Códigos y Criptografía
Grado en Ingeniería Informática

Examen escrito 1 (10% nota final)
2022

Fecha: 18 de octubre de 2022
Hora: 11:05–11:55
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 segundo ejercicio es un ejercicio "bonus" que permite obtener un 20% adicional.

Ejercicios: pueden encontrarse en las próximas 2 páginas.

Ejercicio 1. *(45%)* Sea $C \subset \mathbb{F}_5^4$ el código lineal generado por los vectores $(1,1,1,1)$ y $(1,2,3,4)$.

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

(b) Escribe una matriz generadora del código C.

(c) Codifica el mensaje $(2,3) \in \mathbb{F}_5^2$ usando el código C.

(d) Comprueba que

$$H = \begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 3 & 1 \end{pmatrix}$$

es una matriz de control de C

(e) Razona si las siguientes palabras de $\mathbb{F}_5^4$ pertenecen al código o no

- $(2,3,4,1)$.
- $(2,3,4,0)$.

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

(g) ¿Cuántos errores puede corregir C? ¿Cuántos errores puede detectar C? ¿Cuántos borrones puede corregir C?

Ejercicio 2. *(extra 20%)* Considera el código C del ejercicio 1.

(a) Calcula razonadamente una matriz generadora sistemática de C

(b) Calcula razonadamente una matriz de control de C.

Ejercicio 3. *(35%)* Sea C el código lineal binario dado por la matriz de control

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

y que tiene la siguiente tabla de síndromes y líderes:

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

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

(b) Comprueba que el vector $(1,1,1,0,0,0)$ pertenece a C.

(c) Considera que el vector $(1,1,1,0,0,0)$ es enviado a través de un canal con ruido y se producen unos ciertos errores y se recibe el vector $\mathbf{r}$. Haz de receptor y decodifica la palabra recibida $\mathbf{r}$, menciona cuantos errores se produjeron y si la decodificación es correcta para los siguientes valores de $\mathbf{r}$:

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

Ejercicio 4. *(20%)*

(a) Proporciona una matriz generadora de un código sobre $\mathbb{F}_8$ de longitud 7 y dimensión 3 que sea MDS (se tiene igualdad en la cota de Singleton).

(b) Comprueba que el código de Hamming binario con parámetros $[7,4,3]_2$ es un código perfecto (se verifica la igualdad para la cota de Hamming).