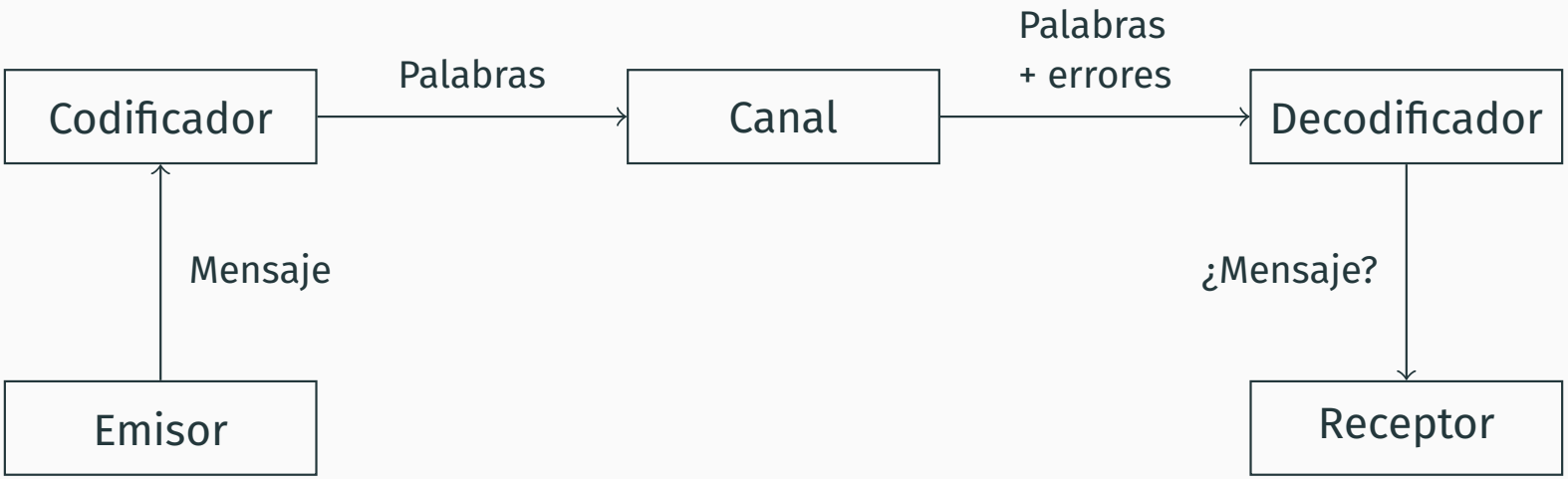
Códigos skew Reed-Solomon y teorema de Artin-Wedderburn efectivo

José Manuel Muñoz Fuentes

21 de junio de 2019

Códigos skew Reed-Solomon

Comunicación



Códigos

Se considera un cuerpo finito F, el espacio vectorial de dimensión n que genera, F^n, y una distancia o métrica en F^n.

Definición

Un **código** es un subconjunto $\mathcal{C}$ de F^n.

Si la distancia entre una palabra $w \in \mathcal{C}$ y la palabra con errores $w + e \in F^n$ es pequeña, reconstruimos w como el elemento de $\mathcal{C}$ más cercano a $w + e$.

Códigos lineales y cíclicos

Para que sea eficiente encontrar el elemento más cercano en $\mathcal{C}$, conviene que $\mathcal{C}$ tenga cierta estructura algebraica.

Definición

Un **código lineal** es un código que es subespacio vectorial de F^n.

Definición

Un **código cíclico** es un código lineal cerrado para la operación

$$(c_0, c_1, \ldots, c_{n-1}) \mapsto (c_{n-1}, c_0, \ldots, c_{n-2})$$

Códigos cíclicos como ideales

Las palabras en un código cíclico se pueden ver como elementos en el anillo de ideales principales

$$\mathcal{R} = \frac{F[x]}{\langle x^n - 1 \rangle}$$

mediante la correspondencia

$$(c_0, c_1, c_2, \dots) \mapsto c_0 + c_1 x + c_2 x^2 + \cdots + \langle x^n - 1 \rangle$$

Así, los códigos cíclicos se corresponden con los ideales de $\mathcal{R}$, que por ser principales están generados por un elemento.

Códigos Reed-Solomon

Definición

Un **código BCH** es un ideal de $\mathcal{R}$ generado por el mcm de los polinomios mínimos en $F[x]$ de α^b, α^{b+1}, $\ldots$, α^{b+2t} para algún α raíz primitiva de $x^n - 1$ y algunos $b, t \in \mathbb{N}$.

Definición

Un **código Reed-Solomon** es un código BCH en el caso $n = |F| - 1$.

Códigos Reed-Solomon

Como $x^{|F|-1} - 1$ descompone en F, un código Reed-Solomon es un ideal de $\mathcal{R}$ generado por

$$g(x) = \prod_{i=1}^{2t} \left(x - \alpha^{b+i}\right)$$

con $\alpha \in F$ y $b, t \in \mathbb{N}$.

Dada una palabra $w \in \mathcal{C}$, todos los elementos de F^n a una distancia de Hamming de t o menos respecto de w tienen por palabra más cercana w. Es decir, los códigos Reed-Solomon permiten corregir t errores.

Codificación Reed-Solomon

Dado un mensaje representado como un elemento de F^k con $k = n - 2t$, se dispone como un polinomio y se multiplica por $g(x)$, teniendo así una palabra de $\mathcal{C} = \mathcal{R}g(x)$.

Algunos algoritmos de decodificación:

- Peterson-Gorenstein-Zierler
- Berlekamp-Massey
- Sugiyama
- Sudan-Guruswami

Polinomios skew

Ahora consideramos un automorfismo $\sigma : F \mapsto F$

Definición

El anillo de **polinomios skew** $R = F[x; \sigma]$ es el conjunto de polinomios de $F[x]$ con la suma habitual y el producto

$$xa = \sigma(a)x$$

No es un anillo conmutativo (si $\sigma \neq id$), pero si σ es de orden μ, entonces $x^\mu - 1$ es central y se tiene un anillo cociente

$$\mathcal{R} = \frac{R}{R(x^\mu - 1)}$$

Códigos skew Reed-Solomon

Definición

Un **código skew cíclico** es un ideal izquierda de $\mathcal{R}$.

Definición

Un **código skew Reed-Solomon** es un código skew cíclico generado por el mcm a la izquierda de

$$x - \sigma^{b}(\beta),\ x - \sigma^{b+1}(\beta),\ \ldots,\ x - \sigma^{b+2t}(\beta)$$

donde $\beta = \frac{\sigma(\alpha)}{\alpha}$ para algún $\alpha \in F$ cuyos conjugados sean una base normal de F y algunos $b, t \in \mathbb{N}$.

Teorema de Artin-Wedderburn efectivo

Teorema de Artin-Wedderburn

Teorema (Artin-Wedderburn)
Todo anillo semisimple es isomorfo a algún producto

$$M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$$

con D_i anillos de división.

En particular, si K es un cuerpo finito:

Teorema (Artin-Wedderburn, álgebras de dimensión finita)
Toda K-álgebra semisimple de dimensión finita es isomorfa a un producto

$$M_{n_1}(E_1) \times \cdots \times M_{n_r}(E_r)$$

con E_i cuerpo extensión de K.

Corolario

Corolario

Si K es un cuerpo finito, toda K-álgebra simple A de dimensión finita con centro $Z(A)$ es isomorfa a $M_n(Z(A))$.

Además, n queda determinado por las dimensiones de A y $Z(A)$.

Estos resultados acotan las posibles estructuras de las K-álgebras semisimples, pero no dan un isomorfismo explícito.

Estructura del anillo $R = F[x; \sigma]$

Siendo σ un automorfismo de F de orden μ, se tiene el subcuerpo $K = F^{\sigma}$.

Proposición

El centro de $R = F[x; \sigma]$ es $K[x^{\mu}]$ y todos sus ideales biláteros son los de la forma $Rq(x^{\mu})x^{k}$ con $q(x^{\mu}) \in K[x^{\mu}]$ y $k \in \mathbb{N}$.

Por ello, para cada $p(x) = q(x^{\mu})x^{k}$ tenemos la K-álgebra cociente de dimensión finita

$$\mathcal{R} = \frac{R}{Rp(x)}$$

Proposición

$\mathcal{R}$ es semisimple si y solo si $k \leq 1$ y $q(x^{\mu})$ es libre de cuadrados en $K[x^{\mu}]$.

Estructura del anillo $R = F[x; \sigma]$

Así, si $\mathcal{R} = \frac{R}{Rp(x)}$ es semisimple, $p(x) = q(x^\mu)$ o $p(x) = q(x^\mu)x$ donde $q(x^\mu) = \prod_i q_i(x^\mu)$.

- Si $p(x) = \prod_i q_i(x^\mu)$ entonces

$$\mathcal{R} \cong \bigoplus_i \frac{R}{Rp_i(x^\mu)} \cong \bigoplus_i \mathcal{R}_i$$

- Si $p(x) = q(x^\mu)x$, entonces

$$\mathcal{R} \cong \frac{R}{Rx} \bigoplus \frac{R}{Rq(x^\mu)} \cong \mathcal{R}_o \bigoplus \mathcal{R}' \cong F \bigoplus \mathcal{R}'$$

  y $\mathcal{R}'$ descompone como en el caso anterior.

Cada $\mathcal{R}_i$ es simple y, por dimensión y por cómo es el centro de $\mathcal{R}_i$, isomorfo a $M_\mu(K(\beta_i))$ con β_i raíz de $q_i(y)$ (tomando $y = x^\mu$).

Construcción del isomorfismo

Para dar un isomorfismo basta con dar un homomorfismo

$$\varphi : R \mapsto \bigoplus_i M_i$$

de núcleo $Rp(x)$, y para ello solo hay que dar la imagen de x y de un $\alpha \in F$ tal que $F = K(\alpha)$ de forma que:

- $p(\varphi(x)) = 0$ y $p'(\varphi(x)) \neq 0$ para $p'(x)$ divisor propio de $p(x)$
- $m(\varphi(\alpha)) = 0$ con m el polinomio mínimo de α en $K[x]$
- $\varphi(x)\varphi(\alpha) = \varphi(\sigma(\alpha))\varphi(x)$

φ^{-1} se puede construir planteando un sistema de ecuaciones a partir de las imágenes por φ de elementos de R.

Caso $x^\mu - 1$

Si $p(x) = x^\mu - 1$, definimos:

$$\varphi(x) = M_B(\sigma), \qquad \varphi(\alpha) = M_B(\lambda_\alpha)$$

donde $M_B : End_K(F) \cong End_K(K^\mu) \to M_\mu(K)$ para alguna base B y siendo λ_α el producto por α en F.

Se observa que este caso se presenta en los códigos skew Reed-Solomon.

Bases polinómica y normal

Para cada base B considerada tenemos un isomorfismo distinto.

Con la base $B = \{1, \alpha, \alpha^2, \ldots, \alpha^{\mu-1}\}$ obtenemos directamente $\varphi(\alpha)$ como la matriz compañera del polinomio mínimo de α.

Si $B = \{\alpha, \sigma(\alpha), \sigma^2(\alpha), \ldots, \sigma^{\mu-1}(\alpha)\}$ es una base, entonces $\varphi(x)$ es la matriz compañera de $x^\mu - 1$, que es una matriz de permutación.

Caso irreducible general

Un caso más general se da cuando $\mathcal{R} = R/Rp(x)$ con $p(x) = q(x^\mu) \in K[x^\mu]$ irreducible. En el caso anterior teníamos $q(y) = y - 1$. Tomamos β raíz de $q(y)$.

Los elementos de $M_\mu(K)$ se pueden ver dentro de $M_\mu(K(\beta))$, que es isomorfo a $\mathcal{R}$.

Volviendo a tomar $\varphi(\alpha) = M_B(\lambda_\alpha)$ y $\varphi(x) = M_B(\sigma)$ se tienen las condiciones

- $m(\varphi(\alpha)) = 0$ con m el polinomio mínimo de α en $K[x]$
- $\varphi(x)\varphi(\alpha) = \varphi(\sigma(\alpha))\varphi(x)$

Pero $p(\varphi(x)) \neq 0$ (de hecho φ vuelve a tener el núcleo $R(x^\mu - 1)$, que no es el que buscamos).

Cuando $p(x)$ tiene raíces

Si $b \in E = K(\beta)$ cumple que $p(b) = q(b^\mu) = 0$, entonces al tomar $\varphi(x) = bM_B(\sigma)$ se cumple la condición que falta manteniendo las otras, pues

$$p(bM_B(\sigma)) = q(b^\mu M_B(\sigma)^\mu) = q(b^\mu I_\mu) = q(b^\mu) = 0$$

Si $p(x)$ tiene raíces en E, se pueden encontrar algunas de ellas calculando las raíces μ-ésimas de β.

En algunos casos, β^μ también es raíz de $q(x)$, por lo que β es raíz de $q(x^\mu) = p(x)$ y no hace falta computar raíces de ningún polinomio.

Cuando $p(x)$ no tiene raíces

Si las raíces de $p(x)$ no están en $E = K(\beta)$, hay que buscar una imagen de x de otra forma. Definimos

$$S = \{A \in M_\mu(E) \,:\, A\,M_B(\lambda_\alpha) - M_B(\lambda_{\sigma(\alpha)})\,A = 0\}$$

S contiene a todos los elementos que, tomados como $\varphi(x)$, hacen que φ satisfaga las condiciones buscadas no relativas a su núcleo.

Proposición

S es un subespacio vectorial de $M_\mu(E)$ de dimensión μ con base

$$\{M_B(\lambda_{\alpha_1}\sigma),\, M_B(\lambda_{\alpha_2}\sigma),\, \ldots,\, M_B(\lambda_{\alpha_\mu}\sigma)\}$$

donde $\{\alpha_1, \ldots, \alpha_\mu\}$ es cualquier K-base de F.

Búsqueda en S

Si $A \in S$ satisface $A^{\mu} = b \cdot I_{\mu}$ con $b \in E$ cualquiera, entonces $p(A) = 0$ si y solo si $q(b) = 0$.

Conjetura

$A^{\mu} = -(-1)^{\mu} \, |A| \cdot I_{\mu} \quad \forall A \in S$

En particular, esta conjetura garantizaría que la potencia μ-ésima de todo elemento de S es una matriz escalar.

Búsqueda en S

Dado $A \in S$ no nulo, podemos explorar todos sus múltiplos a la vez. Como $A^\mu = a \cdot I_\mu$ para algún $a \in E$, si $b^\mu a$ es una raíz de $q(x)$, entonces

$$p(bA) = q(b^\mu A^\mu) = q(b^\mu a) = 0$$

y podemos tomar $\varphi(x) = bA$.

Se puede comprobar si existe b comprobando si, para cada r raíz de $q(x)$, r/a tiene alguna raíz μ-ésima en E; en tal caso, $b^\mu = r/a$ y por tanto $b^\mu a = r$.

Búsqueda en S

De esta forma, la búsqueda en S se reduce a la búsqueda en el espacio proyectivo

$$PG(\mu - 1,\, E) \cong \frac{S \setminus \{0\}}{\sim}$$

con $\sim$ la relación de equivalencia que identifica los elementos proporcionales.

Si los valores de A^{μ} se distribuyen uniformemente en $E^{\times}$, uno de cada $\mathrm{mcd}(\mu, |E| - 1) \leq \mu$ elementos de S nos permitirán encontrar una imagen de x con la que φ tiene el núcleo buscado.

Caso general

Cuando $p(x)$ es un producto de polinomios centrales, se puede descomponer $\mathcal{R}$ como suma directa de los $\mathcal{R}_i$, que dan lugar a los casos anteriores.

Para construir el isomorfismo inverso, en lugar de resolver un sistema, se puede resolver un sistema más pequeño en cada sumando y combinar los resultados usando los idempotentes centrales de $\mathcal{R}$.

Construcción de códigos skew RS

Recordemos que los códigos skew cíclicos se describen como ideales izquierda en $\mathcal{R} = R/R(x^\mu - 1)$.

Como $\mathcal{R} \cong M_\mu(K)$ y $M_\mu(K)$ descompone como la suma de ideales izquierda columna

$$M = \bigoplus_i M_\mu(K)E_i$$

con E_i la matriz con un 1 en la posición i, i, computando

$$g_i(x) = \varphi^{-1}(E_i)$$

tenemos unos ideales izquierda $\mathcal{R}g_i(x)$. Calculando el mcd de varios de ellos obtenemos generadores de ideales con más elementos.

Cambiando de base, es decir, tomando $g_i(x) = \varphi^{-1}(A^{-1}E_iA)$ con A una matriz regular, obtenemos otros códigos distintos.