TEORÍA DE CÓDIGOS Y CRIPTOGRAFÍA | **Examen 13-1-2012**

SOLUCIONES

1. Sea $C = \{21234, 42413, 13142, 34321, 00000\} \subset \mathbb{F}_5^5$.

(i) Calcular los parámetros $(n, M, d)_q$ del código C.

(ii) Decidir si C es un código lineal y en caso afirmativo dar una matriz generadora.

Solución:

(i) q es el cardinal del alfabeto en el que están escritas las palabra del código, en nuestro caso $\mathbb{F}_5$, por lo tanto $q = 5$. n es la longitud de las palabras del código, por lo tanto $n = 5$. M es el cardinal de C, así $M = |C| = 5$. Para calcular d tenemos que calcular la mínima distancia de Hamming entre todas las palabras del código, en nuestro caso $d(x, y) = 5$ para todo $x, y \in C$ distintos. Así hemos visto que C es un $(5, 5, 5)_5$-código.

(ii) Si denotamos por $u = 13142$, se observa que $21234 = 2u$, $42413 = 4u$ y $34321 = 3u$. Esto nos permite asegurar que $C = \langle u \rangle_{\mathbb{F}_5}$, por lo tanto C es un código lineal sobre $\mathbb{F}_5$ generado por u. Así una matriz generadora de C es

$$G = (13142) \in M_{1x5}(\mathbb{F}_5).$$

2. Demostrar que el código lineal generado por la matriz

$$\mathcal{G} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 2 \end{pmatrix} \in M_{2x4}(\mathbb{F}_3)$$

es un código Hamming $Ham(r, q)$ y determinar r y q.

Solución 1: La matriz $\mathcal{G}$ es equivalente a la siguiente matriz en forma estándar

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

Así construimos la matriz de paridad siguiente

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

Tenemos que las columnas de H son vectores representativos de $\mathbb{P}^1(\mathbb{F}_3)$. Por lo tanto $C_{\mathcal{G}}$ es el código de Hamming $Ham(2, 3)$.

Solución 2: Se observa que la matriz H obtenida anteriormente no tiene ninguna columna formada por ceros, ni ningún par de columnas son proporcionales. Además la segunda columna es igual a la suma de la tercera y la cuarta columna. Por lo tanto tenemos que $C_{\mathcal{G}}$ es un $[4, 2, 3]_3$-código. Además se tiene

$$3^2 \left(\begin{pmatrix} 4 \\ 0 \end{pmatrix} + \begin{pmatrix} 4 \\ 1 \end{pmatrix} (3 - 1) \right) = 3^4.$$

Esto es, $C_{\mathcal{G}}$ es un código lineal perfecto con $d = 3$. Por lo tanto es un código Hamming $Ham(r, q)$. Aquí se tiene $q = 3$ y $4 = (3^r - 1)/(3 - 1)$, de lo que se deduce $r = 2$. Así concluimos que $C_{\mathcal{G}}$ es el código de Hamming $Ham(2, 3)$.

3. Se está utilizando un código lineal sobre $\mathbb{F}_5$ que tiene la matriz generadora:

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

y el alfabeto

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

El número correspondiente a cada letra de la tabla anterior lo pasamos a base 5. Así todos los números de la tabla anterior se pueden escribir como x_0+5x_1. Esto es, como $(x_0, x_1) \in \mathbb{F}_5^2$. Ahora, cada letra del alfabeto la codificamos mediante $(x_0, x_1)\mathcal{G} = (y_0, y_1, z_0, z_1) \in \mathbb{F}_5^4$, obteniendo una pareja de letras correspondiente a la pareja de números $(y_0 + 5y_1, z_0 + 5z_1)$.

(i) Codificar la palabra CASA .

(ii) Recibimos el mensaje VPCC. Asegúrate qué nos han querido decir usando decodificación por mínima distancia.

Solución: (i) Vamos a codificar la palabra **CASA** utilizando el código generado por la matriz $\mathcal{G}$:

$$\begin{aligned} \text{C} \leftrightarrow 2 = 2 + 5 \cdot 0 \leftrightarrow (2,0) &\xrightarrow{\cdot\mathcal{G}} (2,2,0,2) \leftrightarrow (12,10) \leftrightarrow \text{MK} \\ \text{A} \leftrightarrow 0 = 0 + 5 \cdot 0 \leftrightarrow (0,0) &\xrightarrow{\cdot\mathcal{G}} (0,0,0,0) \leftrightarrow (0,0) \leftrightarrow \text{AA} \\ \text{S} \leftrightarrow 18 = 3 + 5 \cdot 3 \leftrightarrow (3,3) &\xrightarrow{\cdot\mathcal{G}} (1,3,3,4) \leftrightarrow (16,23) \leftrightarrow \text{QY} \end{aligned}$$

Por lo tanto **CASA** se codifica como **MKAAQYAA**.

(ii) Recordemos que el método de decodificación por síndromes es un algoritmo que nos permite la decodificiación por mínima distancia para códigos lineales. Además sabemos que si el código tiene distancia $d = 2t + 1$ ó $d = 2t + 2$, entonces si se ha cometido hasta t errores, entonces el código los corrige.
Calculemos en primer lugar la distancia del código generado por $\mathcal{G}$. Utilizando el método de Gauss por filas vemos que $\mathcal{G}$ es equivalente a la siguiente matriz en forma estándar

$$\begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 4 & 4 \end{pmatrix}.$$

Así construimos la matriz de paridad siguiente

$$H = \begin{pmatrix} 4 & 1 & 1 & 0 \\ 3 & 1 & 0 & 1 \end{pmatrix}.$$

Se observa que esta matriz no tiene ninguna columna formada por ceros, ni ningún par de columnas son proporcionales. Además la segunda columna es igual a la suma de la tercera y la cuarta columna. Por lo tanto vemos que $d = 3$. Esto nos asegura que el código $C_{\mathcal{G}}$ corrige cuando se han cometido sólo errores simples, ya que $d = 3 = 2 \cdot 1 + 1$.

El código utilizado asigna a cada letra del alfabeto un digrafo escrito con letras del mismo alfabeto. Así el mensaje recibido hay que dividirlo en digrafos, para posteriormente escribirlo como vectores de $\mathbb{F}_5^4$. En nuestro caso:

$$\left\{ \begin{array}{l} \texttt{V} \leftrightarrow 21 = 1 + 4 \cdot 5 \leftrightarrow (1,4) \\ \texttt{P} \leftrightarrow 15 = 0 + 3 \cdot 5 \leftrightarrow (0,3) \end{array} \right\} \Leftrightarrow \texttt{VP} \leftrightarrow (1,4,0,3)$$

$$\left\{ \begin{array}{l} \texttt{C} \leftrightarrow 2 = 2 + 0 \cdot 5 \leftrightarrow (2,0) \\ \texttt{C} \leftrightarrow 2 = 2 + 0 \cdot 5 \leftrightarrow (2,0) \end{array} \right\} \Leftrightarrow \texttt{CC} \leftrightarrow (2,0,2,0)$$

Hemos visto que $C_{\mathcal{G}}$ es 1-corrector. Si nos mandan una palabra código $c \in C_{\mathcal{G}}$ y hemos recibido $x = c + e$, donde $e \in \mathbb{F}_5^4$ es el error, si $\omega(e) \leq 1$ el código $C_{\mathcal{G}}$ corregirá correctamente. Si $\omega(e) = 0$ esto quiere decir

que $c = x \in C_{\mathcal{G}}$. Si $\omega(e) = 1$, entonces $e = \alpha \cdot e_i$ para $i \in \{1, 2, 3, 4\}$, e_i un vector de la base canónica de $\mathbb{F}_5^4$ y $\alpha \in \mathbb{F}_5$. Así tendríamos que $c = x - \alpha \cdot e_i$. ¿Cómo calcular i? Respuesta: Aplicando síndromes. Recordemos la definición del síndrome de $x \in \mathbb{F}_5^4$ con respecto a una matriz de paridad H: $s_H(x) := x \cdot H^t$. En nuestro caso tendríamos:

$$s_H(x) = s_H(c + e) = s_H(c) + s_H(e) = s_H(e) = \alpha \cdot s_H(e_i) = \alpha \cdot {H_i}^t$$

donde H_i denota la columna i-ésima de H.
Denotemos por $x_1 = (1, 4, 0, 3)$ y $x_2 = (2, 0, 2, 0)$. Vamos a decodificar utilizando el método de los síndromes:

$$s_H(x_1) = (1, 4, 0, 3)H^t = (3, 0) = 3 \cdot {H_3}^t \quad \Longrightarrow \quad c_1 = x_1 - 3 \cdot e_3 \quad \Longrightarrow \quad c_1 = (1, 4, 2, 3)\,,$$

$$s_H(x_2) = (2, 0, 2, 0)H^t = (0, 1) = 1 \cdot {H_4}^t \quad \Longrightarrow \quad c_2 = x_2 - 1 \cdot e_4 \quad \Longrightarrow \quad c_2 = (2, 0, 2, 4)\,.$$

Las palabra del código $C_{\mathcal{G}}$ son de la forma $(y_1, y_2, y_3, y_4) = (x_0 + x_1, x_0, x_1, x_0 + 2x_1)$ donde $x_0, x_1 \in \mathbb{F}_5$, entonces la letra codificada corresponde al número $y_2 + y_3 5$. En nuestro caso obtenemos:

$$\begin{array}{lllll} c_1 = (1, 4, 2, 3) & \Longrightarrow & n_1 = 4 + 2 \cdot 5 = 14 & \Longrightarrow & \texttt{O} \\ c_2 = (2, 0, 2, 4) & \Longrightarrow & n_2 = 0 + 2 \cdot 5 = 10 & \Longrightarrow & \texttt{K} \end{array}$$

Por lo tanto la palabra enviada es:

$$\texttt{OK}\,.$$

4. Calcular $A_q(4, 3)$ para $q = 2$ y $q = 3$.

Solución:

$q = 2$. Sea C un $(4, M, 3)_2$-código. Siempre podemos suponer $0000 \in C$. Como $d = 3$ en C no puede haber palabras con menos de tres 1's, sólo puede haber una palabra con tres 1's. y no puede haber una con mas de tres 1's. Por lo tanto C es equivalente al código $\{0000, 1110\}$. Así demostramos: $A_2(4, 3) = 2$.

$q = 3$. La cota de Singleton nos dice $A_3(4, 3) \leq 3^2$. Veamos que de hecho se da la igualdad. Utilizando el código del ejercicio 2 vemos que es un $(4, 3^2)_3$-código. Ahora nos falta por ver que $d = 3$. Igual que hemos visto en la solución del citado ejercicio, una matriz de paridad es

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

Se observa que esta matriz no tiene ninguna columna formada por ceros, ni ningún par de columnas son proporcionales. Además la segunda columna es igual a la suma de la tercera y la cuarta columna. Por lo tanto vemos que $d = 3$. También podríamos haber visto que $d = 3$ utilizando que el código del ejercicio 2 es un código de Hamming y por lo tanto sabemos que tiene distancia 3. Concluimos que $A_3(4, 3) = 9$.
Otra forma de ver que $A_3(4, 3) = 9$ es observando que como $d = 3$ podemos intentar buscar un código de Hamming $Ham(r, q)$ con $n = 4$ y $q = 3$. Sabemos que la longitud de las palabras de un código de Hamming ternario es $(3^r - 1)/2$. Así que tenemos que resolver la ecuación $(3^r - 1)/2 = 4$. Se obtiene $r = 2$. Por lo tanto, como $Ham(2, 3)$ es un código perfecto, tenemos que $A_3(4, 3)$ es igual al cardinal de $Ham(2, 3)$, esto es, $3^{n-r} = 9$. Observar que esto no es válido para $A_2(4, 3)$, ya que la longitud de las palabras de un código de Hamming binario es impar.

5. Determinar cuales de las siguientes afirmaciones son ciertas. O en caso contrario dar un contraejemplo.
Para todo n, d, q enteros positivos se tiene:

(i) $A_q(n,d) < A_q(n+2, 2d)$**.**

(ii) $A_q(n,d) = A_q(n+2, 2d)$**.**

(iii) $A_q(n,d) > A_q(n+2, 2d)$**.**

Solución 1: Veamos que las tres afirmaciones son falsas. Para ello vamos a utilizar repetidamente la cota de Singleton que nos dice $A_q(n,d) \leq q^{n-d+1}$. Recordemos que

$$A_q(n,1) = q^n \qquad \text{y} \qquad A_q(n,n) = q.$$

Las anteriores igualdades se demuestran viendo que si $\mathcal{A}$ es un alfabeto de q elementos entonces los códigos $\mathcal{A}^n$ y $Rep_q(n)$ tienen q^n y q elementos respectivamente. La cota de Singleton completa la demostración de las anteriores igualdades.
Tomemos $n = 2$ y $d = 2$, Entonces $A_q(2,2) = q = A_q(2+2, 2\cdot 2) = A_q(4,4)$. Esto demuestra que las afirmaciones (i) y (iii) son falsas.
Para ver que la afirmación (ii) es falsa en general veamos que para $n = 2$, $d = 1$ y $q = 2$ no se tiene $A_q(n,d) = A_q(n+2, 2d)$. Esto es, vamos a ver que $A_2(2,1) \neq A_2(4,2)$. Hemos visto que $A_2(2,1) = 2^2$. Ahora determinemos $A_2(4,2)$. La cota de Singleton nos asegura que $A_2(4,2) \leq 2^3$. Veamos que se da la igualdad, para ello vamos a construir un $(4,8,2)_2$-código. Sea C el código lineal generado por la matriz

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

Una matriz de paridad esta dada por $(1\,1\,1\,1)$. Como ninguna columna es 0 y todas son iguales se tiene que la distancia del código es 2. Así hemos demostrado $A_2(2,1) = 4 < 8 = A_2(4,2)$.

Solución 2: Veamos que las tres afirmaciones son falsas. Recordemos que

$$A_q(n,n) = q,$$

ya que la cota de Singleton nos asegura que $A_q(n,n) \leq q$ y el código $Rep_q(n)$ tienen q elementos.
Igual que antes para ver que las afirmaciones (i) y (iii) son falsas usamos $n = d = 2$. Obteniendo $A_q(2,2) = q = A_q(2+2, 2\cdot 2) = A_q(4,4)$. Para demostrar que (ii) es falso utilizamos $d = n > 2$. Así tenemos $A_q(n,n) = n$, mientras que $A_q(2+n, 2\cdot n) = 0$, ya que $2n > 2 + n$ si $n > 2$.