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
Tema 4: CÓDIGOS CÍCLICOS

Mayo de 2017

Tema 4

Códigos cíclicos

1 Definición y construcción de códigos cíclicos

Sea $C \subseteq \mathbb{F}_q^n$ un (n,k)-código lineal. Se dice que C es **cíclico** si se satisface la siguiente propiedad:

$$\forall c_0 \dots c_{n-1} \in C,\ c_{n-1}c_0 \dots c_{n-2} \in C.$$

Observamos que si C es un código cíclico, entonces dada $c_0 \dots c_{n-1} \in C$, se tiene que las palabras $c_{n-1}c_0 \dots c_{n-2}$, $c_{n-2}c_{n-1}c_0 \dots c_{n-3}$, $\dots$, y $c_1 \dots c_{n-1}c_0$ están también en C.

Por otro lado, también podemos caracterizar los códigos cíclicos fijandonos solamente en lo que sucede en una base del código, tal y como se indica en el siguiente resultado:

Proposición 1.1 (Caracterización de los códigos cíclicos) *Sea $C \subseteq \mathbb{F}_q^n$ un (n,k)-código lineal con base $\mathcal{B} = \{\boldsymbol{x}_1, \dots, \boldsymbol{x}_k\}$. Entonces, C es cíclico si y, solo si, para todo $\boldsymbol{x}_i \in \mathcal{B}$, con $i = 1, \dots, k$, se tiene $x_{in-1}x_{i0} \dots x_{in-2} \in C$, siendo $\boldsymbol{x}_i = x_{i0} \dots x_{in-2}x_{in-1}$.*

Si dada una palabra $\mathbf{x} = x_0 \dots x_{n-1} \in \mathbb{F}_q^n$ llamamos a $x_{n-1}x_0 \dots x_{n-2}$ la **traslación cíclica** de $\mathbf{x}$, la proposición anterior nos indica que un código lineal es cíclico si y, solo si, la traslación cíclica de las palabras de una base están también en C. Esta caracterización nos simplificará el estudio de si un código es cíclico, cuando conozcamos una base del mismo.

Ejemplo Sea $C \subseteq \mathbb{F}_2^7$ el código lineal cuya matriz generadora viene dada por:

$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$. Entonces, una base de C es

$$\mathcal{B} = \{1101000, 0110100, 0011010, 0001101\}$$

y para las tres primeras palabras de esta base se cumple que sus traslaciones cíclicas son otra palabra de la misma base, por lo que también son palabras de C. Por tanto, solo nos queda estudiar lo que sucede con la traslación cíclica de la última palabra de la base, que es 0001101. Ahora, como estamos trabajando en $\mathbb{F}_2$, se cumple que

$$1000110 = 1101000 + 0110100 + 0011010,$$

así que la traslación cíclica de la última palabra de la base es también otra palabra de C. Por consiguiente, aplicando la Proposición 1.1, podemos afirmar que C es un código cíclico.

Además de la caracterización que hemos visto de los códigos cíclicos estudiando únicamente lo que sucede en un base, vamos a encontrar otra fijandonos en una estructura subyacente de los códigos cíclicos. Para ello, necesitamos recordar cómo se contruye el anillo cociente $\mathbb{F}_q[x]/(x^n - 1)$, donde $\mathbb{F}_q[x]$ el anillo de los polinomios en la variable x, y se puede relacionar con $\mathbb{F}_q^n$. En $\mathbb{F}_q[x]$ definimos la relación de equivalencia

$$\forall f(x), g(x) \in \mathbb{F}_q[x], \quad f(x)\mathfrak{R}g(x) \Leftrightarrow (x^n - 1)|f(x) - g(x),$$

esto es, $f(x) - g(x)$ es múltiplo de $x^n - 1$. Entonces el conjunto cociente, denotado por $\mathbb{F}_q[x]/(x^n - 1)$, está definido por

$$\mathbb{F}_q[x]/(x^n - 1) = \{\overline{f(x)} \mid f(x) \in \mathbb{F}_q[x]\}$$

y en cada clase de equivalencia $\overline{f(x)}$ podemos elegir como representante el polinomio de grado a lo sumo $n-1$ que esté en ella, que será el resto de dividir $f(x)$ por $x^n - 1$.

Por tanto,

$$\mathbb{F}_q[x]/(x^n - 1) = \{\overline{a_0 + a_1x + \cdots + a_{n-1}x^{n-1}} \,|\, a_i \in \mathbb{F}_q,\ i = 0, \ldots, n-1\}.$$

Observamos que hay tantas clases de equivalencia como polinomios de grado menor que n en $\mathbb{F}_q[x]$.

Podemos establecer un isomorfismo de espacios vectoriales entre $\mathbb{F}_q^n$ y $\mathbb{F}_q[x]/(x^n - 1)$ mediante $\psi(a_0 \ldots a_{n-1}) = \overline{a_0 + a_1x + \cdots + a_{n-1}x^{n-1}}$.

Si $C \subseteq \mathbb{F}_q^n$ es un código, denotamos por $C(x)$ a $\psi(C)$, esto es,

$$C(x) = \{\overline{a_0 + a_1x + \cdots + a_{n-1}x^{n-1}} \in \mathbb{F}_q[x]/(x^n - 1)|a_0a_1 \ldots a_{n-1} \in C\}.$$

Observamos que si C es un código cíclico, entonces dada $c_0 \dots c_{n-1} \in C$, se tiene que $c_{n-1}c_0 \dots c_{n-2}$, $c_{n-2}c_{n-1}c_0 \dots c_{n-3}, \dots, c_1 \dots c_{n-1}c_0 \in C$ y esto implica que si $\overline{\mathbf{c}(x)} = \overline{\sum_{i=0}^{n-1} c_i x^i}$, se sigue que $x\overline{\mathbf{c}(x)} = \overline{c_{n-1} + \sum_{i=0}^{n-2} c_i x^{i+1}} \in C(x)$ y en general $x^k\overline{c(x)} = \overline{\sum_{i=1}^{k} c_{n-i}x^{k-i} + \sum_{i=0}^{n-k-1} c_i x^{i+k}} \in C(x)$ para $k < n$. Utilizamos esta propiedad de los códigos cíclicos para caracterizarlos:

Proposición 1.2 (Caracterización de los códigos cíclicos) *Sea $C \subseteq \mathbb{F}_q^n$ un código lineal. Entonces, C es cíclico si y, solo si, $C(x)$ es un ideal de $\mathbb{F}_q[x]/(x^n - 1)$.*

La importancia de la proposición anterior quedará de manifiesto en el siguiente apartado, donde explotaremos esta característica de los códigos cíclicos.

2 Polinomio generador y matriz generadora de un código cíclico

Como hemos indicado, usando Teoría de Anillos, vamos a poder conocer más sobre la estructura de $C(x)$, cuando C es un código cíclico:

Proposición 2.1 *Sea $C \subseteq \mathbb{F}_q^n$ un código cíclico. Entonces, existe un único polinomio mónico $g(x)$ de grado mínimo tal que*

$$C(x) = (\overline{g(x)}) = \{\overline{t(x)g(x)} \in \mathbb{F}_q[x]/(x^n - 1) \mid t(x) \in \mathbb{F}_q[x]\}.$$

Además, $g(x)$ es un factor de $x^n - 1$ en $\mathbb{F}_q[x]$.

Cuando $C \subseteq \mathbb{F}_q^n$ es un código cíclico, al polinomio mónico $g(x)$ de grado mínimo tal que $C(x) = (\overline{g(x)})$ se le llama **polinomio generador de** C. Por tanto, es fácil determinar todos los códigos cíclicos de una longitud determinada n sobre $\mathbb{F}_q$: basta con hallar los polinomios mónicos que dividen a $x^n - 1$ y tomar cada uno de ellos como polinomio generador del código cíclico buscado.

Ejemplo Para calcular los códigos cíclicos de longitud 7 en $\mathbb{F}_2$, debemos determinar los factores irreducibles sobre $\mathbb{F}_2$ de $x^7 - 1$. Ahora,

$$x^7 - 1 = (x^3 + x + 1)(x^3 + x^2 + 1)(x + 1)$$

Entonces, hay 2^3 códigos distintos $C_i(x) = (\overline{g_i(x)})$, con $i = 1, \dots, 8$, donde

$$\begin{array}{ll} g_1(x) = 1, & g_2(x) = x + 1 \\ g_3(x) = x^3 + x + 1 & g_4(x) = x^3 + x^2 + 1 \\ g_5(x) = x^4 + x^2 + x + 1 & g_6(x) = x^4 + x^3 + x^2 + 1 \\ g_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 & g_8(x) = x^7 - 1 \end{array}$$

Observamos que $C_1(x) = \mathbb{F}_2[x]/(x^7 - 1)$ y, por tanto, $C_1 = \mathbb{F}_2^7$ y $C_8(x) = 0$, luego $C_8 = \{0000000\}$.

Este polinomio generador de un código cíclico nos sirve para determinar una matriz generadora del mismo, tal y como nos indica el siguiente resultado:

Proposición 2.2 (Matriz generadora) *Sea $C \subset \mathbb{F}_q^n$ un código cíclico con polinomio generador $g(x) = \sum_{i=0}^{n-k} g_i x^i$ de grado $n-k$. Entonces, C es un código de dimensión k y una matriz generadora es*

$$\begin{pmatrix} g_0 & g_1 & \dots & g_{n-k} & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_{n-k} & 0 & \dots & 0 \\ & & & & & & & \\ 0 & \dots & 0 & g_0 & g_1 & g_2 & \dots & g_{n-k} \end{pmatrix}.$$

Ejemplo Si consideramos C_3 el código binario cíclico de longitud 7 con polinomio generador $g_3(x) = x^3 + x + 1$, entonces aplicando la Proposición 2.2 una matriz generadora de C_3 viene dada por

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

Obviamente, la matriz generadora G_3 es de tamaño 4×7 y con rango 4, pues C es dimensión 4.

En cambio, si tomasemos el código cíclico binario C_1 de longitud 7 con polinomio generador $g_1(x) = 1$, entonces de la Proposición 2.2 deducimos que una matriz generadora de C_1 es la matriz identidad I_7.

3 Polinomio de control y matriz de control de un código cíclico

Si C es un código cíclico de longitud n y dimensión k con polinomio generador $g(x)$, que será de grado $n-k$, sabemos que $g(x)$ es un divisor de $x^n - 1$ y que existe $h(x) \in \mathbb{F}_q[x]$, de grado precisamente k, tal que $g(x)h(x) = x^n - 1$. A este polinomio $h(x)$, que también es mónico y que verifica $g(x)h(x) = x^n - 1$, se le denomina **polinomio de control del código cíclico** C.

Justificamos en la siguiente proposición el denominar a $h(x)$ polinomio de control:

Proposición 3.1 ***(Matriz de control)*** *Sea $C \subset \mathbb{F}_q^n$ un código cíclico con polinomio de control $h(x) = \sum_{i=0}^{k} h_i x^i$ de grado k. Entonces, una matriz de control de C es*

$$\begin{pmatrix} h_k & h_{k-1} & \dots & h_0 & 0 & 0 & \dots & 0 \\ 0 & h_k & h_{k-1} & \dots & h_0 & 0 & \dots & 0 \\ & & & & & & & \\ & & & & & & & \\ 0 & \dots & 0 & h_k & h_{k-1} & h_{k-2} & \dots & h_0 \end{pmatrix}.$$

Observamos que si $C \subset \mathbb{F}_q^n$ es un código cíclico con polinomio de control $h(x) = \sum_{i=0}^{k} h_i x^i$, la matriz H que figura en la proposición anterior nos permite deducir que $C^\perp$ es otro código cíclico puesto que una base de él es la formada por las filas de H y esta base verifica la Proposición 1.1. También lo podríamos verificar estudiando si $h_0^{-1} \sum_{i=0}^{k} h_i x^{k-i}$, que lo obtenemos de la expresión de H, es un divisor de $x^n - 1$ y comprobando que este polinomio genera el ideal de $C^\perp(x)$. En cualquier caso, deducimos que un polinomio generador para $C^\perp$ es $h_0^{-1} \sum_{i=0}^{k} h_i x^{k-i}$. Obviamente, $C^\perp$, que tiene dimensión $n - k$ si C es de dimensión k por ser su dual, tiene un polinomio generador de grado k.

Ejemplo Si consideramos C_3 el código binario cíclico de longitud 7 con polinomio generador $g_3(x) = x^3 + x + 1$, sabemos que su polinomio de control viene dado por $h_3(x) = x^4 + x^2 + x + 1$. Entonces, aplicando la Proposición 3.1 una matriz de control de C_3 viene dada por

$$H_3 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Vemos que la matriz de control H_3 es de tamaño 3×7 y con rango 3, pues C es de dimensión 4. Además, esta matriz genera a $C_3^\perp$, que es también cíclico, y el polinomio generador de $C_3^\perp$ viene dado por $1 + x^2 + x^3 + x^4$, que es precisamente el polinomio $g_6(x)$ del ejemplo de la sección anterior, en el que se calculaban todos los polinomios generadores de códigos cíclicos binarios de longitud 7. Observamos con este ejemplo que el polinomio de control $h(x)$ de un código cíclico C no tiene que ser necesariamente el polinomio generador de $C^\perp$, aunque $h(x)$ tenga el grado adecuado para generar $C^\perp$, sea mónico y divisor de $x^n - 1$.

4 Codificación y decodificación de un código cíclico

Sea $C \subseteq \mathbb{F}_q^n$ un código cíclico de dimensión k con polinomo generador $g(x)$. Supongamos que queremos transmitir un mensaje que contiene la palabra $\mathbf{a} = a_0 \dots a_{k-1} \in \mathbb{F}_q^k$ y que queremos codificar $\mathbf{a}$ usando el código C. Podemos hacerlo de dos modos:

1. Si $\mathbf{a} = a_0 \dots a_{k-1}$, la codificamos como $(a_0 \dots a_{k-1})G$, donde G es una matriz generadora de C. Observamos que G se obtiene de forma fácil a partir de

$g(x)$, usando la Proposición 2.2. Pero para la palabra de longitud n que tiene el receptor, una vez que la haya decodificado para corregir los errores que se hayan producido en la transmisión, no es inmediato calcular sus coordenadas en la base formada por las palabras que constituyen la matriz generadora G y que nos darían, precisamente, $a_0 \dots a_{k-1}$.

2. Si $\mathbf{a} = a_0 \dots a_{k-1}$, construimos el polimonio $b(x) = \sum_{i=0}^{k-1} a_i x^{n-1-i}$. Dividimos $b(x)$ por $g(x)$ y obtenemos $r(x)$ de grado menor que $n-k$ tal que $b(x) = t(x)g(x)+r(x)$. Entonces, codificamos $\mathbf{a}$ usando $b(x)-r(x)$, que es una palabra del $C(x)$, con la ventaja frente al método anterior de que en las k últimas posiciones de esta palabra van las letras de a y esto facilita los cálculos que debe hacer el receptor, una vez que se han corregido los errores que se hayan podido producir en la transmisión, para llegar a $\mathbf{a}$.

Nos preocupamos ahora por cómo puede corregir el receptor los errores producidos en la transmisión, esto es, del proceso de decodificar la palabra recibida. Al ser también códigos lineales, cuando usamos un código cíclico podemos aplicar cualquiera de los dos métodos generales que se utilizan en la decodificación de palabras codificadas con códigos lineales: el método de los líderes y el método de los síndromes. Pero para los códigos cíclicos existe otro método que explota el que las traslaciones cíclicas de palabras de C estén en C. Es el llamado método de decodificación cíclica que explicamos a continuación.

4.1 Método de decodificación cíclica

Sea $C \subseteq \mathbb{F}_q^n$ un código cíclico cuya matriz de control es H y su distancia mínima es d. Supongamos que hemos recibido una palabra $\mathbf{y} = y_0 \dots y_{n-1} \in \mathbb{F}_q^n$ tal que su síndrome es no nulo, esto es, $\mathbf{y} \notin C$ y queremos decodificarla. Como ya se ha indicado, podríamos emplear, por ejemplo, la decodificación por síndromes, que es un método válido para cualquier código lineal, puesto que disponemos de una matriz de control de C. Así, siguiendo el procedimiento explicado en el tema anterior deberíamos calcular la tabla de síndromes (dando un líder para cada síndrome) y localizar aquel líder que tuviese el mismo síndrome que la palabra recibida, decodificando ésta como la diferencia entre la recibida y el líder. Pero en el caso de emplear códigos cíclicos, el proceso anterior puede simplificarse utilizando el llamado método de decodificación cíclica, que está basado en el hecho de que si una palabra $\mathbf{c} = c_0 \dots c_{n-1} \in C$, entonces también pertenece a C la palabra $\mathbf{c}^{(1)} = c_{n-1}c_0 \dots c_{n-2} \in C$. En esencia, el método consiste en fijar una posición de la palabra (por ejemplo, la última) y calcular los síndromes de palabras líder que tengan en esa posición un valor no nulo (lo que llamaremos tabla reducida de síndromes) y compararlo con el síndrome de la palabra recibida. Si coincide, significa que en las posiciones no nulas de las palabras líder se ha producido error y lo podemos corregir. Si no coincide el síndrome de nuestra palabra con ninguna de los de la tabla reducida, significa que en esas posiciones fijadas no se ha producido error y se repite el proceso con $y_{n-1}y_0 \dots y_{n-2}$, $y_{n-2}y_{n-1}y_0 \dots y_{n-3}$, etc. Al igual que en

el cálculo de la tabla de síndromes, siempre empezaremos calculando los síndromes de palabras líder con menor peso y que éste sea a lo sumo $\left[\frac{d-1}{2}\right]$, que son las clases para las que se puede garantizar decodificación única.

Algoritmo del método de decodificación cíclica

Dada $\mathbf{y} = y_0 \dots y_{n-1} \in \mathbb{F}_q^n$ e $i = 1, \dots, n-1$, denotaremos por

$$\mathbf{y}^{(i)} = y_{n-i} y_{n-i+1} \cdots y_{n-1} y_0 \cdots y_{n-i-1}.$$

Así, $\mathbf{y}^{(1)} = y_{n-1} y_0 \dots y_{n-2}$, $\mathbf{y}^{(2)} = y_{n-2} y_{n-1} y_0 \dots y_{n-3}, \dots$. A $\mathbf{y}$ se la denotará por $\mathbf{y}^{(0)}$.

Para describir este método, la componente de la palabra en la que nos fijamos es la última, aunque se puede realizar el proceso fijandose en cualquiera de las componentes.

- Paso 1: Se construye una tabla reducida de síndromes para los líderes con peso menor o igual que $[\frac{d-1}{2}]$ y que tengan última componente no nula.
- Paso 2: Se toma $i = 0$.
- Paso 3: Se calcula $S(\mathbf{y}^{(i)})$. Si $S(\mathbf{y}^{(i)})$ coincide con alguno de los síndromes $S(\mathbf{e})$ de la tabla reducida, significa que se ha producido en $y^{(i)}$ el error $\mathbf{e}$, por lo que $x^{(i)} = (\mathbf{y}^{(i)} - \mathbf{e}) = x_{n-i} x_{n-i+1} \dots x_{n-1} x_0 \dots x_{n-i-1}$ es la i-ésima traslación de la palabra emitida y, por tanto, $\mathbf{x} = x_0 \dots x_{n-1}$, finalizando el proceso. En caso contrario, se va al paso 4.
- Paso 4: Si $S(\mathbf{y}^{(i)})$ no coincide con ninguno de los $S(\mathbf{e})$ de la tabla reducida significa que la última posición de $y^{(i)}$ es correcta y se va al paso 5.
- Paso 5: Se aumenta en una unidad el índice i, verificando que el nuevo índice sea, a lo sumo, $n-1$ y se reitera el paso 3. Si el nuevo índice es n, se va al Paso 6.
- Paso 6: Si no hemos sido capaces de calcular $\mathbf{x}$ mediante el proceso anterior, significa que la palabra recibida tiene más errores que los que es capaz de corregir C, por lo que ampliaremos la tabla reducida con líderes de peso mayor que $[\frac{d-1}{2}]$ y que tengan la última componente no nula y síndrome diferente a los que figuran en la tabla reducida. Entonces, reiteraremos el procedimiento de los pasos anteriores con esta nueva tabla de síndromes hasta lograr la decodificación, que podrá ser no única.

Ejemplo Se considera el código cíclico binario de longitud 7, distancia mínima 3 y cuya matriz de control viene dada por

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

Supongamos que hemos recibido la palabra $\mathbf{y} = 0011110$. Entonces, $S(\mathbf{y}) = 111$, por lo que sabemos que $\mathbf{y} \notin C$.

1. Calculamos la tabla reducida de síndromes:

Líder	**Síndrome**
0000001	001

2. $S(\mathbf{y}^{(0)}) = 111 \neq 001 = S(0000001)$, luego la última componente de $\mathbf{y}$ es correcta.
3. $S(\mathbf{y}^{(1)}) = 011 \neq 001 = S(0000001)$, luego la última componente de $\mathbf{y}^{(1)}$ es correcta.
4. $S(\mathbf{y}^{(2)}) = 001 = S(0000001)$, luego la última componente de $\mathbf{y}^{(2)}$ debe corregirse para obtener $\mathbf{x}^{(2)} = \mathbf{y}^{(2)} - 0000001 = 1000110$ y entonces $\mathbf{x} = 0011010$.

5 Ejemplo de códigos cíclicos: Códigos BCH

Por Teoría de Anillos, si n y q son coprimos entre sí, sabemos que $x^n - 1$ se puede expresar como producto de polinomios mónicos $f_i(x)$ irreducibles sobre $\mathbb{F}_q$, esto es, $x^n - 1 = \prod f_i(x)$ y que si α_i es una raíz de f_i, entonces $t(\alpha_i) = 0$ si y, solo si, $t(x) = f_i(x)a(x)$ para algún polinomio $a(x)$. Esto nos sirve para caracterizar a los códigos cíclicos, usando las raíces de su polinomio generador de la forma siguiente:

Proposición 5.1 *Sea $C \subset \mathbb{F}_q^n$ un código cíclico con polinomio generador $g(x) = \prod_{i=1}^{s} f_i(x)$, siendo f_i polinomio irreducible sobre $\mathbb{F}_q$, y sea α_i una raíz de $f_i(x)$ en una extensión apropiada de $\mathbb{F}_q$. Entonces,*

$$C(x) = \{\overline{t(x)} \in \mathbb{F}_q[x]/(x^n - 1) \,|\, t(\alpha_1) = \cdots = t(\alpha_s) = 0\}.$$

A las raíces del polimonio generador de un código cíclico se les llaman **ceros** del código. Observamos que los ceros siempre son raíces n-ésimas de la unidad. Estos ceros nos sirven para dar otra construcción de los códigos cíclicos: si partimos de un subconjunto de raíces n-ésimas de la unidad, para cada una de ellas le localizamos el polinomio irreducible del que es raíz y construimos el código C cuyo polinomio generador sea el mínimo común múltiplo de de estos polinomios irreducibles. Además, si $\alpha_1, \ldots, \alpha_r$ son los ceros del código cíclico que buscamos, la matriz

$$H_1 = \begin{pmatrix} 1 & \alpha_1 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \ldots & \alpha_2^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_r & \ldots & \alpha_r^{n-1} \end{pmatrix}$$

funciona como una "matriz de control" en el sentido que $c \in C$ si y, solo si, $cH_1^t = 0$.

Un tipo de códigos que se contruyen de esta manera son los códigos BCH: Sean n, $q = p^r$ dos números naturales coprimos entre sí. Sea m el orden multiplicativo de q módulo n, es decir, el número natural más pequeño tal que $q^m \equiv 1 \bmod n$. Sea δ un número natural tal que $2 \leq \delta \leq n$ y sea $\alpha \in \mathbb{F}_{q^m}$ una raíz primitiva n-ésima de la unidad. Se llama **código BCH en sentido estricto sobre $\mathbb{F}_q$ de longitud n y distancia mínima prevista** δ al código cíclico cuyo polinomio generador tiene por raíces a $\{\alpha, \alpha^2, \ldots, \alpha^{\delta-1}\}$. Se puede demostrar que la distancia mínima del código así construido es, al menos, δ.

Ejemplo Consideramos $q = 2$, $n = 2^3 - 1 = 7$ y $\delta = 3$. Entonces, debemos considerar un código cíclico cuyo polinomio generador tenga por raíces a α, y α^2, siendo α una raíz primitiva séptima de la unidad. Ahora, si $f(x) \in \mathbb{F}_2[x]$, entonces $f(\alpha^2) = f(\alpha)^2$, luego α y α^2 tienen el mismo polinomio irreducible. Además, $m = 3$, luego el polinomio irreducible que tiene a α como raíz es de grado 3. Pero $x^7 - 1 = (x-1)(x^3 + x^2 + 1)(x^3 + x + 1)$ en $\mathbb{F}_2[x]$, así que α es raíz de $(x^3 + x^2 + 1)$ ó de $(x^3 + x^2 + 1)$. Supongamos que α es raíz de $(x^3 + x^2 + 1)$. Entonces, este polinomio será el polinomio generador del código BCH buscado. Si aumentaramos en una unidad la distancia prevista, esto es, pidieramos $\delta = 4$, entonces para hallar el código BCH C_1 que tiene también por cero a α, raíz primitiva séptima de la unidad con polinomio irreducible (x^3+x^2+1), debemos incluir en el polinomio generador de C_1 al polinomio irreducible que tenga a α^3, como raíz. Pero el polinomio irreducible de α^3 es, en este caso, $(x^3 + x + 1)$, con lo que C_1 tendrá por polinomio generador a $(x^3 + x^2 + 1)(x^3 + x + 1)$.