Funciones de Hilbert en Álgebra y Geometría

Rafael Heraclio Villarreal Rodríguez
CINVESTAV-IPN

XXX Semana Nacional de Investigación y Docencia en Matemáticas, 2 al 6 de marzo del 2020,
Departamento de Matemáticas
Universidad de Sonora.
Miercoles 4 de Marzo, 12:00 hrs.

En esta plática vamos a considerar un campo base K que puede ser:

$$K = \mathbb{Q},$$
$$K = \mathbb{R},$$
$$K = \mathbb{C},$$
$K = \mathbb{Z}_p$, enteros módulo un primo p.

$K = \mathbb{F}_q$, campo finito con q elementos.

Sean K un campo,

$S = K[t_1, \ldots, t_s]$ anillo de polinomios con coeficientes en K en las variables $t_1, \ldots, t_s$,

$g_1, \ldots, g_n$ polinomios en S,

$$I = (g_1, \ldots, g_n) = \{h_1 g_1 + \cdots + h_n g_n \colon h_i \in S \, \forall i\}$$

ideal de S generado por $g_1, \ldots, g_n$.

Los 3 invariantes fundamentales del ideal I son:

$\dim(S/I)$, *dimensión*,

$\deg(S/I)$, *grado*,

$\mathrm{reg}(S/I)$, *regularidad*.

Antes de definir la *dimensión*, el *grado*, y la *regularidad*, vamos a introducir 3 problemas en donde estos invariantes juegan un papel importante.

Problema: ¿Como podemos definir y calcular la dimensión de una variedad afín?

Problema: ¿Como podemos calcular el número de raices de un polinomio en varias variables sobre un campo finito?

Problema: ¿Como podemos resolver el problema de interpolación polinomial en varias variables?

La dimensión de una variedad afín

Una *variedad afín* X es el conjunto de ceros de un sistema finito de ecuaciones polinomiales:

$$X := V_{K^s}(g_1, \ldots, g_n) = \{P \in K^s \colon g_i(P) = 0 \text{ para todo } i\},$$

donde $g_1, \ldots, g_n$ son polinomios en $S = K[t_1, \ldots, t_s]$.

Si $X \neq \emptyset$, la dimensión de X se define como:

$$\dim(X) := \dim(S/I(X)),$$

donde $I(X)$ es el ideal anulador de X que consiste de todos los polinomios de S que se anulan en X.

Teorema Si $K = \mathbb{C}$ y $I = (g_1, \ldots, g_n)$, entonces $X = V_{K^s}(I) \neq \emptyset$ y la dimensión de X es igual a $\dim(S/I)$.

El grado y los ceros de polinomios

Si $X \subset K^s$, $|X| < \infty$, y $0 \neq f \in S$, entonces el número de raices de f en X está dado en términos del grado por

$$|V_X(f)| = \begin{cases} \deg(S/(I(X), f)) & \text{si } (I(X)\colon f) \neq I(X), \\ 0 & \text{si } (I(X)\colon f) = I(X). \end{cases}$$

Donde $(I(X)\colon f) := \{g \in S \mid gf \in I(X)\}$.

Corolario

Si $K = \mathbb{F}_q$ es un campo finito y $0 \neq f \in S$, entonces

$$|V_{\mathbb{F}_q^s}(f)| = \deg(S/(I(\mathbb{F}_q^s), f)) \text{ si } (I(\mathbb{F}_q^s)\colon f) \neq I(\mathbb{F}_q^s),$$

$V_{\mathbb{F}_q^s}(f) = \emptyset$ si $(I(\mathbb{F}_q^s)\colon f) = I(\mathbb{F}_q^s)$, y $I(\mathbb{F}_q^s) = (\{t_i^q - t_i\}_{i=1}^s)$.

La regularidad en interpolación polinomial

Sean K un campo,

$S = K[t_1, \ldots, t_s]$ anillo de polinomios con coeficientes en K en las variables $t_1, \ldots, t_s$,

$S_{\leq}d$ espacio vectorial de los $f \in S$ con $\mathrm{grado}(f) \leq d$,

$X = \{P_1, \ldots, P_m\}$ un conjunto finito de puntos distintos en el espacio afín $\mathbb{A}^s := K^s$,

$d \geq 1$ un entero.

Problema de Interpolación Polinomial:

Dados escalares $c_1, \ldots, c_m$ en K, ¿existe $f \in S_{\leq}d$ tal que $f(P_i) = c_i$ para $i = 1, \ldots, m$?

Funciones de Hilbert

Sea $S = K[t_1, \ldots, t_s]$ un anillo de polinomios y sea $I \subsetneq S$ un ideal. La *función de Hilbert afín* de S/I se define como

$$H_I^a(d) := \dim_K(S_{\leq d}/I_{\leq d}) \quad d = 0, 1, 2, \ldots,$$

donde $I_{\leq d}$ es $S_{\leq d} \cap I$.

Teorema (Hilbert)

Existe un único polinomio $h_I(z) \in \mathbb{Q}[z]$ tal que

$$H_I^a(d) = h_I(d) \quad \text{para } d \gg 0.$$

El polinomio $h_I(z)$ se llama el *polinomio de Hilbert* de S/I.

Dimensión, grado, y regularidad

Podemos escribir el polinomio de Hilbert de S/I como:

$$h_I(z) = a_k z^k + a_{k-1} z^{k-1} + \cdots + a_1 z + a_0,$$

donde $a_k \neq 0$ y $a_i \in \mathbb{Q}$ para todo i.

Definimos:

(*dimensión*) $\dim(S/I) := k = grado(h_I(z))$,

(*grado*) $\deg(S/I) := k!\, a_k$,

(*regularidad*) $\mathrm{reg}(S/I)$ es el menor entero $r \geq 0$ tal que $H_I^a(d) = h_I(d)$ para $d \geq r$.

El grado es siempre un entero positivo, es decir, $k!\, a_k$ es un entero positivo.

El cálculo de

$$\dim(S/I), \text{ *dimensión*},$$
$$\deg(S/I), \text{ *grado*},$$
$$\operatorname{reg}(S/I), \text{ *regularidad*}.$$

se puede realizar usando bases de Gröbner. El sistema de software algebraico *Macaulay2* tiene funciones para calcular estos invariantes de manera directa.

Proposición

Si $I \subsetneq S$ es un ideal, entonces

$$\begin{aligned}\dim(S/I) &= \operatorname{grado}(h_I(z)) \\ &= \max\{n \mid \text{existe una cadena } \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n \\ &\quad \text{de ideales primos de } S\}.\end{aligned}$$

- Este resultado nos dice que el grado del polinomio de Hilbert de S/I es la dimensión de Krull de S/I como anillo.

- Si $K = \mathbb{C}$ y $\mathbb{A}^s = K^s$ tiene la topología de Zariski, entonces $\dim(S)$ es igual a

$$\max\{n \mid \text{ existe una cadena } Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_n \\ \text{de conjuntos cerrados irreducibles de } \mathbb{A}^s\}.$$

Ejemplo

Sean $S = K[t_1, \ldots, t_s] = S_0 \oplus S_1 \oplus \cdots \oplus S_d \oplus \cdots$
con la graduación estandar, i.e.,

$S_0 = K$, *constantes,*

$S_1 = Kt_1 \bigoplus \cdots \bigoplus Kt_s$, *formas lineales,*

$S_2 = \bigoplus_{i \leq j} Kt_1 t_j$, *formas cuadráticas,*

$S_d = \bigoplus_{(a_1,\ldots,a_s) \in \mathbb{N}^s, \sum_{i=1}^s a_i = d} Kt_1^{a_1} \cdots t_s^{a_s}$, *formas de grado* d.

Continuación Ejemplo

Si $I = (0)$, tenemos $S_{\leq d}/I_{\leq d} = S_{\leq d} = S_0 \oplus \cdots \oplus S_d$

$$\begin{aligned} H_I^a(d) &= \dim_K(S_{\leq d}) = \sum_{i=0}^{d} \dim_K(S_i) = \sum_{i=0}^{d} \binom{i+s-1}{s-1} \\ &= \binom{d+s}{s} = \frac{(d+1)\cdots(d+s)}{s!}. \end{aligned}$$

Por lo tanto el polinomio de Hilbert de S es:

$$h_I(z) = \binom{z+s}{s} = \frac{(z+1)\cdots(z+s)}{s!},$$

luego los invariantes básicos de S son

$$\dim(S) = grado(h_I(z)) = s, \quad \deg(S) = 1, \quad \mathrm{reg}(S) = 0.$$

Consideremos un sistema de ecuaciones polinomiales

$$g_i(t_1, \ldots, t_s) = 0 \qquad \text{para } i = 1, \ldots, s$$

y sea $V_{K^s}(g_1, \ldots, g_n)$ la variedad afín de todas las soluciones de este sistema.

Teorema

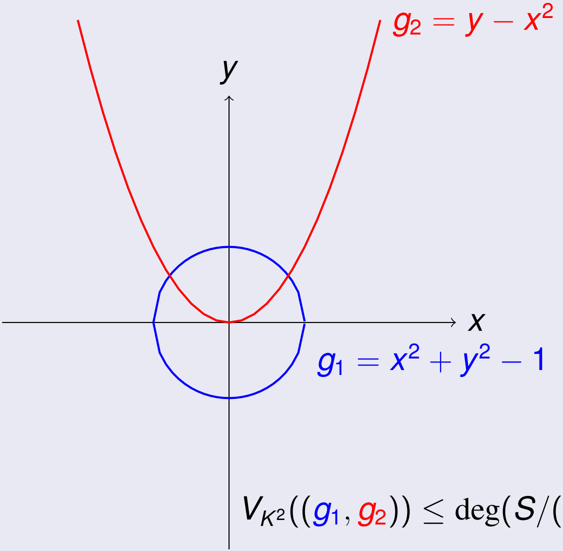
Suponiendo que $\dim(S/(g_1, \ldots, g_n)) = 0$, *tenemos:*

(a) $|V_{K^s}(g_1, \ldots, g_n)| \leq \deg(S/(g_1, \ldots, g_n))$,

(b) *Si* $K = \mathbb{C}$ *y* $(g_1, \ldots, g_n) \subsetneq S$, *entonces* $V_{K^s}(g_1, \ldots, g_n) \neq \emptyset$, *y además*

$$|V_{K^s}(g_1, \ldots, g_n)| = \deg(S/\mathrm{rad}(g_1, \ldots, g_s)).$$

Example



$$V_{K^2}((g_1, g_2)) \leq \deg(S/(g_1, g_2)) = 4$$

Continuación Ejemplo

Sean $S = K[x, y]$,

$g_1 = x^2 + y^2 - 1$ (círculo),

$g_2 = y - x^2$ (parábola).

Consideremos el ideal $I = (g_1, g_2) = (y^2 + y - 1, x^2 - y)$.

Como $\dim(S/(g_1, g_2)) = 0$, por el teorema anterior tenemos:

$$|V_{K^2}(I)| \leq \deg(S/I) = 4$$

con igualdad si $K = \mathbb{C}$ pués $I = \mathrm{rad}(I)$.

Supongamos $K = \mathbb{Q}$, entonces un punto (x_0, y_0) en $V_{\mathbb{Q}^2}(I)$ satisface la ecuación $y^2 + y - 1 = 0$. Como esta ecuación no tiene raices en $\mathbb{Q}$ obtenemos $V_{\mathbb{Q}^2}(I) = \emptyset$

Continuación Ejemplo

Supongamos $K = \mathbb{R}$, entonces un punto (x_0, y_0) en $V_{\mathbb{Q}^2}(I)$ satisface la ecuación $y_0^2 + y_0 - 1 = 0$. Como las raices reales de esta ecuación son

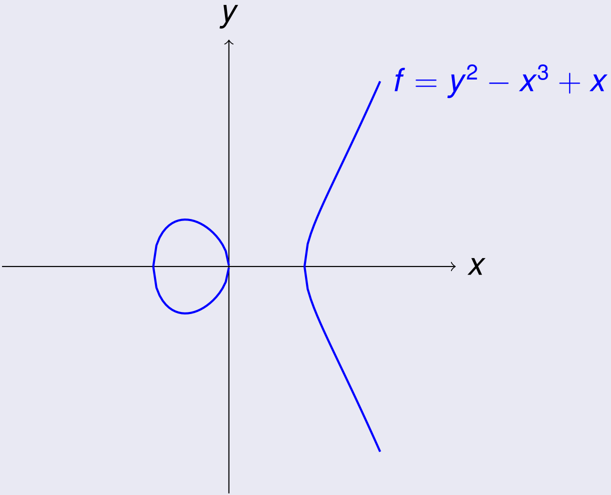
$$\frac{(-1 \pm \sqrt{5})}{2}$$

y $y_0 = x_0^2 \geq 0$ obtenemos que $|V_{\mathbb{R}^2}(I)| = 2$.

Supongamos $K = \mathbb{C}$, tenemos 2 raices cuadradas reales de $\frac{(-1+\sqrt{5})}{2}$ y 2 raices cuadradas complejas de $\frac{(-1-\sqrt{5})}{2}$ $\therefore$

$$V_{\mathbb{C}^2}(I) = \left\{ \left(\pm\sqrt{\frac{(-1 \pm \sqrt{5})}{2}}, \frac{(-1 \pm \sqrt{5})}{2} \right) \right\} \therefore |V_{\mathbb{C}^2}(I)| = 4.$$

Curva elíptica sobre el campo finito $K = \mathbb{F}_{71}$



Continuación Ejemplo

La curva elíptica $C = V_{K^2}(f) \cup \{\mathcal{O}\}$ tiene estructura de grupo. Estas curvas se usan en criptografía.

Como $\partial f/\partial x = -3x^2 + 1$ y $\partial f/\partial y = 2y$, para todo punto (x_0, y_0) sobre la curva $V_{K^2}(f)$ las derivadas parciales no se anulan simultaneamente. Para ver esto supongamos si se anulan ambas derivadas parciales:

$$3x_0^2 = 1, \quad 2y_0 = 0, \quad y_0^2 - x_0^3 + x_0 = 0,$$

$\therefore x_0 \neq 0$, $y_0 = 0$, y $x_0^3 = x_0$. Luego de la última ecuación obtenemos $x_0^2 = 1$, lo que contradice la ecuación $3x_0^2 = 1$

A las curvas cuyas derivadas parciales en cada punto sobre la curva no se anulan se les llama suaves. Toda curva elíptica es suave.

Continuación Ejemplo

$S = K[x, y]$, $K = \mathbb{F}_{71}$, $X = K^2$.

Cuantos ceros tiene $f = y^2 - x^3 + x$ en $\mathbb{F}_{71}^2$?

Usando *Macaulay2*, obtenemos que el polinomio

$$f = y^2 - x^3 + x$$

tiene 71 ceros en $X = K^2$. La correspondiente curva elíptica

$$C = V_X(f) \cup \{\mathcal{O}\}$$

tiene 72 puntos. En este caso $I(X) = (x^{71} - x, y^{71} - y)$,

$$|V_X(f)| = \deg(\mathbb{F}_{71}[x, y]/(I(X), f)) = 71$$

Interpolación en una variable

Sean K un campo,

$S = K[t]$ anillo de polinomios en una variable t,

$S_{\leq d}$ espacio vectorial de los $f \in S$ con $\mathrm{grado}(f) \leq d$,

$X = \{P_1, \ldots, P_m\}$ un conjunto de puntos distintos en K,

$d \geq 1$ un entero.

Problema de Interpolación:

Dados escalares $c_1, \ldots, c_m$ en K, ¿existe $f \in K[t]_{\leq} d$ tal que $f(P_i) = c_i$ para $i = 1, \ldots, m$?

Sea $K = \mathbb{F}_q$ un campo finito. Hay una función K-lineal

$$T_d\colon S_{\leq d} \to K^m, \qquad f \mapsto (f(P_1), \ldots, f(P_m))\,.$$

La imagen de $S_{\leq d}$ bajo T_d, denotada por $C_X(d)$, se llama *código Reed–Solomon* de grado d en X.

Reformulación Problema de Interpolación:

¿para que valores de d se satisface $C_d(X) = K^m$?

¿cual es el menor entero $d \geq 1$ tal que $C_d(X) = K^m$?

El *ideal anulador* de X, denotado por $I(X)$, es el conjunto de todos los polinomios de $K[t]$ que se anulan en todos los puntos de X.

Por lo tanto
$$S_{\leq d}/I(X)_{\leq d} \simeq C_X(d).$$
Usando el algoritmo de la división obtenemos:
$$I(X) = ((t - P_1)\cdots(t - P_m)).$$
Recordar que la *función de Hilbert Afín* de $S/I(X)$, se denota por $H_X^a(d)$, y esta definida como
$$H_X^a(d) := \dim_K(S_{\leq d}/I(X)_{\leq d}) = \dim_K(C_X(d)).$$

Sea $g(t) = (t - P_1) \cdots (t - P_m)$. Es fácil ver que

$\{\overline{1}, \overline{t}, \ldots, \overline{t^d}\}$ is a K-basis of $S_{\leq} d/(g(t))_{\leq d}$ si $d < m - 1$,

$\{\overline{1}, \overline{t}, \ldots, \overline{t^{m-1}}\}$ is a K-basis of $S_{\leq} d/(g(t))_{\leq d}$ si $d \geq m - 1$.

Por lo tanto obtenemos:

$$H_X^a(d) = \begin{cases} d + 1 & \text{si } 1 \leq d < m - 1 \\ m & \text{si } d \geq m - 1. \end{cases}$$

En particular $H_X^a(d) = m$ si y solo si $C_X(d) = K^m$.

El menor entero $d \geq 1$ para el que existe Interpolación polinomial es $d = m - 1$. Este número se llama la *regularidad* de $S/I(X)$ y se denota por $\mathrm{reg}(S/I(X))$.

La *distancia mínima* de $C_X(d)$, denotada por $\delta_X(d)$, se define como

$$\delta_X(d) := \min\{|X \setminus V_X(f)| \; : \; f \in S_{\leq d} \setminus I(X)\},$$

donde $V_X(f) = \{\alpha \in X | \, f(\alpha) = 0\}$.

Proposición

Supongamos que para algún $d \geq 1$ no hay interpolación polinomial, es decir, $d < \operatorname{reg}(S/I) = m - 1$. Entonces La distancia mínima de $C_X(d)$ es

$$\delta_X(d) = m - d \geq 2.$$

Demostración

Notar $|X \setminus V_X(f)| = m - d$, donde $f = (t - P_1) \cdots (t - P_d)$. Por lo tanto $\delta_X(d) \leq m - d$.

Sea f cualquier polinomio en $S_{\leq d} \setminus I(X)$. Entonces f tiene a lo más d raices X, esto es, $|V_X(f)| \leq d$. Entonces

$$|X \setminus V_X(f)| \geq m - d.$$

Luego entonces $\delta_X(d) \geq m - d$.

Parámetros Basicos de $C_X(d)$

- Longitud: $m = |X| = \deg(S/I(X))$
- Dimensión: $\dim_K(C_X(d)) = d + 1$ para $d < m - 1$
- *Distancia mínima*: $\delta_X(d) = m - d$ para $d < m - 1$
- $\delta_X(d) = |X| - \dim_K(C_X(d)) + 1$ (en general "$\leq$")

Generalizando los Códigos Reed-Solomon

Sean $K = \mathbb{F}_q$ un campo,

$X = \{P_1, \dots, P_m\} \subset K^s$,

$S = K[t_1, \dots, t_s]$ anillo de polinomios,

El *código afín tipo Reed–Muller* es:

$$C_X(d) := \{(f(P_1), \dots, f(P_m)) | \, f \in S_{\leq d}\} \subset K^m.$$

Parámetros básicos

- Longitud: $\deg(S/I(X)) = |X| = m$,
- Dimensión: $H_I^a(d) = \dim_K(C_X(d))$
- *Distancia mínima*:

$$\delta_X(d) := \min\{|X \setminus V_X(f)| \, : \, f \in S_{\leq d} \setminus I(X)\},$$

donde $V_X(f) = \{\alpha \in X | \, f(\alpha) = 0\}$.

Cota de Singleton

$$\delta_X(d) \leq |X| - \dim_K(C_X(d)) + 1.$$

La distancia mínima es difícil de calcular.

Funciones de Hilbert de ideales graduados

- Sea $S = K[t_1, \ldots, t_s] = \bigoplus_{d=0}^{\infty} S_d$ un anillo de polinomios con la graduación estándar, K un campo.
- $I \subset S$ es un ideal graduado de dimensión $k = \dim(S/I)$
- La *función de Hilbert* de S/I es:

$$H_I(d) := \dim_K(S_d/I_d), \quad d = 0, 1, 2, \ldots$$

Theorem (Hilbert)

Existe un polinomio $h_I(t) \in \mathbb{Q}[t]$ de grado $k - 1$ tal que

$$H_I(d) = h_I(d) \text{ para } d \gg 0$$

- El *grado* de S/I, denotado por $\deg(S/I)$, es el entero positivo

$$\deg(S/I) := \begin{cases} (k-1)! \lim_{d\to\infty} H_I(d)/d^{k-1} & \text{si } k \geq 1 \\ \dim_K(S/I) & \text{si } k = 0. \end{cases}$$

- La *regularidad* de S/I, denotado $\operatorname{reg}(S/I)$, es el menor entero $r \geq 0$ tal que $H_I(d) = h_I(d)$ para $d \geq r$.

Ideales anuladores

El siguiente objetivo es generalizar los códigos afines tipo Reed–Muller usando el espacio proyectivo.

- $\mathbb{P}^{s-1}$ es el espacio proyectivo sobre $K = \mathbb{F}_q$
- $\mathbb{X}$ es un subconjunto de $\mathbb{P}^{s-1}$
- $I(\mathbb{X}) \subset S$ es el *ideal anulador* de $\mathbb{X}$
- $S/I(\mathbb{X})$ es un anillo graduado Cohen–Macaulay de dimensión de Krull 1
- La función de Hilbert de $S/I(\mathbb{X})$ se denota por $H_{\mathbb{X}}(d)$

Códigos proyectivos tipo Reed–Muller

Sea $K = \mathbb{F}_q$ un campo finito,

$\mathbb{X} = \{[P_1], \ldots, [P_m]\} \subset \mathbb{P}^{s-1}$ con $m = |\mathbb{X}|$.

Fijamos un entero $d \geq 1$. Hay una función K-lineal:

$$T_d \colon S_d \to K^m, \qquad f \mapsto (f(P_1), \ldots, f(P_m))\,.$$

La imagen de S_d bajo T_d, denotada $C_{\mathbb{X}}(d)$, se llama un *código proyectivo de tipo Reed–Muller* de grado d.

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

(a) *longitud*: $|\mathbb{X}|$,

(b) *dimensión*: $\dim_K C_{\mathbb{X}}(d)$,

(c) *distancia mínima*:

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

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

Lo siguiente da la bien conocida relación entre códigos de tipo Reed-Muller y funciones de Hilbert:

(a) $\deg(S/I(\mathbb{X})) = |\mathbb{X}|$.

(b) $H_{\mathbb{X}}(d) = \dim_K C_{\mathbb{X}}(d)$ for $d \geq 0$.

(c) $\delta_{\mathbb{X}}(d) = 1$ for $d \geq \operatorname{reg}(S/I)$.

(d) Cota de Singleton: $\delta_{\mathbb{X}}(d) \leq |\mathbb{X}| - H_{\mathbb{X}}(d) + 1$.

Lemma

Si $0 \neq f \in S$ es homogeneo, entonces el número de ceros de f en $\mathbb{X}$ está dado por

$$|V_{\mathbb{X}}(f)| = \begin{cases} \deg(S/(I(\mathbb{X}), f)) & si\ (I(\mathbb{X})\colon f) \neq I(\mathbb{X}), \\ 0 & si\ (I(\mathbb{X})\colon f) = I(\mathbb{X}). \end{cases}$$

Example

Usando *Macaulay2*, obtenemos que el polinomio

$$f = t_1^3 + t_2^3 + t_3^3 + t_1 t_2 t_3$$

tiene 18 ceros en $\mathbb{X} = \mathbb{P}^2$ sobre el campo $K = \mathbb{F}_{13}$. Notar que el ideal anulador de $\mathbb{P}^2$ es:

$$I(\mathbb{X}) = (t_1^{13} t_2 - t_1 t_2^{13},\ t_1^{13} t_3 - t_1 t_3^{13},\ t_2^{13} t_3 - t_2 t_3^{13}).$$

Sea $I = I(\mathbb{X})$. La distancia mínima se expresa como:

$$\begin{aligned}
\delta_{\mathbb{X}}(d) &= \min\{\|T_d(f)\| \colon T_d(f) \neq 0; f \in S_d\}, \\
&= \min\{|\mathbb{X} \setminus V_{\mathbb{X}}(f)| \;:\; f \in S_d \setminus I(\mathbb{X})\} \\
&= |\mathbb{X}| - \max\{\deg(S/(I, f))| \, f \in S_d \setminus I, \, (I \colon f) \neq I\}
\end{aligned}$$

Para códigos tipo Reed-Muller esta fórmula en términos del grado permite calcular la distancia mínima usando bases de Gröbner.

Example

Sean $S = \mathbb{F}_3[t_1, t_2, t_3]$ y $\mathbb{X}$ el conjunto de puntos en $\mathbb{P}^2$:

$$[(1,1,0)],\ [(1,-1,0)],\ [(1,0,1)],$$
$$[(1,0,-1)], [(1,-1,-1)], [(1,1,1)].$$

Entonces $I(\mathbb{X}) = (t_2^2 t_3 - t_2 t_3^2,\ \ t_1^2 - t_2^2 + t_2 t_3 - t_3^2)$ y los parámetros básicos de $C_{\mathbb{X}}(d)$ son:

d	1	2	3
$\lvert\mathbb{X}\rvert$	6	6	6
$H_{\mathbb{X}}(d)$	3	5	6
$\delta_{\mathbb{X}}(d)$	3	2	1

Existen enteros $r \geq 1$ y $r_1 \geq 1$ tales que

$$1 = H_{\mathbb{X}}(0) < H_{\mathbb{X}}(1) < \cdots < H_{\mathbb{X}}(r-1) < H_{\mathbb{X}}(d) = |\mathbb{X}|$$

para $d \geq r = \operatorname{reg}(S/I(\mathbb{X}))$,

$$\delta_{\mathbb{X}}(1) > \delta_{\mathbb{X}}(2) > \cdots > \delta_{\mathbb{X}}(r_1) = \delta_{\mathbb{X}}(d) = 1 \ \text{ para } \ d \geq r_1.$$

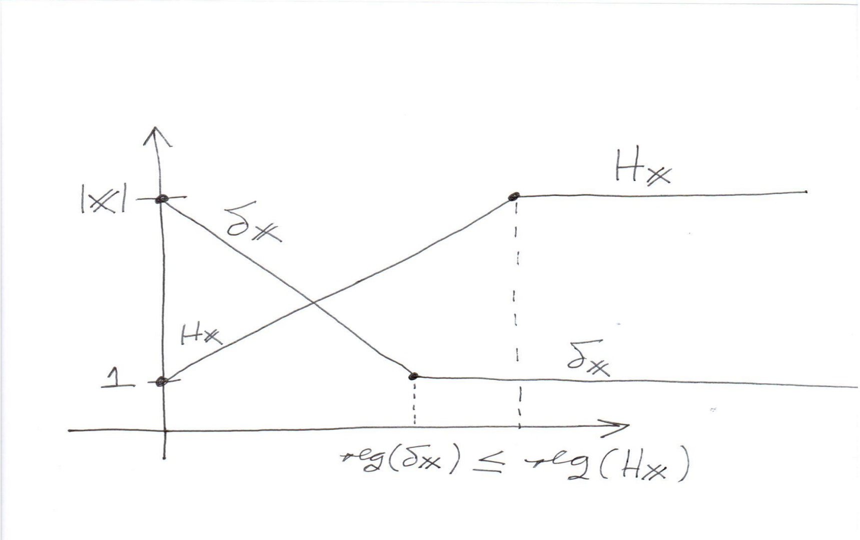
El entero r_1, denotado por $\operatorname{reg}(\delta_{\mathbb{X}})$, se llama el índice de regularidad de $\delta_{\mathbb{X}}$.

En general $\operatorname{reg}(\delta_{\mathbb{X}}) \leq \operatorname{reg}(S/I(\mathbb{X}))$. En efecto, usando

$$\delta_{\mathbb{X}}(d) \leq |\mathbb{X}| - H_{\mathbb{X}}(d) + 1,$$

obtenemos que $\delta_{\mathbb{X}}(d) = 1$ para $d \geq \operatorname{reg}(S/I(\mathbb{X}))$.

Comparando las funciones $H_{I(\mathbb{X})}$ y $\delta_{\mathbb{X}}$



Ejemplo

Sea K el campo $\mathbb{F}_3$. Consideremos el conjunto

$$\mathbb{X} = \{[1,1,1],[1,-1,0],[1,0,-1],[0,1,-1],[1,0,0]\} \subset \mathbb{P}^2$$

Usando *Macaulay2*, obtenemos que $\operatorname{reg}(S/I(\mathbb{X})) = 3$.

Tenemos que $\delta_{\mathbb{X}}(1) = 1$ pues el polinomio $t_1 + t_2 + t_3$ se anula en todos los puntos de $\mathbb{X} \setminus \{[1,0,0]\}$.

Por lo tanto $1 = \operatorname{reg}(\delta_{\mathbb{X}}) < \operatorname{reg}(S/I(\mathbb{X})) = 3$

Existen muchas familias donde $\operatorname{reg}(\delta_{\mathbb{X}}) = \operatorname{reg}(S/I(\mathbb{X}))$.

Problema Principal:

Si $\mathbb{X}$ tiene una "buena" estructura algebraica o combinatoria encontrar fórmulas, en términos de s, q, d, y la estructura de $\mathbb{X}$, para los *parámetros básicos* de $C_{\mathbb{X}}(d)$:

(a) $H_{\mathbb{X}}(d)$,

(b) $\deg(S/I(\mathbb{X}))$,

(c) $\delta_{\mathbb{X}}(d)$,

(d) $\operatorname{reg}(S/I(\mathbb{X}))$.

En particular nos interesan los siguientes casos:

- $\mathbb{X}$ está parametrizado por monomios $y^{v_1}, \ldots, y^{v_s}$.
- $\mathbb{X}$ es un "conjunto cartesiano proyectivo anidado".

THE END