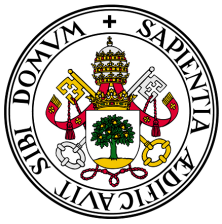


Universidad de Valladolid

Facultad de Ciencias

Trabajo de Fin de Máster

Máster en Matemáticas

Invariantes homológicos de ideales graduados y su aplicación en Teoría de Códigos

Autor: Rodrigo San José Rubio
Tutores: Philippe Gimenez y Diego Ruano

Índice general

Introducción

El objetivo de este trabajo es estudiar la conexión entre varios invariantes homológicos y la teoría de códigos. Para ello, nos basamos principalmente en los resultados obtenidos por el grupo liderado por Rafael H. Villarreal, ver por ejemplo [6], [14] y [20]. Para poder estudiar esta conexión, es necesario profundizar algo más en álgebra conmutativa, para lo cual se utilizan referencias como [10], [21] o [28]. A la hora de presentar ejemplos es muy útil usar sistemas de álgebra computacional como [9] o [12], así que en el trabajo también se incluyen procedimientos en estos sistemas para realizar los cálculos.

El tema del trabajo se encuentra en la intersección entre el álgebra conmutativa y la teoría de códigos, y es por eso que en diversas partes del trabajo tenemos distintos objetivos. Por una parte, se introduce una formulación algebraica de la distancia mínima de los códigos tipo Reed-Muller proyectivos mediante la función distancia mínima, y se introduce además otra función, la función huella, que nos permite acotar inferiormente la función distancia mínima. Estas funciones se pueden definir para ideales homogéneos en general y se pueden estudiar sus propiedades en ese caso, lo cual es de interés en álgebra conmutativa. Además, estas funciones se pueden generalizar para tratar los pesos de Hamming generalizados. Por otro lado, podemos utilizar el conocimiento teórico sobre estas funciones para recuperar la distancia mínima, o cotas inferiores de ella, para algunos tipos de códigos particulares, como los códigos cartesianos o los parametrizados por un toro proyectivo.

En el capítulo 1 estudiamos algunos conceptos de álgebra conmutativa que no se llegan a ver en el grado o el máster, y además profundizamos en varios conceptos ya conocidos de álgebra conmutativa. Por otro lado, también recordamos algunas nociones básicas de teoría de códigos e introducimos algunos tipos de códigos particulares sobre los que hablaremos más adelante en el trabajo.

El capítulo 2 está dedicado al estudio teórico, desde el punto de vista del álgebra conmutativa, de la función distancia mínima y la función huella, así como de sus generalizaciones. También se calculan fórmulas en casos particulares que serán útiles para algunos tipos de códigos, como se ve en el último capítulo, y se ven propiedades de las funciones que hemos definido que son similares a las de la distancia mínima o los pesos de Hamming generalizados en teoría de códigos.

En el capítulo 3 complementamos lo que hemos visto en el capítulo 2 mostrando la relación entre las funciones que hemos definido y los parámetros de los códigos tipo Reed-Muller proyectivos. Primero estudiamos cómo expresar el número de ceros de

un conjunto de polinomios en una variedad proyectiva definida por un conjunto finito de puntos con el grado, y luego vemos que, en cierto modo, las funciones que hemos definido generalizan la distancia mínima y los pesos de Hamming generalizados del código. Posteriormente se presentan algunas aplicaciones prácticas y ejemplos ilustrativos de los resultados que hemos mostrado, utilizando resultados que hemos obtenido previamente en el capítulo 2.

La memoria pretende ser un texto autocontenido (incluimos un capítulo entero dedicado a preliminares) que cubre una cantidad considerable de material distribuido en diversos artículos (por ejemplo, [6], [14], [20], [22]), varios de los cuales son relativamente recientes, con una notación consistente y de la forma más clara posible. En este sentido se incluyen algunos ejemplos y procedimientos de estos artículos, pero también se añaden varios ejemplos y procedimientos propios en Macaulay2 [12], sobre todo en las últimas secciones de la memoria, donde se ilustran los resultados y definiciones que hemos dado a lo largo del trabajo.

Notación

A lo largo de la memoria se irá introduciendo notación específica, que se explicará en cada caso, pero hay parte de la notación que es común a toda la memoria y que presentamos a continuación:

- K denotará un cuerpo, en principio arbitrario, aunque en la parte de aplicaciones será siempre finito.
- R denotará un anillo conmutativo, unitario y *noetheriano*. $S = K[x_1, \ldots, x_n]$ denotará el anillo de polinomios con coeficientes en el cuerpo K y n variables.
- I denotará un ideal arbitrario de R. Como vamos a trabajar habitualmente con anillos graduados, I será homogéneo en la mayoría de los casos, pero lo mencionaremos explícitamente.
- M denotará un R-módulo arbitrario.
- El ideal $\mathfrak{m}$ será el ideal homogéneo maximal de un anillo local R. Habitualmente será el del anillo de polinomios S, y entonces $\mathfrak{m} = (x_1, \ldots, x_n)$. Denotaremos con las letras $\mathfrak{p}$ y $\mathfrak{q}$ a los ideales primos y primarios, respectivamente.

Capítulo 1

Preliminares

En esta sección vamos a introducir y recordar algunos resultados de álgebra conmutativa que serán necesarios para el resto del trabajo. Usaremos las referencias [1], [4], [8], [10], [21] y [28] para aspectos generales de álgebra conmutativa. Para temas relacionados con bases de Gröbner, utilizamos [7].

1.1. Dimensión de Krull y altura

Definición 1.1.1. Sea R un anillo.

- El conjunto de ideales primos de R se llama *espectro* de R, y se denota por $\mathrm{Spec}(R)$.
- Una *cadena* de ideales primos de R es una sucesión finita estrictamente creciente de ideales primos
$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n.$$
El entero n se llama *longitud* de la cadena.
- La *dimensión de Krull* de R, denotada por $\dim(R)$, es el supremo de las longitudes de todas las cadenas de ideales primos en R.
- Sea $\mathfrak{p}$ un ideal primo de R. La *altura* de $\mathfrak{p}$, denotada por $\mathrm{ht}(\mathfrak{p})$, es el supremo de las longitudes de todas las cadenas de ideales primos
$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n = \mathfrak{p}$$
que acaban en $\mathfrak{p}$. Equivalentemente, $\mathrm{ht}(\mathfrak{p}) = \dim R_{\mathfrak{p}}$.
- Sea I un ideal de R. Entonces $\mathrm{ht}(I)$, la *altura* de I, se define como
$$\mathrm{ht}(I) = \mathrm{mín}\{\mathrm{ht}(\mathfrak{p}) \mid I \subset \mathfrak{p} \text{ y } \mathfrak{p} \in \mathrm{Spec}(R)\}.$$

Lema 1.1.2. *Se tiene que* $\mathrm{ht}(I) + \dim(R/I) \leq \dim(R)$.

Demostración. Supongamos que $\mathrm{ht}(I) \geq r$ y $\dim(R/I) \geq s$. Basta ver que $\dim(R) \geq r+s$. Por hipótesis tenemos una cadena de primos $I \subset \mathfrak{q}_0 \subset \cdots \subset \mathfrak{q}_s$. Entonces $\mathrm{ht}(\mathfrak{q}_0) \geq \mathrm{ht}(I) \geq r$, así que podemos encontrar primos $\mathfrak{p}_i$, $i = 0, 1, \ldots, r$ de manera que

$$\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_r = \mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_s$$

es una cadena de ideales primos de R con longitud $r+s$. □

La diferencia $\dim(R) - \dim(R/I)$ se llama *codimensión* de I (denotada $\mathrm{codim}(I)$), y $\dim(R/I)$ se llama la *dimensión* de I. En estos términos, el lema 1.1.2 nos dice que $\mathrm{ht}(I) \leq \mathrm{codim}(I)$.

Definición 1.1.3. Sea M un R-módulo.

- Sean N_1 y N_2 dos submódulos de M. Su *ideal cociente* se define como

$$(N_1 :_R N_2) = \{x \in R \mid xN_2 \subset N_1\}.$$

- El *anulador* de M es el ideal

$$\mathrm{ann}_R(M) = \{x \in R \mid xM = 0\}.$$

  Esto se puede ver como $(0 :_R M)$. Si $m \in M$, el *anulador* de m es $\mathrm{ann}(m) = \mathrm{ann}(Rm)$.

Definición 1.1.4. La *dimensión* de un R-módulo es $\dim(M) = \dim(R/\operatorname{ann}(M))$ y la *codimensión* de M es $\mathrm{codim}(M) = \dim(R) - \dim(M)$.

Definición 1.1.5. Decimos que $a \in R$ es un *divisor de cero* de M si existe un elemento no nulo $x \in M$ tal que $ax = 0$. De no ser así, decimos que a es un no divisor de cero, o un elemento *M-regular* (diremos simplemente *regular*). Al conjunto de divisores de cero de M lo denotaremos por $\mathcal{Z}(M)$.

Observación 1.1.6. Es directo comprobar que un elemento f es divisor de cero en R/I si y solo si $(I : f) \neq I$.

Lema 1.1.7 [1, Cor. 11.18]**.** *Sea R un anillo local, x un elemento de $\mathfrak{m}$ (el ideal maximal) que es un no divisor de cero. Entonces* $\dim R/(x) = \dim R - 1$.

1.2. Descomposición primaria de módulos

En el grado se estudia la descomposición primaria en anillos noetherianos. En esta sección vamos a ver como se extiende esta teoría a módulos sobre anillos noetherianos, con especial énfasis en el concepto de primos asociados. Como referencias, vamos a utilizar principalmente [21] y [28].

Definición 1.2.1. Sea M un R-módulo. Un ideal primo $\mathfrak{p}$ de R se llama *primo asociado* de M si $\mathfrak{p}$ es el anulador $\operatorname{ann}(x)$ para algún $x \in M$. El conjunto de los primos asociados de M se denota $\operatorname{Ass}_R(M)$ o $\operatorname{Ass}(M)$. Para un ideal I de R, los primos asociados del R-módulo R/I se llaman *divisores primos* o *primos asociados* de I, y denotamos $\operatorname{Ass}(I) = \operatorname{Ass}(R/I)$.

Observación 1.2.2. Equivalentemente, podemos definir $\operatorname{Ass}_R(M)$ como el conjunto de ideales primos $\mathfrak{p}$ de R tales que existe un monomorfismo φ de R-módulos

$$R/\mathfrak{p} \hookrightarrow M.$$

Observamos que $\mathfrak{p} = \operatorname{ann}(\phi(1))$.

Teorema 1.2.3 [21, Thm. 6.1]**.** *Sea M un R-módulo no nulo.*

(a) *Cualquier elemento maximal de la familia $F = \{\operatorname{ann}(x) \mid 0 \neq x \in M\}$ es un primo asociado de M. En particular, $\operatorname{Ass}(M) \neq \emptyset$.*

(b) *El conjunto de divisores de cero de M es la unión de todos los primos asociados de M:*

$$\mathcal{Z}(M) = \bigcup_{\mathfrak{p} \in \operatorname{Ass}(M)} \mathfrak{p}.$$

Demostración.

(a) Tenemos que probar que si $\operatorname{ann}(x)$ es un elemento maximal de F, entonces es primo: si $a, b \in R$ cumplen $abx = 0$ pero $bx \neq 0$, entonces, por maximalidad, $\operatorname{ann}(bx) = \operatorname{ann}(x)$; en consecuencia, $ax = 0$.

(b) Si $ax = 0$ para algún $x \neq 0$, entonces $a \in \operatorname{ann}(x) \in F$, y por (a) existe un primo asociado de M que contiene a $\operatorname{ann}(x)$.

□

En el caso graduado, el siguiente resultado nos garantiza que podemos trabajar exclusivamente con ideales homogéneos.

Lema 1.2.4 [4, Lem. 1.5.6]**.** *Sea R un anillo graduado, y M un R-módulo graduado. Si $\mathfrak{p} \in \operatorname{Ass}(M)$, entonces $\mathfrak{p}$ es homogéneo y existe un elemento homogéneo $m \in M$ tal que $\mathfrak{p} = \operatorname{ann}(m)$.*

Demostración. Elegimos un elemento $x \in M$ con $\mathfrak{p} = \operatorname{ann}(x)$. Sea $x = x_m + \cdots + x_n$ su descomposición como suma de elementos homogéneos x_i de grado i. Análogamente, descomponemos un elemento $a = a_p + \cdots + a_q$ de $\mathfrak{p}$. Puesto que $ax = 0$, tenemos que $a_p x_m = 0$. De $a(a_p x) = 0$, deduciríamos que $a_p^2 x_{m+1} = 0$, e iterando, $a_p^i x_{m+i-1} = 0$ para todo $i \geq 1$. En consecuencia, a_p^{n-m+1} anula a x. Puesto que $\mathfrak{p}$ es primo, $a_p \in \mathfrak{p}$. El siguiente paso sería hacer lo mismo con $a - a_p$, e iterando vemos que cada componente homogénea de a está en $\mathfrak{p}$.

Para probar la segunda parte, usamos que $\mathfrak{p}$ está generado por elementos homogéneos, lo cual nos dice que $\mathfrak{p}$ anula todas las componentes homogéneas de x. Así que si denotamos $\mathfrak{a}_i = \operatorname{ann}(x_i)$, entonces $\mathfrak{p} \subset \mathfrak{a}_i$ (cada generador homogéneo va a anular todas las componentes homogéneas de x). Por otro lado, puesto que $p = \operatorname{ann}(x)$, $\bigcap_{i=m}^{n} \mathfrak{a}_i \subset \mathfrak{p}$, por lo que $\bigcap_{i=m}^{n} \mathfrak{a}_i = \mathfrak{p}$. Como $\mathfrak{p}$ es primo, ha de ser $\mathfrak{a}_j = \mathfrak{p}$ para algún j ([1, Prop. 1.11]). □

Lema 1.2.5 [23, Lem. 1.3.9]**.** *Sea $V \neq \{0\}$ un espacio vectorial sobre un cuerpo infinito K. Entonces V no es unión finita de subespacios propios de V.*

Demostración. Razonamos por reducción al absurdo. Suponemos que existen subespacios propios $V_1, \ldots, V_m$ de V tales que $V = \bigcup_{i=1}^{m} V_i$, donde m es el menor entero positivo con esta propiedad. Sean

$$v_1 \in V_1 \setminus (V_2 \cup \cdots \cup V_m) \text{ y } v_2 \in V_2 \setminus (V_1 \cup V_3 \cup \cdots \cup V_m).$$

Elegimos $m+1$ escalares no nulos distintos $k_0, \ldots, k_m$ en K. Consideramos los vectores $\beta_i = v_1 - k_i v_2$ para $i = 0, \ldots, m$. Para algún j debe haber dos vectores distintos $\beta_r, \beta_s \in V_j$. Puesto que $\beta_r - \beta_s \in V_j$, tenemos que $v_2 \in V_j$, por lo que debe ser $j = 2$ por la elección de v_2. Pero $\beta_r \in V_2$ implica que $v_1 \in V_2$, una contradicción. □

Proposición 1.2.6 [23, Prop. 1.3.10]**.** *Sea S el anillo de polinomios y $\mathfrak{m}$ su ideal homogéneo maximal. Sea $I \subset S$ un ideal homogéneo. Si K es infinito y $\mathfrak{m}$ no está en $\operatorname{Ass}(S/I)$, entonces existe $h_1 \in S_1$ tal que $h_1 \notin \mathcal{Z}(S/I)$.*

Demostración. Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ los primos asociados de S/I. Como S/I es graduado, por el lema 1.2.4, $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ son ideales homogéneos. Razonamos por reducción al absurdo. Supongamos que S_1, la parte de grado 1 de S, está contenida en $\mathcal{Z}(S/I)$. Por el teorema 1.2.3, tenemos que $\mathcal{Z}(S/I) = \cup_{i=1}^{m} \mathfrak{p}_i$. En consecuencia

$$S_1 \subset (\mathfrak{p}_1)_1 \cup (\mathfrak{p}_2)_1 \cup \cdots \cup (\mathfrak{p}_m)_1 \subset S_1,$$

donde $(\mathfrak{p}_i)_1$ es la parte homogénea de grado 1 del ideal homogéneo $\mathfrak{p}_i$. Puesto que K es infinito, por el lema 1.2.5 deducimos que $S_1 = (\mathfrak{p}_i)_1$ para algún i. Así que $\mathfrak{p}_i = \mathfrak{m}$, una contradicción. □

Definición 1.2.7. Sea M un R-módulo.

- El *soporte* de M, denotado por $\operatorname{Supp}(M)$, es el conjunto de los ideales primos $\mathfrak{p}$ de R tales que $M_{\mathfrak{p}} \neq 0$, donde $M_{\mathfrak{p}}$ es la localización de M en el primo $\mathfrak{p}$.
- Los *primos minimales* de M son los elementos minimales de $\operatorname{Supp}(M)$ con respecto a la inclusión.
- Un primo minimal de M se llama *primo asociado aislado* de M. Un primo asociado de M que no es aislado se llama *primo asociado inmerso*.

Definición 1.2.8. Sea R un anillo, M un R-módulo y $N \subset M$ un submódulo. Decimos que N es un *submódulo primario* de M si se da la siguiente condición para todo $r \in R$ y $x \in M$:

$$x \notin N \text{ y } rx \in N \Rightarrow r^n M \subset N \text{ para algún } n.$$

Esta condición solo depende del módulo cociente M/N, y se puede rescribir de la siguiente manera:

$$\text{si } r \in R \text{ es un divisor de cero en } M/N \text{ entonces } r \in \sqrt{\operatorname{ann}(M/N)}.$$

Un ideal primario es simplemente un submódulo primario del R-módulo R.

Teorema 1.2.9 [21, Thm. 6.6]**.** *Sea R un anillo noetheriano y M un R-módulo finitamente generado. Entonces un submódulo $N \subset M$ es primario si y solo si* $\operatorname{Ass}(M/N) = \{\mathfrak{p}\}$ *(solo tiene un elemento). En esta situación, si* $\operatorname{ann}(M/N) = I$*, entonces I es primario y $\sqrt{I} = \mathfrak{p}$.*

El teorema anterior nos da una definición alternativa para módulo primario.

Definición 1.2.10. Si $\operatorname{Ass}(M/N) = \{\mathfrak{p}\}$ decimos que $N \subset M$ es un submódulo $\mathfrak{p}$-*primario.*

Teorema 1.2.11 [21, Thm 6.7]**.** *Si N y N' son submódulos $\mathfrak{p}$-primarios de M, entonces también lo es $N \cap N'$.*

Definición 1.2.12. Sea M un R-módulo, y $N \subset M$ un submódulo. Decimos que N es *reducible* si se puede escribir como una intersección $N = N_1 \cap N_2$ de dos submódulos N_1, N_2 con $N_i \neq N$. Si no se da lo anterior, decimos que N es *irreducible.*

Proposición 1.2.13. *Si M es un módulo noetheriano, entonces cualquier submódulo N de M se puede escribir como intersección finita de submódulos irreducibles.*

Demostración. Sea $\mathcal{F}$ el conjunto de los submódulos $N \subset M$ que no admiten tal expresión. Si $\mathcal{F} \neq \emptyset$, entonces tiene un elemento maximal N_0. Pero entonces N_0 es reducible, por lo que $N_0 = N_1 \cap N_2$, y $N_i \notin \mathcal{F}$. Cada N_i es intersección de un número finito de submódulos irreducibles, por lo que también lo es N_0, que es una contradicción. □

Definición 1.2.14. Sea M un R-módulo, y $N \subsetneq M$ un submódulo propio. Una *descomposición primaria irredundante* de N es una expresión de N como intersección de submódulos $N = N_1 \cap \cdots \cap N_r$, tal que:

(a) (Los submódulos son primarios) $\operatorname{Ass}(M/N_i) = \{\mathfrak{p}_i\}$ para todo i.

(b) (Irredundante) $N \neq N_1 \cap \cdots \cap N_{i-1} \cap N_{i+1} \cap \cdots \cap N_r$ para todo i.

(c) (Minimal) $\mathfrak{p}_i \neq \mathfrak{p}_j$ si $N_i \neq N_j$.

Por la proposición 1.2.13, todo submódulo N de un R-módulo noetheriano M admite una descomposición en submódulos irreducibles. En el siguiente teorema veremos que en un submódulo propio irreducible de M es un submódulo primario. Quitando submódulos innecesarios de la intersección, y teniendo en cuenta 1.2.11, vemos que existe una descomposición primaria irredundante de N.

Teorema 1.2.15 [21, Thm. 6.8]**.** *Sea M un R-módulo finitamente generado.*

(a) *Un submódulo propio irreducible de M es un submódulo primario.*

(b) *Si $N = N_1 \cap \cdots \cap N_r$ con $\mathrm{Ass}(M/N_i) = \{\mathfrak{p}_i\}$ es una descomposición primaria irredundante de un submódulo propio $N \subsetneq M$, entonces $\mathrm{Ass}(M/N) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$.*

(c) *Cualquier submódulo propio N de M tiene una descomposición primaria (irredundante). Si N es un submódulo propio de M y $\mathfrak{p}$ es un primo asociado minimal de M/N, entonces la componente $\mathfrak{p}$-primaria de N es $\varphi_{\mathfrak{p}}^{-1}(N_{\mathfrak{p}})$, donde $\varphi_{\mathfrak{p}} : M \to M_{\mathfrak{p}}$ es la aplicación canónica. En consecuencia, esa componente está unívocamente determinada por M, N y $\mathfrak{p}$.*

Corolario 1.2.16. *Si $I \subsetneq R$ es un ideal propio de R, entonces I tiene una descomposición primaria irredundante $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ tal que $\mathfrak{q}_i$ es un ideal $\mathfrak{p}_i$-primario y $\mathrm{Ass}(R/I) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$.*

Demostración. Sea $(0) = I/I = (\mathfrak{q}_1/I) \cap \cdots \cap (\mathfrak{q}_r/I)$ una descomposición primaria irredundante del ideal cero en R/I. Entonces $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ y $\mathfrak{q}_i/I$ es $\mathfrak{p}_i$-primario, ya que $\mathrm{Ass}((R/I)/(\mathfrak{q}_i/I)) = \mathrm{Ass}(R/\mathfrak{q}_i) = \{\mathfrak{p}_i\}$. Por el teorema 1.2.9, $\mathfrak{q}_i$ es un ideal $\mathfrak{p}_i$-primario. □

1.3. Anillos y módulos Cohen-Macaulay

En esta sección vamos a estudiar los anillos y módulos Cohen-Macaulay. Como referencias, vamos a utilizar principalmente [4], [10] y [28].

Definición 1.3.1. Sea M un R-módulo. Una sucesión de elementos $x_0, \ldots, x_d$ de R se llama *sucesión M-regular* si cumple

(a) $(x_0, \ldots, x_d)M \neq M$, y

(b) para cada $i = 0, \ldots, n$, x_i es un no divisor de cero en $M/(x_0, \ldots, x_{i-1})M$.

Una sucesión R-regular se llama simplemente *sucesión regular*.

Ejemplo 1.3.2. El ejemplo clásico de sucesión regular es la sucesión $x_1, \ldots, x_n$ (en cualquier orden) de variables en el anillo de polinomios $S = K[x_1, \ldots, x_n]$.

Antes de continuar vamos a realizar un breve inciso para explicar la forma en que se enuncian los siguientes resultados. Siguiendo la notación de [4], si tenemos un anillo graduado R, se dice que un ideal homogéneo $\mathfrak{m}$ de R es **maximal* si cualquier otro ideal homogéneo que lo contenga es igual a R. El anillo R se llama **local* si tiene un único ideal *maximal $\mathfrak{m}$. Esta última situación se suele denotar por $(R, \mathfrak{m})$, que es la notación que se usa para anillos locales. La razón es que este tipo de anillos juegan, en el caso graduado, el mismo papel que los anillos locales, y cumplen resultados análogos a los que cumplen los anillos locales. Es habitual enunciar los resultados para anillos locales, y así lo vamos a hacer en lo que sigue, pero en este trabajo realmente los vamos a aplicar a anillos *locales (como el anillo de polinomios), por eso es importante incidir sobre lo anterior.

Diremos que una sucesión M-regular $x_1, \ldots, x_d$ contenida en el ideal $I \subset R$ es *maximal* en I si $x_1, \ldots, x_{d+1}$ no es una sucesión M-regular para cualquier $x_{d+1} \in I$. El siguiente resultado nos permite dar la definición de profundidad de un ideal.

Teorema 1.3.3 (Northcott y Rees, [17, Thm. 121])**.** *Sea R un anillo noetheriano, I un ideal en R, y M un R-módulo finitamente generado. Suponemos que $IM \neq M$. Entonces dos sucesiones M-regulares maximales contenidas en I tienen la misma longitud.*

Definición 1.3.4. Sea $(R, \mathfrak{m})$ un anillo local (noetheriano) y sea $M \neq 0$ un R-módulo.

- La *profundidad* de M, denotada por $\operatorname{depth}(M)$, es la longitud de cualquier sucesión M-regular maximal que esté contenida en $\mathfrak{m}$.
- Se dice que M es un *módulo Cohen-Macaulay* si $\operatorname{depth}(M) = \dim(M)$. Si $I \subset R$ es un ideal y $M = R/I$ es Cohen-Macaulay, se dice que I es *Cohen-Macaulay*.
- Se dice que R es un *anillo Cohen-Macaulay* si R es Cohen-Macaulay como R-módulo.

Observación 1.3.5. Por el lema 1.1.7, se tiene que $\operatorname{depth}(M) \leq \dim(M)$.

Ejemplo 1.3.6. De nuevo, el ejemplo más sencillo es el del anillo de polinomios $S = K[x_1, \ldots, x_n]$, en el cual se tiene que $\operatorname{depth}(S) = \dim(S) = n$, por lo que es Cohen-Macaulay.

Otro ejemplo es cualquier anillo noetheriano de dimensión 0, por la observación 1.3.5.

El siguiente resultado es similar al que se tiene para la dimensión de Krull de un ideal.

Lema 1.3.7 [28, Lem. 2.3.10]**.** *Sea $(R, \mathfrak{m})$ un anillo local, I un ideal de R y $x \in \mathfrak{m}$ un elemento regular de $M = R/I$. Entonces* $\operatorname{depth}(M/xM) = \operatorname{depth}(M) - 1$.

Definición 1.3.8. Sea $I \subset R$ un ideal. Si I está generado por una sucesión regular decimos que I es una *intersección completa*.

Definición 1.3.9. Sea $I \subset R$ un ideal. Decimos que I es *no mezclado* si $\mathrm{ht}(I) = \mathrm{ht}(\mathfrak{p})$ para todo $\mathfrak{p}$ en $\mathrm{Ass}(R/I)$.

Teorema 1.3.10 [4, Thm. 2.1.3]**.** *Sea $(R, \mathfrak{m})$ un anillo noetheriano local y M un R-módulo finitamente generado. Se tiene que $M_\mathfrak{p}$ es Cohen-Macaulay para todo $\mathfrak{p} \in \mathrm{Spec}(R)$, y si $M_\mathfrak{p} \neq 0$, entonces $\dim(M) = \dim(M_\mathfrak{p}) + \dim(M/\mathfrak{p}M)$.*

Observación 1.3.11. En particular, si consideramos $M = R$ en el teorema 1.3.10, tenemos que $\dim(R_\mathfrak{p}) = \mathrm{ht}(\mathfrak{p}) = \mathrm{codim}(\mathfrak{p})$ para todo $\mathfrak{p} \in \mathrm{Supp}(R)$.

De lo anterior deducimos que si tenemos un ideal I no mezclado en un anillo local R que sea Cohen-Macaulay, entonces $\dim(R/I) = \dim(R/\mathfrak{p})$ para todo $\mathfrak{p} \in \mathrm{Ass}(R/I)$. En efecto, $\mathrm{codim}(I) \geq \mathrm{ht}(I) = \mathrm{ht}(\mathfrak{p}) = \mathrm{codim}(\mathfrak{p})$, por lo que $\dim(R/I) \leq \dim(R/\mathfrak{p})$. Pero $\mathfrak{p} \supset I$, por lo que $\dim(R/\mathfrak{p}) \leq \dim(R/I)$, así que tenemos la igualdad. Este hecho lo utilizaremos implícitamente en muchos de los razonamientos que haremos en las secciones posteriores.

Proposición 1.3.12 [28, Prop. 2.3.24]**.** *Sea $(R, \mathfrak{m})$ un anillo local Cohen-Macaulay y sea I un ideal de R. Si I es una intersección completa, entonces I es no mezclado y R/I es Cohen-Macaulay.*

Teorema 1.3.13 (Unmixedness theorem, [28, Thm. 2.3.27])**.** *Un anillo R es Cohen-Macaulay si y solo si cualquier ideal propio I de R de altura r generado por r elementos es no mezclado.*

1.4. Resoluciones libres graduadas

En esta sección vamos a considerar anillos graduados arbitrarios (noetherianos) R, y luego hablaremos sobre el anillo graduado $S = K[x_1, \ldots, x_n] = \oplus_{d=0}^{\infty} S_d$ de los polinomios sobre un cuerpo K. Vamos a revisar algunos conceptos sobre resoluciones, que se pueden encontrar en mayor detalle en [8] o [24].

Definición 1.4.1. Sea $R = \oplus_{d \in \mathbb{Z}} R_d$ un anillo graduado, y $M = \oplus_{t \in \mathbb{Z}} M_t$, $N = \oplus_{t \in \mathbb{Z}} N_t$ R-módulos graduados.

- Dado el R-módulo M, llamaremos *módulo desplazado* de M, y lo denotaremos por $M(d)$ para un cierto $d \in \mathbb{Z}$, al R-módulo graduado $M(d) = \oplus_{t \in \mathbb{Z}} M_{d+t}$. Llamaremos *módulo libre desplazado* a un R-módulo isomorfo a $R(d_1) \oplus \cdots \oplus R(d_m)$, para unos ciertos $d_1, \ldots, d_m \in \mathbb{Z}$.

- Un homomorfismo de módulos $\varphi : M \to N$ se dice que es un *homomorfismo graduado de grado d* si $\varphi(M_t) \subset N_{t+d}$. A los homomorfismos graduados de grado 0 los llamaremos simplemente *homomorfismos graduados*.

- Una *resolución libre graduada* del R-módulo graduado M es una sucesión exacta
$$\cdots \longrightarrow F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0 \ ,$$
donde cada F_l es un módulo libre graduado desplazado de la forma $R(-d_1) \oplus \cdots \oplus R(-d_p)$ y cada homomorfismo φ_l es un homomorfismo graduado. Si cada φ_l lleva la base estándar de F_l a un sistema de generadores minimal de $\mathrm{Im}(\varphi_l)$ se dice que la resolución es *minimal*.

Es conocido que la resolución minimal es única salvo isomorfismo:

Teorema 1.4.2 [11, Thm. 1.6]**.** *Sea M un R-módulo graduado finitamente generado. Si F y G son resoluciones libres graduadas minimales de M, entonces existe un isomorfismo entre ambas resoluciones $F \to G$ que induce la aplicación identidad en M. Además, cualquier resolución libre de M contiene una resolución libre minimal como sumando directo.*

En el caso del anillo de polinomios tenemos el siguiente resultado debido a Hilbert.

Teorema 1.4.3 (Teorema de las Sizigias de Hilbert Graduado, [8, Chapter 6, Thm. 3.8])**.** *Sea $S = K[x_1, \ldots, x_n]$. Entonces cualquier S-módulo graduado finitamente generado tiene una resolución libre graduada finita de longitud a lo sumo n.*

Desde el punto de vista computacional, es posible construir resoluciones de un S-módulo M mediante el uso de bases de Gröbner para calcular módulos de sizigias. En este sentido, un resultado debido a Schreyer ([8, Chapter 5, Thm. 3.3]) nos permite obtener una resolución finita (en general no minimal) de un S-módulo mediante el cálculo de una única base de Gröbner. Si lo que nos interesa es una resolución minimal, existen métodos para extraer la resolución minimal a partir de una resolución que obtengamos. Así que podemos construir resoluciones de S-módulos, pero es un proceso computacionalmente costoso, a pesar del resultado de Schreyer.

La resolución minimal de un S-módulo M nos proporciona mucha información sobre M. Una forma de organizarla especialmente útil es la que se conoce como *diagrama de Betti*, que vamos a presentar a continuación. Sea
$$0 \longrightarrow F_s \longrightarrow \cdots \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$
la resolución libre minimal del S-módulo M finitamente generado, donde $F_i = \bigoplus_j S(-j)^{\beta_{i,j}}$ para cada i; es decir, F_i está generado por $\beta_{i,j}$ elementos de grado j. Los $\beta_{i,j}$ se llaman los *números de Betti graduados* de M, a veces escritos como $\beta_{i,j}(M)$. Estos números se presentan habitualmente en una tabla, conocida como *diagrama de Betti*, que tiene la siguiente forma:

	0	1	$\cdots$	s
i	$\beta_{0,i}$	$\beta_{1,i+1}$	$\cdots$	$\beta_{s,i+s}$
$i+1$	$\beta_{0,i+1}$	$\beta_{1,i+2}$	$\cdots$	$\beta_{s,i+s+1}$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
j	$\beta_{0,j}$	$\beta_{1,j+1}$	$\cdots$	$\beta_{s,j+s}$

Consiste en una tabla con $s+1$ columnas, etiquetadas de 0 a s, correspondientes a los módulos libres $F_0, \ldots, F_s$. Las filas están denotadas por enteros consecutivos que corresponden a los grados. Es habitual escribir - en vez de 0 en la tabla, y en ocasiones se omiten las etiquetas de las filas y las columnas cuando están claros por el contexto. La columna m-ésima nos da los grados de los generadores de F_m.

Observación 1.4.4. Es importante notar que la entrada correspondiente a la columna j y fila i es $\beta_{i,i+j}$ y no $\beta_{i,j}$.

Ejemplo 1.4.5. Consideramos la resolución minimal del ideal $I = \langle x^2, xy, xz, y^3 \rangle \subset S = \mathbb{Q}[x, y, z]$

$$0 \longrightarrow F_2 = S(-4) \xrightarrow{\varphi_2} F_1 = S(-3)^3 \bigoplus S(-4) \xrightarrow{\varphi_1} F_0 = S(-2)^3 \bigoplus S(-3) \xrightarrow{\varphi_0} I \longrightarrow 0.$$

A partir de la resolución minimal construimos el siguiente diagrama de Betti:

	0	1	2
2	3	3	1
3	1	1	-

Directamente a partir de la tabla podemos obtener algunos invariantes importantes:

Definición 1.4.6. Sea M un S-módulo finitamente generado (que admite una resolución finita por ser S un anillo de polinomios). A la menor longitud de todas las resoluciones libres finitas de M se la llama *dimensión proyectiva* de M y la denotaremos por $\mathrm{pd}(M)$. Esto coincide con la longitud de la resolución minimal por el teorema 1.4.2.

Podemos leer la dimensión proyectiva a partir del diagrama de Betti como el ancho de la tabla del diagrama de Betti, es decir, la etiqueta de la última columna. Esto se puede escribir como

$$\mathrm{pd}(M) = \mathrm{máx}\{i : \beta_{i,j}(M) \neq 0 \text{ para algún } j\}.$$

Definición 1.4.7. Sea M un S-módulo finitamente generado y $\beta_{i,j}(M)$ sus números de Betti. Entonces la *regularidad de Castelnuovo-Mumford* de M es

$$\mathrm{reg}(M) = \mathrm{máx}\{j - i : \beta_{i,j}(M) \neq 0\}.$$

Vemos que la regularidad también podemos leerla a partir del diagrama de Betti, en este caso fijándonos en la altura de la tabla o la etiqueta de la última fila.

Por otro lado, la dimensión proyectiva y la regularidad son dos medidas de la complejidad de un módulo. El Teorema de las Sizigias de Hilbert proporciona una cota bastante buena para la dimensión proyectiva, pero la regularidad no la tenemos tan acotada. Por ello la regularidad ha sido un invariante interesante para estudiar en álgebra conmutativa, como se puede ver en [24] por ejemplo.

Ejemplo 1.4.8. A partir del diagrama de Betti del ejemplo 1.4.5 podemos obtener la dimensión proyectiva y la regularidad del ideal I: $\mathrm{pd}(I) = 2$, $\mathrm{reg}(I) = 3$.

De las definiciones podemos obtener fácilmente que

$$\mathrm{pd}(S/I) = \mathrm{pd}(I) + 1,$$
$$\mathrm{reg}(I) = \mathrm{reg}(S/I) + 1.$$

Esto se ve fácilmente observando que si tenemos la resolución minimal de I

$$0 \longrightarrow F_s \longrightarrow \cdots \longrightarrow F_0 \longrightarrow I \longrightarrow 0,$$

entonces obtenemos otra resolución minimal para S/I

$$0 \longrightarrow F_s \longrightarrow \cdots \longrightarrow F_0 \longrightarrow S \longrightarrow S/I \longrightarrow 0,$$

y viceversa.

Entre la dimensión proyectiva y la profundidad hay una relación importante que viene dada por la siguiente fórmula:

Teorema 1.4.9 (Fórmula de Auslander-Buchsbaum, [10, Thm. 19.9 & Ex. 19.8])**.** *Sea $R = R_0 \oplus R_1 \oplus \cdots$ un anillo graduado, finitamente generado como álgebra sobre un cuerpo R_0. Sea $P = R_1 \oplus R_2 \oplus \cdots$ el ideal homogéneo maximal. Si M es un R-módulo graduado finitamente generado de dimensión proyectiva finita, entonces*

$$\mathrm{pd}(M) = \mathrm{depth}(P, R) - \mathrm{depth}(P, M) = \mathrm{depth}(R) - \mathrm{depth}(M).$$

En el caso del anillo de polinomios $S = k[x_1, \ldots, x_n]$ la fórmula se reduce a

$$\mathrm{pd}(M) = n - \mathrm{depth}(M).$$

Por tanto, podemos obtener $\mathrm{depth}(M)$ a partir de $\mathrm{pd}(M)$. Este último invariante sabemos obtenerlo a partir del diagrama de Betti, luego también podemos obtener $\mathrm{depth}(M)$ de la tabla.

Ejemplo 1.4.10. Considerando los datos del ejemplo 1.4.8, puesto que el número de variables es 3 y $\mathrm{pd}(S/I) = 3$, tenemos que $\mathrm{depth}(S/I) = 0$.

1.5. Función de Hilbert

Consideramos el anillo de polinomios $S = K[x_1, \ldots, x_n]$, el anillo de polinomios en n variables sobre un cuerpo K. Vamos a recordar los conceptos de función, polinomio y serie de Hilbert de un S-módulo M, así como ver su relación con algunos invariantes del módulo M. Como referencias, utilizaremos principalmente [4], [8] y [28].

Definición 1.5.1. Si M es un módulo graduado finitamente generado sobre $S = K[x_1, \ldots, x_n]$, entonces la *función de Hilbert* $H_M(d)$ está definida por

$$H_M(d) = \dim_K M_d,$$

donde $\dim_K$ es la dimensión como espacio vectorial sobre K (es fácil comprobar que M_d es un espacio vectorial sobre K de dimensión finita). Cuando consideremos $M = S/I$, siendo I un ideal de S, escribiremos $H_I(d)$ para denotar a la función de Hilbert de S/I.

Ejemplo 1.5.2. Para $S = K[x_1, \ldots, x_n]$ y $d \geq 0$

$$H_S(d) = \dim_K S_d = \binom{d+n-1}{n-1}.$$

Si convenimos que $\binom{a}{b} = 0$ si $a < b$, entonces la fórmula anterior se da para todo t.

La función de Hilbert es aditiva en sucesiones exactas cortas:

Proposición 1.5.3. *Sean M, N y P S-módulos finitamente generados. Si tenemos una sucesión exacta*

$$0 \longrightarrow M \xrightarrow{\alpha} P \xrightarrow{\beta} N \longrightarrow 0$$

donde α y β son homomorfismos graduados, entonces $H_P = H_M + H_N$.

Demostración. De la sucesión exacta anterior se deduce otra sucesión exacta entre K-espacios vectoriales de dimensión finita

$$0 \longrightarrow M_d \xrightarrow{\alpha_d} P_d \xrightarrow{\beta_d} N_d \longrightarrow 0$$

donde α_d y β_d son las restricciones a los elementos homogéneos de grado d del espacio de salida de cada homomorfismo. El resultado se obtiene teniendo en cuenta la fórmula

$$\dim_K P_d = \dim_K \ker(\beta_d) + \dim_K \operatorname{Im}(\beta_d).$$

□

Teorema 1.5.4 [8, Chapter 6, Thm. 4.4]**.** *Sea $S = K[x_1, \ldots, x_n]$ y sea M un S-módulo graduado finitamente generado. Entonces, para cualquier resolución graduada de M*

$$0 \longrightarrow F_k \longrightarrow F_{k-1} \longrightarrow \cdots \longrightarrow F_0 \longrightarrow M \longrightarrow 0,$$

tenemos

$$H_M(d) = \dim_k M_d = \sum_{j=0}^{k} (-1)^j \dim_k (F_j)_d = \sum_{j=0}^{k} (-1)^j H_{F_j}(d).$$

Demostración. Como en la proposición 1.5.3, obtenemos una sucesión exacta de K-espacios vectoriales de dimensión finita

$$0 \longrightarrow (F_k)_d \xrightarrow{\varphi_k} (F_{k-1})_d \xrightarrow{\varphi_{k-1}} \cdots \xrightarrow{\varphi_1} (F_0)_d \xrightarrow{\varphi_0} M_d \longrightarrow 0.$$

Para una sucesión exacta de espacios vectoriales como la anterior se cumple que $\sum_{j=0}^{k}(-1)^{j+1}\dim_K(F_j)_d + \dim_K M_d = 0$ (la suma alternada de las dimensiones es 0). Por tanto,

$$\dim_K M_d = \sum_{j=0}^{k}(-1)^j \dim_K(F_j)_d.$$

□

Teorema 1.5.5 [8, Chapter 6, Prop. 4.7]**.** *Sea $S = K[x_1, \ldots, x_n]$ y M un S-módulo graduado finitamente generado. Entonces existe un único polinomio HP_M tal que*

$$H_M(d) = HP_M(d)$$

para todo d suficientemente grande.

Demostración. Por 1.5.3, para un módulo libre desplazado de la forma

$$F = S(-e_1) \oplus \cdots \oplus S(-e_m),$$

la función de Hilbert es

$$H_F(d) = \sum_{i=1}^{m} \binom{d - e_i + n - 1}{n - 1}.$$

Vemos que es un polinomio para d suficientemente grande ($d \geq \text{máx}(e_1, \ldots, e_m)$). Se concluye observando que todo S-módulo finitamente generado admite una resolución libre graduada finita y usando 1.5.4. □

El polinomio $HP_M(d)$ del teorema anterior se conoce como *polinomio de Hilbert* de M. Si consideramos un S-módulo de la forma $M = S/I$, siendo I un ideal homogéneo de S, escribiremos $HP_I(d)$ para denotar al polinomio de Hilbert de S/I. En esta situación, resulta que el grado d del polinomio de Hilbert de S/I coincide con la dimensión de Krull de S/I menos 1 (es decir, nos daría la dimensión de la variedad proyectiva que define el ideal). Esto se puede ver en más detalle en [4, Chapter 4].

Definición 1.5.6. Sea $k = \dim S/I$ la dimensión de Krull de S/I, y sea c_{k-1} el coeficiente de d^{k-1} en el polinomio de Hilbert de S/I. Si $k \geq 1$, entonces llamamos a $c_{k-1}(k-1)!$ el *grado* de S/I y lo denotamos por $\deg(S/I)$. Si $k = 0$, entonces $\deg(S/I) = \dim_K(S/I)$.

Observación 1.5.7. Denotando $k = \dim S/I$, el grado se puede expresar como

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

Lema 1.5.8. *Sea $I \subset S$ un ideal generado por formas lineales. Entonces S/I es isomorfo a un anillo de polinomios. En particular,* $\deg(S/I) = 1$.

Demostración. Si $I = \langle f_1, \ldots, f_r \rangle$, con $f_i \in S_1$, $i = 1, \ldots, r$, y linealmente independientes, entonces podemos encontrar un cambio de variables que envíe $f_i \mapsto x_i$. Este cambio nos da un automorfismo del anillo de polinomios S, de manera que obtenemos $S/I \cong S/(x_1, \ldots, x_r) \cong K[x_{r+1}, \ldots, x_n]$. Pero sabemos que $\dim_K(K[x_{r+1}, \ldots, x_n]_d) = \binom{n-r+d-1}{d}$, así que $\deg(S/I) = \deg(K[x_{r+1}, \ldots, x_n]) = 1$. □

Definición 1.5.9. El *índice de regularidad* de S/I, denotado por $\mathrm{ri}(S/I)$, es el menor entero $r \geq 0$ tal que $H_I(d) = HP_I(d)$ para $d \geq r$.

Observación 1.5.10. Si $I \subset S$ es un ideal homogéneo Cohen-Macaulay de dimensión 1, entonces $\mathrm{reg}(S/I)$, la regularidad de Castelnuovo-Mumford de S/I, es igual a $\mathrm{ri}(S/I)$, el índice de regularidad de S/I (ver [11, Cor. 4.8]). En este caso, llamaremos a ambos invariantes regularidad de S/I y los denotaremos por $\mathrm{reg}(S/I)$.

Definición 1.5.11. Sea $M = \oplus_{d=0}^{\infty} M_d$ un S-módulo graduado finitamente generado por elementos de grado positivo. La serie de potencias formal

$$HS_M(t) = \sum_{d=0}^{\infty} H_M(d)t^d = \sum_{d=0}^{\infty} \dim_K M_d t^d.$$

se llama *serie de Hilbert* de M. De nuevo, si $M = S/I$, con $I \subset S$ un ideal homogéneo, entonces denotaremos por $HS_I(t)$ a la serie de Hilbert de S/I.

Si consideramos la graduación estándar en el anillo de polinomios $S = K[x_1, \ldots, x_n]$ (es decir, $\deg(x_i) = 1$, $i = 1, \ldots, n$), tenemos el siguiente resultado.

Teorema 1.5.12 (Teorema de Hilbert-Serre, [28, Thm. 5.1.4])**.** *Sea $M = \oplus_{d=0}^{\infty} M_d$ un S-módulo graduado finitamente generado de dimensión ρ. Existe un único polinomio $h(t) \in \mathbb{Z}[t]$ tal que*

$$HS_M(t) = \frac{h(t)}{(1-t)^{\rho}}$$

y $h(1) \neq 0$.

Observación 1.5.13. Por el teorema 1.5.12 podemos escribir:

$$HS_M(t) = \frac{h(t)}{(1-t)^{\rho}} = h(t)\left(1 + \rho t + \cdots + \binom{d+\rho-1}{\rho-1}t^d + \cdots\right),$$

donde $\binom{d+\rho-1}{\rho-1} = 0$ si $d < 0$. Si $h(t) = \sum_{i=0}^{l} a_i t^i$, entonces el coeficiente de t^d en $HS_M(t)$ es

$$H_M(d) = \sum_{i=0}^{l} a_i \binom{d-i+\rho-1}{\rho-1}.$$

De nuevo vemos que para d suficientemente grande, $H_M(d)$ es un polinomio. En particular, si $M = S/I$, el coeficiente líder del polinomio de Hilbert $HP_I(t)$ es igual a $h(1)/(\rho-1)!$, así que $h(1) = \deg(S/I)$.

Definición 1.5.14. Sea $I \subset S$ un ideal homogéneo. El *a-invariante* del anillo graduado S/I, denotado por $a(S/I)$, es el grado de $HS_I(t)$ como función racional, es decir, $a(S/I) = \deg(h(t)) - \rho$.

El a-invariante, la regularidad de Castelnuovo-Mumford y la profundidad de M están estrechamente relacionadas.

Teorema 1.5.15 [27, Cor. B.4.1]**.** *$a(M) \leq \operatorname{reg}(M) - \operatorname{depth}(M)$, con igualdad si M es Cohen-Macaulay.*

Lema 1.5.16 [28, Ex. 5.1.20]**.** *Si $I \subset S$ es un ideal generado por polinomios homogéneos $f_1, \ldots, f_r$, con $r = \operatorname{ht}(I)$ y $\delta_i = \deg(f_i)$, entonces la serie de Hilbert de S/I viene dada por*

$$HS_I(t) = \frac{\prod_{i=1}^{r}(1 - x^{\delta_i})}{(1-x)^n}.$$

Lema 1.5.17 [22, Lem. 2.11]**.** *Si $I \subset S$ es un ideal que es una intersección completa y está generado por polinomios homogéneos $f_1, \ldots, f_r$, con $r = \operatorname{ht}(I)$ y $\delta_i = \deg(f_i)$, entonces el grado y la regularidad de S/I vienen dados por $\deg(S/I) = \delta_1 \cdots \delta_r$ y $\operatorname{reg}(S/I) = \sum_{i=1}^{r}(\delta_i - 1)$.*

Demostración. La fórmula para el grado se deduce de la observación 1.5.13 y el lema 1.5.16. Por otro lado, S/I es Cohen-Macaulay por 1.3.12, así que la fórmula para la regularidad se deduce del teorema 1.5.15 y el lema 1.5.16. □

Lema 1.5.18 [18, Cor. 5.1.20]**.** *Sea M un S-módulo finitamente generado, y sea $K \subset L$ una extensión de cuerpos. Entonces tenemos que $H_M(i) = H_{M \otimes_K L}(i)$ para todo $i \in \mathbb{Z}$.*

Teorema 1.5.19 [23, Thm. 1.5.25]**.** *Sea $I \subset S$ un ideal homogéneo. Si $\operatorname{depth}(S/I) > 0$, y H_I es la función de Hilbert de S/I, entonces $H_I(i) \leq H_I(i+1)$ para $i \geq 0$.*

Demostración. Si K es infinito, por la proposición 1.2.6, existe $h \in S_1$ que es un no divisor de cero en S/I. El homomorfismo de K-espacios vectoriales

$$(S/I)_i \to (S/I)_{i+1},\ \bar{z} \mapsto \overline{hz}$$

es inyectivo, por lo que $H_I(i) = \dim_K(S/I)_i \leq \dim_K(S/I)_{i+1} = H_I(i+1)$.

Si K es finito, consideramos la clausura algebraica $\overline{K}$ de K. Denotamos $\overline{S} = S \otimes_K \overline{K} \cong \overline{K}[x_1, \ldots, x_n]$ e $\overline{I} = I\overline{S}$. Entonces $(S/I) \otimes_K \overline{K} \cong \overline{S}/\overline{I}$, así que por el lema 1.5.18 tenemos que $H_I(i) = H_{\overline{I}}(i)$. Aplicando el caso previo a $H_{\overline{I}}(i)$ obtenemos el resultado. □

Lema 1.5.20 [23, Lem. 1.5.26]**.** *Sea $I \subset S$ un ideal homogéneo. Se tiene lo siguiente:*

(a) *Si $S_i = I_i$ para algún i, entonces $S_l = I_l$ para todo $l \geq i$.*

(b) *Si $\dim(S/I) \geq 2$, entonces $\dim_K(S/I)_i > 0$ para todo $i \geq 0$.*

Demostración.

(a) Es suficiente probarlo para el caso $l = i+1$. Puesto que $I_{i+1} \subset S_{i+1}$, basta con ver que $S_{i+1} \subset I_{i+1}$. Sea $x^\alpha \in S_{i+1}$ un monomio no nulo. Entonces existe un j tal que $x_j \mid x^\alpha$. En consecuencia, $x^\alpha \in S_1 S_i = S_1 I_i \subset I_{i+1}$.

(b) Si $\dim_K(S/I)_i = 0$ para algún i, entonces $S_i = I_i$. En consecuencia, $H_I(j) = 0$ para todo $j \geq i$, por lo que su polinomio de Hilbert sería constante igual a 0. Esto es una contradicción porque el grado del polinomio de Hilbert es $\dim(S/I) - 1 \geq 1$.

□

Teorema 1.5.21 ([6, Thm. 2.9], [23, Thm. 1.5.27])**.** *Sea $I \subset S$ un ideal homogéneo con* $\operatorname{depth}(S/I) > 0$*. Se da lo siguiente.*

(a) *Si* $\dim(S/I) \geq 2$*, entonces $H_I(i) < H_I(i+1)$ para $i \geq 0$.*

(b) *Si* $\dim(S/I) = 1$*, entonces existe un entero r y una constante c tal que:*

$$1 = H_I(0) < H_I(1) < \cdots < H_I(r-1) < H_I(i) = c \text{ para } i \geq r.$$

Demostración. Como en la demostración del teorema 1.5.19, podemos usar el lema 1.5.18 y suponer que K es infinito. Por la proposición 1.2.6 existe $h \in S_1$ que es un no divisor de cero en S/I. De la sucesión exacta

$$0 \longrightarrow (S/I)[-1] \xrightarrow{h} S/I \longrightarrow S/(I,h) \longrightarrow 0,$$

deducimos que $H_I(i+1) = H_I(i) + H_M(i+1)$ (por 1.5.3), donde $M = S/(I,h)$. Sea $r \geq 0$ el primer entero tal que $H_I(r) = H_I(r+1)$. Por la igualdad anterior, tenemos que $H_M(r+1) = 0$, luego $M_{r+1} = (0)$ (el módulo 0) y $S_{r+1} = (I,h)_{r+1}$. Por el lema 1.5.20, $M_k = (0)$ para $k \geq r+1$. Luego hemos visto que en el primer momento en que se de la igualdad $H_I(r) = H_I(r+1)$, la función de Hilbert debe ser constante.

Para el caso (a), vemos que no puede darse nunca $H_I(r) = H_I(r+1)$, porque entonces la función de Hilbert sería constante para valores suficientemente grandes, por lo que el polinomio de Hilbert sería de grado 0 (ver teorema 1.5.5), en contradicción con que $\dim(S/I) \geq 2$.

Para el caso (b), como $\dim(S/I) = 1$, la función de Hilbert debe ser constante para valores suficientemente grandes porque el polinomio de Hilbert es de grado 0. En consecuencia, la función de Hilbert de S/I es constante para $k \geq r$ y estrictamente creciente para $0 \leq k \leq r-1$. □

Lema 1.5.22 [6, Lem. 2.10]**.** *Sean $I \subset J \subset S$ ideales homogéneos de la misma altura. Se tiene lo siguiente:*

(1) *Si I y J son no mezclados, entonces $I = J$ si y solo si* $\deg(S/I) = \deg(S/J)$.

(2) *Si* $I \subsetneq J$, *entonces* $\deg(S/I) > \deg(S/J)$.

El siguiente resultado se conoce habitualmente como *aditividad del grado*, y lo vamos a utilizar frecuentemente, tanto en la forma siguiente como en la de la consecuencia que vamos a ver.

Proposición 1.5.23 [16, Lem. 5.3.11]**.** *Sea* $I \subset S$ *un ideal homogéneo y sea* $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$ *su descomposición primaria irredundante. Entonces*

$$\deg(S/I) = \sum_{\mathrm{ht}(\mathfrak{q}_i)=\mathrm{ht}(I)} \deg(S/\mathfrak{q}_i).$$

Lema 1.5.24 [14, Lem. 3.3]**.** *Sea* $I \subset S$ *un ideal homogéneo radical no mezclado. Si* $F = \{f_1, \ldots, f_r\}$ *es un conjunto de polinomios homogéneos de* $S \setminus \{0\}$, $(I : (F)) \neq I$, *y* $\mathcal{A}$ *es el conjunto de los primos asociados de* S/I *que contienen a* F, *entonces* $\mathrm{ht}(I) = \mathrm{ht}(I, F)$, $\mathcal{A} \neq \emptyset$ *y*

$$\deg(S/(I, F)) = \sum_{\mathfrak{p} \in \mathcal{A}} \deg(S/\mathfrak{p}).$$

Demostración. Puesto que $I \neq (I : (F))$, existe un $g \in S \setminus I$ tal que $g(F) \subset I$. Por tanto, el ideal (F) está contenido en el conjunto de divisores de cero de S/I. Por el teorema 1.2.3, y teniendo en cuenta que I es no mezclado, obtenemos que (F) está contenido en un primo asociado $\mathfrak{p}$ de S/I de altura $\mathrm{ht}(I)$. En consecuencia, $I \subset (I, F) \subset \mathfrak{p}$, por lo que $\mathrm{ht}(I) = \mathrm{ht}(I, F)$. Así que el conjunto de los primos asociados de (I, F) de altura igual a $\mathrm{ht}(I)$ es no vacío e igual a $\mathcal{A}$. Entonces tenemos una descomposición primaria irredundante

$$(I, F) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r \cap \mathfrak{q}'_{r+1} \cap \cdots \cap \mathfrak{q}'_t, \tag{1.5.1}$$

donde $\sqrt{\mathfrak{q}_i} = \mathfrak{p}_i$, $\mathcal{A} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$, y $\mathrm{ht}(\mathfrak{q}'_i) > \mathrm{ht}(I)$ para $i > r$. Podemos suponer que los primos asociados de S/I son $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ con $r \leq m$. Puesto que I es radical, tenemos que $I = \cap_{i=1}^m \mathfrak{p}_i$. Ahora probamos la siguiente igualdad:

$$\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_m = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r \cap \mathfrak{q}'_{r+1} \cap \cdots \cap \mathfrak{q}'_t \cap \mathfrak{p}_{r+1} \cap \cdots \cap \mathfrak{p}_m. \tag{1.5.2}$$

La inclusión "$\supset$" es clara porque $\mathfrak{q}_\mathfrak{i} \subset \mathfrak{p}_i$ para $i = 1, \ldots, r$. La otra inclusión se obtiene teniendo en cuenta que el lado derecho de la ecuación (1.5.2) es igual a $(I, F) \cap \mathfrak{p}_{r+1} \cap \cdots \cap \mathfrak{p}_m$, y, por tanto, contiene a $I = \cap_{i=1}^m \mathfrak{p}_i$. Observamos que $\sqrt{\mathfrak{q}'_j} = \mathfrak{p}'_j \not\subset \mathfrak{p}_i$ para todo i, j, y $\mathfrak{p}_j \not\subset \mathfrak{p}_i$ para $i \neq j$. Si ahora localizamos la ecuación (1.5.2) en el ideal primo $\mathfrak{p}_i$ para $i = 1, \ldots, r$, obtenemos que $\mathfrak{p}_i = I_{\mathfrak{p}_i} \cap S = (\mathfrak{q}_i)_{\mathfrak{p}_i} \cap S = \mathfrak{q}_i$ para $i = 1, \ldots, r$. Usando la ecuación (1.5.1) y la aditividad del grado (proposición 1.5.23) se obtiene el resultado. □

Vemos que el cálculo de la dimensión, grado, a-invariante o índice de regularidad se puede reducir a calcular la serie de Hilbert de S/I. Para ello, podemos utilizar sistemas de álgebra computacional como [9] o [12]. A partir de una resolución libre

graduada se puede obtener la función de Hilbert, y, en consecuencia, la serie de Hilbert, mediante el cálculo de una base de Gröbner (usando el teorema de Schreyer, [8, Chapter 5, Thm. 3.3]). También existen métodos de cálculo para obtener directamente la serie de Hilbert (ver [16], [18]). Para algunos invariantes, como la regularidad de Castelnuovo-Mumford o la profundidad, existen métodos de cálculo que no requieren pasar por la construcción de la resolución o de la serie de Hilbert (ver [3], [24]).

1.6. Huella de un ideal

En esta sección vamos a revisar algunos resultados básicos y definiciones de bases de Gröbner y huella de un ideal. Las referencias principales que utilizaremos son [7] y [10]. También incluimos resultados de [14] y [23].

Consideramos el anillo de polinomios $S = K[x_1, \ldots, x_n]$ sobre un cuerpo K, y denotamos por $\mathcal{M}$ al conjunto de monomios en S. Vamos a denotar a los monomios de $\mathcal{M}$ por x^α, con $\alpha \in \mathbb{Z}^n_{\geq 0}$.

Definición 1.6.1. Un orden total $\prec$ en $\mathcal{M}$ se llama *orden monomial* si

(a) $1 \preceq x^\alpha$ para todo $x^\alpha \in \mathcal{M}$, y

(b) si $x^\alpha, x^\beta \in \mathcal{M}$, $x^\alpha \preceq x^\beta$ implica $x^\alpha x^\gamma \preceq x^\beta x^\gamma$ para todo $x^\gamma \in \mathcal{M}$.

Ejemplo 1.6.2. Sea $S = K[x_1, \ldots, x_n]$ el anillo de polinomios sobre un cuerpo K.

(a) El *orden lexicográfico* con $x_n \prec \cdots \prec x_1$ se define por $x^\alpha \prec x^\beta$ si la primera entrada no nula de izquierda a derecha de $\beta - \alpha$ es positiva.

(b) El *orden lexicográfico inverso graduado* con $x_n \prec \cdots \prec x_1$ se define por $x^\alpha \prec x^\beta$ si $\sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i$, o si $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$ y la primera entrada no nula de derecha a izquierda de $\beta - \alpha$ es negativa.

Definición 1.6.3. Sea $\prec$ un orden monomial en S y sea $(0) \neq I \subset S$ un ideal. Si f es un polinomio no nulo en S, podemos escribir

$$f = a_1 x^{\alpha_1} + \cdots + a_r x^{\alpha_r},$$

con $a_i \in K^*$ para todo i y $x^{\alpha_1} \succ \cdots \succ x^{\alpha_r}$.

- El *monomio líder* de f es x^{α_1} y se denota por $\mathrm{in}_\prec(f)$.
- El *coeficiente líder* de f es a_1 y se denota por $\mathrm{lc}_\prec(f)$.
- El *término líder* de f es $a_1 x^{\alpha_1}$ y se denota por $\mathrm{lt}_\prec(f)$.
- El *ideal inicial* de I, denotado por $\mathrm{in}_\prec(I)$, es el ideal monomial

$$\mathrm{in}_\prec(I) = (\{\mathrm{in}_\prec(f) \mid f \in I\}).$$

Podemos escribir $\mathrm{in}(f)$, $\mathrm{lc}(f)$, $\mathrm{lt}(f)$ e $\mathrm{in}(I)$ omitiendo la mención al orden monomial $\prec$ si no hay confusión, aunque en general sí explicitaremos el orden monomial.

Teorema 1.6.4 (Algoritmo de división, [7, Thm. 3, Chapter 2])**.** *Sea $\prec$ un orden monomial en $\mathcal{M}$, y sea $F = (f_1, \ldots, f_s)$ una s-upla ordenada de polinomios en $K[x_1, \ldots, x_n]$. Entonces cualquier $f \in K[x_1, \ldots, x_n]$ se puede escribir como*

$$f = q_1 f_1 + q_2 f_2 + \cdots + q_s f_s + r,$$

donde $q_i, r \in K[x_1, \ldots, x_n]$, y $r = 0$ o r es combinación lineal, con coeficientes en K, de monomios, ninguno de los cuales es divisible por ninguno de los monomios $\mathrm{in}_\prec(f_1), \ldots, \mathrm{in}_\prec(f_s)$. A r se le llama resto de la división. Además, si $q_i f_i \neq 0$, entonces $\mathrm{in}_\prec(f) \succeq \mathrm{in}_\prec(q_i f_i)$.

Definición 1.6.5. Un subconjunto $\mathcal{G} = \{g_1, \ldots, g_r\}$ de I se llama una *base de Gröbner* de I si

$$\mathrm{in}_\prec(I) = (\mathrm{in}_\prec(g_1), \ldots, \mathrm{in}_\prec(g_r)).$$

Observación 1.6.6. Fijado un orden monomial, cualquier ideal distinto de (0) admite una base de Gröbner, y cualquier base de Gröbner de un ideal I es un sistema de generadores de I.

Definición 1.6.7. Sea $I \subset S$ un ideal.

- La *huella* de I (con respecto a un orden monomial $\prec$ en $\mathcal{M}$) es el conjunto

$$\Delta_\prec(I) = \{x^\alpha \in \mathcal{M} \mid x^\alpha \notin \mathrm{in}_\prec(I)\}.$$

- Los elemento de $\Delta_\prec(I)$ se llaman *monomios estándar* de I.
- Un polinomio f se llama *estándar* si $f \neq 0$ y f es una combinación K-lineal de monomios estándar.

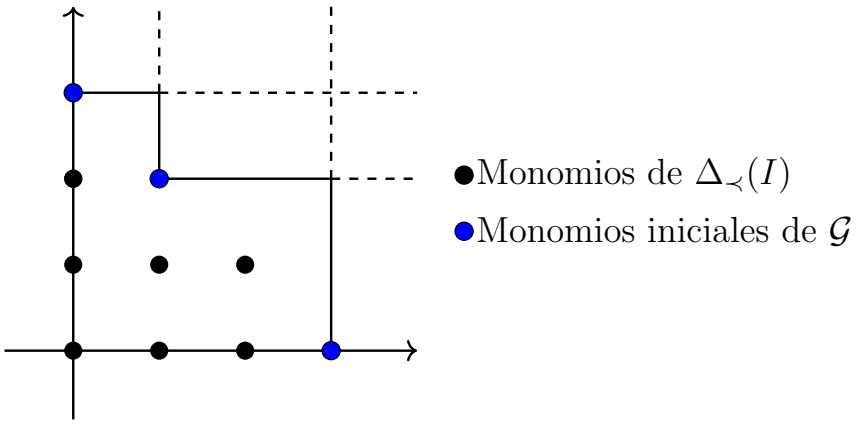
Por el algoritmo de división 1.6.4, cualquier clase de equivalencia de S/I admite un representante que es un polinomio estándar.

Proposición 1.6.8. *Sea $I \subset S$ un ideal y $\prec$ un orden monomial. El conjunto $\Delta_\prec(I)$ forma una base (como K-espacio vectorial) de S/I.*

Proposición 1.6.9 [7, Prop. 9, Chapter 9]**.** *Sea I un ideal homogéneo y sea $\prec$ un ideal monomial sobre S. Entonces el ideal inicial $\mathrm{in}_\prec(I)$ tiene la misma función de Hilbert que I.*

Ambos resultados son consecuencia de dos resultados más generales debidos a Macaulay ([10, Thm. 15.3] y [10, Thm. 15.26], también se pueden ver en [24]) que generalizan lo que hemos visto en esta sección a S-módulos finitamente generados.

Ejemplo 1.6.10. Sea $I = (x^3 - x, xy^2 - x, y^3 - y) \subset \mathbb{Q}[x, y]$ y consideramos el orden monomial $\prec$ lexicográfico con $y \prec x$. Es sencillo comprobar que $\mathcal{G} = \{x^3 - x, xy^2 - x, y^3 - y\}$ es una base de Gröbner de I para el orden $\prec$. Tenemos que $\text{in}_\prec(x^3 - x) = x^3$, $\text{in}_\prec(xy^2 - x) = xy^2$, y $\text{in}_\prec(y^3 - y) = y^3$. A partir de estos iniciales podemos determinar $\Delta_\prec(I)$. Para ello, vamos a representar un monomio $x^\alpha y^\beta$ por el punto $(\alpha, \beta) \in \mathbb{N}^2$, de manera que, representando los monomios que hemos obtenido, obtenemos:



Vemos que $\Delta_\prec(I) = \{1, x, x^2, y, xy, x^2y, y^2\}$. Por la proposición 1.6.8, este conjunto forma una base como $\mathbb{Q}$-espacio vectorial de $\mathbb{Q}[x, y]/I$.

Lema 1.6.11 [23, Lem. 1.6.13]**.** *Sea $I \subset S$ un ideal generado por $\mathcal{G} = \{g_1, \ldots, g_r\}$, entonces*

$$\Delta_\prec(I) \subset \Delta_\prec(\text{in}_\prec(g_1), \ldots, \text{in}_\prec(g_r)),$$

con igualdad si $\mathcal{G}$ es una base de Gröbner.

Demostración. Sea $x^\alpha \in \Delta_\prec(I)$. Si $x^\alpha \notin \Delta_\prec(\text{in}_\prec(g_1), \ldots, \text{in}_\prec(g_r))$, entonces $x^\alpha = x^\gamma \text{in}_\prec(g_i)$ para algún i y algún $x^\gamma \in \mathcal{M}$. Así que $x^\alpha = \text{in}_\prec(x^\gamma g_i)$, con $x^\gamma g_i \in I$, lo que contradice que $x^\alpha \in \Delta_\prec(I)$. La última parte se deduce de la definición de base de Gröbner. □

Lema 1.6.12 [14, Lem. 4.7]**.** *Sea $\prec$ un orden monomial, sea $I \subset S$ un ideal, sea $F = \{f_1, \ldots, f_r\}$ un conjunto de polinomios de S de grado positivo, y sea $\text{in}_\prec(F) = \{\text{in}_\prec(f_1), \ldots, \text{in}_\prec(f_r)\}$ el conjunto de monomios iniciales de F. Si $(\text{in}_\prec(I) : (\text{in}_\prec(F))) = \text{in}_\prec(I)$, entonces $(I : (F)) = I$.*

Demostración. Sea g un polinomio de $(I : (F))$, es decir, $gf_i \in I$ para $i = 1, \ldots, r$. Es suficiente ver que $g \in I$. Sea $g_1, \ldots, g_s$ una base de Gröbner de I. Entonces, por el algoritmo de división 1.6.4 podemos escribir $g = \sum_{i=1}^s h_i g_i + h$, donde $h = 0$ o h es una suma finita de monomios que no están en $\text{in}_\prec(I) = (\text{in}_\prec(g_1), \ldots, \text{in}_\prec(g_s))$. Habremos terminado si probamos que $h = 0$. Si $h \neq 0$, entonces hf_i está en I,

así que $\text{in}_\prec(hf_i) = \text{in}_\prec(h)\,\text{in}_\prec(f_i)$ está en el ideal $\text{in}_\prec(I)$ para $i = 1, \ldots, r$. En consecuencia, $\text{in}_\prec(h)$ está en $(\text{in}_\prec(I) : (\text{in}_\prec(F)))$. Por hipótesis, $\text{in}_\prec(h)$ está en $\text{in}_\prec(I)$, una contradicción. □

Lema 1.6.13 [23, Lem. 1.6.15]**.** *Sea $\mathcal{G} = \{g_1, \ldots, g_r\}$ una base de Gröbner de I. Si para algún i, la variable x_i no divide a $\text{in}_\prec(g_j)$ para todo j, entonces x_i es un elemento regular en S/I.*

Demostración. Supongamos que $x_i f \in I$. Por el algoritmo de división 1.6.4 podemos escribir $f = g + h$, donde $g \in I$ y h es 0 o un polinomio estándar. Queremos ver que entonces $f \in I$, así que es suficiente ver que $h = 0$. Si $h \neq 0$, entonces $x_i\,\text{in}_\prec(h) \in \text{in}_\prec(I)$. En consecuencia, por las hipótesis sobre x_i, obtenemos que $\text{in}_\prec(h) \in \text{in}_\prec(I)$, una contradicción. □

Este lema nos dice que si x_i es un divisor de cero en S/I para todo i, entonces cualquier variable x_i debe aparecer en algún monomio $\text{in}_\prec(g_j)$ para algún j.

1.7. Ideal de anulación de un conjunto finito de puntos

En esta sección vamos a estudiar algunas propiedades sobre los ideales de anulación de conjuntos finitos de puntos que vamos a necesitar más adelante. Como referencias, utilizamos principalmente [18] y [23].

Definición 1.7.1. Sea K un cuerpo. Definimos el *espacio proyectivo* de dimensión $n-1$ sobre K, denotado por $\mathbb{P}^{n-1}_K$ o $\mathbb{P}^{n-1}$ si no hay confusión sobre K, como el espacio cociente

$$(K^n \setminus \{0\})/\sim$$

donde dos puntos α, β en $K^n \setminus \{0\}$ son equivalentes bajo $\sim$ si $\alpha = c\beta$ para algún $c \in K$. Es habitual denotar la clase de equivalencia de α por $[\alpha]$.

Definición 1.7.2. Sea $\mathbb{X}$ un subconjunto de $\mathbb{P}^{n-1}$.

- El *ideal de anulación* de $\mathbb{X}$, denotado por $I(\mathbb{X})$, es el ideal homogéneo generado por los polinomios homogéneos en S que se anulan en todos los puntos de $\mathbb{X}$.
- Para un ideal homogéneo $I \subset S$ definimos su *conjunto de ceros* relativo a $\mathbb{X}$ como
$$V_{\mathbb{X}}(I) = \{[\alpha] \in \mathbb{X} \mid f(\alpha) = 0, \forall f \in I \text{ homogéneo}\}.$$
- Si $f \in S$ es homogéneo, el *conjunto de ceros* de f, denotado por $V_{\mathbb{X}}(f)$, es el conjunto de todos los $[\alpha] \in \mathbb{X}$ tales que $f(\alpha) = 0$.

Lema 1.7.3 [18, Cor. 6.3.19]**.** *Sea $[\alpha] \in \mathbb{P}^{n-1}$ con $\alpha = (\alpha_1, \ldots, \alpha_n)$ y sea $I_{[\alpha]}$ su ideal de anulación. Entonces se tiene que*

$$I_{[\alpha]} = (\{\alpha_i x_j - \alpha_j x_i \mid 0 \leq i < j \leq n\}).$$

Observación 1.7.4. En el lema anterior, debe ser $\alpha_k \neq 0$ para algún k. En ese caso, podemos expresar el ideal como

$$I_{[\alpha]} = (\{x_i - \frac{\alpha_i}{\alpha_k} x_k \mid i = 1, \ldots, n, i \neq k\}).$$

Corolario 1.7.5. *Se tiene que* $I_{[\alpha]}$ *es un ideal primo,* $\deg(S/I_{[\alpha]}) = 1$ *y* $\mathrm{ht}(I_{[\alpha]}) = n - 1$.

Demostración. Por la expresión que hemos visto en la observación 1.7.4 vemos que $S/I_{[\alpha]} \cong K[x_k]$ (es un caso particular de 1.5.8). Así que tenemos automáticamente que $I_{[\alpha]}$ es un ideal primo porque el cociente es un dominio de integridad, $\deg(S/I_{[\alpha]}) = 1$ por ser isomorfo a un anillo de polinomios, y $\mathrm{ht}(I_{[\alpha]}) = n-1$ porque la altura y la codimensión coinciden para un ideal primo en el anillo de polinomios S por ser Cohen-Macaulay. □

Observación 1.7.6. Si tenemos un subconjunto finito $\mathbb{X} \subset \mathbb{P}^{n-1}$, entonces tenemos

$$I(\mathbb{X}) = \bigcap_{[\beta] \in \mathbb{X}} I_{[\beta]}.$$

En efecto, un polinomio está en $I(\mathbb{X})$ si y solo si se anula en todos sus puntos. Como cada $I_{[\beta]}$ es primo, la expresión anterior es, de hecho, la descomposición primaria de $I(\mathbb{X})$.

Corolario 1.7.7. *Si* $\mathbb{X} \subset \mathbb{P}^{n-1}$ *es un conjunto finito, entonces* $\deg(S/I(\mathbb{X})) = |\mathbb{X}|$.

Demostración. Se deduce de la observación 1.7.6 y la proposición 1.5.23. □

Si $\mathbb{X}$ es un subconjunto de $\mathbb{P}^{n-1}$ es habitual denotar a la función de Hilbert de $S/I(\mathbb{X})$ por $H_{\mathbb{X}}$.

Proposición 1.7.8 [18, Thm. 6.3.23]**.** *Si* $\mathbb{X} \subset \mathbb{P}^{n-1}$ *es un conjunto finito, entonces*

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

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

Demostración. Si vemos que $S/I(\mathbb{X})$ es Cohen-Macaulay y $\dim(S/I(\mathbb{X})) = 1$, entonces tendremos $\dim(S/I(\mathbb{X})) = \mathrm{depth}(S/I(\mathbb{X})) = 1 > 0$ y el resultado se obtendría a partir del teorema 1.5.21.

Sea $[P]$ un punto de $\mathbb{X}$, con $P = (\alpha_1, \ldots, \alpha_n)$ y $\alpha_k \neq 0$ para algún k. Sea $I_{[P]}$ el ideal generado por los polinomios homogéneos de S que se anulan en $[P]$. Entonces hemos visto en los resultados previos que $I_{[P]}$ es un ideal primo de altura $n-1$,

$$I_{[P]} = (\{\alpha_k x_i - \alpha_i x_k \mid i = 1, \ldots, n, i \neq k\}),\ I(\mathbb{X}) = \bigcap_{[Q] \in \mathbb{X}} I_{[Q]},$$

y la última expresión es la descomposición primaria de $I(\mathbb{X})$. Puesto que $I_{[P]}$ tiene altura $n-1$ para cualquier $[P] \in \mathbb{X}$, obtenemos que la altura de $I(\mathbb{X})$ es $n-1$, y la dimensión de $S/I(\mathbb{X})$ es 1. Por tanto, $\operatorname{depth}(S/I(\mathbb{X})) \leq 1$. Para terminar, observamos que $\mathfrak{m} = (x_1, \ldots, x_n)$ no es un primo asociado de $I(\mathbb{X})$, es decir, $\operatorname{depth}(S/I(\mathbb{X})) > 0$ y $S/I(\mathbb{X})$ es Cohen-Macaulay. □

Ejemplo 1.7.9. Sea $K = \mathbb{F}_5$, y consideramos los puntos $[P_1] = [1:1]$, $[P_2] = [2:1]$, $[P_3] = [3:2]$ en $\mathbb{P}^1_K$. Entonces tenemos que $I_{[P_1]} = (x_1 - x_2)$, $I_{[P_2]} = (x_1 - 2x_2)$ y $I_{[P_3]} = (2x_1 - 3x_2)$. Así que si consideramos $\mathbb{X} = \{[P_1], [P_2], [P_3]\} \subset \mathbb{P}^1_K$, tenemos que

$$I(\mathbb{X}) = I_{[P_1]} \cap I_{[P_2]} \cap I_{[P_3]} = (2x_1^3 + x_1^2 x_2 - 2x_1 x_2^2 - x_2^3).$$

1.8. Códigos tipo Reed-Muller

En esta sección vamos a introducir las familias de códigos tipo Reed-Muller proyectivos y su conexión con los ideales de anulación y funciones de Hilbert. Como referencia, vamos a utilizar principalmente [20] y [23].

Definición 1.8.1. Sea $K = \mathbb{F}_q$ un cuerpo finito. Un *código lineal* es un subespacio vectorial de K^m, $m \in \mathbb{N}$.

Sea $K = \mathbb{F}_q$ un cuerpo finito y sea $\mathbb{X} = \{[P_1], \ldots, [P_m]\} \neq \emptyset$ un subconjunto de $\mathbb{P}^{n-1}$ con $m = |\mathbb{X}|$. La mayoría de lo que vamos a decir a continuación es válido si K es cualquier cuerpo, pero el caso interesante para teoría de códigos es el de K finito.

Fijamos un grado $d \geq 0$. Para cada i existe un $f_i \in S_d$ tal que $f_i(P_i) \neq 0$. En efecto, supongamos que $P_i = (a_1, \ldots, a_n)$. Entonces existe al menos un k en $\{1, \ldots, n\}$ tal que $a_k \neq 0$. Si elegimos $f_i(x_1, \ldots, x_n) = x_k^d$ se tiene que $f_i \in S_d$ y $f_i(P_i) \neq 0$. Tenemos una aplicación K-lineal:

$$\operatorname{ev}_d : S_d = K[x_1, \ldots, x_n]_d \to K^{|\mathbb{X}|}, \;\; f \mapsto \left(\frac{f(P_1)}{f_1(P_1)}, \ldots, \frac{f(P_m)}{f_m(P_m)} \right).$$

Definición 1.8.2. Con la notación anterior:

- La aplicación ev_d se llama *aplicación de evaluación.*
- La imagen de S_d bajo ev_d, denotada por $C_{\mathbb{X}}(d)$, se llama *código tipo Reed-Muller proyectivo* de grado d sobre el conjunto $\mathbb{X}$. También se llama *código de evaluación* asociado a $\mathbb{X}$.

El núcleo de la aplicación de evaluación ev_d es $I(\mathbb{X})_d$. En consecuencia, hay un isomorfismo de K-espacios vectoriales $S_d/I(\mathbb{X})_d \cong C_{\mathbb{X}}(d)$. Si $\mathbb{X}$ es un subconjunto de $\mathbb{P}^{n-1}$ es habitual denotar a la función de Hilbert de $S/I(\mathbb{X})$ por $H_{\mathbb{X}}$. Así que $H_{\mathbb{X}}(d)$ es igual a $\dim_K C_{\mathbb{X}}(d)$.

Definición 1.8.3. Sea $0 \neq v \in C_{\mathbb{X}}(d)$.

- El *peso de Hamming* de v, denotado por $\|v\|$, es el número de entradas no nulas de v.
- La *distancia mínima* de $C_{\mathbb{X}}(d)$, denotada por $\delta_{\mathbb{X}}(d)$ o $\delta(C_{\mathbb{X}}(d))$, está definida por
$$\delta_{\mathbb{X}}(d) = \min\{\|v\| : 0 \neq v \in C_{\mathbb{X}}(d)\}.$$

Definición 1.8.4. Los *parámetros básicos* del código lineal $C_{\mathbb{X}}(d)$ son su *longitud*: $|\mathbb{X}|$; su *dimensión*: $\dim_K(C_{\mathbb{X}}(d))$; y su *distancia mínima*: $\delta_{\mathbb{X}}(d)$.

Observación 1.8.5. La notación habitual en teoría de códigos, que no vamos a seguir en esta parte por conveniencia para la parte de álgebra conmutativa, es usar n para la longitud, k para la dimensión y d para la distancia mínima. En ese caso se suelen escribir los parámetros de esta manera: $[n, k, d]$. El significado de estos parámetros es que el código que consideramos se puede utilizar para codificar palabras de longitud k (vectores de K^k) en palabras de longitud n (vectores de K^n), de manera que se pueden detectar $d-1$ errores y corregir $\lfloor \frac{d-1}{2} \rfloor$ con una redundancia de $n-k$ posiciones.

Lema 1.8.6 [20, Lem. 2.13]**.** *Se tiene que:*

(a) *La aplicación* ev_d *está bien definida, es decir, la definición no depende del conjunto de representantes elegidos para los puntos de* $\mathbb{X}$*.*

(b) *Los parámetros básicos de* $C_{\mathbb{X}}(d)$ *son independientes de* $f_1, \ldots, f_m$*.*

Demostración.

(a) Si $P'_1, \ldots, P'_m$ es otro conjunto de representantes, existen $\lambda_1, \ldots, \lambda_m \in K^*$ tales que $P'_i = \lambda_i P_i$, $1 \leq i \leq m$. En consecuencia, $f(P'_i)/f_i(P'_i) = f(P_i)/f_i(P_i)$ para todo $f \in S_d$ y $1 \leq i \leq m$.

(b) Sean $f'_1, \ldots, f'_m$ polinomios homogéneos de S de grado d tales que $f'_i(P_i) \neq 0$ para $i = 1, \ldots, m$, y sea
$$\mathrm{ev}'_d : S_d \to K^{|\mathbb{X}|}, \;\; f \mapsto \left(\frac{f(P_1)}{f'_1(P_1)}, \ldots, \frac{f(P_m)}{f'_m(P_m)} \right)$$
la aplicación de evaluación construida con $f'_1, \ldots, f'_m$. Entonces $\ker(\mathrm{ev}_d) = \ker(\mathrm{ev}'_d)$ y $\|\mathrm{ev}_d(f)\| = \|\mathrm{ev}'_d(f)\|$ para todo $f \in S_d$. Se deduce que los parámetros básicos de $\mathrm{ev}_d(S_d)$ y $\mathrm{ev}'_d(S_d)$ son los mismos.

□

La función de Hilbert y la distancia mínima están relacionadas mediante la cota de Singleton (que, según la notación habitual de teoría de códigos, es $d \leq n-k+1$) de la siguiente manera:
$$1 \leq \delta_{\mathbb{X}}(d) \leq |\mathbb{X}| - H_{\mathbb{X}}(d) + 1.$$

En particular, si $d \geq \operatorname{reg}(S/I(\mathbb{X})) \geq 1$, entonces $\delta_{\mathbb{X}}(d) = 1$. En consecuencia, los códigos de tipo Reed-Muller $C_{\mathbb{X}}(d)$ potencialmente buenos solo pueden ocurrir para $1 \leq d < \operatorname{reg}(S/I(\mathbb{X}))$.

Lema 1.8.7 [20, Lem. 2.14]**.** *Sea $\mathbb{Y} = \{[\alpha], [\beta]\}$ un subconjunto de $\mathbb{P}^{n-1}$ con dos elementos. Se tiene lo siguiente:*

(a) $\operatorname{reg}(S/I(\mathbb{Y})) = 1$.

(b) *Existe $h \in S_1$, una forma de grado 1, tal que $h(\alpha) \neq 0$ y $h(\beta) = 0$.*

(c) *Para cada $d \geq 1$, existe $f \in S_d$, una forma de grado d, tal que $f(\alpha) \neq 0$ y $f(\beta) = 0$.*

(d) *Si $\mathbb{X}$ es un subconjunto de $\mathbb{P}^{n-1}$ con al menos dos elementos y $d \geq 1$, entonces existe $f \in S_d$ tal que $f \notin I(\mathbb{X})$ y $(I(\mathbb{X}) : f) \neq I(\mathbb{X})$.*

Demostración.

(a) Como $H_{\mathbb{Y}}(0) = 1$ y $|\mathbb{Y}| = 2$, por la proposición 1.7.8 obtenemos que $H_{\mathbb{Y}}(1) = |\mathbb{Y}| = 2$. En consecuencia, $S/I(\mathbb{Y})$ tiene regularidad igual a 1.

(b) Consideramos la aplicación de evaluación

$$\operatorname{ev}_1 : S_1 \to K^2, \;\; f \mapsto (f(\alpha)/f_1(\alpha), f(\beta)/f_2(\beta)).$$

Por la parte (a), $\dim_K(\operatorname{Im}(\operatorname{ev}_1)) = \dim_K(S/I(\mathbb{Y}))_1 = 2$, por lo que esta aplicación es sobre. Así que $(1, 0)$ está en la imagen de ev_1 y se obtiene el resultado.

(c) Se deduce de la parte (b), tomando $f = h^d$.

(d) Por la parte (c), existen distintos $[\alpha]$, $[\beta]$ en $\mathbb{X}$ y $f \in S_d$ tales que $f(\alpha) \neq 0$, $f(\beta) = 0$. Así que $f \notin I(\mathbb{X})$. Observamos que $f(\beta) = 0$ si y solo si $f \in I_{[\beta]}$. En consecuencia, por el teorema 1.2.3 (b) y la observación 1.7.6, f es un divisor de cero de $S/I(\mathbb{X})$, es decir, $(I(\mathbb{X}) : f) \neq I(\mathbb{X})$.

□

Proposición 1.8.8 [20, Prop. 2.15]**.** *Existe un entero $r_0 \geq 0$ tal que*

$$|\mathbb{X}| = \delta_{\mathbb{X}}(0) > \delta_{\mathbb{X}}(1) > \cdots > \delta_{\mathbb{X}}(d) = \delta_{\mathbb{X}}(r_0) = 1 \text{ para } d \geq r_0.$$

Demostración. Supongamos que $\delta_{\mathbb{X}}(d) > 1$. Es suficiente ver que $\delta_{\mathbb{X}}(d) > \delta_{\mathbb{X}}(d+1)$. Elegimos $g \in S_d$ tal que $g \notin I(\mathbb{X})$ y tal que

$$|V_{\mathbb{X}}(g)| = \max\{|V_{\mathbb{X}}(f)| : \operatorname{ev}_d(f) \neq 0; f \in S_d\}.$$

Entonces $\delta_{\mathbb{X}}(d) = |\mathbb{X}| - |V_{\mathbb{X}}(g)| \geq 2$. En consecuencia, existen dos puntos distintos $[\alpha], [\beta]$ en $\mathbb{X}$ tales que $g(\alpha) \neq 0$ y $g(\beta) \neq 0$. Por el lema 1.8.7, existe una forma lineal

$h \in S_1$ tal que $h(\alpha) \neq 0$ y $h(\beta) = 0$. Así que el polinomio hg no está en $I(\mathbb{X})$, tiene grado $d+1$, y tiene al menos $|V_{\mathbb{X}}(g)|+1$ ceros. Se deduce que $\delta_{\mathbb{X}}(d) > \delta_{\mathbb{X}}(d+1)$. □

El entero r_0 de la proposición anterior (el menor posible) se llama *regularidad de la distancia mínima* de $S/I(\mathbb{X})$. Por lo que hemos visto antes, en general se tiene que $r_0 \leq r = \mathrm{reg}(S/I(\mathbb{X}))$. Calcular r_0 es un problema difícil, mientras que calcular la regularidad de $S/I(\mathbb{X})$ en algunos casos particulares (por ejemplo, si $\mathbb{X}$ está parametrizado por monomios) se puede hacer de manera efectiva.

La siguiente proposición resume las relaciones que conocemos entre los códigos de tipo Reed-Muller proyectivos y la teoría de funciones de Hilbert.

Proposición 1.8.9 [20, Prop. 2.16]**.** *Se tiene lo siguiente:*

(a) $H_{\mathbb{X}}(d) = \dim_K(C_{\mathbb{X}}(d))$ *para* $d \geq 0$.

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

(c) $\delta_{\mathbb{X}}(d) = 1$ *para* $d \geq \mathrm{reg}(S/I(\mathbb{X}))$.

(d) $S/I(\mathbb{X})$ *es un anillo graduado Cohen-Macaulay de dimensión 1.*

(e) $C_{\mathbb{X}}(d) \neq (0)$ *para* $d \geq 1$.

Demostración.

(a) El núcleo de la aplicación de evaluación ev_d es $I(\mathbb{X})_d$, por lo que tenemos un isomorfismo de espacios vectoriales $S_d/I(\mathbb{X})_d \cong C_{\mathbb{X}}(d)$. En consecuencia, $H_{\mathbb{X}}(d)$ es igual a $\dim_K(C_{\mathbb{X}}(d))$.

(b) Se deduce del corolario 1.7.7.

(c) Para $d \geq \mathrm{reg}(S/I(\mathbb{X}))$, se tiene que $H_{\mathbb{X}}(d) = |\mathbb{X}|$ por 1.7.8. Por la parte (a), tenemos que $C_{\mathbb{X}}(d)$ es igual a $K^{|\mathbb{X}|}$. En consecuencia, $\delta_{\mathbb{X}}(d) = 1$.

(d) Lo hemos visto en la demostración de 1.7.8.

(e) Se deduce de la proposición 1.7.8.

□

Hasta ahora hemos estudiado lo que serían los parámetros básicos del código, pero hay más parámetros interesantes que se pueden estudiar en un código para distintos tipos de aplicaciones. En este sentido vamos a introducir los pesos de Hamming generalizados (ver [29]). Estos parámetros, desde el punto de vista práctico, tienen como principal aplicación la caracterización de la seguridad de un canal de tipo "Wired-tap channel II", ver [29].

Definición 1.8.10. Sea C un código de longitud m y dimensión k y sea $1 \leq r \leq k$ un entero. Dado un subcódigo D de C (es decir, D es un subespacio vectorial de C), el *soporte* $\chi(D)$ de D es el conjunto de posiciones no nulas para algún elemento de D, es decir,

$$\chi(D) = \{i \mid \exists (a_1, \ldots, a_m) \in D, a_i \neq 0\}.$$

El *peso de Hamming generalizado r-ésimo* de C, denotado por $\delta_r(C)$, es el tamaño del menor soporte de un subcódigo de dimensión r, es decir,

$$\delta_r(C) = \text{mín}\{|\chi(D)| : D \text{ es un subcódigo de } C \text{ con } \dim_K(D) = r\},$$

donde $|\chi(D)|$ denota el cardinal de $\chi(D)$.

Observación 1.8.11. La distancia mínima del código es el primer peso de Hamming generalizado, $\delta_1(C)$.

Ejemplo 1.8.12. Sea $C = \{(0,0,0,0), (0,0,0,1), (1,1,1,0), (1,1,1,1)\} \subset \mathbb{F}_2^4$ un código lineal, y sean $D_1 = \{(0,0,0,0), (0,0,0,1)\}$, $D_2 = \{(0,0,0,0), (1,1,1,0)\}$, y $D_3 = \{(0,0,0,0), (1,1,1,1)\}$ subcódigos de C. Entonces $\chi(D_1) = \{4\}$, $\chi(D_2) = \{1,2,3\}$, y $\chi(D_3) = \{1,2,3,4\}$. De aquí se deduciría que $\delta(C) = \delta_1(C) = 1$. Por otro lado, el código es de dimensión 2, luego $\delta_2(C) = 4$ (porque está el vector $(1,1,1,1)$).

La *jerarquía de pesos* del código lineal C es el conjunto de enteros $\{\delta_r(C) \mid 1 \leq r \leq k\}$.

Teorema 1.8.13 [29, Thm. 1 (Monotonía)]**.** *Para un código lineal C de longitud m y dimensión $k > 0$ tenemos*

$$1 \leq \delta_1(C) < \cdots < \delta_k(C) \leq m.$$

Demostración. Que $\delta_{r-1}(C) \leq \delta_r(C)$ es trivial. Solo hay que probar que se dan las desigualdades estrictas. Sea D un subcódigo de C con $|\chi(D)| = \delta_r(C)$ y $\dim_K(D) = r$. Sea $i \in \chi(D)$ y $D_i = \{x \in D \mid x_i = 0\}$. Entonces $\dim_K(D_i) = r - 1$ y $\delta_{r-1}(C) \leq |\chi(D_i)| \leq |\chi(D)| - 1 = \delta_r(C) - 1$. □

Corolario 1.8.14 [29, Cor. 1 (Cota de Singleton Generalizada)]**.** *Para un código lineal C de longitud m y dimensión k tenemos que $\delta_r(C) \leq m - k + r$.*

Demostración. Utilizando el teorema 1.8.13 tenemos $\delta_K(C) \leq m = m - k + k$. Razonando por inducción teniendo en cuenta la desigualdades estrictas de 1.8.13 se obtiene el resultado. □

Observación 1.8.15. Vemos que la desigualdad de 1.8.14 para $r = 1$ no es otra cosa que la cota de Singleton $d \leq m - k + 1$.

Lema 1.8.16 [14, Lem. 2.1]**.** *Sea D un subcódigo de C de dimensión $r \geq 1$. Si $\beta_1, \ldots, \beta_r$ es base como K-espacio vectorial de D con $\beta_i = (\beta_{i,1}, \ldots, \beta_{i,m})$ para $i =$*

$1, \ldots, r$, *entonces* $\chi(D) = \bigcup_{i=1}^{r} \chi(\beta_i)$ *y el número de elementos de* $\chi(D)$ *es el número de columnas no nulas de la matriz:*

$$\begin{pmatrix} \beta_{1,1} & \cdots & \beta_{1,i} & \cdots & \beta_{1,m} \\ \beta_{2,1} & \cdots & \beta_{2,i} & \cdots & \beta_{2,m} \\ \vdots & \cdots & \vdots & \cdots & \vdots \\ \beta_{r,1} & \cdots & \beta_{r,i} & \cdots & \beta_{r,m} \end{pmatrix}.$$

1.8.1. Códigos cartesianos

En esta sección vamos a introducir unos códigos tipo Reed-Muller particulares, los códigos cartesianos, que se obtienen al considerar conjuntos de puntos obtenidos mediante el producto cartesiano. Es interesante introducirlos porque podemos obtener resultados adicionales para este tipo de códigos, como veremos en los capítulos siguientes. Como referencias, utilizamos [20] y [23].

Sea $K = \mathbb{F}_q$ un cuerpo finito, sea $A_2, \ldots, A_n$ una colección de subconjuntos de K, y sea

$$\mathcal{X} = [1 \times A_2 \times \cdots \times A_n]$$

la imagen de $1 \times A_2 \times \cdots \times A_n \setminus \{0\}$ bajo la aplicación $K^n \setminus \{0\} \to \mathbb{P}^{n-1}$, $x \to [x]$. $C_{\mathcal{X}}(d)$ se llama el d-ésimo *código cartesiano anidado afín.*

A continuación vamos a introducir los códigos cartesianos anidados proyectivos, que se definen de forma parecida a los anteriores. Sea $K = \mathbb{F}_q$ un cuerpo finito, sea $A_1, \ldots, A_n$ una colección de subconjuntos de K, y sea

$$\mathcal{X} = [A_1 \times \cdots \times A_n]$$

la imagen de $A_1 \times \cdots \times A_n \setminus \{0\}$ bajo la aplicación $K^n \setminus \{0\} \to \mathbb{P}^{n-1}$, $x \to [x]$. Algunas veces denotaremos por $\mathcal{X}^*$ al producto cartesiano $A_1 \times \cdots \times A_n$ en el espacio afín.

Definición 1.8.17. El conjunto $\mathcal{X}$ se llama un *conjunto cartesiano anidado proyectivo* si

(a) $\{0, 1\} \subset A_i$ para $i = 1, \ldots, n$,

(b) $a/b \in A_j$ para $1 \leq i < j \leq n$, $a \in A_j$, $0 \neq b \in A_i$, y

(c) $d_1 \leq \cdots \leq d_n$, donde $d_i = |A_i|$ para $i = 1, \ldots, n$.

Si $\mathcal{X}$ es un conjunto cartesiano anidado proyectivo, llamamos a $C_{\mathcal{X}}(d)$ *código cartesiano anidado proyectivo.*

Ejemplo 1.8.18. Sea K un cuerpo finito de característica p. Si consideramos $K_1 \subset K_2 \subset \cdots \subset K_n$ subcuerpos de K, entonces el conjunto

$$\mathcal{X} = [K_1 \times K_2 \times \cdots \times K_n] \subset \mathbb{P}^{n-1}$$

es un conjunto cartesiano anidado proyectivo. Este es uno de los ejemplos más habituales de código cartesiano anidado proyectivo, y estudiaremos un caso particular en todo detalle en el ejemplo 3.3.8.

1.8.2. Códigos parametrizados

En esta sección introducimos otro tipo particular de códigos para los cuales también obtendremos resultados adicionales. Como referencias, vamos a utilizar principalmente [13], [25] y [26].

Definición 1.8.19. Sea $K^* = K \setminus \{0\}$ el grupo multiplicativo de K. El toro proyectivo sobre $\mathbb{P}^{n-1}$, denotado por $\mathbb{T}_{n-1}$ (o $\mathbb{T}$ si no hay confusión), viene dado por

$$\mathbb{T}_{n-1} = \{[t_1 : \cdots : t_n] \in \mathbb{P}^{n-1} : t_i \in K^*\}.$$

Esta noción admite una generalización natural, que vamos a ver a continuación. Sea $L = K[z_1, \ldots, z_s]$ un anillo de polinomios sobre el cuerpo K y sea $z^{\alpha_1}, \ldots, z^{\alpha_n}$ un conjunto finito de monomios. Como es habitual, si $\alpha_i = (\alpha_{i1}, \ldots, \alpha_{is}) \in \mathbb{N}^s$, entonces denotamos

$$z^{\alpha_i} = z_1^{\alpha_{i1}} \cdots z_s^{\alpha_{is}} \text{ para } i = 1, \ldots, n.$$

Consideramos el siguiente conjunto parametrizado por estos monomios

$$X = \{[t_1^{a_{11}} \cdots t_s^{a_{1s}} : \cdots : t_1^{a_{n1}} \cdots t_s^{a_{ns}}] \in \mathbb{P}^{n-1} \mid t_i \in K^*\}.$$

Llamamos a X un *conjunto tórico parametrizado por lo monomios* $z^{\alpha_1}, \ldots, z^{\alpha_n}$. Al código de tipo Reed-Muller asociado $C_X(d)$ se le llama un *código parametrizado por monomios*, o simplemente *código parametrizado*. En esta situación tenemos que X es un subgrupo del toro proyectivo $\mathbb{T}_{n-1}$. Observamos que si consideramos los monomios $z_1, \ldots, z_n$, el conjunto X parametrizado por ellos es precisamente el toro proyectivo $\mathbb{T}_{n-1}$.

En esta situación, obtener el ideal $I(\mathbb{X})$ utilizando 1.7.6 puede ser muy pesado (porque estamos evaluando en muchos puntos). El siguiente resultado nos permite calcular este ideal de una forma alternativa cuando trabajamos sobre un cuerpo finito, que es lo habitual.

Proposición 1.8.20 [26, Cor. 1]**.** *Sea $B = K[x_1, \ldots, x_n, y_1, \ldots, y_s, z]$ un anillo de polinomios sobre el cuerpo finito $K = \mathbb{F}_q$, y sean $f_1, \ldots, f_s$ monomios de $R = K[y_1, \ldots, y_s]$. Si X es el conjunto tórico parametrizado por esos monomios, entonces*

$$I(X) = (\{x_i - f_i z\}_{i=1}^n \cup \{y_i^q - y_i\}_{i=1}^s \cup \{f_i^{q-1} - 1\}_{i=1}^n) \cap S.$$

En particular, para el caso de $X = \mathbb{T}_{n-1}$ se conoce exactamente el ideal y algunos de sus invariantes:

Proposición 1.8.21 [25, Prop. 2.1]**.** *Para el toro proyectivo $\mathbb{T}_{n-1} \subset \mathbb{P}^{n-1}$ se tiene que*

(a) $I(\mathbb{T}_{n-1}) = (\{x_i^{q-1} - x_1^{q-1}\}_{i=2}^n)$.

(b) $HS_{\mathbb{T}_{n-1}}(t) = \frac{(1-t^{q-1})^{n-1}}{(1-t)^n}$.

(c) $\operatorname{reg}(S/I(\mathbb{T}_{n-1})) = (n-1)(q-2)$ *y* $\deg(S/I(\mathbb{T}_{n-1})) = (q-1)^{n-1}$.

También podemos encontrar fácilmente una fórmula para la dimensión a partir del resultado anterior.

Corolario 1.8.22 [25, Cor. 2.2]**.** *Si* $\mathbb{T}_{n-1} \subset \mathbb{P}^{n-1}$ *es un toro proyectivo, entonces la longitud del código* $C_{\mathbb{T}_{n-1}}(d)$ *es* $(q-1)^{n-1}$ *y su dimensión viene dada por*

$$\dim_K C_{\mathbb{T}_{n-1}}(d) = \sum_{j=0}^{\lfloor \frac{d}{q-1} \rfloor} (-1)^j \binom{n-1}{j} \binom{n-1+d-j(q-1)}{n-1}.$$

Demostración. Por la proposición 1.8.21, la longitud de $C_{\mathbb{T}_{n-1}}(d)$ es $(q-1)^{n-1}$ y la serie de Hilbert de $S/I(\mathbb{T}_{n-1})$ viene dada por

$$\begin{aligned} HS_{\mathbb{T}_{n-1}}(t) = \sum_{d=0}^{\infty} H_{\mathbb{T}_{n-1}}(d) t^d &= \frac{(1-t^{q-1})^{n-1}}{(1-t)^n} \\ &= \left(\sum_{j=0}^{n-1} (-1)^j \binom{n-1}{j} t^{j(q-1)} \right) \left(\sum_{i=0}^{\infty} \binom{n-1+i}{n-1} t^i \right). \end{aligned}$$

Comparando los coeficientes de t^d, obtenemos

$$H_{\mathbb{T}_{n-1}}(d) = \sum_{i+j(q-1)=d} (-1)^j \binom{n-1}{j} \binom{n-1+i}{n-1}.$$

En consecuencia, tomando $i = d - j(q-1)$ obtenemos la expresión buscada para $\dim_K C_{\mathbb{T}_{n-1}}(d)$. □

Ejemplo 1.8.23. Consideramos $K = \mathbb{F}_5$, y consideramos $\mathbb{T}_3$. Por la proposición 1.8.21 tenemos

$$\begin{aligned} &I(\mathbb{T}_3) = (x_2^4 - x_1^4, x_3^4 - x_1^4, x_4^4 - x_1^4) \\ &HS_{\mathbb{T}_3}(t) = \frac{(1-t^4)^3}{(1-t)^4} = \frac{t^9 + 3t^8 + 6t^7 + 10t^6 + 12t^5 + 12t^4 + 10t^3 + 6t^2 + 3t + 1}{1-t} \\ &\operatorname{reg}(S/I(\mathbb{T}_3)) = 9, \ \deg(S/I(\mathbb{T}_3)) = 64. \end{aligned}$$

El grado también se puede obtener sumando los coeficientes del polinomio del numerador de $HS_{\mathbb{T}_3}(t)$ (después de simplificar $(1-t)^3$). La longitud del correspondiente código proyectivo es entonces 64 (el número de puntos, que es el grado del ideal), y podemos usar 1.8.22 para calcular la dimensión del correspondiente código proyectivo para cada d:

d	1	2	3	4	5	6	7	8	9
$\dim_K C_{\mathbb{T}_3}(d)$	4	10	20	32	44	54	60	63	64

Capítulo 2

Funciones distancia mínima y huella de un ideal homogéneo

Sea $S = K[x_1, \ldots, x_n] = \oplus_{d=0}^{\infty} S_d$ el anillo de polinomios sobre un cuerpo K, con un orden monomial $\prec$, y sea I un ideal homogéneo de S. En este capítulo vamos a estudiar dos funciones asociadas a I: la función distancia mínima δ_I y la función huella fp_I. Veremos en el capítulo 3 que la función distancia mínima está relacionada con la distancia mínima en teoría de códigos (ver teorema 3.2.2). El interés de la función huella reside en que es más fácil de calcular que la función distancia mínima, y en algunos casos es cota inferior o coincide con la función distancia mínima. En este capítulo estudiamos diversas propiedades de estas funciones, la aplicación a códigos corresponde al siguiente capítulo. Como referencias, vamos a utilizar principalmente [6], [14], [20], [22] y [23].

2.1. Función distancia mínima

Vamos a comenzar estudiando la función distancia mínima. Para ello, primero definimos el conjunto $\mathcal{F}_d$, que es el conjunto de todos los polinomios de grado $d \geq 0$ que son divisores de cero en S/I:

$$\mathcal{F}_d = \{f \in S_d \mid f \notin I, (I : f) \neq I\},$$

donde $(I : f) = \{h \in S \mid hf \in I\}$ es el ideal cociente. Observamos que $\mathcal{F}_0 = \emptyset$.

Observación 2.1.1. El conjunto $\mathcal{F}_d$ puede ser vacío para algunos valores de d. Si todos los primos asociados de S/I están generados minimalmente por polinomios de grado al menos $r \geq 2$, entonces $\mathcal{F}_d = \emptyset$ para $1 \leq d < r$ (ver 1.2.3 (b)). Por otro lado, si I es primo, entonces $\mathcal{F}_d$ es vacío para $d \geq 0$.

Lema 2.1.2 [22, Lem. 3.7]**.** *Sea $I \subset S$ un ideal homogéneo radical no mezclado y sea $\mathrm{Ass}(S/I) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$. Si $f \in \mathcal{F}_d$ para algún $d \geq 1$, entonces*

$$\deg(S/(I : f)) = \sum_{f \notin \mathfrak{p}_i} \deg(S/\mathfrak{p}_i).$$

Demostración. Puesto que I es un ideal radical, tenemos que $I = \cap_{i=1}^{m} \mathfrak{p}_i$. A partir de las siguientes igualdades

$$(I : f) = \cap_{i=1}^{m} (\mathfrak{p}_i : f) = \cap_{f \notin \mathfrak{p}_i} \mathfrak{p}_i,$$

y usando la aditividad del grado (1.5.23), se obtiene el resultado. □

Definición 2.1.3. La *función distancia mínima* de I, denotada por δ_I, es la función $\delta_I : \mathbb{N} \to \mathbb{Z}$ dada por

$$\delta_I(d) = \begin{cases} \deg(S/I) - \max\{\deg(S/(I,f)) \mid f \in \mathcal{F}_d\} & \text{si } \mathcal{F}_d \neq \emptyset, \\ \deg(S/I) & \text{si } \mathcal{F}_d = \emptyset. \end{cases}$$

Lema 2.1.4 ([6, Lem. 3.1], [14, Lem. 4.1])**.** *Sea $I \subset S$ un ideal homogéneo no mezclado, sea $\prec$ un orden monomial, y sea F un conjunto finito de polinomios homogéneos de S tales que $(I : (F)) \neq I$. Se da lo siguiente.*

(a) $\operatorname{ht}(I) = \operatorname{ht}(I, F)$.

(b) $\deg(S/(I,F)) < \deg(S/I)$ *si I es un ideal no mezclado y $(F) \not\subset I$.*

(c) $\deg(S/I) = \deg(S/(I : (F))) + \deg(S/(I,F))$ *si I también es radical.*

(d) $\deg(S/(I,F)) \leq \deg(S/(\operatorname{in}_\prec(I), \operatorname{in}_\prec(F))) \leq \deg(S/I)$.

Demostración.

(a) Vamos a ver que $S/(I,F)$ y S/I tienen la misma dimensión. Puesto que $(I : (F)) \neq I$, todos los elementos de F son divisores de cero en S/I. Como I es no mezclado, existe un primo asociado $\mathfrak{p}$ de S/I tal que $(F) \subset \mathfrak{p}$ y $\dim(S/I) = \dim(S/\mathfrak{p})$. Puesto que $I \subset (I,F) \subset \mathfrak{p}$, obtenemos que $\dim(S/(I,F)) = \dim(S/I)$.

(b) La desigualdad se deduce de la parte (a) y el lema 1.5.22 (b).

(c) Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ los primos asociados de S/I. Como I es un ideal radical, se tienen las descomposiciones

$$I = \bigcap_{i=1}^{m} \mathfrak{p}_i \text{ y } (I : (F)) = \bigcap_{i=1}^{m} (\mathfrak{p}_i : (F)).$$

Observamos que $(\mathfrak{p}_i : (F)) = S$ si $F \subset \mathfrak{p}_i$ y $(\mathfrak{p}_i : (F)) = \mathfrak{p}_i$ si $F \not\subset \mathfrak{p}_i$. En consecuencia, usando la aditividad del grado de la proposición 1.5.23 y el lema 1.5.24 obtenemos

$$\deg(S/(I : (F))) = \sum_{F \not\subset \mathfrak{p}_i} \deg(S/\mathfrak{p}_i) \text{ y } \deg(S/(I,F)) = \sum_{F \subset \mathfrak{p}_i} \deg(S/\mathfrak{p}_i).$$

Por tanto, $\deg(S/I) = \sum_{i=1}^{m} \deg(S/\mathfrak{p}_i) = \deg(S/(I : (F))) + \deg(S/(I,F))$.

(d) Para simplificar la notación vamos a denotar $J = (I, F)$, $L = (\mathrm{in}_\prec(I), \mathrm{in}_\prec(F))$ y $F = \{f_1, \ldots, f_r\}$. Por (a) tenemos que $\dim(S/J) = \dim(S/I)$. Además, S/I y $S/\mathrm{in}_\prec(I)$ tienen la misma función de Hilbert, y también $S/\mathfrak{p}$ y $S/\mathrm{in}_\prec(\mathfrak{p})$ ($\mathfrak{p}$ un ideal primo como en (a)), así que tenemos

$$\dim(S/\mathrm{in}_\prec(I)) = \dim(S/I) = \dim(S/\mathfrak{p}) = \dim(S/\mathrm{in}_\prec(\mathfrak{p})).$$

En consecuencia, tomando alturas en la inclusiones $\mathrm{in}_\prec(I) \subset L \subset \mathrm{in}_\prec(\mathfrak{p})$, obtenemos $\mathrm{ht}(I) = \mathrm{ht}(L)$.

Consideramos una base de Gröbner $\mathcal{G} = \{g_1, \ldots, g_r\}$ de I. Entonces J está generado por $\mathcal{G} \cup F$, y por el lema 1.6.11 se tienen las inclusiones

$$\begin{aligned}\Delta_\prec(J) = \Delta_\prec(I, F) &\subset \Delta_\prec(\mathrm{in}_\prec(g_1), \ldots, \mathrm{in}_\prec(g_r), \mathrm{in}_\prec(F)) = \Delta_\prec(\mathrm{in}_\prec(I), \mathrm{in}_\prec(F)) \\ &= \Delta_\prec(L) \subset \Delta_\prec(\mathrm{in}_\prec(g_1), \ldots, \mathrm{in}_\prec(g_r)) = \Delta_\prec(I).\end{aligned}$$

Así que tenemos que $\Delta_\prec(J) \subset \Delta_\prec(L) \subset \Delta_\prec(I)$. Observamos que $H_I(d)$ es precisamente el número de monomios estándar de grado d. En consecuencia, $H_J(d) \leq H_L(d) \leq H_I(d)$ para $d \geq 0$. Si $\dim(S/I) = 0$, entonces

$$\deg(S/J) = \sum_{d\geq 0} H_J(d) \leq \deg(S/L) = \sum_{d\geq 0} H_L(d) \leq \deg(S/I) = \sum_{d\geq 0} H_I(d).$$

Supongamos ahora que $\dim(S/I) \geq 1$. Por el teorema 1.5.5, H_J, H_L, H_I son funciones polinomiales de grado igual a $k = \dim(S/I) - 1$. Por tanto,

$$k! \lim_{d\to\infty} \frac{H_J(d)}{d^k} \leq k! \lim_{d\to\infty} \frac{H_L(d)}{d^k} \leq k! \lim_{d\to\infty} \frac{H_I(d)}{d^k},$$

es decir, $\deg(S/J) \leq \deg(S/L) \leq \deg(S/I)$.

□

El siguiente lema nos da una versión más refinada de 2.1.4 (c) para el caso en el que F es un único polinomio.

Lema 2.1.5 [22, Lem. 3.1]**.** *Sea $I \subset S$ un ideal homogéneo no mezclado. Si $f \in S \setminus I$ es homogéneo y $(I : f) \neq I$, entonces*

$$\deg(S/I) = \deg(S/(I : f)) + \deg(S/(I, f)), \text{ en particular } \deg(S/(I, f)) < \deg(S/I).$$

Demostración. Utilizando que I es no mezclado, es fácil ver que S/I, $S/(I : f)$ y $S/(I, f)$ tienen la misma dimensión de Krull. En efecto, para $S/(I, f)$ lo hemos visto en el lema 2.1.4 (a). Para el otro caso, si $I = \cap_{i=1}^r \mathfrak{q}_i$ es una descomposición primaria de I, con $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$, $i = 1, \ldots, r$, entonces $(I : f) = \cap_{i:f\notin\mathfrak{q}_i}(\mathfrak{q}_i : f)$ es una descomposición primaria de $(I : f)$. Como $(I : f) \neq I$ y $f \in S \setminus I$, $(I : f)$ no es el

total y la intersección anterior es no vacía. Cualquiera de los $(\mathfrak{q}_i : f)$ que aparecen son $\mathfrak{p}_i$-primarios. Tomando un i de los que aparecen en la intersección se tiene

$$I \subset (I : f) \subset \mathfrak{p}_i.$$

Tomando alturas obtenemos $\dim(S/I) = \dim(S/(I : f))$.

Por otro lado, tenemos la sucesión exacta

$$0 \longrightarrow (S/I)[-d] \xrightarrow{f} S/I \longrightarrow S/(I, f) \longrightarrow 0.$$

Por tanto, por la aditividad de las funciones de Hilbert 1.5.3, tenemos

$$H_I(i) = H_{(I:f)}(i - d) + H_{(I,f)}(i) \text{ para } i \geq 0. \tag{2.1.1}$$

Si $\dim(S/I) = 0$, entonces por la ecuación 2.1.1 se tiene que

$$\sum_{i\geq 0} H_I(i) = \sum_{i\geq 0} H_{(I:f)}(i) + \sum_{i\geq 0} H_{(I,f)}(i).$$

En consecuencia, por la definición de grado, se obtiene el resultado para este caso. Si $k = \dim(S/I) - 1$ y $k \geq 1$, por el teorema 1.5.5, $H_I(i)$, $H_{(I,j)}(i)$, y $H_{(I:f)}(i)$ son funciones polinomiales de grado k (para i suficientemente grande). Entonces, dividiendo la ecuación 2.1.1 por i^k y tomando límites cuando i tiende a infinito, se obtiene el resultado. □

Observación 2.1.6. Sea $I \subset S$ un ideal homogéneo no mezclado de dimensión 1. Si $f \in S_d$, entonces $(I : f) = I$ si y solo si $\dim(S/(I, f)) = 0$. En este caso $\deg(S/(I, f))$ puede ser mayor que $\deg(S/I)$. Por ejemplo, si consideramos el ideal $I = (x_1, x_2) \subset K[x_1, x_2, x_3]$, es no mezclado de dimensión 1, y $\deg(S/(I, x_3^d)) = d > \deg(S/I) = 1$ si $d \geq 2$.

A continuación vemos una fórmula alternativa para la función distancia mínima válida para ideales homogéneos no mezclados.

Teorema 2.1.7 [20, Thm. 4.4]**.** *Sea $I \subset S$ un ideal homogéneo no mezclado y sea $\prec$ un orden monomial en S. Si $\Delta_\prec(I)_d^p$ es el conjunto de polinomios estándar homogéneos de grado d y $S_d \not\subset I$, entonces*

$$\begin{aligned}\delta_I(d) &= \min\{\deg(S/(I : f)) \mid f \in S_d \setminus I\} \\ &= \min\{\deg(S/(I : f)) \mid f \in \Delta_\prec(I)_d^p\}.\end{aligned}$$

Demostración. La segunda igualdad es clara porque por el algoritmo de división cualquier $f \in S_d \setminus I$ se puede escribir como $f = g + h$, donde $g \in I$ y $h \in \Delta_\prec(I)_d^p$, y $(I : f) = (I : h)$. Si $\mathcal{F}_d = \emptyset$, $\delta_I(d) = \deg(S/I)$ y para cualquier $f \in S_d \setminus I$, se tiene que $(I : f) = I$. Así que en ese caso se da la igualdad. Supongamos que $\mathcal{F}_d \neq \emptyset$. Sea $f \in \mathcal{F}_d$. Puesto que I es no mezclado, razonando como al principio del lema

2.1.5, tenemos que S/I, $S/(I:f)$, y $S/(I,f)$ tienen la misma dimensión. Tenemos las siguientes sucesiones exactas:

$$0 \longrightarrow (I:f)/I \longrightarrow S/I \longrightarrow S/(I:f) \longrightarrow 0,$$

$$0 \longrightarrow ((I:f)/I)[-d] \longrightarrow (S/I)[-d] \xrightarrow{f} S/I \longrightarrow S/(I,f) \longrightarrow 0.$$

Usando la aditividad de las funciones de Hilbert obtenemos

$$\begin{aligned} H_{(I:f)/I}(i) &= H_I(i) - H_{(I:f)}(i), \\ H_{(I:f)/I}(i-d) &= H_I(i-d) - H_I(i) + H_{(I,f)}(i), \end{aligned} \tag{2.1.2}$$

para $i \geq 0$. Por definición de $\delta_I(d)$ es suficiente con ver la siguiente igualdad

$$\deg(S/(I:f)) = \deg(S/I) - \deg(S/(I,f)). \tag{2.1.3}$$

Si $\dim(S/I) = 0$, entonces sumando en las ecuaciones de 2.1.2, teniendo en cuenta que al sumar para todo $i \geq 0$ el desplazamiento en $-d$ no es relevante, se tiene que

$$\sum_{i\geq 0} H_I(i) - \sum_{i\geq 0} H_{(I:f)}(i) = \sum_{i\geq 0} H_{(I,f)}(i).$$

En consecuencia, por la definición de grado, se da la igualdad de 2.1.3. Si $k = \dim(S/I)-1$, por el teorema de Hilbert-Serre 1.5.12, H_I, $H_{(I,f)}$, y $H_{(I:f)}$ son funciones polinomiales de grado k. Entonces si dividimos las ecuaciones 2.1.2 por i^k y tomamos límites cuando i tiende a infinito, se obtiene la igualdad de 2.1.3 (de nuevo, en el límite el desplazamiento en $-d$ no es relevante).

□

Observación 2.1.8. Sea I un ideal que no es primo, y sea $\mathfrak{p}$ un primo asociado de I. Entonces existe un $f \in S_d$, $d \geq 1$, tal que $(I:f) = \mathfrak{p}$. Observamos que $f \in \mathcal{F}_d$. Por el teorema 2.1.7 se tiene que $\delta_I(d) = 1$.

A la función $\vartheta(d,1) = \min\{\deg(S/(I:f)) \mid f \in S_d \setminus I\}$ del teorema 2.1.7 la llamaremos *función de Vasconcelos* más adelante (en 2.4.13), y veremos un resultado similar al del teorema 2.1.7 en un contexto más general, pero para ideales radicales.

Teorema 2.1.9 [22, Thm. 3.6]**.** *Sea $I \subset S$ un ideal homogéneo no mezclado y sea $d \geq 1$ un entero. Se da lo siguiente:*

(a) $\delta_I(d) \geq 1$.

(b) *Si* $\dim(S/I) \geq 1$ *y* $\mathcal{F}_d \neq \emptyset$ *para* $d \geq 1$, *entonces* $\delta_I(d) \geq \delta_I(d+1) \geq 1$ *para* $d \geq 1$.

Demostración. Se demuestra un resultado más general en 2.4.10. □

Teorema 2.1.10 [20, Thm. 4.5]**.** *Sea $\prec$ un orden monomial y sea $I \subset S$ un ideal no mezclado de dimensión ≥ 1 tal que x_i es un divisor de cero de S/I para $i = 1, \ldots, n$. Se da lo siguiente:*

(a) *El conjunto $\mathcal{F}_d = \{f \in S_d \mid f \notin I, (I : f) \neq I\}$ es no vacío para $d \geq 1$.*

(b) $\deg(S/(I, x^\alpha)) \leq \deg(S/(\text{in}_\prec(I), x^\alpha)) \leq \deg(S/I)$ *para algún* $x^\alpha \in \Delta_\prec(I) \cap S_d$.

(c) $\delta_I(d) \geq \delta_I(d+1)$ *para* $d \geq 1$.

(d) *Si I es un ideal radical y sus primos asociados están generados por formas lineales, entonces existe un entero $r_0 \geq 1$ tal que*

$$\delta_I(1) > \delta_I(2) > \cdots > \delta_I(r_0) = \delta_I(d) = 1 \text{ para } d \geq r_0.$$

Demostración.

(a) Puesto que $\dim(S/I) \geq 1$, existe $1 \leq l \leq s$ tal que $x_l^d \notin I$, y $(I : x_l^d) \neq I$ porque x_l^d es un divisor de cero de S/I. Así que $x_l^d \in \mathcal{F}_d$.

(b) Puesto que cualquier monomio estándar de grado d es un divisor de cero, por el lema 2.1.4 (d), obtenemos las desigualdades de (b).

(c) El conjunto $\mathcal{F}_d$ es no vacío para $d \geq 1$ por la parte (a). Por el teorema 2.1.9 (b) tenemos que $\delta_I(d) \geq \delta_I(d+1)$ para $d \geq 1$.

(d) Por el lema 2.1.4, $\delta_I(d) \geq 1$ para $d \geq 1$. Supongamos que $\delta_I(d) > 1$. Por la parte (c) es suficiente ver que $\delta_I(d) > \delta_I(d+1)$. Elegimos un polinomio $F \in S_d$ tal que $F \notin I$, $(I : F) \neq I$ y $\deg(S/(I, F)) = \text{máx}\{\deg(S/(I, f)) \mid f \notin I, f \in S_d, (I : f) \neq I\}$. Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ los primos asociados de I. Entonces, por el lema 1.5.24, se tiene que

$$\delta_I(d) = \deg(S/I) - \deg(S/(I, F)) = \sum_{i=1}^{m} \deg(S/\mathfrak{p}_i) - \sum_{F \in \mathfrak{p}_i} \deg(S/\mathfrak{p}_i) \geq 2.$$

En consecuencia, hay dos primos asociados $\mathfrak{p}_k \neq \mathfrak{p}_j$ tales que F no está en $\mathfrak{p}_k \cup \mathfrak{p}_j$ (al estar generados por formas lineales, $\deg(S/\mathfrak{p}_i) = 1$ por 1.5.8). Elegimos una forma lineal h en $\mathfrak{p}_k \setminus \mathfrak{p}_j$, que existe porque I es no mezclado y $\mathfrak{p}_k$ está generado por formas lineales. Entonces $hF \notin I$ porque $hF \notin \mathfrak{p}_j$, y hF es un divisor de cero de S/I porque $(I : F) \neq I$. Puesto que $F \notin \mathfrak{p}_k$ y $hF \in \mathfrak{p}_k$, por el lema 1.5.24 obtenemos

$$\deg(S/(I, F)) = \sum_{F \in \mathfrak{p}_i} \deg(S/\mathfrak{p}_i) < \sum_{hF \in \mathfrak{p}_i} \deg(S/\mathfrak{p}_i) = \deg(S/(I, hF)).$$

Así que $\delta_I(d) > \delta_I(d+1)$.

□

Es interesante estudiar bajo qué condiciones la función distancia mínima decrece estrictamente como en 2.1.10 (d). En este sentido tenemos los dos resultados siguientes.

Corolario 2.1.11 [20, Cor. 4.6]**.** *Sea $I \subset S$ un ideal monomial Cohen-Macaulay libre de cuadrados. Entonces existe un entero $r_0 \geq 0$ tal que*

$$\delta_I(1) > \delta_I(2) > \cdots > \delta_I(r_0) = \delta_I(d) = 1 \text{ para } d \geq r_0.$$

Demostración. Si I es primo, entonces I está generado por un subconjunto de $\{x_1, \ldots, x_n\}$, $\deg(S/I) = 1$ (por 1.5.8), y $\mathcal{F}_d = \emptyset$ para todo d. Así que podemos suponer que I tiene al menos dos primos asociados. Cualquier ideal Cohen-Macaulay es no mezclado por el teorema 1.3.13 (aplicado al ideal cero de S/I). Entonces el grado de S/I es el número de primos asociados de S/I. Por tanto, podemos suponer que todas las variables son divisores de cero en S/I y el resultado se deduce del teorema 2.1.10 (d). □

El siguiente resultado generaliza 2.1.10 (d), ya que no pedimos que las variables x_i, $i = 1, \ldots, n$ sean divisores de cero en S/I.

Teorema 2.1.12 [22, Thm. 3.8]**.** *Sea $I \subset S$ un ideal homogéneo radical no mezclado. Si todos los primos asociados de S/I están generados por formas lineales, entonces existe un entero $r_0 \geq 1$ tal que*

$$\delta_I(1) > \delta_I(2) > \cdots > \delta_I(r_0) = \delta_I(d) = 1 \text{ para } d \geq r_0.$$

Demostración. Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ los primos asociados de I. Como $\mathfrak{p}_i$ está generado por formas lineales, entonces $\deg(S/\mathfrak{p}_i) = 1$ para todo i por 1.5.8. Si I es primo, entonces $I = \mathfrak{p}_1$ (el único que hay) y $\mathcal{F}_d = \emptyset$ para $d \geq 1$. Por tanto, $\delta_I(d) = \deg(S/\mathfrak{p}_i) = 1$ para $d \geq 1$, y podemos tomar $r_0 = 1$. Podemos asumir ahora que I tiene al menos dos primos asociados, es decir, $m \geq 2$. Como $I \subsetneq \mathfrak{p}_1$, existe una forma de grado 1 en $\mathfrak{p}_1 \setminus I$. En consecuencia, como I es un ideal radical, tenemos que $h^d \in \mathfrak{p}_1 \setminus I$. Así que $\mathcal{F}_d \neq \emptyset$ para $d \geq 1$. Por el teorema 2.1.9 (b), se tiene que $\delta_I(d) \geq \delta_I(d+1) \geq 1$ para $d \geq 1$. Por tanto, si suponemos que $\delta_I(d) > 1$, es suficiente con ver que $\delta_I(d) > \delta_I(d+1)$. Por el teorema 2.1.7, existe $f \in \mathcal{F}_d$ tal que $\delta_I(d) = \deg(S/(I : f))$. Entonces, por el lema 2.1.2, se tiene

$$\delta_I(d) = \deg(S/(I : f)) = \sum_{f \notin \mathfrak{p}_i} \deg(S/\mathfrak{p}_i) \geq 2.$$

Así que hay dos primos asociados $\mathfrak{p}_k \neq \mathfrak{p}_j$ tales que f no está en $\mathfrak{p}_k \cup \mathfrak{p}_j$. Elegimos una forma lineal h en $\mathfrak{p}_k \setminus \mathfrak{p}_j$. Entonces $hf \notin I$ porque $hf \notin \mathfrak{p}_j$, y hf es un divisor de cero en S/I porque $(I : f) \neq I$. Puesto que $f \notin \mathfrak{p}_k$ y $hf \in \mathfrak{p}_k$, se obtiene la desigualdad estricta

$$\{\mathfrak{p}_i \mid hf \notin \mathfrak{p}_i\} \subsetneq \{\mathfrak{p}_i \mid f \notin \mathfrak{p}_i\}.$$

En consecuencia, por el lema 2.1.2, tenemos

$$\deg(S/(I:f)) = \sum_{f \notin \mathfrak{p}_i} \deg(S/\mathfrak{p}_i) > \sum_{hf \notin \mathfrak{p}_i} \deg(S/\mathfrak{p}_i) = \deg(S/(I:hf)).$$

Así que, por el teorema 2.1.7, tenemos que $\delta_I(d) > \delta_I(d+1)$. □

Definición 2.1.13. El entero r_0 del teorema anterior (y los resultados previos) se llama *índice de regularidad* de δ_I, y se denota por $\operatorname{reg}(\delta_I)$.

En el caso de que I sea el ideal de anulación de un conjunto finito de puntos del espacio proyectivo sobre un cuerpo finito, se tiene que $\operatorname{reg}(\delta_I) \leq \operatorname{reg}(S/I)$ (ver el capítulo 3). Un problema interesante es, precisamente, ver para qué tipos de ideales se cumple la relación anterior. Por ejemplo, se sabe que se tiene esa relación si $I = I(G)$ es el ideal de aristas de un grafo G bipartito y Cohen-Macaulay. En este contexto se tiene la siguiente conjetura.

Conjetura 2.1.14 [22, Conj. 4.2]**.** Sea $I \subset S$ un ideal homogéneo radical no mezclado. Si todos los primos asociados de I están generados por formas lineales, entonces $\delta_I(d) = 1$ para $d \geq \operatorname{reg}(S/I)$, es decir, $\operatorname{reg}(\delta_I) \leq \operatorname{reg}(S/I)$.

Esta conjetura ha sido probada para ideales de aristas asociados a grafos Cohen-Macaulay en [22], pero sigue abierta en gran cantidad de casos, por ejemplo si I es el ideal de aristas de un grafo bipartito no mezclado.

Vamos a introducir el siguiente invariante numérico que se utilizará para expresar el índice de regularidad de la función distancia mínima (proposición 2.1.18).

Definición 2.1.15. El v-*número* de un ideal homogéneo I, denotado $\mathrm{v}(I)$, viene dado por

$$\mathrm{v}(I) = \begin{cases} \min\{d \geq 1 \mid \text{ existe } f \in S_d \text{ y } \mathfrak{p} \in \operatorname{Ass}(I) \text{ con } (I:f) = \mathfrak{p}\} & \text{si } I \subsetneq \mathfrak{m}, \\ 0 & \text{si } I = \mathfrak{m}, \end{cases}$$

donde $\mathfrak{m} = (x_1, \ldots, x_n)$ es el ideal homogéneo maximal de S.

El v-número es finito para cualquier ideal homogéneo por la definición de primo asociado. Si $\mathfrak{p}$ es un ideal primo y $\mathfrak{p} \neq \mathfrak{m}$, entonces $\mathrm{v}(\mathfrak{p}) = 1$.

Sea $I \subsetneq \mathfrak{m} \subset S$ un ideal homogéneo y sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ sus primos asociados. Se puede definir el v-número de I localmente en cada $\mathfrak{p}_i$ por

$$\mathrm{v}_{\mathfrak{p}_i}(I) = \min\{d \geq 1 \mid \exists f \in S_d \text{ con } (I:f) = \mathfrak{p}_i\}.$$

El v-número de I es igual a $\min\{\mathrm{v}_{\mathfrak{p}_1}(I), \ldots, \mathrm{v}_{\mathfrak{p}_m}(I)\}$. Vamos a dar una descripción alternativa del v-número utilizando los grados iniciales de algunos módulos. Esto nos permitirá calcular el v-número utilizando [12] (ver ejemplo 2.1.17). Para un módulo graduado $M \neq 0$ denotamos por $\alpha(M) = \min\{\deg(f) \mid f \in M, f \neq 0\}$. Por convención, para $M = 0$ vamos a establecer $\alpha(0) = 0$.

Proposición 2.1.16 [6, Prop. 4.2]**.** *Sea $I \subset S$ un ideal homogéneo no mezclado. Entonces $I \subsetneq (I : \mathfrak{p})$ para $\mathfrak{p} \in \mathrm{Ass}(I)$,*

$$\mathrm{v}(I) = \mín\{\alpha((I : \mathfrak{p})/I) \mid \mathfrak{p} \in \mathrm{Ass}(I)\},$$

y $\alpha((I : \mathfrak{p})/I) = \mathrm{v}_{\mathfrak{p}}(I)$ para $\mathfrak{p} \in \mathrm{Ass}(I)$.

Demostración. Como paso preliminar de la demostración vamos a establecer que para un primo $\mathfrak{p} \in \mathrm{Ass}(I)$ tenemos

$$(I : f) = \mathfrak{p} \text{ si y solo si } f \in (I : \mathfrak{p}) \setminus I.$$

Si $(I : f) = \mathfrak{p}$, es claro que tenemos $f \in (I : \mathfrak{p})$ y puesto que $(I : f) \neq S$, se deduce que $f \notin I$. Recíprocamente, si $f \in (I : \mathfrak{p}) \setminus I$, entonces $\mathfrak{p} \subset (I : f)$. Sea $\mathfrak{q} \in \mathrm{Ass}(I : f)$, el cual es un conjunto no vacío puesto que $f \notin I$. Puesto que $\mathrm{Ass}(I : f) \subset \mathrm{Ass}(I)$ e I es no mezclado, tenemos que $\mathrm{ht}(\mathfrak{q}) = \mathrm{ht}(\mathfrak{p})$ y $\mathfrak{p} \subset (I : f) \subset \mathfrak{q}$. Se deduce que $\mathfrak{p} = (I : f) = \mathfrak{q}$.

La inclusión estricta $I \subsetneq (I : \mathfrak{p})$ se deduce de la equivalencia anterior, ya que por la definición de primo asociado, $\mathfrak{p} = \mathrm{ann}(f)$ para algún $f \in S/I$, luego $(I : f) = \mathfrak{p}$, que por la equivalencia anterior implica que $f \in (I : \mathfrak{p}) \setminus I$.

Por otro lado, la equivalencia que hemos visto implica que $\alpha((I : \mathfrak{p})/I) = \mathrm{v}_{\mathfrak{p}}(I)$, y prueba la igualdad

$$\{f \mid (I : f) = \mathfrak{p} \text{ para algún } \mathfrak{p} \in \mathrm{Ass}(I)\} = \bigcup_{\mathfrak{p} \in \mathrm{Ass}(I)} (I : \mathfrak{p}) \setminus I.$$

El resultado se obtiene considerando el menor grado de un elemento homogéneo en los conjuntos anteriores. □

Ejemplo 2.1.17. Sea $S = \mathbb{Q}[x_1, x_2, x_3, x_4]$ un anillo de polinomios sobre $K = \mathbb{Q}$ y sea I el ideal de S dado por

$$I = (x_2^{10}, x_3^9, x_4^4, x_2x_3x_4^3) \cap (x_1^4, x_3^4, x_4^3, x_1x_3x_4^2) \cap (x_1^4, x_2^5, x_4^3) \cap (x_1^3, x_2^5, x_3^{10}).$$

Vamos a utilizar el siguiente procedimiento en [12] para calcular el v-número de I.

```
S=QQ[x1,x2,x3,x4]
I=intersect(ideal(x2^10,x3^9,x4^4,x2*x3*x4^3),ideal(x1^4,x3^4,x4^3,
x1*x3*x4^2),ideal(x1^4,x2^5,x4^3),ideal(x1^3,x2^5,x3^10))
p=associatedPrimes I
apply(apply(apply(p,x->quotient(I,x)),y->y/I),z-> flatten flatten degrees
mingens z)
```

Obtenemos que los primos asociados de I son $\mathfrak{p}_1 = (x_1, x_2, x_3)$, $\mathfrak{p}_2 = (x_1, x_2, x_4)$, $\mathfrak{p}_3 = (x_1, x_3, x_4)$ y $\mathfrak{p}_4 = (x_2, x_3, x_4)$. Por la proposición 2.1.16 (es lo que utiliza el procedimiento), obtenemos que $\mathrm{v}_{\mathfrak{p}_i}(I) = 18$ para $i = 1, 2$, $\mathrm{v}_{\mathfrak{p}_3}(I) = 15$ y $\mathrm{v}_{\mathfrak{p}_4}(I) = 12$, luego $\mathrm{v}(I) = 12$.

Proposición 2.1.18 [6, Prop. 4.6]**.** *Sea $I \subsetneq \mathfrak{m} \subset S$ un ideal homogéneo no mezclado cuyos primos asociados están generados por formas lineales. Entonces* $\operatorname{reg}(\delta_I) = \operatorname{v}(I)$.

Demostración. Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ los primos asociados de I. Podemos asumir que I no es un ideal primo, ya que en ese caso tendríamos $\operatorname{reg}(\delta_I) = \operatorname{v}(I) = 1$. Si $d_1 = \operatorname{v}(I)$, existen $f \in S_{d_1}$ y $\mathfrak{p}_i$ tales que $(I : f) = \mathfrak{p}_i$. Entonces, por el teorema 2.1.7, se tiene que $\delta_I(d_1) = 1$. Así que $\operatorname{reg}(\delta_I) \leq \operatorname{v}(I)$.

Para ver la desigualdad contraria, escribimos $d_0 = \operatorname{reg}(\delta_I)$. Entonces $\delta_I(d_0) = 1$. Observamos que $\mathfrak{m}^{d_0} \not\subset I$, ya que si no $\mathcal{F}_{d_0} = \emptyset$ y por la definición $\delta_I(d_0)$ es igual a $\deg(S/I)$, una contradicción porque $I \subsetneq \mathfrak{m}$ y por el lema 1.5.22 $\deg(S/I) > 1$. Entonces, por el teorema 2.1.7, hay un $f \in S_{d_0} \setminus I$ tal que $\delta_I(d_0) = \deg(S/(I : f)) = 1$. Sea $I = \cap_{i=1}^m \mathfrak{q}_i$ la descomposición primaria minimal de I, donde $\mathfrak{q}_i$ es un ideal $\mathfrak{p}_i$-primario. Observamos que $(\mathfrak{q}_i : f)$ es un ideal primario si $f \notin \mathfrak{q}_i$ porque $S/(\mathfrak{q}_i : f)$ está inmerso en $S/\mathfrak{q}_i$. En consecuencia, la descomposición primaria de $(I : f)$ es $\cap_{f \notin \mathfrak{q}_i}(\mathfrak{q}_i : f)$. Por tanto, por la aditividad del grado 1.5.23, tenemos que $(I : f) = (\mathfrak{q}_k : f)$ para algún k tal que $f \notin \mathfrak{q}_k$ y $\deg(S/(\mathfrak{q}_k : f)) = 1$. Puesto que $S/\mathfrak{p}_k$ también tiene grado 1 y $(\mathfrak{q}_k : f) \subset \mathfrak{p}_k$, por el lema 1.5.22, tenemos que $(I : f) = (\mathfrak{q}_k : f) = \mathfrak{p}_k$, así que $\operatorname{v}(I) \leq \operatorname{reg}(\delta_I)$. □

A continuación vemos un lema que nos permite comparar la función distancia mínima generalizada de ideales relacionados por la contención.

Lema 2.1.19 [6, Lem. 4.17]**.** *Si I, I' son ideales homogéneos no mezclados de la misma altura y J es un ideal homogéneo tal que $I' = (I : J)$, entonces $\mathcal{F}_d(I') \subset \mathcal{F}_d(I)$ y*

$$\deg(S/I') - \delta_{I'}(d) \leq \deg(S/I) - \delta_I(d).$$

Demostración. Sea $f \in \mathcal{F}_d(I')$. Entonces $f \notin I'$ y $(I' : f) \neq I'$, y puesto que tenemos las siguientes relaciones

$$I' \subsetneq (I' : f) = ((I : J) : f) = (I : (fJ)) = ((I : f) : J)$$

deducimos que $(I : f) \neq I$ (si no el último ideal de la línea anterior sería I'). Observamos que $I \subset I'$, así que $f \notin I$. La segunda afirmación se deduce de la desigualdad

$$\begin{aligned} \deg(S/I') - \delta_{I'}(d) &= \text{máx}\{\deg(S/(I', f)) \mid f \in \mathcal{F}_d(I')\} \\ &\leq \text{máx}\{\deg(S/(I, g)) \mid g \in \mathcal{F}_d(I)\} = \deg(S/I) - \delta_I(d). \end{aligned}$$

Esta desigualdad es consecuencia de que si $f \in \mathcal{F}_d(I')$, entonces $\operatorname{ht}(I', f) = \operatorname{ht}(I')$, y puesto que $f \in \mathcal{F}_d(I)$ se tiene que $\operatorname{ht}(I, f) = \operatorname{ht}(I)$ por el lema 2.1.4 (a). Luego $\deg(S/(I', f)) \leq \deg(S/(I, f))$. □

Presentamos ahora uno de los resultados principales de la sección. La desigualdad del teorema siguiente cuando I es el ideal de anulación de un conjunto finito de puntos proyectivos es la cota de Singleton.

Teorema 2.1.20 [6, Thm. 4.19]**.** *Sea $I \subset S$ un ideal homogéneo no mezclado cuyos primos asociados están generados por formas lineales y tales que existe $h \in S_1$ regular en S/I. Si* $\dim(S/I) = 1$*, entonces*

$$\delta_I(d) \leq \deg(S/I) - H_I(d) + 1 \text{ para todo } d \geq 1.$$

Demostración. Hacemos la demostración por inducción en $\deg(S/I)$. Si $\deg(S/I) = 1$, entonces $I = \mathfrak{p}$ es un ideal primo generado por formas lineales, $H_I(d) = 1$ para todo $d \geq 0$ (ver 1.5.21) y $\mathcal{F}_d(I) = \emptyset$ para todo $d \geq 1$. Lo último se deduce de que para cualquier ideal primo $\mathfrak{p}$, $(\mathfrak{p} : f) \neq \mathfrak{p}$ implica que $f \in \mathfrak{p}$. Así que el resultado se verifica en este caso. Sea $v = \mathrm{v}(I)$ el v-número de I. Por la proposición 2.1.16, $v = \alpha((I : \mathfrak{p})/I)$ para algún $\mathfrak{p} \in \mathrm{Ass}(I)$. Sea $I' = (I : \mathfrak{p})$. La sucesión exacta corta

$$0 \longrightarrow I'/I \longrightarrow S/I \longrightarrow S/I' \longrightarrow 0$$

junto con la propiedad de que I es no mezclado demuestran que $\dim(I'/I) = 1$ y $\mathrm{depth}(I'/I) = 1$. En consecuencia, $H_{I'/I}(d) = 0$ para $d < \alpha((I : \mathfrak{p})/I) = v$ y $H_{I'/I}(d) > 0$ para $d \geq \alpha((I : \mathfrak{p})/I) = v$, así que $H_{I'}(d) = H_I(d)$ para $d < v$ y $H_I(d) > H_{I'}(d)$ para $d \geq v$. La última afirmación nos da que $\deg(S/I) > \deg(S/I')$. Esto también se deduce del lema 1.5.22 (b).

Si $d < v$ deducimos del lema 2.1.19, la hipótesis de inducción y $H_{I'}(d) = H_I(d)$ que

$$\deg(S/I) - \delta_I(d) \geq \deg(S/I') - \delta_{I'}(d) \geq H_{I'}(d) - 1 = H_I(d)_1,$$

que es la desigualdad que buscábamos. Si $d \geq v$, sabemos que existe $f \in S_v$ tal que $(I : f) = \mathfrak{p}$, así que $(I : h^{d-v}f) = \mathfrak{p}$. En consecuencia, $\delta_I(d) = 1$, y puesto que $\deg(S/I) \geq H_I(d)$ para cualquier d (ver 1.5.21), obtenemos el resultado. □

Sin embargo, la situación para $\dim(S/I) \geq 2$ es bastante diferente, como vemos en la siguiente proposición.

Proposición 2.1.21 [6, Prop. 4.21]**.** *Sea $I \subset S$ un ideal homogéneo no mezclado. Si* $\dim(S/I) \geq 2$*, entonces*

$$\delta_I(d) > \deg(S/I) - H_I(d) + 1 \text{ para algún } d \geq 1.$$

Demostración. Observamos que $\mathfrak{m} = (x_1, \ldots, x_n)$ no es un primo asociado de I, es decir, $\mathrm{depth}(S/I) \geq 1$ (porque es no mezclado de dimensión ≥ 2). Supongamos que $\mathcal{F}_d = \emptyset$ para algún $d \geq 2$. Como $H_I(0) = 1$ y $\delta_I(d)$ es igual a $\deg(S/I)$, por el teorema 1.5.21, se tiene que $H_I(d) > 1$ y se da la igualdad. Supongamos ahora que $\mathcal{F}_d \neq \emptyset$ para $d \geq 2$. Para cada $d \geq 2$, elegimos $f_d \in \mathcal{F}_d$ tal que

$$\delta_I(d) = \deg(S/I) - \deg(S/(I, f_d)).$$

Como H_I es estrictamente creciente por el teorema 1.5.21, usando el lema 2.1.4 (b), obtenemos

$$\deg(S/(I, f_d)) < \deg(S/I) < H_I(d) - 1$$

para $d \gg 0$. En consecuencia, se da la desigualdad buscada para $d \gg 0$. □

Para calcular la función distancia mínima, podemos utilizar el siguiente resultado.

Proposición 2.1.22 [22, Thm. 6.1]. *Fijamos un orden monomial $\prec$ en S. Si $\Delta_\prec(I) \cap S_d = \{x^{\alpha_1}, \ldots, x^{\alpha_s}\}$ y $F_{\prec,d} = \{f = \sum_i \lambda_i x^{\alpha_i} \mid f \neq 0, \lambda_i \in K, (I : f) \neq I\}$, entonces*

$$\begin{aligned}\delta_I(d) &= \deg(S/I) - \max\{\deg(S/(I,f)) \mid f \in \mathcal{F}_d\} \\ &= \deg(S/I) - \max\{\deg(S/(I,f)) \mid f \in \mathcal{F}_{\prec,d}\}.\end{aligned}$$

Demostración. Sea f un elemento cualquiera de $\mathcal{F}_d$, y sea $\mathcal{G} = \{g_1, \ldots, g_r\}$ una base de Gröbner de I. Por el algoritmo de división 1.6.4, podemos escribir $f = g + h$, donde $g = \sum_{i=1}^r a_i g_i \in I$ y h es un polinomio homogéneo estándar de S/I de grado d. Vemos que $(I : f) = (I : h)$, así que $h \in \mathcal{F}_{\prec,d}$. Como además se tiene que $(I, f) = (I, h)$, se obtiene el resultado. □

Observación 2.1.23. Vemos que $\mathcal{F}_d \neq \emptyset$ si y solo si $\mathcal{F}_{\prec,d} \neq \emptyset$. Si $K = \mathbb{F}_q$ es un cuerpo finito, entonces el número de polinomios estándar de grado d es $q^l - 1$, donde l es el número de monomios estándar de grado d. Por tanto, se puede calcular $\delta_I(d)$ para valores pequeños de l y q.

Se pueden obtener cotas superiores de $\delta_I(d)$ fijando un subconjunto $\mathcal{F}'_{\prec,d}$ de $\mathcal{F}_{\prec,d}$ y calculando

$$\delta'_I(d) = \deg(S/I) - \max\{\deg(S/(I,f)) \mid f \in \mathcal{F}'_{\prec,d}\} \geq \delta_I(d).$$

Es habitual usar el conjunto $\mathcal{F}'_{\prec,d} = \{f = \sum_i \lambda_i x^{\alpha_i} \mid f \neq 0, \lambda_i \in \{0,1\}, (I : f) \neq I\}$ o un subconjunto de él.

Encontrar cotas inferiores de $\delta_I(d)$ es más difícil. Para estimar $\delta_I(d)$ por debajo se introduce la *función huella* de I en la sección 2.2.

2.2. Función huella

En esta sección introducimos la función huella de un ideal I. Esta función numérica se define de manera similar a la función distancia mínima δ_I, pero utilizando un orden monomial y el ideal inicial de I. El objetivo es ver que bajo ciertas condiciones la función huella es una cota inferior de la función distancia mínima. En consecuencia, también es importante ver cuando la función huella es mayor que 1, ya que entonces nos servirá para acotar la distancia mínima en el caso de códigos (cuando $I = I(\mathbb{X})$ es el ideal de anulación de un conjunto finito de puntos del espacio proyectivo).

Denotaremos por $\mathcal{M}_{\prec,d}$ al conjunto de los divisores de cero de $S/\operatorname{in}_\prec(I)$ de grado $d \geq 1$ que están en $\Delta_\prec(I)$:

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

Definición 2.2.1. La *función huella* de I, denotada por fp_I, es la función $\mathrm{fp}_I : \mathbb{N}_+ \to \mathbb{Z}$ dada por

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

Teorema 2.2.2 [23, Thm. 2.3.2]**.** *Sea I un ideal homogéneo no mezclado y sea $\prec$ un orden monomial. Se tiene lo siguiente.*

(a) $\delta_I(d) \geq \mathrm{fp}_I(d)$ *y* $\delta_I(d) \geq 0$ *para* $d \geq 1$.

(b) $\mathrm{fp}_I(d) \geq 0$ *si* $\mathrm{in}_\prec(I)$ *es no mezclado.*

Demostración. Lo demostramos con mayor generalidad en 2.4.10. □

Si $\mathrm{fp}_I(d) = \delta_I(d)$ para $d \geq 1$ (y un cierto orden monomial $\prec$), en ocasiones se dice que I es un *ideal Geil-Carvalho* (para ese orden). El siguiente resultado nos da una condición para que I sea Geil-Carvalho.

Proposición 2.2.3 [23, Prop. 2.3.3]**.** *Si I es un ideal monomial no mezclado y $\prec$ es un orden monomial cualquiera, entonces $\delta_I(d) = \mathrm{fp}_I(d)$ para $d \geq 1$.*

Demostración. Lo demostraremos con mayor generalidad en 2.4.12. □

A continuación vemos que en algunos casos se puede expresar la función huella en términos del grado de ideales cociente.

Corolario 2.2.4 [22, Cor. 3.4]**.** *Sea I un ideal homogéneo y sea $\prec$ un orden monomial. Si* $\mathrm{in}_\prec(I)$ *es un ideal no mezclado y $\mathcal{M}_{\prec,d} \neq \emptyset$, entonces*

$$\mathrm{fp}_I(d) = \min\{\deg(S/(\mathrm{in}_\prec(I) : x^\alpha)) \mid x^\alpha \in S_d \setminus \mathrm{in}_\prec(I)\}.$$

Demostración. Sea $x^\alpha \in \mathcal{M}_{\prec,d}$. Por el lema 2.1.5 (b) se tiene la igualdad

$$\deg(S/(\mathrm{in}_\prec(I) : x^\alpha)) = \deg(S/\mathrm{in}_\prec(I)) - \deg(S/(\mathrm{in}_\prec(I), x^\alpha)).$$

En este caso $\deg(S/(\mathrm{in}_\prec(I) : x^\alpha)) \leq \deg(S/\mathrm{in}_\prec(I))$. En consecuencia, observando que $\deg(S/\mathrm{in}_\prec(I))$ es igual a $\deg(S/I)$, obtenemos

$$\begin{aligned} \mathrm{fp}_I(d) &= \deg(S/I) - \max\{\deg(S/(\mathrm{in}_\prec(I), x^\alpha)) \mid x^\alpha \in \mathcal{M}_{\prec,d}\} \\ &= \min\{\deg(S/(\mathrm{in}_\prec(I) : x^\alpha)) \mid x^\alpha \in \mathcal{M}_{\prec,d}\} \\ &= \min\{\deg(S/(\mathrm{in}_\prec(I) : x^\alpha)) \mid x^\alpha \in S_d \setminus \mathrm{in}_\prec(I)\}. \end{aligned}$$

□

El siguiente resultado mejora ligeramente la cota inferior para la función huella obtenida en el teorema 2.2.2.

Proposición 2.2.5 [23, Prop. 2.3.6]**.** *Sea $I \subset S$ un ideal homogéneo no mezclado, sea $\prec$ un orden monomial en S, y sea $d \geq 1$ un entero. Entonces $\mathrm{fp}_I(d) \geq 1$ si $\mathrm{in}_\prec(I)$ es no mezclado.*

Demostración. Si $\mathcal{M}_{\prec,d} = \emptyset$, entonces $\mathrm{fp}_I(d) = \deg(S/I) \geq 1$. Supongamos ahora que $\mathcal{M}_{\prec,d} \neq \emptyset$. Como $\mathrm{in}_\prec(I)$ es no mezclado, por el corolario 2.2.4, $\mathrm{fp}_I(d) \geq 1$. Esto también es consecuencia del resultado más general 2.4.10. □

2.3. Fórmulas para intersecciones completas

En esta sección estudiamos la función huella, con respecto a un orden monomial $\prec$ que supondremos *graduado*, de ideales homogéneos de $S = K[x_1, \ldots, x_n]$ que son intersección completa. Para ideales homogéneos de dimensión ≥ 1 (por ejemplo los correspondientes a los códigos que hemos definido), cuyo ideal inicial sea una intersección completa, se obtiene una fórmula para la función huella y una cota inferior fina para la correspondiente función distancia mínima. Como referencia, utilizamos principalmente [20], [22] y [23].

Comenzamos con la siguiente desigualdad entre números enteros, que es algo tediosa de probar y por eso no incluimos la demostración.

Proposición 2.3.1 [20, Prop. 5.7]**.** *Sean $1 \leq e_1 \leq \cdots \leq e_m$ y $0 \leq b_i \leq e_i - 1$ para $i = 1, \ldots, m$ enteros, y sea b_0 otro entero. Si $b_0 \geq 1$, entonces*

$$\prod_{i=1}^{m}(e_i - b_i) \geq \left(\sum_{i=1}^{k+1}(e_i - b_i) - (k-1) - b_0 - \sum_{i=k+2}^{m} b_i\right) e_{k+2} \cdots e_m$$

para $k = 0, \ldots, m-1$, donde $e_{k+2} \ldots e_m = 1$ y $\sum_{i=k+2}^{m} b_i = 0$ si $k = m-1$.

Proposición 2.3.2 [22, Prop. 5.1]**.** *Sea $I \subset S$ un ideal homogéneo y sea $\prec$ un orden monomial. Supongamos que $\mathrm{in}_\prec(I)$ es una intersección completa de altura r generada por $x^{\alpha_1}, \ldots, x^{\alpha_r}$ con $d_i = \deg(x^{\alpha_i})$ y $d_i \geq 1$ para todo i. Se da lo siguiente.*

(a) *I es una intersección completa y $\dim(S/I) = n - r$.*

(b) *$\deg(S/I) = d_1 \cdots d_r$ y $\mathrm{reg}(S/I) = \sum_{i=1}^{r}(d_i - 1)$.*

(c) *$1 \leq \mathrm{fp}_I(d) \leq \delta_I(d)$ para $d \geq 1$.*

Demostración.

(a) Los anillos S/I y $S/\mathrm{in}_\prec(I)$ tienen la misma dimensión. En consecuencia, $\dim(S/I) = n - r$. Como $\prec$ es un orden graduado, existen $f_1, \ldots, f_r$ polinomios homogéneos en I con $\mathrm{in}_\prec(f_i) = x^{\alpha_i}$ para $i \geq 1$. Puesto que

$$\mathrm{in}_\prec(I) = (\mathrm{in}_\prec(f_1), \ldots, \mathrm{in}_\prec(f_r)),$$

los polinomios $f_1, \ldots, f_r$ forman una base de Gröbner de I, y en particular generan I. Así que I es un ideal homogéneo de altura r generado por r polinomios, es decir, I es una intersección completa.

(b) Se deduce directamente de la parte (a) y el lema 1.5.17.

(c) Usando la parte (a) y la proposición 1.3.12 tenemos que I es un ideal no mezclado Cohen-Macaulay. El resultado se deduce del teorema 2.2.2 y la proposición 2.2.5 ($\text{in}_\prec(I)$ es una intersección completa, luego por 1.3.12 también es no mezclado).

□

Lema 2.3.3 [22, Lem. 5.2]**.** *Sea $I \subset S$ un ideal que es una intersección completa generado minimalmente por $x^{\alpha_1}, \ldots, x^{\alpha_r}$ y sea $x^a = x_1^{a_1} \cdots x_n^{a_n}$ un divisor de cero de S/I que no está en I. Se da lo siguiente.*

(a) *x^{α_i} y x^{α_j} no tienen variables en común para $i \neq j$.*

(b) *Si $x_j^{a_j}$ es regular en S/I y $x^c = x^a/x_j^{a_j}$, entonces $(I : x^a) = (I : x^c)$.*

(c) *Si x_j es un divisor de cero en S/I, entonces existe un único $\alpha_i = (\alpha_{i,1}, \ldots, \alpha_{i,n})$ tal que $\alpha_{i,j} > 0$, es decir, x_j aparece en exactamente un x^{α_i}. Si $\alpha_j > \alpha_{i,j}$ y $x^c = x^a/x_j$, entonces $(I : x^a) = (I : x^c)$.*

(d) *Para cada i existe un x^{β_i} que divide a x^{α_i} de manera que $\deg(x^{\beta_i}) < \deg(x^{\alpha_i})$ y $(I : x^a) = (I : x^\beta)$, donde $x^\beta = x^{\beta_1} \cdots x^{\beta_r}$.*

Demostración.

(a) Supongamos que x^{α_i} y x^{α_j} tienen alguna variable en común, con $i < j$, y de manera que no haya $i < k < j$ tal que x^{α_k} tenga una variable en común con x^{α_i}. Denotamos $m = \text{mcm}(x^{\alpha_i}, x^{\alpha_j})$, $d = \text{mcd}(x^{\alpha_i}, x^{\alpha_j})$. Entonces $\overline{m} = \bar{0}$ en $S/(x^{\alpha_1}, \ldots, x^{\alpha_{j-1}})$, y $m = x^{\alpha_j}(x^{\alpha_i}/d)$, luego x^{α_j} no es regular en $S/(x^{\alpha_1}, \ldots, x^{\alpha_{j-1}})$, una contradicción.

(b) La inclusión "$\supset$" es obvia. Para ver la otra inclusión, consideramos x^δ en $(I : x^a)$, es decir, $x^\delta x^a = x^\delta x_j^{a_j} x^c$ está en I. En consecuencia, $x^\delta x^c$ está en I porque $x_j^{a_j}$ es regular en S/I. Luego x^δ está en $(I : x^c)$.

(c) Si x_j es un divisor de cero en S/I, entonces x_j está en algún primo asociado de S/I. En consecuencia, por la parte (a), x_j debe aparecer en un único x_i^α para algún i. Luego se tiene que $\alpha_{i,j} > 0$. Afirmamos que $((x^{\alpha_k}) : x^a) = ((x^{\alpha_x}) : x^c)$ para todo k. Si $k \neq i$, por la parte (a), x_j es regular en $S/(x^{\alpha_k})$. En consecuencia, como en la demostración de la parte (b), obtenemos la igualdad correspondiente. Ahora suponemos que $k = i$. La inclusión "$\supset$" es obvia. Para ver la otra inclusión, consideramos x^δ en $((x^{\alpha_i}) : x^a)$, es decir, $x^\delta x^a = x^\gamma x^{\alpha_i}$ para algún x^γ. Puesto que $a_j > \alpha_{i,j} > 0$, x_j debe dividir a x^γ. Entonces podemos escribir $x^\delta x^c = x^\omega x^{\alpha_i}$, donde $x^\omega = x^\gamma/x_j$. Así que x^δ está en $((x^{\alpha_i}) : x^c)$. Esto completa la prueba de la afirmación anterior. En consecuencia se tiene que

$$\begin{aligned}(I : x^a) &= ((x^{\alpha_1}) : x^a) + \cdots + ((x^{\alpha_r}) : x^a) \\ &= ((x^{\alpha_1}) : x^c) + \cdots + ((x^{\alpha_r}) : x^c) = (I : x^c).\end{aligned}$$

(d) Usando la parte (a) y sucesivamente aplicando las partes (b) y (c) a x^a, obtenemos un monomio x^β que divide a x^a tal que se satisfacen las siguientes condiciones: (1) todas las variables que aparecen en x^β son divisores de cero en S/I, (2) si $x^\beta = x_1^{\gamma_1} \cdots x_n^{\gamma_n}$ y $\gamma_j > 0$, entonces $\alpha_{i,j} \geq \gamma_{i,j}$, donde x^{α_i} es el único monomio, entre $x^{\alpha_1}, \ldots, x^{\alpha_r}$, que contiene a x_j, y (3) $(I : x^a) = (I : x^\beta)$. Sea x^{β_i} el producto de todos los $x_j^{\gamma_j}$ tales que x_j aparece en x^{α_i}. Claramente x^{β_i} divide a x^{α_i}, y $\deg(x^{\alpha_i}) > \deg(x^{\beta_i})$ porque x^a no está en I por hipótesis.

□

El siguiente resultado da apoyo a la conjetura 2.1.14.

Proposición 2.3.4 [22, Prop. 5.3]**.** *Sea $I \subset S$ un ideal monomial de dimensión ≥ 1 y que es una intersección completa generada minimalmente por $x^{\alpha_1}, \ldots, x^{\alpha_r}$. Si $d_i = \deg(x^{\alpha_i})$ para $i = 1, \ldots, r$, se da lo siguiente.*

(a) $\operatorname{reg}(S/I) = \sum_{i=1}^{r}(d_i - 1)$,

(b) $\delta_I(d) = 1$ *si* $d \geq \operatorname{reg}(S/I)$,

(c) $\delta_I(d) \leq (d_{k+1} - l)d_{k+2} \cdots d_r$ *si* $d < \operatorname{reg}(S/I)$, *donde* $0 \leq k \leq r-1$ *y* l *son enteros tales que* $d = \sum_{i=1}^{k}(d_i - 1) + l$ *y* $1 \leq l \leq d_{k+1} - 1$.

Demostración.

(a) Se deduce directamente del lema 1.5.17.

(b) Por el lema 2.3.3 (a), los monomios x^{α_i} y x^{α_j} no tienen variables en común para $i \neq j$. Para cada i elegimos x_{j_i} en x^{α_i}. Si I es primo, entonces $I = (x_{j_1}, \ldots, x_{j_r})$, $\operatorname{reg}(S/I) = 0$, $\mathcal{F}_d = \emptyset$ y $\delta_I(d) = 1$ para $d \geq 1$. En consecuencia, podemos suponer que I no es primo. Afirmamos que $\mathcal{F}_d \neq \emptyset$ para $d \geq 1$. Como I no es primo, existe un m tal que x_{j_m} es un divisor de cero en S/I que no está en I. Si una variable x_t no está en x^{α_i} para ningún i, entonces x_t es un elemento regular en S/I, y $\mathcal{F}_d \neq \emptyset$ porque $x_{j_m}x_t^{d-1}$ está en $\mathcal{F}_d$. Si cualquier variable x_t está en x^{α_i} para algún i, entonces cualquier monomio de grado d es un divisor de cero en S/I porque cualquier variable x_t pertenece al menos a algún primo asociado de S/I. Como $\dim(S/I) \geq 1$, se tiene que $\mathfrak{m}^d \not\subset I$. Elegimos un monomio x^a de grado d que no esté en I. Entonces $\mathcal{F}_d \neq \emptyset$ porque x^a está en $\mathcal{F}_d$. Esto completa la demostración de la afirmación que hemos hecho. Escribimos $x^{c_i} = x^{\alpha_i}/x_{j_i}$ para $i = 1, \ldots, r$ y $x^c = x^{c_1} \cdots x^{c_r}$. Entonces se ve que $(I : x^c) = (x_{j_1}, \ldots, x_{j_r})$ y $\deg(S/(I : x^c) = 1$. Observamos que x^c es un divisor de cero en S/I, $x^c \notin I$ y $\deg(x^c) = \operatorname{reg}(S/I)$ (apartado (a)). En consecuencia, por el teorema 2.1.7, obtenemos que $\delta_I(d) = 1$ para $d = \operatorname{reg}(S/I)$. En consecuencia, por el teorema 2.1.9 (b), deducimos que $\delta_I(d) = 1$ para $d \geq \operatorname{reg}(S/I)$.

(c) Existe un monomio x^a de grado l que divide a $x^{\alpha_{k+1}}$ porque l es un entero positivo menor o igual a $d_{k+1} - 1$. De nuevo escribimos $x^{c_i} = x^{\alpha_i}/x_{j_i}$, $x^c = x^{c_1} \cdots x^{c_k}x^a$ y $x^\gamma = x^{\alpha_{k+1}}/x^a$. Entonces tenemos que

$$(I : x^c) = (x_{j_1}, \ldots, x_{j_k}, x^\gamma, x^{\alpha_{k+2}}, \ldots, x^{\alpha_r}).$$

En consecuencia, por el lema 1.5.17, tenemos que $\deg(S/(I : x^c)) = (d_{k+1} - l)d_{k+2} \cdots d_r$ porque $(I : x^c)$ es una intersección completa. Puesto que $\deg(x^c) = d = \sum_{i=1}^{k}(d_i - 1) + l$, x^c no está en I, y x^c es un divisor de cero en S/I, por el teorema 2.1.7 obtenemos que $\deg(S/(I : x^c)) \geq \delta_I(d)$, como se pedía.

□

A continuación presentamos el resultado principal de esta sección.

Teorema 2.3.5 [22, Thm. 5.5]**.** *Sea $I \subset S$ un ideal monomial de dimensión ≥ 1 que es una intersección completa y que está generado minimalmente por $x^{\alpha_1}, \ldots, x^{\alpha_r}$, y sea $d \geq 1$ un entero. Si $d_i = \deg(x^{\alpha_i})$ para $i = 1, \ldots, r$ y $d_1 \leq \cdots \leq d_r$, entonces*

$$\delta_I(d) = \mathrm{fp}_I(d) = \begin{cases} (d_{k+1} - l)d_{k+2} \cdots d_r & \text{si } d < \sum_{i=1}^{r}(d_i - 1), \\ 1 & \text{si } d \geq \sum_{i=1}^{r}(d_i - 1), \end{cases}$$

donde $0 \leq k \leq r - 1$ y l son los únicos enteros tales que $d = \sum_{i=1}^{k}(d_i - 1) + l$ y $1 \leq l \leq d_{k+1} - 1$.

Demostración. Por 1.3.12, I es no mezclado. En consecuencia, por la proposición 2.2.3, $\delta_I(d) = \mathrm{fp}_I(d)$ para $d \geq 1$. En consecuencia, por la proposición 2.3.4, es suficiente con ver que

$$\mathrm{fp}_I(d) \geq (d_{k+1} - 1)d_{k+2} \cdots d_r \text{ para } d < \mathrm{reg}(S/I).$$

Sea x^a un monomio de grado d tal que $x^a \notin I$ y $(I : x^a) \neq I$. Por el lema 2.3.3 (d), para cada i existe un monomio x^{β_i} que divide a x^{α_i}, con $\deg(x^{\beta_i}) < \deg(x^{\alpha_i})$ y $(I : x^a) = (I : x^\beta)$, donde $x^\beta = x^{\beta_1} \cdots x^{\beta_r}$. Se puede escribir

$$x^{\alpha_i} = x_1^{\alpha_{i,1}} \cdots x_n^{\alpha_{i,n}} \text{ y } x^{\beta_i} = x_1^{\beta_{i,1}} \cdots x_n^{\beta_{i,n}}$$

para $i = 1, \ldots, r$. Por el lema 2.3.3 (a), los monomios x^{α_i} y x^{α_j} no tienen variables en común para $i \neq j$. Como $(I : x^\beta)$ es un ideal monomial, se deduce que

$$(I : x^a) = (I : x^\beta) = (\{x_1^{\alpha_{i,1} - \beta_{i,1}} \cdots x_n^{\alpha_{i,n} - \beta_{i,n}}\}_{i=1}^{r}).$$

Por tanto, considerando $g_i = x_1^{\alpha_{i,1} - \beta_{i,1}} \cdots x_n^{\alpha_{i,n} - \beta_{i,n}}$ para $i = 1, \ldots, r$ y observando que g_i y g_j no tienen variables en común para $i \neq j$, tenemos que $g_1, \ldots, g_r$ forman una sucesión regular, es decir, $(I : x^a)$ es de nuevo una intersección completa. Así que, por el lema 1.5.17, obtenemos

$$\deg(S/(I : x^a)) = \prod_{i=1}^{r}\left(\sum_{j=1}^{n}(\alpha_{i,j} - \beta_{i,j})\right) = \prod_{i=1}^{r}(\deg(x^{\alpha_i}) - \deg(x^{\beta_i})).$$

En consecuencia, tomando $b_i = \deg(x^{\beta_i})$ para $i = 1, \ldots, r$, obtenemos

$$\deg(S/(I : x^a)) = \prod_{i=1}^{r}(d_i - b_i).$$

Luego, por el teorema 2.1.7, es suficiente con ver la desigualdad

$$\deg(S/(I : x^a)) = \prod_{i=1}^{r}(d_i - b_i) \geq (d_{k+1} - l)d_{k+2} \cdots d_r.$$

Observando que $d = \deg(x^a) = \sum_{i=1}^{k}(d_i - 1) + l \geq \deg(x^\beta) = \sum_{i=1}^{r} b_i$, se tiene que

$$\left(d_{k+1} + \sum_{i=1}^{k}(d_i - 1) - \sum_{i=1}^{r} b_i\right) d_{k+2} \cdots d_r \geq (d_{k+1} - l)d_{k+2} \cdots d_r.$$

Deducimos que es suficiente con probar la desigualdad

$$\prod_{i=1}^{r}(d_i - b_i) \geq \left(\sum_{i=1}^{k+1}(d_i - b_i) - k - \sum_{i=k+2}^{r} b_i\right) d_{k+2} \cdots d_r,$$

que se obtiene a partir de la proposición 2.3.1 con $b_0 = 1$ y $m = r$. □

Teorema 2.3.6 [22, Thm. 5.6]**.** *Sea $I \subset S$ un ideal homogéneo de dimensión ≥ 1 y sea $\prec$ un orden monomial. Si $\mathrm{in}_\prec(I)$ es una intersección completa de altura r generada por $x^{\alpha_1}, \ldots, x^{\alpha_r}$ con $d_i = \deg(x^{\alpha_i})$ y $1 \leq d_i \leq d_{i+1}$ para $i \geq 1$, entonces $\delta_I(d) \geq \mathrm{fp}_I(d) \geq 1$ y la función huella en grado $d \geq 1$ viene dada por*

$$\mathrm{fp}_I(d) = \begin{cases} (d_{k+1} - l)d_{k+2} \cdots d_r & \text{si } 1 \leq d < \sum_{i=1}^{r}(d_i - 1), \\ 1 & \text{si } d \geq \sum_{i=1}^{r}(d_i - 1), \end{cases}$$

donde $0 \leq k \leq r - 1$ y l son los únicos enteros tales que $d = \sum_{i=1}^{k}(d_i - 1) + l$ y $1 \leq l \leq d_{k+1} - 1$.

Demostración. Por la proposición 2.3.2 se tiene que $\delta_I(d) \geq \mathrm{fp}_I(d) \geq 1$. Puesto que $\mathrm{fp}_I(d)$ es igual a $\mathrm{fp}_{\mathrm{in}_\prec(I)}(d)$ para $d \geq 1$, la fórmula para $\mathrm{fp}_I(d)$ se deduce directamente del teorema 2.3.5. □

Saber si en el teorema 2.3.6 se da la igualdad $\delta_I(d) = \mathrm{fp}_I(d)$ para $d \geq 1$ es una pregunta abierta (para algún orden). En el teorema 2.3.5 hemos visto un caso en el que se obtiene la igualdad. En el capítulo 3 veremos algunas aplicaciones y ejemplos de estos resultados para el caso de códigos cartesianos.

La fórmula del teorema 2.3.5 también es válida en dimensión 0 para $d < \sum_{i=1}^{r}(d_i - 1)$. Ahora, para $d \geq \sum_{i=1}^{r}(d_i - 1)$, el conjunto $\mathcal{F}_d$ es vacío porque $(S/I)_d = (0)$, así que por definición tenemos que $\delta_I(d) = \deg(S/I)$.

La aplicación más básica es para intersecciones completas en $\mathbb{P}^1$.

Corolario 2.3.7 [23, Cor. 2.5.10]**.** *Si* $\mathbb{X}$ *es un subconjunto finito de* $\mathbb{P}^1$ *e* $I(\mathbb{X})$ *es una intersección completa, entonces*

$$\delta_{I(\mathbb{X})}(d) = \mathrm{fp}_{I(\mathbb{X})}(d) = \begin{cases} |\mathbb{X}| - d & si\ 1 \leq d \leq |\mathbb{X}| - 2, \\ 1 & si\ d \geq |\mathbb{X}| - 1. \end{cases}$$

Demostración. Sea f el generador de $I(\mathbb{X})$. En este caso $d_1 = \deg(f) = |\mathbb{X}|$ y $\mathrm{reg}(S/I(\mathbb{X})) = |\mathbb{X}| - 1$. Por la proposición 1.8.9 y el teorema 2.3.6 se tiene que

$$\delta_{\mathbb{X}}(d) = \delta_{I(\mathbb{X})}(d) \geq \mathrm{fp}_{I(\mathbb{X})}(d) = |\mathbb{X}| - d \text{ para } 1 \leq d \leq |\mathbb{X}| - 2,$$

y $\delta_{\mathbb{X}}(d) = 1$ para $d \geq |\mathbb{X}| - 1$ (la igualdad $\delta_{\mathbb{X}}(d) = \delta_{I(\mathbb{X})}(d)$ la veremos con mayor generalidad en el capítulo siguiente). Supongamos que $1 \leq d \leq |\mathbb{X}| - 2$. Elegimos $[P_1], \ldots, [P_d]$ puntos en $\mathbb{P}^1$. Por el lema 1.7.3, el ideal de anulación $I_{[P_i]}$ de $[P_i]$ es un ideal principal generado por una forma lineal h_i. Observamos que $V_{\mathbb{X}}(h_i)$, el conjunto de ceros de h_i en $\mathbb{X}$, es igual a $\{[P_i]\}$. Considerando $h = h_1 \cdots h_d$, obtenemos un polinomio homogéneo de grado d con exactamente d ceros. En consecuencia, $\delta_{\mathbb{X}}(d) \leq |\mathbb{X}| - d$. □

Ejemplo 2.3.8. Consideramos el ideal $I = (x_3^4 - x_4^4, x_2^4 - x_4^4, x_1^4 - x_4^4) \subset S = K[x_1, \ldots, x_4]$, con $K = \mathbb{F}_5$. Se puede comprobar que $\mathrm{in}_{\prec}(I) = (x_1^4, x_2^4, x_3^4)$ para el orden $\prec$ lexicográfico inverso graduado con $x_1 \succ x_2 \succ x_3 \succ x_4$. Por tanto, tenemos que el inicial de I es una intersección completa de altura 3. Así que utilizando el teorema 2.3.6 podemos obtener $\mathrm{fp}_I(d)$. En esta situación tenemos $r = 3$, $d_1 = d_2 = d_3 = 4$, y $\sum_{i=1}^{r}(d_i - 1) = 9$. Aplicando el teorema obtenemos:

d	1	2	3	4	5	6	7	8	9
$\mathrm{fp}_I(d)$	48	32	16	12	8	4	3	2	1

Con el siguiente procedimiento en [12] podemos comprobar el resultado usando directamente la definición de la función huella:

```
q=5
G=GF(q,Variable=>a)
S=G[x_1..x_4];
I=ideal(x_3^4-x_4^4,x_2^4-x_4^4,x_1^4-x_4^4)
M=coker gens gb I, degree M, regularity M
init=ideal(leadTerm gens gb I)
fp=(d) ->degree M -max apply(flatten entries basis(d,M),x-> if not
quotient(init,x)==init then degree ideal(init,x) else 0)
apply(1..regularity M, x->fp(x))
```

Podemos aprovechar este ejemplo sencillo para comentar cómo funciona el procedimiento anterior en Macaulay2, ya que los siguientes, que serán más complicados, se pueden entender con facilidad si se entiende este. En primer lugar, con

`G=GF(q,Variable=>a)` definimos el cuerpo donde vamos a trabajar, con tamaño q (potencia de un primo) y raíz primitiva a. El anillo de polinomios y el ideal que consideramos se define de la forma que aparece en el procedimiento. Posteriormente definimos `M=coker gens gb I`, que no es otra cosa que S/I, ya que lo que hacemos es calcular una base de Gröbner de I, coger el conjunto de generadores $\{g_1, \ldots, g_l\}$, y calcular el conúcleo del morfismo φ que va de S^l en S definido por $\varphi(e_i) = g_i$, donde e_i tiene todas las componentes nulas menos la i-ésima, que es 1. Obviamente, $\mathrm{Im}(\varphi) = I$ y $\mathrm{coker}(\varphi) = S/\mathrm{Im}(\varphi) = S/I$. Al poner `degree M, regularity M` simplemente imprimimos en pantalla el grado y la regularidad de S/I.

Con `init=ideal(leadTerm gens gb I)` simplemente tomamos los generadores de una base de Gröbner de I y consideramos el ideal generado por sus términos iniciales, que es el inicial de I. A continuación, al escribir `fp=(d)->f(d)` y después de la flecha una función $f(d)$ que dependa de d, lo que hacemos es definir una función $\mathrm{fp}(d)$ que asigna a cada valor de d lo que aparece después de la flecha. En este caso, lo que hacemos a la derecha es calcular la función huella según la definición. Para ello, usamos `apply(lista,función)`, que devuelve la lista que se obtiene al aplicar la función de la derecha a cada elemento de la lista que se da como argumento. Esta función que aplicamos se puede definir con `x->f(x)` de manera análoga a lo que ya hemos explicado. En este caso la lista que queremos usar son los monomios de grado d de la huella del ideal, así que consideramos una base de grado d de S/I con `basis(d,M)`, consideramos la lista de sus elementos con `entries`, y eliminamos separadores innecesarios con `flatten`. La función que aplicamos sobre cada elemento x de esta lista nos devuelve el grado del ideal $\mathrm{in}(I) + x$ si $(\mathrm{in}(I) : x) \neq I$, y 0 en otro caso, luego con considerar el máximo de la lista que se obtiene y restarlo del grado de I se obtiene el valor de la función huella. Finalmente, utilizamos otro `apply` para obtener la lista de valores de $\mathrm{fp}(d)$ para $1 \leq d \leq \mathrm{reg}(S/I)$.

2.4. Generalizaciones

En esta sección vamos a generalizar la noción de función distancia mínima y de función huella, de manera que, adelantando lo que vamos a ver en el capítulo 3, podremos tratar no solo la distancia mínima de los códigos tipo Reed-Muller proyectivos, si no también los pesos generalizados de Hamming. La razón de no hacer un tratamiento totalmente unificado directamente en el caso general es porque el caso de la distancia mínima ha recibido más atención y hay resultados adicionales interesantes (además de que para generalizar algunos resultados es necesario hacer hipótesis adicionales). Como referencias, vamos a utilizar principalmente [6] y [14].

Sean $d, r \in \mathbb{N}_+$. Definimos $\mathcal{F}_{d,r}$ como el conjunto

$$\begin{aligned}\mathcal{F}_{d,r} =&\{\{f_1, \ldots, f_r\} \subset S_d \mid \overline{f_1}, \ldots, \overline{f_r} \text{ son linealmente independientes sobre K,} \\ &(I : (f_1, \ldots, f_r)) \neq I\},\end{aligned}$$

donde $\overline{f} = f + I$ es la clase de f módulo I.

Observación 2.4.1. $\mathcal{F}_{d,1}$ es el conjunto $\mathcal{F}_d$ que hemos definido anteriormente.

Definición 2.4.2. Sea $I \subset S$ un ideal homogéneo. La *función distancia mínima generalizada* de I es la función $\delta_I : \mathbb{N}_+ \times \mathbb{N}_+ \to \mathbb{Z}$ dada por

$$\delta_I(d,r) = \begin{cases} \deg(S/I) - \text{máx}\{\deg(S/(I,F)) \mid F \in \mathcal{F}_{d,r}\} & \text{si } \mathcal{F}_{d,r} \neq \emptyset, \\ \deg(S/I) & \text{si } \mathcal{F}_{d,r} = \emptyset. \end{cases}$$

Observación 2.4.3. Para $r = 1$ obtenemos la función distancia mínima: $\delta_I(d,1) = \delta_I(d)$. Ahora podemos observar también que para tratar la función distancia mínima habría sido suficiente obtener resultados sobre $S/(I,f)$ con $f \in S$, en vez de $S/(I,F)$ para un conjunto de polinomios F, pero varios de los lemas y resultados que hemos utilizado están enunciados en el caso más general de un conjunto de polinomios, ya que de esta manera podemos utilizarlos directamente en esta nueva situación.

A continuación vamos a introducir un resultado que va a ser útil a la hora de realizar cálculos. Para ello, primero tenemos que definir un nuevo conjunto. Sea $\prec$ un orden monomial, y sea $\mathcal{F}_{\prec,d,r}$ el conjunto de todos los subconjuntos $F = \{f_1, \ldots, f_r\}$ de S_d tales que $(I : (F)) \neq I$, f_i es un polinomio estándar para todo i, $\overline{f_1}, \ldots, \overline{f_r}$ son linealmente independientes sobre el cuerpo K, y $\text{in}_\prec(f_1), \ldots, \text{in}_\prec(f_r)$ son monomios distintos. Sea $F = \{f_1, \ldots, f_r\}$ un conjunto de polinomios estándar. Es fácil ver que $\overline{f_1}, \ldots, \overline{f_r}$ son linealmente independientes sobre K si $\text{in}_\prec(f_1), \ldots, \text{in}_\prec(f_r)$ son monomios distintos.

Proposición 2.4.4 [14, Prop. 4.8]**.** *La función distancia mínima generalizada de I está dada por*

$$\delta_I(d,r) = \begin{cases} \deg(S/I) - \text{máx}\{\deg(S/(I,F)) \mid F \in \mathcal{F}_{\prec,d,r}\} & \textit{si } \mathcal{F}_{\prec,d,r} \neq \emptyset, \\ \deg(S/I) & \textit{si } \mathcal{F}_{\prec,d,r} = \emptyset. \end{cases}$$

Demostración. Sea $F = \{f_1, \ldots, f_r\}$ en $\mathcal{F}_{d,r}$. Por el algoritmo de división 1.6.4, cualquier f_i se puede escribir como $f_i = p_i + h_i$, donde p_i está en I_d y h_i es una combinación K-lineal de monomios estándar de grado d. Sea $H = \{h_1, \ldots, h_r\}$. Observamos que $(I : (F)) = (I : (H))$, $(I,F) = (I,H)$, $\overline{f_i} = \overline{h_i}$ para $i = 1, \ldots, r$. Por tanto, $H \in \mathcal{F}_{d,r}$, es decir, podemos asumir que $f_1, \ldots, f_r$ son polinomios estándar. También podemos asumir que $\text{lc}(f_i) = 1$ (coeficiente líder). Fijando $KF = Kf_1 + \cdots + Kf_r$, afirmamos que existe un conjunto $G = \{g_1, \ldots, g_r\}$ formado por polinomios homogéneos estándar de S/I de grado d tales que $KF = KG$, $\text{in}_\prec(g_1), \ldots, \text{in}_\prec(g_r)$ son monomios distintos, y $\text{in}_\prec(f_i) \succeq \text{in}_\prec(g_i)$ para todo i. Argumentamos por inducción sobre r. El caso $r = 1$ es obvio. Supongamos que $r > 1$. Permutando los polinomios f_i si es necesario, podemos suponer que $\text{in}_\prec(f_1) \succeq \cdots \succeq \text{in}_\prec(f_r)$. Si $\text{in}_\prec(f_1) \succ \text{in}_\prec(f_2)$, se obtiene el resultado aplicando la hipótesis de inducción a $f_2, \ldots, f_r$. Si $\text{in}_\prec(f_1) = \text{in}_\prec(f_2)$, existe un $k \geq 2$ tal que $\text{in}_\prec(f_1) = \text{in}_\prec(f_i)$ para todo $i \geq k$ y $\text{in}_\prec(f_1) \succ \text{in}_\prec(f_i)$ para $i > k$. Definimos $h_i = f_1 - f_i$ para $i = 2, \ldots, k$ y $h_i = f_i$ para $i = k+1, \ldots, r$. Observamos que $\text{in}_\prec(f_1) \succ h_i$ para $i \geq 2$ y que

$h_2, \ldots, h_r$ son polinomios estándar de grado d que son linealmente independientes sobre K. En consecuencia, se obtiene la afirmación aplicando la hipótesis de inducción a $H = \{h_2, \ldots, h_r\}$. La expresión pedida para $\delta_I(d, r)$ se deduce directamente del teorema 3.2.2. □

Observación 2.4.5. El resultado anterior generaliza la proposición 2.1.22 a esta nueva situación con la función distancia mínima generalizada.

Definición 2.4.6. Sea I un ideal homogéneo de S. La función $\mathrm{hyp}_I : \mathbb{N}_+ \times \mathbb{N}_+ \to \mathbb{N}$ dada por

$$\mathrm{hyp}_I(d, r) = \begin{cases} \text{máx}\{\deg(S/(I, F)) \mid F \in \mathcal{F}_{d,r}\} & \text{si } \mathcal{F}_{d,r} \neq \emptyset, \\ 0 & \text{si } \mathcal{F}_{d,r} = \emptyset, \end{cases}$$

se llama *función hyp* de I.

Observación 2.4.7. Para $r = 1$, se suele denotar $\mathrm{hyp}_I(d, 1) = \mathrm{hyp}_I(d)$. Encontrar cotas superiores para $\mathrm{hyp}_I(d, r)$ es equivalente a encontrar cotas inferiores para $\delta_I(d, r)$. Esta función la utilizaremos únicamente para simplificar la notación en algunas situaciones.

Al igual que con la función distancia mínima, es interesante obtener cotas inferiores para $\delta_I(d, r)$, ya que calcular su valor es un problema difícil. Es por ello por lo que también se introduce una generalización de la función huella. Para ello, primero definimos $\mathcal{M}_{\prec,d,r}$ como el conjunto de todos los subconjuntos M de $\Delta_\prec(I)_d = \Delta_\prec(I) \cap S_d$ con r elementos distintos tales que $(\mathrm{in}_\prec(I) : (M)) \neq \mathrm{in}_\prec(I)$.

Definición 2.4.8. La *función huella generalizada* de I es la función $\mathrm{fp}_I : \mathbb{N}_+ \times \mathbb{N}_+ \to \mathbb{Z}$ dada por

$$\mathrm{fp}_I(d, r) = \begin{cases} \deg(S/I) - \text{máx}\{\deg(S/(\mathrm{in}_\prec(I), M)) \mid M \in \mathcal{M}_{\prec,d,r}\} & \text{si } \mathcal{M}_{\prec,d,r} \neq \emptyset, \\ \deg(S/I) & \text{si } \mathcal{M}_{\prec,d,r} = \emptyset. \end{cases}$$

Observación 2.4.9. Para $r = 1$, obtenemos la función huella del ideal I: $\mathrm{fp}_I(d, 1) = \mathrm{fp}_I(d)$.

Sea I un ideal homogéneo, sea $\Delta^p_\prec(I)_d$ el conjunto de los polinomios estándar de S/I de grado d, y sea $\mathcal{F}^p_{\prec,d,r}$ el conjunto de todos los subconjuntos de $\Delta^p_\prec(I)_d$ con r elementos. Recordamos que $H_I(d)$ es precisamente el número de monomios estándar de grado d. Si $K = \mathbb{F}_q$ es un cuerpo finito, entonces

$$|\Delta^p_\prec(I)_d| = q^{H_I(d)} - 1 \text{ y } |\mathcal{F}^p_{\prec,d,r}| = \binom{q^{H_I(d)} - 1}{r}.$$

En consecuencia (recordar el teorema 2.4.4), calcular $\delta_I(d, r)$ es muy difícil porque hay que determinar cuáles de los polinomios de $\mathcal{F}^p_{\prec,d,r}$ están en $\mathcal{F}_{\prec,d,r}$, y después calcular los grados correspondientes. Calcular $\mathrm{fp}_I(d, r)$ es mucho más fácil porque solo

necesitamos determinar el conjunto $\Delta_\prec(I)_{d,r}$ de todos los subconjuntos de $\Delta_\prec(I)_d$ con r elementos, y se tiene que

$$|\Delta_\prec(I)_{d,r}| = \binom{H_I(d)}{r},$$

que es mucho menor que el tamaño de $\mathcal{F}^p_{\prec,d,r}$.

Es habitual presentar la información de la función huella y de la función distancia mínima generalizada en forma de matriz. La *matriz huella* $(\mathrm{fp}_I(d,r))$ y la *matriz de pesos* $(\delta_I(d,r))$ de I son las matrices cuyas entradas (d,r) son $\mathrm{fp}_I(d,r)$ y $\delta_I(d,r)$, respectivamente.

El siguiente resultado muestra que las entradas de cualquier fila (respectivamente columna) de la matriz de pesos de I forman una sucesión no decreciente (respectivamente no creciente). También vemos que la función huella generalizada es cota inferior de la función distancia mínima generalizada, y cuando son ambas mayores o iguales que 1.

Teorema 2.4.10 [6, Thm. 3.9]**.** *Sea $I \subset S$ un ideal homogéneo no mezclado, sea $\prec$ un orden monomial en S, y sean $d \geq 1$, $r \geq 1$ enteros. Se da lo siguiente.*

(a) $\mathrm{fp}_I(d,r) \leq \delta_I(d,r)$ *para* $1 \leq r \leq H_I(d)$.

(b) $\delta_I(d,r) \geq 1$.

(c) $\mathrm{fp}_I(d,r) \geq 1$ *si* $\mathrm{in}_\prec(I)$ *es no mezclado.*

(d) $\delta_I(d,r) \leq \delta_I(d,r+1)$.

(e) *Si existe un* $h \in S_1$ *regular en* S/I*, entonces* $\delta_I(d,r) \geq \delta_I(d+1,r) \geq 1$.

Demostración.

(a) Si $\mathcal{F}_{d,r} = \emptyset$, entonces $\delta_I(d,r) = \deg(S/I) \geq \mathrm{fp}_I(d,r)$. Supongamos ahora que $\mathcal{F}_{d,r} \neq \emptyset$. Sea F cualquier conjunto en $\mathcal{F}_{\prec,d,r}$. Por el lema 1.6.12, $\mathrm{in}_\prec(F)$ está en $\mathcal{M}_{\prec,d,r}$, y por el lema 2.1.4, $\deg(S/(I,F)) \leq \deg(S/(\mathrm{in}_\prec(I), \mathrm{in}_\prec(F)))$. En consecuencia, por la proposición 2.4.4 y el lema 2.1.4 (b), $\mathrm{fp}_I(d,r) \leq \delta_I(d,r)$.

(b) Si $\mathcal{F}_{d,r} = \emptyset$, entonces $\delta_I(d,r) = \deg(S/I) \geq 1$, y si $\mathcal{F}_{d,r} \neq \emptyset$, entonces usando el lema 2.1.4 (b) se deduce que $\delta_I(d,r) \geq 1$.

(c) Si $\mathcal{M}_{\prec,d,r} = \emptyset$, entonces $\mathrm{fp}_I(d,r) = \deg(S/I) \geq 1$. Supongamos ahora que $\mathcal{M}_{\prec,d,r}$ es no vacío y elijamos $M \in \mathcal{M}_{\prec,d,r}$ tal que

$$\mathrm{fp}_I(d,r) = \deg(S/I) - \deg(S/(\mathrm{in}_\prec(I), M)).$$

Como $\mathrm{in}_\prec(I)$ es no mezclado, por el lema 2.1.4 (b), $\mathrm{fp}_I(d,r) \geq 1$.

(d) Si $\mathcal{F}_{d,r+1}$ es vacío, entonces $\delta_I(d,r) \leq \deg(S/I) = \delta_I(d,r+1)$. Podemos suponer entonces que $\mathcal{F}_{d,r+1}$ es no vacío y elegimos $F = \{f_1, \ldots, f_{r+1}\}$ en $\mathcal{F}_{d,r+1}$ tal que $\mathrm{hyp}_I(d,r+1) = \deg(S/(I,F))$. Escribimos $F' = \{f_1, \ldots, f_r\}$ y observamos que $I \subsetneq (I : (F)) \subset (I : (F'))$, así que $F' \in \mathcal{F}_{d,r}$. Por el lema 2.1.4, se tiene que $\mathrm{ht}(I) = \mathrm{ht}(I,F) = \mathrm{ht}(I,F')$. Tomando funciones de Hilbert en la sucesión exacta corta

$$0 \longrightarrow (I,F)/(I,F') \longrightarrow S/(I,F') \longrightarrow S/(I,F) \longrightarrow 0$$

se deduce que $\deg(S/(I,F')) \geq \deg(S/(I,F))$. En consecuencia,

$$\mathrm{hyp}_I(d,r) \geq \deg(S/(I,F')) \geq \deg(S/(I,F)) = \mathrm{hyp}_I(d,r+1),$$

por lo que $\delta_I(d,r) \leq \delta_I(d,r+1)$.

(e) Por la parte (b), $\delta_I(d,r) \geq 1$ para $d \geq 1$. Supongamos que $\mathcal{F}_{d,r} = \emptyset$. Entonces $\delta_I(d,r) = \deg(S/I)$. Si el conjunto $\mathcal{F}_{d+1,r}$ es vacío, se tiene que

$$\delta_I(d,r) = \delta_I(d+1,r) = \deg(S/I).$$

Si el conjunto $\mathcal{F}_{d+1,r}$ es no vacío, entonces hay un $F \in \mathcal{F}_{d+1,r}$ tal que

$$\delta_I(d+1,r) = \deg(S/I) - \deg(S/(I,F)) \leq \deg(S/I) = \delta_I(d,r).$$

Así que podemos suponer ahora que $\mathcal{F}_{d,r} \neq \emptyset$. Elegimos $F = \{f_1, \ldots, f_r\}$ en $\mathcal{F}_{d,r}$ tal que

$$\delta_I(d,r) = \deg(S/I) - \deg(S/(I,F)).$$

Por hipótesis existe $h \in S_1$ tal que $(I : h) = I$. En consecuencia, el conjunto $h\overline{F} = \{h\overline{f}_i\}_{i=1}^r$ es linealmente independiente sobre K, $hF \subset S_{d+1}$, y

$$I \subsetneq (I : F) \subset (I : hF),$$

es decir, hF está en $\mathcal{F}_{d+1,r}$. Observamos que existe $\mathfrak{p} \in \mathrm{Ass}(S/I)$ que contiene a (I,F) (ver lema 2.1.4 (a)). Por tanto, los ideales (I,F) y (I,hF) tienen la misma altura, ya que un ideal primo $\mathfrak{p} \in \mathrm{Ass}(S/I)$ contiene a (I,F) si y solo si $\mathfrak{p}$ contiene a (I,hF). Tomando funciones de Hilbert en la sucesión exacta

$$0 \longrightarrow (I,F)/(I,hF) \longrightarrow S/(I,hF) \longrightarrow S/(I,F) \longrightarrow 0$$

se deduce que $\deg(S/(I,hF)) \geq \deg(S/(I,F))$. Como consecuencia obtenemos

$$\begin{aligned}\delta_I(d,r) &= \deg(S/I) - \deg(S/(I,F)) \geq \deg(S/I) - \deg(S/(I,hF)) \\ &\geq \deg(S/I) - \max\{\deg(S/(I,F')) \mid F' \in \mathcal{F}_{d+1,r}\} = \delta_I(d+1,r).\end{aligned}$$

□

Ejemplo 2.4.11. Sea $S = K[x_1, \ldots, x_6]$ el anillo de polinomios sobre el cuerpo finito $K = \mathbb{F}_3$ y sea I el ideal $(x_1x_6 - x_3x_4, x_2x_6 - x_3x_5)$. La regularidad y el grado de S/I son 2 y 4, respectivamente, y $H_I(1) = 6$, $H_I(2) = 19$. Vamos a utilizar el siguiente procedimiento en [12] para obtener la matriz huella y algunos valores de la función distancia mínima generalizada:

```
q=3,S=ZZ/3[x1,x2,x3,x4,x5,x6],I=ideal(x1*x6-x3*x4,x2*x6-x3*x5)
G=gb I
M=coker gens gb I, regularity M, degree M
init=ideal(leadTerm gens gb I)
apply(primaryDecomposition(I),dim)--Es no mezclado
er=(x)->if not quotient(init,x)==init then degree ideal(init,x) else 0
fpr=(d,r)->degree M - max apply(apply(apply(subsets(flatten entries
basis(d,M),r),toSequence),ideal),er)
genmd=(d,r)->degree M - max apply(apply(subsets(apply(apply(apply(
toList(set(0..q-1))^**(hilbertFunction(d,M))-(set{0})^**
(hilbertFunction(d,M)),toList),x->basis(d,M)*vector deepSplice x),
z->ideal(flatten entries z)),r),ideal),x->if #set flatten entries mingens
ideal(leadTerm gens x)==r and not quotient(I,x)==I then degree(I+x) else 0)
hilbertFunction(1,M),apply((1..6),x->fpr(1,x))
genmd(1,1)
L={x1,x2,x3,x4,x5,x6}
linearforms=(d,r)->degree M-max apply(apply(apply((subsets(apply(apply((
subsets(L,d)),product),x->x%G),r)),toList),ideal),x->if #set flatten
entries mingens ideal(leadTerm gens x)==r and not quotient(I,x)==I then
degree(I+x) else 0)
apply(2..5,x->linearforms(1,x))
--Nos da una cota superior para genm. Junto con la cota inferior de fpr,
nos da el valor de genmd(1,2..5)
```

Sobre el procedimiento, para calcular la función huella se procede de manera similar a como hemos explicado en 2.3.8, utilizando `subsets(lista,r)` para obtener los subconjuntos de tamaño r de una lista. En cuanto a la función distancia mínima generalizada, hay alguna complicación adicional. Como lista primera se consideran todos los elementos del producto cartesiano K^k (menos el elemento con todas las componentes nulas), donde k es la dimensión de $(S/I)_d$, dada por la función de Hilbert. Esto se puede conseguir en este caso con `toList(set(0..q-1))^**(hilbertFunction(d,M))-(set0)^**(hilbertFunction(d,M))`, ya que `^**` calcula precisamente este producto cartesiano. Al multiplicar escalarmente cada vector de este producto por el vector formado por los elementos de la base de $(S/I)_d$ obtenemos todas las posibles combinaciones lineales en K, luego obtenemos todo $(S/I)_d$. Esto lo hacemos con `x->basis(d,M)*vector deepSplice x`. Posteriormente, tomamos subconjuntos de tamaño r, y para cada uno de ellos se comprueba que sean linealmente independientes en S/I, por ejemplo comprobando que los iniciales sean monomios distintos con `#set flatten entries mingens ideal(leadTerm gens x)==r`, y se comprueba que sean no divisores de 0 con el cociente, devolviendo entonces el grado

del ideal suma, y 0 en caso de que no se de lo anterior. Calculando el máximo y restando del grado se obtiene la función distancia mínima generalizada. En la parte final repetimos el cálculo anterior utilizando únicamente monomios para dar una cota superior.

En cuanto a los resultados, para la matriz huella obtenemos

$$(\mathrm{fp}_I(d,r)) = \begin{pmatrix} 1 & 3 & 4 & 4 & 4 & 4 & \infty \\ 1 & 1 & 1 & 1 & 2 & 3 & 3 \end{pmatrix},\ d = 1,2 \text{ y } r = 1,\dots,7,$$

donde ∞ en este caso es $4 = \deg(S/I)$ ($-\infty$ es lo que se obtiene con el procedimiento al hacer el máximo de un conjunto vacío). Para $\delta_I(d,r)$, con el procedimiento calculamos directamente $\delta_I(1,1) = 3$, y para el resto de valores utilizamos la cota inferior de la función huella 2.4.10 (a) y la cota superior obtenida con el procedimiento considerando únicamente monomios, de manera que obtenemos $(\delta_I(1,1),\dots,\delta_I(1,5)) = (3,3,4,4,4)$.

Si para un cierto orden se tiene que $\mathrm{fp}_I(d,r) = \delta_I(d,r)$ para $d \geq 1$ y $r \geq 1$, a veces se dice que I es un *ideal fuertemente Geil-Carvalho* (para ese orden).

Proposición 2.4.12 [6, Prop. 3.13]**.** *Si I es un ideal monomial no mezclado y $\prec$ es cualquier orden monomial, entonces $\delta_I(d,r) = \mathrm{fp}_I(d,r)$ para $d \geq 1$ y $r \geq 1$, es decir, I es fuertemente Geil-Carvalho.*

Demostración. La desigualdad $\delta_I(d,r) \geq \mathrm{fp}_I(d,r)$ se deduce del teorema 2.4.10 (a). Para ver la otra desigualdad observamos que $\mathcal{M}_{\prec,d,r} \subset \mathcal{F}_{\prec,d,r}$ porque se tiene que $I = \mathrm{in}_\prec(I)$. También observamos que $\mathcal{M}_{\prec,d,r} = \emptyset$ si y solo si $\mathcal{F}_{\prec,d,r} = \emptyset$, como se deduce del lema 1.6.12. En consecuencia, se tiene que $\mathrm{fp}_I(d,r) \geq \delta_I(d,r)$. □

Vamos a introducir otra función numérica que va a coincidir con la función distancia mínima generalizada en algunas situaciones importantes.

Definición 2.4.13. La *función de Vasconcelos* de I es la función $\vartheta_I : \mathbb{N}_+ \times \mathbb{N}_+ \to \mathbb{N}$ dada por

$$\vartheta_I(d,r) = \begin{cases} \min\{\deg(S/(I:(F))) \mid F \in \mathcal{F}_{d,r}\} & \text{si } \mathcal{F}_{d,r} \neq \emptyset, \\ \deg(S/I) & \text{si } \mathcal{F}_{d,r} = \emptyset. \end{cases}$$

Teorema 2.4.14 [6, Thm. 3.5]**.** *Sea $I \subset S$ un ideal homogéneo no mezclado y radical. Entonces*

$$\vartheta_I(d,r) = \delta_I(d,r) \text{ para } d \geq 1 \text{ y } 1 \leq r \leq H_I(d).$$

Demostración. Si $\mathcal{F}_{d,r} = \emptyset$, entonces $\delta_I(d,r)$ y $\vartheta_I(d,r)$ son iguales a $\deg(S/I)$. Ahora supongamos que $\mathcal{F}_{d,r} \neq \emptyset$. Usando el lema 2.1.4 (c), obtenemos

$$\begin{aligned} \vartheta_I(d,r) &= \min\{\deg(S/(I:(F))) \mid F \in \mathcal{F}_{d,r}\} \\ &= \min\{\deg(S/I) - \deg(S/(I,F)) \mid F \in \mathcal{F}_{d,r}\} \\ &= \deg(S/I) - \max\{\deg(S/(I,F)) \mid F \in \mathcal{F}_{d,r}\} = \delta_I(d,r). \end{aligned}$$

□

Para $r = 1$ vimos (teorema 2.1.7) que no hacía falta la hipótesis de que I fuera radical. Pero para $r \geq 2$ es esencial, como vemos en el siguiente ejemplo 2.4.15.

Ejemplo 2.4.15. Sea I el ideal (x_1^2, x_1x_2, x_2^2) del anillo de polinomios $S = K[x_1, x_2]$ sobre un cuerpo K y sea $F = \{x_1, x_2\}$. I es primario y su único primo asociado es (x_1, x_2). Entonces $(I : (F)) = (I, F) = (x_1, x_2)$ y

$$3 = \deg(S/I) \neq \deg(S/(I : (F)) + \deg(S/(I, F)) = 2.$$

Proposición 2.4.16 [6, Prop. 3.14]**.** *Si $I \subset S$ es un ideal homogéneo no mezclado y $\dim(S/I) \geq 1$, entonces*

$$\delta_I(d, H_I(d)) = \deg(S/I) \text{ para } d \geq 1.$$

Demostración. Sea $r = H_I(d)$. Es suficiente con ver que $\mathcal{F}_{d,r} = \emptyset$. Razonamos por reducción al absurdo. Supongamos que $\mathcal{F}_{d,r}$ es no vacío y sea $F = \{f_1, \ldots, f_r\}$ un elemento de $\mathcal{F}_{d,r}$. Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ los primos asociados de I. Como $I \subsetneq (I : (F))$, podemos elegir $g \in S$ tal que $g(F) \subset I$ y $g \notin I$. Entonces (F) está contenido en $\cup_{i=1}^m \mathfrak{p}_i$, así que $(F) \subset \mathfrak{p}_i$ para algún i. Puesto que $r = H_I(d)$, se tiene que

$$S_d/I_d = K\overline{f}_1 \oplus \cdots \oplus K\overline{f}_r \Rightarrow S_d = Kf_1 + \cdots + Kf_r + I_d.$$

Luego $S_d \subset \mathfrak{p}_i$, es decir, $\mathfrak{m}^d \subset \mathfrak{p}_i$, donde $\mathfrak{m} = (x_1, \ldots, x_n)$. En consecuencia, $\mathfrak{p}_i = \mathfrak{m}$, una contradicción porque I es no mezclado y $\dim(S/I) \geq 1$. □

Ejemplo 2.4.17. Sea $S = K[x_1, x_2, x_3]$ un anillo de polinomios sobre un cuerpo K, y sean $(\mathrm{fp}_I(d, r))$ y $(\delta_I(d, r))$ la matriz huella y la matriz de pesos del ideal $I = (x_1^3, x_2x_3)$. La regularidad y el grado de S/I son 3 y 6. Adaptando el procedimiento del ejemplo 2.4.11 obtenemos:

$$(\mathrm{fp}_I(d, r)) = \begin{pmatrix} 3 & 5 & 6 & \infty & \infty & \infty \\ 2 & 3 & 4 & 5 & 6 & \infty \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}.$$

Si $r > H_I(d)$, entonces $\mathcal{M}_{\prec,d,r} = \emptyset$ y la entrada (d, r) de esta matriz es igual a 6 (escribimos ∞ porque es lo que sale del procedimiento al hacer el máximo del conjunto vacío). Por la proposición 2.4.12, $(\mathrm{fp}_I(d, r))$ es igual a $(\delta_I(d, r))$. Además, la función de Hilbert vale $3, 5, 6$ para $d = 1, 2, 3$, respectivamente. Así que comprobamos que se cumple la proposición 2.4.16.

Capítulo 3

Pesos de Hamming generalizados de los códigos tipo Reed-Muller

En este capítulo veremos que la función distancia mínima de un ideal homogéneo en el anillo de polinomios con coeficientes en un cuerpo generaliza la distancia mínima de los códigos de tipo Reed-Muller proyectivos sobre cuerpos finitos, en el sentido de que la función distancia mínima coincide con la distancia mínima del código cuando $I = I(\mathbb{X})$ es el ideal de anulación de un conjunto finito de puntos del espacio proyectivo. Esto lo haremos utilizando la distancia mínima generalizada, que no solo nos va a dar una formulación algebraica de la distancia mínima, si no que también nos va a permitir obtener los pesos de Hamming generalizados de los códigos tipo Reed-Muller. De esta manera, obtendremos los pesos de Hamming generalizados en términos de los invariantes algebraicos y la estructura del ideal de anulación correspondiente al código. Como referencias, vamos a utilizar principalmente [6], [14], [20] y [23].

3.1. Cálculo del número de ceros usando el grado

En esta sección vamos a estudiar una fórmula en términos del grado para calcular el número de ceros comunes de un conjunto de polinomios en un conjunto finito de puntos del espacio proyectivo sobre un cuerpo. Estos resultados se utilizarán para las secciones posteriores.

El siguiente lema motiva la utilización de la condición $(I : (F)) \neq I$ para discriminar casos en muchos de los resultados que hemos visto.

Lema 3.1.1 [14, Lem. 3.1]**.** *Sea $\mathbb{X}$ un subconjunto finito de $\mathbb{P}^{s-1}$ sobre un cuerpo K. Si $F = \{f_1, \ldots, f_r\}$ es un conjunto de polinomios homogéneos de $S \setminus \{0\}$, entonces $V_{\mathbb{X}}(F) = \emptyset$ si y solo si $(I(\mathbb{X}) : (F)) = I(\mathbb{X})$.*

Demostración.

⇒) Razonamos por reducción al absurdo, así que suponemos que $I(\mathbb{X}) \subsetneq (I(\mathbb{X}) : (F))$. Elegimos un polinomio homogéneo g tal que $gf_i \in I(\mathbb{X})$ para

todo i y $g \notin I(\mathbb{X})$. Entonces, existe un $[\alpha] \in \mathbb{X}$ tal que $g(\alpha) \neq 0$. Por tanto, $f_i(\alpha) = 0$ para todo i, es decir, $[\alpha] \in V_{\mathbb{X}}(F)$, una contradicción.

$\Leftarrow$) Podemos escribir $\mathbb{X} = \{[P_1], \ldots, [P_m]\}$ y $I(\mathbb{X}) = \cap_{i=1}^{m} \mathfrak{p}_i$, donde $\mathfrak{p}_i$ es igual a $I_{[P_i]}$, el ideal de anulación de $[P_i]$. De nuevo razonamos por reducción al absurdo y suponemos que $V_{\mathbb{X}}(F) \neq \emptyset$. Elegimos $[P_i] \in V_{\mathbb{X}}(F)$. Por simplicidad de notación vamos a suponer que $i = 1$. Observamos que $(\mathfrak{p}_1 : (F)) = (1)$. En consecuencia,

$$\bigcap_{i=1}^{m} \mathfrak{p}_i = I(\mathbb{X}) = (I(\mathbb{X}) : (F)) = \bigcap_{i=1}^{m} (\mathfrak{p}_i : (F)) = \bigcap_{i=2}^{m} (\mathfrak{p}_i : (F)) \subset \mathfrak{p}_1.$$

Por tanto, $\mathfrak{p}_i \subset (\mathfrak{p}_i : (F)) \subset \mathfrak{p}_1$ para algún $i \geq 2$. Se deduce que $\mathfrak{p}_i = \mathfrak{p}_1$, una contradicción.

□

Lema 3.1.2 [14, Lem. 3.2]**.** *Sea $\mathbb{X}$ un subconjunto finito de $\mathbb{P}^{s-1}$ sobre un cuerpo K, y sea $I(\mathbb{X}) \subset S$ su ideal de anulación. Si $F = \{f_1, \ldots, f_r\}$ es un conjunto de polinomios homogéneos de $S \setminus \{0\}$, entonces*

$$|\mathbb{X} \setminus V_{\mathbb{X}}(F)| = \begin{cases} \deg(S/(I(\mathbb{X}) : (F))) & \text{si } (I(\mathbb{X}) : (F)) \neq I(\mathbb{X}), \\ \deg(S/I(\mathbb{X})) & \text{si } (I(\mathbb{X}) : (F)) = I(\mathbb{X}). \end{cases}$$

Demostración. Sean $[P_1], \ldots, [P_m]$ los puntos de $\mathbb{X}$ con $m = |\mathbb{X}|$. Entonces sabemos que $I(\mathbb{X}) = \bigcap_{i=1}^{m} I_{[P_i]}$ es una descomposición primaria de $I(\mathbb{X})$ (ver observación 1.7.6).

Supongamos que $(I(\mathbb{X}) : (F)) \neq I(\mathbb{X})$. Denotamos $I = I(\mathbb{X})$ y $\mathfrak{p}_i = I_{[P_i]}$ para $i = 1, \ldots, m$. Observamos que $(\mathfrak{p}_j : f_i) = (1)$ si y solo si $f_i \in \mathfrak{p}_j$ si y solo si $f_i(P_j) = 0$. Entonces,

$$(I : (F)) = \bigcap_{i=1}^{r} (I : f_i) = \left(\bigcap_{f_1(P_j) \neq 0} \mathfrak{p}_j \right) \bigcap \cdots \bigcap \left(\bigcap_{f_r(P_j) \neq 0} \mathfrak{p}_j \right) = \bigcap_{[P_j] \notin V_{\mathbb{X}}(F)} \mathfrak{p}_j.$$

En consecuencia, por la aditividad del grado 1.5.23, tenemos que $\deg(S/(I : (F)))$ es igual a $|\mathbb{X} \setminus V_{\mathbb{X}}(F)|$ (recordamos que $\deg(S/I_{[P_i]}) = 1$, ver corolario 1.7.5). Si $(I(\mathbb{X}) : (F)) = I(\mathbb{X})$, entonces $V_{\mathbb{X}}(F) = \emptyset$ por el lema 3.1.1. Por tanto, $|V_{\mathbb{X}}(F)| = 0$ y se obtiene el resultado ya que $|\mathbb{X}| = \deg(S/I(\mathbb{X}))$. □

Lema 3.1.3 [14, Lem. 3.4]**.** *Sea $\mathbb{X}$ un conjunto finito de $\mathbb{P}^{s-1}$ sobre un cuerpo K, y sea $I(\mathbb{X}) \subset S$ su ideal de anulación. Si $F = \{f_1, \ldots, f_r\}$ es un conjunto de polinomios homogéneos de $S \setminus \{0\}$, entonces el número de puntos de $V_{\mathbb{X}}(F)$ está dado por*

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

Demostración. Sean $[P_1], \ldots, [P_m]$ los puntos de $\mathbb{X}$ con $m = |\mathbb{X}|$. Supongamos que $(I(\mathbb{X}) : (F)) \neq I(\mathbb{X})$. Sea $\mathcal{A}$ el conjunto de los $I_{[P_i]}$ que contienen a F. Observamos que $f_j \in I_{[P_i]}$ si y solo si $f_j(P_i) = 0$. Entonces, $[P_i]$ está en $V_{\mathbb{X}}(F)$ si y solo si $F \subset I_{[P_i]}$. Por tanto, $[P_i]$ está en $V_{\mathbb{X}}(F)$ si y solo si $I_{[P_i]}$ está en $\mathcal{A}$. En consecuencia, por el lema 1.5.24 tenemos

$$|V_{\mathbb{X}}(F)| = \sum_{[P_i] \in V_{\mathbb{X}}(F)} \deg(S/I_{[P_i]}) = \sum_{F \subset I_{[P_i]}} \deg(S/I_{[P_i]}) = \deg(S/(I(\mathbb{X}), F)).$$

Si suponemos $(I(\mathbb{X}) : F) = I(\mathbb{X})$, entonces por el lema 3.1.1 tenemos que $V_{\mathbb{X}}(f) = \emptyset$ y $|V_{\mathbb{X}}(f)| = 0$. □

Proposición 3.1.4 [14, Prop. 3.5]**.** *Si $\mathbb{X}$ es un subconjunto finito de $\mathbb{P}^{s-1}$, entonces*

$$\deg(S/I(\mathbb{X})) = \deg(S/(I(\mathbb{X}) : (F))) + \deg(S/(I(\mathbb{X}), F)).$$

Demostración. Se deduce de los lemas 3.1.2 y 3.1.3. □

El resultado anterior también es una consecuencia directa del lema 2.1.4 (c), que es más general.

Corolario 3.1.5 [14, Cor. 4.2]**.** *Sea $\mathbb{X}$ un subconjunto finito de $\mathbb{P}^{s-1}$, sea $I(\mathbb{X}) \subset S$ su ideal de anulación, y sea $\prec$ un orden monomial. Si F es un conjunto finito de polinomios homogéneos de S y $(I(\mathbb{X}) : (F)) \neq I(\mathbb{X})$, entonces*

$$|V_{\mathbb{X}}(F)| = \deg(S/(I(\mathbb{X}), F)) \leq \deg(S/(\mathrm{in}_{\prec}(I(\mathbb{X})), \mathrm{in}_{\prec}(F))) \leq \deg(S/I(\mathbb{X})),$$

y $\deg(S/(I(\mathbb{X}), F)) < \deg(S/I(\mathbb{X}))$ si $(F) \not\subset I(\mathbb{X})$.

Demostración. Se deduce de los lemas 3.1.3 y 2.1.4. □

3.2. Pesos de Hamming generalizados de los códigos tipo Reed-Muller

La función distancia mínima de un ideal homogéneo tiene interés por sí misma y por eso la hemos estudiado desde un punto de vista más general, y en el caso de códigos, junto con la función huella que hemos introducido, nos permitiría tratar la distancia mínima con métodos algebraicos (ver [20]). Esto se puede generalizar, utilizando la distancia mínima generalizada, para obtener los pesos de Hamming generalizados del código, que es lo que haremos en esta sección. Como referencias, vamos a utilizar principalmente [6] y [14].

Lema 3.2.1 [14, Cor. 4.2]**.** *Sea $\mathbb{X} = \{[P_1], \ldots, [P_m]\}$ un subconjunto finito de $\mathbb{P}^{s-1}$, y sea D un subespacio vectorial de $C_{\mathbb{X}}(d)$ de dimensión $r \geq 1$. Se da lo siguiente.*

(a) *Existen* $\overline{f_1}, \ldots, \overline{f_r}$ *elementos de* S_d/I_d *linealmente independientes tales que* $D = \oplus_{i=1}^{r} K\beta_i$*, donde* β_i *es* $(f_i(P_1), \ldots, f_i(P_m))$*, y el soporte* $\chi(D)$ *de* D *es igual a* $\cup_{i=1}^{r}\chi(\beta_i)$*.*

(b) $|\chi(D)| = |\mathbb{X} \setminus V_{\mathbb{X}}(f_1, \ldots, f_r)|$.

(c) $\delta_r(C_{\mathbb{X}}(d)) = \min\{|\mathbb{X} \setminus V_{\mathbb{X}}(F)| : F = \{f_i\}_{i=1}^{r} \subset S_d, \{\overline{f_i}\}_{i=1}^{r}$ *linealmente independientes sobre* $K\}$ *(*$\delta_r(C)$ *es el peso de Hamming generalizado* r*-ésimo de* C*).*

Demostración.

(a) Se deduce del lema 1.8.16 y utilizando el hecho de que la aplicación de evaluación ev_d induce un isomorfismo entre S_d/I_d y $C_{\mathbb{X}}(d)$.

(b) Consideramos la matriz A con filas $\beta_1, \ldots, \beta_r$. Observamos que la i-ésima columna de A es no nula si y solo si $[P_i]$ está en $\mathbb{X} \setminus V_{\mathbb{X}}(f_1, \ldots, f_r)$. Es suficiente observar que el número de columnas no nulas de A es $|\chi(D)|$ (ver lema 1.8.16).

(c) Se deduce de la parte (b), utilizando la definición de peso de Hamming generalizado r-ésimo de $C_{\mathbb{X}}(d)$.

□

Ahora presentamos uno de los resultados principales de esta sección.

Teorema 3.2.2 [14, Thm. 4.5]**.** *Sea* K *un cuerpo, y sea* $\mathbb{X}$ *un subconjunto finito de* $\mathbb{P}^{s-1}$*. Si* $|\mathbb{X}| \geq 2$ *y* $\delta_{\mathbb{X}}(d, r)$ *es el peso de Hamming generalizado* r*-ésimo de* $C_{\mathbb{X}}(d)$*, entonces*

$$\delta_{\mathbb{X}}(d, r) = \delta_{I(\mathbb{X})}(d, r) = \vartheta_{I(\mathbb{X})}(d, r) \text{ para } d \geq 1 \text{ y } 1 \leq r \leq H_{I(\mathbb{X})}(d),$$

y $\delta_{\mathbb{X}}(d, r) = r$ *para* $d \geq \mathrm{reg}(S/I(\mathbb{X}))$*.*

Demostración. La igualdad $\delta_{I(\mathbb{X})}(d, r) = \vartheta_{I(\mathbb{X})}(d, r)$ se deduce de 2.4.14. Para la otra, si $\mathcal{F}_{d,r} = \emptyset$, entonces utilizando los lemas 3.1.2, 3.1.3, y 3.2.1 obtenemos que $\delta_{\mathbb{X}}(d, r)$ y $\delta_{I(\mathbb{X})}(d, r)$ son iguales a $\deg(S/I(\mathbb{X})) = |\mathbb{X}|$. Supongamos que $\mathcal{F}_{d,r} \neq \emptyset$ y sea $I = I(\mathbb{X})$. Utilizando el lema 3.2.1 y la fórmula para $V_{\mathbb{X}}(F)$ del lema 3.1.3, obtenemos

$$\begin{aligned}
\delta_{\mathbb{X}}(d, r) &\overset{(3.2.1)}{=} \min\{|\mathbb{X} \setminus V_{\mathbb{X}}(F)| : F \in \mathcal{F}_{d,r}\} \\
&\overset{(3.1.3)}{=} |\mathbb{X}| - \max\{\deg(S/(I, F)) \mid F \in \mathcal{F}_{d,r}\} \\
&= \deg(S/I) - \max\{\deg(S/(I, F)) \mid F \in \mathcal{F}_{d,r}\} = \delta_I(d, r).
\end{aligned}$$

Como $H_I(d) = HP_I(d) = \deg(S/I) = |\mathbb{X}|$ para $d \geq \mathrm{reg}(S/I)$, utilizando la cota de Singleton generalizada 1.8.14 para los pesos de Hamming generalizados y que la sucesión de la jerarquía de pesos es estrictamente monótona (ver 1.8.13), obtenemos que $\delta_{\mathbb{X}}(d, r) = r$ para $d \geq \mathrm{reg}(S/I)$. □

Observación 3.2.3. Sea $\mathbb{X}$ un conjunto finito de puntos proyectivos sobre un cuerpo K. Se da lo siguiente.

(a) $r \leq \delta_{\mathbb{X}}(d,r) \leq |\mathbb{X}|$ para $d \geq 1$ y $1 \leq r \leq H_{I(\mathbb{X})}(d)$. Esto se deduce del hecho de que la jerarquía de pesos es una sucesión creciente (ver 1.8.13).

(b) Si $d \geq \operatorname{reg}(S/I(\mathbb{X}))$, entonces $C_{\mathbb{X}}(d) = K^{|\mathbb{X}|}$ y $\delta_{\mathbb{X}}(d,r) = r$ para $1 \leq r \leq |\mathbb{X}|$.

(c) Por la proposición 2.4.16 y el teorema 3.2.2, $\delta_{\mathbb{X}}(d, H_{\mathbb{X}}(d)) = |\mathbb{X}|$.

(d) Si $r > H_{I(\mathbb{X})}(d)$, entonces $\mathcal{F}_{d,r} = \emptyset$ y $\delta_{I(\mathbb{X})}(d,r) = |\mathbb{X}|$.

A continuación presentamos otro de los resultados principales de la sección.

Teorema 3.2.4 [14, Thm. 4.9]**.** *Sea K un cuerpo, sea $\mathbb{X}$ un subconjunto finito de $\mathbb{P}^{s-1}$, y sea $\prec$ un orden monomial. Si $|\mathbb{X}| \geq 2$ y $\delta_{\mathbb{X}}(d,r)$ es el peso de Hamming generalizado r-ésimo de $C_{\mathbb{X}}(d)$, entonces*

$$\operatorname{fp}_{I(\mathbb{X})}(d,r) \leq \delta_{\mathbb{X}}(d,r) \text{ para } d \geq 1 \text{ y } 1 \leq r \leq H_{I(\mathbb{X})}(d).$$

Demostración. Se deduce del lema 1.6.12, del lema 2.1.4, del teorema 3.2.2, y de la proposición 2.4.4. También es consecuencia directa de 2.4.10 y 3.2.2. □

En el siguiente resultado vemos que las columnas de la matriz de pesos $(\delta_{\mathbb{X}}(d,r))$ forman una sucesión decreciente.

Teorema 3.2.5 [6, Thm. 5.3]**.** *Sea $\mathbb{X}$ un conjunto finito de puntos en $\mathbb{P}^{s-1}$, sea $I = I(\mathbb{X})$ su ideal de anulación, y sea $1 \leq r \leq |\mathbb{X}|$ un entero fijo. Entonces hay un entero $d_0 \geq 1$ tal que*

$$\delta_I(1,2) > \delta_I(2,r) > \cdots > \delta_I(d_0,r) = \delta_I(d,r) = r \text{ para } d \geq d_0.$$

Demostración. Sean $[P_1], \ldots, [P_m]$ los puntos de $\mathbb{X}$. Por el teorema 3.2.2 existe un subcódigo lineal D de $C_{\mathbb{X}}(d)$ de dimensión r tal que $\delta_I(d,r) = \delta_{\mathbb{X}}(d,r) = |\chi(D)|$. Elegimos una base $\beta_1, \ldots, \beta_r$ de D como K-espacio vectorial. Cada β_i se puede escribir (suponiendo que la primera coordenada no nula de cada P_i es 1) como

$$\beta_i = (\beta_{i,1}, \ldots, \beta_{i,k}, \ldots, \beta_{i,m}) = (f_i(P_1), \ldots, f_i(P_k), \ldots, f_i(P_m))$$

para algún $f_i \in S_d$. Consideramos la matriz B cuyas filas son $\beta_1, \ldots, \beta_m$:

$$B = \begin{pmatrix} f_1(P_1) & \cdots & f_1(P_k) & \cdots & f_1(P_m) \\ f_2(P_1) & \cdots & f_2(P_k) & \cdots & f_2(P_m) \\ \vdots & \cdots & \vdots & \cdots & \vdots \\ f_r(P_1) & \cdots & f_r(P_k) & \cdots & f_r(P_m) \end{pmatrix}$$

Como B tiene rango r, permutando columnas y aplicando operaciones elementales por filas, la matriz B se puede llevar a la forma:

$$B' = \begin{pmatrix} g_1(Q_1) & & & & g_1(Q_{r+1}) & \cdots & g_1(Q_m) \\ & g_2(Q_2) & & \mathbf{0} & g_2(Q_{r+1}) & \cdots & g_2(Q_m) \\ \mathbf{0} & & \ddots & & \vdots & & \\ & & & g_r(Q_r) & g_r(Q_{r+1}) & \cdots & g_r(Q_m) \end{pmatrix},$$

donde $g_1, \ldots, g_r$ son polinomios linealmente independientes sobre el cuerpo K módulo I de grado d, $Q_1, \ldots, Q_m$ son una permutación de $P_1, \ldots, P_m$, las primeras r columnas de B' forman una matriz diagonal tal que $g_i(Q_i) \neq 0$ para $i = 1, \ldots, r$, y los ideales $(f_1, \ldots, f_r)$ y $(g_1, \ldots, g_r)$ son iguales. Sea D' el subespacio lineal generado por las filas de B'. Las operaciones aplicadas a B no han modificado el tamaño del soporte de D (lema 1.8.16), es decir, $|\chi(D)| = |\chi(D')|$.

Observamos que $\delta_r(C_{\mathbb{X}}(d))$ depende únicamente de $\mathbb{X}$, es decir, $\delta_r(C_{\mathbb{X}}(d))$ es independiente de como ordenemos los puntos en $\mathbb{X}$ (se puede ver por el teorema 3.2.2). Sea $\mathrm{ev}'_d : S_d \to K^m$ la aplicación de evaluación, $f \mapsto (f(Q_1), \ldots, f(Q_m))$, relativa a los puntos $[Q_1], \ldots, [Q_m]$. Por el teorema 1.8.13, $\delta_{\mathbb{X}}(d, r) \geq r$.

Primero suponemos que $\delta_{\mathbb{X}}(d, r) = r$ para algún $d \geq 1$ y $r \geq 1$. Entonces la columna i-ésima de B' es nula para $i > r$. Para cada $1 \leq i \leq r$ elegimos $h_i \in S_1$ tal que $h_i(Q_i) \neq 0$. Los polinomios $h_1 g_1, \ldots, h_r g_r$ son linealmente independientes módulo I porque $(h_i g_i)(Q_j)$ no es 0 si $i = j$ y es 0 si $i \neq j$. La imagen de $Kh_1g_1 \oplus \cdots \oplus Kh_rg_r$, bajo la aplicación ev'_{d+1}, es un subcódigo D'' de $C_{\mathbb{X}}(d+1)$ de dimensión r y $|\chi(D'')| = r$. Por tanto, $\delta_{\mathbb{X}}(d+1, r) \leq r$, y entonces $\delta_{\mathbb{X}}(d+1, r) = r$.

A continuación suponemos que $\delta_{\mathbb{X}}(d, r) > r$. Entonces B' tiene una columna no nula $(g_1(Q_k), \ldots, g_r(Q_k))^t$ para algún $k > r$. Es suficiente probar que $\delta_{\mathbb{X}}(d, r) > \delta_{\mathbb{X}}(d+1, r)$. Por 1.8.7 (b), para cada $1 \leq i \leq r$ hay un $h_i \in S_1$ tal que $h_i(Q_i) \neq 0$ y $h_i(Q_k) = 0$. Sea B'' la matriz:

$$B'' = \begin{pmatrix} h_1g_1(Q_1) & & & & h_1g_1(Q_{r+1}) & \cdots & h_1g_1(Q_m) \\ & h_2g_2(Q_2) & & \mathbf{0} & h_2g_2(Q_{r+1}) & \cdots & h_2g_2(Q_m) \\ \mathbf{0} & & \ddots & & \vdots & & \\ & & & h_rg_r(Q_r) & h_rg_r(Q_{r+1}) & \cdots & h_rg_r(Q_m) \end{pmatrix}.$$

La imagen de $Kh_1g_1 \oplus \cdots \oplus Kh_rg_r$, bajo la aplicación ev'_{d+1}, es un subcódigo V de $C_{\mathbb{X}}(d+1)$ de dimensión r porque el rango de B'' es r, y puesto que la columna k-ésima de B'' es nula, obtenemos

$$\delta_{\mathbb{X}}(d, r) = |\chi(D)| = |\chi(D')| > |\chi(V)| \geq \delta_{\mathbb{X}}(d+1, r).$$

En consecuencia, $\delta_{\mathbb{X}}(d, r) > \delta_{\mathbb{X}}(d+1, r)$. □

Con el teorema 3.2.5 podemos recuperar el siguiente resultado de [13].

Corolario 3.2.6 ([6, Cor. 5.5], [13, Thm. 12]). *Si* $\mathbb{X}$ *es un conjunto parametrizado por monomios en un toro proyectivo y* $1 \leq r \leq |\mathbb{X}|$ *es un entero fijo, entonces existe un entero* $d_0 \geq 1$ *tal que*

$$\delta_r(C_{\mathbb{X}}(1)) > \delta_r(C_{\mathbb{X}}(2)) > \cdots > \delta_r(C_{\mathbb{X}}(d_0)) = \delta_r(C_{\mathbb{X}}(d)) = r \text{ para } d \geq d_0.$$

Demostración. Se deduce directamente de los teoremas 3.2.2 y 3.2.5. □

3.3. Distancia mínima de códigos cartesianos

En esta sección vamos a ver algunas aplicaciones de los resultados que hemos visto hasta ahora para el caso particular de códigos cartesianos. Como referencias, vamos a utilizar principalmente [14], [20] y [23].

3.3.1. Distancia mínima de códigos cartesianos proyectivos

En esta sección vamos a presentar una conjetura interesante sobre la distancia mínima de los códigos cartesianos proyectivos, viendo casos en los que se cumple. También vamos a dar algún contraejemplo, ya que se ha demostrado que no es cierta en general. Como referencias, vamos a utilizar [5], [14], [20] y [23].

Vamos a utilizar las notaciones que hemos introducido en la sección 1.8.1. Comenzamos presentando la conjetura que hemos mencionado.

Conjetura 3.3.1 ([5], [20, Conj. 6.2]). Sea $C_{\mathcal{X}}(d)$ el d-ésimo código cartesiano proyectivo anidado en el conjunto $\mathcal{X} = [A_1 \times \cdots \times A_n]$ con $d_i = |A_i|$ para $i = 1, \ldots, n$. Entonces su distancia mínima viene dada por

$$\delta_{\mathcal{X}}(d) = \begin{cases} (d_{k+2} - l + 1)d_{k+3} \cdots d_n & \text{si } d \leq \sum_{i=2}^{n}(d_i - 1), \\ 1 & \text{si } d \geq \sum_{i=2}^{n}(d_i - 1) + 1, \end{cases}$$

donde $0 \leq k \leq s-2$ y l son los únicos enteros tales que $d = \sum_{i=2}^{k+1}(d_i - 1) + l$ y $1 \leq l \leq d_{k+2} - 1$.

En lo que sigue vamos a seguir denotando $\mathcal{X} = [A_1 \times \cdots \times A_n]$ un conjunto proyectivo cartesiano anidado y $C_{\mathcal{X}}(d)$ su correspondiente d-ésimo código tipo Reed-Muller proyectivo. A lo largo de esta sección $\prec$ es el orden lexicográfico en S con $x_1 \prec \cdots \prec x_n$.

Proposición 3.3.2 ([5], [20, Prop. 6.3]). *El ideal inicial* $\text{in}_{\prec}(I(\mathcal{X}))$ *está generado por el conjunto de todos los monomios* $x_i x_j^{d_j}$ *con* $1 \leq i < j \leq s$,

$$\deg(S/I(\mathcal{X})) = 1 + \sum_{i=2}^{n} d_i \cdots d_n, \text{ y } \operatorname{reg}(S/I(\mathcal{X})) = 1 + \sum_{i=2}^{n}(d_i - 1).$$

Carvalho, Lopez-Neumann, y López [5] demostraron que la conjetura se puede reducir a la siguiente.

Conjetura 3.3.3 ([5], [20, Conj. 6.4])**.** Si $0 \neq f \in S_d$ es un polinomio estándar con respecto a $\prec$, tal que $(I(\mathcal{X}) : f) \neq I(\mathcal{X})$ y $1 \leq d \leq \sum_{i=2}^{n}(d_i - 1)$, entonces

$$|V_{\mathcal{X}}(f)| \leq \deg(S/I(\mathcal{X})) - (d_{k+2} - l + 1)d_{k+3} \cdots d_n,$$

donde $0 \leq k \leq n-2$ y l son enteros tales que $d = \sum_{i=2}^{k+1}(d_i - 1) + l$ y $1 \leq l \leq d_{k+2} - 1$.

Esta conjetura no es cierta en general, como vemos en el ejemplo 3.3.8. Sin embargo, hay resultados similares al de la conjetura que son ciertos, como veremos en el teorema 3.3.6.

A continuación vamos a ver una fórmula para el grado y la vamos a utilizar para dar una cota superior para $|V_{\mathcal{X}}(f)|$.

Proposición 3.3.4 [20, Prop. 5.3]**.** *Sea $d_1, \ldots, d_n$ una sucesión no decreciente de enteros positivos con $d_1 \geq 2$ y $n \geq 2$, y sea L el ideal de $S = K[x_1, \ldots, x_n]$ generado por el conjunto de todos los $x_i x_j^{d_j}$ tales que $1 \leq i < j \leq n$. Sea $x^a = x_r^{a_r} \cdots x_n^{a_n}$ un monomio estándar de S/L con respecto al orden monomial $\prec$. Si $a_r \geq 1$, $a_i = 0$ para $i < r$, y $1 \leq r \leq n$, entonces $0 \leq a_i \leq d_i - 1$ para $i > r$ y*

$$\deg S/(L, x^a) = \begin{cases} \deg S/L - \sum_{i=2}^{n}(d_i - a_i) \cdots (d_n - a_n) - 1 & \text{si } r = n, a_n \leq d_n, \\ \deg S/L - 1 & \text{si } r = n, a_n \geq d_n + 1, \\ \deg S/L - \sum_{i=2}^{r+1}(d_i - a_i) \cdots (d_n - a_n) & \text{si } r < n, a_r \leq d_r, \\ \deg S/L - (d_{r+1} - a_{r+1}) \cdots (d_n - a_n) & \text{si } r < n, a_r \geq d_r + 1. \end{cases}$$

Teorema 3.3.5 [20, Thm. 6.5]**.** *Sea $\prec$ el orden lexicográfico en S con $x_1 \prec \cdots \prec x_n$ y sea $f \neq 0$ un polinomio estándar con $\mathrm{in}_{\prec}(f) = x_r^{a_r} \cdots x_n^{a_n}$ y $a_r \geq 1$. Entonces $0 \leq a_i \leq d_i - 1$ para $i > r$ y*

$$\begin{aligned} |V_{\mathcal{X}}(f)| &\leq \deg(S/(\mathrm{in}_{\prec}(I(\mathcal{X})), \mathrm{in}_{\prec}(f))) \\ &= \begin{cases} \deg(S/I(\mathcal{X})) - \sum_{i=2}^{r+1}(d_i - a_i) \cdots (d_n - a_n) & \text{si } a_r \leq d_r, \\ \deg(S/I(\mathcal{X})) - (d_{r+1} - a_{r+1}) \cdots (d_n - a_n) & \text{si } a_r \geq d_r + 1, \end{cases} \end{aligned}$$

donde $(d_i - a_i) \cdots (d_n - a_n) = 1$ si $i > s$ y $a_i = 0$ para $i < r$.

Demostración. Por la proposición 3.3.2 el ideal inicial de $I(\mathcal{X})$ está generado por el conjunto de todos los $x_i x_j^{d_j}$ tales que $1 \leq i < j \leq n$ y el grado de $S/(\mathrm{in}_{\prec}(I(\mathcal{X}))$ es igual al grado de $S/I(\mathcal{X})$. Como $\mathrm{in}_{\prec}(f)$ es un monomio estándar, se deduce que $0 \leq a_i \leq d_i - 1$ para $i > r$. Observamos que si f no es un divisor de cero de $S/I(\mathcal{X})$, entonces $V_{\mathcal{X}}(f) = \emptyset$. En consecuencia, la desigualdad se obtiene del corolario 3.1.5 y la igualdad se deduce de la proposición 3.3.4. □

Teorema 3.3.6 [20, Thm. 6.6]**.** *Sea $\prec$ el orden lexicográfico en S con $x_1 \prec \cdots \prec x_n$. Si $0 \neq f \in S_d$ es un polinomio estándar tal que $1 \leq d \leq \sum_{i=2}^{n}(d_i - 1)$ y x_1 divide a $\mathrm{in}_\prec(f)$, entonces*

$$|V_{\mathcal{X}}(f)| \leq \deg(S/I(\mathcal{X})) - (d_{k+2} - l + 1)d_{k+3} \cdots d_n,$$

donde $0 \leq k \leq n-2$ y l son enteros tales que $d = \sum_{i=2}^{k+1}(d_i - 1) + l$ y $1 \leq l \leq d_{k+2} - 1$.

Demostración. Por el lema 3.1.3 podemos suponer que $(I(\mathcal{X}) : f) \neq I(\mathcal{X})$. Sea $x^a = \mathrm{in}_\prec(f)$ el monomio líder de f. Por la proposición 3.3.2, podemos escribir

$$x^a = x_1^{a_1} \cdots x_n^{a_n},$$

con $a_1 \geq 1$, $0 \leq a_i \leq d_i - 1$ para $i > 1$. Por los lemas 3.1.3 y 3.1.5 es suficiente ver que se da la siguiente desigualdad

$$\deg(S/(\mathrm{in}_\prec(I(\mathcal{X})), x^a)) \leq \deg(S/I(\mathcal{X})) - (d_{k+2} - l + 1)d_{k+3} \cdots d_n. \tag{3.3.1}$$

Si sustituimos $l = \sum_{i=1}^{n} a_i - \sum_{i=2}^{k+1}(d_i - 1)$ en la ecuación (3.3.1), y usamos la fórmula para el grado de $S/(\mathrm{in}_\prec(I(\mathcal{X})), x^a)$ dada en el teorema 3.3.5, solo tenemos que ver que se dan las siguientes desigualdades para $r = 1$:

$$\begin{aligned}\sum_{i=2}^{r+1}(d_i - a_i) \cdots (d_n - a_n) \geq \\ \left(\sum_{i=2}^{k+2}(d_i - a_i) - (k-1) - a_1 - \sum_{i=k+3}^{n} a_i\right) d_{k+3} \cdots d_n \text{ si } a_r \leq d_r,\end{aligned} \tag{3.3.2}$$

$$\begin{aligned}\prod_{i=r+1}^{n}(d_i - a_i) \geq \\ \left(\sum_{i=2}^{k+2}(d_i - a_i) - (k-1) - a_1 - \sum_{i=k+3}^{n} a_i\right) d_{k+3} \cdots d_n \text{ si } a_r \geq d_r + 1,\end{aligned} \tag{3.3.3}$$

para $0 \leq k \leq n-2$, donde $(d_i - a_i) \cdots (d_n - a_n) = 1$ si $i > n$ y $a_i = 0$ para $i < r$.

Si suponemos $r = 1$, las ecuaciones (3.3.2) y (3.3.3) son la misma. En consecuencia, solo debemos probar la desigualdad

$$\prod_{i=2}^{n}(d_i - a_i) \geq \left(\sum_{i=2}^{k+2}(d_i - a_i) - (k-1) - a_1 - \sum_{i=k+3}^{n} a_i\right) d_{k+3} \cdots d_n,$$

para $0 \leq k \leq n-2$. Esta desigualdad se obtiene tomando $m = n-1$, $e_i = d_{i+1}$, $b_i = a_{i+1}$ para $i = 1, \ldots, m$, y $b_0 = a_1$ en la proposición 2.3.1. □

Sea $\mathcal{L}_d$ el K-espacio vectorial generado por todos los $x^a \in S_d$ tales que x_1 divide a x^a y sea C_d la imagen de $\mathcal{L}_d$ bajo la aplicación de evaluación ev_d. Del siguiente resultado se deduce que la distancia mínima de $C_{\mathcal{X}}(d)$ propuesta en la conjetura 3.3.1 es de hecho la distancia mínima de un código de evaluación lineal C_d.

Corolario 3.3.7 [20, Cor. 6.9]. *Sea $\mathcal{L}_d$ el K-espacio vectorial generado por todos los $x^a \in S_d$ tales que x_1 divide a x^a. Si $1 \leq d \leq \sum_{i=2}^{n}(d_i - 1)$, entonces*

$$\text{máx}\{|V_{\mathcal{X}}(f)| : f \notin I(\mathcal{X}), f \in \mathcal{L}_d\} = \deg(S/I(\mathcal{X})) - (d_{k+2} - l + 1)d_{k+3} \cdots d_n,$$

donde $0 \leq k \leq n-2$ y l son enteros, $d = \sum_{i=2}^{k+1}(d_i - 1) + l$, y $1 \leq l \leq d_{k+2} - 1$.

Demostración. Sea $f \in \mathcal{L}_d \setminus I(\mathcal{X})$. Sea $\prec$ el orden lexicográfico con $x_1 \prec \cdots \prec x_n$ y sea $\mathcal{G}$ la base de Gröbner de $I(\mathcal{X})$ dada en [5, Prop. 2.11], es decir, $\mathcal{G} = \{x_i \prod_{a_j \in A_j}(x_j - a_j x_i) : i < j,\ i, j = 1, \ldots, n\}$. Por el algoritmo de división 1.6.4, podemos escribir $f = \sum_{i=1}^{r} a_i g_i + g$, donde $g_i \in \mathcal{G}$ para todo i y g es un polinomio estándar de grado d. El polinomio g está de nuevo en $\mathcal{L}_d \setminus I(\mathcal{X})$. En efecto, si $g \notin \mathcal{L}_d$, hay al menos un monomio de g que no contiene a x_1. Entonces, si ponemos $x_1 = 0$ en la última igualdad, obtenemos otra igualdad de la forma $0 = \sum_{i=1}^{r'} b_i g_i + h$, donde h es un polinomio estándar no nulo de $I(\mathcal{X})$, una contradicción. En consecuencia, por el teorema 3.3.6, se obtiene la desigualdad $\leq$ porque $|V_{\mathcal{X}}(f)| = |V_{\mathcal{X}}(g)|$. Para ver la igualdad, observamos que, de acuerdo a la demostración de [5, Lem. 3.1], existe un polinomio f de grado d en $\mathcal{L}_d \setminus I(\mathcal{X})$ cuyo número de ceros en $\mathcal{X}$ es igual al lado derecho de la igualdad pedida. □

Ejemplo 3.3.8 ([14, Ex. 6.1], [23, Ex. 3.5.8]). Sea $K = \mathbb{F}_4$, sea $\mathcal{X}$ el conjunto cartesiano anidado proyectivo

$$\mathcal{X} = [K_1 \times K_2 \times K_3] \subset \mathbb{P}^2$$

donde $K_1 = K_2 = \mathbb{F}_2$, $K_3 = \mathbb{F}_4$, y sea $I = I(\mathcal{X})$ el ideal de anulación de $\mathcal{X}$. El ideal I está generado por $x_1x_2^2 - x_1^2x_2$, $x_1x_3^4 - x_1^4x_3$, $x_2x_3^4 - x_2^4x_3$ (se puede ver con la expresión que utilizamos en la demostración de 3.3.7), $\text{reg}(S/I) = 5$, y $\deg(S/I) = 13$ (por 3.3.2). Para calcular la función distancia mínima generalizada y la función huella generalizada (en este caso para $r = 1$) utilizamos la definición de la función huella y 2.4.4, de manera que podemos obtenerlas con el siguiente procedimiento en [12].

```
q=4
G=GF(q,Variable=>a)
S=G[x3,x2,x1,MonomialOrder=>Lex]
I=ideal(x1*x2^2-x1^2*x2,x1*x3^4-x1^4*x3,x2^4*x3-x2*x3^4)
M=coker gens gb I, degree M, regularity M
init=ideal(leadTerm gens gb I)
H=(d)->hilbertFunction(d,M), apply(1..regularity(M),H)
h=(d)->degree M - max apply(apply(apply(apply(toList (set(0,a,a^2,a^3))^**
(hilbertFunction(d,M))-(set{0})^** (hilbertFunction(d,M)),toList),x->
basis(d,M)*vector deepSplice x),z->ideal(flatten entries z)), x-> if not
quotient(I,x)==I then degree ideal(I,x) else 0)
--h(d) es la funcion distancia minima en d
apply(1..regularity(M)-1,h) -- Para d>3 lleva demasiado tiempo
f=(x)-> if not quotient(init,x)==init then degree ideal(init,x) else 0
fp=(d) ->degree M -max apply(flatten entries basis(d,M),f)
```

```
--fp(d) es la funcion huella en d
apply(1..regularity(M),fp)
f=x3*(x3^3-x2^3-x1^3+x1^2*x2), degree ideal(I,f)
```

Para el orden lexicográfico con $x_1 \prec x_2 \prec x_3$ los resultados que se obtienen son los siguientes:

d	1	2	3	4	5	$\cdots$
$\lvert\mathcal{X}\rvert$	13	13	13	13	13	$\cdots$
$H_{\mathcal{X}}(d)$	3	6	9	12	13	$\cdots$
$\delta_{\mathcal{X}}(d,1)$	8	4	3	1	1	$\cdots$
$\mathrm{fp}_{I(\mathcal{X})}(d,1)$	8	4	3	1	1	$\cdots$

En el procedimiento hemos puesto como comentario que calcular la función distancia mínima para $d = 4$ lleva mucho tiempo. Pero en realidad para saber que $\delta_{\mathcal{X}}(d,1) = 1$ para $d \geq 4$ nos basta con encontrar un polinomio f de grado 4 cuya evaluación en los puntos de $\mathcal{X}$ nos de un vector de peso 1. El polinomio $f = x_3(x_3^3 - x_2^3 - x_1^3 + x_1^2x_2)$ se anula en todos los puntos de $\mathcal{X} \setminus \{[e_3]\}$ y $f(e_3) = 1$, donde $e_3 = (0,0,1)$, por lo que obtenemos $\delta_{\mathcal{X}}(d,1) = 1$ para $d \geq 4$. Observamos que en este ideal se tiene la igualdad $\delta_{\mathcal{X}}(d,1) = \mathrm{fp}_{I(\mathcal{X})}(d,1)$ para $d \geq 1$.

Por otro lado, este ejemplo contradice la conjetura 3.3.1, ya que los valores que deberíamos obtener, siguiendo la notación de la conjetura, serían los siguientes:

d	1	2	3	4	5	$\cdots$
k	0	1	1	1		
l	1	1	2	3		
$\delta_{\mathcal{X}}(d,1)$	8	4	3	2	1	$\cdots$

Vemos que la conjetura 3.3.1 falla en grado $d = 4$ en este caso.

Ejemplo 3.3.9. Vamos a continuar con el ejemplo 3.3.8, calculando la matriz huella $(\mathrm{fp}_{I(\mathcal{X})}(d,r))$ y la matriz de pesos $(\delta_{\mathcal{X}}(d,r))$. Estas matrices son de dimensiones 5×13 porque la regularidad y el grado de $S/I(\mathcal{X})$ son 5 y 13, respectivamente. Con el siguiente procedimiento en [12] podemos calcular directamente la matriz huella para el orden lexicográfico con $x_1 \prec x_2 \prec x_3$.

```
q=4
G=GF(q,Variable=>a)
S=G[x3,x2,x1,MonomialOrder=>Lex]
I=ideal(x1*x2^2-x1^2*x2,x1*x3^4-x1^4*x3,x2^4*x3-x2*x3^4)
M=coker gens gb I, degree M, regularity M
init=ideal(leadTerm gens gb I)
er=(x)-> if not quotient(init,x)==init then degree ideal (init,x) else 0
fpr=(d,r)->degree M - max apply(apply(apply(subsets(flatten entries
basis(d,M),r),toSequence),ideal),er)
```

```
g=(r)->apply(sort toList(set(1..regularity(M))**set{r}),fpr)
--g(r) es la r-esima columna de la matriz huella
apply(1..3,g)
```

La matriz que se obtiene es la siguiente:

$$(\mathrm{fp}_{I(\mathcal{X})}(d,r)) = \begin{pmatrix} 8 & 12 & 13 & \infty & \infty & \infty & \infty & \infty & \infty & \infty & \infty & \infty & \infty \\ 4 & 7 & 8 & 11 & 12 & 13 & \infty & \infty & \infty & \infty & \infty & \infty & \infty \\ 3 & 4 & 6 & 7 & 8 & 10 & 11 & 12 & 13 & \infty & \infty & \infty & \infty \\ 1 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & \infty \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \end{pmatrix}.$$

Si $r > H_{\mathcal{X}}(d)$, entonces $\mathcal{M}_{\prec,d,r} = \emptyset$ y la entrada (d,r) de esta matriz es igual a $|\mathcal{X}| = 13$, pero escribimos ∞ para que concuerde con lo que se obtiene del procedimiento (que, al hacer el máximo en un conjunto vacío devuelve $-\infty$, por lo que el procedimiento da como resultado $\deg(S/I)+\infty = \infty$). Por el teorema 3.2.4, obtenemos $(\mathrm{fp}_{I(\mathcal{X})}(d,r)) \leq (\delta_{\mathcal{X}}(d,r))$. Por el ejemplo 3.3.8 tenemos que $\mathrm{fp}_{I(\mathcal{X})}(d,1) = \delta_{\mathcal{X}}(d,1)$ para $d \geq 1$. También se da la igualdad $\mathrm{fp}_{I(\mathcal{X})}(d,2) = \delta_{\mathcal{X}}(d,2)$ para $d \geq 1$. Esto lo podemos comprobar considerando las siguientes parejas de polinomios $F^d = \{f_{1,d}, f_{2,d}\}$ de grado d: $F^1 = \{x_1 - x_2, x_1 - x_3\}$, $F^2 = \{(x_1 - x_2)(x_1 - x_3), (x_1 - x_2)x_2\}$, $F^3 = \{(x_1-x_2)(x_1-x_3)x_2, (x_1-x_2)x_2^2\}$ y $F^4 = \{(x_1-x_2)(x_1-x_3)x_2^2, (x_1-x_2)(x_2-x_3)x_2x_3\}$.

Utilizando el siguiente procedimiento en [12] podemos calcular $|V_{\mathcal{X}}(F^d)|$, donde $V_{\mathcal{X}}(F^d)$ es la variedad en $\mathcal{X}$ definida por F^d.

```
q=4
G=GF(q,Variable=>a)
S=G[x3,x2,x1,MonomialOrder=>Lex]
I=ideal(x1^2*x2-x1*x2^2,x1*x3^4-x1^4*x3,x2^4*x3-x2*x3^4)
f1=x1-x2, f2=x1-x3, quotient(I,ideal(f1,f2))==I
degree (I+ideal(f1,f2))
f1=(x1-x2)*(x1-x3), f2=(x1-x2)*x2, quotient(I,ideal (f1,f2))==I
degree (I+ideal(f1,f2))
f1=(x1-x2)*(x1-x3)*x2, f2=(x1-x2)*x2^2, quotient(I,ideal (f1,f2))==I
degree (I+ideal(f1,f2))
f1=(x1-x2)*(x1-x3)*x2^2, f2=(x1-x2)*(x2-x3)*x2*x3, quotient (I,ideal(f1,
f2))==I
degree (I+ideal(f1,f2))
```

Los resultados que obtenemos son $|V_{\mathcal{X}}(F^1)| = \deg(S/(I,F^1)) = 1$, $|V_{\mathcal{X}}(F^2)| = \deg(S/(I,F^2)) = 6$, $|V_{\mathcal{X}}(F^3)| = \deg(S/(I,F^3)) = 9$ y $|V_{\mathcal{X}}(F^4)| = \deg(S/(I,F^4)) = 10$. Por otro lado, hemos obtenido también que $(I : F^d) \neq I$ para $d = 1,\ldots,4$, así que restando a $\deg(S/I(\mathcal{X})) = 13$ los valores anteriores, obtenemos cotas superiores de $\delta_{\mathcal{X}}(d,2)$ para $d = 1,\ldots,4$. Pero estos valores coinciden con $\mathrm{fp}_{I(\mathcal{X})}(d,2)$ para $d = 1,\ldots,4$, así que por el teorema 3.2.4 tenemos que $\mathrm{fp}_{I(\mathcal{X})}(d,2) = \delta_{\mathcal{X}}(d,2)$ para $d = 1,\ldots,4$. Además, como para $d \geq \mathrm{reg}(S/I(\mathcal{X})) = 5$ se tiene que $\delta_{\mathcal{X}}(d,2) = 2$ (ver 3.2.3), obtenemos que la igualdad se da para $d = 1,\ldots,\mathrm{reg}(S/I(\mathcal{X}))$. De forma

análoga a lo que hemos hecho en el caso de $r = 2$, se puede comprobar que en este ejemplo $\mathrm{fp}_{I(\mathcal{X})}(d, r)$ es igual a $\delta_{\mathcal{X}}(d, r)$ para todo d, r (ver [14, Ex. 6.3]), es decir, I es fuertemente Geil-Carvalho.

Se pueden calcular algunos valores de la función distancia mínima generalizada directamente con el procedimiento que presentamos a continuación (como los correspondientes a $(d, r) = (1, 2)$ y $(d, r) = (1, 3)$), pero la gran mayoría de los valores requieren demasiado tiempo (y memoria) para ser calculados de esta manera.

```
q=4;
G=GF(q,Variable=>a);
S=G[x3,x2,x1,MonomialOrder=>Lex];
I=ideal(x1^2*x2-x1*x2^2,x1*x3^4-x1^4*x3,x2^4*x3-x2*x3^4);
M=coker gens gb I;
init=ideal(leadTerm gens gb I);
genmd=(d,r)->degree M - max apply(apply(subsets(apply(apply(apply(toList(
set(0,a,a^2,a^3))^**(hilbertFunction(d,M))-(set{0})^**(hilbertFunction(d,
M)),toList),x->basis(d,M)*vector deepSplice x),z->ideal(flatten entries z)
),r),ideal),x->if #set flatten entries mingens ideal(leadTerm gens x)==r
and not quotient(I,x)==I then degree(I+x) else 0)
apply(2..3,x->genmd(1,x))
```

3.3.2. Distancia mínima de códigos cartesianos afines

En esta sección, como aplicación de los teoremas 2.3.6 y 3.2.2, recuperamos la fórmula para la distancia mínima de un código cartesiano afín examinando el ideal de anulación correspondiente al código.

Corolario 3.3.10 [23, Cor. 3.3.1]**.** *Sea K un cuerpo y sea $C_{\mathcal{X}}(d)$ el código tipo Reed-Muller projectivo de grado d en el conjunto finito $\mathcal{X} = [1 \times A_2 \times \cdots \times A_s] \subset \mathbb{P}^{s-1}$. Si $1 \leq d_i \leq d_{i+1}$ para $i \geq 2$, con $d_i = |A_i|$, y $d \geq 1$, entonces la distancia mínima de $C_{\mathcal{X}}(d)$ viene dada por*

$$\delta_{\mathcal{X}}(d) = \begin{cases} (d_{k+2} - l)d_{k+3} \cdots d_n & \text{si } d \leq \sum_{i=2}^{n}(d_i - 1) - 1, \\ 1 & \text{si } d \geq \sum_{i=2}^{n}(d_i - 1), \end{cases}$$

donde $k \geq 0$ y l son los únicos enteros tales que $d = \sum_{i=2}^{k+1}(d_i - 1) + l$ y $1 \leq l \leq d_{k+2} - 1$.

Demostración. Sea $\succ$ el orden lexicográfico inverso graduado en S con $x_n \succ \cdots \succ x_2 \succ x_1$. Consideramos $f_i = \prod_{\gamma \in A_i}(x_i - \gamma x_1)$ para $i = 2, \ldots, n$. Se tiene que $f_2, \ldots, f_n$ es una base de Gröbner de $I(\mathcal{X})$ cuyo ideal inicial está generado por $x_2^{d_2}, \ldots, x_n^{d_n}$ (ver [19, Prop. 2.5]). Por el teorema 3.2.2 se tiene la igualdad $\delta_{\mathcal{X}}(d) = \delta_{I(\mathcal{X})}(d)$ para

$d \geq 1$. En consecuencia, la desigualdad "$\geq$" se deduce directamente del teorema 2.3.6. Supongamos que $d < \sum_{i=2}^{n}(d_i - 1)$. Para ver la otra desigualdad observamos que hay un polinomio $f \in S_d$ que es producto de formas lineales tal que $|V_{\mathcal{X}}(f)|$, el número de ceros de f en $\mathcal{X}$, es igual a $d_2 \cdots d_n - (d_{k+2} - l)d_{k+3} \cdots d_n$ (ver [19, P. 15-16]). Como $|\mathcal{X}|$ es igual a $d_2 \cdots d_n$, obtenemos que $\delta_{\mathcal{X}}(d)$ es menor o igual que $(d_{k+2} - l)d_{k+3} \cdots d_n$. □

Con técnicas similares a las que hemos usado en la sección sobre códigos cartesianos proyectivos se pueden obtener fórmulas para algunos otros parámetros. Por ejemplo, mencionamos a continuación algunos resultados interesantes sobre el segundo peso de Hamming generalizado.

Teorema 3.3.11 [14, Thm. 9.3]**.** *Sean A_i, $i = 1, \ldots, n-1$, subconjuntos de $\mathbb{F}_q$, y sea $\mathcal{X} \subset \mathbb{P}^{n-1}$ el conjunto cartesiano proyectivo dado por $\mathcal{X} = [A_1 \times \cdots \times A_{n-1} \times \{1\}]$. Si $d_i = |A_i|$ para $i = 1, \ldots, n-1$ y $2 \leq d_1 \leq \cdots \leq d_{n-1}$, entonces*

$$\delta_{\mathcal{X}}(d, 2) = \begin{cases} (d_{k+1} - l + 1)d_{k+2} \cdots d_{n-1} - d_{k+3} \cdots d_{n-1} & si\ k < n-3, \\ (d_{k+1} - l + 1)d_{k+2} \cdots d_{n-1} - 1 & si\ k = n-3, \\ d_{n-1} - l + 1 & si\ k = n-2, \\ 2 & si\ d \geq \sum_{i=1}^{n-1}(d_i - 1), \end{cases}$$

donde $0 \leq k \leq n-2$ y l son enteros tales que $d = \sum_{i=1}^{k}(d_i - 1) + l$ y $1 \leq l \leq d_{k+1} - 1$.

Observación 3.3.12. Vemos ejemplos de estos resultados en la siguiente sección, ya que los códigos parametrizados que vamos a estudiar son un caso particular de códigos cartesianos afines.

En [2] se encuentra una expresión (no del todo sencilla de evaluar) para el peso de Hamming generalizado r-ésimo de un código cartesiano afín utilizando técnicas distintas a las que estamos considerando en este trabajo. En todo caso, es interesante encontrar fórmulas alternativas fáciles de evaluar, como la que acabamos de ver, para los pesos generalizados de Hamming de los códigos cartesianos afines.

3.4. Distancia mínima de códigos parametrizados

En esta sección vamos a presentar brevemente algunos resultados sobre los códigos parametrizados sobre un toro proyectivo y ver algunos ejemplos de los códigos que se obtienen. Como referencias, vamos a utilizar principalmente [13] y [25].

De nuevo, con técnicas de álgebra conmutativa como las que hemos desarrollado en el trabajo (obteniendo fórmulas y cotas para el grado, y también para el número de ceros de polinomios) se puede obtener la distancia mínima de códigos parametrizados cuando $X = \mathbb{T}_{n-1}$. De hecho, estos resultados se pueden obtener también como consecuencia de los de códigos cartesianos afines.

Teorema 3.4.1 [25, Thm. 3.5]. *Si $X = \mathbb{T}_{n-1} \subset \mathbb{P}^{n-1}$ es un toro proyectivo y $d \geq 1$, entonces la distancia mínima de $C_X(d)$ viene dada por*

$$\delta_d = \begin{cases} (q-1)^{n-(k+2)}(q-1-l) & si\ \ d \leq (q-2)(n-1)-1, \\ 1 & si\ \ d \geq (q-2)(n-1), \end{cases}$$

donde k y l son los únicos enteros tales que $k \geq 0$, $1 \leq l \leq q-2$ y $d = k(q-2)+l$.

La siguiente proposición es una consecuencia inmediata del resultado anterior. Recordamos que un código lineal se dice que es MDS (maximum distance separable) si se da la igualdad en la cota de Singleton.

Proposición 3.4.2 [25, Prop. 3.6]. *Si X es un toro proyectivo en $\mathbb{P}^1$, entonces $C_X(d)$ es un código MDS y su distancia mínima viene dada por*

$$\delta(C_X(d)) = \begin{cases} q-1-d & si\ \ 1 \leq d \leq q-3, \\ 1 & si\ \ d \geq q-2. \end{cases}$$

Si X es un toro proyectivo en $\mathbb{P}^2$, entonces la distancia mínima de $C_X(d)$ viene dada por

$$\delta(C_X(d)) = \begin{cases} (q-1)^2 - d(q-1) & si\ \ 1 \leq d \leq q-2, \\ 2q-d-3 & si\ \ q-1 \leq d \leq 2q-5, \\ 1 & si\ \ d \geq 2q-4. \end{cases}$$

Teorema 3.4.3 ([13, Thm. 18], [14, Cor. 9.4]). *El segundo peso de Hamming generalizado del código $C_{\mathbb{T}_{n-1}}(d)$, $n \geq 3$, $d \geq 1$, viene dado por*

$$\delta_2(C_{\mathbb{T}_{n-1}}(d)) = \begin{cases} (q-1)^{n-(k+3)}[(q-1)(q-l)-1] & si\ \ 1 \leq d \leq \eta, \\ q-l & si\ \ \eta < d < r, \\ 2 & si\ \ d \geq r, \end{cases}$$

donde k y l son los únicos enteros tales que $d = k(q-2)+l$, $k \geq 0$, $1 \leq l \leq q-2$, $\eta = (q-2)(n-2)$ y $r = (q-2)(n-1)$.

Observación 3.4.4. En el caso $n < 3$, se tiene lo siguiente (ver [13, Rem. 4]): si $n = 2$ y $q = 3$, entonces $\delta_2(C_{\mathbb{T}_1}(d)) = 2$ para todo $d \geq 1$. Además, si $q > 3$, se tiene que

$$\delta_2(C_{\mathbb{T}_1}(d)) = \begin{cases} q-d & \text{si}\ \ 1 \leq d \leq q-3, \\ 2 & \text{si}\ \ d > q-3. \end{cases}$$

Ejemplo 3.4.5. Consideramos $\mathbb{F}_q$ con $q = 5$. Vamos a estudiar los parámetros de $C_{\mathbb{T}_{n-1}}(d)$ para $n = 2, \ldots, 4$. El ideal de anulación lo podemos obtener con 1.8.20 o 1.8.21. De cara a implementarlo en Macaulay2, se puede calcular $I(\mathbb{T}_3)$ y luego obtener los otros por eliminación de variables. El siguiente procedimiento calcula los distintos ideales de anulación y utiliza la función distancia mínima para obtener la distancia mínima de los códigos.

```
n=4 --El mayor n que vayamos a usar
s=n
q=5
G=GF(q,Variable=>a)
R=G[z,y_1..y_s,t_1..t_n];
T=ideal join(apply(1..n,x->t_x-y_x*z),apply(1..s,x->y_x^q-y_x),
apply(1..s,x->y_x^(q-1)-1))
J=eliminate(eliminate(T,toList (y_1..y_s)),z)
L=apply(0..n-2,x-> eliminate(J,toList (t_(n-x+1)..t_(n))))
Y=apply(0..n-2,x->substitute(L#x,G[t_1..t_(n-x)]))
A=set apply(1..q-1,x->a^x)+set {0}
h=(d,I)->degree I - max apply(apply(apply(apply(toList (A)^**
(hilbertFunction(d,I))-(set{0})^**(hilbertFunction(d,I)), toList),
x->basis(d,coker gens I)*vector deepSplice x),z->ideal(flatten entries z))
,x-> if not quotient(I,x)==I then degree ideal(I,x) else 0)
--h(d,I) es la funcion distancia minima de I
reg=apply(0..n-2,x->regularity(coker gens gb L#x))
apply(1..reg#2,x-> h(x,Y#2))
h(1,Y#1)
h(1,Y#0)
```

Con el procedimiento anterior solo podemos calcular de manera efectiva algunos valores, pero obviamente podemos utilizar la fórmula para la distancia mínima 3.4.1 y obtener $\delta_{\mathbb{T}_{n-1}}(d)$, $2 \leq n \leq 4$, $1 \leq d \leq \operatorname{reg}(S/I(\mathbb{T}_{n-1})) = (n-1)(q-1)$. Los resultados que se obtienen para la distancia mínima en términos de n y d son los siguientes:

$n\backslash d$	1	2	3	4	5	6	7	8	9
2	3	2	1	–	–	–	–	–	–
3	12	8	4	3	2	1	–	–	–
4	48	32	16	12	8	4	3	2	1

Por otro lado, sabemos que la longitud del código es $(q-1)^{n-1}$ y también conocemos la dimensión por 1.8.22, así que, para estos códigos que estamos considerando podemos dar la distancia mínima en una tabla en términos de la longitud y la dimensión, que es lo habitual. Vamos a utilizar en lo que sigue n y k para denotar la longitud y la dimensión del código, que es la notación estándar en teoría de códigos.

$n\backslash k$	2	3	4	6	10	13	15	16	20	32	44	54	60	63	64
4	**3**	**2**	**1**	–	–	–	–	–	–	–	–	–	–	–	–
16	–	**12**	–	**8**	4	**3**	**2**	**1**	–	–	–	–	–	–	–
64	–	–	48	–	32	–	–	–	16	12	8	4	**3**	**2**	**1**

Estos valores los podemos comparar con los mejores valores conocidos de distancia mínima para códigos con la misma longitud y dimensión que los que hemos obtenido

para ver cómo de buenos son los parámetros de estos códigos. Para ello, se puede utilizar [15]. En la tabla hemos puesto en negrita los valores que alcanzan el mejor valor conocido para la distancia mínima para códigos con esos parámetros, que en este ejemplo es de hecho óptima excepto en el caso de $n = 16$, $k = 6$, que se sabe que la cota inferior para la distancia mínima es 8 y la cota superior es 9.

Este mismo procedimiento se puede hacer para distintos cuerpos, y en general se encuentra que para k pequeño (respecto a n) o k grande (próximo a n) se obtienen códigos con parámetros muy cercanos a los óptimos, por ejemplo $n = 36$, $k = 6$, y distancia mínima 24 (la cota inferior es 25 y la superior 27 para la distancia mínima óptima), o $n = 64$, $k = 6$ y distancia mínima 48 (la cota inferior es 49 y la superior 53). Para valores de k intermedios sí hay una diferencia razonable con el valor óptimo de la distancia mínima.

Ejemplo 3.4.6. Continuando con el ejercicio anterior, podemos calcular el segundo peso de Hamming generalizado de los códigos que hemos considerado. Lo podríamos calcular directamente con la función distancia mínima generalizada (cambiando simplemente la función del procedimiento del ejemplo anterior), pero es muy poco práctico en esta situación (lleva demasiado tiempo). En cualquier caso, como tenemos la fórmula 3.4.3 para el segundo peso de Hamming generalizado, lo podemos calcular y obtenemos los siguientes valores (n y k son de nuevo la longitud y la dimensión del código).

$n\backslash k$	2	3	4	6	10	13	15	16	20	32	44	54	60	63	64
4	**4**	**3**	**2**	–	–	–	–	–	–	–	–	–	–	–	–
16	–	**15**	–	11	7	4	**3**	**2**	–	–	–	–	–	–	–
64	–	–	60	–	44	–	–	–	28	15	11	7	4	**3**	**2**

En este caso hemos puesto en negrita los valores que cumplen la cota de Singleton generalizada. Cuando un código cumple lo anterior para un peso de Hamming generalizado r-ésimo, se dice que es r-MDS. Una propiedad interesante de estos códigos es que existe un α (en principio distinto para cada $C_{\mathbb{T}_{n-1}}(d)$) tal que son r-MDS para $\alpha \leq r \leq |\mathbb{T}_{n-1}|$ (ver [13, Cor. 1.]).

Bibliografía

[1] M. F. Atiyah, I. G. Macdonald. Introduction to Commutative Algebra. Addison-Wesley, 1969.

[2] P. Beelen, M. Datta. Generalized Hamming weights of affine Cartesian codes. Finite Fields Appl 51 (2018) 130-145.

[3] I. Bermejo, P. Gimenez. Saturation and Castelnuovo-Mumford regularity. Journal of Algebra 303 (2006) 592-617.

[4] W. Bruns, J. Herzog. Cohen-Macaulay rings. Second Edition. Cambridge Studies in Advanced Mathematics 39. Cambridge University Press, 1998.

[5] C. Carvalho, V. G. Lopez Neumann, H. H. López. Projective Nested cartesian Codes. Bulletin of the Brazilian Mathematical Society, New Series 48 (2017) 283-302.

[6] S. M. Cooper, A. Seceleanu, Ş. O. Tohăneanu, M. Vaz Pinto, R. H. Villarreal. Generalized minimum distance functions and algebraic invariants of Geramita ideals. Advances in Applied Mathematics 112 (2020), 101940.

[7] D. A. Cox, J. Little, D. O'Shea. Ideals, Varieties, and Algorithms. Fourth Edition. Undergraduate Texts in Mathematics. Springer, 2015.

[8] D. A. Cox, J. Little, D. O'Shea. Using Algebraic Geometry. Second Edition. Graduate Texts in Mathematics, Vol. 185. Springer, 2005.

[9] W. Decker, G.-M. Greuel, G. Pfister, H. Schönemann. Singular 4.1.2. A Computer Algebra System for Polynomial Computations, `http://www.singular.uni-kl.de`, 2019.

[10] D. Eisenbud. Commutative Algebra with a View Toward Algebraic Geometry. Graduate Texts in Mathematics, Vol. 150. Springer, 1995.

[11] D. Eisenbud. The Geometry of Syzygies. Graduate Texts in Mathematics, Vol. 229. Springer, 2005.

[12] D. Grayson, M. Stillman. Macaulay2, a software system for research in algebraic geometry. `https://faculty.math.illinois.edu/Macaulay2/`.

[13] M. González-Sarabia, E. Camps, E. Sarmiento, R.H. Villarreal. The second generalized Hamming weight of some evaluation codes arising from a projective torus. Finite Fields Appl. 52 (2018) 370-394.

[14] M. González-Sarabia, J. Martínez-Bernal, R.H. Villarreal, C.E. Vivares. Generalized minimum distance functions. Journal of Algebraic Combinatorics 50 (2019) 317-346.

[15] M. Grassl. Bounds on the minimum distance of linear codes and quantum codes. Online available at `http://www.codetables.de`. Accessed on 2021-04-02.

[16] G.-M. Greuel, G. Pfister. A Singular Introduction to Commutative Algebra. Second Edition. Springer, 2008.

[17] I. Kaplansky. Commutative Rings. University of Chicago Press, 1974.

[18] M. Kreuzer, L. Robbiano. Computational Commutative Algebra 2. Springer, 2005.

[19] H. H. López, C. Rentería, R.H. Villarreal. Affine cartesian codes. Designs, Codes and Cryptography 71 (2014) 5-19.

[20] J. Martínez-Bernal, Y. Pitones, R.H. Villarreal. Minimum distance functions of graded ideals and Reed-Muller-type codes. Journal of Pure and Applied Algebra 221 (2017) 251-275.

[21] H. Matsumura. Commutative ring theory. Cambridge Studies in Advanced Mathematics 8. Cambridge University Press, 1989.

[22] L. Núñez-Betancourt, Y. Pitones, R.H. Villarreal. Footprint and Minimum Distance Functions. Communications of the Korean Mathematical Society 33 (2018) 85-101.

[23] Y. Pitones. Minimum Distance Functions and Reed-Muller-Type Codes. PhD thesis, CINVESTAV, México, 2019.

[24] R. San José. Regularidad de Castelnuovo-Mumford e ideales iniciales genéricos. Trabajo de Fin de Grado, U. Valladolid, 2020.

[25] E. Sarmiento, M. Vaz Pinto, R.H. Villarreal. The minimum distance of parameterized codes on projective tori. AAECC 22, 249–264 (2011).

[26] A. Tochimani, R.H. Villarreal. Vanishing Ideals over Finite Fields. Mathematical Notes 105, 429-438 (2019).

[27] W. V. Vasconcelos. Computational Methods in Commutative Algebra and Algebraic Geometry. Algorithms and Computation in Mathematics, Volume 2. Springer, 1998.

[28] R. H. Villarreal. Monomial Algebras, Second Edition. Monographs and Research Notes in Mathematics. Chapman and Hall/CRC, 2015.

[29] V. K. Wei. Generalized Hamming weights for linear codes. IEEE Transactions on Information Theory 37 (1991) 1412-1418.