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.