Códigos y Criptografía
Grado en Ingeniería Informática

Examen escrito 1 (10% nota final)
2021

Fecha: 26 de octubre de 2021
Hora: 12:05–12:55
Lugar: Aula 101

Ayuda permitida: cualquier tipo de material impreso: notas, apuntes, libros, ejercicios resueltos, ...
No se permite ninguna ayuda de forma electrónica, salvo una sencilla calculadora y un ordenador portátil o tablet con un lector de ficheros pdf abierto donde se puede consultar un libro electrónico o las pizarras de clase. En particular no debe tenerse abierto un explorador, SageMath o cualquier programa de email/mensajería. El wifi y datos deben estar desactivados.
Preferentemente, se usará una calculadora de bolsillo. En el caso de no tener una calculadora de bolsillo, se podrá usar la calculadora de Windows/Linux.
Cualquier otro tipo de ayuda electrónica no se puede utilizar. Esto incluye calculadoras científicas avanzadas, teléfono móvil, tablets/pdas, smartwatchs, reproductores de música, . . .

Nota: la resolución de los ejercicios debe **justificarse** de forma **razonada**.

Nota: escribe tu nombre y apellidos y DNI/NIE en todas las hojas que entregues.

Nota: El porcentaje al principio de cada ejercicio indica su valor en el examen. El último ejercicio es un ejercicio "bonus" que permite obtener un 25% adicional.

Ejercicios: pueden encontrarse en las próximas 2 páginas.

Ejercicio 1. *(45%)* Sea $C \subset \mathbb{F}_3^4$ el código lineal dado por la matriz de generadora

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

(a) ¿Cuál es la longitud y la dimensión de C?

(b) Codifica el mensaje $(1,1) \in \mathbb{F}_3^2$ usando el código C.

(c) Calcula una matriz de control del código C.

(d) Razona si las siguientes palabras de $\mathbb{F}_3^4$ pertenecen al código o no

- $(2,2,1,0)$.
- $(2,2,2,0)$.

(e) ¿Cuál es la distancia mínima de C? ¿Es C un código MDS (i.e. sus parámetros verfican con igualdad la cota de Singleton)?

Ejercicio 2. *(35%)* Sea C el código lineal binario dado por la matriz de control

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

y que tiene la siguiente tabla de síndromes y líderes:

Síndrome	Líder
(0,0,0)	(0,0,0,0,0,0)
(1,1,1)	(1,0,0,0,0,0)
(1,0,1)	(0,1,0,0,0,0)
(1,1,0)	(0,0,1,0,0,0)
(1,0,0)	(0,0,0,1,0,0)
(0,1,0)	(0,0,0,0,1,0)
(0,0,1)	(0,0,0,0,0,1)
(0,1,1)	-

(a) A partir de la tabla de síndromes y líderes, deduce la capacidad correctora del código C.

(b) Usando la tabla de síndromes y líderes, decodifica las siguientes palabras recibidas de $\mathbb{F}_2^6$ y menciona cuantos errores se han cometido.

- $(1,0,1,0,1,0)$
- $(1,0,1,0,1,1)$
- $(1,0,1,0,0,1)$

Ejercicio 3. *(20%)* Sea C un código lineal binario de longitud 10 y dimensión 3.

(a) Proporciona una cota superior para la distancia mínima de C de acuerdo a la cota de Plotkin.

(b) ¿Puede existir un código binario de longitud 10 y dimensión 3 que sea MDS? Es decir, que cuyos parámetros verifiquen con igualdad la cota de Singleton.

Ejercicio 4. *(extra 25%)*

(a) Encuentra un elemento primitivo de $\mathbb{F}_{11}$.

(b) Considera $\mathbb{F}_8$ dado por $\mathbb{F}_2[X]/(X^3 + X + 1)$. Y sea $\alpha = X$ un elemento primitivo de $\mathbb{F}_8$.

- Calcula $\alpha^5 + \alpha^6$. Expresa la respuesta por un polinomio (o vector) y por una potencia de α.
- Calcula $(X + X^2)(1 + X^2)$. Expresa la respuesta por un polinomio (o vector) y por una potencia de α.

Ejercicio 1. *(45%)* Sea $C \subset \mathbb{F}_3^4$ el código lineal dado por la matriz de generadora

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

(a) ¿Cuál es la longitud y la dimensión de C?

(b) Codifica el mensaje $(1,1) \in \mathbb{F}_3^2$ usando el código C.

(c) Calcula una matriz de control del código C.

(d) Razona si las siguientes palabras de $\mathbb{F}_3^4$ pertenecen al código o no

- $(2,2,1,0)$.
- $(2,2,2,0)$.

(e) ¿Cuál es la distancia mínima de C? ¿Es C un código MDS (i.e. sus parámetros verfican con igualdad la cota de Singleton)?

a) $\left(\begin{array}{cc|cc} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 2 \end{array}\right)$ $k = 2$, $n = 4$

b) $\mathbb{F}_3$

+	0	1	2
0	0	1	2
1	1	1	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$$(1,1)\cdot\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 2 \end{pmatrix} = (1, 1, 1, 1+2) = (1,1,1,0)$$

c) $[H] = [-A^t, I_{n-k}]$

$A = -P$ $\quad 3 \cdot 2 = 1$

$P = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$ $\quad 0\,1\,2\,(0,1,2)$
$-0 \cdot 2 \cdot 1$

$-P = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix} \Rightarrow -P^t = \begin{pmatrix} 2 & 0 \\ 2 & 1 \end{pmatrix}$

$H = \left(\begin{array}{cc|cc} 2 & 0 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{array}\right)$ //

e) $\mathcal{L}_1$ es li?

$d_1 > 1$ todo $\neq 0$

¿2 son li?

Si $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ y $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ son iguales $A = 2$

d) Mirar síndromes, si es 0, pertenece

$\vec{v} = (2,2,1,0)$ $\quad S(\vec{v}) = H \cdot \vec{v}^t$

$$S(\vec{v}) = \begin{pmatrix} 2 & 0 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 2 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \end{pmatrix} \Rightarrow \text{No pertenece}$$

$\vec{v} = (2,2,2,0)$

$$S(\vec{v}) = \begin{pmatrix} 2 & 0 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 2 \\ 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \Rightarrow \text{Sí}$$

Ejercicio 2. *(35%)* Sea C el código lineal binario dado por la matriz de control

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

y que tiene la siguiente tabla de síndromes y líderes:

Síndrome	Líder
(0,0,0)	(0,0,0,0,0,0)
(1,1,1)	(1,0,0,0,0,0)
(1,0,1)	(0,1,0,0,0,0)
(1,1,0)	(0,0,1,0,0,0)
(1,0,0)	(0,0,0,1,0,0)
(0,1,0)	(0,0,0,0,1,0)
(0,0,1)	(0,0,0,0,0,1)
(0,1,1)	-

(a) A partir de la tabla de síndromes y líderes, deduce la capacidad correctora del código C.

(b) Usando la tabla de síndromes y líderes, decodifica las siguientes palabras recibidas de $\mathbb{F}_2^6$ y menciona cuantos errores se han cometido.

- $(1,0,1,0,1,0)$
- $(1,0,1,0,1,1)$
- $(1,0,1,0,0,1)$

a) Como el síndrome es la columna correspondiente a la posición del error y cada líder a lo sumo presenta un único error, por lo tanto, se deduce que es 1.

b) $S(\vec{r_1}) = H \cdot \vec{r}_1^{\,t} = \begin{pmatrix}1&1&1&1&0&0\\1&0&1&0&1&0\\1&1&0&0&0&1\end{pmatrix}\begin{pmatrix}1\\0\\1\\0\\1\\0\end{pmatrix} = \begin{pmatrix}0\\1\\1\end{pmatrix}$

como el sindrome tiene lider, no decodificamos = error

$S(\vec{r}_2) = H \cdot \vec{r}_2^{\,t} = \begin{pmatrix}1&1&1&1&0&0\\1&0&1&0&1&0\\1&1&0&0&0&1\end{pmatrix}\begin{pmatrix}1\\0\\1\\0\\1\\1\end{pmatrix} = \begin{pmatrix}0\\1\\0\end{pmatrix}$

Lider = (0,0,0,0,1,0)

(1,0,1,0,1,1) − (0,0,0,0,1,0) = (1,0,1,0,0,1)

Hay un error

$S(\vec{r}_3) = H \cdot \vec{r}_3^{\,t} = \begin{pmatrix}1&1&1&1&0&0\\1&0&1&0&1&0\\1&1&0&0&0&1\end{pmatrix}\begin{pmatrix}1\\0\\1\\0\\0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\end{pmatrix}$

Lider: (0,0,0,0,0,0) No hay error ✓

Ejercicio 3. *(20%)* Sea C un código lineal binario de longitud 10 y dimensión 3.

(a) Proporciona una cota superior para la distancia mínima de C de acuerdo a la cota de Plotkin.

(b) ¿Puede existir un código binario de longitud 10 y dimensión 3 que sea MDS? Es decir, que cuyos parámetros verifiquen con igualdad la cota de Singleton.

a) $d \leq \frac{10 \cdot 2^2 \cdot (2-1)}{2^3 - 1} = \frac{40}{7} \approx 5,7$

b) $10 + 1 \geq 3 + 5,7$ ✓

cumple la regla, pero no la igualdad

por lo que no es mds

Ejercicio 4. *(extra 25%)*

(a) Encuentra un elemento primitivo de $\mathbb{F}_{11}$.

(b) Considera $\mathbb{F}_8$ dado por $\mathbb{F}_2[X]/(X^3 + X + 1)$. Y sea $\alpha = X$ un elemento primitivo de $\mathbb{F}_8$.

- Calcula $\alpha^5 + \alpha^6$. Expresa la respuesta por un polinomio (o vector) y por una potencia de α.
- Calcula $(X + X^2)(1 + X^2)$. Expresa la respuesta por un polinomio (o vector) y por una potencia de α.

$\alpha^0, \ldots, \alpha^{7-2}$

a) $\mathbb{F}_{11} - \{0\} \subset \mathbb{F}_{11}^* =$

$\alpha^{q-1} = 1$

$2^0 = 1$
$2^1 = 2$
$2^2 = 4$
$2^3 = 8$
$2^4 = 5$
$2^5 = 10$
$2^6 = 9$
$2^7 = 7$
$2^8 = 3$
$2^9 = 6$

$3^0 = 1$
$3^1 = 3$
$3^2 = 9$
$3^3 = 27 \cdot 11 = 16 \cdot 11 = 5$
$3^4 = 81 = 4$
$3^5 = 1$

$4^0 = 1$
$4^1 = 5$
$4^3 = 9$
$4^4 = 3$
$4^5 = 1$

$5^0 = 1$
$5^1 = 5$
$5^2 = 3$
$5^3 = 4$
$5^4 = 9$
$5^5 = 12$
$5^6 = 5$
$5^7 =$
$5^8 =$
$5^9 =$
$5^{10} =$

en $\mathbb{F}_{11} - \{0\} = \mathbb{F}_{11}^* = \langle 2 \rangle$

b) $\mathbb{F}_8 = \{a_0^2 + a_1^2 x + a_1^2 x^2 \mid a_i \in \mathbb{F}_2\}$

$\alpha = [x]$

$\alpha^5 + \alpha^6 = x^6 + x^5 \mid x^3 + x + 1$

$x^3 = x + 1$

$x^6 = x^3 \cdot x^3 = (x+1)(x+1) = x^2 + x + x + 1 =$

$x^2 + 2x + 1 = x^2 + 1$

$x^5 = x^3 \cdot x^2 = x^2 \cdot (x+1) = (x^3 + x^2) =$

$= x^2 + x + 1$

$x^6 + x^5 = x^2 + 1 + x^2 + x + 1 = x$ //

$(0, 1, 0)$

$(X + X^2)(1 + X^2)$.

b2) $(x+x^2)(1+x^2) = x + x^3 + x^2 + x^4 =$

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

$= (1,1,0) = \alpha^3$

$\alpha = x \quad \alpha^2 = x^2 \quad \alpha^3 = x^3 = x + 1$