

Funciones numéricas de ideales graduados

Yuriko Pitones

Centro de Investigación en Matemáticas, CIMAT-México

Seminario GASIULL
Universidad de la Laguna
Abril 2021

Contenido

- Notación y definiciones
 - Función de Hilbert
 - Multiplicidad
- Función de distancia mínima
 - Mínima distancia de códigos Reed-Muller
 - Pesos generalizados
- Cotas
 - Función Huella

Contenido

- Notación y definiciones
 - Función de Hilbert
 - Multiplicidad
- Función de distancia mínima
 - Mínima distancia de códigos Reed-Muller
 - Pesos generalizados
- Cotas
 - Función Huella

Contenido

- Notación y definiciones
 - Función de Hilbert
 - Multiplicidad
- Función de distancia mínima
 - Mínima distancia de códigos Reed-Muller
 - Pesos generalizados
- Cotas
 - Función Huella

- $R = K[x_1, \dots, x_n] = \bigoplus_{d=0}^{\infty} R_d = R_0 \oplus R_1 \oplus R_2 \oplus \dots$.
- $I \neq (0)$ un ideal graduado de R .
- $R/I = \{\bar{f} = f + I \mid f \in R\}$

- $R = K[x_1, \dots, x_n] = \bigoplus_{d=0}^{\infty} R_d = R_0 \oplus R_1 \oplus R_2 \oplus \dots$.
- $I \neq (0)$ un ideal graduado de R .
- $R/I = \{\bar{f} = f + I \mid f \in R\}$

Función de Hilbert de R/I , $H_I : \mathbb{N} \rightarrow \mathbb{N}$.

$$H_I(d) := \dim_K R_d / I_d.$$
$$I_d = R_d \cap I$$

- $R = K[x_1, \dots, x_n] = \bigoplus_{d=0}^{\infty} R_d = R_0 \oplus R_1 \oplus R_2 \oplus \dots$.
- $I \neq (0)$ un ideal graduado de R .
- $R/I = \{\bar{f} = f + I \mid f \in R\}$

Función de Hilbert de R/I , $H_I : \mathbb{N} \rightarrow \mathbb{N}$.

$$H_I(d) := \dim_{\mathbb{K}} R_d / I_d.$$

$$I_d = R_d \cap I$$

Hilbert Series of S/I

$$\text{Hilb}_{S/I}(t) = \sum_{i \geq 0} \dim_{\mathbb{K}}(S_i / I_i) t^i.$$

Teorema de
Hilbert-Serre

$$\text{Hilb}_{R/I}(t) = \frac{h(t)}{(1-t)^{k-1}}$$

Polinomio de Euler

Teorema de
Hilbert-Serre

$$\text{Hilb}_{R/I}(t) = \frac{h(t)}{(1-t)^{k-1}}$$

Polinomio de Euler

Definición

El grado o multiplicidad: R/I

$$e(R/I) = h(1)$$

Ejemplo (fácil)

- $S = K[x, y, z]/(x^2, xy^2, y^3)$

Ejemplo (fácil)

- $S = K[x, y, z]/(x^2, xy^2, y^3)$
base de S_0 :

Ejemplo (fácil)

- $S = K[x, y, z]/(x^2, xy^2, y^3)$
base de S_0 : $\{1\}$

Ejemplo (fácil)

- $S = K[x, y, z]/(x^2, xy^2, y^3)$
base de S_0 : $\{1\}$
base de S_1 :

Ejemplo (fácil)

- $S = K[x, y, z]/(x^2, xy^2, y^3)$
base de S_0 : $\{1\}$
base de S_1 : $\{x, y, z\}$

Ejemplo (fácil)

- $S = K[x, y, z]/(x^2, xy^2, y^3)$
 - base de S_0 : $\{1\}$
 - base de S_1 : $\{x, y, z\}$
 - base de S_2 :

Ejemplo (fácil)

- $S = K[x, y, z]/(x^2, xy^2, y^3)$

base de S_0 : $\{1\}$

base de S_1 : $\{x, y, z\}$

base de S_2 : $\{xy, xz, y^2, yz, z^2\}$

Ejemplo (fácil)

- $S = K[x, y, z]/(x^2, xy^2, y^3)$

base de S_0 : $\{1\}$

base de S_1 : $\{x, y, z\}$

base de S_2 : $\{xy, xz, y^2, yz, z^2\}$

base de S_3 : $\{xyz, xz^2, yz^2, y^2z, z^3\}$

base de S_4 : $\{xyz^2, xz^3, yz^3, y^2z^2, z^4\}$

base de S_5 : $\{xyz^3, xz^4, yz^4, y^2z^3, z^5\}$

Ejemplo (fácil)

- $S = K[x, y, z]/(x^2, xy^2, y^3)$

base de S_0 :

$\{1\}$

base de S_1 :

$\{x, y, z\}$

base de S_2 :

$\{xy, xz, y^2, yz, z^2\}$

base de S_3 :

$\{xyz, xz^2, yz^2, y^2z, z^3\}$

base de S_4 :

$\{xyz^2, xz^3, yz^3, y^2z^2, z^4\}$

base de S_5 :

$\{xyz^3, xz^4, yz^4, y^2z^3, z^5\}$

\vdots

\vdots

base de S_i :

$\{xyz^{i-2}, xz^{i-1}, yz^{i-1}, y^2z^{i-2}, z^i\}$ para $i \geq 3$

Ejemplo (fácil)

- $S = K[x, y, z]/(x^2, xy^2, y^3)$

base de S_0 :

$$\{1\}$$

base de S_1 :

$$\{x, y, z\}$$

base de S_2 :

$$\{xy, xz, y^2, yz, z^2\}$$

base de S_3 :

$$\{xyz, xz^2, yz^2, y^2z, z^3\}$$

base de S_4 :

$$\{xyz^2, xz^3, yz^3, y^2z^2, z^4\}$$

base de S_5 :

$$\{xyz^3, xz^4, yz^4, y^2z^3, z^5\}$$

\vdots

\vdots

base de S_i : $\{xyz^{i-2}, xz^{i-1}, yz^{i-1}, y^2z^{i-2}, z^i\}$ para $i \geq 3$

- Serie de Hilbert de S

$$\text{Hilb}_S(t) = 1 + 3t + 5t^2 + 5t^3 + 5t^4 + 5t^5 + \dots = \frac{1+2t+2t^2}{1-t}$$

Ejemplo (fácil)

- $S = K[x, y, z]/(x^2, xy^2, y^3)$

base de S_0 :

$$\{1\}$$

base de S_1 :

$$\{x, y, z\}$$

base de S_2 :

$$\{xy, xz, y^2, yz, z^2\}$$

base de S_3 :

$$\{xyz, xz^2, yz^2, y^2z, z^3\}$$

base de S_4 :

$$\{xyz^2, xz^3, yz^3, y^2z^2, z^4\}$$

base de S_5 :

$$\{xyz^3, xz^4, yz^4, y^2z^3, z^5\}$$

\vdots

\vdots

base de S_i : $\{xyz^{i-2}, xz^{i-1}, yz^{i-1}, y^2z^{i-2}, z^i\}$ para $i \geq 3$

- Serie de Hilbert de S

$$\text{Hilb}_S(t) = 1 + 3t + 5t^2 + 5t^3 + 5t^4 + 5t^5 + \dots = \frac{1+2t+2t^2}{1-t}$$

- Multiplicidad de S

$$e(S) = 1 + 2 + 2 = 5$$

Remarks:

- $I \subset R$, $I = q_1 \cap \dots \cap q_m$ (descomposición primaria irredundante)

$$e(R/I) = \sum_{ht(I)=ht(q_i)} e(R/q_i).$$

- I es un ideal radical no-mezclado, $f \in R$ un polinomio homogéneo tal que $(I : f) \neq I$ y \mathcal{A} es el conjunto de todos los primos asociados de R/I que contienen a f , entonces $ht(I) = ht(I, f)$

$$e(R/(I, f)) = \sum_{p \in \mathcal{A}} e(R/p).$$

$$\mathcal{F}_t = \{f \in R_t \mid f \notin I, (I : f) \neq I\}.$$

$$\mathcal{F}_t = \{f \in R_t \mid f \notin I, (I:f) \neq I\}.$$

$(I:f) \neq I$ es equivalente a $f \in \mathfrak{p}$ para algún $\mathfrak{p} \in \text{Ass}(R/I)$

$\text{Ass}(R/I)$ es el conjunto de primos asociados de R/I .

La δ -función de I , es la función $\delta_I: \mathbb{N}_+ \rightarrow \mathbb{Z}$ dado por

$$\delta_I(t) = \begin{cases} e(R/I) - \text{máx}\{e(R/(I,f)) \mid f \in \mathcal{F}_t\} & \text{si } \mathcal{F}_t \neq \emptyset, \\ e(R/I) & \text{si } \mathcal{F}_t = \emptyset. \end{cases}$$

Theorem 1 (Núñez-Betancourt, Pitones, Villarreal (2020))

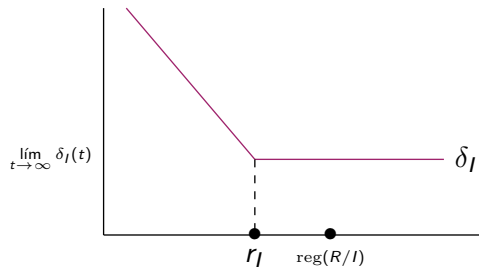
Supongamos que I es un ideal radical. Entonces, $\delta_I(d)$ es una función decreciente.

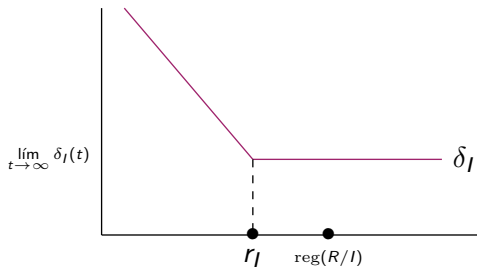
$$\delta_I(1) > \delta_I(2) > \cdots > \delta_I(r_I) = \delta_I(d) \text{ para } d \geq r_I.$$

Definition 2

Sea I un ideal radical. El índice de regularidad de I , denotado por r_I , es definido por

$$r_I = \min\{s \in \mathbb{N} \mid \delta_I(s) = \lim_{t \rightarrow \infty} \delta_I(t)\}.$$





r_I es el punto de estabilización de la δ -función, en general, r_I es difícil de calcular. Esta relacionado con la multiplicidad de Castelnuovo–Mumford.

Sea $K = \mathbb{F}_q$ un campo finito. Un *código lineal* \mathcal{C} es un subespacio de K^m , para algún m .

Parámetros básicos

- Longitud: m .
- Dimensión: $\dim_K \mathcal{C}$.
- Distancia mínima: $\delta(\mathcal{C}) := \min\{\|v\| : 0 \neq v \in \mathcal{C}\}$.

$\|v\|$: # de entradas no cero de v (peso de Hamming).

- $\mathbb{Y} = \{P_1, \dots, P_m\}$

- $\mathbb{Y} = \{P_1, \dots, P_m\}$

- $\mathbb{Y} = \{P_1, \dots, P_m\}$
- Definimos una K -aplicación lineal:

$$\begin{aligned} \text{ev}_d : R_d &\longrightarrow K^{|\mathbb{Y}|} \\ f &\mapsto (f(P_1), \dots, f(P_m)) \end{aligned}$$

- $Y = \{P_1, \dots, P_m\}$
- Definimos una K -aplicación lineal:

$$\begin{aligned} ev_d : R_d &\longrightarrow K^{|Y|} \\ f &\mapsto (f(P_1), \dots, f(P_m)) \end{aligned}$$

- ev_d es una *aplicación evaluación* .

- $\mathbb{Y} = \{P_1, \dots, P_m\}$
- Definimos una K -aplicación lineal:

$$\begin{aligned} ev_d : R_d &\longrightarrow K^{|\mathbb{Y}|} \\ f &\mapsto (f(P_1), \dots, f(P_m)) \end{aligned}$$

- ev_d es una *aplicación evaluación*.
- La imagen de R_d bajo ev_d , denotada por $C_{\mathbb{Y}}(d)$ es un *Código tipo-Reed-Muller* de grado d sobre el conjunto \mathbb{Y} .

$$ev_d : R_d \longrightarrow K^{|\mathbb{Y}|}, f \mapsto (f(P_1), \dots, f(P_m))$$

$$\begin{aligned} \ker(ev_d) &= \{f \in R_d \mid f(P_i) = 0 \ \forall P_i \in \mathbb{Y}\} \\ &= I(\mathbb{Y})_d. \end{aligned}$$

Ideal anulador de \mathbb{Y} .

$$ev_d : R_d \longrightarrow K^{|\mathbb{Y}|}, f \mapsto (f(P_1), \dots, f(P_m))$$

$$\begin{aligned} \ker(ev_d) &= \{f \in R_d \mid f(P_i) = 0 \ \forall P_i \in \mathbb{Y}\} \\ &= I(\mathbb{Y})_d. \end{aligned}$$

Ideal anulador de \mathbb{Y} .

Entonces existe un isomorfismo de K -espacios vectoriales:

$$R_d/I(\mathbb{Y})_d \simeq C_{\mathbb{Y}}(d).$$

Definición 1

Los parámetros básicos del código lineal $C_{\mathbb{Y}}(d)$ son:

- Longitud: $|\mathbb{Y}|$
- Dimensión: $\dim_{\mathbb{K}}(C_{\mathbb{Y}}(d))$
- Distancia mínima: $\delta_{\mathbb{Y}}(d)$

$$\delta_{\mathbb{Y}}(d) := \min\{\|v\| : 0 \neq v \in C_{\mathbb{Y}}(d)\}$$

donde $\|v\|$ es el número de entradas no cero de v .

$$\begin{aligned} \text{ev}_d : R_d &\longrightarrow K^{|\mathbb{Y}|} \\ f &\mapsto (f(P_1), \dots, f(P_m)) \end{aligned}$$

$$\begin{aligned} \text{ev}_d : R_d &\longrightarrow K^{|\mathbb{Y}|} \\ f &\mapsto (f(P_1), \dots, f(P_m)) \end{aligned}$$

Para $f \in R_d$, denotamos $\|f\|$ el número de no ceros de f en \mathbb{Y} .

$$\|f\| = |\mathbb{Y}| - |V_{\mathbb{Y}}(f)|$$

$V_{\mathbb{Y}}(f) = \{P \in \mathbb{Y} \mid f(P) = 0\}$, Conjunto de ceros de f .

$$\begin{aligned} \text{ev}_d : R_d &\longrightarrow K^{|\mathbb{Y}|} \\ f &\mapsto (f(P_1), \dots, f(P_m)) \end{aligned}$$

Para $f \in R_d$, denotamos $\|f\|$ el número de no ceros de f en \mathbb{Y} .

$$\|f\| = |\mathbb{Y}| - |V_{\mathbb{Y}}(f)|$$

$V_{\mathbb{Y}}(f) = \{P \in \mathbb{Y} \mid f(P) = 0\}$, Conjunto de ceros de f .

$$\begin{aligned} \delta_{\mathbb{Y}}(d) &= \min\{\|f\| : f \in R_d\}, \\ &= \min\{|\mathbb{Y}| - |V_{\mathbb{Y}}(f)| : f \in R_d\} \end{aligned}$$

$$\begin{aligned} \text{ev}_d : R_d &\longrightarrow K^{|\mathbb{Y}|} \\ f &\mapsto (f(P_1), \dots, f(P_m)) \end{aligned}$$

Para $f \in R_d$, denotamos $\|f\|$ el número de no ceros de f en \mathbb{Y} .

$$\|f\| = |\mathbb{Y}| - |V_{\mathbb{Y}}(f)|$$

$V_{\mathbb{Y}}(f) = \{P \in \mathbb{Y} \mid f(P) = 0\}$, Conjunto de ceros de f .

$$\begin{aligned} \delta_{\mathbb{Y}}(d) &= \min\{\|f\| : f \in R_d\}, \\ &= \min\{|\mathbb{Y}| - |V_{\mathbb{Y}}(f)| : f \in R_d\} \\ &= |\mathbb{Y}| - \max\{|V_{\mathbb{Y}}(f)| : f \in R_d \end{aligned}$$

Sea f un polinomio homogéneo de R , el conjunto de ceros de f en \mathbb{Y} es denotado por $V_{\mathbb{Y}}(f)$. Tenemos la siguiente fórmula para calcular el número de elementos de $V_{\mathbb{Y}}(f)$.

$$|V_{\mathbb{Y}}(f)| = \begin{cases} e(S/(I(\mathbb{Y}), f)) & \text{si } (I(\mathbb{Y}): f) \neq I(\mathbb{Y}), \\ 0 & \text{si } (I(\mathbb{Y}): f) = I(\mathbb{Y}). \end{cases}$$

Sea f un polinomio homogéneo de R , el **conjunto de ceros** de f en \mathbb{Y} es denotado por $V_{\mathbb{Y}}(f)$. Tenemos la siguiente fórmula para calcular el número de elementos de $V_{\mathbb{Y}}(f)$.

$$|V_{\mathbb{Y}}(f)| = \begin{cases} e(S/(I(\mathbb{Y}), f)) & \text{si } (I(\mathbb{Y}): f) \neq I(\mathbb{Y}), \\ 0 & \text{si } (I(\mathbb{Y}): f) = I(\mathbb{Y}). \end{cases}$$

Teorema (J. Martínez-Bernal, – ,R. Villarreal (2017))

Si $|\mathbb{Y}| \geq 2$, entonces $\delta_{\mathbb{Y}}(d) = \delta_{I(\mathbb{Y})}(d) \geq 1$ para $d \geq 1$.

Proof sketch.

- $\delta_{I(\mathbb{Y})}(d) = e(R/I(\mathbb{Y})) - \max\{e(R/(I(\mathbb{Y}), f)) \mid f \in \mathcal{F}_d\}.$

-

$$\begin{aligned}\delta_{\mathbb{Y}} &= \min\{\|f\| : f \in R_d\} \\ &= |\mathbb{Y}| - \max\{|V_{\mathbb{Y}}(f)| : f \in R_d\}.\end{aligned}$$

- De la observación anterior tenemos que $e(S/I(\mathbb{Y}), f) = |V_{\mathbb{Y}}(f)|$, además $e(R/I(\mathbb{Y})) = |\mathbb{Y}|$ y por lo tanto

$$\delta_{\mathbb{Y}} = e(R/I(\mathbb{Y})) - \max\{e(R/I(\mathbb{Y}), f) : f \in \mathcal{F}_d\}.$$



Sea $I = I(\mathbb{Y})$ y $F = \{f_1, \dots, f_r\}$ y considere
 $\mathcal{F}_{t,r} = \{F \subset R_t \mid F \not\subset I, (I: F) \neq I\}$.

Sea $I = I(\mathbb{Y})$ y $F = \{f_1, \dots, f_r\}$ y considere
 $\mathcal{F}_{t,r} = \{F \subset R_t \mid F \not\subset I, (I:F) \neq I\}$.

La δ -función de I , es la función $\delta_{r,I}: \mathbb{N}_+ \rightarrow \mathbb{Z}$ dado por

$$\delta_{r,I}(t) = \begin{cases} e(R/I) - \max\{e(R/(I,F)) \mid F \in \mathcal{F}_{t,r}\} & \text{si } \mathcal{F}_{t,r} \neq \emptyset, \\ e(R/I) & \text{si } \mathcal{F}_{t,r} = \emptyset. \end{cases}$$

Sea $I = I(\mathbb{Y})$ y $F = \{f_1, \dots, f_r\}$ y considere
 $\mathcal{F}_{t,r} = \{F \subset R_t \mid F \not\subset I, (I:F) \neq I\}$.

La δ -función de I , es la función $\delta_{r,I}: \mathbb{N}_+ \rightarrow \mathbb{Z}$ dado por

$$\delta_{r,I}(t) = \begin{cases} e(R/I) - \max\{e(R/(I,F)) \mid F \in \mathcal{F}_{t,r}\} & \text{si } \mathcal{F}_{t,r} \neq \emptyset, \\ e(R/I) & \text{si } \mathcal{F}_{t,r} = \emptyset. \end{cases}$$

Entonces: $\delta_r(C_{\mathbb{Y}}(d)) = \delta_{r,I}(d)$

$$\mathcal{M}_{\prec, d} := \{x^a \mid x^a \in \Delta_{\prec}(I)_d, (\text{in}_{\prec}(I) : x^a) \neq \text{in}_{\prec}(I)\},$$

Definición

La **función huella** de I , denotada por fp_I , es la función $\text{fp}_I: \mathbb{N}_+ \rightarrow \mathbb{Z}$ dada por

$$\text{fp}_I(d) := \begin{cases} e(R/I) - \max\{e(R/(\text{in}_{\prec}(I), x^a)) \mid x^a \in \mathcal{M}_{\prec, d}\} & \text{si } \mathcal{M}_{\prec, d} \neq \emptyset, \\ e(R/I) & \text{si } \mathcal{M}_{\prec, d} = \emptyset. \end{cases}$$

Sean I un ideal graduado no-mezclado y \prec un orden monomial. Las siguientes se satisfacen.

- (i) $\delta_I(d) \geq \text{fp}_I(d)$ y $\delta_I(d) \geq 0$ para $d \geq 1$.
- (ii) $\text{fp}_I(d) \geq 0$ si $\text{in}_{\prec}(I)$ es no-mezclado.

Sean I un ideal graduado no-mezclado y \prec un orden monomial. Las siguientes se satisfacen.

- (i) $\delta_I(d) \geq \text{fp}_I(d)$ y $\delta_I(d) \geq 0$ para $d \geq 1$.
- (ii) $\text{fp}_I(d) \geq 0$ si $\text{in}_{\prec}(I)$ es no-mezclado.

- $e(R/I) = e(R/\text{in}_{\prec}(I))$
- $e(R/(I, f)) \leq e(R/(\text{in}_{\prec}(I), \text{in}_{\prec}(f)))$

Gracias!