CUERPOS FINITOS Y CÓDIGOS CORRECTORES DE ERRORES

MARÍA CHARA

RESUMEN. Notas del curso básico "Cuerpos Finitos y códigos correctores de errores" dictado durante el Encuentro Nacional de Algebra, La Falda, Argentina, Julio 2019. En este curso veremos algunas nociones básicas sobre la teoría de cuerpos finitos, sus propiedades, algunos resultados fundamentales, polinomios sobre cuerpos finitos y estructura de los cuerpos finitos. Como aplicación, daremos una introducción a la teoría de códigos correctores de errores. Veremos algunos ejemplos clásicos de códigos lineales sobre cuerpos finitos como los códigos de Hamming, los Reed-Solomon, los códigos cíclicos y los códigos BCH. Estudiaremos cotas clásicas para los parámetros de estos códigos y sus capacidades de detección y de corrección de errores.

ÍNDICE

1. CUERPOS FINITOS

1.1. Introducción. En esta primera parte, vamos a presentar algunos resultados básicos sobre cuerpos finitos, que serán las base para el capítulo siguiente y las aplicaciones. Empezaremos por la definición y por la presentación de algunos resultados básicos como la existencia y la unicidad de los cuerpos finitos, y el hecho de que el grupo multiplicativo de un cuerpo finito es cíclico. Luego discutiremos la clausura algebraica de un cuerpo finito y su grupo de Galois. Seguidamente, estudiaremos los conjugados de un elemento y las raíces de un polinomio irreducible, y la determinación de la cantidad de polinomios mónicos irreducibles de un cierto grado sobre un cuerpo finito. Finalmente, consideraremos la norma y la traza relativa a extensiones finitas de cuerpos finitos.

1.2. Estructura de los cuerpos finitos.

Definición 1. Un *anillo* $(R, +, \cdot)$ es una terna compuesta de un conjunto (no vacío) R y dos operaciones $+$ y $\cdot$ tales que:

- $(R, +)$ es un grupo abeliano;

Agradecimientos: a Gustavo Cabaña, Horacio Navarro y Ricardo Toledano, por la lectura detallada de estas páginas, por sus correcciones y comentarios constructivos.

- $(R, \cdot)$ es un semigrupo;
- se cumplen las leyes distributivas: $a \cdot (b + c) = a \cdot b + a \cdot c$ y $(b + c) \cdot a = b \cdot a + c \cdot a$, para $a, b, c \in R$.

Un anillo es *conmutativo* si $(R, \cdot)$ es un semigrupo abeliano. Si existe en R un elemento $1 \neq 0$ tal que $a \cdot 1 = 1 \cdot a = a$ para todo $a \in R$, decimos que R es un *anillo con unidad*. Se dice que un anillo con unidad R es un *anillo con división* si para todo $a \neq 0$ en R existe un elemento $b \in R$ (que en general se denota a^{-1}) tal que $a \cdot b = b \cdot a = 1$.

Definición 2. Un *cuerpo* $(F, +, \cdot)$ es un anillo conmutativo con división.

Un cuerpo F tiene *característica* $e \neq 0$ si e es el menor entero positivo que satisface que $e \cdot a = 0$ para todo a en F. Si no hay ningún entero positivo con esa propiedad la característica del cuerpo es cero.

Proposición 3. *Si la característica de un cuerpo F no es cero, entonces es un número primo p.*

Demostración. Sea p el menor entero positivo tal que $p \cdot a = 0$ para todo $a \in F$, y supongamos que $p = r \cdot s$ con r, y s enteros positivos mayores que 1. Entonces como $1 \in F$ tenemos que

$$0 = p \cdot 1 = (r \cdot s) \cdot 1 = (r \cdot 1)(s \cdot 1);$$

y como F es un dominio integral (no tiene divisores propios de cero) entonces debe ser que $r \cdot 1 = 0$ o $s \cdot 1 = 0$ y por lo tanto $r \cdot a = (r \cdot 1) \cdot a = 0$ o $s \cdot a = (s \cdot 1) \cdot a = 0$ para todo $a \in F$ contradiciendo el hecho de que p era el menor. Por lo tanto p debe ser primo. □

Un cuerpo se llama *finito* cuando tiene una cantidad finita de elementos. Todos los cuerpos finitos tienen característica p prima (pero no es cierto que todo cuerpo de característica prima sea finito). En efecto, si F es un cuerpo con n elementos, no puede ser que $1,\ 1+1,\ 1+1+1, \ldots, \overbrace{1+1+1+1+\cdots+1}^{n+1 \text{ sumandos}}$ sean todos distintos. Entonces existe un $i > j$ tal que $i \cdot 1 = j \cdot 1$ y por lo tanto $(i - j) \cdot 1 = 0$. Sea p el menor entero tal que $p \cdot 1 = 0$. Luego, $p \cdot \alpha = 0$ para todo $\alpha \in F$ y por lo tanto la característica de F es positiva, y por la proposición anterior, p es un número primo.

Para un número primo p, el cociente $\mathbb{Z}/p\mathbb{Z}$ forma un cuerpo. También denotamos $\mathbb{Z}/p\mathbb{Z}$ por $\mathbb{F}_p$. $\mathbb{F}_p$ es un cuerpo primo en el sentido de que no tiene subcuerpos propios. Hay exactamente p elementos en $\mathbb{F}_p$.

Ejemplo 4. $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ es un cuerpo finito con dos elementos, pero $\mathbb{Z}/4\mathbb{Z}$ no es un cuerpo.

Con cada cuerpo F tenemos un grupo multiplicativo de elementos no nulos de F que denotaremos por F^*. El grupo multiplicativo de un cuerpo finito cualquiera es cíclico. Este resultado se obtiene utilizando el Teorema Fundamental de Grupos Abelianos.

Proposición 5. *Sea F un cuerpo finito con q elementos. Entonces:*

(i) *existe un primo p tal que $\mathbb{F}_p \subset F$;*
(ii) *$q = p^n$ para algún entero $n \geq 1$;*
(iii) *$\alpha^q = \alpha$ para todo $\alpha \in F$.*
(iv) *$x^q - x$ se descompone en factores lineales en $F[x]$.*

Demostración. (i) Como F tiene una cantidad finita de elementos, su característica debe ser un número primo p. Luego $\mathbb{F}_p$ es un subcuerpo primo de F.

(ii) Consideremos F como espacio vectorial sobre $\mathbb{F}_p$. Como F es finito, también su dimensión $n = \dim_{\mathbb{F}_p} F$ es finita y si $\{\alpha_1, \ldots, \alpha_n\}$ es una base de F sobre $\mathbb{F}_p$ entonces cada elemento de F puede representarse unívocamente como $a_1\alpha_1 + \cdots + a_n\alpha_n$ con $a_1, \ldots, a_n \in \mathbb{F}_p$. Luego $q = p^n$.

(iii) Si $\alpha = 0$ entonces $\alpha^q = \alpha$. Supongamos ahora que $\alpha \neq 0$. Como todos los elementos no nulos de F forman un grupo multiplicativo F^* de orden $q-1$, tenemos que $\alpha^{q-1} = 1$, y por lo tanto $\alpha^q = \alpha$.

(iv) Si $\alpha_1, \ldots, \alpha_q$ son todos los elementos de F, entonces $x^q - x = (x - \alpha_1) \cdots (x - \alpha_q)$. □

Ejemplo 6. Si denotamos por $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$ tenemos que $(\mathbb{F}_4, +, \cdot)$ es un cuerpo con

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

Más aún, $\mathbb{F}_4$ es el único cuerpo finito con 4 elementos, salvo isomorfismos.

Lema 7. *Si F es un cuerpo finito de característica prima p y $n \geq 1$, entonces para cualquier α y β en F se cumple que*

$$(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}.$$

Demostración. Vamos a probarlo por inducción en n. Para $n = 1$ el resultado vale pues por el Teorema del Binomio

$$(\alpha + \beta)^p = \sum_{k=0}^{p} \binom{p}{k} \alpha^k \beta^{n-k}$$

y para $0 < k < p$ el número $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ debe ser divisible por p pues p no puede dividir a $k!(p-k)!$. Luego, todos los términos de la suma son 0 excepto el primero y el último. Por lo tanto $(\alpha + \beta)^p = \alpha^p + \beta^p$.

Ahora supongamos que el resultado se cumple para todo k, con $1 \leq k \leq n$. Por la hipótesis de inductiva,

$$(\alpha + \beta)^{p^{n+1}} = ((\alpha + \beta)^p)^{p^n} = (\alpha^p + \beta^p)^{p^n} = (\alpha^p)^{p^n} + (\beta^p)^{p^n} = \alpha^{p^{n+1}} + \beta^{p^{n+1}}.$$

Por lo tanto, el lema es verdadero para $n + 1$ y la demostración está completa. □

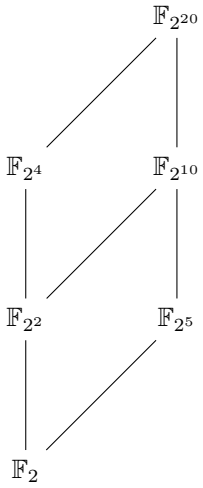
Recordemos que para $f \in \mathbb{F}_q[x]$, el anillo de clases residuales $\mathbb{F}_q[x]/(f(x))$ es un cuerpo si y sólo si f es irreducible. Además, si $f(x) \in \mathbb{F}_q[x]$ es un polinomio irreducible de grado d entonces $\mathbb{F}_q[x]/(f(x))$ es un cuerpo finito con q^d elementos:

$$\mathbb{F}_q[x]/(f(x)) \simeq \mathbb{F}_{q^d}.$$

Teorema 8. *Existe un único cuerpo (salvo isomorfismos) con q elementos si y sólo si $q = p^n$ para algún primo p y algún entero positivo n. Este cuerpo se denota por $\mathbb{F}_q$ y es el cuerpo de descomposición de $x^q - x$ sobre $\mathbb{F}_p$.*

El teorema anterior nos garantiza que hay cuerpos finitos con 2, 3, 4 y 5 elementos ya que todos esos números son primos o potencias de un primo, pero no existe ningún cuerpo finito con 6 elementos. Además, podemos caracterizar las extensiones de un cuerpo finito.

Teorema 9. *Si $\mathbb{F}_q$ es el cuerpo finito con $q = p^n$ elementos, entonces cada subcuerpo de $\mathbb{F}_q$ tiene orden p^m, donde m es un divisor positivo de n. Recíprocamente, si m es un divisor positivo de n, entonces existe exactamente un subcuerpo de $\mathbb{F}_q$ con p_m elementos.*



2. Códigos

2.1. Introducción. En 1948, Claude Shannon publicó el artículo *A mathematical theory of communication*, en el que demostró que, dado un canal de comunicación ruidoso, existe un número llamado la capacidad del canal, tal que la comunicación confiable se puede lograr a cualquier tasa por debajo de la capacidad del canal, si se utilizan técnicas adecuadas de codificación y decodificación en el mensaje. Esto marcó el inicio de la teoría de la códigos correctores de errores, es decir la teoría que estudia el problema de transmitir un mensaje de manera segura (confiable) a través de un canal no seguro (ruidoso) que puede producir errores y la recuperación de mensajes corruptos.

Los principales problemas de la teoría de códigos correctores de errores son:

1. Construir códigos que puedan corregir un número máximo de errores usando una cantidad mínima de redundancia.
2. Construir códigos (como arriba) con procedimientos de codificación y decodificación eficientes.

2.1.1. Definiciones básicas. En estas notas nos vamos a concentrar únicamente en códigos lineales definidos sobre cuerpos finitos, aunque estos pueden definirse más generalmente como un subconjunto no vacío de A^n siendo $A = \{a_1, a_2, \ldots, a_q\}$ un alfabeto.

Definición 10. Un *código lineal* C sobre $\mathbb{F}_q$ es un subespacio vectorial de $\mathbb{F}_q^n$, para algún n natural. Los elementos de C se llaman palabras o palabras código. Decimos que n es la *longitud* del código, y si k es la dimensión de C como espacio vectorial sobre $\mathbb{F}_q$, entonces decimos que la *dimensión del código* es k.

La longitud y la dimensión del código son dos parámetros importantes que nos permiten, por un lado comparar diferentes códigos, y por el otro lado, "medir" la bondad del código. Otro parámetro importante, es la distancia que introducimos a continuación.

Definición 11. La *distancia de Hamming* entre dos vectores de $\mathbb{F}_q^n$ es la cantidad de posiciones en las cuales esos vectores difieren. Es decir, $d : \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow [0, n]$ se define por $d(x, y) = \#\{i : x_i \neq y_i, 1 \leq i \leq n\}$ donde $x = (x_1, \ldots, x_n)$ e $y = (y_1, \ldots, y_n)$.

Lema 12. *La función d es un métrica. Es decir, satisface:*

(i) $d(x, y) = 0$ *si y sólo si* $x = y$ *y* $d(x, y) \geq 0$ *para todo* $x, y \in \mathbb{F}_q^n$*;*

(ii) $d(x,y) = d(y,x)$ *para todo* $x, y \in \mathbb{F}_q^n$;

(iii) $d(x,z) \leq d(x,y) + d(y,z)$ *para todo* $x, y, z \in \mathbb{F}_q^n$.

Demostración. Ejercicio. □

Definición 13. La *distancia mínima* de un código C, denotada $d(C)$ (o simplemente d), es el mínimo de todos los valores $d(x,y)$, donde x e y son palabras distintas de C, es decir $d(C) = \text{mín}\{d(x,y) : x, y \in C, x \neq y\}$. El *peso* w de una palabra código es la cantidad de coordenadas no nulas, es decir $w(x) = d(x,0)$ para todo $x \in C$, donde $0 = (0, \ldots, 0)$.

Lema 14. *Si* $x, y \in \mathbb{F}_q^n$ *entonces* $d(x,y) = w(x-y)$.

Demostración. Ejercicio. □

Si C es un subespacio k-dimensional de $\mathbb{F}_q^n$, entonces decimos que el código lineal C es un $[n,k]$-código y si queremos especificar la distancia mínima decimos que es un $[n,k,d]$-código.

Proposición 15. *Sea* C *un* $[n,k,d]$*-código y sea* $w(C) = \text{mín}\{w(x) : x \in C, x \neq 0\}$ *el peso mínimo del código. Entonces* $w(C) = d(C)$.

Demostración. Sean x, y en C tales que $d(C) = d(x,y)$. Entonces $d(C) = d(x,y) = w(x-y) \geq w(C)$. Por otro lado, si $z \in C$ satisface $w(C) = w(z)$, entonces $w(C) = w(z) = d(z,0) \geq d(C)$. Luego $w(C) = d(C)$. □

Podemos apreciar la importancia de este resultado en el siguiente ejemplo.

Ejemplo 16. Supongamos que tenemos el código binario de longitud 7 que consiste en las tuplas:

$$\begin{aligned} C = \{&(0000000), (0001111), (0010101), (0011010), (0100110), (0101001), (0110011), (0111100), \\ &(1000011), (1001100), (1010110), (1011001), (1100101), (1101010), (1110000), (1111111)\}. \end{aligned}$$

Es una tarea sencilla aunque tediosa verificar que el conjunto anterior es efectivamente un código sobre $\mathbb{F}_2$. Calcular todas las distancias entre pares de palabras no nulas del código es un trabajo largo y tedioso. Sin embargo, es mucho más sencillo calcular el peso de cada palabra no nula para chequear que es 3. Luego, la distancia mínima de este código es 3 y cómo veremos más adelante, esto significa que este código es capaz de detectar hasta 2 errores cometidos, pero puede corregir correctamente hasta un error.

2.1.2. El problema de la decodificación. Supongamos que nos envían una palabra código x de un $[n,k,d]$-código C y recibimos un vector y de $\mathbb{F}_q^n$ que puede ser distinto de x. Es razonable decodificar y como la palabra código z tal que $d(y,z)$ sea lo más pequeña posible. Esto se denomina *decodificación del vecino más cercano* y funcionará mejor cuando se cumpla:

(i) cada símbolo transmitido tiene la misma probabilidad $p < 1/2$ de ser recibido con error;

(ii) si un símbolo es recibido con error, cada uno de los $q-1$ posibles errores tiene la misma probabilidad.

Ejemplo 17. Sea C_1 el código lineal sobre $\mathbb{F}_2$ definido como $C_1 = \{(0), (1)\}$. Este código, no es capaz de detectar ni de corregir errores. Si en cambio consideramos el código lineal $C_2 = \{(00); (11)\}$ entonces este código es capaz de detectar hasta un error, pero no es capaz de corregirlo. Si consideramos el código lineal $C_3 = \{(000), (111)\}$ entonces tendremos un código capaz de detectar hasta 2 errores pero de corregir correctamente sólo un error. Por ejemplo, si se envía la palabra $x = (000)$ y se recibe el vector $y = (010)$ sabremos que se cometió un error en la transmisión

(pues y no es una palabra del código) y la podemos decodificar correctamente como x, ya que $d(x,y) < d(y,(111))$. Sin embargo, si al enviar x recibimos $z = (011)$ el código será capaz de detectar que se cometió un error en la transmisión pero al decodificarlo con el vecino más cercano, lo hará erróneamente como la palabra código (111).

Es posible determinar la cantidad máxima de errores que un código de distancia mínima d puede detectar y corregir.

Teorema 18. *Un $[n,k,d]$-código C puede:*

(i) *detectar hasta $d-1$ errores;*
(ii) *corregir hasta $\lfloor \frac{d-1}{2} \rfloor$ errores.*

Demostración. (i) Supongamos que una palabra código x es transmitida y se recibe un vector y con a lo sumo $d-1$ errores. Entonces y no puede ser una palabra del código pues la distancia mínima de C es d y $d(x,y) \leq d-1 < d(C)$. Por lo tanto, se detectó que se han cometido errores en la transmisión.

(ii) Sea $t = \lfloor \frac{d-1}{2} \rfloor$ y supongamos que una palabra código x es transmitida y se recibe un vector y con a lo sumo t errores. Entonces $d(x,y) \leq t$. Si z es otra palabra código cualquiera, entonces como $d(x,z) \leq d(x,y) + d(y,z)$ tenemos que $d(y,z) \geq d(x,z) - d(x,y) \geq d - t > t$ y por lo tanto, x es la palabra código más cercana a y. □

2.2. Algunas cotas básicas. Uno de los problemas básicos de la teoría de códigos es construir, sobre un alfabeto fijo $\mathbb{F}_q$, códigos cuyas dimensiones y distancias mínimas sean grandes comparadas con su longitud. Sin embargo existen algunas restricciones, ya que si la dimensión de un código es grande en comparación con la longitud, entonces su distancia mínima deberá ser pequeña. La cota más simple para estos parámetros es la siguiente.

Proposición 19 (Cota de Singleton)**.** *Para un $[n,k,d]$-código C se verifica que*

$$k + d \leq n + 1.$$

Demostración. Consideremos el subespacio vectorial $E \in \mathbb{F}_q^n$ dado por

$$E = \{(a_1, \ldots, a_n) \in \mathbb{F}_q^n : a_i = 0 \text{ para todo } i \geq d\}.$$

Cada $a \in E$ tiene peso $w(a) \leq d-1$, y por lo tanto $E \cap C = \emptyset$. Como $\dim E = d-1$ tenemos que

$$k + (d-1) = \dim C + \dim E = \dim(C+E) + \dim(C \cap E) = \dim(C+E) \leq n.$$ □

Esta cota muestra que a mayor capacidad de corrección, menor es la capacidad del código para transmitir un mensaje, y recíprocamente. Lo mejor que podemos esperar de los parámetros de un código es que se cumpla la igualdad. Los códigos que satisfacen la igualdad en la cota de Singleton se llaman *códigos MDS* (códigos con distancia máxima separables). Se puede probar, que si $n \leq q+1$, existen códigos MDS sobre $\mathbb{F}_q$ para todas las dimensiones $k \leq n$ (Códigos de Reed-Solomon).

La cota de Singleton no considera el tamaño del alfabeto. Existen otras cotas superiores para los parámetros k y d en función de la longitud n y del tamaño q del alfabeto. En general obtener cota inferiores para la distancia mínima de un código es un problema mucho más difícil. Sólo se conocen cotas inferiores para d generales para algunas clases de códigos, como los códigos BCH o los códigos de Goppa. Una de las razones principales por las que cobraron mucho interés los códigos algebraico-geométricos es que para esta amplia clase de códigos una buena cota inferior para la distancia mínima es conocida.

2.3. Codificación y decodificación.

Definición 20. Dada una base $\mathcal{B} = \{v_1, \ldots, v_k\}$ de un código C se define una *matriz generadora* del código G como la matriz cuyas filas son los vectores v_i de la base.

G no está unívocamente determinada por C, sino que depende la la elección de la base. Recíprocamente, dada una matriz de $n \times k$ cuyas filas son linealmente independientes, existe un [n,k]-código para el cual esta matriz es la matriz generadora.

Observación 21. Si dos matrices son equivalentes por filas entonces definen el mismo código.

Para un [n,k]-código C sobre $\mathbb{F}_q$ podemos definir una forma de codificar mensajes usando una matriz generadora G. Los mensajes son vectores arbitrarios de $\mathbb{F}_q^k$ y podemos codificarlos con la inyección de $\mathbb{F}_q^k$ en $\mathbb{F}_q^n$ que lleva un mensaje $u \in \mathbb{F}_q^k$ en una palabra código $c = uG \in \mathbb{F}_q^n$.

Ejemplo 22. Sea C el código binario, es decir sobre $\mathbb{F}_2$, de longitud 4 y dimensión 2 generado por la matriz

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

Entonces $C = \{(0000), (1011), (0101), (1110)\}$. Por lo tanto la distancia mínima del código es $d(C) = 2$.

Definición 23. Una matriz generadora se dice que está en *forma estándar* si es de la forma $G = (I_k|A)$ donde I_k es la matriz identidad de $k \times k$ y A es una matriz de $k \times n - k$.

Si G está en forma estándar, entonces codificar y decodificar mensajes es trivial ya que en esta situación el esquema resulta

$$u \in \mathbb{F}_q^k \quad \longrightarrow \quad c = uG = (u|uA) \in \mathbb{F}_q^n \quad \longrightarrow \quad u = c_{|_{\mathbb{F}_q^k}} \in \mathbb{F}_q^k.$$

Claramente para toda matriz generadora hay una matriz equivalente por renglones que está en forma estándar, y por lo tanto si C tiene una matriz G que no está en forma estándar podemos conseguir un código equivalente cuya matriz generadora es la forma escalonada reducida por renglones de la matriz G.

En $\mathbb{F}_q^n$ podemos definir un producto interno como

$$\langle a, b \rangle = \sum_{i=1}^{n} a_i b_i,$$

para $a = (a_1, \ldots, a_n)$ y $b = (b_1, \ldots, b_n)$ en $\mathbb{F}_q^n$.

Definición 24. Si C es un código sobre $\mathbb{F}_q$, entonces

$$C^\perp = \{u \in \mathbb{F}_q^n : \langle u, c \rangle = 0 \text{ para todo } c \in C\}$$

se llama *código dual* de C. Un código C se llama *auto dual* si $C^\perp = C$.

Proposición 25. *Si C es un $[n,k]-$código sobre $\mathbb{F}_q$ entonces $C^\perp$ es un $[n, n-k]-$código sobre $\mathbb{F}_q$.*

Demostración. Ejercicio. □

Definición 26. Una matriz H de $(n-k) \times n$ que es una matriz generadora de $C^\perp$ se llamará *matriz de control* o *matriz de chequeo de paridad* del código C.

Claramente, una matriz de control de C es una matriz de rango $n-k$ que satisface que para todo vector $x \in \mathbb{F}_q^n$ se verifica que $x \in C$ si y sólo si $Hx^T = 0$. Por lo tanto, esta matriz permite decidir (o controlar) si un vector está en el código o no.

Lema 27. *Sea C un $[n,k]$-código sobre $\mathbb{F}_q$ con matriz de control H. Entonces una matriz G de $k \times n$ es una matriz generadora de C si y sólo si sus filas son linealmente independientes y $HG^T = 0$.*

No hay una manera efectiva de calcular la distancia mínima de un código a partir de su matriz generadora, sin embargo, esto es posible a partir de la matriz de control.

Teorema 28. *Sea C un $[n,k,d]$-código y sea H una matriz de control para C. Entonces*

$$d = \text{mín}\{r : \text{ hay } r \text{ columnas linealmente dependientes en } H\}.$$

Es decir, H tiene d columnas linealmente dependientes pero cualquier conjunto de $d-1$ columnas son linealmente independientes.

Demostración. Sean H^1, H^2, ..., H^n las columnas de H. Entonces

$$c = (c_1, \ldots, c_n) \in C \iff cH^T = 0 \iff c_1H^1 + \cdots + c_nH^n = 0.$$

Si $c \in C$ es una palabra de peso mínimo d tenemos que H tiene d columnas linealmente dependientes en H, y no puede haber ninguna cantidad menor de columnas linealmente dependientes porque en ese caso habría palabras no nulas en C con peso menor a d. Recíprocamente, si hay r columnas linealmente dependientes entonces hay palabras de peso r y la distancia mínima es el menor de esos pesos. □

Si la matriz generadora G de un código C se encuentre en forma estándar, es decir $G = (I_k|A)$ entonces una matriz de control para C es $H = (-A^T|I_{n-k})$ donde I_{n-k} es la matriz identidad de tamaño $n-k$. En efecto,

$$GH^T = (I_k|A)\begin{pmatrix} -A \\ I_{n-k} \end{pmatrix} = -A + A = 0.$$

Una matriz H de esta forma se dice que está en *forma estándar como matriz de paridad* (aunque no está en forma estándar como matriz generadora de $C^\perp$).

Ejemplo 29. Consideremos el código lineal sobre $\mathbb{F}_q$ cuya matriz de control es

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

y veamos cómo encontrar una matriz generadora para el código y sus parámetros.

Como H es una matriz de tamaño 3×6 entonces la longitud del código es 6 y la dimensión es 3. Además como hay tres columnas linealmente dependientes y cualquier par de columnas son linealmente independientes entonces la distancia mínima es $d = 3$. Por otro lado, como H está en forma estándar como matriz de paridad entonces

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

y por lo tanto $C = \{(000000), (100011), (010101), (001110), (110111), (011011), (101101), (111000)\}$.

Usando la matriz generadora sabemos cómo codificar y un mensaje. Ahora nos interesa conocer algún método para recuperar un mensaje que se ha transmitido con error para poder decodificar y recuperar el mensaje original.

Con la matriz de control podemos determinar si un vector recibido es una palabra del código o no. Si no lo es, debemos elegir aquella palabra con la mínima distancia a una palabra del código, pues siempre suponemos que el número de errores es mínimo. Supongamos que se envía una palabra código $x = (x_1, \ldots, x_n)$ a través de un canal pero se recibe el vector $y = (y_1, \ldots, y_n)$. Definimos el vector de error como $e = y - x$. El decodificador deberá decidir a partir de y cuál fue la palabra enviada, o equivalentemente, cuál fue el error cometido.

Definición 30. Si C es un $[n, k]-$código sobre $\mathbb{F}_q$ y $a \in \mathbb{F}_q^n$, definimos la *clase lateral izquierda* $a + C$ como $a + C = \{a + x : x \in C\}$.

Recordemos que como $C \in \mathbb{F}_q^n$ es un espacio vectorial, entonces el cociente

$$\mathbb{F}_q^n / C = \{a + C : a \in \mathbb{F}_q^n\}$$

también es un espacio vectorial formado por todas las clases laterales con las operaciones

$$\alpha(a + C) = \alpha a + C \qquad (a + C) + (b + C) = (a + b) + C$$

con $\alpha \in \mathbb{F}_q$ y $a, b \in \mathbb{F}_q^n$, y además $|\mathbb{F}_q^n / C| = |\mathbb{F}_q^n| / |C| = q^n / q^k = q^{n-k}$.

Teorema 31. *Si C es un $[n, k]-$código sobre $\mathbb{F}_q$ entonces cada vector de $\mathbb{F}_q^n$ pertenece a una clase lateral de C. Cada clase contiene q^k vectores y hay q^{n-k} clases disjuntas, ya que dos clases laterales o son disjuntas o coinciden.*

Para cada clase lateral elegimos como líder a un vector que tenga peso mínimo, y si hay más de uno con peso mínimo elegimos a cualquiera de ellos. Entonces, si C es un $[n, k]-$código podemos escribir

$$\mathbb{F}_q^n = (0 + C) \cup (a_1 + C) \cup \cdots \cup (a_s + C)$$

donde $s = q^{n-k} - 1$ y $0, a_1, \ldots, a_s$ son los líderes de cada clase lateral de C.

Para decodificar un vector recibido debemos determinar a qué clase lateral pertenece para luego restarle el líder de la clase y obtener así una palabra código. Para utilizar este método debemos ordenar q^n vectores ordenados por clases, distinguiendo al líder de cada clase.

Ejemplo 32 (Continuación del ejemplo 22). Si $C = \{(0000), (1011), (0101), (1110)\}$ entonces las clases laterales son

$$(0000) + C = \{(0000), (1011), (0101), (1110)\}$$
$$(1000) + C = \{(1000), (0011), (1101), (0110)\}$$
$$(0100) + C = \{(0100), (1111), (0001), (1010)\}$$
$$(0010) + C = \{(0010), (1001), (0111), (1100)\}$$

Como este código tiene distancia mínima 2 es capaz de detectar cuando se ha cometido un error. Ademas, este método permite corregir hasta un error si el mismo ocurre en cualquiera de las tres primeras posiciones (pero no en la cuarta). Por ejemplo, si se envía la palabra código $x = (0101)$ pero se recibe la palabra $y = (1101)$, sabemos que y no es un palabra código por lo que detectamos que se cometió un error, y como $y \in (1000) + C$ entonces decodificamos a y como $y - (1000) = x$. Sin embargo, si se comete un error en el último dígito, y al enviar la palabra $x = (0101)$ se recibe el vector $z = (0100)$ entonces nuevamente podemos detectar que se ha cometido un error, pero la decodificación por este método nos devolverá erróneamente la palabra (0000). Para asegurarnos que podemos

corregir correctamente un error en cualquier coordenada, deberíamos utilizar un código cuya distancia mínima sea al menos 3.

Otro método para decodificar utilizando códigos lineales es la decodificación de síndrome.

Definición 33. Si C es un $[n,k]-$código sobre $\mathbb{F}_q$ y H es una matriz de paridad para C, entonces para cualquier vector $y \in \mathbb{F}_q^n$ definimos el *síndrome* de y como $S(y) = yH^T$.

Claramente, $S(y) = 0$ si y sólo si $y \in C$ y dos vectores u y v están en la misma clase lateral de C si y sólo si $S(u) = S(v)$. Luego, para detectar si se ha cometido un error en la transmisión de un mensaje basta con calcular el síndrome del mensaje recibido y, y sabremos que no es una palabra código si $S(y) \neq 0$ y en ese caso para decodificar el mensaje hacemos $y - a_j$ donde a_j es el lider de la clase lateral que tiene el mismo síndrome que y (para ello debemos calcular los síndromes de todos los lideres de las clases laterales.)

Ejemplo 34 (Continuación del ejemplo 22). Para el código $C = \{(0000), (1011), (0101), (1110)\}$ una matriz de control es

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

Los síndromes de los líderes de las clases laterales son $S(0000) = (00)$, $S(1000) = (10)$, $S(0100) = (01)$ y $S(0010) = (11)$. Entonces si al enviar la palabra $x = (0101)$ recibimos el vector $y = (1101)$, calculamos $S(y) = S(1101) = (10)$ y detectamos que se ha cometido un error. Además como $S(y) = S(1000)$ decodificamos a y como $y - (1000) = x$.

Ejercicio 35. Hacer una tabla de síndromes y líderes para el código binario cuya matriz generadora es

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

¿Cuáles son los parámetros de este código? ¿Cuántos errores puede detectar? ¿y corregir?

2.4. Códigos especiales.

2.4.1. Códigos de Hamming. Vamos a estudiar ahora una clase particular de códigos llamados Códigos de Hamming. Estos son un tipo particular de los denominados *códigos perfectos* que son códigos que corrigen hasta t errores en donde las esferas de radio t centradas en las palabras códigos cubren completamente y de forma disjunta a $\mathbb{F}_q^n$ (satisfacen lo que se llama la cota de Hamming). Los códigos de Hamming, pueden corregir hasta un error, y su característica principal es que están definidos sobre cualquier cuerpo finito y poseen facilidad para codificar y decodificar mensajes.

Definición 36. Un código binario de Hamming H_r de largo $n = 2^r - 1$, se define por su matriz de control cuyas columnas consisten en todos los vectores binarios no nulos de largo r. Esto nos da un $[n,k,d]$-código lineal sobre $\mathbb{F}_2$ con $n = 2^r - 1$, $k = 2^r - r - 1$ y $d = 3$.

Ejemplo 37. Una matriz de control para el $[7,4,3]-$código H_3 es:

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

donde podemos reconocer que las columnas de H son las expresiones binarias de los números del 1 al 7. Para encontrar las $2^4 = 16$ palabras código de C tenemos que resolver las ecuaciones determinadas por H:

$$\begin{cases} x_4 + x_5 + x_6 + x_7 &= 0 \\ x_2 + x_3 + x_6 + x_7 &= 0 \\ x_1 + x_3 + x_5 + x_7 &= 0 \end{cases}$$

Una base se obtiene tomando x_1, x_2, x_3 y x_4 como variables libres y por lo tanto una matriz generadora para este código es

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

La decodificación con este código es particularmente fácil. Observemos que los líderes de las clases son todos vectores de peso menor o igual a 1 y el síndrome correspondiente se puede interpretar como el número binario que nos indica la columna en la que ocurrió el error de transmisión. Por ejemplo, si queremos enviar el mensaje (0110) y al codificar obtenemos la palabra código $x = (0110011)$ pero al enviarla se recibe el vector $y = (0100011)$. Entonces su síndrome es $S(y) = yH^T = (011)$ que son los dígitos del número 3 en binario. Corregimos la tercera posición y recuperamos $x = (0110011)$.

Los códigos binarios de Hamming pueden generalizarse a cualquier alfabeto $\mathbb{F}_q$.

Definición 38. Un código q-ario de Hamming $H_{q,r}$ de largo $n = (q^r - 1)/(q - 1)$, se define por su matriz de control cuyas columnas se eligen de la siguiente manera: se elige primeramente una columna no nula $H^1 \in V_1 = \mathbb{F}_q^r$. Luego se elige cualquier columna no nula $H^2 \in V_2 = V_1 \setminus \{\alpha H^1 : \alpha \in \mathbb{F}_q^*\}$. Continuamos eligiendo columnas no nulas de esta forma y descartamos múltiplos escalares de las columnas elegidas hasta agotar todas las columnas de $\mathbb{F}_q^r$. Esto nos da un $[n, k, d]$-código lineal sobre $\mathbb{F}_2$ con $n = (q^r - 1)/(q - 1)$, $k = n - r$ y $d = 3$.

Una forma fácil de construir una matriz de control para $H_{q,r}$ es tomar todos los vectores de $\mathbb{F}_q^r$ cuya primer coordenada no nula es 1. En efecto hay $q^r - 1$ vectores no nulos y el primer elemento puede ser $1, 2, \ldots, q - 1$. Luego tendremos $(q^r - 1)/(q - 1)$ vectores cuya primer coordenada no nula es 1.

Ejemplo 39. El código $H_{3,3}$ tiene parámetros $[13, 10, 3]$ y una matriz de control es

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

La decodificación en este caso es similar al caso binario. Si cometemos un error en la coordenada i, el vector que recibiremos es $y = c + e$ donde $e = \alpha e_i$ siendo e_i el i-ésimo vector canónico y $\alpha \in \mathbb{F}_q^*$. Luego el síndrome es

$$s(y) = yH^T = cH^T + eH^T = 0 + \alpha\, e_i H^T = \alpha\, (H^i)^T$$

que nos da α multiplicado por la i-ésima columna de H (transpuesta), y por lo tanto el síndrome nos identifica en qué coordenada se ha cometido el error.

Ejemplo 40. Si consideramos el código del ejemplo anterior $H_{3,3}$ y recibimos la palabra $y = 1101112211201$, al calcular su síndrome obtenemos

$$yH^T = (201) = 2(102) = 2\,\text{columna 7 de H.}$$

Por lo tanto hay un error de magnitud 2 en la coordenada 7 de y y se puede corregir como $c = y - 2e_7 = 1101110211201$.

2.4.2. Códigos de Reed-Solomon. Escribamos al cuerpo finito con q elementos como $\mathbb{F}_q = \{0, \alpha_1, \alpha_2, \ldots, \alpha_{q-1}\}$. Para $r \in \mathbb{N}_0$ definimos

$$L_r = \{f \in \mathbb{F}_q[x] : deg\, f \leq r\} \cup \{0\}.$$

L_r es un espacio vectorial sobre $\mathbb{F}_q$ de dimensión $r+1$ (una base es $\{\alpha_1, x, x^2, \ldots, x^r\}$).

Definición 41. El código de Reed-Solomon $RS(k,q)$ se define para $k \leq q-1$ como

$$RS(k,q) = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_{q-1})) : f \in L_{k-1}\}.$$

$RS(k,q)$ es un código lineal sobre $\mathbb{F}_q$ (Ejercicio) de longitud $n = q-1$. Para encontrar su dimensión notemos que $RS(k,q)$ es la imagen de la transformación lineal $\sigma : L_{k-1} \to \mathbb{F}_q^{q-1}$ tal que $\sigma_(f) = (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_{q-1}))$, por lo tanto $\dim RS(k,q) \leq \dim L_{k-1} = k$, y probaremos que es una transformación inyectiva para obtener que $\dim RS(k,q) = k$. En efecto, si $\sigma(f) = (0,0,\ldots,0)$ con $f \neq 0$ entonces f tiene al menos $q-1$ raíces en $\mathbb{F}_q$ pero como $f \in L_{k-1}$ entonces $deg\, f \leq k-1 \leq q-2$, lo cual es absurdo.

Para calcular la distancia mínima d de $RS(k,q)$, consideremos $f \neq 0$ tal que $\sigma(f)$ tiene peso d. Entonces f tiene al menos $n-d$ ceros (la cantidad de coordenadas no nulas de $\sigma(f)$) y por lo tanto $deg\, f \geq n-d$. Pero como $f \in L_{k-1}$ entonces $n - d = deg\, f \leq k-1$. Por la cota de Singleton, sabemos que $d + k \leq n+1$ y por lo tanto debe ser que $d = n+1-k$.

Hemos probado que para cada $k \leq q-1$, el código de Reed-Solomon $RS(k,q)$ es un código MDS con parámetros $n = q-1$, k, $d = n-k+1$.

2.4.3. Códigos cíclicos.

Definición 42. Decimos que un $[n,k]$-código C es un código cíclico si para todo $(c_0, c_1, \ldots, c_{n-1}) \in C$ tenemos que $(c_1, \ldots, c_{n-1}, c_0) \in C$.

Ejercicio 43. El código binario $C = \{000, 110, 101, 011\}$ es un $[3,2,2]-$código cíclico.

Para facilitar el trabajo con códigos cíclicos, vamos a introducir ahora una manera algebraica de caracterizarlos. Consideremos

$$\begin{array}{rccc} \pi : & \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q[x]/(x^n-1) \\ & (a_0, a_1, \ldots, a_{n-1}) & \to & a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \end{array}$$

Como π es un isomorfismo de espacios vectoriales sobre $\mathbb{F}_q$ podemos identificar $\mathbb{F}_q^n$ con $\mathbb{F}_q[x]/(x^n-1)$ y a C con

$$\pi(C) = \{c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} : c = (c_0, c_1, \ldots, c_{n-1})\}.$$

Ejemplo 44. Si $C = \{000, 110, 101, 011\}$ entonces

$$\pi(C) = \{0, 1+x, 1+x^2, x+x^2\} \subset \mathbb{F}_2[x]/(x^3-1).$$

Podemos ver que $\pi(C)$ es un ideal de $\mathbb{F}_2[x]/(x^3-1)$. Más aún, es el ideal generado por $(x+1)$.

Teorema 45. *Un código C de $\mathbb{F}_q^n$ es cíclico si y sólo sí $\pi(C)$ es un ideal de $\mathbb{F}_q[x]/(x^n-1)$.*

Demostración. El teorema se obtiene de hecho de que si $(c_0, c_1, \ldots, c_{n-1}) \in C$ entonces

$$x(c_0 + c_1x + \cdots + c_{n-1}x^{n-1}) = c_0x + c_1x^2 + \cdots + c_{n-1}x^n \mod (x^n-1) = c_{n-1} + c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1}.$$

□

El siguiente resultado reúne algunos hechos básicos de los códigos cíclicos.

Teorema 46. *Sea C un ideal de $\mathbb{F}_q[x]/(x^n-1)$, es decir un código cíclico de longitud n. Entonces existe un único polinomio mónico de grado mínimo $g(x)$ en C tal que $g(x)$ genera a C y divide a x^n-1. Además, si $g(x) = g_0 + g_1x + \cdot + g_rx^r$ entonces $g_0 \neq 0$, C tiene dimensión $n-r$ y la matriz generadora de C es*

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & \cdots & g_r & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & \cdots & g_r & 0 & \cdots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \cdots & \cdots & g_r & \cdots & 0 \\ \vdots & \vdots & & \ddots & \ddots & \ddots & & & \ddots & \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & \cdots & g_r \end{pmatrix}$$

Demostración. Supongamos que C contiene dos polinomios mónicos $g_1(x)$ y $g_2(x)$ de grado mínimo distintos. Entonces $g_1(x) - g_2(x)$ es un polinomio no nulo de C de grado menor lo cual es absurdo. Luego hay un sólo polinomio $g(x)$ mónico de grado mínimo en C.

Ahora, como C es un ideal entonces $\langle g(x)\rangle \subset C$. Por otro lado, supongamos que $c(x) \in C$. Entonces existen $q(x)$ y $r(x)$ tales que

$$c(x) = q(x)g(x) + r(x) \qquad 0 \leq deg\, r(x) < deg\, g(x).$$

Como $g(x)$ tiene grado mínimo, debe ser que $r(x) = 0$ y por lo tanto $c(x) = q(x)g(x) \in \langle g(x)\rangle$. Luego $C = \langle g(x)\rangle$.

Si dividimos $x^n - 1$ por $g(x)$ tenemos que

$$x^n - 1 = p(x)g(x) + s(x) \qquad 0 \leq deg\, s(x) < deg\, g(x).$$

Como en $\mathbb{F}_q[x]/(x^n-1)$ tenemos que $x^n - 1 = 0 \in C$ entonces $s(x) \in C$ y como tiene grado menor que $g(x)$ debe ser $s(x) = 0$. Luego $g(x)$ divide a $x^n - 1$.

Para demostrar que C tiene dimensión $n-r$ vamos a mostrar que $C = \langle g(x)\rangle = \{u(x)g(x) : deg\, u(x) < n-r\}$. Sabemos que $x^n - 1 = p(x)g(x)$ con $deg\, p(x) = n-r$. Si $v(x) \in C$ entonces $v(x) = f(x)g(x)$ para algún $f(x) \in \mathbb{F}_q[x]/(x^n-1)$ y dividiendo a $f(x)$ por $p(x)$ tenemos $f(x) = h(x)p(x) + u(x)$ con $deg\, u(x) < n-r$. Entonces

$$v(x) = f(x)g(x) = h(x)p(x)g(x) + u(x)g(x) = h(x)(x^n-1) + u(x)g(x)$$

y por lo tanto $v(x) = u(x)g(x)$ en $\mathbb{F}_q[x]/(x^n-1)$, que es lo que queríamos probar. Esto también prueba que

$$\{g(x), xg(x), \ldots, x^{n-r+1}g(x)\}$$

es una base de C.

Supongamos ahora que $g(x) = g_0 + g_1x + \cdot + g_rx^r$ y que $g_0 = 0$. Entonces $g(x) = xg_1(x)$ con $deg\, g_1(x) < r$, pero esto es absurdo pues

$$g_1(x) = 1 \cdot g_1(x) \equiv x^n \cdot g_1(x) = x^{n-1}g(x) \in C$$

y es de grado menor que $g(x)$. Luego $g_0 \neq 0$. Finalmente, G es la matriz generadora de C pues

$$\{g(x), xg(x), \ldots, x^{n-r+1}g(x)\}$$

es una base de C. □

En el siguiente ejemplo veremos que en realidad, un código cíclico puede estar generado por otros polinomios además del polinomio generador.

Ejemplo 47. Consideremos el código cíclico C en $\mathbb{F}_2[x]/(x^3-1)$ generado por $1+x$, es decir $C = \langle 1+x \rangle$. Por el teorema anterior, $\dim C = 3-1 = 2$ y C está formado por los múltiplos de $1+x$:

$$0, \qquad 1+x, \qquad x(1+x) = x+x^2, \qquad (1+x)(1+x) = 1+x^2.$$

Luego

$$C = \{0, 1+x, 1+x^2, x+x^2\} = \{000, 110, 101, 011\}.$$

Sin embargo, notemos que

$$\langle 1+x^2 \rangle = \{0, 1+x^2, x(1+x^2), (1+x)(1+x^2)\} = \{0, 1+x^2, 1+x, x+x^2\} = C,$$

es decir, C también está generado por $1+x^2$ que no divide a x^3-1.

Dado que todo código cíclico de longitud n sobre $\mathbb{F}_q$ está generado por un divisor mónico de x^n-1, si somos capaces de factorizar al polinomio x^n-1 en $\mathbb{F}_q$ entonces podremos saber cuáles son todos los códigos cíclicos q-arios de longitud n. Sin embargo, podría suceder que algunos de ellos sean equivalentes entre sí.

2.4.4. Códigos BCH. Los códigos BCH una clase particular de códigos cíclicos que permiten corregir un número arbitrario de t errores. Llevan el nombre quienes los propusieron: Bose, Chaudhuri y Hocquenghem. Estos códigos tienen una gran versatilidad para el diseño, ya que existe un gran número de polinomios generadores previamente tabulados. De esta forma, el usuario sólo debe determinar unos parámetros de diseño, que dependen del número de errores que desee corregir y posteriormente, con esos parámetros buscar el polinomio generador en una tabla. Existen además algoritmos eficientes para su decodificación. Los parámetros de diseño se determinan a partir de las ecuaciones

$$n = q^m - 1, \qquad n-k = mt, \qquad d = 2t+1.$$

Definición 48. Sea α un elemento primitivo de $\mathbb{F}_{q^m}$ y denotemos por $M^{(i)}(x)$ al polinomio mínimo de α^i sobre $\mathbb{F}_q$. Un código BCH (primitivo) sobre $\mathbb{F}_q$ de largo $n = q^m - 1$ y distancia mínima de diseño d es un código cíclico generado por

$$g(x) = \text{mcm}\{M^{(a)}(x), M^{(a+1)}(x), \ldots, M^{(a+d-2)}(x)\}$$

para algún entero a.

Ejemplo 49. Si consideramos el código cíclico BCH con $m = 1$ entonces $n = q-1$. Sea α un elemento primitivo de $\mathbb{F}_q$ y sea C el $[n,k]-$código cíclico q-ario generado por

$$g(x) = (x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{n-k}).$$

En este caso, C es equivalente al $RS(k,q)$.

Ejemplo 50. Consideramos α un elemento primitivo de $\mathbb{F}_{16} = \mathbb{F}_{2^4}$ con $\alpha^4 + \alpha + 1 = 0$ y tomemos $d = 5$. Vamos a construir el código BCH binario de largo $n = 16 - 1 = 15$ y distancia de diseño 5. Necesitamos calcular los polinomios $M^{(1)}(x)$, $M^{(2)}(x)$, $M^{(3)}(x)$ y $M^{(4)}(x)$, que son los polinomios mínimos de α^i sobre $\mathbb{F}_2$. Sabemos que $M^{(1)}$, el polinomio mínimo de α, es $M^{(1)} = x^4 + x + 1$. Además como $q = 2$ entonces $M^{(1)}(x) = M^{(2)}(x) = M^{(4)}(x)$ (Ejercicio).

Nos falta calcular $M^{(3)}(x)$. Para calcular el polinomio mínimo de α^3 podemos calcular sus potencias y buscar una relación de dependencia lineal. Sea $\beta = \alpha^3$.

$$\begin{aligned}
\beta^0 =& (\alpha^3)^0 = 1\\
\beta^1 =& (\alpha^3)^1 = \alpha^3\\
\beta^2 =& (\alpha^3)^2 = \alpha^6 = \alpha^2\alpha^4 = \alpha^2(\alpha+1) = \alpha^3 + \alpha^2\\
\beta^3 =& (\alpha^3)^3 = \alpha^9 = \alpha\alpha^8 = \alpha(\alpha^4)^2 = \alpha(\alpha+1)^2 = \alpha^3 + \alpha\\
\beta^4 =& (\alpha^3)^4 = (\alpha^4)^3 = (\alpha+1)^3 = \alpha^3 + \alpha^2 + \alpha + 1
\end{aligned}$$

Entonces $\beta^4 + \beta^3 + \beta^2 + \beta + 1 = 0$ y podemos probar por inspección que $M^{(3)}(x) = x^4 + x^3 + x^2 + x + 1$. Luego

$$g(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1) = x^8 + x^7 + x^6 + x^4 + 1.$$

Ejercicio 51. Verificar que $g(x) = x^8 + x^7 + x^6 + x^4 + 1$ divide a $x^{15} - 1$ en $\mathbb{F}_{16}[x]$.

Referencias

[1] G. Cabaña. *Códigos algebraicos geométricos: aplicaciones del álgebra y la geometría a la teoría de la información.*, Monografía Programa Becas CIN, UNL, 2013. I.N. Herstein. *Topics in Algebra*, Xerox College Pub., second edition, 1975.

[2] Harald Niederreiter and Chaoping Xing, *Algebraic Geometry in Coding Theory and Cryptography*. Princeton University Press, NJ, USA, 2009.

[3] H. Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[4] J.H. van Lint. *Introduction to Coding Theory*, volume 86 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, third edition, 1998.

[5] J. Walker. *Codes and curves*, volume 7 of *Student Mathematical Library.*. AMS, 2000.

Universidad Nacional del Litoral - CONICET

Email address: charamaria@gmail.com