Teoría de códigos y polinomios torcidos

Adrián Ranea Robles

Universidad de Granada

24 de mayo de 2016

Contenidos

Introducción

Los códigos correctores de errores

Los códigos correctores de errores se utilizan para detectar y corregir errores que ocurren cuando la información se transmite por una canal con ruido.

Algunas aplicaciones;

- Reproductores de CD
- Envío de fotografías del espacio a la Tierra

Para ello añaden redundancia al mensaje.

El código de repetición

Caso 1.

- $1 \rightarrow$ «sí»
- $0 \rightarrow$ «no»
- ¿Qué pasa si hay un error?

Caso 2.

- $111 \rightarrow$ «sí»
- $000 \rightarrow$ «no»
- Se puede corregir un error:
  - $001, 010, 100 \rightarrow 000$
  - $110, 101, 011 \rightarrow 111$

Preliminares

Primeras definiciones

Llamaremos alfabeto al conjunto de símbolos que utiliza un código. En nuestro caso, utilizaremos los cuerpos finitos $\mathbb{F}_q$.

Un código de bloque consiste en una función codificadora $E : \mathbb{F}_q^k \to \mathbb{F}_q^n$ y una función decodificadora $D : \mathbb{F}_q^n \to \mathbb{F}_q^k$, con $k < n$. Los elementos de $\mathbb{F}_q^k$ se llaman mensajes, los de $\mathbb{F}_q^n$ palabras y los de $Im(E) \subset \mathbb{F}_q^n$ se llaman palabras código.

Primeras definiciones

Código de repetición:

- $111 \rightarrow$ «sí» $\equiv 1$
- $000 \rightarrow$ «no» $\equiv 0$

111 y 000 son las palabras código. La codificación y la decodificación son las siguientes:

$$E(1) = 111$$
$$E(0) = 000$$
$$D(111) = 1 = D(110) = D(101) = D(011)$$
$$D(000) = 0 = D(001) = D(010) = D(100)$$

Paramétros importantes

- La longitud de código, n.
- El número total de palabras código, M.
- La distancia mínima entre pares de palabras código, d.

La distancia (de Hamming) entre dos palabra código $d(\mathbf{x}, \mathbf{y})$ es el número de posiciones en los que $\mathbf{x}$ e $\mathbf{y}$ difieren. Esta distancia es una métrica en $\mathbb{F}_q^n$.

Código de repetición:

- $111 \rightarrow$ «sí»
- $000 \rightarrow$ «no»

Paramétros importantes

- La longitud de código, n.
- El número total de palabras código, M.
- La distancia mínima entre pares de palabras código, d.

La distancia (de Hamming) entre dos palabra código $d(\mathbf{x}, \mathbf{y})$ es el número de posiciones en los que $\mathbf{x}$ e $\mathbf{y}$ difieren. Esta distancia es una métrica en $\mathbb{F}_q^n$.

Código de repetición: $n = 3, M = 2, d = 3$

- $111 \rightarrow$ «sí»
- $000 \rightarrow$ «no»

Corrigiendo y detectando errores

- El decodificador debe decidir que palabra código fue transmitida.
- Esquema básico de decodificación vecino más cercano: elegir la palabra código más «cercana» a la palabra recibida.
- Supone que el canal es simétrico:
  - Cada símbolo transmitido tiene la misma probabilidad de recibirse erróneamente.
  - Si un símbolo se recibe erróneamente, cada uno de los otros posibles errores es equiprobable.

Corrigiendo y detectando errores

Proposición

Un código con una distancia mínima d puede detectar hasta $d - 1$ errores y corregir hasta $\lfloor (d-1)/2 \rfloor$ errores.

Código de repetición: $n = 3, M = 2, d = 3$

- $111 \rightarrow$ «sí»
- $000 \rightarrow$ «no»

Corrigiendo y detectando errores

Proposición

Un código con una distancia mínima d puede detectar hasta $d - 1$ errores y corregir hasta $\lfloor (d-1)/2 \rfloor$ errores.

Código de repetición: $n = 3, M = 2, d = 3$

- $111 \rightarrow$ «sí»
- $000 \rightarrow$ «no»

Detecta hasta 2 errores y corrige hasta 1 error.

Teoría de códigos algebraica

Códigos lineales

Un código lineal de longitud n sobre $\mathbb{F}_q$ es un subespacio vectorial del espacio vectorial $\mathbb{F}_q^n$.

Un $[n, k]$-código lineal es un código lineal de longitud n sobre sobre $\mathbb{F}_q$ con dimensión k como subespacio vectorial.

Podemos identificar el espacio de mensajes con el espacio vectorial $\mathbb{F}_q^k$. Así, las funciones de codificación/decodificación serían:

$$E : \mathbb{F}_q^k \to \mathbb{F}_q^n, \; D : \mathbb{F}_q^n \to \mathbb{F}_q^k$$

Códigos lineales

Proposición

Sea C un código lineal. Toda combinación lineal de palabras código de C es una palabra código de C.

Proposición

La distancia mínima $d(C)$ de un código lineal C es igual a la mínima distancia entre los pares $(\mathbf{x}, 0)$ con $\mathbf{x}$ no nulo.

Códigos lineales

Límite de Singleton

Si C es un $[n, k]$-código lineal entonces $d \leq n - k + 1$.

A los códigos que consiguen la igualdad se les llama códigos separables de distancia máxima.

Ejemplo: Reed-Solomon. Utilizado en CDs, DVDs, Blu-ray, QR, ...

Códigos lineales

Matriz generatriz y codificación

Una matriz G de tamaño $k \times n$ cuyas filas forman una base para un $[n, k]$-código lineal se llama matriz generatriz del código.

Si C es un $[n, k]$-código lineal con matriz generatriz G, entonces la función de codificación puede escribirse como:

$$E : \mathbb{F}_q^k \to \mathbb{F}_q^n$$
$$\mathbf{x} \mapsto \mathbf{x}G$$

Códigos lineales

Matriz generatriz y codificación. Ejemplo

Sea C el código linear sobre $\mathbb{F}_2^4$ de dimensión 2 con matriz generatriz

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

Multiplicando los elementos $\mathbb{F}_2^2$ con G obtenemos el código C:

$$\{ \qquad\qquad\qquad\qquad \}$$

Códigos lineales

Matriz generatriz y codificación. Ejemplo

Sea C el código linear sobre $\mathbb{F}_2^4$ de dimensión 2 con matriz generatriz

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

Multiplicando los elementos $\mathbb{F}_2^2$ con G obtenemos el código C:

$$\{0000, \qquad\qquad\qquad\qquad \}$$

Códigos lineales

Matriz generatriz y codificación. Ejemplo

Sea C el código linear sobre $\mathbb{F}_2^4$ de dimensión 2 con matriz generatriz

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

Multiplicando los elementos $\mathbb{F}_2^2$ con G obtenemos el código C:

$$\{0000, 1011, \qquad\qquad\}$$

Códigos lineales

Matriz generatriz y codificación. Ejemplo

Sea C el código linear sobre $\mathbb{F}_2^4$ de dimensión 2 con matriz generatriz

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

Multiplicando los elementos $\mathbb{F}_2^2$ con G obtenemos el código C:

$$\{0000, 1011, 0101, \qquad \}$$

Códigos lineales

Matriz generatriz y codificación. Ejemplo

Sea C el código linear sobre $\mathbb{F}_2^4$ de dimensión 2 con matriz generatriz

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

Multiplicando los elementos $\mathbb{F}_2^2$ con G obtenemos el código C:

$$\{0000, 1011, 0101, 1100\}$$

Códigos lineales

Clases laterales y decodificación

Sea C un $[n, k]$-código lineal sobre $\mathbb{F}_q$ y $\mathbf{a}$ un vector de $\mathbb{F}_q^n$. El conjunto $\mathbf{a} + C = \{\mathbf{a} + \mathbf{x} \mid \mathbf{x} \in C\}$ se llama una clase lateral de C.

Proposición

Si C es un $[n, k]$ código lineal sobre $\mathbb{F}_q$, entonces cada vector de $\mathbb{F}_q^n$ está en alguna clase lateral de C, cada clase lateral contiene q^k vectores y dos clases laterales son idénticas o disjuntas.

Códigos lineales

Clases laterales y decodificación

Esquema vecino más cercano:

Códigos lineales

Clases laterales y decodificación

Esquema vecino más cercano:

1. Particionamos $\mathbb{F}_q^n$ en clases laterales de C.

Códigos lineales

Clases laterales y decodificación

Esquema vecino más cercano:

1. Particionamos $\mathbb{F}_q^n$ en clases laterales de C.
2. Para cada clase lateral, elegimos un representante con número de componentes no nulas mínimo.

Códigos lineales

Clases laterales y decodificación

Esquema vecino más cercano:

1. Particionamos $\mathbb{F}_q^n$ en clases laterales de C.
2. Para cada clase lateral, elegimos un representante con número de componentes no nulas mínimo.

Al recibir una palabra $\mathbf{y}$:

Códigos lineales

Clases laterales y decodificación

Esquema vecino más cercano:

1. Particionamos $\mathbb{F}_q^n$ en clases laterales de C.
2. Para cada clase lateral, elegimos un representante con número de componentes no nulas mínimo.

Al recibir una palabra $\mathbf{y}$:

1. Buscamos la clase lateral que contiene a $\mathbf{y}$. Esta será de la forma $\mathbf{e} + C$

Códigos lineales

Clases laterales y decodificación

Esquema vecino más cercano:

1. Particionamos $\mathbb{F}_q^n$ en clases laterales de C.
2. Para cada clase lateral, elegimos un representante con número de componentes no nulas mínimo.

Al recibir una palabra $\mathbf{y}$:

1. Buscamos la clase lateral que contiene a $\mathbf{y}$. Esta será de la forma $\mathbf{e} + C$
2. $\mathbf{y} - \mathbf{e}$ fue la palabra de código enviada.

Códigos lineales

Clases laterales y decodificación

Sea $C = \{0000, 1011, 0101, 1100\}$.

Las clases laterales de C son:

Códigos lineales

Clases laterales y decodificación

Sea $C = \{0000, 1011, 0101, 1100\}$.

Las clases laterales de C son:

$$0000 + C = \{0000, 1011, 0101, 1110\}$$

Códigos lineales

Clases laterales y decodificación

Sea $C = \{0000, 1011, 0101, 1100\}$.

Las clases laterales de C son:

$$0000 + C = \{0000, 1011, 0101, 1110\}$$
$$1000 + C = \{1000, 0011, 1101, 0110\}$$

Códigos lineales

Clases laterales y decodificación

Sea $C = \{0000, 1011, 0101, 1100\}$.

Las clases laterales de C son:

$$0000 + C = \{0000, 1011, 0101, 1110\}$$
$$1000 + C = \{1000, 0011, 1101, 0110\}$$
$$0100 + C = \{0100, 1111, 0001, 1010\}$$

Códigos lineales

Clases laterales y decodificación

Sea $C = \{0000, 1011, 0101, 1100\}$.

Las clases laterales de C son:

$$0000 + C = \{0000, 1011, 0101, 1110\}$$
$$1000 + C = \{1000, 0011, 1101, 0110\}$$
$$0100 + C = \{0100, 1111, 0001, 1010\}$$
$$0010 + C = \{0010, 1001, 0111, 1100\}$$

Códigos cíclicos

Un código lineal C de longitud n es cíclico si verifica:

$$(c_0, c_1, \ldots, c_{n-1}) \in C \implies (c_{n-1}, c_0, \ldots, c_{n-1}) \in C$$

Los códigos cíclicos se pueden implementar de forma eficiente usando dispositivos hardware llamados registros de desplazamiento.

Códigos cíclicos

Representación polinomial

$$\phi : \mathbb{F}_q^n \to \mathbb{F}_q[x]/(x^n - 1)$$
$$(c_0, c_1, \ldots, c_{n-1}) \mapsto c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$$

- ϕ es un isomorfismo de espacios vectoriales.

Son equivalentes:

i) $(c_0, c_1, \ldots, c_{n-1}) \in C \implies (c_{n-1}, c_0, \ldots, c_{n-2}) \in C$

ii) $x(c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}) \in \phi(C)$

Códigos cíclicos

Representación polinomial

La equivalencia se basta en la siguiente igualdad en $\mathbb{F}_q[x]/(x^n - 1)$:

$$x(c_0 + c_1 x + \cdots + c_{n-1} x^{n-1})$$

Códigos cíclicos

Representación polinomial

La equivalencia se basta en la siguiente igualdad en $\mathbb{F}_q[x]/(x^n - 1)$:

$$\begin{aligned} & x(c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}) \\ & \quad = xc_0 + xc_1 x + \cdots + xc_{n-1} x^{n-1} \end{aligned}$$

Códigos cíclicos

Representación polinomial

La equivalencia se basta en la siguiente igualdad en $\mathbb{F}_q[x]/(x^n - 1)$:

$$\begin{aligned} & x(c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}) \\ & \quad = xc_0 + xc_1 x + \cdots + xc_{n-1} x^{n-1} \\ & \quad = c_0 x + c_1 x^2 + \cdots + c_{n-1} x^n \end{aligned}$$

Códigos cíclicos

Representación polinomial

La equivalencia se basta en la siguiente igualdad en $\mathbb{F}_q[x]/(x^n - 1)$:

$$\begin{aligned} & x(c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}) \\ &= x c_0 + x c_1 x + \cdots + x c_{n-1} x^{n-1} \\ &= c_0 x + c_1 x^2 + \cdots + c_{n-1} x^n \\ &= c_{n-1} + c_0 x + c_1 x^2 + \cdots + c_{n-2} x^{n-1} \end{aligned}$$

Códigos cíclicos

Representación polinomial

Si $f(x) \in \phi(C)$, entonces

$$\left\{xf(x), x^2 f(x), x^3 f(x), \ldots, x^{n-1} f(x)\right\}$$

también están en $\phi(C)$.

Usando la linealidad de C se deduce:

$$\forall p(x) \in \mathbb{F}_q[x]/(x^n - 1),\ p(x)f(x) \in \phi(C)$$

Códigos cíclicos

Representación polinomial

Teorema

Los códigos cíclicos de longitud n sobre $\mathbb{F}_q$ son justamente los ideales del anillo $\mathbb{F}_q[x]/(x^n - 1)$

Proposición

Sea C un código cíclico de longitud n. Entonces C está generado por un divisor $g(x)$ de $(x^n - 1)$ en $\mathbb{F}_q[x]$. Si $g(x)$ mónico y de grado mínimo, $g(x)$ es único y se llama el polinomio generador de C.

Códigos cíclicos

Codificación

Dado un mensaje $\mathbf{a} = (a_0, \ldots, a_{n-1})$, y su representación polinomial $a(x)$, mediante multiplicación de polinomios podemos realizar la codificación:

$$\begin{aligned} E : \mathbb{F}_q[x]/(x^n - 1) &\to \mathbb{F}_q[x]/(x^n - 1) \\ a(x) &\mapsto a(x)g(x) \end{aligned}$$

Códigos cíclicos

Matriz generatriz

Lema

Sea C un código cíclico con polinomio generador $g(x) = g_0 + g_1 x + \cdots + g_r x^r$ de grado r. Entonces la dimensión de C es $n - r$ y una matriz generatriz para C es la siguiente matriz $(n - r) \times n$:

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_r & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_r & 0 & \cdots & 0 \\ 0 & 0 & g_0 & g_1 & \cdots & g_r & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \cdots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_r \end{pmatrix}$$

Códigos cíclicos

Matriz generatriz. Demostración

g_0 no puede ser 0 (en caso contrario $(0, g_1, \ldots, g_r, 0, \ldots) \in C \Rightarrow (g_1, \ldots, g_r, 0, \ldots) \in C$)

Las $n - r$ filas de la matriz G son linealmente independientes por la forma escalonada de la matriz.

Estas $n - r$ filas representan los polinomios código $g(x), xg(x), \ldots, x^{n-r-1}g(x)$. Veamos que forman un sistema de generadores.

Códigos cíclicos

Matriz generatriz. Demostración

$c(x) \in C \implies \exists m(x) \in \mathbb{F}_q[x]/(x^n - 1)$ tal que:

$$\begin{aligned} c(x) &= m(x)g(x) \\ &= (m_0 + m_1 x + \cdots + m_{n-r-1}x^{n-r-1})g(x) \\ &= m_0 g(x) + m_1 x g(x) + \cdots m_{n-r-1}x^{n-r-1}g(x) \end{aligned}$$

$\implies$ G es una matriz generatriz de C y la dimensión de C es $n - r$ $\square$.

Códigos cíclicos

Listado de códigos

Proposición

Hay una correspondencia uno a uno entre los divisores mónicos de $x^n - 1$ en $\mathbb{F}_q[x]$ y los códigos cíclicos sobre $\mathbb{F}_q$ de longitud n.

Este resultado facilita el listado de todos los códigos cíclicos de una longitud dada. Veamos un ejemplo.

Códigos cíclicos

Listado de codigos

Vamos a calcular todos los códigos cíclicos sobre $\mathbb{F}_2$ de longitud 4. La factorización de $x^4 + 1$ es $(x + 1)^4$, luego sus factores mónicos son:

Códigos cíclicos

Listado de codigos

Vamos a calcular todos los códigos cíclicos sobre $\mathbb{F}_2$ de longitud 4. La factorización de $x^4 + 1$ es $(x + 1)^4$, luego sus factores mónicos son:

$$g_0(x) = 1$$

Códigos cíclicos

Listado de codigos

Vamos a calcular todos los códigos cíclicos sobre $\mathbb{F}_2$ de longitud 4. La factorización de $x^4 + 1$ es $(x + 1)^4$, luego sus factores mónicos son:

$$g_0(x) = 1$$
$$g_1(x) = x + 1$$

Códigos cíclicos

Listado de codigos

Vamos a calcular todos los códigos cíclicos sobre $\mathbb{F}_2$ de longitud 4. La factorización de $x^4 + 1$ es $(x + 1)^4$, luego sus factores mónicos son:

$$g_0(x) = 1$$
$$g_1(x) = x + 1$$
$$g_2(x) = (x + 1)^2 = x^2 + 1$$

Códigos cíclicos

Listado de codigos

Vamos a calcular todos los códigos cíclicos sobre $\mathbb{F}_2$ de longitud 4. La factorización de $x^4 + 1$ es $(x + 1)^4$, luego sus factores mónicos son:

$$g_0(x) = 1$$
$$g_1(x) = x + 1$$
$$g_2(x) = (x + 1)^2 = x^2 + 1$$
$$g_3(x) = (x + 1)^3 = x^3 + x^2 + x + 1$$

Códigos cíclicos

Listado de codigos

Vamos a calcular todos los códigos cíclicos sobre $\mathbb{F}_2$ de longitud 4. La factorización de $x^4 + 1$ es $(x + 1)^4$, luego sus factores mónicos son:

$$
\begin{aligned}
g_0(x) &= 1 \\
g_1(x) &= x + 1 \\
g_2(x) &= (x + 1)^2 = x^2 + 1 \\
g_3(x) &= (x + 1)^3 = x^3 + x^2 + x + 1 \\
g_4(x) &= (x + 1)^4 = x^4 + 1
\end{aligned}
$$

Códigos cíclicos

Listado de códigos. Ejemplo

El primer y el último factor generan los códigos triviales $\mathbb{F}_2[x]/(x^4+1)$ y $\{0\}$ respectivamente. El resto de polinomios generan los códigos:

Códigos cíclicos

Listado de códigos. Ejemplo

El primer y el último factor generan los códigos triviales $\mathbb{F}_2[x]/(x^4+1)$ y $\{0\}$ respectivamente. El resto de polinomios generan los códigos:

$$g_1(x) \to C_1 = \{0, x+1, x^2+1, x^2+x, x^3+1, x^3+x, x^3+x^2, x^3+x^2+x+1\}$$

Códigos cíclicos

Listado de códigos. Ejemplo

El primer y el último factor generan los códigos triviales $\mathbb{F}_2[x]/(x^4+1)$ y $\{0\}$ respectivamente. El resto de polinomios generan los códigos:

$$g_1(x) \to C_1 = \{0, x+1, x^2+1, x^2+x, x^3+1, x^3+x, x^3+x^2, x^3+x^2+x+1\}$$

$$g_2(x) \to C_2 = \{0, x^2+1, x^3+x, x^3+x^2+x+1\}$$

Códigos cíclicos

Listado de códigos. Ejemplo

El primer y el último factor generan los códigos triviales $\mathbb{F}_2[x]/(x^4+1)$ y $\{0\}$ respectivamente. El resto de polinomios generan los códigos:

$$g_1(x) \to C_1 = \{0, x+1, x^2+1, x^2+x, x^3+1, x^3+x, x^3+x^2, x^3+x^2+x+1\}$$

$$g_2(x) \to C_2 = \{0, x^2+1, x^3+x, x^3+x^2+x+1\}$$

$$g_3(x) \to C_3 = \{0, x^3+x^2+x+1\}$$

Códigos cíclicos

Listado de códigos. Ejemplo

El primer y el último factor generan los códigos triviales $\mathbb{F}_2[x]/(x^4+1)$ y $\{0\}$ respectivamente. El resto de polinomios generan los códigos:

$$g_1(x) \to C_1 = \{0, x+1, x^2+1, x^2+x, x^3+1, x^3+x, x^3+x^2, x^3+x^2+x+1\}$$
$$g_2(x) \to C_2 = \{0, x^2+1, x^3+x, x^3+x^2+x+1\}$$
$$g_3(x) \to C_3 = \{0, x^3+x^2+x+1\}$$

C_1 es un código $[4,3]$-cíclico, C_2 es un código $[4,2]$-cíclico y C_3 es un código $[4,1]$-cíclico.

Códigos cíclicos torcidos

Códigos cíclicos torcidos

Sea θ un automorfismo de $\mathbb{F}_q$. Un código θ-cíclico es un código lineal C_θ verificando:

$$(a_0, a_1, \ldots, a_{n-1}) \in C_\theta \Rightarrow (\theta(a_{n-1}), \theta(a_0), \ldots, \theta(a_{n-2}))$$

Consideramos el anillo de polinomios torcidos sobre $\mathbb{F}_q$, esto es, la extensión de Ore:

$$\mathbb{F}_q[x, \theta] = \{a_0 + a_1 x + \cdots + a_{n-1} x^{n-1},\ a_i \in \mathbb{F}_q,\ n \in \mathbb{N}\}$$

donde la regla de multiplicación es $xa = \theta(a)x$.

Códigos cíclicos torcidos

Anillo de polinomios torcidos

$\mathbb{F}_q[x, \theta]$

- tiene un algoritmo de división euclídeo por la izquierda y por la derecha.
- es un dominio de ideales principales por la izquierda y por la derecha.

Denotamos por $K \subset \mathbb{F}_q$ al subcuerpo cuyos elementos se quedan fijos por θ.

Códigos cíclicos torcidos

Centro del anillo de polinomios torcidos

Proposición

Los elementos centrales de $\mathbb{F}_q[x, \theta]$ son de la forma $\sum_{i=0}^{m} c_i x^{i|\theta|}$ donde $c_i \in K$ y $|\theta|$ es el orden del automorfismo θ. Simbólicamente:

$$Z(\mathbb{F}_q[x, \theta]) = K[x^{|\theta|}]$$

Códigos cíclicos torcidos

Centro del anillo de polinomios torcidos. Demostración

Sea $g(x) = \sum_{i=0}^{m} g_i x^i \in Z(\mathbb{F}_q[x, \theta])$.

$$g(x)a_0 = \sum_{i=0}^{m} g_i \theta^i(a_0) x^i$$

$$a_0 g(x) = \sum_{i=0}^{m} a_0 g_i x^i$$

$$\implies a_0 = \theta^i(a_0) \; \forall a_0 \in \mathbb{F}_q \implies g(x) \in \mathbb{F}_q[x^{|\theta|}]$$

Códigos cíclicos torcidos

Centro del anillo de polinomios torcidos. Demostración

$$g(x) = \sum_{i=0}^{m} g_i x^i$$

$$g(x)\ b_1 x = \sum_{i=0}^{m} g_i \theta^i(b_1) x^{i+1}$$

$$b_1 x\ g(x) = \sum_{i=0}^{m} b_1 \theta(g_i) x^{i+1}$$

$$\Longrightarrow\ g_i = \theta(g_i)\ \Longrightarrow\ g_i \in K\ \Longrightarrow\ g(x) \in K[x^{|\theta|}]$$

Códigos cíclicos torcidos

Centro del anillo de polinomios torcidos. Demostración

Sea $c\ x^{j|\theta|} \in K[x^{|\theta|}]$, $f(x) = \sum_{i=0}^{m} f_i x^i \in \mathbb{F}_q[x, \theta]$.

$$c\ x^{j|\theta|} \times f(x) = \sum_{i=0}^{m} c\ \theta^{j|\theta|}(f_i) x^{i+j|\theta|}$$

$$f(x) \times c\ x^{j|\theta|} = \sum_{i=0}^{m} f_i \theta^i(c) x^{i+j|\theta|}$$

$$\Longrightarrow\ c\ x^{j|\theta|} \in Z(\mathbb{F}_q[x, \theta])$$

Por linealidad, $K[x^{|\theta|}] \subset Z(\mathbb{F}_q[x, \theta])$ $\square$

Códigos cíclicos torcidos

Resultados conocidos

Proposición

Los elementos centrales de $\mathbb{F}_q[x, \theta]$ son los generadores de los ideales biláteros de $\mathbb{F}_q[x, \theta]$ y $(x^n - 1) \subset \mathbb{F}_q[x, \theta]$ es un ideal bilátero.

Proposición

El anillo $\mathbb{F}_q[x, \theta]/(x^n - 1)$ es un anillo de ideales principales por la izquierda cuyos ideales por la izquierda están generados por un divisor de $x^n - 1$ en $\mathbb{F}_q[x, \theta]$.

Códigos cíclicos torcidos

Representación polinomial «torcida»

$$\phi : \mathbb{F}_q^n \to \mathbb{F}_q[x, \theta]/(x^n - 1)$$
$$(c_0, c_1, \ldots, c_{n-1}) \mapsto c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$$

- ϕ es un isomorfismo de $\mathbb{F}_q$-módulos

Son equivalentes:

$$(c_0, c_1, ..., c_{n-1}) \in C \Rightarrow (\theta(c_{n-1}), \theta(c_0), ..., \theta(c_{n-2})) \in C$$
$$x(c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}) \in \phi(C)$$

Códigos cíclicos torcidos

Representación polinomial «torcida»

La equivalencia se basta en la siguiente igualdad en $\mathbb{F}_q[x, \theta]/(x^n - 1)$:

$$x(c_0 + c_1 x + \cdots + c_{n-1} x^{n-1})$$

Códigos cíclicos torcidos

Representación polinomial «torcida»

La equivalencia se basta en la siguiente igualdad en $\mathbb{F}_q[x, \theta]/(x^n - 1)$:

$$x(c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}) = xc_0 + xc_1 x + \cdots + xc_{n-1} x^{n-1}$$

Códigos cíclicos torcidos

Representación polinomial «torcida»

La equivalencia se basta en la siguiente igualdad en $\mathbb{F}_q[x, \theta]/(x^n - 1)$:

$$
\begin{aligned}
& x(c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}) \\
& \quad = x c_0 + x c_1 x + \cdots + x c_{n-1} x^{n-1} \\
& \quad = \theta(c_0) x + \theta(c_1) x^2 + \cdots + \theta(c_{n-1}) x^n
\end{aligned}
$$

Códigos cíclicos torcidos

Representación polinomial «torcida»

La equivalencia se basta en la siguiente igualdad en $\mathbb{F}_q[x, \theta]/(x^n - 1)$:

$$
\begin{aligned}
& x(c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}) \\
& \quad = x c_0 + x c_1 x + \cdots + x c_{n-1} x^{n-1} \\
& \quad = \theta(c_0) x + \theta(c_1) x^2 + \cdots + \theta(c_{n-1}) x^n \\
& \quad = \theta(c_{n-1}) + \theta(c_0) x + \theta(c_1) x^2 + \cdots + \theta(c_{n-2}) x^{n-1}
\end{aligned}
$$

Códigos cíclicos torcidos

Representación polinomial «torcida»

Si $f(x) \in \phi(C)$, entonces

$$\left\{xf(x), x^2 f(x), x^3 f(x), \ldots, x^{n-1} f(x)\right\}$$

también están en $\phi(C)$.

Usando la linealidad de C se deduce:

$$\forall p(x) \in \mathbb{F}_q[x, \theta]/(x^n - 1),\ p(x)f(x) \in \phi(C)$$

Códigos cíclicos torcidos

Representación polinomial «torcida»

Teorema

Los códigos θ-cíclicos de longitud n sobre $\mathbb{F}_q$ son justamente los ideales por la izquierda del anillo $\mathbb{F}_q[x, \theta]/(x^n - 1)$.

Códigos cíclicos torcidos

Representación polinomial «torcida»

Un factor por la derecha de grado $n - k$ de $x^n - 1$ genera un $[n, k]$-código lineal.

$\mathbb{F}_q[x, \theta]$ no es en general un dominio de factorización única. Como hay muchos mas factores por la derecha que en el caso conmutativo, existen más codigos θ-cíclicos que cíclicos.

Nótese que aunque la factorización no sea única, los grados de los polinomios torcidos irreducibles en la factorización de un elemento en $\mathbb{F}_q[x, \theta]$ si son únicos salvo permutación.

Códigos cíclicos torcidos

Ejemplo

Vamos a buscar todos los [4, 2]-códigos θ-cíclicos con $\theta(a) = a^2$ sobre $\mathbb{F}_4$.

Sea α un generador del grupo multiplicativo de $\mathbb{F}_4$, esto es, un cero de $z^2 + z + 1 \in \mathbb{F}_2$ en $\overline{\mathbb{F}_2}$. Así, $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$.

Calculamos los factores mónicos por la derecha de grado dos de $x^4 + 1 \in \mathbb{F}_4[x, \theta]$.

Códigos cíclicos torcidos

Ejemplo

$$
\begin{aligned}
g_1(x) &= x^2 + 1 \\
g_2(x) &= x^2 + \alpha x + \alpha^2 \\
g_3(x) &= x^2 + \alpha^2 x + \alpha \\
g_4(x) &= x^2 + \alpha^2 x + \alpha^2 \\
g_5(x) &= x^2 + x + \alpha \\
g_6(x) &= x^2 + x + \alpha^2 \\
g_7(x) &= x^2 + \alpha x + \alpha
\end{aligned}
$$

Códigos cíclicos torcidos

Ejemplo

Las factorizaciones correspondientes son:

$$\begin{aligned} x^4+1 &= (x^2+1)(x^2+1) \\ &= (x^2+\alpha x+\alpha)(x^2+\alpha x+\alpha^2) \\ &= (x^2+\alpha^2 x+\alpha^2)(x^2+\alpha^2 x+\alpha) \\ &= (x^2+\alpha^2 x+\alpha)(x^2+\alpha^2 x+\alpha^2) \\ &= (x^2+x+\alpha^2)(x^2+x+\alpha) \\ &= (x^2+x+\alpha)(x^2+x+\alpha^2) \\ &= (x^2+\alpha x+\alpha^2)(x^2+\alpha x+\alpha) \end{aligned}$$

Códigos cíclicos torcidos

Ejemplo

Como $x^4 + 1 = (x + 1)(x + 1)(x + 1)(x + 1)$, los factores irreducibles de $x^4 + 1 \in \mathbb{F}_4[x, \theta]$ en cualquier descomposicón son todos de grado uno. Por lo tanto, ninguno de los $g_i(x)$ anteriores es irreducible.

El polinomio g_1 genera el único $[4, 2]$-código cíclico sobre $\mathbb{F}_4$. Los otros polinomios generan un código $[4, 2]$ (los seis códigos son equivalentes).

Para más información:

www.github.com/ranea/teoriacodigos

GRACIAS