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 4:
Codificación y decodificación de un código cíclico

Mayo de 2017

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

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

Así, $\mathbf{y}^{(1)} = y_{n-1}y_0 \dots y_{n-2}$, $\mathbf{y}^{(2)} = y_{n-2}y_{n-1}y_0 \dots y_{n-3}$,.... 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 $\mathbf{x} = 0011010$.