LECCIONES

de

Elementos de Algebra. Aplicaciones

por

María Jesús Iranzo Aznar

y

Francisco Pérez Monasor

Curso 2004-2005

Departamento de Algebra.

Facultad de Matemáticas. Universitat de València

Programa

Introducción a la Teoría de Códigos.

Una de las áreas de aplicación más actuales del álgebra es la teoría de códigos. Siempre que se transmite una información (por ejemplo vía satélite) o se almacena (por ejemplo en un disco óptico), el receptor deberá poder corregir los errores producidos por posibles interferencias, ruidos etc. Cuando la información se representa en forma digital, el uso de los códigos correctores de errores hace posible corregir tales errores. Aunque la importancia del álgebra, y en particular de los cuerpos finitos, no fué tan manifiesta en los comienzos de esta teoría, en los últimos años ha impactado con gran fuerza en su desarrollo.

La teoría de códigos surge con la llegada de los ordenadores, cuya fiabilidad era baja comparada con la de los actuales. Mientras R.W. Hamming trabajaba para los laboratorios Bell, pensó que si una máquina era capaz de detectar errores, sería posible para la máquina corregirlos. Hamming diseñó una forma de codificar información tal que, si un error se detectaba, podía ser corregido. Basado en parte en su trabajo, C. Shannon desarrolló la estructura teórica para la ciencia de la teoría de códigos.

Existe otro aspecto en el mundo de la comunicación relacionado con el anterior, que es más antiguo y que trata de la creación y descodificación de mensajes secretos : la criptología. Etimológicamente criptología significa escritura secreta. Actualmente tiene el significado de ciencia de la comunicación segura. Su objetivo es que dos partes puedan intercambiar información, sin que una tercera no autorizada la descifre. Esto se realiza mediante sistemas cifrados o criptosistemas. La criptografía es la ciencia de diseñar criptosistemas . El criptoanálisis trata de romper los criptosistemas para así apoderarse de la información cifrada.

Las lecciones que vamos a exponer constituyen una introducción a la teoría de códigos y se han desarrollado en la asignatura optativa **Elementos de Algebra. Aplicaciones.** durante los cursos 2000-01 al 2007-08.

Lección 1. Primeros conceptos.

Supongamos que deseamos transmitir un mensaje y que en el proceso de la transmisión dicho mensaje puede alterarse. El problema es asegurar que el mensaje sea recibido correctamente. Para ello se codificará dicho mensaje, de forma que las palabras resultantes sean muy diferentes, así, aunque haya alteraciones, la palabra recibida se parecerá más a la enviada que a cualquier otra. El receptor del mensaje tiene la lista de las posibles palabras del código y puede comparar la recibida para encontrar la más similar y descodificar. El proceso es por tanto el siguiente:

i) Sale un mensaje, ii) se codifica, iii) atraviesa un canal, iv) se descodifica, v) llega el mensaje al usuario.

Por ejemplo suponer que los mensajes a enviar son: sí o no y que se envía el mensaje sí. Se codifica sí=00000 y no=11111. Sale el mensaje codificado y atraviesa un canal que lo altera y aparece 01001. se descodifica como 00000 y el mensaje que llega al usuario es sí.

(1.1) **Definición**. Sea F un conjunto de símbolos, llamado el alfabeto ($|F| = q > 1$) y sea n un entero positivo. Una palabra de longitud n sobre F es una n-tupla de símbolos de F. Escribiremos $a_1a_2...a_n$ en lugar de $(a_1, a_2, \ldots, a_n)$. Un código de longitud n es un subconjunto C de F^n con $|C| \geq 1$. Sus elementos se llaman palabras código. En el ejemplo anterior $F = \{0, 1\}$ y $C = \{00000, 11111\}$. Este es un código binario. En general si $|F| = q$ se dice que el código es q-ario.

Ejemplos.

i) El código de Polivio (208 a.C.). Se considera el alfabeto griego S que tiene 24 letras. Se utiliza el conjunto $A = \{1, 2, 3, 4, 5\}$ y a cada letra griega se le asocia el correspondiente elemento del conjunto $C = \{11, 12, 13, 14, 15, 21, 22, 23, 24, 25, ..., 54\}$, de forma que C es un código de tamaño 24 y longitud 2. Este código persigue claridad y facilidad de transmisión de mensajes, pero no permite detectar ni corregir errores.

ii) El código Morse. Se usa para transmisiones telegráficas. Sirve para codificar un mensaje fuente en el lenguaje usual. Aquí $S = \{a, b, c, ..., z\}$ y $A = \{., -, \}$,es decir se usan tres símbolos: punto, raya y espacio. A las letras que aparecen más frecuentemente se les asocia las sucesiones más sencillas de símbolos, por ejemplo: ., -, .-.No es un código

de longitud fija. Los espacios se usan para separar palabras (6 espacios) o letras entre palabras (3 espacios). Este código no permite corregir y/o detectar errores y no tiene fines criptográficos.

iii) Código ASCII(American Standard Code for Information Interchange). Usa palabras de 7 bits. Aquí $C = \{0000000, 0000001, ..., 1111111\}$, su tamaño es 128. Se usa para representar caracteres alfanuméricos y caracteres especiales en los ordenadores. Al código ASCII se le añade un bit de paridad para que el número de 1 de la palabra resultante sea par. Este nuevo código se dice código ASCII con control de paridad. Este código permite detectar un error.

iv) Suponer que A debe llegar a encontrarse con B y ambos disponen de un mismo mapa, pero solo B sabe el camino a seguir.Suponer que B tiene que transmitir NNWWNWWW. Los cuatro mensajes son: N,S,E,W. Se pueden codificar en palabras código binarias. El código de menor tamaño a usar sería $C_1 = \{00, 01, 10, 11\}$ con $N = 00$,$W = 01$,$E = 10$,$S = 11$, identificando así los cuatro mensajes con los cuatro elementos de F^2, $F = \{0, 1\}$. Considerar el código binario de longitud 3 $C_2 = \{000, 011, 101, 110\}$. Notar que si se produce un error en una palabra código, se detectará y el receptor puede solicitar una nueva transmisión. Puede suceder que B no tenga la posibilidad de una nueva transmisión, es decir que sea un canal de transmisión en una sola dirección. Se trata pues no solo de detectar el error sino de poder corregirlo. Por adecuadas adiciones de dos dígitos posteriores a cada palabra de C_2, tendríamos el nuevo código $C_3 = \{00000, 01101, 10110, 11011\}$, que es un código binario de longitud 5. Si un único error aparece en cualquier palabra del código C_3, somos capaces no solo de detectarlo sino también de corregirlo, puesto que la palabra recibida será más cercana a la transmitida que a cualquier otra. Esto puede hacerse más preciso introduciendo la llamada **distancia de Hamming**.

(1.2) **Definición**. Sean v,w palabras de longitud n. La distancia de Hamming $d(v, w)$ es el número de coordenadas en que difieren v y w.

(1.3) **Proposición**.i) $d(v, w) = 0 \iff v = w$. ii) $d(v, w) = d(w, v)$. iii) $d(v, w) + d(w, z) \geq d(v, z)$.

Dem. Para probar la última afirmación basta considerar que la distancia de Hamming es el menor número de cambios necesarios para convertir una palabra en otra.

Consideremos de nuevo el código C_3. Notar que la distancia mínima entre dos palabras código distintas es 3. Este es un código que permite corregir un error, ya que si aparece una palabra en la que se ha producido un error, no hay dos palabras del código con distancia ≤ 1 con dicha palabra. Sin embargo si se producen dos errores , por ejemplo se recibe 10001, entonces no se sabe si la enviada es 11011 o 00000. Ahora bien, dicho código puede detectar dos errores, ya que si una palabra difiere en dos coordenadas de una palabra código, no puede pertenecer a este por lo comentado al principio.

Un parámetro asociado a un código C, que da una idea de lo bueno que es el código para corregir errores es la **distancia mínima**, denotada por $d(C)$ y que se define como la menor distancia entre dos palabras código distintas entre sí. Así $d(C_1) = 1$, $d(C_2) = 2$, $d(C_3) = 3$.

(1.4) **Definición**. Sea e un entero positivo. El código C se dice que corrige hasta e errores (C es un código e**-corrector**) si se cumple que para cualquier palabra w existe a lo más una palabra código $c \in C$ que satisface $d(w, c) \leq e$.

(1.5) **Teorema**. i)Un código C puede detectar hasta e errores en cualquier palabra si $d(C) \geq e + 1$. ii) Un código C puede corregir hasta e errores en cualquier palabra si y solo si $d(C) \geq 2e + 1$.

Dem. i) Suponer $d(C) \geq e + 1$ y que se transmite una palabra código c y se producen e errores o menos. Entonces la palabra recibida no puede ser palabra código y por tanto se detecta como errónea. ii) Suponer que $d = d(C) \geq 2e + 1$. Si existe una palabra w de forma que existen $c_1, c_2 \in C$, $c_1 \neq c_2$ con $d(c_1, w) \leq e$ y $d(c_2, w) \leq e$, entonces $d(c_1, c_2) \leq 2e$, lo que es una contradicción, así C corrige hasta e errores. Recíprocamente, suponer que C corrige hasta e errores. Si $d \leq 2e$, considerar la parte entera f de $d/2$. Entonces $f \leq d/2 \leq e$. Además $d - f \leq e$, ya que si d es par $f = d/2$ y si d es impar $d - f = 2f + 1 - f = f + 1 = (d + 1)/2 \leq e$ pues $d + 1 \leq 2e$. Sean c_1, c_2 palabras código tales que $d(c_1, c_2) = d$ y sea w la palabra obtenida cambiando f coordenadas de c_1 de las d en que difieren c_1 y c_2, hasta que coincidan con sus correspondientes en c_2, así $d(c_1, w) = f \leq e$ y $d(c_2, w) = d - f \leq e$ y C no corregiría e errores.

Se suele emplear la notación (n, M, d)-código para indicar que es un código de longitud n, con M palabras código y distancia mínima d. Así en los ejemplos anteriores C_1 es un

(2,4,1)-código, C_2 es un (3,4,2)-código y C_3 es un (5,4,3)-código.

Códigos equivalentes.

(1.6) **Definición**. Dos códigos q-arios son equivalentes si uno puede ser obtenido del otro por una combinación de operaciones de los tipos siguientes: a) permutación de las posiciones del código, b) permutación de los símbolos que aparecen en una posición fijada.

Notar que si se escribe el código como una $M \times n$-matriz cuyas filas son las palabras código, las operaciones del tipo a) corresponden a permutaciones de sus columnas y las operaciones del tipo b) corresponden a un re-etiquetado de los símbolos de una columna dada.

Ejemplo. El código ternario $C = \{012, 120, 201\}$ es equivalente al ternario con repetición de longitud 3: $\{000, 111, 222\}$. Basta aplicar a los símbolos de la segunda posición la permutación (0,2,1) y a los símbolos de la tercera posición la permutación (0,1,2).

Claramente las distancias entre las palabras código no se alteran al pasar de un código a otro equivalente y por tanto dos códigos equivalentes tienen los mismos parámetros: (n, M, d) y corregirán el mismo número de errores.

Un buen (n, M, d)-código tiene n pequeña (para hacer más rápida la transmisión), M grande (para permitir transmitir una variedad amplia de mensajes) y d grande (para poder corregir varios errores). Lo que a menudo se conoce como principal problema en la teoría de códigos es optimizar uno de los parámetros para valores dados de los otros dos. Concretamente , encontrar el mayor tamaño de un código de longitud y distancia mínima dadas. Se denota por $A_q(n, d) = \max\{M | \exists (n, M, d)\text{-código } q\text{-ario}\}$.

(1.7) **Teorema**. i) $A_q(n, 1) = q^n$. ii) $A_q(n, n) = q$.

Dem. i) El mayor $(n, M, 1)$-código q-ario es F^n. ii) Si dos palabras cualesquiera del código deben diferir en todas sus coordenadas, no podemos tener más de q palabras en dicho código. Ahora bien, el código q-ario con repetición de longitud n es un (n, q, n)-código, así $A_q(n, n) = q$.

(1.8) **Lema**. Cualquier (n, M, d)-código q-ario sobre un alfabeto $F = \{0, 1, ..., q-1\}$ es equivalente a un (n, M, d)-código que contiene la palabra 00...0.

Dem. Elegir cualquier palabra código $x_1x_2...x_n$ y para cada $x_i \neq 0$ aplicar a los

símbolos en la posición i de las palabras código, la permutación $(0, x_i)$.

Notar que no es decisivo en la demostración el haber considerado la palabra 00...0.

Pasamos a continuación a probar que si $A_2(5,3) = 4$. Además existe, salvo equivalencia, un único $(5,4,3)$-código binario .

Sabemos que C_3 es un $(5,4,3)$-código binario, luego $A_2(5,3) \geq 4$. Sea C un $(5,M,3)$-código binario con $M \geq 4$. Por el lema anterior podemos suponer que $0 = 00...0 \in C$. C tiene a lo más una palabra con 4 ó 5 unos, ya que en otro caso existirían dos palabras código x e y con $d(x,y) \leq 2$, lo que es contradictorio pues $d(C) = 3$. Como $0 \in C$ no pueden existir palabras código con 1 ó 2 unos exactamente y como $M \geq 4$, al menos habrá dos palabras código con exactamente 3 unos. Reordenando las posiciones, si es necesario, podemos suponer que en C están las palabras $00000, 11100, 00111$. Notar que 11111 no puede estar pues $d(C) = 3$. Tampoco pueden existir otras palabras código con exactamente tres unos. Como $M \geq 4$, existirá una con cuatro unos que será 11011. Se concluye así que $A_2(5,3) = 4$ y que, salvo equivalencia, existe un único $(5,4,3)$-código binario.

Continuando con el caso binario, si $x, y \in F^n$, siendo F cuerpo isomorfo a $\mathbf{Z/2Z}$, se define, como es usual, $x + y = (x_1 + y_1)...(x_n + y_n)$ y $x \bigcap y = (x_1.y_1)(x_2.y_2)...(x_n.y_n)$.

(1.9) **Definición**. Se llama **peso de** x y se escribe $w(x)$ al número de unos de la palabra x. Es claro que si x e y son dos palabras $d(x,y) = w(x+y)$. Es sencillo probar:

(1.10) **Lema**. Si x e y pertenecen a F^n entonces $d(x,y) = w(x) + w(y) - 2w(x \bigcap y)$.

Dem. $d(x,y) = w(x+y) =$ número de unos en $x+$ el número de unos en y -2(número de posiciones en que a la vez x e y tienen un uno)$= w(x) + w(y) - 2w(x \bigcap y)$.

(1.11) **Teorema**. Sea d impar. Entonces existe un (n,M,d)-código binario si y solo si existe un $(n+1, M, d+1)$-código binario.

Dem. Suponer que existe un (n,M,d)-código binario. Sea $\tilde{C}$ el código de longitud $n+1$ que se obtiene extendiendo cada palabra $x = x_1x_2...x_n$ a $\tilde{x} = x_1x_2...x_n0$ si $w(x)$ es par ó $x_1x_2...x_n1$ si $w(x)$ es impar. Como el peso de las palabras extendidas es par, $d(\tilde{x}, \tilde{y})$ es par cualesquiera que sean $\tilde{x}, \tilde{y}$. Así $d(\tilde{C})$ es par. Suponer que $d(x,y) = d$ impar. Por el lema anterior, la paridad de $w(x)$ y $w(y)$ es distinta. Así $d(\tilde{x}, \tilde{y}) = d+1$ luego $d \leq d(\tilde{C}) \leq d+1$ y como $d(\tilde{C})$ es par, debe coincidir con $d+1$. Así $\tilde{C}$ es un $(n+1, M, d+1)$-código.

Recíprocamente, suponer que D es un $(n+1, M.d+1)$-código con d impar. Elijamos

$x, y \in D$ tales que $d(x, y) = d + 1$. Elegir una posición en que x e y difieran y borrar las coordenadas en esta posición de todas las palabras de D. El resultado es un (n, M, d)-código.

(1.12) **Corolario**. Si d es impar entonces $A_2(n+1, d+1) = A_2(n, d)$. Equivalentemente , si d es par entonces $A_2(n-1, d-1) = A_2(n, d)$.

Volviendo al caso general q-ario, finalizaremos esta lección de primeros conceptos con dos desigualdades que relacionan el tamaño de un código con su distancia mínima.

(1.13) **Teorema**. Sea C un código de longitud n sobre un alfabeto de q símbolos, con distancia mínima d.

a) (**Cota de Hamming**). Si $d \geq 2e + 1$ entonces :

$$|C| \leq q^n / \sum_{i=0}^{e} \binom{n}{i} (q-1)^i$$

b) (**Cota de Singleton**):

$$|C| \leq q^{n-d+1}$$

.

Dem. a) Sea c una palabra código. Contemos las palabras w tales que $d(c, w) \leq e$. ¿Cuántas palabras satisfacen $d(c, w) = i$, $i \leq e$?. Debemos hacer i errores eligiendo i coordenadas para cambiar (en $\binom{n}{i}$ formas) y cambiando la entrada en cada una de las coordenadas a un símbolo diferente del de c ($q - 1$ posibilidades para cada una de las i coordenadas). Así el número de palabras w con $d(c, w) \leq e$ es :

$$\sum_{i=0}^{e} \binom{n}{i} (q-1)^i$$

Podemos considerar estas palabras formando una esfera de radio e y con centro en la palabra código c. Si hacemos esto para todas las palabras del código observamos que no hay solapamiento entre las esferas, dado que el código es por hipótesis e-corrector, así que no existen palabras que puedan estar a distancia $\leq e$ de dos palabras código distintas. Por tanto:

$$|C| \sum_{i=0}^{e} \binom{n}{i} (q-1)^i \leq q^n$$

de donde se deduce a).

b) Miremos las palabras código c_1 y c_2, $c_1 \neq c_2$, observando sus primeras $n-d+1$ coordenadas. Las partes que vemos son diferentes, ya que si las primeras $n-d+1$ coordenadas de c_1 y c_2 son las mismas, entonces deberían diferir en las restantes $n-(n-d+1) = d-1$ coordenadas y se seguiría que $d(c_1, c_2) \leq d-1$, lo que es contradictorio. Así el número de palabras del código no excede de q^{n-d+1}.

Los códigos que alcanzan estas cotas tienen una importancia especial, llamándose **perfectos** si alcanzan la cota de Hamming y **MDS-códigos** si alcanzan la de Singleton. Cuando introduzcamos códigos lineales, justificaremos la notación MDS (maximum-distance separable).

El código con repetición de longitud n sobre F, que consiste de las palabras $aa...a$ con $a \in F$ es un MDS-código trivial. Este código tiene q palabras (una para cada símbolo) y la distancia mínima es n . Se alcanza la cota de Singleton ya que $q^{n-d+1} = q^{n-n+1} = q$.

Notar que si C es perfecto, F^n queda recubierto por esferas disjuntas de un radio dado, cuyos centros son las palabras código, es decir que aparece una partición de F^n. Considerar el código binario con repetición de longitud 4 : $C = \{0000, 1111\}$, en este caso $d = 4 \geq 2.1 + 1$, es decir es un código 1-corrector.Considerar las esferas con centro las palabras del código y radio 1. Así tenemos la de centro 0000 que está formada por dicha palabra y $1000, 0100, 0010, 0001$ y la esfera de centro 1111 y radio 1 formada por dicha palabra y $0111, , 1011, 1101, 1110$. es claro que la unión de tales esferas no es $(\mathbf{Z}/\mathbf{2Z})^4$ (por ejemplo 1100 no pertenece a ninguna de ellas). Así no alcanza la cota de Hamming. Sin embargo un código binario con repetición con n impar sí que alcanza la cota de Hamming, ya que si $n = 2e+1$ y $w \in (\mathbf{Z}/\mathbf{2Z})^n$, w puede tener un número de unos menor ó igual que e y por tanto está en la esfera de centro 00...0 o bien tiene un número de unos mayor ó igual que $e+1$, en cuyo caso el número de ceros es menor ó igual que $n-e-1 = e$, luego está en la esfera de centro 11..1. Este código se dice que es un código perfecto trivial.

(1.14) **Definición**. Sea C un (n, M)-código q-ario. Se define la **tasa de información** (o de transmisión) de C como $R = (1/n) \log_q M$.

Esta definición trata de dar la relación que hay entre los símbolos del código dedicados a la información y los dedicados a la redundancia.

Ejemplo. Sea $C = \{00, 01, 10, 11\}$ entones $R = (1/2)\log_2 4 = 1$. Si se añade el bit de paridad pasamos a $\tilde{C} = \{000, 011, 101, 110\}$ y $\tilde{R} = (1/3)\log_2 4 = 2/3$. La tasa de información ha disminuido. Dada la tasa , no podemos determinar si el código permite detectar y/o corregir errores. La tasa mide la eficiencia del código. Los códigos más eficientes son los de tasa igual a 1.

Comentarios finales.

a) El código que se utiliza para generar la letra del NIF, se realiza en la siguiente forma. se toma el DNI y se calcula el resto al dividirlo por 23. La letra viene dada por la sucesión:

$$TRWAGMYFPDXBNJZSQVHLCKE$$

asociando la letra correspondiente, en el orden dado, a los diferentes restos:

0,1,2,...,22.

b) En los viajes por el espacio se usaron códigos para enviar las imágenes tomadas. El Mariner 9 (1979) tomó fotos en blanco y negro de Marte. Las imágenes eran de 600x600 y con 64 niveles de gris. Se usó un código binario de tamaño 64, concretamente un (32,64,16)-código (**código de Reed-Muller**). este es un código 7-corrector y $R = (1/32)\log_2 64 = 6/32 = 3/16$.

El Voyager (1979-81) tomó fotos en color de Júpiter y Saturno de 4096 colores. Se usó un (24,4096,8)-código (**código de Golay)**. Es un código 3-corrector y $R = (1/24)\log_2 4096 = 12/24 = 1/2$.

Estudiaremos estos códigos en lecciones posteriores.

Ejercicios.

1. Demostrar que un (n, q, n)-código q-ario es equivalente a un código con repetición.

2. Demostrar que un $(3, M, 2)$-código 3-ario debe tener $M \leq 9$.

3. Construir, si es posible, un $(n.M.d)$-código binario con los parámetros:

$(6, 2, 6), (3, 8, 1), (4, 8, 2), (5, 3, 4), (8, 30, 3)$.

4. Razonar que $\{(a, b, a + b)|a, b \in F\}$, donde F es un cuerpo con q elementos, es un $(3, q^2, 2)$-código q-ario.

5. Demostrar que si existe un (n, M, d)-código binario con d par, entonces existe un (n, M, d)-código binario en el que todas las palabras son de peso par.

6. Probar que el número de códigos binarios no equivalentes , de longitud n con exactamente dos palabras es n.

7. Probar que si existe un código ternario 2-corrector perfecto de longitud n, entonces $2n^2 + 1$ debe de ser potencia de 3.

8. Demostrar que cualquier $(q + 1, M, 3)$-código q-ario satisface $M \leq q^{q-1}$.

9. Demostrar que un código perfecto tiene distancia mínima impar.

10. Demostrar que $A_2(8, 5) = 4$.

11. Sea C un $(n, q^{n-3}, 3)$-código q-ario. Probar que $n \leq q^2 + q + 1$.

12. Razonar que no existe un $(6, 9, 3)$-código binario.

Lección 2. Códigos y diseños.

(2.1) **Definición**. Un diseño es un par (V, B) donde $V = \{v_1, ..., v_n\}$ es un conjunto finito a cuyos elementos se les llama **variedades** ó puntos y $B = \{B_1, ..., B_m\}$ formado por subconjuntos de V, que se dicen **bloques**.

El nombre de variedades para los elementos de V, es debido a la utilización de diseños en los experimentos realizados en la agricultura. Por ejemplo para observar el efecto que producen diferentes variedades de fertilizantes aplicadas a distintos terrenos.

(2.2) **Definición**. Sean (V, B) un diseño , k y r números naturales. Se dice que (V, B) es una **configuración táctica** si se verifican las condiciones siguientes:

a) $|B_i| = k$ para cualquier B_i de B.

b) para cada $v_i \in V$ se tiene que $|\{B_j \in B | v_i \in B_j| = r$.

Notar que si (V, B) es una configuración táctica, se tiene: $nr = mk$. En efecto, contemos los elementos de $\{(v_i, B_j)|v_i \in B_j\}$. Por una parte como cada bloque tiene k elementos y hay m bloques , dicho conjunto tendrá mk elementos. Por otra parte cada variedad pertenece a r bloques y hay n variedades. Así $nr = mk$.

Asociada a una configuración táctica tenemos una $n \times m$-matriz llamada **matriz de incidencia** A. Si A=(a_{ij}) $a_{ij} = 1$ si $v_i \in B_j$ y $a_{ij} = 0$ si $v_i \notin B_j$. Es claro que el número de unos de cada fila es r y el número de unos de cada columna es k.

Ejemplo. Sea $V = \{1, 2, 3, 4\}$, y $B_1 = \{1, 3, 4\}$, $B_2 = \{2, 3, 4\}$, $B_3 = \{1, 2, 4\}$ y $B_4 = \{1.2, 3\}$. La matriz de incidencia asociada es :

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

Una clase especial de configuraciones es la de las configuraciones **simétricas**. En ellas el número de variedades coincide con el de bloques y como consecuencia también $r = k$. El ejemplo anterior es de una configuración simétrica.

Un tipo de configuraciones que nos va a resultar de interés especial es el de las configuraciones BBD (balanced block design), a las que nos referiremos como (m, n, r, k, λ)-diseños, que son configuraciones tácticas con $n \geq k \geq 2$ y cada par $v_i, v_j \in V$,$v_i \neq v_j$,

pertenece a exactamente λ bloques. Si además es simétrico diremos que es un (n, k, λ)-diseño.

Ejemplo. Sea $V = \{1, 2, 3, 4, 5, 6, 7\}$ y $B_1 = \{1, 2, 4\}$, $B_2 = \{2, 3, 5\}$, $B_3 = \{3, 4, 6\}$, $B_4 = \{4, 5, 7\}$,$B_5 = \{1, 5, 6\}$,$B_6 = \{2, 6, 7\}$, $B_7 = \{7, 1, 3\}$. (V, B) es un $(7, 7, 3, 3, 1)$-diseño. Además tiene una representación geometríca muy interesante. Representando las variedades por puntos y los bloques por rectas y un círculo, aparece la representación del **plano proyectivo de Fano**.

Además de la relación anteriormente obtenida, para los parámetros de una configuración táctica, para un BBD se obtiene también:

$$r(k-1) = \lambda(n-1)$$

En efecto, fijada una variedad v_i, el número de pares ordenados (v_j, B_l) tales que $v_i \neq v_j$ y $\{v_i, v_j\} \subseteq B_l$ es , por una parte , $\lambda(n-1)$. Ahora bien , v_i pertenece a r bloques y en cada uno de ellos hay $k-1$ variedades distintas de v_i. Así dicho número es también igual a $r(k-1)$. De ahí la igualdad.

Si A es la matriz de incidencia de un BBD, el producto de una fila consigo misma es igual a r y el de dos filas distintas entre sí es igual a λ. Por lo tanto se tiene:

$$AA' = \begin{pmatrix} r & \lambda & \dots & \lambda \\ \lambda & r & \dots & \lambda \\ \vdots & \ddots & \ddots & \vdots \\ \lambda & \lambda & \dots & r \end{pmatrix}$$

cuyo determinante es:

$$\det \begin{pmatrix} r+\lambda(n-1) & \lambda & \dots & \lambda \\ r+\lambda(n-1) & r & \dots & \lambda \\ \vdots & \ddots & \ddots & \vdots \\ r+\lambda(n-1) & \lambda & \dots & r \end{pmatrix} =$$

$$(\mathrm{r}+\lambda(n-1))\det \begin{pmatrix} 1 & \lambda & \dots & \lambda \\ 1 & r & \dots & \lambda \\ \vdots & \ddots & \ddots & \vdots \\ 1 & \lambda & \dots & r \end{pmatrix} = (r+\lambda(n-1))\det \begin{pmatrix} 1 & \lambda & \dots & \lambda \\ 0 & r-\lambda & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & r-\lambda \end{pmatrix} =$$

$$(\mathrm{r}+\lambda(n-1))(r-\lambda)^{n-1}$$

Así si $n = k$ se sigue $r = \lambda$ y rang$AA' = 1$. Si $k < n$ entonces $r \neq \lambda$ y $\det(AA') \neq 0$, así se tiene: $n =$rang$AA' \leq$rang$A \leq$mín(n, m) luego $n \leq m$ (conocida como **desigualdad de Fisher**) y como $nr = mk$ se deduce $r \geq k$.

Sea A la matriz de incidencia del $(7, 7, 3, 3, 1)$- diseño estudiado antes. Sea B la 7×7-matriz obtenida reemplazando en la A los ceros por los unos y los unos por los ceros. Sea C el código binario formado por las filas de A , las filas de B y las palabras $0 = 0000000$ y $1 = 1111111$. Veamos que $d(C) = 3$.

Sabemos que cada fila de A tiene exactamente tres unos y que dos filas distintas tienen exactamente un uno en común. De ahí que:

$$d(a_i, a_j) = 3 + 3 - 2 = 4$$

si $i \neq j$.

Puesto que la distancia entre palabras no se altera cambiando los ceros por los unos y viceversa, tenemos:

$$d(b_i, b_j) = 4$$

si $i \neq j$.

Es claro que $d(0, y) = 3, 4, 7$ si $y = a_i, b_j, 1$, $d(1, y) = 3, 4, 7$ si $y = b_j, a_i, 0$ y $d(a_i, b_i) = 7$ si $i = 1, ..., 7$. Queda por analizar $d(a_i, b_j)$ con $i \neq j$. Pero a_i y b_j difieren en los lugares en que coinciden a_i y a_j así que:

$$d(a_i, b_j) = 7 - d(a_i, a_j) = 3$$

Así $d(C) = 3$ y se tiene:

$$16(\binom{7}{0} + \binom{7}{1}) = 2^4(1 + 7) = 2^7$$

es decir que **C es un código perfecto**.

Este código tiene una propiedad notable: la suma de dos palabras del código es una palabra código. Pertenecerá a un clase importante de códigos: los codigos lineales.

Notar también que la existencia de un $(7, 16, 3)$-código perfecto prueba que $A_2(7, 3) = 16$ y por (1.12) es también $A_2(8, 4) = 16$.

Lección 3. Cuerpos finitos

Para el desarrollo de la Lección 3, necesitamos recordar:

1. Si G es un grupo finito y $g \in G$ entonces i) $o(g) = | < g > |$ ii) $g^{|G|} = 1$.

2. Si $o(g) = n$ entonces $o(g^m) = n/m.c.d(n, m)$.

3. Si G es un grupo cíclico con n elementos, para cada $d|n$ existe un único subgrupo S de G, tal que $|S| = d$.

4. Si $a, b \in G$ con $o(a) = n$ y $o(b) = m$ siendo $m.c.d.(n, m) = 1$ y $ab = ba$ entonces $o(ab) = nm$.

5. Algoritmo de la división en $k[x]$.

Sean $f(x), g(x) \in k[x]$, polinomios no cero. Entonces existen dos únicos polinomios $q(x), r(x) \in k[x]$ tales que $f(x) = g(x)q(x) + r(x)$ con $r(x) = 0$ o grad $r(x) <$ grad $g(x)$.

6. Si k es un cuerpo, $k[x]$ es un D.I.P.

7. Si k es un cuerpo, todo polinomio de grado mayor o igual que 1, se factoriza como producto de polinomios irreducibles (dicha factorización es única salvo orden y multiplicación por constantes no cero.).

8. Si φ es la función de Euler , se tiene:

i) $\varphi(p^n) = p^{n-1}(p-1)$ si $n \geq 1$, p primo.

ii) $\varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2)$ siendo m.c.d.$(n_1, n_2) = 1$.

(3.1) **Lema**. Sea k un cuerpo finito. Entonces:

i) mín $\{n \in N, n \neq 0 | n1_k = 0\}$ es un número primo.

ii) Si p es el primo de i) y F es la intersección de todos los subcuerpos de k (llamado el cuerpo primo de k), entonces $F \cong \mathbf{Z}/p\mathbf{Z}$.

Dem. i) Como k es finito existen $n, m \in \mathbf{N}$ con $n > m$ de forma que $n1_k = m1_k$, luego $(n-m)1_k = 0$. Si mín $\{n \in N, n \neq 0 | n1_k = 0\} = rs$ con $1 \neq r, s$, entonces $0 = (rs)1_k = (r1_k)(s1_k)$ luego $r1_k = 0$ ó $s1_k = 0$ lo que es contradictorio.

ii) Sea p el número primo de la parte i). Si se establece una aplicación $\phi : \mathbf{Z} \to k$ dada por : $\phi(n) = n1_k$, ϕ es un homomorfismo de anillos, Ker$\phi = (p) = p\mathbf{Z}$ y $\mathbf{Z}/p\mathbf{Z} \cong \phi(\mathbf{Z})$ es un subcuerpo de k contenido en F, luego debe coincidir con F.

(3.2) **Definición**. Al primo p de la parte i) del resultado anterior se le llama **característica de** k y se denota car k.

Notar que cualesquiera que sean $a, b \in k$ se tiene: $(a+b)^p = a^p + b^p$. Además $k^p = k$.

(3.3) **Lema**. Si k es un cuerpo finito se tiene que $|k| = (\text{car}k)^n$ para algún $n \in \mathbf{N}$.

Dem. Considerar el cuerpo primo F de k. Sabemos que $|F| = \text{car}k$ y considerando a k como F-espacio vectorial, necesariamente de tipo finito, tenemos la tesis, con $n = \dim_F k$.

(3.4) **Teorema**. Si k es un cuerpo finito, cada $a \in k$ es raíz del polinomio $x^{|k|} - x$.

Dem. La afirmación es claramente cierta para $a = 0$. Si $a \neq 0$ entonces $a \in k^*$ que es un grupo multiplicativo finito de orden $|k| - 1$ luego $a^{|k|-1} = 1$ así : $a^{|k|} = a$.

Pasamos a continuación a demostrar un resultado muy importante sobre la estructura de los subgrupos finitos del grupo multiplicativo de un cuerpo (ver también el ejercicio 8).

(3.5) **Teorema**. Si k es un cuerpo y $S \leq k^*$, S finito, entonces S es cíclico.

Previamente demostraremos :

(3.6) **Lema**. Si G es un grupo finito abeliano, existe $g \in G$ cuyo orden es divisible por los órdenes de todos los elementos de G.

Dem. Sea $a \in G$ con $o(a) = {p_1}^{e_1}...{p_k}^{e_k} = m$, $e_i \geq 0 \ \forall i$ y $b \in G$ con $o(b) = {p_1}^{f_1}...{p_k}^{f_k} = n$, $f_i \geq 0 \ \forall i$. Suponer que después de una reordenación , si es necesaria, se tiene:

$$e_1 \leq f_1, e_2 \leq f_2, ..., e_h \leq f_h$$

$$e_{h+1} \geq f_{h+1}, e_{h+2} \geq f_{h+2}, ..., e_k \geq f_k$$

Si $r = {p_1}^{e_1}...{p_h}^{e_h}$ y $s = {p_{h+1}}^{f_{h+1}}...{p_k}^{f_k}$, entonces m.c.m. $(m.n) = m.n/r.s$, $o(a^r) = {p_{h+1}}^{e_{h+1}}...{p_k}^{e_k} = m/r$ y $o(b^s) = {p_1}^{f_1}...{p_h}^{f_h} = n/s$. Ambos son primos entre sí y como a^r y b^s conmutan se tiene que : $o(a^r b^s) = m.n/r.s = \text{m.c.m.}(m, n)$.

Aplicando este proceso sucesivamente , se puede construir un elemento cuyo orden sea el mínimo común múltiplo de los órdenes de los elementos de G.

Nota. Se puede obtener una demostración más elegante del resultado anterior, utilizando el teorema de estructura de grupos finitos abelianos, que se incluye en el apéndice.

(3.7) **Lema**. Si G es un grupo finito abeliano, G es cíclico si y solo si $|G|$ es el menor entero positivo n tal que $a^n = 1\ \forall a \in G$.

Dem. Si G es cíclico existe $a \in G$ tal que $< a >= G$ y $|G| = o(a) = n$ que es el menor entero positivo tal que $a^n = 1$, y si $x \in G$ entonces $x^n = 1$.

Recíprocamente, suponer que $|G|$ es el menor entero n tal que $a^n = 1\ \forall a \in G$. Sea $g \in G$ cuya existencia afirma el resultado anterior. Entonces $x^{o(g)} = 1\ \forall x \in G$. por tanto $|G| \leq o(g)$. Por otra parte, como $o(g)$ divide a $|G|$ se sigue que $|G| = o(g)$ y $G =< g >$.

Demostración del (3.5) Teorema.

Sea S un subgrupo finito de k^*. Así S es finito y abeliano. Veamos que $|S|$ es el menor n tal que $a^n = 1\ \forall a \in S$. Si m es tal que $a^m = 1\ \forall a \in S$, considerar el polinomio $x^m - 1 \in k[x]$. Dicho polinomio tiene al menos $|S|$ raices luego: $|S| \leq m$. Basta ahora aplicar (3.7) Lema.

(3.8) **Corolario**. Si k es un cuerpo finito entonces k^* es un grupo finito cíclico.

Nota. Si $k^* =< a >$, se dice que a es un **elemento primitivo** de k.

(3.9) **Proposición**. Sea k un cuerpo y $f(x)$ un polinomio irreducible en $k[x]$. Sea $E = k[x]/(f(x))$, entonces E es un cuerpo. Si además k tiene q elementos y el grado de $f(x)$ es n, entonces E tiene q^n elementos.

Dem. E es un anillo conmutativo y con unidad, con las operaciones internas:

$$(g(x) + (f(x))) + (h(x) + (f(x))) = (g(x) + h(x)) + (f(x))$$

$$(g(x) + (f(x))).(h(x) + (f(x))) = g(x).h(x) + (f(x))$$

Además si $g(x) + (f(x)) \neq 0$ se tiene que $g(x) \notin (f(x))$ luego m.c.d. $(g(x), f(x)) = 1$ y por la identidad de Bezout existen polinomios $a(x), b(x) \in k[x]$ tales que: $a(x)g(x) + b(x)f(x) = 1$. Así:

$$(a(x) + (f(x))(g(x) + (f(x))) = 1 + (f(x))$$

y $a(x) + (f(x))$ es el inverso de $g(x) + (f(x))$.

Notar que si grad$f(x) = n$ y consideramos a $k[x]$ como k-espacio vectorial y a $(f(x))$ como subespacio, los elementos $1 + (f(x)), x + (f(x)), ..., x^{n-1} + (f(x))$ constituyen un sistema libre del k-espacio vectorial cociente $k[x]/(f(x))$. Además es sistema generador

ya que dado $h(x) \in k[x]$, por el algoritmo de la división $h(x) = f(x)q(x) + r(x)$ con $r(x) = 0$ ó grad $r(x)$ <grad $f(x)$ y $h(x) + (f(x)) = r(x) + (f(x))$.

Como consecuencia:

$$\dim_k E = n = \text{grad} f(x)$$

y si $|k| = q$ se sigue que $|E| = q^n$.

(3.10) **Corolario**. Sea k un cuerpo y $f(x)$ un polinomio irreducible en $k[x]$, entonces $(f(x))$ es un ideal maximal de $k[x]$.

Dem. Es claro que $(f(x))$ no coincide con $k[x]$. Además si existe I, ideal de $k[x]$, tal que $(f(x)) \subset I \subseteq k[x]$ y $g(x) \in I - (f(x))$, como $g(x) + (f(x))$ es unidad de $k[x]/(f(x))$, existe $h(x) \in k[x]$ tal que $(g(x) + (f(x)))(h(x) + (f(x))) = 1 + (f(x))$, de donde se deduce que $1 \in I$ y por lo tanto $I = k[x]$.

Suponer que $f(x)$ es mónico e irreducible en $k[x]$, de grado n y que a es una raíz de $f(x)$ en un cuerpo K, que contiene a k como subcuerpo (K extensión de k). Podemos definir una aplicación $\varphi : k[x] \longrightarrow k[a]$ mediante $\varphi(g(x)) = g(a)$. Es sencillo probar que es homomorfismo de anillos y que como $(f(x))$ es maximal en $k[x]$ y está contenido en Kerφ, ambos deben de coincidir. Así $k[x]/(f(x)) \cong k[a]$ y podemos describir los elementos del cuerpo $k[x]/(f(x))$ como expresiones polinómicas en a de grado menor estrictamente que n. Notar que $f(x)$ es el único polinomio mónico irreducible en $k[x]$ que tiene a a como raíz, así se le llamará el **polinomio irreducible de a sobre k** (Irr(a, k)).

Ejemplos.

i) Sea $f(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbf{Z}/2\mathbf{Z}[x]$. Dicho polinomio es irreducible pues no tiene raices en $\mathbf{Z}/2\mathbf{Z}$ y los posibles polinomios cuadráticos son : x^2, x^2+1, x^2+x+1 siendo el producto de dos cualesquiera de ellos distinto de $f(x)$. Así $\mathbf{Z}/2\mathbf{Z}[x]/(x^4+x^3+x^2+x+1)$ es un cuerpo de 16 elementos y si a es raíz de dicho polinomio en una extensión de $\mathbf{Z}/2\mathbf{Z}$, dichos elementos son: $0, 1, a, a+1, a^2, a^2+1, a^2+a+1, a^2+a, a^3, a^3+1, a^3+a, a^3+a^2, a^3+a+1, a^3+a^2+1, a^3+a^2+a, a^3+a^2+a+1$. Notar que $a^4 = a^3 + a^2 + a + 1$. así :$a^5 = a^4 + a^3 + a^2 + a = 1$, así que $o(a) = 5$ y a no es un elemento primitivo del cuerpo.

ii) Sea ahora $f(x) = x^4 + x + 1$, que por el mismo razonamiento que en i) se tiene que es irreducible en $\mathbf{Z}/2\mathbf{Z}[x]$ y sea b raíz de $f(x)$ en una extensión de $\mathbf{Z}/2\mathbf{Z}$. El cuerpo $\mathbf{Z}/2\mathbf{Z}[x]/(x^4 + x + 1)$ es también un cuerpo de 16 elementos , así $o(b)|15$, como $b^3 \neq 1$ y

$b^5 \neq 1$ se concluye que $o(b) = 15$ y b es un elemento primitivo del cuerpo. Así $\mathbf{Z}/2\mathbf{Z}[b] = \{o, 1, b, b^2, ..., b^{14}\}$.

El siguiente resultado es fundamental para el desarrollo de esta lección.

(3.11) **Teorema**. Sea $|k| = q$ y $n \in \mathbf{N}$, entonces:

$$x^{q^n} - x = \prod f(x)$$

donde el producto se realiza sobre todos los polinomios mónicos irreducibles $f(x) \in k[x]$ cuyo grado divide a n.

Dem. Suponer que $x^{q^n} - x = h(x)^2 g(x)$ con grad $h(x) \geq 1$, entonces: $-1 = 2h(x)h'(x)g(x) + h(x)^2 g'(x) = h(x)(2h'(x)g(x) + h(x)g'(x))$, que no es posible. Así los factores de $x^{q^n} - x$ son distintos entre sí.

Sea $f(x)$ irreducible en $k[x]$ de grado d. Considerar el cuerpo $E = k[x]/(f(x))$ de orden q^d. Sabemos que : $(x + (f(x))^{q^d} = x + (f(x))$ es decir: $x^{q^d} \equiv x(f(x))$. Por un proceso de inducción se llega a que para cualquier $t \in \mathbf{N}$ se tiene : $x^{q^{td}} = (x^{q^{(t-1)d}})^{q^d} \equiv x^{q^d} \equiv x(f(x))$.

Supongamos que d divide a n. Así existirá t tal que $n = td$ y por tanto $x^{q^n} \equiv x(f(x))$, es decir $f(x)$ será un factor irreducible de $x^{q^n} - x$.

Recíprocamente, suponer que $x^{q^n} \equiv x(f(x))$ y sea $n = td + r$ con $r = 0$ ó $r < d$. Entonces: $x \equiv x^{q^n} = (x^{q^{td}})^{q^r} \equiv x^{q^r}(f(x))$. Por lo tanto, si $g(x) = \sum a_i x^i \in k[x]$, entonces:

$$g(x)^{q^r} = \sum a_i^{q^r} x^{iq^r} \equiv \sum a_i x^i \ (f(x))$$

pues sabemos que como $|k| = q$ se tiene $a_i^q = a_i \ \forall i$. Así cada elemento de E es raíz de $x^{q^r} - x$ y como $|E| = q^d$, debe ser $r = 0$ y d divide a n.

A continuación introducimos la función de Möbius, que nos permitirá demostrar la existencia de cuerpos finitos, de orden cualquier potencia de un número primo.

(3.12) **Definición**. Definimos una aplicación $\mu : \mathbf{N} \to \{-1, 0, 1\} \subseteq \mathbf{Z}$ de la siguiente forma:

$\mu(n) =$

i) (-1)^k si $n = p_1...p_k$, con $p_i \neq p_j$ si $i \neq j$.

ii) 1 si $n = 1$.

iii)0 en otro caso.

A dicha aplicación se le llama **función de Möbius**.

(3.13) **Lema**. Si $n > 1$ entonces:

$$\sum_{d|n} \mu(d) = 0$$

Dem. Si n tiene exactamente s primos distintos en su descomposición en factores primos, se tiene:

$$\sum_{d|n} \mu(d) = \sum_{i=0}^{s} \binom{s}{i} (-1)^i = (1-1)^s = 0$$

(3.14) **Teorema**. (Inversión de Möbius) Sea $f : \mathbf{N} \to \mathbf{C}$ una aplicación. Si $g : \mathbf{N} \to \mathbf{C}$ es una aplicación definida por:

$$g(n) = \sum_{d|n} f(d)$$

entonces:

$$f(n) = \sum_{d|n} \mu(d) g(n/d)$$

Dem.

$$\sum_{d|n} \mu(d) g(n/d) = \sum_{d|n} \mu(d) \sum_{d'|n/d} f(d') = \sum_{dd'|n} \mu(d) f(d') =$$

$$\sum_{d'|n} \sum_{d|n/d'} \mu(d) f(d') = \sum_{d'|n} f(d') \sum_{d|n/d'} \mu(d) = f(n)$$

(3.15) **Definición**. Si $|k| = q$, denotaremos por $\mathbf{N(n, q)}$ el número de los polinomios mónicos irreducibles de grado n en $k[x]$.

(3.16) **Teorema**.

$$N(n, q) = 1/n \sum_{d|n} \mu(d) q^{n/d}$$

Por tanto $N(n, q) \geq (1/n)(q^n - [(q^n - 1)/(q - 1)]) > 0$.

Dem. Por (3.10):

$$q^n = grad(x^{q^n} - x) = \sum_{\text{grad} f(x)|n} \text{grad} f(x) = \sum_{d|n} dN(d,q)$$

Por el teorema anterior tenemos que:

$$N(n,q) = 1/n \sum_{d|n} \mu(d) q^{n/d}$$

El resto de la afirmación se sigue de :

$\sum_{d|n} \mu(d) q^{n/d} \geq q^n - q^{n-1} - q^{n-2} - ... - q - 1 = q^n - [(q^n - 1)/(q-1)] > 0$

Si k es un cuerpo finito, sabemos que su orden es una potencia de un número primo. Si recíprocamente p es un número primo y $n \in \mathbf{N}$, veamos que existe un cuerpo de p^n elementos.

(3.17) **Teorema**. Para cada potencia q de un número primo , existe un cuerpo de q elementos. Además dos cuerpos de q elementos son isomorfos.

Dem. Sea $q = p^n$. Considerar $\mathbf{Z}/p\mathbf{Z}$. Por el Teorema anterior, existe $f(x) \in \mathbf{Z}/p\mathbf{Z}[x]$ mónico irreducible de grado n. Considerar $\mathbf{Z}/p\mathbf{Z}[x]/(f(x))$. Sabemos que es un cuerpo de p^n elementos.

En cuanto a la unicidad, sea F un cuerpo de p^n elementos. Sabemos que los elementos de F son raíces de $x^{p^n} - x \in \mathbf{Z}/p\mathbf{Z}[x]$. Además por (3.10) $f(x)|x^{p^n} - x$. Sea a raíz de $f(x), a \in F$. Definamos una aplicación $\phi : \mathbf{Z}/p\mathbf{Z}[x] \to F$, dada por $\phi(g(x)) = g(a)$. Dicha aplicación es un homomorfismo de anillos y $(f(x)) = Ker(\phi)$. Así $\mathbf{Z}/p\mathbf{Z}[x]/(f(x)) \cong \phi(\mathbf{Z}/p\mathbf{Z}[x]) \subseteq F$. Como $|\mathbf{Z}/p\mathbf{Z}[x]/(f(x))| = p^n = |F|$ se sigue:

$$\mathbf{Z}/p\mathbf{Z}[x]/(f(x)) \cong F$$

El cuerpo de p^n elementos se suele denotar por $GF(p^n)$ en memoria de **E. Galois** que fué su descubridor. En lo sucesivo escribiremos $GF(q)$ para indicar el cuerpo de q elementos , donde q es una potencia de un número primo.

Polinomios irreducibles y elementos conjugados.

Sea $a \in GF(q^m)$ y $GF(q^n)$ el menor subcuerpo de $GF(q^m)$ conteniendo a $GF(q)$ al que pertenece a. Se deduce inmediatamente que el grado de $f(x)$=Irr$(a, GF(q))$ es n, ya que si fuera igual a r, tendríamos el homomorfismo $\varphi : GF(q)[x] \to GF(q)[a]$, dado por $\varphi(g(x)) = g(a)$ con $(f(x)) = Ker(\varphi)$ y $GF(q)[x]/(f(x)) \cong GF(q)[a] \subseteq GF(q^n)$ luego $q^r = q^n$ y $r = n$.

Como $a \in GF(q^n)$, por (3.4) sabemos que $a^{q^n} = a$ y por (3.11) $n|m$. Notar que los elementos: $a, a^q, ..., a^{q^{n-1}}$ son distintos entre sí y son raíces del polinomio $f(x)$. Dichos elementos se dicen **conjugados de** a **respecto de** $GF(q)$ ($GF(q)$-conjugados). Notar que si $a \neq 0$ entonces $a^{q^n-1} = 1$, luego $o(a)|q^n - 1$ y por 2. de los preliminares de esta lección , se sigue que todos los elementos $GF(q)$- conjugados tienen el mismo orden que a.

Ejemplos.

i) Sea a elemento de orden 3 en $GF(16)$. El menor subcuerpo en el se encuentra a es $GF(4)$. Los $GF(2)$-conjugados de a son a, a^2 y Irr$(a, GF(2))$= (x-a)(x-a^2).

ii) Sea a elemento de orden 63 en GF(4^3). El menor subcuerpo en el que se encuentra a es $GF(4^3)$ y los $GF(4)$-conjugados de a son: a, a^4, a^{16}.

iii) Considerar el polinomio $x^3 + x + 1$ que es irreducible en $GF(2)[x]$ y sea $a \in GF(8)$ raíz de dicho polinomio. También son raices a^2 y a^4. Además $a \neq 0$, luego $o(a) = 7$. Notar que $a^4 = a^2 + a$, $a^5 = a^3 + a^2 = a^2 + a + 1$ y a^6 $= a^3 + a^2 + a = a^2 + 1$. Los elementos a^3, a^6, a^5 son $GF(2)$-conjugados y darán origen al polinomio:

$(x - a^3)(x - a^6)(x - a^5) = (x^2 - a^6x - a^3x + a^2)(x - a^5) = x^3 - (a^6 + a^3)x^2 + a^2x - a^5x^2 + a^4x + ax - 1 = x^3 + (a^6 + a^3 + a^5)x^2 + (a^4 + a^2 + a)x + 1 = x^3 + (a^2 + 1 + a + 1 + a^2 + a + 1)x^2 + (a^2 + a + a^2 + a)x + 1 = x^3 + x^2 + 1.$

Como consecuencia obtenemos la factorización en polinomios irreducibles en $GF(2)[x]$ de $x^7 - 1$:

$$x^7 - 1 = (x - 1)(x^3 + x + 1)(x^3 + x^2 + 1)$$

El código ISBN.

Cada libro tiene un International Standard Book Number (ISBN). Es una palabra con 10 dígitos, que se distribuyen en cuatro bloques, el primero asignado al país (idioma), el segundo a la editorial, el tercero está formado por los dígitos que la editorial asigna al libro y finalmente los diez dígitos $x_1x_2...x_{10}$ deben satisfacer:

$$\sum_{i=1}^{10} ix_i \equiv 0(11)$$

así:

$$x_1 + 2x_2 + 3x_3 + ... + (11-1)x_{10} \equiv 0(11)$$

, es decir:

$$x_1 + 2x_2 + 3x_3 + ... + 11x_{10} \equiv x_{10}(11)$$

y por tanto:

$$x_1 + 2x_2 + 3x_3 + ... + 9x_9 \equiv x_{10}(11)$$

. La editorial esta obligada a poner x cuando el dígito x_{10} debe ser 10. Así se tiene por ejemplo: 055010206x.

El código ISBN está diseñado para detectar: a) un único error y b) un doble error creado por transposición de dos dígitos. El esquema de detectar el error es como sigue: se recibe $y_1y_2...y_{10}$, se calcula $Y = \sum_{i=1}^{10} iy_i$. Si Y no es congruente con 0 módulo 11, hay errores. Consideremos los casos:

a) La palabra recibida difiere de la enviada en un dígito solamente, es decir en lugar x_j se recibe $x_j + a$ con $a \neq 0$,entonces $Y = \sum_{i=1}^{10} iy_i = \sum_{i=1}^{10} ix_i + ja \equiv ja(11)$ y $ja \not\equiv 0(11)$.

b) Si y es x excepto en dos dígitos x_j, x_k transpuestos, entonces $Y = \sum_{i=1}^{10} iy_i = \sum_{i=1}^{10} ix_i + (k-j)x_j + (j-k)x_k \equiv (k-j)x_j + (j-k)x_k$,así $(k-j)x_j + (j-k)x_k = (k-j)(x_j - x_k) \not\equiv 0(11)$ si $k \neq j$ y $x_j \neq x_k$. Notar que es fundamental que $\mathbf{Z}/11\mathbf{Z}$ es cuerpo y así el producto de elementos no cero es no cero.

El ISBN no puede corregir un error, a menos que sepamos cual es el dígito erróneo.

Ejemplo. suponer que se lee 02011x5027. Así :

$1.0+2.2+3.0+4.1+5.1+6.x+7.5+8.0+9.2+10.7 \equiv 0(11)$, de donde $6x+4 \equiv 0(11)$ y $x = 3$.

Ejercicios.

1. Demostrar que $GF(p^m)$ es isomorfo a un subcuerpo de $GF(p^n)$ si y solo si m divide a n.

2. Sea p un primo. Probar que $p^m - 1$ divide a $p^n - 1$ si y solo si m divide a n.

3. Demostrar que todo elemento de un cuerpo finito se puede expresar como la suma de dos cuadrados.

4. Demostrar que , excepto para el caso $|k| = 2$, la suma de todos los elementos de un cuerpo finito k es 0.

5. Si $|F| = q$, q impar, probar que el producto de todos los elementos no ceros de F es igual a -1.

6. Encontrar todos los elementos primitivos de $GF(7)$ y de GF(9).

7. Demostrar que si $GF(p^n)^* =< a >$, entonces el grado del polinomio mónico irreducible de a sobre $GF(p)$ es n. ¿Es cierto el recíproco?.

8. i) Sea n un entero positivo. Probar que $n = \sum_{d|n} \varphi(d)$ donde $\varphi(d)$ es la función de Euler de d.

ii) Sea G un grupo de orden n. Si para cada d divisor de n existen a lo más d elementos $g \in G$ verificando $g^d = 1$, probar que G es cíclico.

iii) Como consecuencia de ii) probar que si k es un cuerpo, todo subgrupo finito de k^* es cíclico.

9. Como consecuencia de la fórmula de inversión de Möbius probar:

$$\varphi(n) = \sum_{d|n} \mu(d) n/d$$

10. Sea k un cuerpo. Probar: i) Si F es el cuerpo primo de k, entonces $F \cong \mathbf{Q}$ ó $F \cong \mathbf{Z}/p\mathbf{Z}$, para algún primo p. ii) Si k^* es cíclico, entonces k es finito.

11. Demostrar que el polinomio $x^4 + 1$ no es irreducible sobre cualquier cuerpo finito.

12. Un polinomio mónico irreducible $f(x) \in GF(p)[x]$ de grado $m > 1$ se dice primitivo para $GF(p^m)$ sobre $GF(p)$, si el menor entero positivo n tal que $f(x)|x^n - 1$ es $n = p^m - 1$. Probar que los polinomios primitivos para $GF(p^m)$ sobre $GF(p)$ son exactamente los polinomios mónicos irreducibles de los elementos primitivos de $GF(p^m)$.

13. Comprobar: i) x^3+x+1 es primitivo para $GF(8)$ sobre $GF(2)$, ii) $x^4+x^3+x^2+x+1$ no es primitivo para $GF(16)$ sobre $GF(2)$.

14. Sea q potencia de un primo y $n \geq 1$ un entero. Probar que $GL(n,q)$ posee un elemento de orden $q^n - 1$.

15. Sea $E = GF(25)$ y $F = GF(5)$ su cuerpo primo. Demostrar que existe $a \in E$ tal que $a^2 = 3$. Probar que $(1, a)$ es una base de E como F-espacio vectorial y que $1 + a$ es un elemento primitivo.

16. Razonar que existe $a \in GF(8)$, tal que $GF(8)^* =< a >$ y $a^3 + a + 1 = 0$. Escribir la tabla aditiva de $GF(8)$, utilizando que $GF(8) = \{0, 1, a, a^2, a^3, a^4, a^5, a^6\}$.

17. Si $a \in GF(q)$, q impar, demostrar que un elemento de $GF(q)^*$ tiene raíz cuadrada en $GF(q)$ si y solo si $a^{q-1/2} = 1$.

18. Probar que si p es un primo y n un entero positivo, entonces $n|\varphi(p^n - 1)$.

Lección 4. Codigos lineales.

En general se supondrá que F es un cuerpo de q elementos y así F^n es un F-espacio vectorial n-dimensional de orden q^n.

(4.1) **Definición**. Se dice que un código C es **lineal** si es subespacio de un F^n, para algún cuerpo finito F. Si además C es k-dimensional , se dirá que C es un (n,k)-código lineal y si su distancia mínima es d, se dirá que es un (n,k,d)-código. El **peso** de una palabra es el número de componentes no cero (o su distancia a la palabra 0).

Notar que si C es un (n,k,d)-código lineal sobre un cuerpo de q elementos, por la cota de Singleton es $q^k \leq q^{n-d+1}$, así será un MDS-código si y solo si $k = n - d + 1$, es decir, si y solo si la distancia mínima es la mayor posible.

(4.2) **Proposición** En un código lineal la distancia mínima es el menor peso de todas las palabras código no cero (o **peso mínimo del código**).

Dem. Sean $x, y \in C$ entonces $x - y \in C$ pues C es lineal. Así $d(x,y) = d(x-y,0) = w(x-y)$.

Sea C el $(4,2)$-código binario lineal $\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$. Si aplicamos la permutación $(0,1)$ a los símbolos en la primera posición, obtenemos el código $\begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$ que no es lineal. Por tanto la noción de equivalencia dada para códigos debe modificarse para códigos lineales, permitiendo sólo las permutaciones de los símbolos en una misma posición, que vienen dadas por multiplicación por escalares no ceros, además de las permutaciones de las posiciones de los símbolos en las palabras código. Así dos códigos lineales sobre un cuerpo finito F se dirán equivalentes si uno puede ser obtenido del otro por una combinación de operaciones de los tipos siguientes:

i) permutación de las posiciones del código

ii) multiplicación de los símbolos que aparecen en una posición dada por un escalar no cero.

(4.3) **Definición**. Una **matriz generadora** de un código lineal es una matriz cuyas filas constituyen una base del código.

(4.4) **Teorema**. Dos $k \times n$ matrices generan códigos lineales equivalentes sobre un cuerpo finito F, si una puede ser obtenida de la otra por una sucesión de operaciones del tipo:

i) Permutación de filas.

ii) Multiplicación de una fila por un escalar no cero.

iii) Sustitución de una fila por ella más un múltiplo escalar de otra.

iv) Permutación de columnas.

v) Multiplicación de cualquier columna por un escalar no cero.

(Observar que las operaciones i), ii) y iii) sobre las filas, simplemente reemplazan una base por otra del mismo código.)

Pasemos a la descripción de un código lineal. La primera forma de describir un código lineal es por medio de una matriz generadora. Notar que cada código lineal tiene un código equivalente con matriz generadora $G = [I_k A]$ donde I_k es la matriz unidad $k \times k$ y A es una matriz $k \times (n-k)$. En efecto, como una matriz generadora de un (n,k)-código lineal C tiene rango k, posee una submatriz regular $k \times k$ que por permutaciones de columnas puede llevarse a ser el primer bloque y mediante operaciones elementales sobre las filas se transforma en I_k. Llamaremos a esta matriz $[I_k A]$ **forma standard**. Si un código tiene una matriz generadora en forma standard se dice que es un **código sistemático**. El razonamiento anterior viene a afirmar que todo código lineal tiene un equivalente sistemático.

Codificando con un código lineal.

Sea C un (n,k)-código sobre F, cuerpo de q elementos, y G matriz generadora de C. Dicho código tiene q^k palabras y así puede emplearse para comunicar hasta q^k mensajes distintos. Dichos mensajes son las q^k k-tuplas de F^k y codificar $x_1 x_2 ... x_k$ será simplemente : $(\mathrm{x}_1 x_2 ... x_k)G = x_1 G_1 + x_2 G_2 + ... + x_k G_k$ donde G_i es la i-ésima fila de G, por tanto el resultado está en el código. En el caso de que se use una forma standard, es decir, $G = [I_k\ A]$, se tiene:

$$(x_1 x_2 ... x_k)G = x_1(10...0a_{11}...a_{1n-k}) + x_2(01...0a_{21}...a_{2n-k}) + ... + x_k(00...1a_{k1}...a_{kn-k}) =$$

$$(\mathrm{x}_1, x_2, ..., x_k, a_{11}x_1 + a_{21}x_2 + ... + a_{k1}x_k, ..., a_{1n-k}x_1 + ... + a_{kn-k}x_k)$$

es decir el mensaje original aparece en los primeros k símbolos de la palabra código.

Descodificando con un código lineal.

Suponer que se envía la palabra del código $x = x_1x_2...x_n$ y se recibe: $y = y_1y_2...y_n$. Se define el **vector error** $e = y - x$. Recordar que si $a \in F^n$, $a + C = \{a + x | x \in C\}$ es una coclase de C, que es la clase de equivalencia de a cuando se define en F^n la relación de equivalencia: $aRb \Leftrightarrow a - b \in C$.

Sabemos que:

i) Cada vector de F^n está en alguna coclase de C.

ii) Cada coclase tiene q^k vectores.

iii)Dos coclases ó son disjuntas ó coinciden.

Ejemplo.Sea C el $(4, 2)$-código binario con matriz generadora :
$G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$
así $C = \{0000, 1011, 0101, 1110\}$. Las coclases de C son:

$0000 + C = C$

$1000 + C = \{1000, 0011, 1101, 0110\}$

$0100 + C = \{0100, 1111, 0001, 1010\}$

$0010 + C = \{0010, 1001, 0111, 1100\}$

Un vector de peso mínimo en una coclase se dice que es un **líder** de la coclase. Una **formación standard** para el (n, k)-código C es una tabla en la que en la primera fila, comenzando con el vector cero, se escriben las palabras código. En las demás filas aparecen las restantes coclases, con el líder siempre a la izquierda. El proceso a seguir es el siguiente:

1. Se colocan las palabras código, comenzando con la cero.

2. Se elige un vector a_1 , no situado en la primera fila, de peso mínimo y se lista la coclase $a_1 + C$, comenzando con a_1.

3. Se elige un vector a_2 que no figure ni en la primera fila ni en la segunda y se lista la coclase $a_2 + C$, comenzando con a_2.

4. Continuar este proceso hasta que todas las coclases aparezcan listadas.

Notar que cada palabra es la suma de la palabra código al comienzo de su columna y el lider de la coclase situado al comienzo de su fila. Cuando se recibe y , se localiza en la formación standard y se descodifica como la palabra código situada al comienzo de su

columna. En el ejemplo citado se podrá corregir un error si aparece en los tres primeros lugares, no así si aparece en el cuarto luigar. En la práctica esta descodificación es muy lenta y se imponen otras formas más sofisticadas.

Pasamos a continuación a la segunda descripción de un código lineal. Previamente recordemos que en F^n el producto interno de dos vectores u, v donde $u = u_1u_2...u_n$ y $v = v_1v_2...v_n$ es el elemento de F: $u_1v_1 + u_2v_2 + ... + u_nv_n$. Si $u.v = 0$ se dice que u y v son ortogonales. Es sencillo probar: i) $u.v = v.u$ ii)$(\lambda u + \mu v).w = \lambda(u.w) + \mu(v.w)$.

(4.5) **Definición**. Si C es un (n, k)-código lineal, se llama **código dual** de C y se escribe $C^\perp = \{v \in F^n | v.u = 0, \forall u \in C\}$.

(4.6) **Proposición**. $C^\perp$ es un $(n, n-k)$-código lineal.

Dem. Sea $G = (a_{ij})$ una matriz generadora de C . Los elementos de $C^\perp$ son $x = x_1x_2...x_n$ tales que:

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{k1} & a_{k2} & \dots & a_{kn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

.

es decir es el núcleo de una aplicación lineal φ de F^n en F^kde rango k y así dim $C^\perp =$ dim Ker$\varphi = n - k$.

(4.7) **Corolario**. Para cualquier (n, k)-código lineal C se tiene $(C^\perp)^\perp = C$.

Dem.$C \subseteq (C^\perp)^\perp$ evidentemente y como dim $(C^\perp)^\perp = n - (n - k) = k$, se sigue la igualdad.

(4.8) **Definición**. Una matriz generadora de $C^\perp$ se dice **matriz de control** de C. Por tanto una matriz de control H de C tiene por filas una base de $C^\perp$ y así: $C = \{x_1x_2...x_n \in F^n | H \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = (0)\}$.

Notar que se obtendría el mismo código C si como matriz de control se considerara una cuyas filas fueran simplemente un sistema generador de $C^\perp$.

(4.9) **Definición**. Un código C se dice **autodual** si $C = C^\perp$.

Ejemplos.

i)El código ASCII es lineal pues es $GF(2)^7$. Una matriz generadora de dicho código es I_7. El código ASCII con control de paridad es también lineal. Basta recordar que en el caso binario se tiene $w(x+y) = w(x)+w(y)-2w(x \bigcap y)$ es decir que $w(x+y) \equiv (w(x)+w(y))(2)$. Este código es un $(8,7)$-código con matriz generadora :

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

En efecto, una palabra de dicho código se puede expresar como:

$$x_1x_2...x_8 = x_1(10000001) + x_2(01000001) + ... + x_7(00000011)$$

pues $x_1 + x_2 + ... + x_7 + x_8 = 0$, es decir $x_1 + x_2 + ... + x_7 = x_8$.

Observar que su dual es el código con repetición.

ii) Sea $F = \mathbf{Z}/3\mathbf{Z}$, entonces el código de matriz generadora : $\begin{pmatrix} 1 & 2 & 1 \\ 2 & 1 & 0 \end{pmatrix}$, no es un código sistemático , pues la matriz $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ tiene rango 1 y es imposible llevarla a la forma I_2 mediante operaciones con las filas.

Así como una matriz generadora de un código es útil a la hora de describir el código, una matriz de control lo es para obtener la distancia mínima del código.

(4.10) **Proposición**. Sea H una matriz de control de un código lineal C. Entonces $d(C)$ es el menor entero positivo r para el que existen r columnas de H linealmente dependientes.

Dem. Sean $H^1, ...H^n$, las columnas de H. Entonces $c_1...c_n$ es palabra código si y solo si : $H^1c_1 + ...H^nc_n = (0)$. Así las palabras código de peso s corresponden a relaciones de dependencia entre subconjuntos de s columnas de H. El peso mínimo de C se corresponderá con el menor cardinal de subconjuntos de columnas de H linealmente dependientes.

El resultado anterior permite también construir una matriz de control de un código de distancia mínima garantizada.

Queda pendiente la siguiente cuestión: ¿cómo encontrar fácilmente una matriz de control de un código?

(4.11) **Teorema**. a) Sean G, H matrices $k \times n$ y $(n-k) \times n$ sobre un cuerpo finito, con filas linealmente independientes. Entonces G y H son generadora y de control de un mismo código si y solo si $GH' = (0)$.

b) Si $G = [I\ A]$ es una matriz generadora de un código C, en forma standard, entonces una matriz de control de C es $H = [-A'I]$.

Dem. a) Es clara. b) Los bloques identidad de G y H aseguran que las correspondientes filas son linealmente independientes. Además $GH' = -IA + AI = (0)$.

(4.12) **Definición**. Sea C un (n,k)-código lineal con matriz de control H. Si $w = x_1x_2...x_n$ es una palabra, se llama **síndrome de** w a la palabra $H \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ que (por comodidad) denotaremos con Hw. Si se transmite c y se recibe w, se tiene $w = c + e$ y $Hw = Hc + He = He$, es decir el síndrome de la palabra recibida coincide con el síndrome del error cometido en la transmisión. Es sencillo probar que los síndromes caracterizan a las coclases del código:

(4.13) **Lema**. Dos vectores u, v están en la misma coclase de un código C si y solo si tienen el mismo síndrome.

Dem. $u + C = v + C \iff u - v \in C \iff H(u-v) = (0) \iff Hu = Hv$.

A veces se escribe $s(u) = Hu$. Utilizando los síndromes, se tendría el siguiente algoritmo de descodificación:

1. Si se recibe el vector w, se calcula su síndrome $Hw = z$.

2. Se localiza dicho síndrome en la columna de síndromes. Corresponderá a una coclase de C cuyo líder se denota por $f(z)$.

3. Se descodifica w como $w - f(z)$.

Por todo lo anterior, es claro que sólo necesitaremos dos columnas: la de los síndromes y la de los líderes.

(4.14) **Proposición**. Si H es una matriz de control de un código lineal t-corrector y w_1, w_2 son palabras tales que $Hw_1 = Hw_2$, y tienen peso menor ó igual que t, entonces $w_1 = w_2$.

Dem. Si $Hw_1 = Hw_2$, entonces $w_1 - w_2 \in C$, pero $w(w_1 - w_2) = d(w_1, w_2) \leq 2t$, luego necesariamente debe ser $w_1 = w_2$.

Como consecuencia de lo anterior, si C es un código lineal t-corrector , se envía c y se recibe w, $w = c + e$, donde e es la palabra error, siendo $w(e) \leq t$. Se calcula el síndrome: $Hw = He = z$ .En la coclase $w+C = e+C$ se ha elegido un líder $f(z)$, que es una palabra de dicha coclase de peso mínimo. Por lo tanto $w(f(z)) \leq w(e) \leq t$ y por el resultado anterior es $f(z) = e$ y la descodificación $w - f(z)$ nos lleva efectivamente a la palabra enviada.

Pasamos a continuación a obtener una cota inferior para el tamaño máximo de un código lineal con longitud y distancia mínima dadas. Es **la cota de Gilbert-Varshamov**, descubierta independientemente por Gilbert (1952) y Varshamov (1957).

(4.15) **Teorema**. Sea q una potencia de un primo. Entonces existe un (n, k)-código lineal q-ario con distancia mínima al menos d, supuesto que se cumpla:

$$\sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i < q^{n-k}$$

Dem. Suponer q, n, k satisfaciendo la desigualdad anterior. Construiremos una matriz H $(n-k) \times n$ sobre un cuerpo F con $|F| = q$, con la propiedad de que no existen $d-1$ columnas linealmente dependientes. Sea $r = n - k$. Como primera columna de H tomaremos cualquier r-tupla no cero de $GF(q)^r$. Como segunda cualquiera que no sea proporcional a la primera. Continuaremos eligiendo sucesivas columnas de forma que cada nueva columna no sea combinación lineal de cualesquiera $d-2$ (o menos) columnas previas. Existen $q-1$ posibles coeficientes no nulos, así cuando tratamos de elegir la $i+1$-ésima columna, las r-tuplas no permitidas serán las

$$N(i) = 1 + \binom{i}{1}(q-1) + \binom{i}{2}(q-1)^2 + ... + \binom{i}{(d-2)}(q-1)^{d-2}$$

combinaciones lineales de $d-2$ o menos columnas. No todas estas combinaciones lineales son vectores distintos, pero aún en el caso peor, en que sí que lo fueran, como el sumatorio no alcanza, por la hipótesis, el número total de r-tuplas, que es q^r, podemos encontrar la columna buscada.

Notar que para las r primeras columnas de H se puede elegir la base canónica de $GF(q)^r$.

Finalizaremos esta lección con **la cota de Plotkin**.

(4.16) **Teorema**. Si C es un (n,k)-código lineal q-ario de distancia mínima d, se tiene:

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

Dem. Sea i, $1 \leq i \leq n$, tal que C contiene al menos una palabra con i-ésima coordenada no cero. Sea D el subespacio de C de todas las palabras código con i-ésima coordenada cero. Si proyectamos $p_i : C \longrightarrow F$, $p_i(x_1...x_n) = x_i$, se tiene que p_i es una aplicación lineal suprayectiva y como $\mathrm{Ker}\, p_i = D$, es $|D| = q^{k-1}$ y el número de palabras código con i-ésima coordenada no cero es $q^k - q^{k-1}$. Sea $L = \{(i,c)|c \in C$, teniendo i-ésima coordenada no cero, $1 \leq i \leq n$ $\}$. Analicemos el cardinal de L desde dos puntos de vista. Cada palabra código c será segundo miembro de $w(c)$ pares ordenados de L, así $|L| = \sum_{c \in C} w(c)$. Por otra parte, dado i, $1 \leq i \leq n$, sabemos que si existe una palabra código con i-ésima coordenada no cero, hay exactamente $q^k - q^{k-1}$ palabras código con i-ésima coordenada no cero. Por lo tanto $|L| = \sum_{c \in C} w(c) \leq n(q^k - q^{k-1})$. Finalmente, como $d = d(C)$ es el peso mínimo de las palabras no cero de C, se tiene:

$$d(q^k - 1) \leq \sum_{c \in C} w(c) \leq nq^{k-1}(q-1)$$

.

Ejercicios .

1. Sea C un $(2k+1,k)$-código binario lineal tal que $C \subseteq C^{\perp}$. Razonar que $C^{\perp} - C$ está formado por todas las palabras que resultan al sumar a las de C la palabra $1 = 111...1$.

2. Si C es un código binario lineal, probar que ó todas las palabras del código tienen peso par ó exactamente la mitad son de peso par y la otra mitad son de peso impar.

3. Sea C el código lineal ternario con matriz generadora :

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$$

listar las palabras de C y hallar $d(C)$. Deducir que C es un código perfecto.

4. Razonar que $A_q(3,2) = q^2$, para cualquier entero $q \geq 2$. Si $B_q(n,d)$ denota el mayor valor de M para el que existe un (n,M,d)-código q-ario lineal (q potencia de un primo), razonar que $B_q(3,2) = q^2$.

5. Sea C el código lineal binario con matriz generadora :

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

encontrar una matriz generadora de C en forma standard.

6. Sea C el código ternario con matriz generadora:

$$G = \begin{pmatrix} 1 & 2 & 2 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 2 & 1 \end{pmatrix}$$

encontrar un código sistemático equivalente a C y una matriz generadora de dicho código.

7. Probar que un código sistemático posee una única matriz generadora en forma standard.

8. Comprobar que el código binario $C =< 1100, 0011 >$ es autodual.

9. Sea $C =< 0110, 1201 >$ un código ternario lineal. Determinar $C^{\perp}$ y una matriz de control de C.

10. Sea C el código binario con matriz generadora:

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

Hallar una matriz de control de C y encontrar su la distancia mínima del código. (Confrontar con 5).

11. Suponer que C es un código binario con matriz de control $H = (h_{ij})$. Sea $\tilde{C}$ el código extendido a partir de C, añadiendo control de paridad a las palabras de C. Probar que $\tilde{C}$ tiene matriz de control :

$$\tilde{H} = \begin{pmatrix} h_{11} & \dots & h_{1n} & 0 \\ h_{21} & \dots & h_{2n} & 0 \\ \vdots & \vdots & \vdots & \vdots \\ h_{r1} & \dots & h_{rn} & 0 \\ 1 & \dots & 1 & 1 \end{pmatrix}$$

12. Sea C un $(n.k)$-código binario lineal. Si C es e-corrector, probar:

$$2^{n-k} \geq 1 + \binom{n}{1} + ... + \binom{n}{e}$$

Deducir que no existe un $(17, 10)$-código binario lineal que corrija más de un error.

13. Un profesor pretende asignar a cada uno de sus 53 alumnos un número de identificación en forma de palabra binaria. Se pide:

i) Encontrar la menor dimensión de un código binario lineal, que pueda servir a tal efecto. (Se supone que no toda palabra del código debe quedar asignada).

ii) Si el código ha de ser 1-corrector, encontrar la menor longitud posible de dicho código.

iii) Obtener una matriz de control para un código que satisfaga i) y ii).

14. Sea C un código binario con matriz de control :

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

Construir la tabla standard y descodificar las palabras recibidas: $11101, 00110, 01101$.

15. Considerar los parámetros $n = 5, k = 3, q = 3, d = 2$. verificar la cota de Gilbert-Varshamov y construir un $(5, 3)$-código ternario lineal con distancia mínima al menos 2.

16. Lo análogo a 15, para los parámetros: $n = 6, k = 3, d = 3$ y para $n = 7, k = 3, d = 4$.

17. Sea E_n el conjunto de todos los elementos de $(\mathbf{Z}/2\mathbf{Z})^n$ que tienen peso par. Demostrar que E_n es el código que surge al añadir a los vectores de $(\mathbf{Z}/2\mathbf{Z})^{n-1}$ un control de paridad. Deducir que E_n es un $(n, 2^{n-1}, 2)$-código lineal. Escribir una matriz generadora de E_n en forma standard. Comprobar que $(E_n)^\perp$ es el código con repetición de longitud n.

18. Sea C un (n, k)-código lineal $(k \geq 1)$. Probar que C es un MDS-código si y solo si $C^\perp$ es un MDS-código.

19. Sea C un (n, k)-código lineal. Probar que C es un MDS-código si y solo si cualesquiera k columnas de una matriz generadora de C son linealmente independientes.

20. Los códigos lineales cuyos parámetros (n, k, d) son de la forma: $(n, n, 1)$,$(n, 1, n)$ y $(n, n-1, 2)$, son ejemplos de MDS-códigos a los que se les llama MDS-códigos triviales. Demostrar que no existen MDS-códigos binarios lineales con $1 < k \leq n-2$. Más aún, si C es un MDS-código binario , debe de ser ó el espacio total ó E_n ó su dual el código con repetición.

21. Sea C el código binario lineal con matriz de control:

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

Si se recibe 110110 y se ha cometido un solo error, ¿cual es la palabra del código enviada?.

22. Sean G_1 y G_2 matrices generadoras de un (n_1, k, d_1)-código lineal y un (n_2, k, d_2)-código lineal respectivamente. Demostrar que los códigos de matrices generadoras :
$\begin{pmatrix} G_1 & O \\ O & G_2 \end{pmatrix}$ y $(\, G_1 \quad G_2\,)$, son $(n_1 + n_2, 2k,$ mín$(d_1, d_2))$ y $(n_1 + n_2, k, d)$-códigos respectivamente, siendo $d \geq d_1 + d_2$.

23. Sea F el cuerpo de cuatro elementos . Escribamos $F = \{0, 1, \omega, \omega^2\}$. Las operaciones en F pueden deducirse de : $1 + 1 = 0$ y $1 + \omega = \omega^2$. Se pide:

i) Construir las tablas aditiva y multiplicativa de F. ii) Sea C el código lineal sobre F con matriz generadora : $\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & \omega & \omega^2 \\ 0 & 0 & 1 & 1 & \omega^2 & \omega \end{pmatrix}$. Hallar una matriz de control de C y la distancia mínima del código.

24. Sea p un número primo con $p \equiv 1(4)$. Justificar la existencia de $a \in GF(p)$ tal que $a^2 = -1$ y construir la matriz

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

justificar que dicha matriz es generadora de un (8,4)-código lineal sobre $GF(p)$, que es autodual.

25. Sea C un $(q+1, 2, q)$-código lineal sobre $GF(q)$, probar que todas las palabras de C distintas de 0 tienen peso q. (Confrontar con el problema 8 de la Lección 5).

26. Sea C un (n, k, d)-código lineal. Probar que C es un MDS-código si y solo si C tiene una palabra de peso mínimo en cualesquiera d coordenadas.

27. Sea C un (n, k)-código lineal binario que tiene una matriz generadora que no contiene columnas nulas. Alinear las 2^k palabras código formando una matriz A, $2^k \times n$.

i) Probar que cada columna de A tiene 2^{k-1} ceros y 2^{k-1} unos.

ii) Usando i) probar que $d(C) \leq n2^{k-1}/2^k - 1$.

iii) ¿Es posible encontrar un $(15, 7)$-código lineal binario con distancia mínima mayor que 7?.

Lección 5 . Códigos de Hamming .

Los códigos de Hamming son una importante familia de códigos lineales 1-correctores. Comenzaremos por el caso binario que, por su simplicidad, puede facilitar el estudio de estos códigos.

(5.1) **Definición**. Sea r entero positivo y H una matriz $r \times (2^r - 1)$, cuyas columnas son las distintas r-tuplas no cero de $GF(2)^r$. Entonces el código que tiene a H como matriz de control, se dice **código de Hamming binario** y se denota $\mathrm{Ham}(r, 2)$.

Notas. i) $\mathrm{Ham}(r, 2)$ tiene longitud $2^r - 1 = n$ y dimensión $n - r$.

ii) Dado que las columnas de H se pueden escribir en cualquier orden , el código $\mathrm{Ham}(r, 2)$, para un r dado, es cualquiera de los equivalentes.

Ejemplos . i) Si $r = 2$ entonces una matriz de control de $\mathrm{Ham}(2, 2)$ es :

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

ii) Si $r = 3$, una matriz de control para $\mathrm{Ham}(3, 2)$ es

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

Si tomamos H en forma standard , es decir:

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

entonces una matriz generadora de $\mathrm{Ham}(3, 2)$ es:

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

.

(5.2) **Proposición** El código $\mathrm{Ham}(r, 2)$ para $r \geq 2$ tiene las siguientes propiedades:

i) Es un $(2^r - 1, 2^r - 1 - r)$-código.

ii) Su distancia mínima es 3, así es un código 1-corrector.

iii) Es perfecto.

Dem. i) Notar que dim $\mathrm{Ham}(r,2)^{\perp} = r$, luego la afirmación es inmediata.

ii) Notar que ninguna de las columnas de H es la nula y dos cualesquiera son linealmente independientes. Además es claro que existen al menos tres columnas linealmente dependientes. Por (4.10) se tiene que $d(\mathrm{Ham}(r,2)) = 3$

iii) Sea $n = 2^r - 1$. Entonces $|\mathrm{Ham}(r,2)| = 2^{n-r}$ y se tiene:

$$2^{n-r}(1 + \binom{n}{1}) = 2^{n-r}(1+n) = 2^{n-r}(1+2^r-1) = 2^n = |GF(2)^n|$$

luego se alcanza la cota de Hamming y así $\mathrm{Ham}(r,2)$ es perfecto.

Descodificando con un código de Hamming binario.

Si se transmite c y se recibe w, como $w = c + e_i$ para algún i, al calcular el síndrome de w tendremos $Hw = He_i$ que es la i-ésima columna de H, lo que significará que el error está en la i-ésima componente. Así bastará efectuar $w - e_i$.

Codigos de Hamming q-arios.

En orden a construir un código lineal con distancia mínima 3, debemos de requerir, en principio, a las columnas de una posible matriz de control H, que dos cualesquiera sean linealmente independientes.

Consideremos $V = GF(q)^r$ y $X = V - \{\bar{0}\}$, así $|X| = q^r - 1$. Dos elementos de X se dirán equivalentes si uno es múltiplo escalar del otro. Cada clase de equivalencia tiene $q-1$ elementos, así hay $n = (q^r-1)/(q-1)$ clases de equivalencia.

Sea Y un conjunto de representantes de dichas clases de equivalencia. Y está formado tomando un vector no cero de cada subespacio 1-dimensional de V. Sea H la $r \times n$ matriz cuyas columnas son los elementos de Y. Se define el **código de Hamming q-ario** de longitud n como el código lineal con matriz de control H. Como sucede en el caso binario los códigos de Hamming q-arios están unívocamente definidos salvo equivalencia.

(5.3) **Proposición**. Los códigos de Hamming q-arios son códigos 1-correctores perfectos.

Dem. De nuevo por la propia definición del código, es claro que es un $(n, M, 3)$-código con $n = (q^r-1)/(q-1)$ y $M = q^{n-r}$. Además se tiene:

$$q^{n-r}(1+n(q-1)) = q^{n-r}(1+q^r-1) = q^n = |GF(q)^n|$$

luego alcanzan la cota de Hamming.

(5.4) **Corolario**. Si q es una potencia de un primo y $n = (q^r-1)/(q-1)$ para algún $r \geq 2$ entonces:

$$A_q(n,3) = q^{n-r}$$

.

Se ha conjeturado que no existen códigos con los parámetros $((q^r-1)/(q-1), q^{n-r}, 3)$ cuando q no es potencia de un primo. Solamente se ha resuelto en el caso $q = 6, r = 2$. La posible existencia de un $(7, 6^5, 3)$-código 6-ario fué considerada por Golay (1.958) y resuelta negativamente por Golomb y Posner (1.964), quienes redujeron el problema al planteado por Euler sobre los 36 oficiales en 1.782, resuelto negativamente por Tarry en 1.901.

El problema de los 36 oficiales es el siguiente. Se consideran 36 oficiales , uno de cada uno de 6 rangos y de cada uno de 6 regimientos. ¿Pueden colocarse en un cuadrado 6x6 de forma que en cada fila y cada columna de dicho cuadrado haya solo un oficial de cada rango y de cada regimiento?

Teniendo en cuenta la respuesta negativa a dicha pregunta , probaremos el siguiente resultado.

(5.5) **Teorema**. No existe un $(7, 6^5, 3)$-código 6-ario.

Dem. Supongamos que existe un $(7, 6^5, 3)$-código 6-ario C sobre el alfabeto $F = \{1, 2, 3, 4, 5, 6\}$. Considerar las 6^5 palabras obtenidas borrando las dos últimas componentes de cada palabra de C. Dichas palabras deben de ser los 6^5 elementos de F^5, pues si dos de ellas coincidieran, se tendrían dos palabras de C a distancia menor o igual que 2, lo que no es posible. Si consideramos las 6^2 palabras código que comienzan con 111, y borramos las tres primeras componentes, aparece un $(4, 6^2, 3)$-código D. Por lo mismo que antes, si se borran dos componentes de las palabras del código D, las 6^2 palabras tienen en las componentes restantes, los 36 elementos de F^2. Si cada palabra $ijkl$ de D se identifica con un oficial de rango i, regimiento j, situado en el lugar (k, l) del cuadrado 6x6, tendríamos una solución al problema de Euler, lo que no es posible.

Descodificando con un código de Hamming q-ario.

Si se recibe la palabra w, $w = c + 0...0b0...0$ donde b aparece en la i-ésima componente y c pertenece al código. Entonces:

$$Hw = H^i b$$

es decir es la i-ésima columna de H multiplicada por b. Si dicho síndrome no es cero, hay error. La palabra enviada se obtiene restando b a la i-ésima componente de w.

Ejemplo. Suponer $q = 3$, $r = 2$,luego $n = (q^r - 1)/(q - 1) = 4$. Considerar:

$$H = \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

Si se recibe 1212, entonces:

$$\begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \end{pmatrix} = 2 \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

v así la palabra enviada es 1012.

El código dual de un código de Hamming

El código $\mathrm{Ham}(r, q)^\perp$ (simplex-code) tiene a H como matriz generadora, donde las columnas de H son los elementos de Y, sistema completo de representantes de los subespacios 1-dimensionales de $GF(q)^r$. Así si $c \in \mathrm{Ham}(r, q)^\perp$, $c \neq 0$, se tiene que

$c = a_1(h_{11}, h_{12}, ..., h_{1n}) + ... + a_r(h_{r1}, h_{r2}, ..., h_{rn}) = (a_1h_{11} + a_2h_{21} + ... + a_rh_{r1}, a_1h_{12} + a_2h_{22} + ... + a_rh_{r2}, ..., a_1h_{1n} + a_2h_{2n} + ... + a_rh_{rn}) = (c_1, c_2, ..., c_n)$

Si $S = \{(b_1, ..., b_r) | a_1b_1 + ... + a_rb_r = 0\}$, S es un subespacio de $GF(q)^r$ de dimensión $r - 1$ y $|S| = q^{r-1}$. Notar que $c_i = 0 \Leftrightarrow H^i \in S$. Así c tendrá $q^{r-1} - 1/q - 1$ coordenadas nulas y por tanto $w(c) = n - (q^{r-1} - 1/q - 1) = (q^r - 1/q - 1) - (q^{r-1} - 1/q - 1) = (q^r - q^{r-1})/q - 1 = q^{r-1}$. Así los parámetros de $\mathrm{Ham}(r, q)^\perp$ son (n, r, q^{r-1}). En particular los de $\mathrm{Ham}(2, q)^\perp$ son $(q + 1, 2, q)$.

Un código no lineal con los mismos parámetros que un código de Hamming

En 1962 Vasil'ev dió la siguiente construcción:

Sea $\lambda : \mathrm{Ham}(r,2) \longrightarrow \mathbf{Z}_2$ una aplicación no lineal , de forma que $\lambda(0) = 0$. Asi existen $c, d \in \mathrm{Ham}(r,2)$ tales que $\lambda(c+d) \neq \lambda(c) + \lambda(d)$. Para cada $x \in \mathbf{Z}_2^n$, sea $\pi(x) = 0$ si $w(x)$ es par y $\pi(x) = 1$ si $w(x)$ es impar. Considerar el código: $C = \{(x, x+c, \pi(x) + \lambda(c))\ \forall x \in \mathbf{Z}_2^n, c \in \mathrm{Ham}(r,2)\}$, donde $n = 2^r - 1$. Se trata de comprobar que C es un $(2^{r+1} - 1, 2^{2n-r}, 3)$- código binario perfecto no lineal. Es claro que la longitud es $2n + 1 = 2(2^r - 1) + 1 = 2^{r+1} - 1$. En cuanto al número de palabras código, será $2^n.2^{2^r-1-r} = 2^{2^r-1+2^r-1-r} = 2^{2n-r}$. Veamos que $d(C) = 3$.

Supongamos que existieran dos palabras código : $(x, x+c, \pi(x) + \lambda(c))$ y $(y, y + d, \pi(y) + \lambda(d))$ a distancia 1. Si $d(x,y) = 1$, suponer que $x_i \neq y_i$, como $x + c = y + d$ se tendría que $c_i \neq d_i$ y las demás coordenadas coincidirían. Así $d(c,d) = 1$, lo que no es posible pues $d(\mathrm{Ham}(r,2)) = 3$. Si $d(x+c, y+d) = 1$ entonces $x = y$, y de nuevo se tendría se tendría que $d(c,d) = 1$, que no es posible. Notar que si $x = y$ y $x + c = y + d$, no puede suceder que las últimas coordenadas de las palabras de C sean distintas.

Supongamos que $d((x, x+c, \pi(x) + \lambda(c)), (y, y+d, \pi(y) + \lambda(d)) = 2$. Si $d(x,y) = 2$, suponer que $x_i \neq y_i, x_j \neq y_j$. Como $x + c = y + d$ se tendría que $d(c,d) = 2$,lo que no es posible. Si $d(x+c, y+d) = 2$, entonces $x = y$ luego $d(c,d) = 2$, imposible. Si $d(x,y) = 1$ y $d(x+c, y+d) = 1$, entonces $\pi(x)+\lambda(c) = \pi(y)+\lambda(d)$ luego $c \neq d$, ya que si $c = d$ entonces $\pi(x) = \pi(y)$, que no es posible. Suponer que $x_i \neq y_i$ y que $x_j + c_j \neq y_j + d_j$. Si $i = j$ $d(c,d) = 1$. Si $i \neq j$, $x_j + c_j \neq y_j + d_j$ siendo $x_j = y_j$, luego $c_j \neq d_j$ y como $x_i + c_i = y_i + d_i$ entonces $c_i \neq d_i$. Para $k \neq i, j$ se tiene $x_k + c_k = y_k + d_k$ luego $c_k = d_k$. Así $d(c,d) = 2$, que no es posible. Si $d(x,y) = 1$ y $\pi(x) + \lambda(c) \neq \pi(y) + \lambda(d)$ de nuevo al ser $x + c = y + d$ se tendría $d(c,d) = 1$, imposible. Si $d(x + c, y + d) = 1$ y $\pi(x) + \lambda(c) \neq \pi(y) + \lambda(d)$ como $x = y$ sería $d(c,d) = 1$, imposible.

Así $d(C) \geq 3$. Además existen palabras en C a distancia 3. En efecto, basta elegir x, y tales que $d(x,y) = 1$ entonces: $d((x, x+0, \pi(x)), (y, y+0, \pi(y)) = 3$.

Como consecuencia del desarrollo anterior se concluye que los parámetros de C son : $(2^{r+1} - 1, 2^{2n-r}, 3)$, que son los parámetros de $\mathrm{Ham}(r+1, 2)$.

Notar que C no es lineal pues $(0, c, \lambda(c)), (0, d, \lambda(d)) \in C$ pero (0,c+d,$\lambda(c)+\lambda(d)) \notin C$.

Una aplicación de los códigos de Hamming.

En este caso $F = \{1, \times, 2\}$ y la longitud de las palabras es 14. Cuando se realiza una

quiniela múltiple y se trata de hacer el menor número posible de 14-columnas, de forma que, en al menos una de ellas, el número de errores cometidos sea a lo más e ($e \leq 14$), el problema es :

Encontrar un subconjunto C de F^{14}, con el menor cardinal (para economizar),de forma que dado cualquier elemento de F^{14} exista al menos un elemento en C cuya distancia sea a lo más e. Es decir se trata de encontrar C de forma que F^{14} aparezca como unión de esferas de radio e y centro en los elementos de C. Diremos que un conjunto C que verifique las condiciones indicadas es solución al problema $Q(3, 14, e)$.En general si $|F| = q$, y e, n son números naturales, a C se le dice solución al problema $Q(q, n, e)$.

El problema que se plantean los quinielistas al intentar asegurar una columna con 13 aciertos es el $Q(3, 14, 1)$, es decir buscar un subconjunto C de F^{14} con el menor número de elementos , de manera que se obtenga al menos una quiniela con 13 aciertos. Se desconoce todavía la solución y se ignora incluso un tamaño aproximado de C.

Si se trata de resolver el problema $Q(q, n, 1)$ para algunos valores de q y de n, por ejemplo en el caso en que q es potencia de primo y $n = (q^r - 1)/(q - 1)$, entonces $\mathrm{Ham}(r, q)$ es un código perfecto 1-corrector, luego F^n se particiona en esferas de radio 1 y centro en las diferentes palabras código. Así, en tal caso, dicho código es solución al problema $Q(q, n, 1)$. Para $n \leq 14$ y $q \leq 3$ se obtiene solución a los problemas : $Q(2, 3, 1)$, $Q(2, 7, 1)$, $Q(3, 4, 1)$ y $Q(3, 13, 1)$ de órdenes 2, 2^4, 3^2 y 3^{10} respectivamente. Los problemas $Q(3, 4, 1)$ y $Q(3, 13, 1)$ son de aplicación directa para los quinielistas. El primero da el número de apuestas que deberán realizarse para conseguir tres aciertos en cuatro partidos y el segundo para conseguir doce aciertos en trece partidos.

Ejercicios

1. Escribir una matriz de control para un código de Hamming binario de longitud 15. Escribir las columnas en orden correspondiente a la representacvión binaria de los enteros positivos. ¿Cuáles de las siguientes palabras son del código?

i)011010110111000 ii)100000000000011 iii)110110110111111

2. Considerando el código Ham$(3,3)$ descodificar la palabra recibida : 1101112211201.

3. Sea C un código ternario lineal con matriz generadora $G = \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 \end{pmatrix}$. Se pide: i) ¿Cuantas palabras hay en C?. ii) Obtener una matriz de control de C. iii) Hallar $d(C)$. iv) ¿Pertenece C a alguna familia de códigos conocida?. v) Descodificar 2212.

4. Si C es un código de Hamming ¿es $C^{\perp}$ también de Hamming?. ¿Es $C^{\perp}$ perfecto?

5. Demostrar que el único código de Hamming autodual es Ham$(2,3)$.

6. Comprobar que los parámetros del código : $(\text{Ham}(2,q))^{\perp}$ son $(q+1, q^2, q)$.

7. Demostrar que un código lineal con los mismos parámetros que un código de Hamming, es un código de Hamming.

8. Demostrar que un código lineal con los parámetros $(q+1, q^2, q)$ es el dual de un código de Hamming.

9. Sea $C = \text{Ham}(2,3)$. Si $x = x_1x_2x_3x_4 \in GF(3)^4$, llamaremos $\bar{x} = x_1 + x_2 + x_3 + x_4$ y $\alpha(x) = \bar{x}\bar{x}\bar{x}\bar{x}$. Sea $D = \{(-x - \alpha(x), x + c, x - c) | x \in GF(3)^4, c \in \text{Ham}(2,3)\}$. Probar que D es un $(12,6,6)$-código lineal autodual. (Confrontar con el código de Golay ternario g_{12}).

Lección 6. Codigos de Golay .

Se consideran códigos perfectos triviales los códigos de repetición con longitud impar y los del tipo F^n, donde F es un alfabeto con q elementos. En la lección anterior hemos comprobado que los códigos q-arios de Hamming son también ejemplos de códigos perfectos, con parámetros: $((q^r-1)/(q-1), q^{n-r}, 3)$. En 1.949 Golay se planteó qué otras ternas de parámetros (n, M, d) corresponderían a códigos perfectos. Encontró las ternas $(23, 2^{12}, 7)$ y $(90, 2^{78}, 5)$ con $q = 2$ y $(11, 3^6, 5)$ si $q = 3$. En su artículo consideró códigos lineales y presentó matrices generadoras de códigos con parámetros $(23, 2^{12}, 7)$ y $(11, 3^6, 5)$, probando además que no existe un código lineal con parámetros $(90, 2^{78}, 5)$. En 1973 J.H.van Lint y A. Tietäväinen probaron el siguiente resultado: Un código q-ario perfecto no trivial, con q potencia de un primo, debe de tener los mismos parámetros que uno de los códigos de Hamming ó de Golay. El teorema de van Lint y Tietäväinen plantea el siguiente problema: encontrar todos los códigos perfectos que tienen parámetros coincidentes con los de los códigos de Hamming ó de Golay. Es sencillo probar que cualquier código lineal con los parámetros de Hamming un código de Hamming (ver ejercicio 7 de la lección anterior), pero permanece sin resolver el problema de encontrar los códigos no-lineales con dichos parámetros. En la lección anterior hemos expuesto el código no lineal de Vasil'ev que tiene los mismos parámetros que un Hamming. Sin embargo los códigos de Golay perfectos son únicos. Este hecho fué probado por V. Pless en 1968 restringiéndose a códigos lineales y por Delsarte y Goethals para códigos sin restricción. En esta lección describiremos de forma elemental los dos códigos de Golay perfectos.

El código de Golay binario g_{24}.

El código de Golay g_{24} es un código lineal binario con matriz generadora $G = [I_{12}\, A]$ donde

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

notar que a partir de la tercera fila, se obtiene dicha matriz desplazando la fila anterior una posición a la izquierda . Calculemos la distancia mínima de este código.

(6.1) **Proposición**. g_{24} es un código autodual.

Dem. Es fácil ver que las filas de G son ortogonales entre sí. La primera fila tiene peso 12 y las demás peso 8. Como cada fila tiene peso par, es ortogonal a sí misma. Así $g_{24} \subseteq g_{24}^{\perp}$. Además $\dim g_{24} = 12$ y $\dim g_{24}^{\perp} = 24 - 12 = 12$, luego $g_{24} = g_{24}^{\perp}$.

Notar que $A = A'$, así $[A\ I_{12}]$ es matriz de control de g_{24}, y por lo anterior será también generadora de g_{24}.

(6.2) **Proposición**. El peso de cada palabra de g_{24} es divisible por 4.

Dem. Basta demostrar que la suma de dos palabras de g_{24} de peso divisible por 4 tiene peso divisible por 4. Sabemos que: $w(x+y) = w(x) + w(y) - 2w(x \bigcap y)$. Recordar que $w(x \bigcap y)$ es el número de posiciones en las que ambas palabras tienen un 1. Como $x.y = 0$ se sigue que $w(x \bigcap y)$ es par y por tanto la tesis.

Como consecuencia del resultado anterior se obtiene que el peso mínimo de g_{24} es un múltiplo de 4 y como G tiene filas de peso 8, puede ser 4 o bien 8.

(6.3) **Proposición**. g_{24} no tiene palabras de peso 4.

Dem. Suponer que existe $u \in g_{24}$ de peso 4. Consideremos u como yuxtaposición de sus mitades izquierda y derecha, ambas de longitud 12: $u = (i|d)$. Sean $G_1 = [I_{12}\, A]$ y $G_2 = [A\, I_{12}]$, ambas generadoras de g_{24}. La palabra i es combinación lineal de las filas de I_{12} y como $u \neq \bar{0}$, es $w(i) \geq 1$. De igual forma usando G_2 y d se llega a $w(d) \geq 1$.

Si $w(i) = 1$, entonces u es una fila de G_1, pero ninguna de ellas tiene peso 4, luego $w(i) \geq 2$. De igual forma $w(d) \geq 2$. Necesariamente se tiene: $w(i) = w(d) = 2$. Al ser

$w(i) = 2$, u debe ser suma de dos filas de G_1, pero ninguna de estas sumas puede tener peso 4. Por lo tanto no pueden existir en g_{24} palabras de peso 4.

(6.4) **Corolario**. g_{24} es un (24,12,8)-código lineal binario.

El código de Golay binario g_{23}

Se obtiene a partir de g_{24} borrando la última coordenada de cada palabra código. Puede probarse que si se borra cualquier coordenada, el código resultante es equivalente al anterior ([7]).

g_{23} es un (23,12,7)-código perfecto ya que :

$$2^{12}(1 + 23 + \binom{23}{2} + \binom{23}{3}) = 2^{23}$$

Los códigos de Golay ternarios.

El código de Golay ternario g_{12} tiene una matriz generadora $G = [I_6\, B]$ donde

$$B = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 2 & 1 \\ 1 & 1 & 0 & 1 & 2 & 2 \\ 1 & 2 & 1 & 0 & 1 & 2 \\ 1 & 2 & 2 & 1 & 0 & 1 \\ 1 & 1 & 2 & 2 & 1 & 0 \end{pmatrix}$$

A partir de la tercera fila, una fila se obtiene de la anterior desplazándola una posición hacia la derecha.

(6.5) **Proposición**.

i) g_{12} es autodual.

ii)B es simétrica.

iii)g_{12} es un (12,6,6)-código.

iv) g_{11}, obtenido pinchando g_{12}, es un (11,6,5)-código perfecto.

Dem. Notar que todas las filas de G tienen peso 6 y son ortogonales a sí mismas y dos a dos. Así $g_{12} \subseteq g_{12}^{\perp}$ y como tienen la misma dimensión, coinciden.

De igual forma que en el párrafo anterior, se tiene que $[-B'\, I_6]$ es también matriz generadora de g_{12}, donde

$$-B' = \begin{pmatrix} 0 & 2 & 2 & 2 & 2 & 2 \\ 2 & 0 & 2 & 1 & 1 & 2 \\ 2 & 2 & 0 & 2 & 1 & 1 \\ 2 & 1 & 2 & 0 & 2 & 1 \\ 2 & 1 & 1 & 2 & 0 & 2 \\ 2 & 2 & 1 & 1 & 2 & 0 \end{pmatrix}$$

Suponer que una palabra código $x = (i|d)$ tiene peso menor o igual que 5, entonces o $w(i) \leq 2$ o $w(d) \leq 2$. Si $w(i) \leq 2$ se tendría:

$$x = \lambda_1(100000b_{11}b_{12}...b_{16}) + \lambda_2(010000b_{21}b_{22}...b_{26}) + ... + \lambda_6(000001b_{61}b_{62}...b_{66})$$

, es decir x sería combinación lineal de a lo más dos filas de B. Como el peso de las filas de B es 6, no puede ser proporcional a una de ellas, así que ó es la suma de dos de ellas ó es la suma de una más 2 por la otra ó 2 por una más 2 por la otra. Se observa que cualquiera de dichos casos no es posible. Lo análogo si $w(d) \leq 2$,considerando como matriz generadora del código a $[-B'\ I_6]$. Finalmente g_{11} es perfecto ya que:

$$3^6(\binom{11}{0} + \binom{11}{1}2 + \binom{11}{2}4) = 3^6.3^5 = 3^{11}$$

Descodificando con g_{24}

Suponer que se recibe la palabra w de forma que $w = c + e$ y $w(e) \leq 3$. Sea $e = (x|y)$, donde tanto x como y son 12-tuplas binarias. Puede suceder:

i) $w(x) \leq 3$ y $w(y) = 0$

ii) $w(x) \leq 2$ y $w(y) = 1$

iii) $w(x) \leq 1$ y $w(y) = 2$

iv) $w(x) = 0$ y $w(y) = 3$

Como $G = [I_{12}|A]$ es matriz generadora de $g_{24} = g_{24}^{\perp}$, G es también matriz de control de g_{24}. Así : $Gw^t = Ge^t = I_{12}x^t + Ay^t = s$, síndrome de w.

Si $w(y) = 0$ y $w(x) \leq 3$, entonces $s = x^t$ luego $w(s) \leq 3$ y $e = (s^t|0)$.

Si $w(y) = 1$ y $w(x) \leq 2$, supongamos que la única coordenada no cero de y es la i-ésima. Entonces:

$s = x^t + Ay^t = x^t + A^i$, luego $w(s + A^i) \leq 2$, $x = (s + A^i)^t$ y $e = ((s + A^i)^t|y^i)$, donde y^i es la 12-tupla binaria con un sólo uno en la i-ésima coordenada.

Si $w(y) = 2$ ó 3 y $w(x) = 0$, entonces $s = Ay^t = A^i + A^j$ ó $A^i + A^j + A^k$, según sea $w(y)$. Como $A^2 = I_{12}$, $y^t = A(A^i + A^j)$ ó $y^t = A(A^i + A^j + A^k)$ y $w(As) = w(y^t) \leq 3$, siendo As un vector con sólo unos en las coordenadas i, j ó en i, j, k, dependiendo del peso. Entonces $e = (0|(As)^t)$.

Si $w(y) = 2$ y $w(x) = 1$, entonces $s = x^t + Ay^t$ y si la coordenada no cero de x es la i-ésima, se tiene: $As = Ax^t + y^t = A^i + y^t$, así $y^t = As + A^i$, $w(As + A^i) = 2$ y e=(x^i|$(As + A^i)^t$), siendo x^i la 12-tupla binaria con un sólo uno en su i-ésima coordenada.

Finalizamos esta lección demostrando que no existen $(90, 2^{78}, 5)$-códigos binarios.

(6.6) **Definición**. Si x e y son n-tuplas binarias diremos que x cubre a y si y solo si $x \cap y = y$. Notar que $x \cap y = y$ si y solo si, supuesto que $x = x_1...x_n$ e $y = y_1...y_n$, $y_i = 1 \Rightarrow x_i = 1$ cualquiera que sea $1 \leq i \leq n$.

(6.7) **Teorema**. No existe un $(90, 2^{78}, 5)$-código binario.

Dem. Supongamos que existe un $(90, 2^{78}, 5)$-código binario C. Podemos suponer que la palabra $00...0 \in C$. Entonces cada palabra no cero de C tiene peso ≥ 5. Sea Y el conjunto de las 90-tuplas binarias que tienen peso 3 y comienzan con 11. Es claro que $|Y| = 88$. Como C es perfecto, para cada $y \in Y$ existe una única palabra código x que dista a lo más 2 de y. Esta palabra código debe tener peso 5 y debe de cubrir a y. Sea X el conjunto de las palabras código de peso 5 y que comienzan con 11. Calcularemos de dos formas distintas el número de elementos de $D = \{(x, y)|x \in X, y \in Y, x \text{ cubre a } y\}$. Por lo anterior cada $y \in Y$ es cubierto por una única palabra de X. Así $|D| = 88$. Por otra parte, cada palabra de X cubre exactamente a tres $y \in Y$ (por ejemplo: si $x = 111110...0$ x cubre a $1110...0, 1101...0, 11001...0$). Así $|D| = 3|X|$, de donde se seguiría que $|X| = 88/3$ lo que no es posible.

Lección 7. Códigos de Reed-Muller.

(7.1) **Definición**. Una **función de Boole** de m variables es una aplicación $f : \mathbf{Z_2}^m \to \mathbf{Z_2}$.

Es sencillo probar que existe una correspondencia biyectiva entre el conjunto de las funciones de Boole de m variables y el de las palabras binarias de longitud 2^m. Si denotamos por B_m el conjunto de todas las funciones de Boole de m variables, se tiene que $|B_m| = 2^{2^m}$.

En B_m se define una suma:

dadas $f, g \in B_m$

$$(f+g)(x_1, ..., x_m) = f(x_1, ..., x_m) + g(x_1, ..., x_m)$$

con la que pasa a ser un grupo abeliano.

Se define también una multiplicación escalar :

dados $t \in \mathbf{Z_2}$ y $f \in B_m$

$$(tf)(x_1, ..., x_m) = tf(x_1, ..., x_m)$$

y B_m pasa a ser un $\mathbf{Z_2}$-espacio vectorial.

(7.2) **Definición**. Un monomio de Boole en las variables $x_1, ..., x_m$ es una expresión de la forma:

$$p = x_{i_1} x_{i_2} ... x_{i_s}$$

(se incluye $1 = x_1^0 x_2^0 .... x_m^0$).

La forma reducida de p es obtenida aplicando las reglas:

$$x_i x_j = x_j x_i, \; x_i^2 = x_i$$

hasta que los factores son distintos. El grado de un monomio de Boole es el grado de su forma reducida , que es el número de variables que contiene.

Un polinomio de Boole es una combinación lineal de monomios de Boole con coeficientes en $\mathbf{Z_2}$. Un polinomio de Boole está en forma reducida si cada monomio suyo está en forma reducida. El grado de un polinomio de Boole es el grado de su forma reducida y este es el mayor grado de los monomios que la forman . Usualmente los polinomios de

Boole estarán en forma reducida. Denotaremos con P_m al conjunto de todos los polinomios de Boole en m variables.

Es claro que el número de monomios de Boole en m variables de grado k es $\binom{m}{k}$. Así el cardinal del conjunto de todos los monomios en m variables es:

$$\binom{m}{0} + \binom{m}{1} + \binom{m}{2} + ... + \binom{m}{m} = 2^m$$

Por lo tanto $|P_m| = 2^{2^m}$.

(7.3) **Teorema**. La aplicación de P_m en B_m que asocia a un polinomio de Boole F la función de Boole f dada por:

$$f(u_1, u_2, ..., u_m) = F(u_1, u_2, ..., u_m)$$

es un isomorfismo de $\mathbf{Z_2}$-espacios vectoriales.

Dem. Es sencillo probar que dicha aplicación es lineal. Por otra parte ambos espacios vectoriales tienen igual orden, así es suficiente probar que cada función de Boole viene inducida por un polinomio de Boole. Lo haremos por inducción sobre m.

Si $m = 1$, las funciones de Boole en 1 variable vienen dadas por las palabras binarias de longitud 2 : 00,11,01,10 las cuales son inducidas por los polinomios de Boole: 0,1,x_1 y $1 + x_1$ respectivamente.

Supongamos que las funciones de Boole en $m - 1$ variables vienen inducidas por polinomios de Boole. Sea $f \in B_m$. Entonces:

$$f(x_1, ..., x_m) = f(0, x_2, ..., x_m) + \pi_1(x_1, ..., x_m)(f(1, x_2, ..., x_m) - f(0, x_2, ..., x_m))$$

con $\pi_1(x_1, ..., x_m) = x_1$.

Definamos las siguientes funciones de Boole en $m - 1$ variables:

$$f_o(x_2, ..., x_m) = f(0, x_2, ..., x_m)$$

$$f_1(x_2, ..., x_m) = f(1, x_2, ..., x_m)$$

Por hipótesis de inducción, existen polinomios de Boole en $m-1$ variables F_o, F_1 tales que :

$$f_o(u_2, ..., u_m) = F_o(u_2, ..., u_m)$$

$$f_1(u_2, ..., u_m) = F_1(u_2, ..., u_m)$$

cualesquiera que sean $u_i \in \mathbf{Z_2}$

La función de Boole π_1 está inducida por el polinomio de Boole x_1. Así el polinomio de Boole :

$$F(x_1, ..., x_m) = F_o(x_2, ..., x_m) + x_1(F_1(x_2, ..., x_m) - F_o(x_2, ..., x_m))$$

induce la función de Boole f.

Ejercicio. Sea f la función de Boole dada por 01100011. Hallar el polinomio de Boole F que la induce.

Consideremos el siguiente diagrama en el que disponemos las posibles 3-tuplas en columnas, ordenadas según la descomposición binaria de los números 0,1,2..,7. Debajo de cada 3-tupla figura la valoración que f toma en dicha 3-tupla

x_1	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_3	0	1	0	1	0	1	0	1
f	0	1	1	0	0	0	1	1

El diagrama análogo para f_o dada por: $f_o(x_2, x_3) = f(0, x_2, x_3)$ es:

x_2	0	0	1	1
x_3	0	1	0	1
f_o	0	1	1	0

y para f_1 dada por $f_1(x_2, x_3) = f(1, x_2.x_3)$ es:

x_2	0	0	1	1
x_3	0	1	0	1
f_1	0	0	1	1

Sabemos que : $F(x_1, x_2, x_3) = F_o(x_2, x_3) + x_1(F_1(x_2, x_3) - F_o(x_2, x_3))$

y las afirmaciones sucesivas.

Cometiendo abuso de lenguaje escribiremos:

$01100011 = 0110 + x_1(0011 - 0110) = 0110 + x_1 0101 = 01 + x_2(10 - 01) + x_1(01 + x_2(01 - 01)) = 01 + x_2 11 + x_1 01 = x_3 + x_2 + x_1 x_3$, que es el polinomio de Boole buscado.

(7.4) **Definición**. Sea m un entero positivo y $0 \leq r \leq m$. Se define el **código de Reed-Muller** $R(r, m)$ de longitud 2^m y orden r, como el conjunto de las palabras binarias de longitud 2^m asociadas a polinomios de Boole de grado menor o igual que r.

Notar que $R(r,m)$ es un código lineal.

Ejemplos.

$R(0,m) = \{0...0, 1...1\}$

$R(m,m) = \mathbf{Z_2}^{2^m}$

$R(1,3) = \{00000000, 00001111, 00110011, 01010101,$

00111100,01011010,01100110, 01101001,

11111111, 11110000,11001100,10101010,

11000011,10100101,10011001,10010110$\}$

dado que los polinomios de Boole en 3 variables de grado menor o igual que 1 son:

$0, x_1, x_2, x_3, x_1+x_2, x_1+x_3, x_2+x_3, x_1+x_2+x_3, 1, 1+x_1, 1+x_2, 1+x_3, 1+x_1+x_2, 1+x_1+x_3, 1+x_2+x_3, 1+x_1+x_2+x_3$

(7.5) **Proposición**. Sea $F(x_1,...,x_m) = x_m + G(x_1,...,x_{m-1})$, donde $G(x_1,...,x_{m-1})$ es un polinomio de Boole. Entonces la función de Boole inducida por F toma los valores 0 y 1 el mismo número de veces, es decir, 2^{m-1} veces.

Dem. Todos los elementos de $\mathbf{Z_2}^m$ se pueden obtener a partir de los de $\mathbf{Z_2}^{m-1}$, añadiendo al final un 1 o un 0. Si $G(x_1,...,x_{m-1}) = 0$, entonces $F(x_1,...,x_{m-1},0) = 0$ y $F(x_1,...,x_{m-1},1) = 1$. Si $G(x_1,...,x_{m-1}) = 1$ entonces $F(x_1,...,x_{m-1},0) = 1$ y $F(x_1,...,x_{m-1},1) = 1+1 = 0$. Así la mitad toma valor 0 y la otra mitad valor 1.

(7.6) **Proposición**. Todas las palabras de $R(1,m)$ tienen peso 2^{m-1} excepto la 00...0 y la 11...1.

Dem. $R(1,m)$ está formado por palabras que, a excepción de 00...0 y 11...1, están inducidas por polinomios de Boole de la forma :

$$x_t + G(x_1,...,x_{t-1},x_{t+1},...,x_m)$$

Por el resultado anterior, sabemos que las correspondientes palabras tienen 2^{m-1} ceros y 2^{m-1} unos.

(7.7) **Proposición**. $R(r,m)$ tiene longitud 2^m y dimensión

$$k = 1 + \binom{m}{1} + ... + \binom{m}{r}$$

Dem. Sabemos que dicho código es isomorfo, como espacio vectorial, al formado por los polinomios de Boole de grado menor o igual que r, que tiene como base la formada por los monomios de grado menor o igual que r.

Notar que la tasa de información de dicho código es:

$$R = (\log_2 2^k)/n = k/2^m$$

Construcción de Plotkin.

(7.8) **Definición**. Sea C_1 un (n, m_1, d_1)-código lineal y C_2 un (n, m_2, d_2)-código lineal sobre un cuerpo F. Se define:

$$C_1 \bigoplus C_2 = \{u(u+v) | u \in C_1, v \in C_2\}$$

donde $u(u+v)$ es la yuxtaposición de las palabras u y $u+v$.

$C_1 \bigoplus C_2$ es un código lineal, ya que :

$u(u+v)+u'(u'+v') = (u+u')(u+u'+v+v') \in C_1 \bigoplus C_2$ y $t(u(u+v)) = tu(tu+tv) \in C_1 \bigoplus C_2$.

Como $u(u+v) = u(u'+v') \Longleftrightarrow u = u'$ y $v = v'$, se sigue que $|C_1 \bigoplus C_2| = m_1 m_2$.

(7.9) **Proposición**.$C_1 \bigoplus C_2$ es un $(2n, m_1 m_2, d')$-código con $d' = \text{mín}(2d_1, d_2)$.

Dem. Sean $x_1 = u_1(u_1 + v_1), x_2 = u_2(u_2 + v_2)$ con $u_1, u_2 \in C_1$ y $v_1, v_2 \in C_2$. Si $v_1 = v_2$ entonces:

$$d(x_1, x_2) = w((u_1 - u_2)(u_1 - u_2)) = 2w(u_1 - u_2) = 2d(u_1, u_2) \geq 2d_1$$

Si $v_1 \neq v_2$ entonces:

$d(x_1, x_2) = w(u_1 - u_2) + w((u_1 - u_2) + (v_1 - v_2)) = d(u_1 - u_2, \bar{0}) + d(u_1 - u_2, v_2 - v_1) \geq d(v_2 - v_1, \bar{0}) = w(v_2 - v_1) = d(v_2, v_1) \geq d_2$

Así $d(x_1, x_2) \geq$ mín $(2d_1, d_2)$. Veamos ahora que dicho mínimo se alcanza.

Si $\text{mín}(2d_1, d_2) = 2d_1$ tomar $u_1, u_2 \in C_1$ con $d(u_1, u_2) = d_1$ y considerar: $x_1 = u_1(u_1 + \bar{0}), x_2 = u_2(u_2 + \bar{0})$ con $v \in C_2$. Entonces:

$$d(x_1, x_2) = w((u_1 - u_2)(u_1 - u_2)) = 2d_1$$

Si mín$(2d_1, d_2) = d_2$ tomar $v_1, v_2 \in C_2$ con $d(v_1, v_2) = d_2$ y considerar $x_1 = \bar{0}(\bar{0} + v_1), x_2 = \bar{0}(\bar{0} + v_2)$, entonces:

$$d(x_1, x_2) = d(v_1, v_2) = d_2$$

.

Notas.

1. dim($C_1 \bigoplus C_2$) = dimC_1 + dimC_2.

En efecto, si $|F| = q$, dimC$_1 = k_1$,dimC$_2 = k_2$, como $|C_1 \bigoplus C_2| = m_1 m_2 = q^{k_1} q^{k_2} = q^{k_1+k_2}$, se sigue la afirmación.

2. Considerar el polinomio de Boole en tres variables

$F(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3 = x_1(x_2 + x_3) + x_2x_3 = x_1G(x_2, x_3) + H(x_2, x_3)$

Si se piensa en $x_2 + x_3$ como polinomio de Boole en dos variables, le corresponde la palabra binaria 0110, que llamaremos x_G, supuesto que llamemos x a la que corresponde a F. A $x_1G(x_2, x_3)$ le corresponde 00000110 es decir $0x_G$. Si se piensa en x_2x_3, como polinomio en dos variables le corresponde 0001, que sería denotada por x_H. Como polinomio en tres variables le correspondería 00010001, que sería x_Hx_H. Así la palabra que correspondería a F sería:

$$x = x_F = 0x_G + x_Hx_H = x_H(x_H + x_G)$$

.

(7.10) **Teorema**. Sea $0 < r < m$, entonces:

$$R(r, m) = R(r, m - 1) \bigoplus R(r - 1, m - 1)$$

Dem. Veamos que $R(r, m) \subseteq R(r, m - 1) \bigoplus R(r - 1, m - 1)$. Sea $x \in R(r, m)$, dada por el polinomio de Boole F de grado menor o igual que r. Escribamos:

$$F(x_1, ..., x_m) = x_1G(x_2, ..., x_m) + H(x_2, ..., x_m)$$

donde $G(x_2, ..., x_m)$ tiene grado menor o igual que $r - 1$ y $H(x_2, ..., x_m)$ tiene grado menor o igual que r.

Si x_G es la palabra binaria correspondiente a G se tiene que $x_G \in R(r-1, m-1)$. Sea x_H la palabra binaria correspondiente a H, entonces $x_H \in R(r, m-1)$. Así a $x_1 G(x_2, ..., x_m)$ le corresponde la palabra $0x_G$ y a H la palabra $x_H x_H$. Por tanto:

$$x = x_F = 0x_G + x_H x_H = x_H(x_H + x_G) \in R(r, m-1) \bigoplus R(r-1, m-1)$$

Para probar la igualdad, veamos que ambos subespacios tienen la misma dimensión. En efecto:

$$\dim R(r,m) = 1 + \binom{m}{1} + ... + \binom{m}{r}$$

Sabemos que : $\binom{m}{r} = \binom{m-1}{r} + \binom{m-1}{r-1}$, por lo tanto:

$\dim R(r,m) = 1 + \binom{m-1}{1} + \binom{m-1}{0} + \binom{m-1}{2} + ... + \binom{m-1}{r} + \binom{m-1}{r-1} = 1 + \binom{m-1}{1} + ... + \binom{m-1}{r} + 1 + \binom{m-1}{1} + \binom{m-1}{r-1} = \dim R(r, m-1) + \dim R(r-1, m-1) = \dim(R(r, m-1) \bigoplus R(r-1, m-1))$.

(7.11) **Corolario**. El código de Reed-Muller $R(m-1, m)$ está formado por todas las palabras binarias de longitud 2^m y peso par. Por tanto si $r < m$, $R(r, m)$ sólo tiene palabras de peso par.

Dem. $R(0,1) = \{00, 11\}$, sólo tiene palabras de peso par (y las tiene a todas). Suponer que $R(m-2, m-1)$ sólo tiene palabras de peso par. Entonces:

$R(m-1, m) = R(m-1, m-1) \bigoplus R(m-2, m-1) = \mathbf{Z_2}^{2^{m-1}} \bigoplus R(m-2, m-1)$.

Si $x \in R(m-1, m)$ entonces $x = y(y+z) = yy + 0z$ con $yy \in \mathbf{Z_2}^{2^m}$, $z \in R(m-2, m-1)$.

Por hipótesis de inducción, $w(0z)$ es par y :

$$w(x) = w(yy) + w(0z) - 2w(yy \bigcap 0z)$$

que es par.

Sea ahora E_{2^m} el conjunto de todas las palabras binarias de longitud 2^m y peso par. Dicho conjunto es un subespacio de $\mathbf{Z_2}^{2^m}$ con $\dim E_{2^m} = 2^m - 1$ (ver ejercicio 17 de la Lección 4). Como por lo anterior tenemos que:

$$R(m-1, m) \subseteq E_{2^m}$$

y

$$\dim R(m-1,m) = 1 + \binom{m}{1} + ... + \binom{m}{m-1} = 2^m - 1$$

deben coincidir. Si $r < m$ entonces $R(r,m) \subseteq R(m-1,m)$ y la afirmación final se sigue inmediatamente.

Ejemplo. $R(2,3)$ está formado por todas las palabras de longitud 8 y peso par. Una matriz generadora es :

$$G = \begin{pmatrix} 10000001 \\ 01000001 \\ 00100001 \\ 00010001 \\ 00001001 \\ 00000101 \\ 00000011 \end{pmatrix}$$

que es matriz generadora del ASCII con control de paridad.

(7.12) **Teorema**. $R(r,m)$ tiene distancia mínima 2^{m-r}, luego sus parámetros son:

$$(2^m, 1 + \binom{m}{1} + ... + \binom{m}{r}, 2^{m-r})$$

.

Dem. Si $m = 1$ tenemos $R(0,1) = \{00, 11\}$, $d(R(0,1)) = 2 = 2^{1-0}$ y $R(1,1) = \mathbf{Z_2}^2 = \{00, 11, 01, 10\}$ y $d(R(1,1)) = 1 = 2^{1-1}$.

Suponer cierta la afirmación para $m-1$. Notar que si $r = 0$ entonces $R(0,m) = \{0...0, 1...1\}$, así $d(R(0,m) = 2^m = 2^{m-0}$ y si $r = m$ $R(m,m) = \mathbf{Z_2}^{2^m}$ y $1 = d(\mathbf{Z_2}^{2^m}) = 2^{m-m}$. Así puede suponerse que $0 < r < m$. En tal caso, sabemos que $R(r,m) = R(r,m-1) \bigoplus R(r-1,m-1)$ y así :

$d(R(r,m)) = \text{mín}\{2d(R(r,m-1)), d(R(r-1,m-1))\} = \text{mín}\{22^{m-r-1}, 2^{m-r}\} = 2^{m-r}$.

Los códigos de Reed-Muller desde un punto de vista geométrico.

Recordemos que si S es un subespacio de $(\mathbf{Z}/2\mathbf{Z})^m$ con dimension igual a k, S es un código lineal y si H es una matriz de control de S, $x_1x_2...x_n \in S$ si y solo si $H \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (0)$.

H es una matriz $(m-k) \times m$ y el código S está formado por las soluciones de un sistema homogéneo de $m-k$ ecuaciones y m incógnitas con rango $m-k$. Las coclases de

S son de la forma $b+S$ con $b \in (\mathbf{Z}/2\mathbf{Z})^m$ y $x \in b+S$ si y solo si $x-b \in S$ si y solo si

$$H\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = H\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

es decir los elementos de $b+S$ son precisamente las soluciones de un sistema de $m-k$ ecuaciones en m incógnitas con rango $m-k$.

En términos geométricos nos referiremos a $(\mathbf{Z}/2\mathbf{Z})^m$ como $EG(m,2)$. Si $\dim S = k$, la coclase $b+S$ se dirá k-plano. Los 0-planos son de la forma : $b+\{0\} = \{b\}$ y se dicen puntos de $EG(m,2)$. Los 1-planos son de la forma $b+\{\lambda c\}$ y se dicen rectas. Así las rectas tienen exactamente dos puntos. Los $m-1$-planos se dicen hiperplanos. Concretamente, un subconjunto de $EG(m,2)$ es un k-plano si y solo si es el conjunto de soluciones de un sistema de $m-k$ ecuaciones lineales en m incógnitas de rango $m-k$.

Ejemplo. Consideremos $EG(3,2)$. Existen $2^3 = 8$ puntos y $\binom{8}{2} = 28$ rectas. Los 2-planos son de la forma: $b+\{\lambda_1 c_1 + \lambda_2 c_2\} = \{b, b+c_1, b+c_2, b+c_1+c_2\}$, con (c_1, c_2) libre. Notar que los tres primeros vectores son arbitrarios pero el cuarto es la suma de los tres. Cada tres puntos distintos determinan un plano, que a su vez viene determinado por cualesquiera 3 de los 4 puntos que tiene. Así hay $\binom{8}{3} / \binom{4}{3} = 14$ planos. Notar que por ejemplo $\{000, 001, 010, 111\}$ no es un plano.

Consideremos el diagrama de una función de Boole en tres variables:

x_1	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_3	0	1	0	1	0	1	0	1
f	0	1	1	0	0	0	1	1

La palabra 01100011 se puede considerar como la función característica (o vector característico) asociada a $\{001, 010, 110, 111\}$ Más generalmente, podemos asociar a cada palabra binaria de longitud 2^m, no solo un polinomio de Boole en m variables, sino un subconjunto de $EG(m,2)$. Además dado $p(x_1, ...x_m)$ polinomio de Boole, se le asocia el subconjunto de $EG(m,2)$:

$$F = \{x_1...x_m | p(x_1, ..., x_m) = 1\}$$

que es el mismo que el asociado a la palabra binaria de longitud 2^m correspondiente.

Establezcamos la notación siguiente:

1) Dada la palabra binaria $a = a_1...a_n$ $(n = 2^m)$ denotaremos con p_a al polinomio de Boole correspondiente y con F_a al subconjunto de $EG(m, 2)$ para el que a es vector característico.

2) Dado un polinomio de Boole $p(x_1, ..., x_m)$, denotaremos con a_p a la palabra asociada y con F_p al subconjunto asociado $(F_p = F_{a_p})$.

3) Dado $F \subseteq EG(m, 2)$, (que normalmente va a ser un plano), denotaremos con a_F al vector característico de F y con p_F al polinomio de Boole asociado. Observar que $w(a_F) = |F|$ y que $a_p = a_{F_p}$ (es decir toda palabra binaria a de longitud 2^m es vector característico del conjunto de m-tuplas en que el polinomio de Boole asociado a dicha palabra se valora 1.)

Vamos a tratar de describir los códigos de Reed-Muller en términos de subconjuntos de $EG(m, 2)$.

Un hiperplano de $EG(m, 2)$ es el conjunto de soluciones de una única ecuación lineal en las variables $x_1, ..., x_m$:

$$a_1x_1 + ... + a_mx_m = e$$

ó

$$a_1x_1 + ... + a_mx_m - e + 1 = 1$$

donde $e = 0, 1$.Así los hiperplanos están asociados a polinomios lineales no constantes

$$p(x_1, ..., x_m) = a_1x_1 + ... + a_mx_m - e + 1$$

(7.13) **Teorema**. Si F es un $(m-k)$-plano en $EG(m, 2)$, el correspondiente polinomio de Boole p_F tiene grado k.

Dem.Sabemos que $x_1...x_m \in F$ si y solo si $x_1...x_m$ satisface un sistema de k ecuaciones lineales en m variables con rango k, lo que puede ser escrito en la forma:

$$l_1(x_1, ..., x_m) = 1$$

.....

$$l_k(x_1, ..., x_m) = 1$$

Luego $x_1...x_m$ es solución de este sistema si y solo si lo es de :

$$\sqcap l_i(x_1, ..., x_m) = 1$$

Notar que el polinomio de la izquierda tiene grado k.

Nota El recíproco del resultado anterior no es cierto. Existen polinomios de Boole cuyos correspondientes subconjuntos no son planos (de cualquier dimensión).

Sin embargo el subconjunto F_p asociado a $p = x_{i_1}...x_{i_s}$ de grado s , es un $(m-s)$-plano, pues es la intersección de los hiperplanos : $x_{i_1} = 1, \ldots, x_{i_s} = 1$.

Recordar que si p, q son polinomios de Boole,se tiene: $a_{p+q} = a_p + a_q$. Así si f es un polinomio de Boole de grado s y $f = \sum p_i$, entonces $a_f = \sum a_{p_i}$. Por lo anterior a_{p_i} es el vector característico de un plano de dimensión $m - \delta(p_i) \geq m - s$. De ahí que a_f es la suma de vectores característicos de planos de dimensión al menos $m - \delta(f)$. Así:

(7.14) **Teorema**. El código de Reed-Muller $R(r, m)$ está generado por los vectores característicos de todos los planos de dimensión al menos $m - r$.

Descodificando los códigos de Reed-Muller

Una de las propiedades de los códigos de Reed-Muller es la facilidad con que pueden descodificarse. Sabemos que una palabra de $R(r, m)$ procede de un polinomio de Boole: $p(x_1, ..., x_m) = \sum_{s=0}^{r} \sum_{i_1,...,i_s} a_{i_1...i_s} x_{i_1}...x_{i_s}$

de grado a lo más r. Así se tiene:

$a_p = \sum_{s=0}^{r} \sum_{i_1,...,i_s} a_{i_1...i_s} a_{x_{i_1}...x_{i_s}}$

Estamos interesados en encontrar la manera de calcular los coeficientes del tipo $a_{k_1...k_r}$. Previamente hacemos las siguientes observaciones:

i) Si F y G son subconjuntos de $EG(m, 2)$, entonces:

$a_F.a_G = 0 \Longleftrightarrow |F \cap G|$ es par.

Es claro que $a_F.a_G = 0 \Longleftrightarrow w(a_F \cap a_G)$ es par. Ahora bien, como $a_F \cap a_G = a_{F \cap G}$, se tiene que $w(a_F \cap a_G) = w(a_{F \cap G}) = |F \cap G|$.

ii) Sean $F = b + S$ y $G = c + T$, planos de $EG(m, 2)$. Entonces ó $F \cap G = \emptyset$ ó $F \cap G = x + S \cap T$ con $x \in F \cap G$.

Si $F \cap G$ no es vacío, sea $x \in F \cap G$. Así $b + S = x + S$ y $c + T = x + T$; si $y \in F \cap G$ $y = x + s = x + t$ con $s \in S, t \in T$ y así $y \in x + S \cap T$. El otro contenido es claro.

iii) Todos los planos de $EG(m,2)$, excepto los puntos, tienen un número par de elementos.

Si $F = b + S$ y dim $S = k$ entonces $|F| = |S| = 2^k$.

Volvemos a la obtención de $a_{k_1 \ldots k_r}$.

Sea $\{j_1, .., j_{m-r}\} = \{k_1, ..., k_r\}^c$el complementario relativo a $\{1, ..., m\}$.

Consideremos $a_p.a_{x_{j_1} \ldots x_{j_{m-r}}}$. Podemos considerar el producto con cada término de a_p separadamente. Sabemos que :

$a_{x_{i_1} \ldots x_{i_s}}.a_{x_{j_1} \ldots x_{j_{m-r}}} = 0 \Longleftrightarrow |F_{x_{i_1} \ldots x_{i_s}} \cap F_{x_{j_1} \ldots x_{j_{m-r}}}| = |F_{x_{i_1} \ldots x_{i_s} x_{j_1} \ldots x_{j_{m-r}}}|$ es par. Pero por un comentario anterior, el último cardinal es par salvo que el plano sea un punto , lo que sucede si y solo si $\{i_1, ..., i_s, j_1, ..., j_{m-r}\} = \{1, ..., m\}$, es decir si y solo si $s = r$ y $\{i_1, ..., i_r\} = \{j_1, ..., j_{m-r}\}^c = \{k_1, ..., k_r\}$. De ahí que al realizar el producto se obtenga:

$$a_p.a_{x_{j_1} \ldots x_{j_{m-r}}} = a_{k_1 \ldots k_r}$$

Esto es solamente un cálculo de dicho coeficiente. Podemos generalizar el proceso tomando $a_p.a_{b+Fx_{j_1} \ldots x_{j_{m-r}}}$ donde $b+Fx_{j_1} \ldots x_{j_{m-r}}$ es un trasladado del plano $Fx_{j_1} \ldots x_{j_{m-r}}$. En este caso tenemos:

$a_{x_{i_1} \ldots x_{i_s}}.a_{b+Fx_{j_1} \ldots x_{j_{m-r}}} = 0 \Longleftrightarrow |F_{x_{i_1} \ldots x_{i_s}} \cap (b + Fx_{j_1} \ldots x_{j_{m-r}})|$ es par. Si denotamos con $N = F_{x_{i_1} \ldots x_{i_s}} \cap (b + Fx_{j_1} \ldots x_{j_{m-r}})$, N se reduce a un punto si y solo si $s = r$ y $\{i_1, ..., i_r\} = \{j_1, ..., j_{m-r}\}^c = \{k_1, ..., k_r\}$.

Puesto que existen 2^{m-r} trasladados distintos del r-plano $Fx_{j_1} \ldots x_{j_{m-r}}$, el conjunto de las m-tuplas binarias aparece particionado en 2^{m-r} subconjuntos (disjuntos dos a dos) cada uno de ellos de cardinal $|S|$. Los vectores característicos asociados a tales subconjuntos tienen tantos unos como $|S|$. Al hacer el producto interno de dichos vectores con a_p, sabemos que el resultado es $a_{k_1 \ldots k_r}$. Habrá 2^{m-r} expresiones para dicho coeficiente y cada una de ellas contiene diferentes coordenadas de a_p. Como la distancia mínima de $R(r,m)$ es 2^{m-r}, si a lo más se han producido $(1/2)(2^{m-r} - 1)$ errores ,a lo sumo habrá $(1/2)(2^{m-r} - 1)$ expresiones incorrectas , luego podremos determinar el valor correcto de dicho coeficiente por lógica mayoritaria.

Ejemplo. Consideremos el código de Reed-Muller $R(2,4)$. Dispongamos , como es

habitual, las 4-tuplas binarias en la forma:

$$\begin{array}{cccccccccccccccc} x_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ x_2 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ x_3 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ x_4 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}$$

Sea $p = a_0 + a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 + a_{12}x_1x_2 + a_{13}x_1x_3 + a_{14}x_1x_4 + a_{23}x_2x_3 + a_{24}x_2x_4 + a_{34}x_3x_4$. Queremos determinar el coeficiente a_{13}. Notar que $\{1,3\}^c = \{2,4\}$ y que $F_{x_2x_4} = \{0101, 0111, 1101, 1111\}$. Los $2^{4-2} = 4$ trasladados de dicho plano son :

$$\{0101, 0111, 1101, 1111\}$$

$$\{0000, 0010, 1000, 1010\}$$

$$\{0100, 0110, 1100, 1110\}$$

$$\{0001, 0011, 1001, 1011\}$$

y los vectores característicos correspondientes:

$$0000010100000101$$

$$1010000010100000$$

$$0000101000001010$$

$$0101000001010000$$

Haciendo los productos de cada uno de ellos con la palabra recibida $c_1c_2....c_{16}$, se obtiene:

$$a_{13} = c_6 + c_8 + c_{14} + c_{16}$$

$$a_{13} = c_1 + c_3 + c_9 + c_{11}$$

$$a_{13} = c_5 + c_7 + c_{13} + c_{15}$$

$$a_{13} = c_2 + c_4 + c_{10} + c_{12}$$

Así, si no ha ocurrido más de un error en los c_i (recordar que la distancia mínima de $R(2,4)$ es 4) podemos recobrar el valor de a_{13} tomando el valor más repetido en los lados derechos de estas expresiones. De igual forma se van obteniendo los otros coeficientes a_{ij}. Después, podemos restar al polinomio p el polinomio $a_{12}x_1x_2 + a_{13}x_1x_3 + a_{14}x_1x_4 + a_{23}x_2x_3 + a_{34}x_3x_4$ para obtener $q = a_0 + a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4$, que es el polinomio asociado a una palabra de $R(1,4)$. Se repite el proceso para determinar los coeficientes a_i.

Ejercicios

1. Hallar los polinomios de Boole que inducen las funciones de Boole siguientes:

i) 00101001 ii)0111001000001110

2. Hallar los polinomios de Boole que inducen las funciones de Boole siguientes:

i) 11011001 ii)00001111 iii) 10100111iv)1101111000011001.

3. Sea C_1 un (n, k_1, d_1)-código lineal y C_2 un (n, k_2, d_2)-código lineal sobre un mismo cuerpo F. Considerar el código $C_1 \oplus C_2$ de la construcción de Plotkin. Si G_1 es matriz generadora de C_1 y G_2 matriz generadora de C_2, razonar que $\begin{pmatrix} G_1 & G_1 \\ O & G_2 \end{pmatrix}$ es matriz generadora de $C_1 \oplus C_2$.

4. Describir los códigos de Reed-Muller $R(r, m)$ para $m = 1, r = 0$ y para $m = 2, r = 0, 1$. Comprobar que $R(0, 1)$ es autodual y que $R(0, 2)$ y $R(1, 2)$ son duales uno del otro.

5. Demostrar que los códigos de Reed-Muller $R(m - r - 1, m)$ y $R(r, m)$ son duales uno del otro.

6. Hallar el coeficiente a_{34} del polinomio de Boole que va asociado a una palabra de longitud 16 de $R(2, 4)$, que se recibe como : 0101000110000001.

7. Hallar el coeficiente a_{13} del polinomio de Boole que va asociado a una palabra de longitud 16 de $R(2, 4)$, que se recibe como 1101111000011001.

8. ¿Qué códigos de Reed-Muller son autoduales?.

9. Demostrar que existen polinomios de Boole $p(x_1, ..., x_m)$ de grado $m - k$ cuyos subconjuntos correspondientes F_p de $EG(m, 2)$ no son planos.

10. Demostrar que existen $2(2^m - 1)$ hiperplanos en $EG(m, 2)$.

11. Hallar una matriz generadora del código de Reed-Muller $R(1, 3)$.

Lección 8. Códigos cíclicos

Una de las clases más importantes de códigos lineales es la clase de los códigos cíclicos. En general estos códigos son mucho mas fáciles de implementar y tienen una gran importancia práctica. Son también de considerable interés desde el punto de vista algebraico.

(8.1) **Definición**. Un código lineal C es un **código cíclico** si siempre que

$c_1c_2\ldots c_{n-1}c_n \in C$, se sigue que $c_nc_1c_2\ldots c_{n-1} \in C$.

Es conveniente cambiar la notación y numerar las coordenadas de 0 a $n-1$ en lugar de 1 a n.

(8.2) **Teorema**. Sea n un entero positivo y F un cuerpo (finito). Se define:

$$\phi : F^n \longrightarrow F[x]/(x^n-1)$$

mediante $\phi(a_0a_1...a_{n-1}) = a_0 + a_1x + ... + a_{n-1}x^{n-1} + (x^n-1)$. Se tiene:

i) ϕ es una aplicación lineal biyectiva entre ambos F-espacios vectoriales.

ii) $\phi(a_{n-1}a_0...a_{n-2}) = \phi(a_0a_1...a_{n-1})(x + (x^n-1))$

iii) Si C es un código lineal, $C \subseteq F^n$, C es cíclico si y solo si $\phi(C)$ es un ideal de $R_n = F[x]/(x^n-1)$.

Dem. Claramente es una aplicación lineal. Si $a_0a_1...a_{n-1}$ es tal que $a_0 + a_1x + ...a_{n-1}x^{n-1} + (x^n-1) = (x^n-1)$, necesariamente $a_0 + a_1x + ...a_{n-1}x^{n-1}$ debe ser el polinomio nulo, así $a_0 = a_1 = ... = a_{n-1} = 0$. Por lo tanto ϕ es inyectiva. Además si $g(x) + (x^n-1) \in R_n$, por el algoritmo de la división, existen $q(x), r(x)$ de forma que $g(x) = (x^n-1)q(x) + r(x)$, con $r(x) = 0$ ó grado $r(x) < n$. Por lo tanto $g(x) + (x^n-1) = r(x) + (x^n-1)$ y ϕ es suprayectiva.

ii)$\phi(a_0a_1...a_{n-1})(x+(x^n-1)) = (a_0+a_1x+...+a_{n-1}x^{n-1}+(x^n-1))(x+(x^n-1)) = a_0x+a_1x^2+...+a_{n-2}x^{n-1}+a_{n-1}x^n+(x^n-1)$. Como $a_{n-1}x^n+(x^n-1) = a_{n-1}+(x^n-1)$ se concluye que dicho producto coincide con $a_0x+a_1x^2+...+a_{n-2}x^{n-1}+a_{n-1}+(x^n-1) = \phi(a_{n-1}a_0...a_{n-2})$.

iii) Si C es cíclico y $a_0a_1...a_{n-1} \in C$, por ii) se tiene que $\phi(a_0a_1...a_{n-1})(x+(x^n-1)) = \phi(a_{n-1}a_0...a_{n-2}) \in \phi(C)$. Por i) sabemos que $\phi(C)$ es un subespacio de R_n, luego si $t \in F$ y $a_0a_1...a_{n-1} \in C$ se tiene que:

$t\phi(a_0a_1...a_{n-1}) = (t + (x^n - 1))(a_0 + a_1x + ... + a_{n-1}x^{n-1} + (x^n - 1)) \in \phi(C)$ luego $(f(x) + (x^n - 1))(a_0 + a_1x + ... + a_{n-1}x^{n-1} + (x^n - 1)) \in \phi(C)$ cualquiera que sea $f(x) \in F[x]$. Recíprocamente, si $\phi(C)$ es un ideal de R_n y $a_0a_1...a_{n-1} \in C$, por ii) se sigue que $\phi(a_{n-1}a_0...a_{n-2}) \in \phi(C)$ luego, como ϕ es biyectiva, se tiene que $a_{n-1}a_0...a_{n-2} \in C$ y C es cíclico.

Atención. Cuando hablemos de polinomios en el código cíclico C nos estaremos refiriendo a las coclases de dichos polinomios módulo el ideal $(x^n - 1)$.

El problema es ahora describir los ideales en el anillo R_n . Primero observemos que todos son principales.

(8.3) **Proposición**. Sea R un anillo conmutativo y con unidad en el que cada ideal es principal. Entonces cualquier anillo cociente de R tiene las mismas propiedades.

Dem. Basta tener en cuenta que los ideales de un cociente R/I son de la forma J/I, con J ideal de R conteniendo a I.

Ejemplos.

1. $C = \{000, 101, 011, 110\}$ es cíclico.

2. $C = \{0000, 1001, 0110, 1111\}$ no es cíclico, pero es equivalente a un cíclico, intercambiando las terceras coordenadas con las cuartas.

3. Sea $R_3 = \mathbf{Z}/\mathbf{2Z}[x]/(x^3-1)$. Considerar el código $C = (1+x^2)$ en R_3. Multiplicando $1 + x^2$ por representantes de los 8 elementos de R_3 y reduciendo módulo $(x^3 - 1)$, se tiene:

$(1 + x^2)x = x + 1$

$(1 + x^2)x^2 = x^2 + x$

$(1 + x^2)(1 + x) = 1 + x^2 + x + x^3 = x + x^2$

$(1 + x^2)(1 + x^2) = 1 + x^2 + x^2 + x^4 = 1 + x$

$(1 + x^2)(x + x^2) = x + x^2 + x^3 + x^4 = x + x^2 + 1 + x = 1 + x^2$

$(1 + x^2)(1 + x + x^2) = 1 + x^2 + x + x^3 + x^2 + x^4 = x + x^4 = x + x = 0$

así aparecen $0, 1 + x, 1 + x^2, x + x^2$ y $C = \{000, 110, 101, 011\}$, citado en 1.

(8.4) **Teorema**. Sea C un código cíclico no cero en R_n. Entonces:

i) Existe un único polinomio mónico $g(x)$ del menor grado posible, perteneciendo a C (la coclase de dicho polinomio).

ii) $C = (g(x))$

iii) $g(x)$ divide a $x^n - 1$.

Dem. i) Sean $g(x)$ y $h(x)$ mónicos, $g(x) \neq h(x)$, pertenecientes a C, del menor grado posible. Entonces $g(x) - h(x)$ pertenece a C y tiene grado más pequeño, lo que no es posible, ya que se encontraría un polinomio mónico en C de grado menor que el de $g(x)$.

ii). Sea $f(x) \in C$, por el algoritmo de la división, se tiene: $f(x) = g(x)q(x) + r(x)$, luego $r(x) \in C$ y debe de ser $r(x) = 0$ pues en otro caso grad $r(x)$ <grad $g(x)$ y se llegaría a contradicción.

iii) De nuevo por el algoritmo de la división se tiene:

$$x^n - 1 = g(x)q(x) + r(x)$$

y módulo $(x^n - 1)$: $r(x) = -g(x)q(x)$ así $r(x) \in (g(x))$, luego debe ser $r(x) = 0$, y $g(x)$ divide a $x^n - 1$.

A dicho polinomio $g(x)$ se le llama **polinomio generador** del código cíclico.

(8.5) **Proposición**. Si $g(x) = g_o + g_1x + ... + x^r$ es el polinomio generador de un código cíclico C, entonces $g_o \neq 0$.

Dem. Suponer que $g_o = 0$, entonces:

$$x^{n-1}g(x) = g_1x^n + g_2x^{n+1} + ... + x^{n+r-1} = g_1 + g_2x + ... + x^{r-1}$$

que pertenecería a C, lo que no es posible.

(8.6) **Teorema**. Un polinomio mónico $g(x) \in F[x]$ es el polinomio generador de un código cíclico si y solo si $g(x)$ divide a $x^n - 1$.

Dem. En (8.4) hemos probado ya una implicación. Supongamos ahora que $g(x)$ divide a $x^n - 1$. Considerar el ideal generado por $g(x)$, (por la coclase de $g(x)$). Si existiera $f(x) \in (g(x))$, $f(x)$ mónico con grad $f(x)$ <grad $g(x)$, existiría $a(x) \in F[x]$ tal que:

$$f(x) + (x^n - 1) = (g(x) + (x^n - 1))(a(x) + (x^n - 1))$$

así $f(x) = a(x)g(x) + (x^n - 1)b(x)$ para algún $b(x) \in F[x]$. Como $g(x)$ divide a $x^n - 1$, se sigue que $g(x)$ divide a $f(x)$, lo que es una contradicción. Por tanto $g(x)$ es el polinomio generador del código cíclico $(g(x))$.

Así, para construir códigos cíclicos de longitud n, debemos de obtener primero la descomposición de $x^n - 1$ en factores irreducibles y listar los divisores de $x^n - 1$. A continuación para cada divisor formaremos el correspondiente ideal en R_n.

Notar que un código cíclico C puede tener otros polinomios que lo generen. Así en el ejemplo 3, C está generado por $1 + x^2$, pero el polinomio generador de C es $1 + x$.

Ejemplo.

Encontrar todos los códigos binarios cíclicos de longitud igual a 3.

$$x^3 - 1 = (x + 1)(x^2 + x + 1)$$

donde $x + 1$ y $x^2 + x + 1$ son irreducibles en $\mathbf{Z_2}[x]$. Los divisores de $x^3 - 1$ son:

$1, x + 1, x^2 + x + 1, x^3 - 1$. Los códigos en R_3 correspondientes son :$R_3, \{0, 1 + x, x + x^2, 1 + x^2\}, \{0, 1 + x + x^2\}, \{0\}$. Dichos códigos tienen sus correspondientes en $\mathbf{Z_2}^3$, a saber:

$$\mathbf{Z_2}^3, \{000, 110, 011, 101\}, \{000, 111\}, \{000\}$$

.

Ejercicios.

1. Comprobar que los códigos lineales siguientes son cíclicos:

i) El $(7,3)$-código binario con matriz generadora

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

ii)El $(4,2)$-código ternario con matriz generadora:

$$G = \begin{pmatrix} 1 & 0 & 2 & 0 \\ 1 & 1 & 2 & 2 \end{pmatrix}$$

2. Un $(9,3)$-código binario C está constituído por las palabras $c_0c_1c_2c_3c_4c_5c_6c_7c_8$ con $c_0 = c_1 = c_2, c_3 = c_4 = c_5, c_6 = c_7 = c_8$. Razonar que C es equivalente a un código cíclico y hallar el polinomio generador de este último.

3. i) Sea $x^n - 1 = g(x)h(x)$ y C un código cíclico de polinomio generador $g(x)$. Probar que $C \subseteq C^{\perp}$ si y solo si $\bar{h}(x)|g(x)$.

ii) Considerar un código binario cíclico de longitud 7 y polinomio generador $1 + x^2 + x^3 + x^4$, ¿es $C \subseteq C^{\perp}$?.

4. Razonar que el código binario de longitud n formado por todas las palabras de peso par (E_n) es un código cíclico de polinomio generador $x + 1$. Razonar que un código binario cíclico $C =< g(x) >$ contiene solo palabras de peso par si y solo si $x + 1$ divide a $g(x)$.

5. Determinar la tabla de líderes y de síndromes para el $(3,1)$-código binario generado por $g(x) = 1 + x + x^2$.

6. ¿Qué códigos cíclicos binarios de longitud 7 contienen a la palabra 0100111?.

7. Demostrar que si C es un código cíclico de polinomio generador $g(x)$ y polinomio de control $h(x)$ (es decir:$g(x)h(x) = x^n - 1$) y $(p(x), h(x)) = 1$, entonces $C = (p(x)g(x))$.

8. Razonar que si un código binario cíclico contiene una palabra de peso impar, entonces contiene a la palabra 1.

9. Sean C_1 y C_2 códigos cíclicos de longitud n sobre un mismo cuerpo F y polinomios generadores respectivos $g_1(x)$ y $g_2(x)$. Probar que $C_1 + C_2$ es también cíclico con polinomio generador m.c.d.$(g_1(x), g_2(x))$.

Lección 9. Matrices generadoras y de control de un código cíclico

(9.1) **Teorema**: Supongamos que $g(x)$ es el polinomio generador del código cíclico C. Si $g(x) = a_r x^r + a_{r-1}x^{r-1} + \ldots + a_0$ con $a_r = 1$ entonces dim $C = n - r$ y una matriz generadora G para C está dada por

$$\begin{pmatrix} g(x) \\ xg(x) \\ \\ \vdots \\ x^{n-r-1}g(x) \end{pmatrix} = \begin{pmatrix} a_o & a_1 & \ldots & a_r & 0 & \ldots & 0 \\ 0 & a_o & a_1 & \ldots & a_r & \ldots & 0 \\ & & & & & & \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & a_o & a_1 & \ldots & a_r \end{pmatrix} = G,$$

Dem. Las filas de G corresponden a los polinomios $g(x), xg(x), ..., x^{n-r-1}g(x)$, así que todas ellas pertenecen a C y claramente son linealmente independientes. Veamos que cualquier palabra de C es combinación lineal de dichas filas. Sea $c \in C$ correspondiente a $f(x)g(x)$. Por el algoritmo de la división $f(x) = h(x)q(x)+r(x)$ con $r(x) = 0$ ó grad$r(x) <$ grad$h(x)$ siendo $x^n - 1 = g(x)h(x)$. Entonces:

$f(x)g(x) = (x^n - 1)q(x) + r(x)g(x) = r(x)g(x)$ (mod$(x^n - 1)$)

y así $f(x)g(x)$ es combinación lineal de los polinomios $x^i g(x)$. Por lo tanto dim $C = n - r = n-$grad$g(x)$ y G es matriz generadora de C.

Si C es un (n, k)-código cíclico con polinomio generador $g(x)$ y $x^n - 1 = g(x)h(x)$, $h(x)$ es un polinomio mónico con grad $h(x) = k$. A dicho polinomio se le dice **polinomio de control** del código C. La razón para este nombre aparece en el siguiente resultado.

(9.2) **Teorema**. Sea C un código cíclico en R_n, con polinomio generador $g(x)$ y polinomio de control $h(x)$. Entonces un elemento $c(x)$ de R_n es una palabra código si y solo si $c(x)h(x) = 0$ en R_n .

Dem. En R_n $g(x)h(x) = x_n - 1 = 0$. Así, si $c(x) \in C$, $c(x) = a(x)g(x)$ para algún $a(x)$, luego $c(x)h(x) = a(x)g(x)h(x) = 0$ en R_n.

Recíprocamente suponer que $c(x)h(x) = 0$ en R_n. Por el algoritmo de la división se tiene: $c(x) = g(x)q(x) + r(x)$ con $r(x) = 0$ ó grad $r(x) < n - k$, entonces $r(x)h(x) = 0$ en R_n y si $r(x) \neq 0$ se tendría grad $r(x)h(x) < n - k + k = n$, lo que no es posible, así debe de ser $r(x) = 0$ y $c(x) \in C$.

En vista del resultado anterior y del hecho de que dim $(h(x)) = n - k =$ dim $C^{\perp}$, se podría pensar que $h(x)$ genera al código dual de C. En general esto no es así. El hecho

de que $c(x)h(x) = 0$ no equivale a afirmar que los correspondientes vectores de F^n sean ortogonales. Sin embargo la condición $c(x)h(x) = 0$ en R_n implica algunas relaciones de ortogonalidad utiles que conducen a una elección natural de una matriz de control.

Ejemplo. Considerar el (7,4)-código binario cíclico C generado por $g(x) = 1+x+x^3$. Como $x^7 - 1 = (x-1)(1+x+x^3)(1+x^2+x^3)$, se tiene que $h(x) = (x-1)(1+x^2+x^3) = 1 + x^2 + x^3 + x + x^3 + x^4 = 1 + x + x^2 + x^4$

Una matriz generadora del código es;

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

Considerar el código cíclico $C_1 = (h(x))$ de dimensión 3. Una matriz generadora de C_1 es :

$$G_1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Observar que la primera fila de G no es ortogonal con la tercera de G_1. Así C_1 no es $C^{\perp}$ Sin embargo escribamos las columnas de G_1 desde la última a la primera:

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

Observar que $GH' = (0)$ y así H es generadora de $C^{\perp}$, que es cíclico de polinomio generador $\bar{h}(x) = 1 + x^2 + x^3 + x^4$.

(9.3) **Teorema**. Sea C un (n,k)-código cíclico con polinomio de control $h(x) = b_o + b_1x + ... + b_kx^k$. Entonces :

i) Una matriz de control de C es:

$$H = \begin{pmatrix} b_k & b_{k-1} & \dots & b_o & 0 & \dots & 0 \\ 0 & b_k & b_{k-1} & \dots & b_o & \dots & 0 \\ & & & & & & \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & b_k & b_{k-1} & \dots & b_o \end{pmatrix}.$$

ii) $C^{\perp}$ es un código cíclico generado por el polinomio $\bar{h}(x) = b_k + b_{k-1}x + ... + b_o x^k$, al que llamaremos **polinomio recíproco** de $h(x)$ (si estamos en el caso no binario habrá que hacerlo mónico).

Dem. i) Sabemos que si $c(x) = c_o + c_1 x + ... + c_{n-1}x^{n-1}$ es de C, entonces $c(x)h(x) = 0$ en R_n, es decir existe $f(x) \in F[x]$ tal que $c(x)h(x) = f(x)(x^n - 1)$. Por lo tanto grad $(c(x)h(x)) = n+$grad $f(x) \leq n - 1 + k$ luego grad$f(x) \leq k - 1$ y los coeficientes de $x^k, x^{k+1}, ..., x^{n-1}$ en el producto $c(x)h(x)$ son ceros. Así:

$$c_o b_k + c_1 b_{k-1} + ... + c_k b_o = 0$$

$$c_1 b_k + c_2 b_{k-1} + ... + c_{k+1} b_o = 0$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$c_{n-k-1} b_k + c_{n-k} b_{k-1+} ... + c_{n-1} b_o = 0$$

Por lo tanto cualquier palabra del código es ortogonal al vector: $b_k b_{k-1} ... b_o 00...0$ y sus permutaciones circulares. Así las filas de H pertenecen a $C^{\perp}$. Como $b_k = 1$ es claro que dichas filas son linealmente independientes y hay $n - k$ filas, que es la dimensión de $C^{\perp}$. Concluimos que H es generadora de $C^{\perp}$.

ii) Si probamos que $\bar{h}(x)$ divide a $x^n - 1$, se seguirá que el código cíclico $(\bar{h}(x))$ tiene matriz generadora H y debe coincidir con $C^{\perp}$. Observar que : $x^k(b_o + b_1(1/x) + ... + b_k(1/x^k) = b_o x^k + b_1 x^{k-1} + ... + b_k = \bar{h}(x)$

Como $h(1/x)g(1/x) = (1/x)^n - 1$, tenemos: $x^k h(1/x) x^{n-k} g(1/x) = x^n (1/x)^n - x^n$, así $\bar{h}(x)$ divide a $x^n - 1$.

Interpretación polinómica de los síndromes.

Sea C un (n, k)-código cíclico. Obtendremos a continuación una matriz generadora de dicho código, de la forma: $[A\ I_k]$. Sea $g(x)$ el polinomio generador de C. Dividir x^{n-k+i} por $g(x)$ para $0 \leq i \leq k - 1$. Así $x^{n-k+i} = g(x)q_i(x) + r_i(x)$ con $r_i(x) = 0$ o el grado de $r_i(x)$ es estrictamente menor que $n - k$, de ahí que $x^{n-k+i} - r_i(x) = g(x)q_i(x)$ que pertenece a C y se obtiene un conjunto de k palabras código linealmente independientes. Así la matriz cuyas filas son estos elementos es generadora de C en la forma deseada y $H =$[$\mathrm{I}_{n-k} R'$] es matriz de control para C. El interés de haber elegido dicha matriz como

generadora de C, está en que permite obtener una interpretación polinómica muy útil del síndrome de un vector.

(9.4) **Teorema**. Sean $u(x)$ y $s(x)$ las representaciones polinómicas de un vector u y su síndrome s. Entonces $s(x)$ es el polinomio resto cuando $u(x)$ se divide por $g(x)$.

Dem. Sea $u(x) = a_0 + a_1x \ldots + a_{n-1}x^{n-1}$ y $H = [I_{n-k}\, R']$. Notar que las $n-k$ primeras columnas de H corresponden a los polinomios $1, x, .., x^{n-k-1}$ y las restantes a las filas de R, es decir : $r_o(x), r_1(x), .., r_{k-1}(x)$, así:

$s(x) = a_o + a_1x \ldots + a_{n-k-1}x^{n-k-1} + a_{n-k}r_o(x) + ... + a_{n-1}r_{k-1}(x) = a_o + a_1x \ldots + a_{n-k-1}x^{n-k-1} + a_{n-k}(x^{n-k} - q_0(x)g(x)) + ... + a_{n-1}(x^{n-1} - q_{k-1}(x)g(x)) = u(x) - (a_{n-k}q_o(x)g(x) + ... + a_{n-1}q_{k-1}g(x)) = u(x) - g(x)q(x)$ así $u(x) = g(x)q(x) + s(x)$. Como el grado de $r_i(x)$ es menor ó igual que $n-k-1$ para todo i, lo mismo se sigue para $s(x)$, y por la unicidad del algoritmo de la división , se concluye que $s(x)$ es el resto de la división de $u(x)$ por $g(x)$. Por tanto el síndrome de un vector puede ser obtenido por división polinómica.

Ejemplo. Considerar el $(7, 4)$-código binario cíclico generado por $g(x) = 1 + x + x^3$. Entonces:

$x^3 = (x^3 + x + 1) + (1 + x)$

$\mathrm{x}^4 = (x^3 + x + 1)x + (x + x^2)$

$\mathrm{x}^5 = (x^3 + x + 1)(x^2 + 1) + (1 + x + x^2)$

$\mathrm{x}^6 = (x^3 + x + 1)(x^3 + x + 1) + (1 + x^2)$

así

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} = [R\ I_4]$$

.

Una matriz de control es :

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

Considerar $u(x) = 1 + x^2 + x^3 + x^5 + x^6$, su síndrome es :

$$Hu(x) = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = x^2$$

Si dividimos $u(x)$ por $g(x)$ tenemos:

$$u(x) = (1 + x + x^3)(1 + x + x^2 + x^3) + x^2$$

con resto x^2, como era de esperar. (Observando la matriz de control obtenida sabemos que el código dado es un Ham$(3, 2)$).

Notar además que el síndrome de una palabra y el de sus permutaciones circulares, están relacionados. En efecto, si $s(x)$ es el síndrome de $u(x)$ y $xs(x)$ tiene grado menor o igual que $n - k - 1$, entonces el síndrome de $xu(x)$ es $xs(x)$. En otro caso, si $s(x) = \sum_{i=0}^{n-k-1} s_i x^i = s'(x) + s_{n-k-1}x^{n-k-1}$ y $g(x) = \sum_{i=0}^{n-k} a_i x^i = g'(x) + x^{n-k}$, se tiene que $xs(x) = xs'(x) + s_{n-k-1}(g(x) - g'(x)) = s_{n-k-1}g(x) + (xs'(x) - s_{n-k-1}g'(x))$ con grad $(xs'(x) - s_{n-k-1}g'(x))$ menor o igual que $n - k - 1$. Así el síndrome de $xu(x)$(que coincide con el de $xs(x)$) es en este caso : $xs'(x) - s_{n-k-1}g'(x)$.

Las observaciones precedentes conducen a un método de descodificación con códigos cíclicos, que se conoce como el **método de atrapar el error** (error trapping).

(9.5) **Lema**. Sea C un (n, k)-código cíclico con $d \geq 2t + 1$ (t-corrector). Suponer que a lo más se han producido t errores al transmitir una palabra $c \in C$. Si el síndrome de la palabra recibida tiene peso menor o igual que t, entonces $e(x) = s(x)$, donde $u(x) = c(x) + e(x)$, $c(x) \in C$ y $s(x)$ es el síndrome de $u(x)$.

Dem. Notar que $w(s(x))$ es menor o igual que t y lo mismo sucede con $e(x)$. Además: $u(x) = c(x) + e(x) = g(x)q(x) + s(x)$ luego $e(x) - s(x) \in C$ y por (4.14) Proposición, se tiene $e(x) = s(x)$.

Denotaremos por $s_i(x)$ =s(x$^i u(x)$ Si $w(s_i(x))$ es menor ó igual que t, por el Lema anterior obtendremos que el error de $x^i u(x)$, que coincide con $x^i e(x)$, es igual a $s_i(x)$. Así $e(x) = x^{n-i}s_i(x)$. Esto permite definir la estrategia de descodificación, conocida como método de atrapar el error. Se tratará de dar condiciones que permitan asegurar que el síndrome de una permutación cíclica de la palabra recibida, tiene el peso acotado por t.

Si C es un (n,k)-código cíclico t-corrector, e la palabra error producida al transmitir la palabra código c, con $w(e)$ menor ó igual que t, de forma que existe i, $0 \leq i \leq n-1$ tal que $x^i e(x)$ tiene todas sus componentes no ceros entre las $n-k$ primeras componentes, entonces el grado de $x^i e(x)$ es menor ó igual que $n-k-1$, luego por la unicidad del algoritmo de la división se tiene $s(x^i u(x))) = x^i e(x)$, y la descodificación es inmediata.

Ejemplos

1. Sea $g(x) = 1 + x^2 + x^3$ el polinomio generador de un (7,4)-código binario cíclico con distancia mínima 3 (1-corrector).

Considerar la palabra código $1 + x + x^5 = (1 + x + x^2)g(x)$. Si en la transmisión se recibe $u(x) = 1 + x + x^5 + x^6$ se debería descodificar como sigue:

i) Dividir $u(x)$ por $g(x)$. Así:

$$u(x) = (1 + x^2 + x^3)(1 + x^3) + x + x^2$$

por tanto $s(x) = x + x^2$. Como $w(s(x)) = 2 > 1$, considerar $xu(x)$.

ii)Como grad $(xs(x)) > n - k - 1 = 2$, sabemos que el síndrome $s(xu(x) = xx - (1 + x^2) = 1$ de peso 1. Así $1 = s(xu(x)) = e(xu(x) = xe(x)$, de donde: $e(x) = x^6$ como era de esperar.

2. Sea $g(x) = 1 + x^4 + x^6 + x^7 + x^8$, polinomio generador de un (15,7)-código binario cíclico C con $d(C) = 5$ es decir C es 2-corrector. Cualquier error de peso menor o igual que 2, contiene las componentes no ceros , después de una cierta permutación circular, entre las 8 primeras componentes y por tanto se va a poder realizar la descodificación. Suponer que se recibe $u = 110011101100010$. Entonces:

i) Dividimos $u(x)$ por $g(x)$:

$$u(x) = g(x)(x + x^2 + x^4 + x^5) + 1 + x^2 + x^5 + x^7$$

ii) Computamos los síndromes $s_i(x)$ de $x^i u(x)$ hasta que obtengamos uno de peso menor o igual que 2. Esto sucede para $i = 7$. Así el error es:

$$e = x^8(100001000000000) = 000000001000010$$

y la palabra enviada es 110011100100000.

Ejercicios.

1. Considerar la descomposición $x^7 - 1 = (x-1)(x^3+x^2+1)(x^3+x+1)$ en $\mathbf{Z}/2\mathbf{Z}[x]$. Sea $g(x) = x^3 + x + 1$, hallar una matriz generadora y otra de control del código cíclico $C = (g(x))$. ¿Es C de algún tipo ya conocido?.

2. Encontrar todos los códigos ternarios cíclicos de longitud 4 y dar una matriz generadora para cada uno de ellos. Concluir que $\mathrm{Ham}(2,3)$ no es equivalente a un código cíclico.

3. Si $g(x) = 1 + x^4 + x^6 + x^7 + x^8$ es el polinomio generador de un $(15,7)$-código binario cíclico C con $d(C) = 5$, hallar por el método de atrapar el error, la palabra enviada si se ha recibido 100100010111100.

4. Sea C un $(q+1, 2, q)$-código sobre $GF(q)$, q impar. Deducir que C no puede ser cíclico. Concluir que $\mathrm{Ham}(2,q)$ no es equivalente a un código cíclico, cuando q es impar.

5. Considerar el polinomio $x^5 + x^4 - x^3 + x^2 - 1$ generando el código cíclico ternario C, cuyos parámetros son $(11, 6, 5)$. Se recibe $u = 22100111000$. Descodificar la palabra recibida por el método de atrapar el error.

Lección 10. BCH-códigos

Hemos estudiado códigos en los que la longitud y la dimensión son fáciles de determinar. Sin embargo encontrar la distancia mínima es más difícil. Examinaremos ahora una construcción que permite encontrar un código de longitud dada y distancia mínima mayor o igual que un valor prefijado. Más aún, podremos dar una cota inferior para la dimensión de dicho código. Esta construcción fué dada independientemente por Bose, Ray-Chaudhuri y Hocquenghem, así se deberían llamar BRH- códigos, pero se conocen como **BCH- códigos** . Los BCH-códigos que pasamos a describir se conocen como BCH-códigos en sentido estricto (narrow sense).

(10.1) **Definición**. Sea $(m.n) = 1$. Sabemos que $m + n\mathbf{Z}$ es una unidad en el anillo $\mathbf{Z/nZ}$, es decir $m + n\mathbf{Z} \in U_n$, grupo multiplicativo de las unidades de $\mathbf{Z/nZ}$. Llamaremos orden de m (mod n) al orden de $m + n\mathbf{Z}$ en dicho grupo, es decir, el menor entero positivo e tal que $m^e \equiv 1(n)$.

(10.2) **Definición**. Una raíz n-ésima primitiva de la unidad en un cuerpo F es un elemento de orden n en el grupo multiplicativo F^*.

(10.3) **Proposición**. Sea q una potencia de un primo y sea $e = o(q)(\mathrm{mod}\, n)$ con $(q, n) = 1$. Entonces el menor cuerpo finito que contiene a $GF(q)$ como subcuerpo y a una n-ésima raíz primitiva de la unidad es $GF(q^e)$.

Dem. Considerar $GF(q^e)$, contiene a $GF(q)$ como subcuerpo y como $n|(q^e - 1)$, contiene una n-ésima raíz primitiva de la unidad, ya que $GF(q^e)^*$ es cíclico. Si $GF(q^m)$ tiene una n-ésima raíz primitiva de la unidad , se sigue que $n|(q^m - 1)$ luego $e|m$ y por el ejercicio 1 de la Lección 3 se tiene que $GF(q^e) \subseteq GF(q^m)$.

Necesitaremos una propiedad básica de los determinantes de Vandermonde. Sean $a_1, ..., a_n$ elementos, distintos entre sí, de un cuerpo F, entonces:

$$\det \begin{pmatrix} 1 & a_1 & (a_1)^2 & \dots & (a_1)^{n-1} \\ 1 & a_2 & (a_2)^2 & \dots & (a_2)^{n-1} \\ \dots & \dots & \dots & & \\ 1 & a_n & (a_n)^2 & \dots & (a_n)^{n-1} \end{pmatrix} \neq 0$$

Los códigos que vamos a contruir son códigos cíclicos de longitud n sobre $GF(q)$ con $(n.q) = 1$. Se supone fijado un entero positivo δ. Se definirá el BCH-código de longitud n

y distancia mínima mayor o igual que δ.

Sea $e = o(q)(\mathrm{mod}\, n)$ y a una raíz n-ésima primitiva de la unidad en $GF(q^e)$. Sea $b \in GF(q^e)$ raíz de $f(x) \in GF(q)[x]$, mónico irreducible de grado e, sabemos que existe un homomorfismo de anilllos:

$$\phi : GF(q)[x] \to GF(q)[b]$$

dado por $\phi(g(x)) = g(b)$ cuyo núcleo es $(f(x))$ luego : $GF(q)[x]/(f(x)) \cong GF(q)[b]$ cuerpo de q^e elementos. Así todo elemento del cuerpo de q^e elementos se expresará en la forma: $c_o + c_1 b + ... + c_{e-1} b^{e-1}$ con los $c_i \in GF(q)$.

Se define el BCH-código de longitud n y distancia designada δ sobre $GF(q)$, como el código de matriz de control:

$$H = \begin{pmatrix} 1 & a & a^2 & \dots & a^{n-1} \\ 1 & a^2 & a^4 & \dots & a^{2(n-1)} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & a^{\delta-1} & a^{2(\delta-1)} & \dots & a^{(\delta-1)(n-1)} \end{pmatrix}$$

Cada elemento de dicha matriz pertenece a $GF(q^e)$, luego viene representado por una e-tupla de elementos de $GF(q)$. Así dicha matriz puede considerarse como una $e(\delta-1) \times n$ matriz sobre $GF(q)$.

(10.4) **Teorema**. El BCH código de longitud n y distancia designada δ sobre $GF(q)$, tiene distancia mínima mayor o igual que δ y dimensión mayor o igual que $n - e(\delta - 1)$.

Dem. Para demostrar que la distancia mínima de este código es mayor o igual que δ, sabemos que basta probar que cualesquiera $\delta - 1$ columnas de una matriz de control son linealmente independientes. Considerar el determinante de la matriz (sobre $GF(q^e)$) formada por $\delta - 1$ columnas:

$$\det \begin{pmatrix} a^{m_1} & \dots & a^{m_{\delta-1}} \\ \vdots & & \vdots \\ a^{m_1(\delta-1)} & \dots & a^{m_{\delta-1}(\delta-1)} \end{pmatrix}$$

La i-ésima columna tiene un factor común $a^{m_i} \neq 0$. Llevando fuera estos factores obtenemos un determinante de Vandermonde $V(a^{m_1}, ..., a^{m_{\delta-1}})$ que no es cero.

Así las columnas elegidas son linealmente independientes sobre $GF(q^e)$ y sobre el subcuerpo $GF(q)$.

La dimensión del código es n menos el rango de dicha matriz . Este rango es menor o igual que $e(\delta - 1)$ que es el número de filas .

(10.5) **Teorema**. Los BCH códigos son cíclicos.

Dem. Sabemos que una palabra $c_o c_1 ... c_{n-1}$ se corresponde con $f(x) = c_o + c_1 x + ... + c_{n-1} x^{n-1}$. La condición de que la palabra pertenezca al BCH código puede ser expresada mediante:

$f(a^i) = c_o + c_1 a^i + ... + c_{n-1} a^{i(n-1)} = 0 \ , i = 1, ..., \delta - 1$

Sea $g(x)$ el mínimo común múltiplo de los polinomios mónicos irreducibles sobre $GF(q)$ de los elementos: $a, a^2, ..., a^{\delta-1}$. Entonces la palabra correspondiente a $f(x)$ está en el BCH código si y solo si $g(x)|f(x)$. Más aún, los elementos $a, a^2, ..., a^{\delta-1}$ son raíces n-ésimas de la unidad, así si $f_i(x)$ es el polinomio mónico irreducible de a^i sobre $GF(q)$ $, i = 1, ..., \delta - 1$ se tiene que $f_i(x)|x^n - 1 \ \forall i$ luego $g(x)|x^n - 1$. Se concluye por tanto que el BCH código es el código cíclico con polinomio generador $g(x)$.

Se puede usar la siguiente observación para mejorar la cota inferior de la dimensión de un BCH código.

(10.6) **Proposición**. Si $f(x) \in GF(q)[x]$ y a es raíz de $f(x)$ en un cuerpo que contiene a $GF(q)$ como subcuerpo, entonces a^q es también raíz de $f(x)$.

Recordemos que una palabra $c_o c_1 ... c_{n-1}$ sobre $GF(q)$ pertenecía al código si y solo si $f(a^i) = 0 \ , i = 1, ..., \delta - 1$ Así si existen i y j tales que $j \equiv iq^m(n)$ para algún m , las condiciones i-ésima y j-ésima son equivalentes, se puede por tanto suprimir la j-ésima y obtener una mayor cota inferior para la dimensión del código.

Ejemplo. Considerar el BCH código binario C de longitud 15 y distancia designada 5. $e = o(2) \pmod{15} = 4$. Así si a es una 15-ésima raíz primitiva de la unidad ($a \in GF(2^4)$)), las palabras código se corresponden con polinomios que tienen raíces: a, a^2, a^3, a^4 . Ahora bien si $f(a) = 0$ como el cuerpo de coeficientes es $GF(2)$, sabemos que será $f(a^2) = f(a^4) = 0$, así es suficiente suponer que a y a^3 son raíces. Recordemos el ejemplo ii) de la Lección 3. Sea $x^4 + x + 1 \in GF(2)[x]$ que es irreducible ya que no tiene raíces en $GF(2)$ y no puede expresarse como producto de dos polinomios de grado dos ($x^2, x^2 + 1, x^2 + x, x^2 + x + 1$). Sea $a \in GF(2^4)$ raíz de $x^4 + x + 1$. Sabemos que $a^{15} = 1$, ya que $GF(2^4)^*$ es un grupo multiplicativo de orden 15. Además $a^3 \neq 1$ pues si $a^3 = 1$ sería $a^4 = a = a + 1$ lo que es

contradicción, y $a^5 \neq 1$ ya que si $a^5 = 1 = a^2 + a$, a sería raíz de $x^2 + x + 1$, que no es múltiplo de $x^4 + x + 1$. Así $o(a) = 15$ y a es una 15-ésima raíz primitiva de la unidad. Se sigue que $o(a^3) = 5$, luego a^3 es raíz de $x^5 - 1 = (x-1)(x^4+x^3+x^2+x+1)$ y el polinomio mónico irreducible de a^3 es $x^4 + x^3 + x^2 + x + 1$ así que el polinomio generador del código es $g(x) =$m.c.m.$(x^4 + x + 1, x^4 + x^3 + x^2 + x + 1) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1) = x^8 + x^7 + x^6 + x^4 + 1$ y dim $C = 15 - 8 = 7$.

Sabemos que $d = d(C) \geq 5$. Veamos que $d = 5$. Recordar que existe un homomorfismo de anillos $\phi : GF(2)[x] \longrightarrow GF(2)[a]$ dado por $\phi(g(x) = g(a)$, cuyo nucleo Ker$\phi = (x^4 + x + 1)$ y $GF(2)[x]/(x^4 + x + 1) \cong GF(2)[a]$ que es $GF(2^4)$. Así todo elemento de $GF(2^4)$ puede verse en la forma $a_0 + a_1a + a_2a^2 + a_3a^3$ con los $a_i \in GF(2)$, e identificarse con la correspondiente cuaterna binaria $a_0a_1a_2a_3$. Por todo ello podemos escribir una matriz de control de C como:

$$H = \begin{pmatrix} 1 & a & a^2 & a^3 & a^4 & a^5 & a^6 & a^7 & a^8 & a^9 & a^{10} & a^{11} & a^{12} & a^{13} & a^{14} \\ 1 & a^3 & a^6 & a^9 & a^{12} & 1 & a^3 & a^6 & a^9 & a^{12} & 1 & a^3 & a^6 & a^9 & a^{12} \end{pmatrix} =$$

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

ya que:

$a^4 = a + 1, a^5 = a^2 + a, a^6 = a^3 + a^2, a^7 = a^4 + a^3 = a^3 + a + 1, a^8 = a^4 + a^2 + a = a + 1 + a^2 + a = a^2 + 1, a^9 = a^3 + a, a^{10} = a^4 + a^2 = a + 1 + a^2, a^{11} = a^3 + a^2 + a, a^{12} = a^4 + a^3 + a^2 = a + 1 + a^3 + a^2, a^{13} = a^4 + a^3 + a^2 + a = a + 1 + a^3 + a^2 + a = a^3 + a^2 + 1, a^{14} = a^4 + a^3 + a = a + 1 + a^3 + a = a^3 + 1$.

Observar que las columnas 4ª,6ª, 7ª,8ª, y 15ª son linealmente dependientes, así la distancia mínima de este código es 5.

(Notar que estos últimos cálculos, válidos en general para llegar a determinar la distancia mínima, podrían omitirse en nuestro caso, observando que la palabra correspondiente a la coclase de $g(x)$ tiene peso 5. Confrontar también con el ejercicio 6 de esta lección).

Notas. Un BCH-código con distancia designada δ puede coincidir con un BCH-código con distancia designada δ', $\delta' > \delta$.

i) Si C es un BCH-código binario, podemos suponer que δ es impar, $\delta = 2t + 1$, ya que el polinomio irreducible de a^{2t} coincide con el irreducible de a^t.

ii) Sea C BCH-código con $n = 31, q = 2$, $\delta = 8$, luego $e = 5$. Sea a una 31-ésima raiz primitiva de la unidad en $GF(2^5)$. En este caso todos los elemetos de $GF(2^5)^*$, distintos de 1, son primitivos. Notar que:

$\mathrm{Irr}(a, GF(2)) = (x - a)(x - a^2)(x - a^4)(x - a^8)(x - a^{16})$

$\mathrm{Irr}(a^3, GF(2)) = (x - a^3)(x - a^6)(x - a^{12})(x - a^{24})(x - a^{17})$

$\mathrm{Irr}(a^5, GF(2)) = (x - a^5)(x - a^{10})(x - a^{20})(x - a^9)(x - a^{18})$

$\mathrm{Irr}(a^7, GF(2)) = (x - a^7)(x - a^{14})(x - a^{28})(x - a^{25})(x - a^{19})$

así C coincide con el BCH-código con $n = 31, q = 2$ y $\delta = 11$. Por lo tanto la distancia mínima de C es mayor o igual que 11.

Un caso importante de BCH códigos es cuando $n = q - 1$. Son los **códigos de Reed-Solomon**. En este caso el orden de q módulo n es 1. Así la cota para un código de distancia designada δ y longitud n es $\dim C \geq n - \delta + 1$.

Por otra parte, si la verdadera distancia mínima es d se tiene $d \geq \delta$ y la cota de Singleton dice que $|C| \leq q^{n-d+1}$, de ahí que $\dim C \leq n - d + 1$ y por tanto $n - d + 1 \leq n - \delta + 1 \leq \dim C \leq n - d + 1$ y la igualdad se cumple. Reunimos estos hechos en el siguiente resultado:

(10.7) **Teorema**. Un código de Reed-Solomon con distancia designada δ tiene distancia mínima δ y dimensión $n - \delta + 1$. De ahí que alcanza la cota de Singleton y es por tanto un MDS-código.

Finalizamos la lección con una aplicación a los códigos de Hamming.

(10.8) **Proposición**. $\mathrm{Ham}(r, 2)$ es equivalente a un código cíclico.

Dem. Considerar $n = 2^r - 1$, $((n.2) = 1)$ entonces $o(2)(mod\, n) = r$. El BCH código binario de distancia designada $\delta = 2$, tiene matriz de control: $H = (1\, a \ldots a^{n-1})$ siendo a una raíz n-ésima primitiva de la unidad en $GF(2^r)$ (un elemento primitivo del cuerpo $GF(2^r)$). Así las entradas de H son todas las r-tuplas binarias no nulas. Se trata de un $\mathrm{Ham}(r, 2)$.

Este resultado no puede extenderse a los códigos de Hamming q-arios. De hecho sabemos que $\mathrm{Ham}(2,3)$ no es equivalente a un código cíclico (ejercicio 2 de la Lección 9).

Ejercicios.

1. Obtener el polinomio generador de un BCH-código ternario 1-corrector de longitud 8.

2. ¿Cual es la dimensión del BCH-código binario de distancia designada 5 y longitud 31?.

3. Describir un $(7, 3)$-código de Reed-Solomon sobre $GF(8)$ por su polinomio generador . ¿Cuántos errores corregirá?

4. Encontrar el polinomio generador de un código de Reed-Solomon 2-corrector sobre $GF(16)$. Dar su longitud y su dimensión.

5. Se conoce que existe una 7-ésima raíz primitiva de la unidad en $GF(8)$ que verifica $a^3 = a + 1$. Razonar que el código C de Reed-Solomon sobre $GF(8)$ generado por : $g(x) = (x - a)(x - a^2)(x - a^3)$ tiene los parámetros: $(7, 4, 4)$. Comprobar que $g(x) = x^3 + a^6x^2 + ax + a^6$ y obtener una matriz generadora de C.

6. Sea C un BCH-código binario de longitud n con $(n, 2) = 1$ y distancia designada δ. Suponer que $n = r\delta$. Probar que $d(C) = \delta$.

7. Se conoce la factorización en polinomios irreducibles de $x^{15} - 1$ en $\mathbf{Z}/\mathbf{2Z}[x]$:

$x^{15} - 1 = (1 + x)(1 + x + x^2)(1 + x + x^4)(1 + x^3 + x^4)(1 + x + x^2 + x^3 + x^4)$

Encontrar el polinomio generador de un BCH-código binario de longitud 15 con distancia designada $\delta = 7$. Concluir que $d(C) = 7$.

8. Encontrar el polinomio generador de un BCH-código binario que sea equivalente a $\mathrm{Ham}(4, 2)$.

9. Hallar todos los BCH-códigos binarios de longitud 15.

10. Encontrar un BCH-código cuyo dual no sea un BCH-código.

Apéndice. El teorema de la dualidad de MacWilliams.

El teorema de dualidad de MacWilliams permite obtener el polinomio enumerador de pesos de un código lineal C a partir del polinomio enumerador de pesos de $C^{\perp}$. Este resultado es de gran utilidad cuando se consideran códigos lineales de un considerable cardinal, tales que sus duales tienen un polinomio enumerador sencillo de obtener. Es el caso de los códigos de Hamming.

Para la demostración del teorema de dualidad necesitaremos algunos resultados previos.

Lema. Si $g \in G$ es un elemento de orden finito, π es un conjunto de números primos y π' su complementario, entonces g se expresa de forma única como $g = g_{\pi}g_{\pi'} = g_{\pi'}g_{\pi}$, donde g_{π} y $g_{\pi'}$ son π-elemento y π'-elemento respectivamente.

Dem. Se dice que un elemento de orden finito es un π-elemento cuando los divisores primos del orden de g pertenecen a π. Suponer que $o(g) = nm$ donde los primos de n son de π y los de m son de π'. sabemos que existen enteros a, b tales que $1 = am+bn$. Entonces $g = g^{am+bn} = g^{am}.g^{bn}$. Notar que g^{am} es un π-elemento pues $(g^{am})^n = 1$ y g^{bn} es un π'-elemento pues $(g^{bn})^m = 1$. Evidentemente ambas potencias de g conmutan. Supongamos que existen x, y en G tales que $g = xy = yx$ siendo x π-elemento e y π'-elemento. Si $t = o(y)$, entonces: $g^t = x^t y^t = x^t$ y como $(o(x), t) = 1$ se tiene: $< x >=< x^t >\leq< g >$, luego x conmuta con g^{am}. análogamente y conmuta con g^{bn}. Como $g = g^{am}g^{bn} = xy$, se tiene que necesariamente $x^{-1}g^{am} = y(g^{bn})^{-1} = 1$. Así $x = g^{am}$ e $y = g^{bn}$. Dada la unicidad, a dichos elementos se les llama la π- parte y la π'-parte de g respectivamente.

Lema. Sea G un grupo finito abeliano y p un primo que divide al orden de G. Entonces existe un elemento de G que tiene orden p.

Dem. Por inducción sobre el orden de G. Si $|G| = p$ existe $a \in G$ tal que $G =< a >$, luego $o(a) = p$. Sea $g \in G$, $g \neq 1$. Si $o(g) = pm$ entonces $o(g^m) = p$. Suponer que $p \not| o(g)$. Como G es abeliano $< g >$ es un subgrupo normal de G y necesariamente p divide al orden de $G/ < g >$. Por hipótesis de inducción existirá $y < g >\in G/ < g >$ tal que $o(y < g >) = p$, luego $y^p < g >=< g >$, así $y^p \in< g >$ y por tanto $y^{po(g)} = 1$. Como $y^{o(g)} \neq 1$, se sigue que $o(y^{o(g)}) = p$.

El resultado anterior puede extenderse a grupo finitos cualesquiera.

Teorema. (Teorema de Cauchy). Si G es un grupo finito y p es primo dividiendo al orden de G, existe $g \in G$ tal que $o(g) = p$.

Dem. Comencemos demostrando la ecuación de las clases. Se define en G la relación de equivalencia: si $x, y \in G$ diremos que y es conjugado con x en G si existe $g \in G$ tal que $y = x^g = g^{-1}xg$. Se denota por $Cl(x)$ a la clase de equivalencia de x (conocida como clase de conjugación de x en G). Se define $\varphi : Cl(x) \longrightarrow D$ por $\varphi(x^g) = C_G(x)g$, donde D es el conjunto de las clases a derecha de $C_G(x)$. Como, $x^{g_1} = x^{g_2} \iff x^{g_1 g_2^{-1}} = x \iff g_1 g_2^{-1} \in C_G(x) \iff C_G(x)g_1 = C_G(x)g_2$, se sigue que φ es una aplicación biyectiva. Así $|Cl(x)| = |G : C_G(x)|$ que divide al orden de G. Notar que hay tantas clases de conjugación de cardinal 1 como elementos del centro de G. De todo ello se deduce la ecuación de las clases de G:

$$|G| = |Z(G)| + \sum |G : C_G(x)|$$

donde el sumatorio se realiza sobre los elementos no pertenecientes al centro de G.

El teorema lo demostraremos por inducción sobre el orden de G. Si G es abeliano, el resultado es cierto por el lema anterior. Sea $x \in G$, $x \notin Z(G)$ así $C_G(x) < G$. Si $p||C_G(x)|$, por hipótesis de inducción se seguirá la tesis. Podemos suponer por tanto que $p \not| |C_G(x)|$ para cualquier $x \notin Z(G)$. Así $p||G : C_G(x)|$, para tales elementos y por la ecuación de las clases, se seguirá que $p||Z(G)|$. Basta entonces aplicar el lema anterior.

Lema. Si G es un p-grupo abeliano finito, G es cíclico si y solo si G tiene un único subgrupo de orden p.

Dem. $\Longrightarrow$) es conocido.

$\Longleftarrow$) Por inducción sobre el orden de G. Sea U el único subgrupo de orden p de G. Establecemos la aplicación

$$\phi : G \longrightarrow G$$

dada por $\phi(x) = x^p$. Como G es abeliano, dicha aplicación es un homomorfismo de grupos. Sea $G^p = \varphi(G)$. Por la hipótesis se tiene $Ker\phi = U$, así $|G^p|p = |G|$. Si $G^p = 1$ sería $G = U$ cíclico. En otro caso, por hipótesis de inducción, G^p es cíclico , así existe $h \in G^p$ tal que $G^p =< h >$. Sea $g \in G$ tal que $h = g^p$ entonces $o(g) = po(h) = p|G^p| = |G|$ y G es cíclico.

Teorema de estructura de grupos finitos abelianos. Si G es un grupo finito abeliano, $G = G_1 \times G_2 \times ... \times G_n$ donde los G_i son grupos cíclicos de ordenes $p_i^{a_i}$ siendo los primos p_i no necesariamente distintos.

Dem. Sea $p||G|$. Llamaremos: $U_p = \{g \in G | g$ es p-elemento$\}$ y $U_{p'} = \{g \in G | g$ es p'-elemento$\}$. Ambos son subgrupos de G. Por el primer Lema tenemos que $G = U_p \times U_{p'}$. Así podemos suponer que G es un p-grupo . Demostraremos por inducción sobre el orden de G la siguiente afirmación:

Si $g \in G$ tiene el orden mayor posible entre los órdenes de los elementos de G, existe $U \leq G$ tal que $G =< g > \times U$.

Una vez probado lo anterior, el resultado se sigue fácilmente.

Si G fuera cíclico $G =< g >$ y el resultado sería cierto. Si G no es cíclico, por el Lema anterior existe $A \leq G$ tal que $|A| = p$ y $A \cap < g >= 1$. Considerar G/A . Es claro que $o(gA)|o(g)$, pero además si $o(gA) = r$ entonces $(gA)^r = A$ luego $g^r \in A \cap < g >= 1$ así $o(g) = r$. Por lo tanto gA tiene el orden mayor posible entre los órdenes de los elementos de G/A. Por hipótesis de inducción existirá $U/A \leq G/A$ tal que $G/A =< gA > \times U/A$. Si $x \in G$, $xA \in G/A$ y existirán i , $0 \leq i \leq r$ y $u \in U$ tales que $xA = (gA)^i uA$. Así $x \in < g > U$ y como $< g > A \cap U = A$, $< g > \cap U =< g > \cap < g > A \cap U =< g > \cap A = 1$. Así $G =< g > \times U$, como queríamos demostrar.

Caracteres de grupos abelianos.

Definición. Sea A un grupo finito abeliano.

a) Un homomorfismo de grupos χ de A en el grupo multiplicativo $\mathbf{C}^*$, se dice que es un caracter de A, es decir es una aplicación $\chi : A \longrightarrow \mathbf{C}^*$ tal que $\chi(a_1 + a_2) = \chi(a_1).\chi(a_2)$ $\forall a_1, a_2 \in A$.

Escribiremos $Ch(A)$ para indicar el conjunto de dichos caracteres de A.

b) Llamaremos caracter trivial de A y lo denotaremos por $\chi = 1_A$, al caracter dado por $\chi(a) = 1$ $\forall a \in A$.

c) Si $\chi \in Ch(A)$, definimos $\bar{\chi}(a) = \bar{\chi(a)}$ (conjugado de $\chi(a)$), $\forall a \in A$

Proposición. Si $\chi \in Ch(A)$, se tiene:

a) $\chi(0) = 1$.

b) $\chi(a)^{|A|} = 1$ $\forall a \in A$, es decir $\chi(a)$ es una $|A|$-ésima raíz de la unidad compleja.

c)$\bar{\chi}(a) = \chi(-a)\ \forall a \in A$.

d) $Ch(A)$ es un grupo vía: $\chi\phi(a) = \chi(a)\phi(a)\ \forall a \in A,\ \forall \chi, \phi \in Ch(A)$.

Dem.a) $\chi(0) = \chi(0+0) = \chi(0)\chi(0)$ lo que implica $\chi(0) = 1$.

b) Como $|A|a = 0\ \forall a \in A$, se tiene que $1 = \chi(0) = \chi(|A|a) = \chi(a)^{|A|}$.

c) $\chi(a)\bar{\chi}(a) = 1 = \chi(a)\chi(-a)$ lo que implica que $\bar{\chi}(a) = \chi(-a)$.

d) Sean $\chi, \phi \in Ch(A)$, se tiene:

$(\chi\phi)(a_1 + a_2) = \chi(a_1 + a_2)\phi(a_1 + a_2) = \chi(a_1)\chi(a_2)\phi(a_1)\phi(a_2) =$

$\chi(a_1)\phi(a_1)\chi(a_2)\phi(a_2) = (\chi\phi)(a_1)(\chi\phi)(a_2)$, así $\chi\phi \in Ch(A)$. El trivial es el neutro y $\bar{\chi}$ el inverso de χ. La asociatividad se sigue de la de $\mathbf{C}^*$.

Ejemplo. Sea $A =< a > \cong C_n$ y sea ϵ una n -ésima raíz primitiva de la unidad compleja. Entonces $Ch(A) = \{1_A, \chi_1, ..., \chi_{n-1}\}$ donde χ_i está definido por $\chi_i(a) = \epsilon^i$. (Notar que un caracter de un grupo cíclico queda fijado dando la imagen de a). Se tiene que $A \cong Ch(A)$ asignando a a^i el caracter χ_i.

Proposición. Si A y B son grupos finitos abelianos se tiene:

$$Ch(A \times B) = \{\chi\phi | \chi \in Ch(A), \phi \in Ch(B)\} \cong Ch(A) \times Ch(B)$$

Donde $\chi\phi(a, b) = \chi(a)\phi(b)\ \forall a \in A, b \in B$

Dem. Para $a_i \in A, b_i \in B$ se tiene:

$\chi\phi((a_1, b_1) + (a_2, b_2)) = \chi\phi(a_1 + a_2, b_1 + b_2) = \chi(a_1 + a_2)\phi(b_1 + b_2) =$

$\chi(a_1)\chi(a_2)\phi(b_1)\phi(b_2) = \chi\phi(a_1, b_1)\chi\phi(a_2, b_2)$

Si $\delta \in Ch(A \times B)$, $\delta(a, b) = \delta(a, 0)\delta(0, b)$. Como $\chi(a) = \delta(a, 0)$ y $\phi(b) = \delta(0, b)$ definen sendos caracteres de A y B respectivamente, tenemos que $\delta = \chi\phi$ y queda probada la primera iguldad. Por otra parte si $(\chi, \phi) \neq (\chi', \phi')$ entonces $\chi\phi \neq \chi'\phi'$. Así el isomorfismo buscado viene dado asignando a (χ, ϕ) el caracter $\chi\phi$.

Corolario. Si A es un grupo finito abeliano se tiene $A \cong Ch(A)$. Por lo tanto $|A| = |Ch(A)|$.

Dem. En el primer párrafo se ha probado que todo grupo finito abeliano es producto directo de grupos cíclicos. Bastará ahora tener en cuenta el ejemplo y la Proposición anteriores.

Definición. Si G es un grupo finito y $\mathbf{C}^G$ es el espacio vectorial complejo de las funciones de G en $\mathbf{C}$, se define un producto escalar:

$$< f, g >= 1/|G| \sum_{x \in G} f(x) g(\bar{x})$$

para $f, g \in \mathbf{C}^G$.

Teorema (Relaciones de ortogonalidad). Si A es un grupo finito abeliano y $\chi, \phi \in Ch(A)$, se tiene:

i)$< \chi, \phi >= 1$ si $\chi = \phi$

ii) $< \chi, \phi >= 0$ si $\chi \neq \phi$.

En particular los caracteres de A forman una base ortonormal del espacio $\mathbf{C}^A$, dotado con el producto escalar $<, >$.

Dem. Se sabe que $|Ch(A)| = |A| = \dim \mathbf{C}^A$. Además es $< \chi, \phi >=< \chi\bar{\phi}, 1_A >$. Como $\bar{\phi}$ es el inverso de ϕ en $Ch(A)$, es suficiente probar que $< \chi, 1_A >= 1$ si $\chi = 1_A$ y que $< \chi, 1_A >= 0$ si $\chi \neq 1_A$. Evidentemente es $< \chi, 1_A >= 1$ si $\chi = 1_A$. Sea ahora $\chi \neq 1_A$. Sea $b \in A$ tal que $\chi(b) \neq 1$. Entonces: $\chi(b) \sum_{a \in A} \chi(a) = \sum_{a \in A} \chi(a + b) = \sum_{a \in A} \chi(a)$. Así $\sum_{a \in A} \chi(a) = 0$ luego $< \chi, 1_A >= 0$.

Teorema de dualidad de MacWilliams.

Definición. Sea C un codigo de longitud n. Sea $A_i = |\{c | c \in C, w(c) = i\}|$. Se define el polinomio enumerador de pesos :

$$W_C(z) = \sum_{i=0}^{n} A_i z^i = \sum_{c \in C} z^{w(c)} \in \mathbf{Z}[z]$$

Teorema de dualidad de MacWilliams. Sea C un (n, k)-código lineal sobre $F = GF(q)$, entonces:

$$W_{C^\perp}(z) = q^{-k}(1 + (q-1)z)^n W_C((1-z)/1 + (q-1)z)$$

Dem. Sea χ un caracter no trivial del grupo aditivo de F. Para $u \in F^n$ definimos $g_u(z) = \sum_{v \in F^n} \chi(u.v) z^{w(v)} \in \mathbf{C}[z]$. $\sum_{c \in C} g_c(z) = \sum_{c \in C} \sum_{v \in F^n} \chi(c.v) z^{w(v)} = \sum_{v \in F^n} z^{w(v)} f(v)$ donde $f(v) = \sum_{c \in C} \chi(c.v)$.

La aplicación que asigna a c el complejo $\chi(c.v)$ define un caracter χ_v de C, de forma que si $v \in C^\perp$, es el caracter trivial de C. Las relaciones de ortogonalidad originan que :

$f(v) = \sum_{c\in C}\chi(c.v) = |C| < \chi_v, 1_C >$ que coincide con $|C|$ si $v \in C^\perp$ ó 0 en otro caso. Se sigue que:

$$\sum_{c\in C} g_c(z) = \sum_{h\in C^\perp} |C| z^{w(h)} = |C| W_{C^\perp}(z)$$

.

Desarrollaremos la parte izquierda de la igualdad anterior:

Para $c = c_1...c_n \in C$ tenemos:

$g_c(z) = \sum_{v\in F^n} \chi(c.v) z^{w(v)} = \sum_{a_1...a_n\in F^n} z^{\sum w(a_i)} \chi(\sum_{i=1}^{n} c_i a_i) =$

$\sum_{a_1...a_n\in F^n} \sqcap_{i=1}^{n} z^{w(a_i)} \chi(c_i a_i) = \sqcap_{i=1}^{n} \sum_{a_i\in F} z^{w(a_i)} \chi(c_i a_i)$

Como $\chi \neq 1_F$, por las relaciones de ortogonalidad será:

$\sum_{a\in F}\chi(a) = 0$, luego $\sum_{a\in F^*} \chi(a) = -1$. Así:

$\sum_{a_i\in F} z^{w(a_i)} \chi(c_i a_i) = \sum_{a\in F} z^{w(a)} = 1+(q-1)z$ si $c_i = 0$ y es igual a $1+z\sum_{a\in F^*} \chi(a) = 1-z$, si $c_i \neq 0$. Por lo tanto:

$$g_c(z) = (1-z)^{w(c)}(1+(q-1)z)^{n-w(c)}$$

Finalmente :

$$W_{C^\perp}(z) = (1/|C|)\sum_{c\in C} g_c(z) = (1/q^k)(1+(q-1)z)^n \sum_{c\in C}((1-z)/1+(q-1)z)^{w(c)} =$$

$(1/\mathrm{q}^k)(1+(q-1)z)^n W_C((1-z)/1+(q-1)z)$.

Ejemplos.

i) $W_{Ham(2,3)}(z) = 1 + 8z^3$ ya que $Ham(2,3)$ es autodual, luego toda palabra no cero tiene peso 3^{2-1} (recordar los parámetros del código dual de $Ham(r,q)$) .

ii) $W_{Ham(3,2)}(z) = (1/8)((1+z)^7 + 7(1-z)^4(1+z)^3) = (1/8)(z^7+7z^6+21z^5+35z^4+36z^3+21z^2+7z+1+7(z^7-z^6-3z^5+3z^4+3z^3-3z^2-z+1)) = (1/8)(8+56z^3+56z^4+8z^7) = 1+7z^3+7z^4+z^7$.

Ayudas para algunos de los problemas

Lección 1.

1. Si A es la $q \times n$ matriz cuyas filas son las palabras código, los q elementos de cada columna deben ser distintos entre sí. Usando permutaciones de símbolos se llegará a que el código con repetición es equivalente al dado.

2. Considerar los pares ordenados que surgen al eliminar de cada palabra código el símbolo situado en tercera posición.

4. No existen palabras código a distancia 1 y $d(000, 101) = 2$.

5. Tomar c_1, c_2 palabras código con $d(c_1, c_2) = d$. Señalar una posición en la que ambas palabras difieran y borrar de cada palabra código el correspondiente símbolo. Pasar a un nuevo código añadiendo control de paridad.

7. Aplicar la cota de Hamming.

12. Suponer que existe y probar que contiene tres palabras con los mismos símbolos en las dos últimas posiciones. Como consecuencia aparece un nuevo código de longitud cuatro y cardinal tres. Razonar que no puede existir dicho código.

Lección 3 .

1. Si $GF(p^m)$ es isomorfo a un subcuerpo de $GF(p^n)$, éste puede considerarse espacio vectorial sobre el primero. Para la otra implicación puede considerarse $f(x)$ mónico irreducible de grado m sobre $\mathbf{Z}/\mathrm{p}\mathbf{Z}$ y tomar una raíz a en $GF(p^n)$ de $f(x)$.

3. Analizar primero el caso car $k = 2$. En otro caso observar que si en k existen n cuadrados, entonces $|k| = 2n-1$. Si A es el conjunto de los cuadrados y $B = \{a-b^2 | b \in k\}$, donde a es un elemento cualquiera de k previamente fijado, entonces $A \cap B \neq \emptyset$.

5. $|GF(q)^*| = q-1$ que es divisible por 2, luego en dicho grupo cíclico existe un único elemento de orden 2.

7. Si el grado fuera d con $d|n$, distinto de n, se llegaría a que el cuerpo $GF(p)[a]$ tendría p^d elementos.

8. i) Considerar $G \cong C_n$. Cada elemento de dicho grupo tiene por orden un divisor de n y para cada divisor d de n hay $\varphi(d)$ elementos de orden d.

ii) Si G_d denota el conjunto de elementos de orden d de G, se trata de razonar que G_n no es vacío.

10. Si k^* es cíclico infinito debe ser isomorfo a $\mathbf{Z}$ y necesariamente $F \cong \mathbf{Q}$, lo que llevaría a contradicción.

11. Si car$k = 2$, el resultado es inmediato. En otro caso, si $x^4 + 1$ es irreducible en $GF(q)[x]$, es un factor de $x^{q^4} - x$. Tomar $a \in GF(q^4)$ raíz de x^4+1 y llegar a contradicción.

14. Considerar la aplicación F-lineal de E en sí mismo, inducida por multiplicación de un generador de E^*, siendo $E = GF(q^n)$ y $F = GF(q)$.

15. Computar $(1 + a)^{12}$ y $(1 + a)^8$.

17. Considerar la aplicación de $GF(q)^*$ en sí mismo que envía cada elemento a su cuadrado. Recordar los resultados básicos de grupos cíclicos finitos.

18. El grupo cíclico $GF(p^n)^*$ tiene $\varphi(p^n - 1)$ elementos generadores, que se pueden distribuir en clases de equivalencia, teniendo en cuenta los polinomios irreducibles sobre $GF(p)$ de dichos elementos.

Lección 4.

1. Notar que $|C| = 2^k$ y $|C^\perp| = 2^{k+1}$. Además $1 \in C$ y $1 + C$ es disjunto con C.

2. Si existe una palabra código c de peso impar y denotamos por P al conjunto de palabras código de peso par y con I al de las de peso impar, se tiene que $c + P \subseteq I$ y que $c + I \subseteq P$.

12. Utilizar la cota de Hamming.

18. Como $(C^\perp)^\perp = C$, bastará probar una implicación. Notar que si C es un MDS-codigo $d = n - k + 1$, luego cualesquiera $n - k$ columnas de una matriz de control de C son linealmente independientes. Así cualquier submatriz de tamaño $(n - k) \times (n - k)$ es regular. Razonar que $d(C^\perp) \geq k + 1$ y utilizar la cota de Singleton .

19. Utilizar 18.

20. Suponer $1 < k < n-2$ y sea C un (n, k)-código binario que es MDS-código. Tomar una matriz generadora de C en forma standard $G = (I|A)$ y deducir que A tiene todas sus entradas iguales a 1. Obtener una palabra código de peso 2 y llegar a contradicción.

24. Como 4 divide a $p - 1$, existirá un elemento $a \in GF(p)^*$ tal que $o(a) = 4$.

25. Comprobar que C es un MDS-código y recordar la demostración de la cota de Plotkin.

26. Si C es MDS-código, sean $i_1, .., i_d$ índices de coordenadas y $\{j_1, .., j_{k-1}\}$ el conjunto

complementario. Considerar las columnas $i_d, j_1, .., j_{k-1}$ de una matriz generadora de C y aplicar el ejercicio 19. Pasar a otra matriz generadora, con I_k en el lugar de la submatriz anterior.

27. Confrontar con la cota de Plotkin.

Lección 5.

5. Confrontar parámetros.

7. Analizar una matriz de control de dicho código.

9. Utilizar el ejercicio 5.

Lección 7.

5. Se puede suponer $0 < r < m$. Utilizar $R(r, m) = R(r, m-1) \bigoplus R(r-1, m-1)$ y el problema 3. Aplicar inducción sobre m.

8. Analizar previamente los casos $r = 0$ y $r = m$. Si $0 < r < m$ usar 5.

Lección 8.

2. C está formado por las palabras binarias de la forma $xxxyyyzzz$. realizar la permutación de posiciones (2,4)(3,7)(6,8). 4. Recordar el problema 17 de la Lección 4.

6. La palabra 0100111 se corresponde con la clase de $x + x^4 + x^5 + x^6 = x(1 + x^2)(1 + x^2 + x^3)$ y sabemos que la descomposición de $x^7 - 1$ en factores irreducibles es $:x^7 - 1 = (x-1)(x^3 + x^2 + 1)(x^3 + x + 1)$.

8. Utilizar el problema 4.

9. Pensar que si C_1 y C_2 son códigos cíclicos cuyos polinomios generadores respectivos son g_1 y g_2, entonces: $C_1 \subseteq C_2$ si y solo si $g_2(x)|g_1(x)$.

Lección 9.

4. Utilizar el ejercicio 25 de la lección 4. Además, si se fijan dos posiciones cualesquiera, las q^2 2-tuplas q-arias aparecen en dichas posiciones en las palabras del código, sin repetición.

Lección 10.

1. Tomar $\delta = 3$. a será una 8-ésima raíz primitiva de la unidad en $GF(3^2)$ .Se trata de determinar $g(x) = \text{m.c.m.}(f_1(x), f_2(x))$ siendo $f_1(x)$ el irreducible de a sobre $GF(3)$ y $f_2(x)$ el de a^2 sobre $GF(3)$. Se sabe que $g(x)$ divide a $x^8 - 1$ y que $x^8 - 1 = (x-1)(x+1)(x^2+1)(x^2-x-1)(x^2+x-1)$ es la factorización en irreducibles.

2. En este caso $q = 2$, $n = 31 = 2^5 - 1$ y a será una 31-ésima raíz primitiva de la unidad en $GF(2^5)$. Notar que a, a^2, a^4 tienen el mismo irreducible.

3. Recordar que los códigos de Reed-Solomon son MDS-códigos.

6. Considerar la factorización:

$x^n - 1 = x^{r\delta} - 1 = (x^r - 1)(1 + x^r + x^{2r} + ... + x^{(\delta-1)r})$

8. Considerar C, BCH-código binario de longitud 15 con distancia prefijada $\delta = 2$. Su matriz de control será $H = (\,1 \quad a \quad a^2 \quad \dots \quad a^{14}\,)$, donde a es una 15-ésima raíz primitiva de la unidad en $GF(2^4)$. Por el ejercicio 7 de la lección 3, el grado del $\mathrm{Irr}(a, GF(2)$ es 4. Recordar la factorización en irreducibles de $x^{15} - 1$.

Bibliografía

1. **N.L. Biggs**. Discrete Mathematics. 1989, Clarendon Press.

2. **P.J. Cameron**. Introduction to Algebra. 1998, Oxford S.P.

3. **R. Hill**. A first course in coding theory. 1986, Clarendon Press.

4. **I.M. Isaacs**. Algebra. A Graduate Course. 1994, Brooks/Cole Pub.Comp.

5. **R. Lidl-H. Niederreiter**. Finite Fields. 1983, Addison-Wesley.

6. **R. Lidl-G. Pilz**. Applied Abstract Algebra. 1984, Springer.

7. **F.J. MacWilliams-N.J.A. Sloane**. The Theory of Error-Correcting Codes. 1977,

North-Holland.

8. **V. Pless**. Introduction to the theory of error correcting codes. 1989, Wiley.

9. **S. Roman**. Coding and Information theory. 1992, Springer.

10. **W. Willems**. Codierungs-theorie. 1999, Walter de Gruyter.