Códigos y criptografía

José Carlos García

2 de marzo de 2016

Índice general

Capítulo 1

Introducción

1.1. Cuerpos finitos

Definición 1 (Cuerpo)**.** *Un **cuerpo** es un anillo conmutativo con unidad en el que todo elemento distinto de 0 tiene inverso.*

Ejemplo 1. $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$ *es anillo conmutativo con unidad, además, si* n *es primo entonces* $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$ *es un cuerpo.*

La suma y el producto de $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$ se define como el resto de la suma de los elementos, para el producto de forma análoga.

Teorema 1. *Si un* K *es finito, entonces* $card(K) = p^r$ *con* $p \in \mathbb{P}$ *y* $r \in \mathbb{N}$

Teorema 2. *Dado* $p \in \mathbb{P}, r \in \mathbb{N}$ *entonces existe un cuerpo* K *tal que* $card(K) = p^r$*. Además, dos cuerpos finitos con el mismo cardinal son isomorfos.*

Definición 2 (Cuerpo finito de q elementos)**.** *Si* $q = p^r$ *denotamos por* $\mathbb{F}_q$ *el cuerpo finito de* q *elementos.*

Ejemplo 2. *Construir un cuerpo con 4 elementos.*
Consideremos $\mathbb{F}_2[x]$ *y el ideal* $< x^2+x+1 >$*, claramente* $< x^2+x+1 >$ *es irreducible en* $\mathbb{F}_2[x]$*, además* $\mathbb{F}_2[x]$ *es D.I.P., no existe ningún ideal* I*,* $< x^2+x+1 > \subset I \subset \mathbb{F}_2[x]$*, por tanto* $< x^2+x+1 >$ *es maximal, de aquí, se tiene que* $\mathbb{F}_2[x]/ < x^2+x+1 >$ *es cuerpo.*
Hacemos $\alpha = x + (x^2+x+1)$*. Los elementos de* $\mathbb{F}_2[x]/ < x^2+x+1 >$ *son:*

$$\begin{aligned} \alpha &= x + (x^2+x+1) \\ \alpha + 1 &= (x+1) + (x^2+x+1) \\ 1 &= 1 + (x^2+x+1) \\ 0 &= 0 + (x^2+x+1) \end{aligned}$$

$card(\mathbb{F}_2[x]/ < x^2+x+1 >) = 4$ *de la observación anterior.*

Algoritmo 1 (Algoritmo de Euclides)**.** *Se define el **algoritmo de Euclides** para calcular**máximo***

***común divisor**, de forma que sean $a, b \in \mathbb{N}$, con $a \geq b$ hacemos:*

$$\begin{aligned}
a &= c_1 b + r_1 \\
b &= c_2 r_1 + r_2 \\
r_1 &= c_3 r_2 + r_3 \\
r_2 &= c_4 r_3 + r_4 \\
&\dots \\
r_{s-2} &= c_s + r_{s-1} + r_s \\
r_{s-1} &= c_{s+1} + r_s
\end{aligned}$$

Podemos obtener $r_s = mcd(a, b)$ del modo siguiente:

$$\begin{aligned}
r_1 &= a - c_1 b \\
b &= c_2(a - c_1 b) + r_2 \\
r_2 &= -c_2 a + (1 + c_1) b
\end{aligned}$$

De este modo, podemos obtener r_s como continuación de a, b, de modo:
$mcd(a, b) = r_s = \lambda a + \mu b$

Observación 1. *λ, μ se obtienen de modo efectivo a partir de las divisiones anteriores.*

Ejemplo 3. *Calcular $mcd(139, 20)$.*
Y además, $\lambda, \mu \in \mathbb{Z}$ tales que $\lambda 139 + \mu 20 = mcd(139, 20)$.
Aplicando el algoritmo de Euclides:

$$\begin{aligned}
139 &= 6 \cdot 20 + 19 \\
20 &= 1 \cdot 19 + 1 \\
19 &= 139 - 6 \cdot 20 \\
1 = 20 - 1 \cdot 19 = 20 - 1(139 - 6 \cdot 20) &= 7 \cdot 20 - 1 \cdot 139
\end{aligned}$$

Observación 2. *El inverso de 20 en $\mathbb{F}_{139}$:*
$7 \cdot 20 - 1 \cdot 139 = 1$.
Si reducimos $\bmod 139$*:*

$$7 \cdot 20 = 1 \mod 139$$

El inverso de 20 en $\mathbb{F}_{139}$ es 7

Capítulo 2

Códigos autocorrectores

2.1. Parámetros de un código

Definición 3 (Alfabeto finito)**.** *Decimos que $\mathcal{A}$ es un **alfabeto finito** si $\mathcal{A}$ es conjunto finito de q símbolos.*

Definición 4 (Código)**.** *Decimos que $\mathcal{C}$ es un **código** si $\mathcal{C} \subset \mathcal{A}^n$, $\mathcal{C} \neq \emptyset$*

Definición 5 (Palabra)**.** *Decimos que x es una **palabra** si $x \in \mathcal{A}$.*

Definición 6 (Palabra-código)**.** *Decimos que c es una **palabra-código** si $c \in \mathcal{C}$.*

Ejemplo 4. *$\mathcal{A} = \mathbb{F}_2$. Tomamos $\mathcal{C} = \mathcal{A}$, aquí hay más probabilidad de error. $\mathcal{C}_2 = \{(000), (111)\} \subset \mathbb{F}_2^3$ código.*

Definición 7 (Parámetros de un código)**.** *Los **parámetros de un código** son:*

- ***Longitud**: n.*
- ***Razón de información:*** $\dfrac{\log_q \#\mathcal{C}}{n}$
- ***Distancia de Hamming:*** *Sean $x = (x_1, x_2, ..., x_n) \in \mathcal{A}^n$, $y = (y_1, y_2, ..., y_n) \in \mathcal{A}^n$ se define $d(x, y) = \#\{i : x_i \neq y_i\}$. Define una distancia métrica.*
- ***Distancia mínima:*** $d(\mathcal{C}) = \text{mín}\{d(c, c') : c, c' \in \mathcal{C}, c' \neq c\}$

Observación 3. *Sea $\mathcal{C}$ un código con distancia mínima $2d(\mathcal{C}) + 1$. Además:*

$$d(x, c_1) \leq d(\mathcal{C})$$

$$d(x, c_2) \leq d(\mathcal{C})$$

Ahora, por la desigualdad triangular

$$d(c_1, c_2) \leq d(c_1, x) + d(c_2, x) \leq d(\mathcal{C}) + d(\mathcal{C})$$

Por tanto, el código se decodificará con mayor facilidad.

Observación 4. *Si $d(\mathcal{C}) = 2d(\mathcal{C})+1$, dos bolas cualesquiera $B(c_1, d(\mathcal{C}))$, $B(c_2, d(\mathcal{C}))$, $c_1 \neq c_2 \in \mathcal{C}$ son disjuntos.*

Definición 8 (Código perfecto). *Un **código perfecto** es un código con* $d(\mathcal{C}) = 2d(\mathcal{C}) + 1$ *y tal que* $\{B(c, d(\mathcal{C}) : c \in \mathcal{C})\} = \mathcal{A}^n$

El **Ejemplo 4** corresponde a un código perfecto.

Notación 1. *Escribimos* $[n, M, d] -$ *código si queremos representar un código de longitud* n*,* M *elementos y diistancia mínima* d*.*

Ejemplo 5. *Sea* $\mathcal{C}_1 = \{0, 1\}$ *y* $\mathcal{C}_2 = \{(000), (111)\} \subset \mathbb{F}_2^3$*.*
Sea $0 < p < \dfrac{1}{2}$ *la probabilidad de que se produzca un error al trasmitir un bit.*
Como $p < \dfrac{1}{2}$ *proponemos un algoritmo de decodificación, por **máximo verosimilitud**, lo más probable es que la palabra enviada del código sea la palabra de las del código que está más cercana a la palabra recibida.*
Para $\mathcal{C}_1$*, la probabilidad de decodificar correctamente la palabra recibida es* $1 - p$*.*
Para $\mathcal{C}_2$*:* (000) *la decodificamos correctamente si al enviarla nos llega* (000)*, la probabilidad de que sea correcta sería* $(1-p)^3$*,* (100)*, la probabilidad de que sea correcta sería* $p(1-p)^2$*,* (010)*, la probabilidad de que sea correcta sería* $p(1-p)^2$ *y* (001) *la probabilidad de que sea correcta sería* $p(1-p)^2$*.*
Por tanto, la probabilidad sería $(1-p)^3 + 3p(1-p)^2$*.*
Si tomamos $p = 0{,}1$*, tendríamos para* $\mathcal{C}_1 : 0{,}9$ *y para* $\mathcal{C}_2 : 0{,}972$*.*

Ejemplo 6. *Sea* $\mathcal{C} = \{(000), (111)\} \subset \mathbb{F}_2^3$*.*

Recibida	Decodificar
(000)	(100)
(100)	(100)
(110)	(100)
(101)	(100)
(010)	(100)
(001)	(100)
(011)	(111)
(111)	(111)

De los que decodificamos como (100) *tenemos una probabilidad de acierto de* $(1-p)^3 + 3p(1-p)^2 + 2p^2(1-p)$*, en el otro caso tenemos* $(1-p)^3 + p(1-p)^2$*.*

2.2. Códigos lineales

Definición 9 (Código lineal). *Un **código lineal*** $\mathcal{C} \subset \mathbb{F}_q^n$ *donde* $\mathcal{C}$ *es un subespacio vectorial de* $\mathbb{F}_q^n$

Gracias a que es una estructura lineal, el código podemos simplificarlo teniendo en cuenta la base del subespacio vectorial.

Definición 10 (Peso de x). *Sea* $x = (x_1, x_2, ..., x_n) \in \mathbb{F}_q^n$*. El **peso** de* x *es* $w(x) = \#\{i : x_i \neq 0\}$

Notación 2. $\mathcal{C} \subset \mathbb{F}_q^n$*. Se define* $W(\mathcal{C}) = \text{mín}\{w(x) : x \in \mathcal{C}/\{0\}\}$

Proposición 1. *Si $\mathcal{C}$ es lineal, entonces $d(\mathcal{C}) = W(\mathcal{C})$*

Demostración. Sean $c_1 \neq c_2 \in \mathcal{C}$ que cumplen que $d(c_1, c_2) = d(\mathcal{C})$
Dado que $d(\mathcal{C}) = d(c_1, c_2) = w(c_1 - c_2)$, pero dado que $c_1 - c_2 \neq 0$, tenemos que $w(c_1 - c_2) \geq W(\mathcal{C})$, por tanto, $d(\mathcal{C}) \geq W(\mathcal{C})$.
Sea $c \in \mathcal{C} - \{0\}$, tal que cumple que $w(c) = W(\mathcal{C})$.
$W(\mathcal{C}) = w(c) = w(c - 0) = d(c, 0) \geq d()$ □

Notación 3. *Si $\mathcal{C} \subset \mathbb{F}_q^n$ lineal, $dim_{\mathbb{F}_1}\mathcal{C} = k$ decimos que $\mathcal{C}$ es un $[n, k] -$ código.*

Definición 11 (Matriz generadora)**.** ***Matriz generadora*** *de un $[n, k] -$ código es un matriz G, con dimensiones $k \times n$ cuyas filas forman una base de $\mathcal{C}$*

Ejemplo 7. *Si $\mathcal{C} = \{(000), (111)\}$, la matriz generadora es* (111)

Definición 12 (Matriz de control de paridad)**.** ***Matriz de control de paridad*** *de un $[n, k] -$ código lineal es una matriz H de orden $(n - k) \times n$ tal que:*

$$\mathcal{C} = \{x \in \mathbb{F}_q^n : xH^t = 0\}$$

Observación 5. *Si $\mathcal{G} = (I_k|P)$ es generadora, con P con $n - k$ columnas, entonces $H = (-p^t|I_{n-k})$ es de control de paridad.*

Ejemplo 8. *En $\mathbb{F}_3^5$ consideramos el código con matriz generadora:*

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

Tratemos de dar una base de la matriz:

$$\mathcal{C} = \{\lambda_1 \vec{u_1} + \lambda_2 \vec{u_2} + \lambda_3 \vec{u_3} : \lambda_i \in \mathbb{F}_3\}$$
$$= \{(\lambda_1, \lambda_2, \lambda_3, \lambda_1 + \lambda_2, \lambda_1 + \lambda_3) : \lambda_i \in \mathbb{F}_3\} =$$
$$= \{(x_1, x_2, x_3, x_4, x_4) \in \mathbb{F}_3^5 : (-x_3 - x_2 + x_4 = 0, x_4 = x_1 + x_2, x_5 = x_1 + x_3)\} =$$

La matriz de las ecuaciones anterior es:

$$\begin{pmatrix} -1 & -1 \\ -1 & 0 \\ 0 & -1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} = (0, 0)$$

La transpuesta de la matriz anterior es la matriz de control de paridad de $\mathcal{C}$

Algoritmo 2 (Algoritmo de decodificación usando el síndrome)**.** *Supongamos que $\mathcal{C} \subset \mathbb{F}_q$ es un código lineal, sea $x \in \mathbb{F}_q^n$, podemos decodificar x usando el código $\mathcal{C}$ comparando x con cada una de las palabras del código.*
Consideramos:

$$x - \mathcal{C} = \{x - c : c \in \mathcal{C}\} = x + \mathcal{C}$$

$x + \mathcal{C}$ es el conjunto de elementos que están en la misma clase $\mathbb{F}_q^n/\mathcal{C}$.
En el conjunto $x - \mathcal{C}$ consideramos un elemento e que tenga peso mínimo.
Si $e \in \mathcal{C}$ será de la forma $e = x - c$. Entonces $c \in \mathcal{C}$ está a la menor distancia de la palabra x.
Podemos decodificar la palabra x por la palabra c, que es $c = x - e$.
*A la palabra e se le llama **vector error** (asociado a x).*

Definición 13 (Sindrome de x)**.** *Sea H la matriz de control de paridad del código $\mathcal{C}$, consideramos $x \in \mathbb{F}_q^n$, se define **el síndrome** de x como $xH \in \mathbb{F}_q^{n-k}$.*

Observación 6. *Dos palabras $x, x' \in \mathbb{F}_q^n$ tienen el mismo síndrome si y sólo si $x + \mathcal{C} = x' + \mathcal{C}$. En efecto, si $x + \mathcal{C} = x' + \mathcal{C} \iff xH^t - x'H^t = 0 \iff xH^t = x'H^t$*

Algoritmo 3 (Algoritmo de decodificación usando síndrome)**.** *A continuación se nuestra el **algoritmo de decodificación usando síndrome***

1. *Para cada clase $x + \mathcal{C}$ de $\mathbb{F}_q^n/\mathcal{C}$ consideramos un $e \in x + \mathcal{C}$ de peso mínimo.*

2. *Para cada clase $x + \mathcal{C}$ calculamos el síndrome xH^t. Asociamos a ese síndrome el vector error e.*

3. *Cuando recibimos una palabra x, calculamos su síndrome, que tiene asociado un vector error e, y decodificamos x por $c = x - e$.*

Ejemplo 9. *En $\mathbb{F}_2^5$ consideramos el código $\mathcal{C}$ con matriz generadora:*

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

Para calcular $\mathbb{F}_2^5/\mathcal{C}$, ampliamos la matriz G de modo que sea una base de $\mathbb{F}_2^5$, de este modo la base de $\mathbb{F}_2^5/\mathcal{C}$ sería lo que se 'amplia'.
Es fácil ver que entonces que $\{(00010) + \mathcal{C}, (00001) + \mathcal{C}\}$ es una base de $\mathbb{F}_2^5/\mathcal{C}$.
De esta definición, las distintas clases de $\mathbb{F}_2^5/\mathcal{C}$ son:

1. $(00000) + \mathcal{C}$

2. $(00010) + \mathcal{C}$

3. $(00001) + \mathcal{C}$

4. $(00011) + \mathcal{C}$

En el caso 1, dado que el (00000) está en el código, es fácil ver que el vector de error es $e = (00000)$.
Por otro lado, al sumar a 2 ella misma, tenemos (00000), por tanto, $e = (00010)$.
Para 3 es análogo, $e = (00001)$.
Finalmente, para el último tenemos $e = (10000)$.

Calculamos ahora los síndromes para cada clase; empezamos calculando una matriz de control de pariedad H del código $\mathcal{C}$, transponiendo G, tenemos:

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

Ahora, para cada clase calculamos xH^t.

1. $(0, 0) \longleftrightarrow e = (00000)$

2. $(1, 0) \longleftrightarrow e = (00010)$

3. $(0, 1) \longleftrightarrow e = (00001)$

4. $(1,1) \longleftrightarrow e = (10000)$

Se puede ver que las últimas componentes de los vectores x coinciden con el valor del síndrome, ***esto no es una casualidad.***

Ahora tomamos cualquier palabra $x = (01101)$ calculamos su síndrome:

$$xH^t = (1,0) \longleftrightarrow e = (00010)$$

Entonces,

$$c = x - e = (01101) - (00010) = (01111)$$

2.2.1. Códigos de Hamming

Supongamos que estamos $\mathbb{F}_q^r$, y queremos un conjunto maximales de vectores de $\mathbb{F}_q^r$, con la condición de que cualesquiera dos vectores del conjunto sean linealmente independientes.
En $\mathbb{F}_q^r - \{0\}$, consideramos la relación de equivalencia:

$$(b_1,...,b_r) \equiv (a_1,...,a_r) \Longleftrightarrow (b_1,...,b_r) = \lambda(a_1,...,a_r), \lambda \in \mathbb{F}_q$$

Cada clase de equivalencia tiene $q-1$ elemento $= (\#(\mathbb{F}_q - \{0\}))$.
Ahora, $\#\{\mathbb{F}_q^r - \{0\}\} = q^r - 1$.
Luego

$$\#\mathbb{F}_q^r - \{0\}/\sim = \frac{q^r-1}{q-1}$$

Al espacio $\mathbb{K}^r - \{0\}/\sim$ se le llama **espacio proyectivo**.

Definición 14 (Código de Hamming)**.** *Consideremos $r \in \mathbb{N}$, $n = \dfrac{q^r-1}{q-1}$. Consideremos una matriz H $r \times n$ cuyas columnas son los representantes de cada una de las clases de equivalencia de $\mathbb{F}_q^r - \{0\}/\sim$.*
Denotamos por $\mathcal{H}(q,r)$ el código cuya matriz de pariedad es H.
A este código se le denomina ***Código de Hamming asociado a*** *r, n*

Ejemplo 10. *$\mathbb{F}_3^2$, $r = 2, q = 3$, entonces $n = \dfrac{3^2-1}{3-1} = 4$.*
Además,

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

La matriz de paridad de $\mathcal{H}(3,2)$, entonces

$$\mathcal{H}(3,2) = \{(x_1,x_2,x_3,x_4) \in \mathbb{F}_3^4 : (x_1,x_2,x_3,x_4) \cdot H^t = 0\} =$$

$$= \{(x_1,x_2,x_3,x_4) \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 2 \end{pmatrix} = (0,0)\} =$$

$$= \{x_1 + x_3 + x_4 = 0, x_2 + x_3 - x_4 = 0\} =$$

$$= \{(-\lambda\mu, -\lambda + \mu, \lambda, \mu) : \lambda, \mu \in \mathbb{F}_3\}$$

Observación 7 (Parámetros del código $\mathcal{H}(q,r)$)**.** *De la definición del código de Hamming, se tiene:*

- *Longitud:* $n = \dfrac{q^r - 1}{q-1}$
- *Dimensión:* $n - r$ *pues rango*$(H) = r$*, dado que* $(a_1, 0, ..., 0), (0, a_2, ..., 0), (0, 0, ..., a_r)$ *con* $a_i \neq 0$.
- *Distancia mínima: 3.*

Proposición 2. $d(\mathcal{H}(q,r)) = 3$

Demostración. Vemos que $\mathcal{H}(q,r)$ no tiene vectores de peso 1 ni 2:
Peso 1: $(0, ..., 0, a_i, 0, ..., 0) \in \mathcal{H}(q,r)$.
Si consideramos el siguiente producto:

$$(0, ..., 0, a_i, 0, ..., 0) \cdot \begin{pmatrix} a_{11} & ... & a_{1r} \\ a_{21} & ... & a_{2r} \\ ... & ... & ... \\ ... & ... & ... \\ a_{r1} & ... & a_{nr} \end{pmatrix} = (0, ..., 0)$$

Además, $a_i \neq 0$, entonces la fila i de H^t es nula. $\longrightarrow\!\longleftarrow$
Peso 2: Análogo. $\square$

Observación 8 (Vector de peso 3 en $\mathcal{H}(q,r)$)**.** *Consideremos las filas* $1, 2$ *de* H^t.
Ahora sean $a = (a_1, ..., a_r), b = (b_1, ..., b_r)$*, dado que* a, b *son linealmente independientes se concluye que* $a + b$ *es linealmente independiente de* a *y* b*. Es decir, alguna fila de la matriz de* H^t *es proporcional a* $a + b$*, de aquí,*

$$(a_1 + b_1, ..., a_r + b_r) = \lambda(c_1, ..., c_r)$$

.
Consideremos $(1, 1, 0, ..., -\lambda, 0, ..., 0) \in \mathcal{H}(q,r)$*, como tiene* 3 *componentes distintas de cero, tenemos que claramente es de peso* 3.

Definición 15 (Código perfecto)**.** *Sea* $\mathcal{H}(q,r)$ *en un* $[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r, 3]-$*código lineal. Un código con estos parámetros se dice que es un* ***código perfecto.***

Consideremos $\mathbb{F}_q^n$, ¿$\#B(x,e)$? $e \leq n$.

1. Hay $n(q-1)$ palabras a distancia 1.
2. Hay $C(n,2)(q-1)^2$ palabras a distancia 2.
3. En general, $C(n,r)(q-1)^r$

De este modo,

$$\#B(x,e) = \sum_{r=0}^{e} C(n,r)(q-1)^r$$

Proposición 3. $\mathcal{H}(q,r)$ *es perfecto.*

Demostración. $d = 3 = 2 \cdot 1 + 1, e = 1$, de este modo:

$$\sum_{c \in \mathcal{H}(q,r)} \#B(c,1) = \#\mathcal{H}(q,r)(1+n(q-1)) = q^{n-r}(1+n(q-1)) = q^{n-r}(1+\frac{q^r-1}{q-1}) = q^{n-r}(q^r) = q^n$$

□

Al ser perfecto, sólo existe una palabra en el código con distancia mínima.

Ejemplo 11. *$\mathcal{C} \subset \mathbb{F}_2^7$ que cumpla que $\#\mathcal{C} = 8$, y $d(\mathcal{C}) = 4$.*
Para ello empezamos de:

$$(0000000)$$
$$(1111000)$$
$$(1011111)$$
$$(0110000)$$

¿?

Ejemplo 12. *Sea $\mathcal{C} \subset \mathbb{F}_2^n$ código perfecto con $d(\mathcal{C}) = 7$. Entonces $n \in \{7, 23\}$*

2.3. Algunos códigos buenos

2.3.1. Códigos de Golay. Ternarios y binario

Veremos que los parámetros de los códigos de Golay son los siguientes:

1. **Ternario**: $[11, 6, 5] - código$
2. **Binario**: $[23, 12, 7] - código$

Definición 16 (Producto espacio vectorial). *Supongamos que $x, y \in \mathbb{F}_q^n$. Definimos el producto de $x = (x_1, ..., x_n), y = (y_1, ..., y_n)$ como*

$$< x, y >= \sum_{i=1}^{n} x_i y_i$$

Definición 17 (Código dual). *$\mathcal{C} \subset \mathbb{F}_q^n$ código lineal. El **código dual** de $\mathcal{C}$ es:*

$$\mathcal{C}^\perp = \{x \in \mathbb{F}_q^n :< x, c >= 0, \forall c \in \mathcal{C}\}$$

Ejemplo 13. *En $\mathbb{F}_2^6$ consideremos $\mathcal{C}$ con matriz generadora:*

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

$$\mathcal{C}^\perp = \{x = (x_1, x_2, x_3, x_4, x_5, x_6) : x \cdot c_1 = 0, x \cdot c_2 = 0, x \cdot c_3\} = \{x_1 + x_4 + x_5 = 0, x_2 + x_4 + x_6 = 0, x_3 + x_5 + x_6 = 0\},$$

donde c_i son los elementos de la base, y $\cdot$ denota el producto espacio vectorial.

Observación 9. *Una matriz generadora del código $\mathcal{C}$ es una matriz de control de paridad $\mathcal{C}^\perp$.*
Por tanto, $\dim \mathcal{C}^\perp{}_{\mathbb{F}_q} = n - \dim \mathcal{C}_{\mathbb{F}_q}$

Definición 18 (Código autodual). *Un código lineal $\mathcal{C} \subset \mathbb{F}_q^n$ es autodual si $\mathcal{C}^\perp = \mathcal{C}$*

Definición 19 (Código extendido). *$\mathcal{C} \subset \mathbb{F}_q^n$ lineal. El código extendido $\mathcal{C} \subset \mathbb{F}_q^{n+1}$ es el código:*

$$\hat{\mathcal{G}} = \{(x_1, x_2, ..., x_n, x_{n+1}) : (x_1, ..., x_n) \in \mathcal{C}, x_1 + x_2 + ... + x_n + x_{n+1} = 0\}$$

Definición 20 (Código de Golay Ternario). *Empezamos de $\mathbb{F}_3^{11}$, $k = 6, d = 5$.*
Sea $\mathcal{G}_3$ una matriz generadora.

$$\mathcal{G}_3 = \left(\begin{array}{cccccc|ccccc} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ \hline 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & -1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & -1 & 1 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & -1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & -1 & -1 & 1 & 0 \end{array}\right)$$

El código extendido $\hat{\mathcal{G}}_3$ tiene matriz generadora:

$$\hat{\mathcal{G}}_3 = \left(\begin{array}{cccccc|ccccc|c} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ \hline 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & -1 & 1 & -1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & -1 & 1 & -1 \\ 0 & 0 & 0 & 1 & 0 & 0 & -1 & 1 & 0 & 1 & -1 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & -1 & 1 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & -1 & -1 & 1 & 0 & -1 \end{array}\right)$$

$\hat{\mathcal{G}}_3$ es autodual, para cualquiera c, c' elementos de la matriz se tiene que $< c, c' >= 0$.
Por linealidad, para cualquier elemento del código también cumple esto. Se concluye entonces que toda palabra de $\hat{\mathcal{G}}_3$ tiene peso múltiplo de 3.
En efecto, si $x = (x_1, ..., x_{12})$, entonces:

$$0 =< x, x >= x_1^2 + ... + x_12^2$$

. Veamos que obviamente $d(\hat{\mathcal{G}}_3) = 6$. Veamos que $\hat{\mathcal{G}} \neq 0$ tiene peso ≥ 6.
Combinaciones de 1 vector de la base.
Combinaciones de 2 vectores

$$\hat{\mathcal{G}} = \{(x_1, x_2, ..., x_n, x_{n+1}) : (x_1, ..., x_n) \in \mathcal{C}, x_1 + x_2 + ... + x_n + x_{n+1} = 0\}$$

De aquí el peso debe cumplir $4 \leq peso \leq 8$, por tanto, necesariamente $peso = 6$.
Combinaciones de tres vectores: $peso \geq 4$ entonces $peso \geq 6$.
Combinaciones de cuatro, cinco, seis vectores: $peso \geq 4, peso \geq 6$.
Luego, $d(\hat{\mathcal{G}}_3) \geq 6$. Como los vectores de la matriz ampliada tiene peso 6, concluimos que $d(\hat{\mathcal{G}}_3) = 6$
Conclusión: $d(\mathcal{G}_3) \geq 5$, pero en la matriz $\mathcal{G}$ hay vectores de peso 5, por tanto, $d(\mathcal{G}_3) = 5$

Proposición 4. *$\mathcal{G}_3$ es perfecto.*

Demostración. $(\#\mathcal{G}_3) \cdot (\#B(x, 2)) = 3^6(1 + C(11, 1)(q - 1) + C(11, 2)(q - 1)^2 = 3^6(1 + 22 + 220) = 3^6(243) = 3^6 3^5$ ☐

Definición 21 (Código de Golay binario). *Sea $n = 23, k = 12, d = 7$, y $\mathcal{G}_2 \subset \mathbb{F}_2^{23}$.*
Consideramos el código de Hamming con matriz de control de paridad:

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

Una matriz generador de $\mathcal{G}_2$ de $\mathcal{H}$:

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

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

Consideramos $\hat{\mathcal{H}}, \hat{\mathcal{H}}^*$

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

$$\hat{\mathcal{G}^*} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

Observación 10. *Usando la misma notación que antes:*

- $\hat{\mathcal{H}} \cap \hat{\mathcal{H}}^* = \{0, 1\}$
- $\hat{\mathcal{H}}, \hat{\mathcal{H}}^*$ *son autoduales.*
- *Las palabras de $\hat{\mathcal{H}}$ y $\hat{\mathcal{H}}^*$ tienen peso múltiplo de 4.*
- $d(\hat{\mathcal{H}}) = d(\hat{\mathcal{H}}^*) = 4$

Consideramos el código $\hat{\mathcal{C}} \subset \mathbb{F}_2^{24}$:

$$\hat{\mathcal{C}} = \{(a + x, b + x, a + b + x) : a, b \in \hat{\mathcal{H}}, x \in \hat{\mathcal{H}}^*\}$$

Proposición 5. *Sean $\{a_1, a_2, a_3, a_4\}, \{b_1, b_2, b_3, b_4\}$ base de $\hat{\mathcal{H}}$ y $\{x_1, x_2, x_3, x_4\}$ base $\hat{\mathcal{H}}^*$ entonces:*

$$\{(a_i, 0, a_i)\}_{i=1,2,3,4} \cup \{(0, b_i, b_i)\}_{i=1,2,3,4} \cup \{(x_i, x_i, x_i)\}_{i=1,2,3,4}$$

son base de $\hat{\mathcal{C}}$

Observación 11. *Sea $D \subset \mathbb{F}_2^{23}$ entonces*

$$\mathcal{G}_2 = D = \{(c_1, ..., c_{23}) \in \mathbb{F}_2^{23} : (c_1, .., c_{23}, c_{24}) \in \hat{\mathcal{C}}\}$$

$\mathcal{G}_2$ tiene dimensión 12 también.

Observación 12. *El código $\hat{\mathcal{C}}$ es autodual.*

Observación 13. *Como $\hat{\mathcal{C}}$ es autodual, y tiene una base cuyos elementos tienen peso múltiplo de 4, se concluye que todos las palabras de $\hat{\mathcal{C}}$ tienen peso múltiplo de 4.*

Proposición 6.

$$d(\hat{\mathcal{C}}) = 8$$

2.4. Códigos cíclicos

Capítulo 3

Criptografía

3.1. Criptosistemas simétricos

3.2. Criptosistemas de clave pública

Autoría

Estas notas se han realizado en base a los apuntes de clase del profesor **Bartolomé López Jiménez** de la Universidad de Cádiz.