Un panorama sobre códigos autocorrectores

Ricardo Podestá

CIEM (CONICET) - FaMAF (UNC)

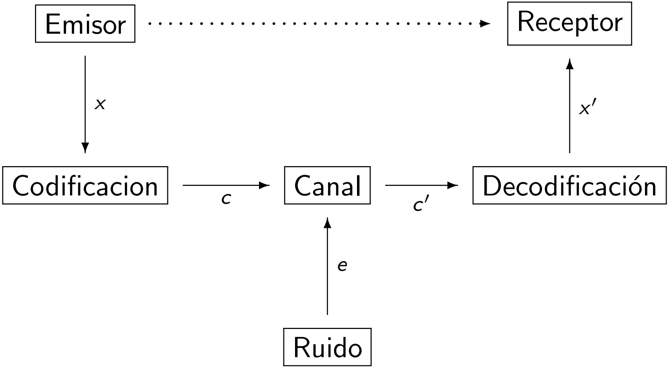
Primer Encuentro Argentino de Cuerpos Finitos y Temas Afines

19 y 20 de Octubre de 2017 / Córdoba, Argentina.

Resumen de la charla

Generalidades sobre códigos

Introducción: el proceso de transmisión



Introducción: detección y corrección de errores

Queremos codificar $\{N, S, E, O\}$.

- $C_1 = \{00, 01, 10, 11\}$
- $C_2 = \{000, 011, 101, 110\}$
- $C_3 = \{000000, 000111, 111000, 111111\}$

- C_1 no detecta ni corrige errores
- C_2 detecta 1-errores pero no corrige errores
- C_3 detecta 2-errores y corrige 1-errores

Secreto: usar redundancia!

Parámetros: alfabetos y códigos

Definición

- Un *alfabeto* es $\mathcal{A} = \{a_1, \ldots, a_q\}$.
- Una *palabra de longitud n* es $a = (a_{i_1}, a_{i_2}, \ldots, a_{i_n}) \in \mathcal{A}^n$.
- Un *código q-ario* sobre $\mathcal{A}$ es $C \subset \mathcal{A}^* = \bigcup_{n\in\mathbb{N}} \mathcal{A}^n$.
- Los elementos de C se llaman *palabras códigos*.
- $M = |C|$ se llama el *tamaño* del código.
- Si $C \subset \mathcal{A}^n$, C es un *código de bloque* de *longitud* n.
- Decimos que C es un (n, M)-*código*.

Es usual darle a $\mathcal{A}$ alguna estructura (anillo, grupo, cuerpo). Lo usual es $\mathcal{A} = \mathbb{F}_q$ cuerpo fintio.

Parámetros: distancia

Definición

- La *distancia de Hamming* $d : \mathcal{A}^n \times \mathcal{A}^n \to [0, n]$ es

$$d(x, y) = \#\{1 \leq i \leq n : x_i \neq y_i\}$$

- la *distancia mínima* de C es

$$d = d_C = \min_{\substack{x,y \in C \\ x \neq y}} d(x, y)$$

- Existen otras métricas (e.g. Lee en $\mathbb{Z}_n$).
- C es un (n, M, d)-*código* si tienen longitud n, tamaño M y distancia mínima d.

Parámetros: distancia

Proposición

Sea C un (n, M, d)-código.

- *C es s-detector si y sólo si $d = s + 1$.*
- *C es t-corrector si y sólo si $d = 2t + 1, 2t + 2$.*

Parámetros: peso

Definición

- el *peso* de $x \in \mathbb{F}_q^n$ es

$$w(x) = \#\{1 \leq i \leq n : x_i \neq 0\}$$

- o sea,

$$w(x) = d(x, 0)$$

- El *peso mínimo de C* es

$$w(C) = \min_{\substack{x \in C \\ x \neq 0}} w(x)$$

Códigos lineales

Sea $\mathcal{A} = \mathbb{F}_q$.

Definición

- Un código lineal sobre $\mathbb{F}_q$ de longitud n y dimensión k es un subespacio $C \subseteq \mathbb{F}_q^n$ con $\dim C = k$.
- Decimos que C es un $[n, k, d]$-código q-ario.

- Notar que $M = q^k$.
- Si C es un código lineal entonces $d(C) = w(C)$ pues

$$d(C) = \min_{x \neq y \in C} d(x, y) = \min_{x \neq y \in C} w(x - y) = \min_{0 \neq x \in C} w(x) = w(C)$$

Cotas básicas

Sea C un $[n,k,d]$-código q-ario (hay algunas versiones no-lineales)

- **Singleton:**
$$k \leq n - d + 1$$
El $=$ da *códigos MDS* (máximo d fijado k).
- **Griesmer:**
$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil$$
- **Hamming y Gilbert:**
$$\sum_{i=0}^{[\frac{d-1}{2}]} \binom{n}{i}(q-1)^i \leq q^{n-k} \leq \sum_{i=0}^{d-1} \binom{n}{i}(q-1)^i$$
El $=$ en Hamming da *códigos perfectos* (las bolas $B(c,t)$ de radio $t = [\frac{d-1}{2}]$ centradas en $c \in C$ empaquetan el espacio).

Construcciones

Modificaciones a un código

- extender / pinchar,
- aumentar / expurgar,
- restricción de coordenadas.

Operaciones entre códigos

- suma directa, suma de Plotkin,
- producto de Kronecker,
- otros: concatenación, pegado, intercalado.

Tipos de códigos: familias

Un *código* será un código de bloque lineal sobre $\mathbb{F}_q$ (clásico).
De estos nos interesan las siguientes familias

- **lineales** (Hamming, Golay, Reed-Muller, GRM).
  herramientas: álgebra lineal y combinatoria.
- **cíclicos** (RS, GRS, BCH, QR, duádicos).
  herramientas: teoría de Galois, algebra conmutativa, teoría de números.
  generalizaciones: nega-cíclicos, consta-cíclicos / transitivos, casi-cíclicos, casi-transitivos, / abelianos, group-codes.
- **alternantes** (Goppa)
- **geométricos** (racionales, elípticos, curvas famosas)
  herramientas: curvas algebraicas, cuerpos de funciones algebraicas, geometría algebraica

Tipos de códigos

Existen otras muchas nociones muy estudiadas también

- lineales vs no lineales (ISBN/EAN-13, Nordstrom-Robinson, Kerdock/Preparata, Goethals, Justesen, Hadamard),
- longitud fija vs longitud variable (Huffman),
- basados en grafos (Gallager, tornado, turbo, LDPC),
- clásicos vs cuánticos,
- clásicos vs convolucionales,
- algebraicos vs geométricos,
- otros alfabetos: grupos, anillos, módulos, etc.

Códigos lineales

Ejemplos triviales

Ejemplos

- Para q y n fijos, existen 2 códigos *triviales* sobre $\mathbb{F}_q$, $\mathbf{0}$ y $\mathbb{F}_q^n$, con parámetros $[n, 0, -]_q$ y $[n, n, 1]_q$.
- El *código de repetición q-ario* es

$$\mathcal{R}_q(n) = \{\mathbf{0}, \mathbf{1}, \mathbf{c_1}, \ldots, \mathbf{c_{q-2}}\} = \langle \mathbf{1} \rangle$$

donde $\mathbb{F}_q = \{0, 1, c_1, \ldots, c_{q-2}\}$ y $\mathbf{c} = cc \cdots c \in \mathbb{F}_q^n$, para $c \in \mathbb{F}_q$, tiene parámetros $[n, 1, n]_q$.
Por ej., $\mathcal{R}_2(3) = \{000, 111\}$ y $\mathcal{R}_3(5) = \{00000, 11111, 22222\}$.

Ejemplos triviales

Ejemplos

- El *código de peso par* es el código binario

$$\mathcal{E}_n = \{x \in \mathbb{F}_2^n : w(x) \equiv 0\,(2)\}$$

  $\mathcal{E}_n$ es lineal y luego $d_C = w_C = 2$. Además, $M = 2^{n-1}$ y por lo tanto $k = n - 1$. Así, $\mathcal{E}_n$ es un $[n, n-1, 2]$-código.

- El *código de paridad q-ario* (o de suma cero) es el código

$$\mathcal{P}_q(n) = \{x \in \mathbb{F}_q^n : \sum_{i=1}^{n} x_i = 0\}$$

  con parámetros $[n, n-1, 2]$.

- Notar que si $q = 2$, $\mathcal{P}_2(n) = \mathcal{E}_n$.

Matriz generadora

- Sea $\mathcal{C}$ un $[n,k]_q$-código.
- Una **matriz generadora** de $\mathcal{C}$ es una matriz $k \times n$ cuyas filas están formadas por los vectores de una base de C.
- G tiene rango k y genera el código pues

$$\mathcal{C} = \{uG : u \in \mathbb{F}_q^k\} = \mathbb{F}_q^k G$$

Matriz generadora: ejemplo

Ejemplo

- *El* **tetracode** *es el código ternario $\mathcal{T}$ generado por*

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$$

- *Luego,*

$$(x, y)G = (x, y, x+y, x+2y) \in \mathcal{T}, \qquad x, y \in \mathbb{F}_3$$

y

$$\mathcal{T} = \{000, 0112, 0221, 1011, 1120, 1202, 2022, 2101, 2210\}$$

- $\mathcal{T}$ *es un* $[4, 2, 3]$*-código.*

Código dual

- Consideremos el producto interno canónico en $\mathbb{F}_q^n$ dado por

$$x \cdot y = x_1 y_1 + \cdots + x_n y_n \qquad x, y \in \mathbb{F}_q^n$$

- Si $\mathcal{C}$ es un $[n, k]_q$-código, el **código dual** de $\mathcal{C}$ es el subespacio

$$\mathcal{C}^{\perp} = \{x \in \mathbb{F}_q^n \ : \ x \cdot c = 0 \quad \forall\, c \in \mathcal{C}\}$$

- C es **auto-ortogonal** si $\mathcal{C} \subset \mathcal{C}^{\perp}$ y **autodual** si $\mathcal{C} = \mathcal{C}^{\perp}$.

Código dual

Tenemos los siguientes resultados básicos sobre códigos duales.

Proposición

Sea $\mathcal{C}$ un $[n,k]_q$-código y G una matriz generadora de $\mathcal{C}$. Entonces,

- $\mathcal{C}^\perp = \{x \in \mathbb{F}_q^n : xG^\top = 0\} = \{x \in \mathbb{F}_q^n : Gx^\top = 0\}$.
- $\mathcal{C}^\perp$ *es un* $[n, n-k]_q$*-código.*
- $(\mathcal{C}^\perp)^\perp = \mathcal{C}$.

Matrices de paridad

- Una **matriz de paridad** de un $[n, k]_q$-código $\mathcal{C}$ es una matriz generadora del dual $\mathcal{C}^\perp$. La denotamos por H.
- Se cumple

$$\mathcal{C} = \{x \in \mathbb{F}_q^n : Hx^\top = 0\} = \{x \in \mathbb{F}_q^n : xH^\top = 0\}$$

- Se tiene

$$0 \longrightarrow \mathbb{F}_q^k \xrightarrow{R_G} \mathbb{F}_q^n \xrightarrow{R_{H^\top}} \mathbb{F}_q^{n-k} \longrightarrow 0,$$

donde G y H son matrices $k \times n$ y $n - k \times n$ de rango máximo, respectivamente. Esto permite generalizar la noción de códigos lineales en otros contextos.

El teorema de Delsarte

Teorema

Sea C *un código lineal en* $\mathbb{F}_{q^m}$. *Entonces*

$$(C_{|\mathbb{F}_q})^\perp = Tr(C^\perp)$$

Matrices de paridad y distancia

Teorema

Sea C un $[n, k, d]_q$-código y H una matriz de paridad de C. Entonces

$$d = \min_{r>0}\{H \text{ tiene } r \text{ columnas linealmente dependientes}\}$$

O sea, H tiene d columnas linealmente dependientes, pero cualquier conjunto de $d-1$ columnas son linealmente independientes.

La cota de Varshamov

Proposición (Gilbert-Varshamov)

Sea $n, k, d, q = p^r, r \in \mathbb{N}$ *con p primo. Si*

$$q^{n-k} > \sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i$$

entonces existe un $[n, k, d_{\mathcal{C}}]_q$*-código* $\mathcal{C}$ *con* $d_{\mathcal{C}} \geq d$.

Códigos de Hamming

- Consideremos la matriz

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \in \mathbb{F}_2^{3\times 7}$$

  cuyas columnas son las $2^3 - 1 = 7$ palabras no-nulas de $\mathbb{F}_2^3$
- H es la matriz de paridad de un $[7, 4, 3]$-código, llamado *código de Hamming binario* $\mathcal{H}_2(3)$.
- Del mismo modo, para cada r se tienen los códigos de Hamming binarios $\mathcal{H}_2(r)$ de longitud $n = 2^r - 1$.

Códigos de Hamming

Los códigos de Hamming q-arios $\mathcal{H}_q(r)$ tienen parámetros

$$n = \frac{q^r - 1}{q - 1}, \qquad k = n - r, \qquad d = 3$$

Ejemplo

El código $\mathcal{H}_3(3)$ tiene parámetros $[13, 10, 3]$ con matriz de paridad

$$H_{3,3} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}.$$

Ejemplo

El código $\mathcal{H}_5(3)$ tiene parámetros $[31, 28, 3]$ con matriz de paridad

$$H_{5,3} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 & 3 & 4 & 4 & 4 & 4 & 4 \\ 1 & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 \end{pmatrix}.$$

Espectro

- Sea C un código de longitud n. Para cada i,

$$A_i = \#\{c \in C : w(c) = i\}$$

- El **espectro** de C es

$$\mathrm{Spec}\,(C) = \{A_0, A_1, \ldots, A_n\}$$

- El **peso máximo** de $\mathcal{C}$ por

$$\mu_C = \max_{c \in C} w(c)$$

- Es claro que

$$A_0 = 1, \quad A_1 = A_2 = \cdots = A_{d-1} = 0, \quad A_{\mu+1} = \cdots = A_n = 0$$

- Notar que si C es un $[n, k, d]$-código entonces

$$A_0 + A_1 + \cdots + A_n = q^k$$

Espectro: Identidades de MacWilliams

El polinomio enumerador de pesos de un $[n,k]$-código C es

$$W_C(x) = \sum_{i=0}^{n} A_i x^i$$

Teorema (MacWilliams)

Si C es un código lineal sobre $\mathbb{F}_q$ entonces

$$W_{C^\perp}(x) = \frac{1}{|C|}\left(1+(q-1)x\right)^n W_C\left(\frac{1-x}{1+(q-1)x}\right)$$

Identidades de MacWilliams

Ejemplo

Si $C = \{000, 111\}$ *entonces* $A_0 = A_3 = 1$, $A_1 = A_2 = 0$. *Por lo tanto* $W_C(s) = 1 + s^3$. *Por la identidad de MacWilliams*

$$\begin{aligned} W_{C^\perp}(x) &= \tfrac{1}{2}(1+x)^3 W_C\left(\tfrac{1-x}{1+x}\right) \\ &= \tfrac{1}{2}(1+x)^3\left(1+\left(\tfrac{1-x}{1+x}\right)^3\right) \\ &= \tfrac{1}{2}\{(1+x)^3+(1-x)^3\} = 1+3x^2 \end{aligned}$$

Luego, $A_0^\perp = 1$, $A_1^\perp = A_3^\perp = 0$, $A_2^\perp = 3$ *y así*

$$C^\perp = \{000, 011, 010, 110\} = \mathcal{E}_3$$

El paper de [CCHKS]

- Kerdock y Preparata códigos no lineales.
- Sus enumeradores de peso satisfacen la identidad de MacWilliams.
- Son lineales sobre $\mathbb{Z}_4$ con la distancia de Lee.
- El mapa de Gray da una isometría entre $\mathbb{Z}_2^{2n}$ y $\mathbb{Z}_4^n$.

Códigos cíclicos: definición

- Un código lineal C es *cíclico* si es cerrado por la permutación cíclica, i.e.

$$c = (c_0, c_1, \ldots, c_{n-1}) \in C \Leftrightarrow s(c) = (c_{n-1}, c_0, \ldots, c_{n-2}) \in C$$

- Los códigos triviales 0, $\mathbb{F}_q^n$, $R_q(n)$, $E_q(n)$ son cíclicos.
- Consideremos la aplicación $\phi : \mathbb{F}_q^n \to \mathbb{F}_q[x]/(x^n - 1)$ dada por

$$(c_0, c_1, \ldots, c_{n-1}) \quad \mapsto \quad c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}$$

- Notar que C es cíclico $\Leftrightarrow \phi(C)$ es ideal en $\mathbb{F}_q[x]/(x^n - 1)$.

Códigos cíclicos: polinomio generador

Teorema

Sea C un código cíclico de longitud n sobre $\mathbb{F}_q$. Entonces,

- *Existe un único polinomio mónico $g(x)$ de grado mínimo r en C y $g(x) \mid x^n - 1$.*
- $C = \langle g(x) \rangle = \{r(x)g(x) : \operatorname{gr} r(x) < n - r\}$.
- $\{g(x), xg(x), \ldots, x^{n-r-1}g(x)\}$ *es una base de C y* $\dim C = k = n - r$.

Este $g(x)$ se dice el *polinomio generador* de C.

Códigos cíclicos: polinomio generador

Teorema

- *Si* $g(x) = x^r + g_{r-1}x^{r-1} + \cdots + g_1 x + g_0$*, entonces* $g_0 \neq 0$ *y* C *tiene matriz generadora*

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & \cdots & g_{r-1} & 1 & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & \cdots & g_{r-1} & 1 & 0 & \cdots & 0 \\ 0 & 0 & g_0 & g_1 & \cdots & \cdots & g_{r-1} & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & \cdots & \cdots & g_{r-1} & 1 \end{pmatrix}$$

Códigos cíclicos binarios de longitud 7

- salen de

$$\begin{aligned} x^7 - 1 &= \Phi_1(x)\Phi_7(x) = (x-1)(x^6 + \cdots + x + 1) \\ &= (x-1)(x^3+x+1)(x^3+x+1) = m_0(x)m_1(x)m_3(x) \end{aligned}$$

donde

$$C_0 = \{0\}, \qquad C_1 = \{1,2,4\}, \qquad C_3 = \{3,5,6\}$$

son los conjuntos ciclotómicos mod 7, y se tiene

$$\begin{aligned} m_0(x) &= (x-\alpha^0), \\ m_1(x) &= (x-\alpha^1)(x-\alpha^2)(x-\alpha^4), \\ m_3(x) &= (x-\alpha^3)(x-\alpha^5)(x-\alpha^6), \end{aligned}$$

donde α es un elemento primitivo de $\mathbb{F}_q^*$.

Códigos cíclicos: polinomio de control

- Sea $C = \langle\langle g(x) \rangle\rangle$ un código cíclico de $\mathbb{F}_q^n$.
- Luego, $x^n - 1 = g(x)h(x)$ para algún polinomio $h(x)$ de grado $n - \operatorname{gr} g(x)$.
- El polinomio $h(x)$ se llama *polinomio de control* de C.

Códigos cíclicos: polinomio de control

Teorema

- $C = \{p(x) \in \mathbb{F}_q[x]/(x^n - 1) : p(x)h(x) = 0\}$.
- *Si* $h(x) = h_{n-r}x^{n-r} + \cdots + h_1 x + h_0$, *entonces la matriz de paridad de* C *está dada por*

$$H = \begin{pmatrix} h_{n-r} & \cdots & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_{n-r} & \cdots & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & 0 & h_{n-r} & \cdots & \cdots & h_0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \cdots & \cdots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & h_{n-r} & \cdots & \cdots & h_0 \end{pmatrix} \in \mathbb{F}_q^{r\times n}$$

- $C^\perp$ *es un código cíclico de dimensión* r, *con polinomio generador*

$$g(x)^\perp = h_0^{-1}h(x)^\top = x^{n-r} + \frac{h_1}{h_0}x^{n-r+1} + \cdots + \frac{h_{n-r-1}}{h_0}x + \frac{h_{n-r}}{h_0}.$$

Ceros de un código cíclico

Teorema

Sea $g(x) = m_{i_1} m_{i_2}(x) \cdots m_{i_t}(x)$ *un producto de factores irreducibles de* $x^n - 1$ *sobre* $\mathbb{F}_q$*, y sean* $\{\alpha_1, \ldots, \alpha_r\}$ *las raíces de* $g(x)$ *en el cuerpo de descomposición de* $x^n - 1$ *sobre* $\mathbb{F}_q$*. Entonces*

$$C = \langle\langle g(x) \rangle\rangle = \{f(x) \in \mathbb{F}_q[x]/(x^n - 1) : f(\alpha_1) = 0, \ldots, f(\alpha_r) = 0\}$$

Más aún, basta tomar una raíz de cada factor irreducible de $g(x)$*. Esto es, si* β_j *es una raíz de* $m_{i_j}(x)$ *para* $1 \leq j \leq t \leq r$*, entonces*

$$C = \langle\langle g(x) \rangle\rangle = \{f(x) \in \mathbb{F}_q[x]/(x^n - 1) : f(\beta_1) = \cdots = f(\beta_t) = 0\}$$

donde β_j *es una raíz de* $m_{i_j}(x)$ *para* $1 \leq j \leq t \leq r$*.*

Ceros de un código cíclico

Observación

Si $\alpha_1, \ldots, \alpha_r$ es un conjunto de raíces de $x^n - 1$ entonces, el código

$$C = \{f(x) \in \mathbb{F}_q[x]/(x^n - 1) : f(\alpha_1) = \cdots = f(\alpha_r) = 0\}$$

tiene polinomio generador

$$g(x) = \mathrm{mcm}\{m_{\alpha_1}(x), m_{\alpha_2}(x), \ldots, m_{\alpha_r}(x)\}$$

Matrices de paridad

- Sean $\alpha_1, \ldots, \alpha_r$ raíces de $x^n - 1$ en alguna extensión $\mathbb{F}_{q^d}/\mathbb{F}_q$.
- Como $\mathbb{F}_{q^d} \simeq \mathbb{F}_q^d$ como $\mathbb{F}_q$-espacio vectorial, cada $\alpha_i^j \in \mathbb{F}_{q^d}$ tiene asociado un vector columna $[\alpha_i^j] \in \mathbb{F}_q^d$.
- Sea H la matriz $rd \times n$ en $\mathbb{F}_q$

$$H = \begin{pmatrix} [\alpha_1^0] & [\alpha_1^1] & \cdots & [\alpha_1^{n-1}] \\ [\alpha_2^0] & [\alpha_2^1] & \cdots & [\alpha_2^{n-1}] \\ \vdots & \vdots & \vdots & \vdots \\ [\alpha_r^0] & [\alpha_r^1] & \cdots & [\alpha_r^{n-1}] \end{pmatrix} \in M_{rd\times n}(\mathbb{F}_q)$$

- Quitando las posibles filas linealmente dependientes de H se obtiene una matriz de paridad H' para el código $C = \{f(x) \in \mathbb{F}_q[x]/(x^n - 1) : f(\alpha_1) = \cdots = f(\alpha_r) = 0\}$.

La cota BCH

Teorema

Sea ω una raíz primitiva n-ésima de la unidad en $\mathbb{F}_q$ y sea C un código cíclico cuyo polinomio generador tiene a las δ raíces

$$\omega^b, \omega^{b+1}, \ldots, \omega^{b+\delta-1}$$

con $b \in \mathbb{N}_0$ y los exponentes consecutivos módulo n. Entonces,

$$d_C \geq \delta + 1$$

Códigos BCH

Definición

- Sea ω una raíz primitiva n-ésima de la unidad en $\mathbb{F}_q$ y sea $g(x)$ el polinomio mónico sobre $\mathbb{F}_q$ de menor grado que tiene a las $\delta - 1$ raíces n-ésimas de la unidad

$$\omega^b, \omega^{b+1}, \ldots, \omega^{b+\delta-2}$$

entre sus ceros con $b \geq 0$, $\delta \geq 2$.

- O sea,

$$g(x) = \mathrm{mcm}\{m_b(x), m_{b+1}(x), \ldots, m_{b+\delta-2}(x)\}$$

- El código cíclico q-ario de longitud n con polinomio generador $g(x)$ se llama *código de BCH con distancia diseñada* δ y se denota por $\mathcal{B} = \mathcal{B}_q(n, \delta, \omega, b)$.

Códigos BCH

Proposición

$\mathcal{B}_q(n, \delta, \omega, b)$ es un $[n, k, d]$ código cíclico sobre $\mathbb{F}_q$ con

$$k \geq n - (\delta - 1)\, o_n(q) \qquad y \qquad d \geq \delta$$

Reed-Solomon

Definición

Un *código de Reed-Solomon q-ario* es un código BCH de longitud $n = q - 1$,

$$\mathcal{RS}_q(\delta, \omega, b) := \mathcal{B}_q(q-1, \delta, \omega, b)$$

- El polinomio minimal de ω^i es simplemente $m_{\omega^i}(x) = x - \omega^i$.
- $\mathcal{RS}_q(\delta, \omega, b)$ tiene polinomio generador

$$g(x) = (x - \omega^b)(x - \omega^{b+1}) \cdots (x - \omega^{b+\delta-2})$$

Reed-Solomon

- Por la cota BCH, $d \geq \delta = n - k + 1$, pero, por la cota de Singleton, se tiene que $d \leq n - k + 1$. Entonces,

$$d = \delta = n - k + 1$$

Proposición

$\mathcal{RS}_q(\delta, \omega, b)$ es un MDS-código con parámetros $[q-1, q-\delta, \delta]$.

Códigos de evaluación: RS

- Sea $n = q - 1$ y β elemento primitivo de $\mathbb{F}_q$.
- Para $1 \leq k \leq n$, consideremos el espacio vectorial de dim k

$$\mathcal{L}_k = \{f \in \mathbb{F}_q[x] : \deg f < k\}$$

y el mapa de evaluación $ev_k : \mathcal{L}_k \to \mathbb{F}_q^n$

$$ev_k(f) = (f(\beta), f(\beta^2), \ldots, f(\beta^n))$$

- Es claro que ev_k es 1-1 y por lo tanto

$$\mathcal{RS}_k := ev_k(\mathcal{L}_k) = \{(f(\beta), f(\beta^2), \ldots, f(\beta^n)) : f \in \mathcal{L}_k\}$$

es un $[n, k]$-código.

Códigos de evaluación: RS

- $\mathcal{RS}_k$ es cíclico, pues
$$(f(\beta^n), f(\beta), f(\beta^2), \dots, f(\beta^{n-1})) = (h(\beta), f(\beta^2), \dots, h(\beta^n))$$
tomando $h(x) = f(\beta x)$.
- Se puede ver que $\mathcal{RS}_k$ tiene $d \geq n - k + 1$ y por Singleton, es un código MDS.
- Se puede ver que $\mathcal{RS}_k = \mathcal{RS}_q(n - k + 1, \omega, 1)$ con ceros $\beta, \beta^2, \dots, \beta^{\delta-1} = \beta^{n-k}$.

Códigos alternantes

- Generalizan a los BCH (H más general).
- Sea $h = (h_1, \ldots, h_n) \in (\mathbb{F}_{q^m})^n$, $\alpha = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{F}_{q^m})^n$ con los h_i's no nulos y los α_i's todos distintos. Sea $H = (h_j \alpha_j^i)_{ij} \in (\mathbb{F}_{q^m})^{r \times n}$ y

$$H' = \begin{pmatrix} [h_1] & [h_2] & \cdots & [h_n] \\ [h_1\alpha_1] & [h_2\alpha_2] & \cdots & [h_n\alpha_n] \\ [h_1\alpha_1^2] & [h_2\alpha_2^2] & \cdots & [h_n\alpha_n^2] \\ \vdots & \vdots & & \vdots \\ [h_1\alpha_1^{r-1}] & [h_2\alpha_2^{r-1}] & \cdots & [h_n\alpha_n^{r-1}] \end{pmatrix} \in (\mathbb{F}_q)^{rm \times n}$$

Alternantes

- Supongamos que $r < n$. El *código alternante* $\mathcal{A} = \mathcal{A}(\alpha, h)$ es el $[n, k, d]$-código sobre $\mathbb{F}_q$ con matriz de paridad H', uego de quitar las filas linealmente dependientes.
- Es decir,
$$\mathcal{A}(\alpha, h) = \{x \in \mathbb{F}_q^n : H'x^\perp = 0\}$$
- Tiene parámetros
$$n, \qquad n - mr \leq k \leq n - r, \qquad d \geq r + 1.$$

Goppa

- Un clase importante de alternantes es cuando el vector h está dado por evaluación de un polinomio $g(x)$.
- Sea $g(x) \in \mathbb{F}_{q^m}[x]$ y sea $S_m = \mathbb{F}_{q^m}[x]/(g(x))$.
- Notar que si $g(\alpha) \neq 0$ entonces$x - \alpha$ tienen inverso en S_m.

Goppa

- En efecto, $g(x) = q(x)(x-\alpha) + g(\alpha)$
- luego $x - \alpha \mid g(x) - g(\alpha)$ y $q(x)(x-\alpha) \equiv -g(\alpha) \mod g(x)$.
- Así, $-g(\alpha)^{-1}q(x)(x-\alpha) \equiv 1 \mod g(x)$ y
- por lo tanto

$$\frac{1}{x-\alpha} = -g(\alpha)^{-1}q(x) = -g(\alpha)^{-1}\left(\frac{g(x)-g(\alpha)}{x-\alpha}\right)$$

en S_m.

Goppa

Definición

Sea $g(x) \in \mathbb{F}_{q^m}[x]$ y $L = \{\alpha_1, \ldots, \alpha_n\} \subset \mathbb{F}_{q^m}$ tal que $g(\alpha_i) \neq 0$ para cada $1 \leq i \leq n$ and $n > \deg g(x) = t$.
El *código de Goppa* q-ario $\Gamma(L, g)$ está defindo por

$$\Gamma(L, g) = \left\{a = (a_1, a_2, \ldots, a_n) \in (\mathbb{F}_q)^n \mid R_a(x) \equiv 0 \mod g(x)\right\}$$

donde

$$R_a(x) = \sum_{i=1}^{n} \frac{a_i}{x - \alpha_i}$$

El polinomio $g(x)$ se llama el *polinomio de Goppa* de $\Gamma(L, g)$.

Goppa

Observación

- El código de Goppa $\Gamma(L,g)$ es un código alternante $\mathcal{A}(\alpha,h)$ con $\alpha=(\alpha_1,\ldots,\alpha_n)$ y $h=(g(\alpha_1)^{-1},\ldots,g(\alpha_n)^{-1})$.
- $\Gamma(L,g)$ tiene parámetros

$$n=|L|, \qquad n-mt\leq k\leq n-t, \qquad d\geq t+1$$

con $t=\deg g(x)$.

Goppa

Observación

Los códigos BCH con $b = 1$ son casos particulares de códigos de Goppa. En efecto,

$$\mathcal{B}_q(n, \delta, \omega) = \Gamma(L, g)$$

con

$$L = \{1, \omega, \ldots, \omega^{n-1}\} \qquad \text{and} \qquad g(x) = x^{\delta-1}$$

Códigos geométricos

Acá empieza la historia...

- Generalizando la construcción de RS como código de evaluación y la de Goppa se llega a los códigos geométricos
- Son códigos de evalución en donde se evaluan funciones racionales de curvas proyectivas en puntos racionales.
- Si F es un cuerpo de funciones racionales sobre $\mathbb{F}_q$, D, G divisores disjuntos con $D = P_1 + \cdots + P_n$ donde P_l son lugares racionales entonces

$$C = C(D, G) = \{(x(P_1), \ldots, x(P_n)) : x \in \mathcal{L}(G)\}$$

  donde $\mathcal{L}(G)$ es el espacio de Riemann-Roch asociado a G.
- Todo código lineal es geométrico ([PSW]).

Problemas abiertos

- ¿Son los códigos cíclicos asintóticamente buenos?
- ¿Cómo construir AG-códigos cíclicos?

gracias!