# Códigos y Criptografía
# Grado en Ingeniería Informática

## Examen escrito 1 (10% nota final)
## 2020

**Fecha:** 04 noviembre 2020
**Hora:** 10:05–10:55
**Lugar:** Aula I+D

**Ayuda permitida:** Cualquier tipo de material impreso: notas, apuntes, libros, ejercicios resueltos, ... No se permite ninguna ayuda de forma electrónica, salvo un ordenador portátil 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.
Cualquier otro tipo de ayuda electrónica no se puede utilizar. Esto incluye calculadoras, teléfono móvil, tablets/pda, smartwatches, reproductores de música, ...

**Nota:** Todas las respuestas deben justificarse de forma razonada.

**Nota:** Escribe tu nombre y apellidos 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.** *(40%)* Sea $C \subset \mathbb{F}_2^7$ el código lineal dado por la matriz generadora

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

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

(b) Codifica el mensaje $(1,0,1,0) \in \mathbb{F}_2^4$ usando el código $C$.

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

(d) ¿Cuál es la distancia mínima de $C$?

**Ejercicio 2.** *(40%)* 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.

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

**Ejercicio 3.** *(20%)* Sea $C$ el código Reed-Solomon $[10, 3, 8]$ sobre $\mathbb{F}_{11}$.

(a) Calcula cuál es el mayor tamaño de lista que se podría usar para decodificar en lista el código $C$ si se quiere mejorar la capacidad correctora única de $C$.

(b) ¿Cuántos errores se pueden corregir si el tamaño de lista es $\ell = 2$?

**Ejercicio 4.** *(extra 25%)*

(a) Encuentra un elemento primitivo de $\mathbb{F}_7$.

(b) Considera $\mathbb{F}_{16}$ dado por $\mathbb{F}_2[X]/(X^4 + X + 1)$. Y sea $\alpha = x$ un elemento primitivo de $\mathbb{F}_{16}$.

- Calcula $\alpha^{13} + \alpha^{14}$. Expresa la respuesta por un polinomio (o vector) y por una potencia de $\alpha$.
- Calcula $(X + X^2)(X^2 + X^3)$. Expresa la respuesta por un polinomio (o vector) y por una potencia de $\alpha$.