

Sobre automorfismos y AG-códigos cíclicos

Gustavo Andrés Cabaña

Instituto de Matemática Aplicada del Litoral (CONICET - UNL)
Facultad de Ciencias Económicas (UNL)

Encuentro Argentino de Cuerpos Finitos

1 Cuerpos de funciones

2 Teoría de Galois

3 AG-Códigos

4 AG-Códigos cíclicos

Cuerpos de funciones

- **Cuerpo de funciones F/K :** Extensión de cuerpos $F \supset K$ tal que F es una extensión algebraica finita de $K(x)$ para algún $x \in F$ que es trascendente sobre K .

$$\begin{array}{c} F \\ | \\ K(x) \\ | \\ K \end{array} < \infty$$

- **Anillo de valuaciones de F/K :** Es un anillo $\mathcal{O} \subset F$ tal que:
 - i) $K \subsetneq \mathcal{O} \subsetneq F$.
 - ii) Para todo $z \in F$ sucede que $z \in \mathcal{O}$ o $z^{-1} \in \mathcal{O}$.

Cuerpos de funciones

- **Proposición:** Sea $\mathcal{O}$ un anillo de valuaciones de F/K , entonces:
 - a) $\mathcal{O}$ es un anillo local, es decir, tiene un único ideal maximal $P = \mathcal{O} \setminus \mathcal{O}^*$.
 - b) Si $0 \neq z \in F$, entonces: $z \in P \Leftrightarrow z^{-1} \notin \mathcal{O}$.
- **Proposición:** Sean $\mathcal{O}$ un anillo de valuaciones de F/K y P su ideal maximal, entonces:
 - a) P es un ideal principal.
 - b) Si $P = t\mathcal{O}$, cada $0 \neq z \in F$ tiene una representación única de la forma $z = t^n u$, con $n \in \mathbb{Z}$ y $u \in \mathcal{O}^*$.
- Si $\mathcal{O}$ es un anillo de valuaciones de F/K con ideal maximal P ,

$$\mathcal{O} = \{z \in F : z^{-1} \notin P\}.$$

$\mathcal{O}_P = \mathcal{O}$ se llama anillo de valuaciones asociado a P .

Cuerpos de funciones

- **Lugar de F/K :** Un lugar P de F/K es el único ideal maximal de un anillo de valuaciones $\mathcal{O}$ de F/K . Todo $t \in P$ tal que $P = t\mathcal{O}$ se llama elemento primo para P . Se denota con $\mathbb{P}(F)$ al conjunto de todos los lugares de F/K .
- **Valuación asociada a $P = t\mathcal{O}$:** $\nu_P : F \rightarrow \mathbb{Z} \cup \{\infty\}$ dada por $\nu_P(t^n u) = n$, si $z = t^n u \neq 0$, y $\nu_P(0) = \infty$.
- **Cuerpo de clases residuales de P :** $F_P = \mathcal{O}_P/P$. La función de clases residuales respecto a P se denota por $x \mapsto x(P)$.
- **Grado de un lugar P :** $\deg P = [F_P : K]$. Si $\deg P = 1$, $F_P \cong K$ y P se llama lugar racional.

Cuerpos de funciones

- F/K , F'/K' cuerpos de funciones tales que $K \subset K'$, $F \subset F'$ y K'/K , F'/F son algebraicas. Sean $P \in \mathbb{P}(F)$ y $Q \in \mathbb{P}(F')$. Se dice que Q divide a P o que Q está arriba de P si $P \subset Q$, denotado por $Q|P$.
- **Índice de ramificación:** $e(Q|P) = e$ el único entero positivo tal que $\nu_Q(x) = e\nu_P(x)$.
- **Grado de inercia:** $f(Q|P) = [F'_Q : F_P]$.
- Si $R|Q$ y $Q|P$, entonces $e(R|P) = e(R|Q)e(Q|P)$ y $f(R|P) = f(R|Q)f(Q|P)$.

Cuerpos de funciones

- **Lema:** Sean F/K un cuerpo de funciones, H, H' extensiones de F y $\sigma : H \rightarrow H'$ un K -automorfismo. Si $F' = \sigma(F)$, entonces:
 - a) Si $Q \in \mathbb{P}(H)$, entonces $\sigma(Q) = \{\sigma(x) : x \in Q\} \in \mathbb{P}(H')$ y $\sigma(\mathcal{O}_Q) = \mathcal{O}_{\sigma(Q)}$.
 - b) Si $0 \neq z \in H'$, entonces $\nu_{\sigma(Q)}(z) = \nu_Q(\sigma^{-1}(z))$.
 - c) Si $Q \in \mathbb{P}(H)$ y $P \in \mathbb{P}(F)$ tales que $Q|P$, entonces $\sigma(Q)|\sigma(P)$ y además $e(\sigma(Q)|\sigma(P)) = e(Q|P)$ y $f(\sigma(Q)|\sigma(P)) = f(Q|P)$.
- **Igualdad fundamental:** Si F'/F es una extensión finita de cuerpos de funciones y $P \in \mathbb{P}(F)$, entonces
$$\sum_{Q|P} e(Q|P) f(Q|P) = [F' : F].$$
- Si F'/F es una extensión de Galois finita, $e(Q|P)$ y $f(Q|P)$ son constantes para todo Q arriba de un lugar fijo P .

Cuerpos de funciones

- Divisores de F/K : $D = \sum_{P \in \mathbb{P}(F)} n_P P$ con una cantidad finita de $n_P \in \mathbb{Z}$ no nulos. Forman un grupo denotado $\text{Div}F$.
- Soporte de D : $\text{sop}D = \{P : n_P \neq 0\}$.
- Para $Q \in \mathbb{P}(F)$, $\nu_Q(D) = n_Q$.
- Orden en $\text{Div}F$: $D_1 \leq D_2$ si y sólo si $\nu_P(D_1) \leq \nu_P(D_2) \forall P \in \mathbb{P}(F)$.
- Divisor efectivo: D es efectivo si $D \geq 0$.
- Grado de un divisor: $\deg D = \sum \nu_P(D) \deg P$.

Cuerpos de funciones

- **Ceros y polos:** $P \in \mathbb{P}(F)$, $z \in F$. P es un cero de z de orden m si $\nu_P(z) = m > 0$. P es un polo de z de orden m si $\nu_P(z) = -m < 0$.
- **Teorema:** Si $z \in F$ es trascendente sobre K , entonces z tiene al menos un cero y un polo. Más aún, z tiene una cantidad finita de ceros y polos.
- **Divisor de ceros, de polos, y principal:** Sean $0 \neq z \in F$, $Z = \{P : \nu_P(z) > 0\}$ y $N = \{P : \nu_P(z) < 0\}$, se definen

$$(z)_0 = \sum_{P \in Z} \nu_P(z) P;$$

$$(z)_\infty = \sum_{P \in N} (-\nu_P(z)) P;$$

$$(z) = (z)_0 - (z)_\infty.$$

Cuerpos de funciones

- **Espacio de Riemann-Roch asociado a un divisor A :** Si $A \in \text{Div} F$, se define $\mathcal{L}(A) = \{z \in F : (z) \geq -A\} \cup \{0\}$, que es un espacio vectorial de dimensión finita sobre K , denotada por $\ell(A)$.
- **Género de un cuerpo de funciones:** El género de F/K es el entero no negativo dado por $g = \text{máx}\{\deg A - \ell(A) + 1 : A \in \text{Div} F\}$.
- **Teorema de Riemann-Roch:** Si $\deg A > 2g - 2$, entonces $\ell(A) = \deg A + 1 - g$.

Teoría de Galois

- **Cuerpo de descomposición:** Una extensión de cuerpos F/E se dice un cuerpo de descomposición para $p(x) \in E[x]$ si F contiene a todas las raíces de $p(x)$ y es el menor cuerpo que las incluye.
- **Polinomio separable:** Si F es un cuerpo de descomposición de $p(x) \in E[x]$, podemos escribir $p(x) = \prod (x - \alpha_i)^{n_i}$ con $\alpha_i \in F$. Si $n_i = 1$ para todo i , se dice que $p(x)$ es separable.

Teoría de Galois

- Una extensión finita de cuerpos F/E es de Galois si y sólo si existe un polinomio separable $p(x) \in E[x]$ tal que F es un cuerpo de descomposición para $p(x)$.
- Grupo de Galois: Si F/E es una extensión de Galois, su grupo de Galois es $\text{Gal}(F/E) = \text{Aut}(F/E)$.
- Una extensión de Galois se dice abeliana (cíclica) si su grupo de Galois lo es.
- Teorema: Si $F_1 \subset F_2 \subset F_3$ es una sucesión de cuerpos y F_3/F_1 es una extensión de Galois abeliana(cíclica), entonces F_3/F_2 y F_2/F_1 son extensiones de Galois abelianas(cíclicas).

Definición

Un $[n, k, d]$ -código sobre $\mathbb{F}_q$ es un subespacio vectorial $\mathcal{C}$ de $\mathbb{F}_q^n$ de dimensión k y distancia mínima $d = \min\{d(x, y) : x, y \in \mathcal{C}, x \neq y\}$.

- $F/\mathbb{F}_q$ cuerpo de funciones algebraicas sobre un cuerpo finito
- $P_1, \dots, P_n$ lugares racionales distintos; $D = P_1 + \dots + P_n$
- $G \in \text{Div} F$ tal que $\text{sop} G \cap \text{sop} D = \emptyset$
- **AG-Códigos:** El código algebraico geométrico asociado a los divisores D y G se define como el subespacio vectorial de $\mathbb{F}_q^n$ dado por

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

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

- **Teorema:** $\mathcal{C}$ es un $[n, k, d]$ código con parámetros

$k = \ell(G) - \ell(G - D)$ y $d \geq n - \deg G$.

- **Corolario:**

a) Si $\deg G < n$, entonces $k = \ell(G) \geq \deg G + 1 - g$ y $d \geq n - \deg G$.
Luego, $k + d \geq n + 1 - g$.

b) Si $2g - 2 < \deg G < n$, entonces $k = \ell(G) = \deg G + 1 - g$.

- **Distancia mínima relativa y Tasa de transmisión:** Dado un $[n, k, d]$ código $\mathcal{C}$, se definen $\delta = d/n$ y $R = k/n$.
- **Familia de códigos asintóticamente buena:** Sea $\{\mathcal{C}_i\}_{i \in \mathbb{N}}$ un familia de códigos con longitudes crecientes, cada uno de ellos con parámetros relativos δ_i y R_i . Se dice que $\{\mathcal{C}_i\}$ es asintóticamente buena si existen $\delta, R > 0$ tales que $\liminf_{i \rightarrow \infty} \delta_i \geq \delta$ y $\liminf_{i \rightarrow \infty} R_i \geq R$.
- Es de interés estudiar ciertas familias de códigos y probar si son, o no, asintóticamente buenas.

AG-Códigos cíclicos

Un AG-código $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(D, G) = \{(x(P_1), \dots, x(P_n)) : x \in \mathcal{L}(G)\}$ es cíclico si y sólo si

$$(x(P_n), x(P_1), \dots, x(P_{n-1})) \in \mathcal{C} \ \forall \ (x(P_1), \dots, x(P_{n-1}), x(P_n)) \in \mathcal{C}$$

Luego, $(x(P_n), x(P_1), \dots, x(P_{n-1})) \in \mathcal{C}$ si y sólo si existe $z \in \mathcal{L}(G)$ tal que $(x(P_n), x(P_1), \dots, x(P_{n-1})) = (z(P_1), z(P_2), \dots, z(P_n))$

Debemos resolver el siguiente sistema:

$$(P) \quad \begin{cases} z(P_1) &= x(P_n) \\ z(P_2) &= x(P_1) \\ &\vdots \\ z(P_n) &= x(P_{n-1}) \end{cases}$$

AG-Códigos cíclicos

Supongamos que existe un automorfismo $\sigma \in \text{Aut}(F)$ tal que $\sigma(P_i) = P_{i-1} \pmod n$ y $\sigma(G) = G$, entonces (P) se satisface tomando $z = \sigma^{-1}(x)$. En efecto, se tiene que

$$z(P_i) = (\sigma^{-1}(x))(P_i) = x(\sigma(P_i)) = x(P_{i-1} \pmod n).$$

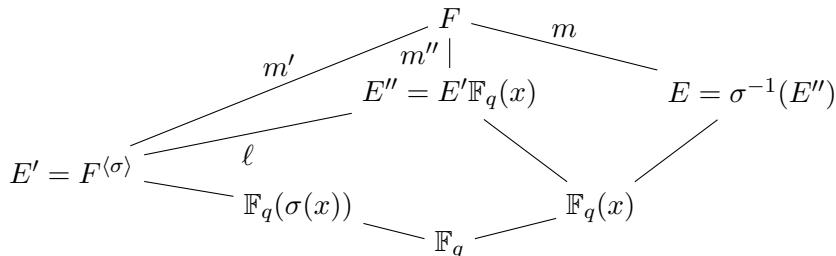
Proposición (CPT)

$$\left. \begin{array}{l} F/\mathbb{F}_q \text{ cpo. de funciones} \\ P_1, \dots, P_n \in \mathbb{P}(F) \\ P_i \neq P_j \ \forall i \neq j \\ \sigma \in \text{Aut}(F/\mathbb{F}_q(x)) \\ \sigma(P_i) = P_{i-1} \pmod n \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} \exists \mathbb{F}_q(x) \subset E \subset F \text{ y } P \in \mathbb{P}(E) \\ F/E \text{ es Galois cíclica} \\ n|m = [F : E] \\ P \text{ se descompone en } P_1, \dots, P_n \\ e(P_i|P)f(P_i|P) = m/n \end{array} \right.$$

AG-Códigos cíclicos

Proposición

$$\left. \begin{array}{l} F/\mathbb{F}_q \text{ cpo. de funciones} \\ P_1, \dots, P_n \in \mathbb{P}(F) \\ P_i \neq P_j \ \forall i \neq j \\ \sigma \in \text{Aut}(F/\mathbb{F}_q) \\ \sigma(P_i) = P_{i-1} \text{ mód } n \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} \exists \mathbb{F}_q(x) \subset E \subset F ; S \in \mathbb{P}(\mathbb{F}_q(x)) \\ \text{y } Q_1, \dots, Q_k \in \mathbb{P}(E) \\ F/E \text{ es Galois cíclica} \\ S \text{ se descompone en } P_1, \dots, P_n \\ P_i | Q_j \text{ para } n/k \text{ índices } i \end{array} \right.$$



Gracias!!!

