OCW
OpenCourseWare

eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea

# Introducción a la Teoría de Códigos

M.A. García, L. Martínez, T. Ramírez

Facultad de Ciencia y Tecnología. UPV/EHU

## Resumen Teórico
## Apartado 4 del Tema 2:
## Códigos perfectos

Mayo de 2017

# 4 Códigos perfectos

Un código $C \subseteq T_n$ con distancia mínima $d$ que alcance la Cota de Hamming se dice que es un **código perfecto**. Esto es, si $C \subseteq T_n$ es un código de bloque sobre el alfabeto $A = \{a_1, \ldots, a_m\}$ de distancia mínima $d$, entonces se dice que $C$ es perfecto, si cumple $|C| \sum_{i=0}^{\left[\frac{d-1}{2}\right]} \binom{n}{i}(m-1)^i = m^n$.

En el último ejemplo del apartado anterior, hemos comentado que el código binario

$$\begin{aligned} C \ = \{&0000000, 0110100, 0011010, 0001101, \\ &1000110, 1001011, 1011100, 0010111, \\ &1010001, 1110010, 0111001, 1111111, \\ &0101110, 1101000, 0100011, 1100101\}. \end{aligned}$$

era un código perfecto y habíamos visto que si recibiamos la palabra $\mathbf{x} = 1000111$, podíamos conocer la palabra emitida que le correspondía. En la siguiente proposición vemos que esta característica la tienen todos los códigos perfectos:

**Proposición 4.1** *Sea $C \subseteq T_n$ un código de bloque de longitud $n$ sobre un alfabeto $A$ de distancia mínima $d$. Entonces, $C$ es perfecto si y, solo si, $\dot{\bigcup}_{c \in C} \overline{B}(\mathbf{c}, \left[\frac{d-1}{2}\right]) = T_n$.*

La interpretación del resultado anterior es la misma que la del último ejemplo del apartado anterior: cada elemento de $T_n$ se encuentra en una única bola cerrada de centro $\mathbf{c}$ y radio $\left[\frac{d-1}{2}\right]$ y, como las bolas son disjuntas, esto implica que cada elemento de $T_n$ admite decodificación única, que es precisamente el centro $\mathbf{c}$ de la bola a la que pertenece el elemento de $T_n$ que hemos considerado.

En el siguiente resultado vemos que la distancia mínima de un código perfecto no puede tomar cualquier valor:

**Proposición 4.2** *Si $C \subseteq T_n$ es un código perfecto, su distancia mínima es un número impar.*

Como consecuencia de la Proposición anterior, podemos deducir la no existencia de códigos perfectos con distancia mínima un número par.

**Ejemplo** Consideramos de nuevo el código binario de longitud 7 cuyas palabras son:

$$\begin{aligned} C \ = \{&0000000, 0001101, 1111111, 1110010, \\ &1101000, 1000110, 0010111, 0111001, \\ &0110100, 0100011, 1001011, 1011100, \\ &0011010, 1010001, 1100101, 0101110\} \end{aligned}$$

Como ya hemos comentado, este código tiene distancia mínima 3. Además, sabemos que si $\mathbf{c}$ y $\mathbf{c}'$ son dos palabras distintas de $C$, se tiene que $\overline{B}(\mathbf{c}, 1) \cap \overline{B}(\mathbf{c}', 1) = \emptyset$ y

podemos calcular para cada $\mathbf{c} \in C$ el cardinal de $\overline{B}(\mathbf{c}, 1)$ que es 8. Así que $C$ es un código perfecto ya que

$$\dot{\bigcup}_{\mathbf{c}\in C} \overline{B}(\mathbf{c}, 1) = \mathbb{F}_2^7.$$

Esto implica que cada palabra de $T_n$ admite, por tanto, decodificación única.

En el Tema 3 estudiaremos una familia de códigos perfectos: los códigos de Hamming, que son códigos de bloque sobre el cuerpo finito $\mathbb{F}_q$ de distancia mínima 3 y longitud $\frac{q^r-1}{q-1}$, siendo $r$ un número natural y $q$ potencia de un primo. De hecho, el código binario del ejemplo anterior va a ser un código de tipo Hamming.