}P(Y=w|X=0)}{\sum_{v\in D_t(0)}P(Y=v|X=0)}\\ &= \frac{\binom{n}{t+1}(q-1)^{t+1}(\frac{p}{q-1})^{t+1}(1-p)^{n-t-1}}{\binom{n}{t}(q-1)^{t}(\frac{p}{q-1})^{t}(1-p)^{n-t}}\\ &= \frac{(n-t)p}{(t+1)(1-p)}\end{aligned}$$

y

$$\frac{P(Y\in D_{t+1}(c)|X=0)}{P(Y\in D_t(c)|X=0)}=\frac{\sum_{w\in D_{t+1}(0)}P(Y=c+w|X=0)}{\sum_{v\in D_t(0)}P(Y=c+v|X=0)}.$$

Para terminar la prueba que establece que

$$\Gamma=\{(w,v)|w\in D_{t+1}(0),v\in D_t(0),d(w,v)=1\}$$

entonces

$$(t+1)|D_{t+1}(0)|=|\Gamma|=(n-t)(q-1)|D_t(0)|.$$

Así nuestra última desigualdad (3) puede ser escrita como:

$$\frac{(n-t)P}{(t+1)(1-p)}<\frac{\frac{1}{t+1}\sum_{(w,v)\in\Gamma}P(Y=c+w|X=0)}{\frac{1}{(n-t)(q-1)}\sum_{(w,v)\in\Gamma}P(Y=c+v|X=0)}.$$

Es evidente que para los números enteros positivos a,b,c_i,d_i $(1\leq i\leq m)$, las desigualdades $\frac{a}{b}\leq\frac{c_i}{d_i}$ implica $\frac{a}{b}\leq\frac{\sum_{i=1}^m c_i}{\sum_{i=1}^m d_i}$. Por lo tanto es suficiente para demostrar que

$$\frac{p}{(q-1)(1-p)}\leq\frac{P(Y=c+w|X=0)}{P(Y=c+v|X=0)}. \quad (4)$$

Para cada $(w, v \in \Gamma)$, con desigualdad estricta para cada $(w, v) \in \Gamma$. Desde

$$|d(c+v,0) - d(c+w,0)| \leq 1.$$

El lado derecho de (4) puede tomar los valores $\frac{p}{(q-1)(1-p)}$, 1 o $\frac{(q-1)(1-p)}{p}$. Por último se debe tener en cuenta que $\frac{p}{(q-1)(1-p)} < \frac{(q-1)(1-p)}{p}$ y que para $0 \neq c \in C$ siempre encontramos alguna $(w, v) \in \Gamma$ de tal manera que

$$\frac{P(Y = c+w|X=0)}{P(Y = c+v|X=0)} = \frac{(q-1)(1-p)}{p}.$$

Capítulo 5

Anexo

5.1. Probabilidad

En esta sección veremos algunas definiciones y teoremas básicos sobre probabilidad.

5.1.1 Definición. Un experimento determinístico es cualquier experimento que, al repetirse bajo las mismas condiciones, genera siempre los mismos resultados.

Un ejemplo, en física, que es un experimento determinístico es la ley de la gravedad.

5.1.2 Definición. Un experimento aleatorio (o estocástico) es cualquier experimento que, al repetirse bajo las mismas condiciones, no genera siempre los mismos resultados.

Ejemplos familiares de estos experimentos son los juegos de azar, como dados, lanzamiento de monedas o juegos de cartas, entre otros.

5.1.3 Definición. Si se realiza un experimento aleatorio, entonces el conjunto Ω de todos los posibles resultados de ese experimento se denomina espacio muestral de resultados). Cualquier subconjunto del espacio muestral se llama evento. Si un evento tiene un solo elemento se llama evento elemental.

5.1.4 Definición. Sean A y B dos eventos de un espacio muestral Ω. Si los sucesos A y B no tienen en común elementos de Ω, entonces se denominan

mutualmente excluyentes (o disyuntos) y su intersección $A \cap B$ es el conjunto vacío. De esto se deduce que el evento $A \cap B$ no puede ocurrir.

5.1.5 Definición. Sean $\Omega \neq \emptyset$ un espacio muestral y $\pounds$ un conjunto de eventos de Ω. Una función $P : \pounds \longrightarrow \mathbb{R}$ se llama una probabilidad si se cumplen las siguientes propiedades:

1. La probabilidad de cualquier evento debe ser siempre mayor o igual que cero, es decir, $P(A) \geqslant 0$, para todo $A \in \pounds$.

2. La probabilidad del espacio muestral siempre es uno, es decir, $P(\Omega) = 1$.

3. Para cada sucesión de eventos $A_1, A_2, ... \in \pounds$ que son mutualmente excluyentes se cumple que

$$P(\bigcup_{n=1}^{\infty} A_n) = \sum_{n=1}^{\infty} P(A_n).$$

A la tripleta $(\Omega, \pounds, P)$ se le llama espacio de probabilidad.

5.1.6 Observación. La serie que aparece en el numeral 3 de la definición 5.1.5 existe (converge) porque el primer axioma asegura que $P(A_n) \geqslant 0$ y el segundo, que

$$P(\bigcup_{n=1}^{\infty} A_n) \leqslant P(\Omega) = 1.$$

Es decir,

$$\sum_{n=1}^{\infty} P(A_n) = P(\bigcup_{n=1}^{\infty} A_n) \leqslant 1 < \infty.$$

5.1.7 Teorema. Para eventos A, B, C de un espacio muestral $\Omega \neq \emptyset$ se tiene:

1. $P(\emptyset) = 0$

2. Si los eventos A, B y C son mutualmente excluyentes, entonces

$$P(A \cup B \cup C) = P(A) + P(B) + P(C).$$

3. $P(\overline{A}) = 1 - P(A)$, siendo $\overline{A}$ el complemento de A

4. $0 \leqslant P(A) \leqslant 1$

5. $P(A) = P(A \cap B) + P(A \cap \overline{B})$.

6. Teorema de adición para 2 eventos o fórmula de Silvester:

$$P(A \cup B) = P(A) + P(B) - P(A \cap B).$$

Demostración. Ver [2] en la página

5.1.8 Definición. Sean A y B dos eventos de un espacio muestral $\Omega \neq \emptyset$. La probabilidad condicional del evento A dado el evento B, simbolizada por $P(A|B)$, se define como

$$P(A|B) = \frac{P(A \cap B)}{P(B)}, \text{ si } P(B) > 0$$

5.1.9 Definición. Una función $X : \Omega \longrightarrow \mathbb{R}$ del espacio muestral Ω de un experimento aleatorio al conjunto $\mathbb{R}$ de los números reales se llama variable aleatoria si tiene la siguiente propiedad: para cada $x \in \mathbb{R}$, el conjunto

$$\{\omega \in \Omega | X(\omega) \leqslant x\}$$

es un evento de Ω.

5.1.10 Observaciones.

1. Las variables aleatorias se simbolizan generalmente con las letras mayúsculas X, Y y Z. Se utiliza su correspondiente letra minúscula (x, y, z en este caso) para designar sus posibles valores. Así, por ejemplo, si X representa a la regla (variable aleatoria) "número de caras que pueden resultar al lanzar una moneda dos veces", entonces sus valores son $x = 1, 2, 3$.

2. Una variable aleatoria es discreta si y sólo si tiene una cantidad finita o infinita enumerable de valores.

Lista de símbolos

$|G|$ cardinalidad, número de elementos del conjunto G

$\mathrm{wt}(x)$ peso de un codeword, número de símbolos del codeword x distintos de cero

$sop(x)$ soporte de un codeword, conjunto formado por todas las posiciones del codeword x distintas de cero

Bibliografía

[1] A. FALDUM, J. LAFUENTE AND G. OCHOA, W. WILLEMS. *Error probabilities for bounded distance decoding.*

[2] H. LLINÁS *Estadística Descriptiva y distribuciones de probabilidad.* Ediciones Uninorte, 2008.

[3] T. BACICHEVA, I. BOUYUKLEIEV, S. DODUNEKOV AND W. WILLEMS, *Teaching linear codes.* Matematica Balkanika, New Series, Vol 19 (2005), Fasc. 1-2, 3-16.

[4] E.R. BERLEKAMP, *Algebraic coding theory.* Revised 1984 edition, Aegean Park Press, 1984.

[5] I. BOUYUKLIEV, *On the binary projective codes with dimension 6.* Bulgarian Academy of Sciences, Preprint No 1/2004, Sofia, 2004.

[6] I. BOUYUKLIEV, S. BOUYUKLIEVA, T.A. GULLIVER AND P.R.J. ÖSTERG????RD, *Classification of optimal binary self-orthogonal codes.* to appear in AAECC.

[7] A. FALDUM, *Trustworthiness of error-correcting codes.* to appear.

[8] F.-W. FU, T. KLØVE AND V.K.-W. *Wel, On the undetected error probability for binary codes.* IEEE Trans. Inform. Theory 49(2)(2003), 382-390.

[9] T. HELLESETH, T. KLØVE AND V. LEVENSHTEIN, *The Simplex codes and even weight binary codes for error correction.* IEEE Trans. Inform. Theory 50 (2004), 2818-2823.

[10] T. HELLESETH, T. KLØVE AND V. LEVENSHTEIN, *Error-correction capability of binary linear codes and the discrete simplex problem.* Preprint version 2004.

[11] T. KLØVE AND V. KORZHIK, *Error detecting codes: General theory and their application in feedback communication systems.* Kluwer Academic Publishers, 1995.

[12] G. POLTYREV, *Bounds on the decoding error probability of binary linear codes via their spectra.* IEEE trans. Inform. Theory 40(1994), 1284-1292.

[13] W. WILLEMS, *Codierungstheorie. DeGruyter,* Berlin, 1999.