OCW
OpenCourseWare

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 2 del Tema 3:
## Matriz generadora de un código lineal

Mayo de 2017

# 2 Matriz generadora de un código lineal

Dado un $(n,k)$-código lineal $C$, sabemos que existe una base $\{\mathbf{c}_1,\ldots,\mathbf{c}_k\}$ de $C$. Estos elementos de la base nos sirven para determinar de forma única todos los elementos de $C$ como combinación lineal de ellos. Si identificamos el elemento $\mathbf{x}=x_1\ldots x_n\in\mathbb{F}_q^n$ con la matriz $(x_1\ldots x_n)\in Mat_{1\times n}(\mathbb{F}_q)$, podemos dar la siguiente definición:

**Definición** Sea $C$ un $(n,k)$-código lineal sobre $\mathbb{F}_q$. Se llama **matriz generadora** de $C$ a una matriz $G\in \mathrm{Mat}_{k\times n}(\mathbb{F}_q)$ cuyas filas forman una base de $C$.

**Ejemplo** El (7,4)-código lineal

$$C=<0110100,0011010,0001101,1000110>$$

tiene por matriz generadora a

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

La ventaja de conocer una matriz generadora $G$ de un $(n,k)$-código lineal sobre $\mathbb{F}_q$ es que a partir de ella se pueden obtener todas las palabras de $C$ de forma sencilla: basta obtener todos los elementos de $\mathbb{F}_q^k$ y calcular los productos $(y_1\ldots y_k)G$, que serán precisamente las palabras del código $C$.

Para algunos $(n,k)$-códigos lineales sobre $\mathbb{F}_q$, de entre las matrices generadoras que podemos hallar vamos a destacar unas con las que va a ser más fácil trabajar:

**Definición** Sea $C$ un $(n,k)$-código lineal con matriz generadora $G\in \mathrm{Mat}_{k\times n}(\mathbb{F}_q)$. Se dice que $G$ está dada en **forma estándar** si $G=(I_k|B)$, donde $B\in \mathrm{Mat}_{k\times n-k}(\mathbb{F}_q)$.

**Ejemplo** El (7,4)-código lineal

$$C=<0110100,0011010,0001101,1000110>$$

tiene por matriz generadora a

$$G_1=\begin{pmatrix}0&1&1&0&1&0&0\\0&0&1&1&0&1&0\\0&0&0&1&1&0&1\\1&0&0&0&1&1&0\end{pmatrix},$$

que no está dada en forma estándar.

En cambio, si realizamos permutación cíclica de las filas de $G_1$, obtenemos otra matriz generadora de $C$,

$$G_2=\begin{pmatrix}1&0&0&0&1&1&0\\0&1&1&0&1&0&0\\0&0&1&1&0&1&0\\0&0&0&1&1&0&1\end{pmatrix},$$

que tampoco está dada en forma estándar. Si a $G_2$ le aplicamos transformaciones elementales por filas, obtenemos otra generadora $G_3$, que sí está dada en forma estándar:

$$G_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

La ventaja que presentan las matrices generadoras en forma estándar frente a las que no lo están es la siguiente: si $C$ es un código lineal sobre $\mathbb{F}_q$ con matriz generadora $G$ dada en forma estándar y si la palabra $\mathbf{c}$ de $C$ tiene coordenadas $(y_1 \dots y_k)$ en la base que forman las filas de $G$, entonces $\mathbf{c} = y_1 \dots y_k c_{k+1} \dots c_n$, esto es, las coordenadas de $C$ en la base formada por las filas de $G$ son precisamente las $k$ primeras letras de $\mathbf{c}$. Es por ello que nos planteamos la siguiente cuestión:

*Dado un $(n,k)$-código lineal $C$ sobre $\mathbb{F}_q$ ¿podemos construir siempre una matriz generadora que esté en forma estándar?*

En un principio, si tenemos en cuenta que la matriz generadora $G$ es de dimensión $k$ y esto implica que $G$ es equivalente a una matriz del tipo $(I_K|B)$, podríamos pensar que es factible obtener siempre una matriz generadora en forma estándar para $C$. Pero, por desgracia, la respuesta a la cuestión planteada es NO. Por ejemplo, si tomamos el código lineal $C =< 100001, 000100 > \subseteq \mathbb{F}_2^6$ cualquier matriz generadora que busquemos no está dada en forma estándar que que las palabras de $C$ siempre llevan un 0 en la segunda posición.

Sin embargo, podemos plantearnos modificar la cuestión anterior y reformularla de la siguiente manera:

*Dado un $(n,k)$-código lineal $C$ sobre $\mathbb{F}_q$ ¿podemos construir un código lineal equivalente a $C$ que admita una matriz generadora que esté en forma estándar?*

Al tratar de contestar la cuestión anterior nos damos cuenta que lo primero que debemos hacer es fijarnos en qué operaciones podemos realizar en las palabras del código $C$ para que el código equivalente resultante siga siendo lineal y posteriormente nos centraremos en cómo construir este código equivalente para que además admita matriz generadora estándar. Así, en primer lugar vamos a determinar qué operaciones elementales se pueden realizar para obtener códigos equivalentes al dado que no pierdan la linealidad. En concreto, si se realizan solamente permutaciones en las posiciones del código y multiplicar los símbolos de una posición fija por un escalar no nulo, es obvio que no perdemos la linealidad del código inicial. Estas restricciones que hay que imponer para que se mantenga el carácter de subespacio vectorial del código equivalente resultante se traducen en que no podemos hacer todo tipo de operaciones elementales en la matriz generadora $G$ para transformarla en otra que esté dada en forma estándar y que genere un código lineal equivalente. En concreto, las operaciones elementales en $G$ que nos llevan a matrices generadoras equivalentes a $G$ y que generan un código equivalente a $C$ son:

1. Permutación de filas
2. Multiplicación de una fila por un escalar no nulo
3. Sumar a una fila una combinación lineal de las restantes filas
4. Permutación de columnas
5. Multiplicar cualquier columna por un escalar no nulo

Es decir, de las operaciones elementales que nos permiten obtener una matriz equivalente a $G$, solamente eliminamos la de sustituir una columna por ella misma más una combinación lineal de las restantes. Esto es lógico porque si pensamos en lo que significa realizar esta operación elemental en términos de las palabras del código, quiere decir que se está mezclando información de varias posiciones.

Observamos que si realizamos solamente las operaciones elementales indicadas en filas lo que estamos haciendo es cambiar una base de $C$ por otra, luego el código obtenido es el mismo. Si además realizamos alguna de las dos operaciones elementales permitidas en columnas, entonces obtenemos otro código lineal que es equivalente al dado. En cualquier caso, si tenemos en cuenta que cualquier matriz generadora de $C$ es de rango $k$, le podemos aplicar las operaciones elementales anteriores para transformar $G$ en otra matriz equivalente a ella que esté dada en forma estándar. Esta matriz es matriz generadora de un código equivalente a $C$. En definitiva, teniendo en cuenta lo anterior se prueba

**Proposición 2.1** *Sea $C$ un $(n,k)$-código lineal. Entonces, existe un $(n,k)$-código lineal $C'$ equivalente a $C$ tal que tiene una matriz generadora dada en forma estándar.*