# Introducción a la Teoría de Códigos

M.A. García, L. Martínez, T. Ramírez

Facultad de Ciencia y Tecnología. UPV/EHU

## Resumen Teórico
## Apartado 5 del Tema 3:
## Ejemplo de códigos lineales:
## Códigos de Hamming

Mayo de 2017

# 5 Ejemplo de códigos lineales: Códigos de Hamming

En $\mathbb{F}_q^r$ consideramos los subespacios vectoriales de dimensión 1. Por Álgebra Lineal sabemos que hay $\frac{q^r-1}{q-1}$ subespacios. De cada uno de estos subespacios tomamos un vector no nulo (una base) y construimos la matriz $H$ de orden $r \times \frac{q^r-1}{q-1}$ cuyas columnas son precisamente los vectores no nulos seleccionados. Entonces, esta matriz $H$ tiene las siguientes propiedades:

1. Es de rango $r$.
2. Dos columnas cualesquiera distintas son siempre linealmente independientes y si tomamos dos columnas de $H$ , $H^{(i)}$ y $H^{(j)}$, entonces existe en $H$ una columna $H^{(k)} = H^{(i)} + H^{(j)}$, esto es, $H^{(i)}$, $H^{(j)}$ y $H^{(k)}$ son linealmente dependientes.

Esta matriz $H$ nos sirve como matriz de control de un código lineal de longitud $\frac{q^r-1}{q-1}$, que tiene dimensión $\frac{q^r-1}{q-1} - r$ y, por la construcción de $H$, distancia mínima 3, llamado $(\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r)$**-código de Hamming**. En algunos textos, se les denomina también códigos de Hamming de parámetros $r$ y $q$, donde $q$ es el cardinal del cuerpo y $r$ el número de filas de $H$. Si $q = 2$, observamos que los códigos de Hamming tienen longitud $2^r - 1$ y dimensión $2^r - 1 - r$.

En la definición dada no se ha especificado el orden de las columnas de $H$. Ello no es obstáculo ya que al cambiar el orden de las columnas de $H$, lo que se obtiene es otro código de Hamming equivalente al dado.

Esta familia de códigos lineales es una de las más estudiadas y conocidas. Además de poder conocer de antemano su distancia mínima, los códigos de Hamming tienen otra propiedad que los hace especialmente interesantes: son códigos perfectos, puesto que alcanzan la cota de Hamming.

**Ejemplo** Si queremos construir un código de Hamming ternario con $r = 2$, éste será de longitud $\frac{3^2-1}{3-1} = 4$ y dimensión $\frac{3^2-1}{3-1} - 2 = 4 - 2 = 2$. Además, su matriz de control vendrá dada por

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

Es fácil ver que una matriz generadora de este código lineal vendrá dada por

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

por lo que $C =< 2210, 1201 >$ .