MATEMÁTICA DISCRETA

Segunda parte: Teoría de códigos

Grado en Matemáticas

2020 - 2021

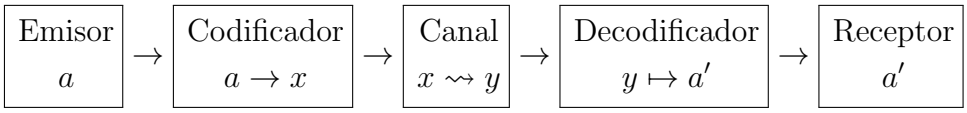
2. BLOQUE II: TEORÍA DE CÓDIGOS

2.1. Tema 4. Codificación de la información. Códigos de repetición y paridad. Distancia de Hamming y capacidad correctora de un código.

Codificación de la información

El esquema general de un proceso de transmisión de información (o datos) es el siguiente, un emisor envía una información a un receptor a través de un canal.

La información enviada debe poder ser transmitida a través del canal. Para ello, debe ser primero codificada en cierto modo. Codificar una determinada información consiste en escribir la información en un alfabeto Σ, es decir mediante un número (finito) de símbolos concretos. El codificador al menos debe hacer que la información generada por el emisor sea susceptible de ser transmitida por el canal. Al transmitir la información en forma codificada (en el lenguaje adecuado) a la salida del canal la información debe decodificarse, para llegar al receptor en su forma original.



Definición 4.1 *Codificar el alfabeto fuente $\mathcal{A} = \{a_1, \ldots, a_m\}$ en el alfabeto código $\Sigma = \{b_1, b_2, \ldots, b_q\}$ es dar una aplicación inyectiva $c : \mathcal{A} \to \mathcal{P}(\Sigma)$. Para cada $a_i \in \mathcal{A}$, $c(a_i)$ es la codificación de a_i y el subconjunto $\mathcal{C} = Im(c)$ es el código empleado. Cada uno de los elementos de $\mathcal{C}$ se denomina palabra código.*

Por simplicidad, puede suponerse que Σ es el alfabeto binario $\{0, 1\}$ y se hablará de codificación binaria. Aunque los términos código y codificación tienen distinto significado, en ocasiones se toman como sinónimos. De esta forma, un código se puede definir como un conjunto finito de palabras en un alfabeto finito.

Definición 4.2 *Se denomina longitud de una palabra del código al número de símbolos que la componen. Si todas las palabras de un código son de la misma longitud n, se dice que el código es un código bloque de longitud n.*

Ejemplo 4.3 *Sea $\mathcal{A} = \{0, 1, 2, \ldots, 9\}$ y $\Sigma = \{0, 1\}$. Dos posibles codificaciones binarias de $\mathcal{A}$ vienen dadas por la tabla siguiente*

Fuente	C_1	C_2
0	0	0101
1	1	1000
2	10	0100
3	11	1100
4	100	0010
5	101	1010
6	110	0110
7	111	0001
8	1000	1001
9	1001	0011

Si $\mathcal{C}$ es un código bloque de longitud n sobre un alfabeto de q símbolos, entonces puede poseer a lo sumo q^n palabras. Por tanto, todo código bloque con m palabras tiene longitud al menos $\lceil log_q(m) \rceil$. De hecho, se puede considerar que de los n símbolos de una palabra, $log_q(m)$ contiene la información y el resto son redundantes.

Definición 4.4 *Dado un código bloque de longitud n con m palabras sobre un alfabeto de q elementos se denomina tasa de transmisión del código a la cantidad*

$$R(\mathcal{C}) = \frac{log_q(m)}{n}.$$

Lógicamente $0 < R(\mathcal{C}) \leq 1$.

En la práctica, los canales por los que se transmite la información pueden sufrir interferencias o perturbaciones (ruido) que producen que los mensajes recibidos no sean iguales que los mensajes que se emitieron. Los códigos correctores de errores tratan de codificar la información de forma que sean capaces de detectar o corregir estas modificaciones (errores).

Definición 4.5 *Sea $x = (x_1, x_2, \ldots, x_n)$ una palabra de un código $\mathcal{C}$ que se transmite por el canal y sea $y = (y_1, y_2, \ldots, y_n)$ la palabra recibida. Se dice que se ha cometido un error en la posición j si $x_j \neq y_j$.*

La noción de detectar un error es clara, se dice que un código $\mathcal{C}$ detecta errores si al transmitir una palabra del código a través de un canal con ruido de forma que se produce algún error, la palabra recibida no pertenece al código. Lógicamente, puede ocurrir que se produzcan una serie de errores de forma que la palabra recibida sea también una palabra del código.

Códigos de repetición y paridad.

Una de las ideas más simple para detectar errores en una transmisión es repetir cada símbolo n veces, o repetir cada secuencia de k símbolos n veces. Si los símbolos fuente son $0, 1$, se pueden codificar de la forma siguiente:

0	$\mapsto$	$(0000\cdots00)$ (n veces)
1	$\mapsto$	$(1111\cdots11)$ (n veces)

obteniendo un código bloque binario de longitud n llamado código de repetición de tamaño n.

Suponiendo que en la transmisión se han producido errores, recibida una palabra, basta con contar el número de 0 y 1 que contiene la palabra recibida y decidir, por un simple criterio de mayoría, su decodificación como la palabra emitida más probable. Esto solo es posible sin ambigüedades si n es impar. Aunque en el modelo presentado se ha definido un código de repetición 1 a n, se puede generalizar a uno del tipo k a kn repitiendo n veces la secuencia de longitud k.

Con esta estrategia se pueden detectar hasta $n-1$ errores, es decir uno menos que la longitud de repetición. Para corregir estos errores producidos en la transmisión, suponiendo que la probabilidad de error no es muy grande, entonces es lógico pensar que la palabra enviada ha sido la que coincide con la recibida en más posiciones. Por ejemplo, con $n = 7$, si se recibe $y = 1000100$ es más lógico pensar que se ha deseado enviar la palabra $x = 0000000$, cometiéndose dos errores, que suponer que la palabra enviada es $x = 1111111$ donde se hubieran cometido 5 errores. De esta forma se puede decir que el código corrige hasta $\lfloor (n-1)/2 \rfloor$ errores. Esta idea es la que después se generalizará para la decodificación por minima distancia.

Sin embargo es evidente que con el código de repetición, la cantidad de información que se transmite es pequeña, es decir, la tasa de transmisión es $1/n$. Para cada bit de información es necesario emitir n bits.

Un buen código será aquel que permita corregir la mayor cantidad posible de errores introduciendo la menor cantidad de símbolos redundantes. Como se ha comprobado con los códigos de repetición, estos dos requerimientos en general se contraponen y se debe buscar un equilibrio entre ambos.

Otro ejemplo simple de codificación son los códigos de paridad. Sea, por ejemplo, un alfabeto fuente de ocho símbolos (las secuencias binarias de 3

bits), la codificación de la fuente se realiza del modo siguiente:

000	0000
001	0011
010	0101
011	0110
100	1001
101	1010
110	1100
111	1111

A cada palabra de tres bits se le añade otro bit al final de forma que se obtiene una secuencia de 4 bits, tal que el número de unos en la palabra sea par. Se puede generalizar el proceso anterior para codificar una fuente de 2^n simbolos con un código bloque de longitud $n+1$.

Es un código bloque de longitud 4 y tasa de transmisión 3/4 (en el caso general $n/(n+1)$). A diferencia del código de repetición, la tasa de transmisión es alta. No obstante este tipo de códigos presentan el inconveniente de que son incapaces de corregir errores aunque si detectar alguno. Si se recibe la palabra 0010, es claro que se ha producido algún error en la transmisión pues ésta no pertenece al código. Sin embargo, aun suponiendo que la probabilidad de error es pequeña, no es posible decidir que palabra se quería realmente enviar. Cualquiera de las palabras $0000, 0011, 0110$ ó 1010 son susceptibles de haber sido enviadas y que en la transmisión se ha cometido únicamente un error. Además, el código presentado no detecta dos errores; si se ha querido enviar 0110 pero se han cometido errores en el primer y último bit, se recibe 1111 que es una palabra del código y el receptor puede pensar que la transmisión ha sido correcta.

No obstante el código de paridad es capaz de corregir la palabra recibida sabiendo que se ha cometido un único error y en que posición se ha cometido. Basta con comprobar la cantidad de unos que hay en el resto de posiciones y obtener la palabra emitida poniendo un 0 en la posición errónea si el número de unos es par y 0 en caso contrario. Este tipo de errores en los que se conoce la posición se denominan borrones por la semejanza que existe con el hecho de recibir una palabra con un "hueco" vacío justo donde se ha cometido el error.

A pesar de la simplicidad del código de paridad, ya que solo es capaz de detectar un error y corregirlo si se conoce la posición, es un código utlizado frecuentemente en la práctica. Por ejemplo el DNI español es un código de paridad. La letra correspondiente a cada número se calcula dividiendo el

número por 23 y dependiendo del resto se le añade una letra según la tabla siguiente.

Resto	Letra	Resto	Letra	Resto	Letra	Resto	Letra	Resto	Letra
0	T	5	M	10	X	15	S	20	C
1	R	6	Y	11	B	16	Q	21	K
2	W	7	F	12	N	17	V	22	E
3	A	8	P	13	J	18	H		
4	G	9	D	14	Z	19	L		

Otros ejemplos de códigos de paridad son: el ISBN donde el último dígito se calcula a partir de la división del resto del número entre 11 (añadiendo el valor X si el resto es 10), los códigos de barras, el número de los cheques bancarios, el número de las tarjetas de crédito, etc.

Distancia de Hamming y capacidad correctora de un código.

La característica principal que permite, en los códigos de repetición, la corrección de errores, es que las palabras que lo forman son lo más distintas posible, con lo que resulta improbable que las alteraciones del canal transformen una en otra. Esta idea de tomar las palabras lo más diferentes posibles es de hecho la base de todos los códigos correctores.

Una forma muy adecuada de medir la separación entre palabras es la distancia de Hamming, introducida por Richard W. Hamming (1915-1998), matemático estadounidense que hizo importantes contribuciones a la informática y a la teoría de códigos.

Definición 4.6 *Sean* $x, y \in \mathbb{F}_q^n$, $x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n)$. *Se llama distancia de Hamming entre* x *e* y *a la cantidad*

$$d(x, y) = \sharp\{i \mid 1 \leq i \leq n,\, x_i \neq y_i\}.$$

La aplicación así definida es efectivamente una distancia en $\mathbb{F}_q^n$, es decir, verifica las propiedades siguientes:

i.) d es no negativa y $d(x, y) = 0$ si y solo si $x = y$.

ii.) $d(x, y) = d(y, x)$.

iii.) $d(x, z) \leq d(x, y) + d(y, z)$.

A partir de la distancia de Hamming se puede definir la distancia mínima de un código.

Definición 4.7 *Dado un código bloque $\mathcal{C}$ se llama distancia mínima del código a*

$$d = d(\mathcal{C}) = min\{d(x, y) \,|\, x, y \in \mathcal{C},\, x \neq y\}.$$

La idea básica es decodificar una palabra utilizando esta distancia. Emitida una palabra $c \in \mathcal{C}$ y recibida y se decodificará usando el criterio de mínima distancia, esto es, decodificaremos y por la palabra de $\mathcal{C}$ más parecida a y (según la distancia de Hamming). De este modo, se supone que el error producido durante la transmisión no ha sido grande.

La decodificación por mínima distancia no siempre es efectiva. El procedimiento falla cuando la palabra más cercana no es única. En cualquier otro caso proporciona una (no necesariamente correcta) decodificación de y. A partir de la distancia mínima es posible determinar la capacidad de un código para detectar y corregir un número determinado de errores.

Teorema 4.8 *Sea $\mathcal{C}$ un código bloque de distancia mínima d. Entonces*

- *$\mathcal{C}$ detecta s errores si y solo si $s < d$.*
- *$\mathcal{C}$ corrige t errores si y solo si $2t < d$.*

Dem.: Sea $\mathbf{c} \in \mathcal{C}$ al palabra enviada, $\mathbf{y}$ la palabra recibida.

- Si $\mathbf{y}$ tiene s errores, $0 < s < d$, entonces $d(\mathbf{c}, \mathbf{y}) = s$ y $\mathbf{y} \notin \mathcal{C}$, pues cualquier palabra de $\mathcal{C}$ está a distancia al menos d de $\mathbf{c}$.
- Si $\mathbf{y}$ tiene t errores, $2t < d$, entonces $d(\mathbf{y}, \mathbf{c}) < d(\mathbf{y}, \mathbf{x}) \forall \mathbf{x} \in \mathcal{C}$. En efecto, las bolas con centro en dos palabras del código y radio $(d-1)/2$ son disjuntas (si no, las palabars estarían a distancia menor que d). Por lo tanto, si $2t < d$, es decir $t < d/2$, entonces $\mathbf{y}$ estará en una y solo una de tales bolas, que tendrá por centro la palabra código más cercana. □

El entero $t := \lfloor \frac{d-1}{2} \rfloor$ se llama **capacidad correctora del código**.

Los códigos de repetición y de paridad vistos anteriormente tienen distancia mínima n y 2 respectivamente. Por tanto, el código de repetición detecta $n-1$ errores y corrige $\lfloor n/2 \rfloor$ errores mientras que el código de paridad detecta 1 error pero no lo corrige.

En cierta forma, la decodificación de un código bloque puede entenderse como una aplicación $d : H \to \mathcal{C}$, donde $H \subseteq \Sigma^n$. Es decir, de todas las palabras que se pueden recibir (Σ^n), existe un subcojunto H tal que éstas son las que se pueden decodificar sin ambiguedad. Si $H = \Sigma^n$, se dice que la decodificación es completa; cualquier palabra de Σ^n se decodifica en una palabra código. En caso contrario la decodificación es incompleta. La decodificación por mínima distancia es, en general incompleta, pues pueden existir palabras $y \in \Sigma^n$ de forma que la distancia mínima de ellas al código se alcanza en más de una palabra del código.

Para cada código bloque existen tres parámetros involucrados en la codificación y decodificación:

- n: la longitud del código,
- M: el número de palabras del código,
- d: la distancia mínima (o en su defecto $t := \lfloor \frac{d-1}{2} \rfloor$, la capacidad correctora del código).

Estos tres parámetros no pueden escogerse arbitrariamente sino que guardan una estrecha relación entre si. Teniendo en cuenta la decodificación por mínima distancia es posible demostrar el siguiente resultado.

Teorema 4.9 (Cota de Hamming) *Sea $\mathcal{C}$ un código bloque de longitud n sobre un alfabeto de q elementos y capacidad correctora t. Si M es el número de palabras del código, entonces:*

$$q^n \geq M\left(1 + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \ldots + \binom{n}{t}(q-1)^t\right).$$

Los códigos para los que se alcanza la igualdad en la cota anterior se denominan **códigos perfectos**.

Dadas dos palabras c_1 y c_2 de un código bloque de longitud n y distancia mínima d, las primeras $n - d + 1$ componentes de ambos no van a coincidir, ya que si las primeras $n - d + 1$ componentes de c_1 y c_2 fuesen las mismas, entonces aunque las restantes $n - (n - d + 1) = d - 1$ componentes fueran distintas, se tendría que $d(c_1, c_2) = d - 1$, lo que es contradictorio. Por lo tanto, el número de palabras del código no puede exceder de q^{n-d+1}.

Teorema 4.10 (Cota de Singleton) *Sea $\mathcal{C}$ un código bloque de longitud n sobre un alfabeto de q elementos y distancia mínima d. Si M es el número de palabras del código, entonces:*

$$M \leq q^{n-d+1}.$$

Los códigos de bloque para los que se alcanza la igualdad en la cota de Singleton se llaman **MDS (máxima distancia de separación)**.

Para finalizar el tema se hará mención brevemente al problema fundamental de la teoría de códigos, es decir el cálculo de

$$A(n,d) = max\{M \mid \text{existe un código de parámetros } n, M, d\},$$

determinando que para códigos binarios

$$\frac{2^n}{\sum_{i=0}^{d-1}\binom{n}{i}} \leq A(n,d) \leq \frac{2^n}{\sum_{i=0}^{t}\binom{n}{i}}$$

2.2. Tema 5. Códigos lineales, matriz generadora y matriz de control. Decodificación por síndrome. Códigos de Hamming, Golay y Reed-Muller

Códigos lineales, matriz generadora y matriz de control

Los procesos de codificación y decodificación de los códigos en bloque son computacionalmente costosos y exigen almacenar en memoria una cantidad considerable de información (todas las palabras del código). Usando las herramientas del álgebra lineal es posible mejorar estos procesos.

Definición 5.1 *Sea $\mathbb{F}_q$ un cuerpo finito de q elementos, un código $\mathcal{C}$ se dice lineal si es un subespacio vectorial de $\mathbb{F}_q^n$.*

Todo código lineal es un código bloque de longitud n dada por el espacio vectorial ambiente. Como espacio vectorial, $\mathcal{C}$ posee una dimensión k, luego su cardinal es siempre una potencia de q, q^k.

Definición 5.2 *Un subconjunto $\mathcal{C} \subseteq \mathbb{F}_q^n$ es un $[n,k,d]$ - código lineal si $\mathcal{C}$ es un subespacio vectorial de dimensión k de $\mathbb{F}_q^n$ y la distancia mínima es d.*

La tasa de transmisión de información de un $[n,k,d]$ - código lineal es

$$R(\mathcal{C}) = \frac{k}{n}\,.$$

Al igual que se define la distancia de Hamming de dos elementos de $\mathbb{F}_q^n$, se puede definir el peso de una palabra que ayuda a determinar la distancia mínima del código únicamente a partir de las palabras del código y no de los pares de palabras.

Definición 5.3 *Sea $x \in F_q^n$, el peso de $x = (x_1, \ldots, x_n)$ se define como*

$$w(x) = \sharp\{i \,|\, x_i \neq 0\}.$$

Proposición 5.4 *Sea $\mathcal{C}$ un código lineal, la distancia mínima del código coincide con el mínimo de los pesos de las palabras no nulas del código, es decir,*

$$d(\mathcal{C}) = \text{mín}\{w(x) \,|\, x \in \mathcal{C} - \{(0, 0, \ldots, 0)\}\}.$$

Todo subespacio vectorial de $\mathbb{F}_q^n$ de dimensión k puede ser interpretado como la imagen de una (no única) aplicación lineal inyectiva $f : \mathbb{F}_q^k \to \mathbb{F}_q^n$. Puede entenderse esta aplicación f como la codificación de la fuente $\mathbb{F}_q^k$.

Definición 5.5 *Dado un código lineal $\mathcal{C}$ de longitud n y dimensión k, se denomina matriz generadora del código a la matriz G de una aplicación inyectiva $f : \mathbb{F}_q^k \to \mathcal{C} \subseteq \mathbb{F}_q^n$. Dicho de otro modo, G es una matriz de tamaño $k \times n$ cuyas filas son una base de $\mathcal{C}$.*

Una matriz generadora G proporciona no solo un código sino una codificación de la fuente ya que $\mathcal{C} = \{xG \,|\, x \in \mathbb{F}_q^k\}$ (los vectores se escriben en fila y el producto del vector x por la matriz G es xG), un mensaje $x \in \mathbb{F}_q^k$ se codifica por $xG \in \mathbb{F}_q^n$. De esta forma, la codificación de la fuente en códigos lineales es muy simple y solo requiere el almacenamiento en memoria de la matriz G.

La matriz generadora describe $\mathcal{C}$ mediante unas ecuaciones paramétricas. Pero hay otra forma habitual de describir un subespacio vectorial de $\mathbb{F}_q^n$, definirlo como el conjunto de soluciones de un sistema lineal homogéneo. En otras palabras, proporcionando las ecuaciones implícitas del subespacio $\mathcal{C}$.

Definición 5.6 *Sea $\mathcal{C}$ un $[n, k, d]$-código lineal, se dice que una matriz de tamaño $(n - k) \times n$ y rango $n - k$ es una matriz de control de $\mathcal{C}$ si*

$$x = (x_1, \ldots, x_n) \in \mathcal{C} \Leftrightarrow Hx^t = (0, \ldots, 0)^t.$$

Las matrices generadoras y de control de un código están estrechamente relacionadas.

Proposición 5.7 *Si G y H son las matrices generadora y de control de un código lineal $\mathcal{C}$, entonces $GH^t = 0$.*

La distancia mínima (peso mínimo) no es el mínimo peso de los vectores de una base (matriz generadora), pero se puede calcular a partir de una matriz de control.

Teorema 5.8 *Si H es una matriz de control del código lineal $\mathcal{C}$, entonces la distancia mínima de $\mathcal{C}$ es d, si y solo si, d es el mayor entero para el que $d-1$ columnas cualesquiera de H son linealmente independientes.*

Dem.: Sean $c_i, 1 \leq i \leq n$, las columnas de H.
Si existen r columnas linealmente dependientes, entonces $\alpha_1 c_1 + \alpha_2 c_2 + \ldots + \alpha_n c_n = 0$, para ciertos escalares, donde $\alpha_i = 0$ para $(n-r)$ subíndices i, pero no todos los r α_i restantes valen cero. Entonces $H(\alpha_1\, \alpha_2 \ldots \alpha_n)^t = 0$, es decir $(\alpha_1\, \alpha_2 \ldots \alpha_n)^t \in \mathcal{C}$ y tiene peso $\leq r$. Luego $d \leq r$.

Por otro lado, si cualesquiera r columnas de H son linealmente independientes, entonces ningún vector de peso $\leq r$ puede pertenecer a $\mathcal{C}$, lo que implica $d > r$. $\square$

Corolario 5.9 *Si $\mathcal{C}$ es un código lineal sobre F_2 y las columnas de H son todas distintas y no nulas, la distancia mínima es al menos* 3.

Como una base de $\mathcal{C}$ no es única, tampoco lo es la matriz generadora. Sin embargo, todas las matrices generadoras de $\mathcal{C}$ son semejantes (dadas G_1, G_2 matrices generadoras del mismo código $\mathcal{C}$, existe una matriz inversible P tal que $G_1 = PG_2$). La matriz de control tampoco es única.

Definición 5.10 *Se dice que dos códigos son equivalentes si uno se puede obtener del otro mediante alguna permutación de las coordenadas en $\mathbb{F}_q^n$.*

Definición 5.11 *Se dice que una matriz generadora, G, está en forma estándar si es de la forma $G = (I_k|A)$, donde I_k denota la matriz identidad de tamaño $k \times k$.*

Si se dispone de una matriz generadora en forma estándar, la operación de codificación asociada es

$$x = (x_1, x_2, \ldots, x_k) \rightarrow xG = (\overbrace{x_1, x_2, \ldots, x_k}^{mensaje}, \overbrace{x_{k+1}, \ldots, x_n}^{control})$$

Los k primeros términos de la palabra código corresponden al mensaje de la fuente y los $n-k$ últimos son símbolos de control. En el caso de que la matriz generadora esté en forma estándar, es muy sencillo calcular una matriz de control.

Teorema 5.12 *Sea $\mathcal{C}$ un $[n,k,d]$-código lineal. La matriz $G = (I_k|A)$ es una matriz generadora de $\mathcal{C}$ si y solo si la matriz $H = (-A^t|I_{n-k})$ es una matriz de control.*

Dado un código lineal, no siempre es posible obtener una matriz generadora en forma estándar, pero siempre existe un código equivalente con esta característica.

Teorema 5.13 *Todo código lineal $\mathcal{C}$ es equivalente a un código $\mathcal{C}'$ que admite una matriz generadora en forma estándar.*

Dem.: [Munuera y Tena, pág. 69-70] Si $\dim \mathcal{C} = k$, una matriz generadora G de $\mathcal{C}$ es $k \times n$ y de rango k. Entonces posee k columnas independientes. Mediante una permutación σ de $\{1, 2, \ldots, n\}$ se puede conseguir que estas columnas sean las k primeras. Así se obtiene una matriz $G' = (A|B)$ con A $k \times k$ y regular, que genera un código $\mathcal{C}'$ equivalente a $\mathcal{C}$. Mediante operaciones elementales con filas puede trasformarse A en I_k. Haciendo estas mismas operaciones con la matriz G' completa se obtiene una matriz $(I_k|B')$ cuyas filas generan el mismo subespacio $\mathcal{C}'$ que G'. $\square$

Como ya se ha comentado, el problema fundamental de la teoría de códigos está relacionado con la existencia de códigos con parámetros fijados. El álgebra lineal también determina otras cotas sobre los parámetros del código. En códigos lineales binarios es posible refinar la cota inferior para $A(n, d)$ obteniendo la cota de Gilbert-Varshamov:

$$A(n, d) \geq \frac{2^{n-1}}{\sum_{i=0}^{d-2} \binom{n-1}{i}}.$$

Existen otro tipo de cotas que relacionan los parámetros de un código, como las siguientes. Las demostraciones de estos resultados se pueden ver en el capítulo 8 del libro de C. Munuera y J. Tena, *Codificación de la Información.*

Teorema 5.14 (Cota de Plotkin) *Sea $\mathcal{C}$ un código lineal $[n, k, d]$ sobre un alfabeto de q elementos. Entonces:*

$$d \leq \frac{nq^{k-1}(q-1)}{q^k - 1}.$$

Esta cota expresa que la distancia mínima de un código es menor o igual al peso promedio de todas sus palabras no nulas.

La cota de Plotkin implica

$$n/d \geq \frac{q^k - 1}{q^{k-1}(q-1)} = \frac{q}{(q-1)} \left(1 - \frac{1}{q^k}\right) \xrightarrow[k \to \infty]{} \frac{q}{(q-1)}.$$

Teorema 5.15 (Cota de Griesmer) *Para todo código lineal de parámetros $[n, k, d]$ sobre un alfabeto de q elementos se verifica que*

$$n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{q^i} \rceil.$$

Decodificación por síndrome.

Debido a la estructura de los códigos lineales es posible realizar la decodificación por mínima distancia de manera más simple.

Sea $\mathcal{C}$ un $[n, k, d]$ código lineal. Transmitida una palabra código $x \in \mathcal{C}$ a través del canal, sea y la palabra recibida. Si $y = x + e$, el vector $e = (e_1, \ldots, e_n)$ representa los errores cometidos y claramente

$$w(e) = \sharp\{ \text{ errores cometidos } \} = d(x, y).$$

La cuestión es cómo decodificar y, es decir, cómo asociar a y una palabra código que tenga el mayor parecido posible con x.

Definición 5.16 *Sea $\mathcal{C}$ un código lineal con matriz de control H y sea $y \in \mathbb{F}_q^n$. Se llama síndrome de y al vector $s(y) = Hy^t \in \mathbb{F}_q^{n-k}$.*

Por definición de la matriz de control, $x \in \mathcal{C}$ si y solo si $s(x) = 0$. Además por ser el síndrome una aplicación lineal $s(y) = s(x+e) = s(x)+s(e) = s(e)$, es decir, recibida una palabra y se conoce el síndrome del error cometido.

Proposición 5.17 *El síndrome del vector recibido y es una combinación lineal de las columnas de H correspondientes a las posiciones en las que se ha cometido un error.*

Ejemplo 5.18 *Sea $\mathcal{C}$ un código que corrige al menos un error y durante la transmisión solo se ha cometido un único error, $w(e) = 1$, es decir $e = (0, \ldots, 0, e_i, 0 \ldots, 0)$. Por ser $d \geq 3$, cualesquiera dos columnas de H son linealmente independientes. Así, el síndrome del vector recibido, y, será múltiplo de una y solo una columna de H. Esa posición es precisamente la posición donde se ha cometido el error, $s(y) = e_i h_i$, de donde se puede deducir el error cometido y el mensaje enviado $x = y - e$.*

Decodificar por mínima distancia quiere decir que recibido y, se decodificará por $y - e \in \mathcal{C}$ si $d(y, y - e) < d(y, y - e')$ para cualquier otra palabra código $y - e' \in \mathcal{C}$. Equivalentemente, el error e es el elemento de $\mathbb{F}_q^n$ de menor peso entre los que satisfacen $s(e) = s(y)$.

Definición 5.19 *Para cada $b \in \mathbb{F}_q^{n-k}$, el elemento de peso mínimo de $s^{-1}(b)$ se denomina error patrón de $s^{-1}(b)$.*

En general, no hay un único elemento con esta condición.

Teorema 5.20 *Sea $t = \lfloor (d-1)/2 \rfloor$ la capacidad correctora del código $\mathcal{C}$. Si en $s^{-1}(b)$ existe un vector e de peso menor o igual que t, entonces dicho vector es el único con esa condición y es, por tanto, el error patrón del conjunto $s^{-1}(b)$.*

Algoritmo 5.21 *Decodificación por síndrome.*

Recibida la palabra $y \in \mathbb{F}_q^n$.

i.) Sea $b = s(y) = Hy^t$ su síndrome.

ii.) Si b no tiene error patrón, no es posible decodificar de forma única.

iii.) Si β_b es el error patrón, se decodifica y por $y - \beta_b$.

El algoritmo anterior corrige t errores. El cálculo de los errores patrón asociados a posibles síndromes, se hace habitualmente de una vez para todas y se almacena en una tabla. De hecho, a partir de la identificación $s^{-1}(b) = \beta_b + \mathcal{C}$, esta tabla se puede ir construyendo tomando e, con $w(e) \leq t$ como error patrón de la clase $s^{-1}(s(e))$.

Códigos de Hamming, Golay y Reed-Muller.

Los siguientes ejemplos muestran algunos código lineales básicos en los que existe un algoritmo de decodificación eficiente.

Fijado un entero positivo r, sea $\mathbb{F}_q^r$ el espacio vectorial de dimensión r. Para cada vector no nulo $h \in \mathbb{F}_q^r$, se denota por $[h]$ el conjunto de los $q-1$ vectores no nulos de F_q^r proporcionales a h. Entonces, existen $h_1, h_2, \ldots, h_n \in \mathbb{F}_q^r - \{0\}$ tales que $\mathbb{F}_q^r - \{0\}$ es unión disjunta de $[h1], \ldots, [h_n]$, siendo $n = (q^r - 1)/(q-1)$.

Definición 5.22 *El r-ésimo código de Hamming sobre F_q es el código lineal, $\mathcal{H}(r)$ cuya matriz de control es $H = (h_1^t, \ldots, h_n^t)$.*

Es evidente que el código $\mathcal{H}(r)$ tiene longitud $n = (q^r - 1)/(q-1)$, dimensión $n - r$ y, si $r \geq 2$, distancia mínima 3. En particular si $q = 2$, $\mathcal{H}(r)$ es un $[2^r - 1, 2^r - r - 1, 3]$ código lineal.

Para $q = 2$, una matriz de control del código de Hamming $\mathcal{H}(r)$ se puede construir tomando como columnas todos los vectores no nulos de $\mathbb{F}_2^r$, por ejemplo, para $r = 3$.

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

Nótese que la matriz de control anterior no está escrita en forma estándar pero esta escritura es más eficiente para la decodificación.

Como la distancia mínima de $\mathcal{H}(r)$ es 3, los códigos de Hamming corrigen 1 error. Si y es la palabra recibida e $y \in \mathcal{C}$, entonces no ha sido alterada en la transmisión. Si ha ocurrido un único error, este ha tenido lugar en la posición que ocupa $s(y)$ en la matriz de control H. Por la disposición de las columnas de H, como representación binaria de los enteros $1, 2, \ldots, 2^r - 1$, basta escribir $s(y)$ en notación decimal y alterar el bit de y correspondiente a esa posición.

Los códigos de Hamming $\mathcal{H}(r)$ son perfectos, como se puede comprobar de forma directa.

Códigos duales. Códigos de Golay

Antes de presentar el código de Golay es necesario introducir los códigos duales.

Definición 5.23 *Sea $\mathcal{C} \subseteq \mathbb{F}_q^n$ un $[n, k, d]$ código lineal. Se llama código dual del código $\mathcal{C}$, al código $\mathcal{C}^\perp$ definido por*

$$\mathcal{C}^\perp = \{x \in \mathbb{F}_q^n \mid x \cdot c = 0, \, \forall c \in \mathcal{C}\},$$

dónde $(x_1, \ldots, x_n) \cdot (c_1, \ldots, c_n) = x_1 c_1 + \ldots + x_n c_n$.

De las definiciones es evidente que si G (resp. H) es una matriz generadora (resp. de control) de $\mathcal{C}$ entonces H es una matriz generadora de $\mathcal{C}^\perp$ y G es una matriz de control de $\mathcal{C}^\perp$. Así pues $\mathcal{C}^\perp$ es un código de longitud n y dimensión $n - k$.

Definición 5.24 *Se dice que un código $\mathcal{C}$ es autodual si $\mathcal{C}^\perp = \mathcal{C}$.*

Si $\mathcal{C}$ es autodual entonces $n = 2k$ y una matriz generadora G es, al mismo tiempo, una matriz de control y se pueden considerar síndromes respecto a ambas matrices.

Sea $\mathcal{C}$ un $[2k, k, d]$ código autodual con matriz generadora $G = (I_k|B)$ y $d \geq 7$ (corrige al menos 3 errorres). El siguiente algoritmo es un método para decodificar palabras en las que se han cometido a lo sumo 3 errores, f^i denota la i-ésima fila de la matriz B, c^i su columna i-ésima y u_i denota el vector i-ésimo de la base canónica de $\mathbb{F}_q^k$.

Algoritmo 5.25 *Decodificación en códigos autoduales binarios.*

Recibida la palabra $y \in \mathbb{F}_2^k$.

i.) Sea $s_1 = s_G(y) = (I_k|B)y^t$. Si $w(s_1) \leq 3$ entonces el error es $e = (s_1^t, 0)$.

ii.) Sea $s_2 = s_H(y) = (B^t|I_k)y^t$. Si $w(s_2) \leq 3$ entonces el error es $e = (0, s_2^t)$.

iii.) Para cada $i = 1, \ldots, k$ si $w(s_2 + f^i) \leq 3$ entonces el error cometido es $e = (u_i, s_2^t + f^i)$.

iv.) Para cada $i = 1, \ldots, k$ si $w(s_1 + c^i) \leq 3$ entonces el error cometido es $e = ((s_1 + c^i)^t, u_i)$.

En todos los casos anteriores, y se decodifica como $y + e$.

Definición 5.26 *El código de Golay extendido, G_{24}, es el código binario de matriz generadora $G = (I_{12}|B)$, siendo B la matriz 12×12:*

$$B = \left(\begin{array}{cccccccccccc|c} 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ \hline 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{array}\right)$$

La matriz B anterior puede escribirse de la forma

$$\begin{pmatrix} A_1 & 1^t \\ 1 & 0 \end{pmatrix}$$

donde la matriz A_1 se puede formar tomando el vector (11011100010) y desplazando cíclicamente una coordenada a la izquierda. El código G_{24} tiene 2^{12} palabras y longitud 24. Además es un código autodual de distancia mínima 8. Si se omite la última coordenada de la matriz G anterior se obtiene el denominado código de Golay G_{23} que es un $[23, 12, 7]$ código lineal que es perfecto, es decir cualquier palabra recibida está a distancia mínima de una única palabra del código.

El algoritmo de decodificación del código de Golay consiste en añadir, si es necesario, un símbolo extra a la palabra recibida y decodificar la palabra resultante mediante el algoritmo descrito para códigos autoduales.

Recibida la palabra $y \in F_2^{23}$, si $y \in G_{23}$ la palabra no ha sufrido alteraciones. En otro caso, se toma $y' = (y, \epsilon) \in \mathbb{F}_2^{24}$ con $\epsilon = 0$ si $w(y)$ es impar y $\epsilon = 1$ si $w(y)$ es par. Se aplica entonces el algoritmo para el código autodual G_{24} obteniendo $\tilde{y} \in G_{24}$. Eliminando la última coordenada se obtiene la decodificación de la palabra recibida.

Si se hubiera utilizado un tablero de síndromes se tendrían que haber calculado $2048 = 2^{11}$ de ellos. Utilizando el hecho de que G_{24} es autodual se reducen considerablemente los cálculos.

Códigos de Reed-Muller

Los códigos de Reed-Muller binarios de primer orden constituyen una familia de códigos, $\mathcal{RM}(m)$ $(m \geq 1)$ cuya característica principal es que tienen una alta capacidad correctora. El código $\mathcal{RM}(5)$ fue el utilizado por el programa Mariner de la NASA.

Para $m \geq 0$ se define de forma recursiva la matriz $G(m)$:

$$G(0) = (1) \qquad G(m) = \begin{pmatrix} G(m-1) & G(m-1) \\ 0 \ldots 0 & 1 \ldots 1 \end{pmatrix}$$

La matriz $G(m)$ puede escribirse también de la forma siguiente. Es una matriz de tamaño $(m+1) \times 2^m$ cuya columna i-ésima es $(1, g_{i-1})^t$ donde g_i es la escritura binaria invertida del número i. Por ejemplo, para $m = 3$, la matriz es

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

Definición 5.27 *Para $m \geq 1$, el m-ésimo código de Reed-Muller de primer orden es el código lineal sobre $\mathbb{F}_2$ que tiene a $G(m)$ como matriz generadora.*

Los parámetros del código $\mathcal{RM}(m)$ son

- $\mathcal{RM}(m)$ tiene longitud 2^m.
- $\mathcal{RM}(m)$ tiene dimensión $m+1$.
- La distancia mínima de $\mathcal{RM}(m)$ es 2^{m-1} luego su capacidad correctora es $2^{m-2}-1$.

El método de decodificación utilizado para los códigos de Reed-Muller es radicalmente distinto de los métodos basados en tableros de síndromes. Sea $a = (a_0, \ldots, a_m) \in \mathbb{F}_2^{m+1}$ el mensaje en el alfabeto fuente. La palabra código correspondiente a dicho mensaje es $x = (x_0, \ldots, x_{n-1}) = aG(m)$. Si al transmitir x se recibe la palabra $y = (y_0, \ldots, y_{n-1})$, el siguiente algoritmo, de mayoría lógica, decodifica obteniendo no la palabra del código x sino el mensaje fuente.

Algoritmo 5.28 *Decodificación de códigos Reed-Muller.*

Sea $y = (y_0, \ldots, y_{n-1})$ la palabra recibida.

i.) Para cada $i = m, \ldots, 1$, sea el conjunto

$$A_i = \{y[k2^i + \alpha] + y[k2^i + 2^{i-1} + \alpha] \,|\, 0 \leq \alpha < 2^{i-1}, 0 \leq k < 2^{m-i}\}$$

ii.) Sea b_i el símbolo más frecuente del conjunto A_i.

iii.) $y' = (y'_0, \ldots, y'_{n-1}) = y - (0, b_1, \ldots, b_m)G(m)$ y b_0 el símbolo mas frecuente en el vector y'.

iv.) El mensaje decodificado es $b = (b_0, \ldots b_m)$.

La salida del algoritmo es directamente el mensaje original y no la palabra código por lo que importa poco que la matriz generadora no está en forma estándar. El método descrito permite corregir, al menos, tantos errores como la capacidad correctora del código, aunque a veces puede corregir más.

4. Bibliografía

Muchos de los tópicos de la asignatura se encuentran en casi cualquier libro de Matematica Discreta. Para el desarrollo de la asignatura se recomiendan los siguientes:

- N. L. Biggs, *Discrete Mathematics.* Oxford University Press. 2002.
- R. P. Grimaldi, *Discrete and combinatorial mathematics, an applied introduction.* Addison-Wesley. 1989.
- C. Munuera, J. Tena, *Codificación de la información.* Serv. Pub. U. de Valladolid. 1997.
- K. H. Rosen, *Discrete mathematics and its applications.* McGraw-Hill. 1999.

Además de la bibliografía ya mencionada, otras referencias utilizadas para la elaboración del proyecto docente son:

- R.B.J. Allenby, A. Slomson, *How to count, an introduction to Combinatorics.* CRC Press. 1991.
- M. Bóna, *A walk through combinatorics. An Introduction to Enumeration and Graph Theory.* World Scientific. 2006.
- P. Fernandez-Gallardo, J.L. Fernández Pérez. *Notas de Matemática Discreta.* Disponible en www.uam.es/pablo.fernandez. 2008.
- J. Gimbert, R. Moreno, J.M. Ribó, M. Valls, *Apropament a la teoria de grafs i als seus algorismes.* U. de LLeida. 1998.
- F. Harary, *Graph Theory.* Addison-Wesley. 1969.
- J. Matousek, J. Nesetril, *Invitation to Discrete Mathematics.* Clarendon Press, Oxford. 1998.