

Métodos del Álgebra Conmutativa en la Teoría de Códigos

Cristo Daniel Alvarado

12 de noviembre de 2024

Índice general

1. Preliminares	2
1.1. Teoría de Códigos	2
1.2. Álgebra	4
1.3. Puntos Gordos (Fat-points)	6
1.4. La distancia mínima y el grado inicial	10

Capítulo 1

Preeliminaries

1.1. Teoría de Códigos

Definición 1.1.1

Un **código** \mathcal{C} es un subconjunto de \mathbb{K}^n , donde \mathbb{K} es un campo. Si \mathcal{C} es un subespacio vectorial, decimos que \mathcal{C} es un **código lineal**.

Los elementos de \mathcal{C} son llamados **palabras**.

Observación 1.1.1

En la definición anterior, el campo \mathbb{K} puede ser finito o infinito, y generalmente se usará $\mathbb{K} = \mathbb{F}_q$.

Observación 1.1.2

Un código lineal puede ser considerado como:

$$\mathcal{C} = \mathcal{L}(w_1, \dots, w_n)$$

si consideramos la base estándar de \mathbb{K}^n , entonces podemos pensar en \mathcal{C} como la imagen de una función lineal $\phi : \mathbb{K}^k \rightarrow \mathbb{K}^n$, con matriz $k \times n$, denotada por G .

En particular:

$$G = \begin{pmatrix} w_1 \\ \vdots \\ w_k \end{pmatrix}$$

además, $\mathcal{C} = \phi(\mathbb{K}^k)$.

Definición 1.1.2

En el ejemplo anterior, G es llamada **matriz generadora de \mathcal{C}** .

En cierto sentido, la matriz \mathcal{C} es la que genera al código.

¿Cómo podemos determinar si $v \in \mathbb{K}^n$ es una palabra de \mathcal{C} ?

Pues en el caso en que $v \in \mathcal{C}$, se tiene que

$$\phi(v) = vG = vw_1 + \dots + v_kw_k$$

y, $\dim_{\mathbb{K}} \mathcal{C} = \dim \mathcal{C}$. n es llamado **longitud (bloque)** de \mathcal{C} .

Notemos que si \mathcal{C} es un subespacio vectorial, podemos considerar al espacio ortogonal:

$$\mathcal{C}^\perp = \left\{ w \in \mathbb{K}^n \mid w \cdot c = 0, \quad \forall c \in \mathcal{C} \right\}$$

Definición 1.1.3

El espacio \mathcal{C}^\perp es llamado **código dual**. Este es un subespacio de \mathbb{K}^n y hacemos que H sea la **matriz generadora de \mathcal{C}^\perp** .

H también es la matriz de chequeo de paridad de \mathcal{C} , pues tenemos que \mathcal{C} es el espacio nulo de H , pues:

$$\dim \mathcal{C} + \dim \mathcal{C}^\perp = n$$

Definición 1.1.4

Si $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in \mathbb{K}^n$, se define la **distancia de Hamming** entre ambos vectores por:

$$d(x, y) = \left| \left\{ i \in \{1, \dots, n\} \mid x_i \neq y_i \right\} \right|$$

Definición 1.1.5

El **peso de Hamming** de un vector $v \in \mathbb{K}^n$ es el número de entradas diferentes de 0 que tiene v :

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

La **distancia mínima de $\mathcal{C} \subseteq \mathbb{K}^n$** se define por:

$$d(\mathcal{C}) = \min \left\{ w(v) \mid v \in \mathcal{C} \setminus \{0\} \right\}$$

Una palabra $v \in \mathcal{C}$ tal que $w(v) = d(\mathcal{C})$ será llamada **palabra de peso mínimo**.

Se tienen los siguientes parámetros básicos de un código lineal \mathcal{C} :

- Dimensión ($\dim_{\mathbb{K}}(\mathcal{C})$).
- Longitud (tamaño de las palabras, n).
- Distancia mínima ($d(\mathcal{C})$).

Observación 1.1.3

$d(\mathcal{C})$ mide la capacidad de detección y corrección de errores en un código.

Proposición 1.1.1

Se tiene lo siguiente:

- (1) La distancia de Hamming es una métrica en \mathbb{K}^n .
- (2) Para cualquier código lineal $[n, \dim_{\mathbb{K}}(\mathcal{C}), d(\mathcal{C})]$ se satisface que:

$$d(\mathcal{C}) \leq n - \dim \mathcal{C} + 1$$

la cota superior es llamada **cota de Singleton**. Cuando $d(\mathcal{C}) = n - \dim \mathcal{C} + 1$, el código es llamado **MDS (maximum distance separable)**.

- (3) Si H es la matriz de chequeo de paridad, entonces $c \in \mathcal{C}$ si y sólo si $Hc^T = 0$.

Demostración:

■

Definición 1.1.6

Diremos que dos códigos son **equivalentes**, se tienen los mismos parámetros.

Definición 1.1.7

Un código es **no degenerado**, si para cualquier matriz generadora M , todas sus columnas son no nulas.

Ejemplo 1.1.1

Considere $\mathbb{K} = \mathbb{F}_2$. Tomemos el código lineal con matriz generadora:

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

tiene los parámetros $[7, 4, 3]$. Si multiplicamos todos los vectores de \mathbb{F}_2^4 , se tiene que \mathcal{C} consta de 16 palabras, tiene 7 con peso de Hamming igual a 3, 7 con peso de Hamming igual a 4 y 1 con peso de Hamming igual a 7, más el vector 0. Por lo que $d(\mathcal{C}) = 3$.

Observación 1.1.4

La equivalencia es en que estamos olvidando la información sobre la estructura de espacio vectorial del código \mathcal{C} , pero estamos preservando información que tiene que ver con la longitud de la palabra, dimensión del espacio y la distancia mínima (lo que sea para lo que sirva).

Ejercicio 1.1.1

Sea \mathcal{C} un $[n, k]$ código lineal no degenerado con matriz generadora G de tamaño $k \times n$. Entonces:

$$d(\mathcal{C}) = n - h$$

donde h es el máximo del número de columnas de la matriz generadora que generan a un subespacio $k - 1$ dimensional.

Demostración:

Ejercicio. ■

1.2. Álgebra

Observación 1.2.1

De ahora en adelante, R será un anillo conmutativo con identidad.

Definición 1.2.1

Sea I un ideal de R , se define el **ideal radical de I** (denotado por \sqrt{I}) por:

$$\sqrt{I} = \left\{ r \in R \mid r^n \in I, \text{ para algún } n \in \mathbb{N} \right\}$$

Definición 1.2.2

Un ideal Q de R es **ideal primario de R** , si siempre que $f \cdot g \in Q$ con $f \notin Q$, entonces $g \in \sqrt{Q}$.

Observación 1.2.2

Si Q es primario, entonces $\sqrt{Q} = P$ es ideal primo

Definición 1.2.3

Si:

$$\text{mín}(Q) = \{P\}$$

(es decir, el mínimo de los ideales primos que contienen a Q es P), decimos que Q es **P -primario**.

Definición 1.2.4

Un ideal $I \subseteq R$ es **Noetheriano**, si es finitamente generado, esto es que existen $f_1, \dots, f_l \in R$ tales que

$$I = \langle f_1, \dots, f_l \rangle$$

por ende, todo $g \in I$ puede ser expresado como:

$$g = r_1 f_1 + \dots + r_l f_l$$

con $r_i \in R$.

Teorema 1.2.1

Podemos expresar a $I \subseteq R$ como:

$$I = Q_1 \cap \dots \cap Q_s$$

donde cada Q_i es P_i -primario y a esta descomposición le llamamos **descomposición primaria minimal**, para la cual se cumple que el ideal

$$P_i = \sqrt{Q_i}$$

es primo.

Demostración:

Ver Hungerford. ■

Definición 1.2.5

Dado un ideal $I \subseteq R$, el conjunto formado a partir del teorema anterior:

$$\text{Ass}(I) = \{P_1, \dots, P_s\}$$

es llamado el **conjunto de primos asociados a I** .

Definición 1.2.6

La altura de un ideal primo $P \subseteq R$ es el supremo de las longitudes n , de las cadenas de ideales primos:

$$P_0 \subsetneq P_1 \subsetneq \dots \subsetneq P_n = P$$

denotado por $ht(P)$.

Definición 1.2.7

Sea $I \subseteq R$. Se define la **altura de I** , como:

$$ht(I) = \min \{ht(P) \mid I \subseteq P\}$$

Definición 1.2.8

La **dimensión de Krull de R** es el máximo de $ht(P)$ tal que P es ideal primo de R . En este caso, la dimensión de Krull de R se denota por $\dim R$.

Cuando $R = K[x_1, \dots, x_n]$, se tiene que:

$$\dim R/I = \dim R - ht(I)$$

y, $\dim R = n$. Para la prueba de esto, vea algún libro de álgebra conmutativa.

Ejemplo 1.2.1

Considere $A = K[x, y, z]/I$ donde $I = \langle xy, xz \rangle$. Una descomposición primaria sería:

$$I = \langle x \rangle \cap \langle y, z \rangle$$

Además,

$$\begin{aligned} ht(I) &= \min \{ht(\langle x \rangle), ht(\langle y, z \rangle)\} \\ &= \min \{1, 2\} \\ &= 1 \end{aligned}$$

Por el hecho anterior, se tiene que

$$\dim K[x, y, z]/\langle xy, xz \rangle = 3 - 1 = 2$$

1.3. Puntos Gordos (Fat-points)

En el espacio afín \mathbb{A}^k (producto de \mathbb{K} consigo mismo k -veces), podemos tomar el conjunto $\mathbb{A}^k \setminus \{(0, \dots, 0)\}$ y definir una equivalencia sobre este conjunto dada como sigue:

$$(a_1, \dots, a_k) \sim (b_1, \dots, b_k)$$

si y sólo si existe $\lambda \in \mathbb{K}$ tal que:

$$(a_1, \dots, a_k) = (\lambda b_1, \dots, \lambda b_k)$$

Se prueba rápidamente que \sim es relación de equivalencia sobre este conjunto.

Denotamos por $[a_1, \dots, a_k] = [a_1 : \dots : a_k]$ a la clase de equivalencia con representante (a_1, \dots, a_k) .

Definición 1.3.1

El conjunto de todas las clases de equivalencia anteriores es denotado por \mathbb{P}^{k-1} y es llamado **espacio proyectivo**.

Un elemento $[a_1, \dots, a_k] \in \mathbb{P}^{k-1}$ es un **punto proyectivo**, a_1, \dots, a_k son llamadas **coordenadas homogéneas**. Un **representante estándar** de un punto proyectivo es un representante con la primer coordenada homogénea igual a 1, esto es, que es de la forma:

$$[0, \dots, 0, 1, a_i, \dots, a_k]$$

Definición 1.3.2

Consideremos el anillo $R = K[x_1, \dots, x_n]$. Una **variedad proyectiva**, es el conjunto de ceros comunes de un conjunto de polinomios homogéneos en R .

Si $X \subseteq \mathbb{P}^{k-1}$, se define el **ideal de anulaci3n** o **ideal de definici3n** de X , denotado por $I(X)$, es el conjunto de todos los polinomios que se anulan en todos los puntos de X .

Definici3n 1.3.3

Una **hipersuperficie** es una variedad generada por una sola variedad polinomial.

Definici3n 1.3.4

La **dimensi3n** de una variedad proyectiva $X \subseteq \mathbb{P}^{k-1}$ es m si $k-1-m$ es el n3mero m3s peque1o de hiperplanos gen3ricos que tienen intersecci3n con X en un conjunto finito de puntos.

El n3mero de este conjunto finito de puntos es llamado el **grado** de X , denotado por $\deg(X)$.

Ejemplo 1.3.1

En particular, si $Q \in \mathbb{P}^{k-1}$ con $Q = [a_1, \dots, a_k]$, entonces

$$I(Q) = \langle \{a_i x_j - a_j x_i \mid 1 \leq i < j \leq k\} \rangle$$

Si $X = \{P_1, \dots, P_m\}$ es un conjunto finito de puntos de \mathbb{P}^{k-1} y su ideal de definici3n

$$I(X) = I(P_1) \cap \dots \cap I(P_m)$$

para cada punto $P_i \in X$.

Definici3n 1.3.5

En lo anterior, tenemos que se denomina un **esquema de puntos reducidos**.

Definici3n 1.3.6

Sea $X = \{P_1, \dots, P_m\} \subseteq \mathbb{P}^{k-1}$ un conjunto finito y n_1, \dots, n_m enteros positivos. Un **esquema de puntos gordos**, es un esquema de puntos proyectivos con ideal de definici3n:

$$I(X) = I(P_1)^{n_1} \cap \dots \cap I(P_m)^{n_m}$$

Observaci3n 1.3.1

En notaci3n de *divisores*, escribimos:

$$\mathcal{Z} = n_1 P_1 + \dots + n_m P_m$$

El **soporte** de \mathcal{Z} es $\text{sup}(\mathcal{Z}) = X$ y los enteros n_i representan la multiplicidad de p_i .

Definici3n 1.3.7

Sea $X = \{P_1, \dots, P_n\} \subseteq \mathbb{P}^{k-1}$. Si consideramos a G como la matriz $k \times n$ con columnas las coordenadas homog3neas de alg3n representante de P_i .

Decimos que X est3n en **posici3n general** si y s3lo si para cualquier $1 \leq c \leq \min\{n, k\}$, cualesquiera c columnas de G generan un espacio c -dimensional de \mathbb{K}^k .

Definición 1.3.8

Si $p = [a_1, \dots, a_k] \in \mathbb{P}^k$ es un punto, entonces podemos asociar una forma lineal $l_p = a_1x_1 + \dots + a_kx_k \in R = K[x_1, \dots, x_n]$.

Inversamente, para cualquier forma lineal $l = b_1x_1 + \dots + b_kx_k$ podemos asociar un punto $l^\nu = [b_1, \dots, b_k] \in \mathbb{P}^k$.

De momento, esto es todo lo que ocupamos de álgebra.

Consideremos \mathcal{C} un $[n, k, d]$ código lineal con matriz generadora G de tamaño $k \times n$, rango $k \geq 1$ y además el código \mathcal{C} es no degenerado. Considere el conjunto de n puntos reducidos (esto es, que la multiplicidad de cada uno es uno), digamos:

$$x_c = \{p_1, \dots, p_n\} \subseteq \mathbb{P}^{k-1}$$

donde las coordenadas homogéneas de los puntos p_i corresponden a las entradas de la i -ésima columna de G , como el rango de G es k , entonces el conjunto de puntos x_c no están todos incluidos en un hiperplano de \mathbb{P}^{k-1} .

Definición 1.3.9

En el caso anterior, el **esquema reducido**, es el ideal de definición de x_c :

$$I(x_c) = I(p_1) \cap \dots \cap I(p_n)$$

Si la matriz G tiene columnas proporcionales, consideremos:

$$\mathcal{Z}_c = m_1p_1 + \dots + m_s p_s$$

donde m_i es la respectiva multiplicidad de dos columnas proporcionales.

Definición 1.3.10

En el caso anterior, el esquema de puntos gordos asociado a \mathcal{C} es el ideal de definición:

$$I(\mathcal{Z}_c) = I(p_1)^{m_1} \cap \dots \cap I(p_s)^{m_s}$$

Ahora analizaremos la conexión entre \mathcal{C} y todas las ideas algebraicas que hemos introducido anteriormente.

Definición 1.3.11

Para un esquema de puntos gordos $\mathcal{Z} \subseteq \mathbb{P}^{k-1}$, denotaremos por $hyp(\mathcal{Z})$ al máximo número de puntos de \mathcal{Z} (contando multiplicidad) que están contenidos en un hiperplano de \mathbb{P}^{k-1} .

Ejemplo 1.3.2

Imaginemos que el esquema de puntos gordos está dado por:

$$\mathcal{Z} = 3p_1 + 2p_2 + p_3 + p_4 \subseteq \mathbb{P}^2$$

con p_1, \dots, p_4 no colineales y p_2, \dots, p_4 colineales, entonces:

$$hyp(\mathcal{Z}) = 5$$

ya que recuerde que estamos contando multiplicidades.

Definición 1.3.12

Decimos que el código \mathcal{C} es **definido por el esquema de puntos gordos** \mathcal{Z}_c .

Proposición 1.3.1

Sea \mathcal{C} un código lineal, $[n, k, d]$ un código lineal con esquema de puntos gordos \mathcal{Z}_c en \mathbb{P}^{k-1} . Entonces:

$$d = n - \text{hyp}(\mathcal{Z}_c)$$

Demostración:

Por definición, la distancia de mínima d de código lineal, existe una palabra no cero $v = (v_1, \dots, v_n) \in \mathcal{C}$ tal que

$$w(v) = d = d(\mathcal{C})$$

y cualquier otra palabra de \mathcal{C} tiene peso de Hamming mayor o igual a d . En particular, cualquier otra palabra con peso menor que d es la palabra cero.

Como $v \in \mathcal{C}$, entonces existe $\alpha = (\alpha_1, \dots, \alpha_k) \in \mathbb{K}^k$ tal que

$$l_i(\alpha) = v_i, \quad \forall i = 1, \dots, n$$

donde l_i son las formas lineales de \mathcal{C} en $\mathbb{K}[x_1, \dots, x_n]$.

También tenemos que existen índices $i_1, \dots, i_{n-d} \in \{1, \dots, n\}$ tales que

$$l_{i_a}(\alpha) = 0$$

con $a = 1, \dots, n-d$ y si $j \in \{1, \dots, n\} \setminus \{i_1, \dots, i_{n-d}\}$, entonces:

$$l_j(\alpha) \neq 0$$

Pero, como

$$l_i = a_{1i}x_1 + \dots + a_{ki}x_k$$

donde a_{ji} son entradas de la matriz generadora G . Entonces:

$$l_i(\alpha) = a_{1i}\alpha_1 + \dots + a_{ki}\alpha_k = L(p_i)$$

donde

$$L(x_1, \dots, x_k) = \alpha_1x_1 + \dots + \alpha_kx_k$$

siendo $P_i = [a_{1i}, \dots, a_{ki}] \in \mathbb{P}^{k-1}$ es la i -ésima columna de G . ¿Cuál es el máximo número de puntos del esquema \mathcal{Z}_c del esquema que contando multiplicidades están en un mismo hiperplano? Pues debe ser $n-d$, ya que esos son los únicos números de puntos que le pegan al cero en las transformaciones l_i en su respectiva i -ésima entrada, luego son ceros de L , por lo que están en el hiperplano generado por la imagen del endomorfismo L . Por lo que:

$$\text{hyp}(\mathcal{Z}_c) = n-d \Rightarrow d = n - \text{hyp}(\mathcal{Z}_c)$$

lo que prueba el resultado. ■

Observación 1.3.2

En la proposición anterior, estamos clasificando cosas en función de si nos da algo o no nos da nada.

Definición 1.3.13

Para un esquema de puntos gordos $\mathcal{Z}_c = m_1 p_1 + \cdots + m_s p_s \subseteq \mathbb{P}^{k-1}$ no todos colineales, si

$$m_1 + \cdots + m_s = n$$

entonces, el valor $n - \text{hyp}(\mathcal{Z})$ se llama la **distancia mínima de \mathcal{Z}** y la denotaremos por $d(\mathcal{Z})$ (n es el número de puntos).

Sea $\mathcal{Z} = m_1 p_1 + \cdots + m_s p_s \subseteq \mathbb{P}^{k-1}$ un esquema de puntos gordos no contenidos todos en un hiperplano con $m_1 \geq m_2 \geq \cdots \geq m_s$. Se tiene que:

$$\text{sup}(\mathcal{Z}) = \{p_1, \dots, p_s\} = X$$

para $i = 1, \dots, s$ supongamos que c_i es el vector columna del punto p_i . Consideremos

$$A(X) = (c_1, \dots, c_s)$$

y,

$$A(\mathcal{Z}) = (\underbrace{c_1, \dots, c_1}_{m_1}, \dots, \underbrace{c_s, \dots, c_s}_{m_s})$$

Teorema 1.3.1

Si $d = d(X)$, entonces

$$m_1 + \dots + m_d \geq d(\mathcal{Z}) \geq m_{s-d+1} + \cdots + m_s$$

además, si $m_1 = \cdots = m_s = m$, entonces

$$d(\mathcal{Z}) = md(X)$$

Ejemplo 1.3.3

Considere

$$\mathcal{Z} = 3p_1 + 2p_2 + p_3 + p_4$$

como en el ejemplo anterior. Se determinó que $\text{hyp}(\mathcal{Z}) = 5$. Se tiene además que $d(\mathcal{Z}) = n - 5 = 7 - 2 = 2$. Se tiene que $X = \{p_1, p_2, p_3, p_4\}$, por lo que $d(X) = 4 - 3 = 1$ y $\text{hyp}(X) = 3$.

1.4. La distancia mínima y el grado inicial

Definición 1.4.1

Sea \mathcal{C} un $[n, k, d]$ código lineal y \mathcal{Z}_c su esquema de puntos gordos. El **grado inicial del ideal** $I(\mathcal{Z}_c)$ denotado como

$$\alpha(\mathcal{Z}) = \alpha(I(\mathcal{Z})) = \min \left\{ t \mid I(\mathcal{Z})_t \neq 0 \right\}$$

(ver anillos graduados).

En el caso anterior, se tiene que:

$$I(\mathcal{Z}) = \bigoplus_{t \geq 0} I(\mathcal{Z})_t$$

Una familia *especial* de códigos es la llamada familia de **códigos evaluación**: sea $X = \{p_1, \dots, p_n\} \subseteq \mathbb{P}^{k-1}$ un conjunto finito. Se tiene que

$$R = \mathbb{K}[x_1, \dots, x_k] = \bigoplus_{t \geq 0} R_t$$

donde R_a es un espacio vectorial de polinomios homogéneos de grado t .

Definimos un mapeo lineal

$$ev_t : R_t \rightarrow \mathbb{K}^n$$

dado por:

$$ev_t(f) = (f(p_1), \dots, f(p_n))$$

Definición 1.4.2

El código **evaluación** es la imagen de $ev_t(R_t) \subseteq \mathbb{K}^n$.

Observación 1.4.1

El código evaluación es un código lineal de orden/grado t en el conjunto X .

Teorema 1.4.1

Todo código lineal es un código evaluación.

Demostración:

■

Proposición 1.4.1

El código evaluación tiene los parámetros básicos que cumplen las igualdades:

- Longitud, $n = |X| = \deg(R/I(X)) = e$, donde e es llamado la multiplicidad de Hilbert-Samuel.
- Dimensión es igual a $H(R/I(X), t)$
- Distancia mínima, $d(ev_t(R_t)) = d$, y

$$d_t = n - \max_{X' \subseteq X} \left\{ |X'| \mid \dim_{\mathbb{K}}(I(X')_t) > \dim_{\mathbb{K}}(I(X)_t) \right\}$$

Nos dedicaremos a probar esta proposición.

Definición 1.4.3

Se define la función de Hilbert de un ideal graduado $I \subseteq R$:

$$H_I(n) = \dim_{\mathbb{K}}(R/I)_n$$

Definición 1.4.4

con lo que se define la serie de Hilbert:

$$\begin{aligned} \text{Hilbert}_I(t) &= \sum_{i \geq 0} \dim_{\mathbb{K}}(R/I)_i t^i \\ &= \sum_{i \geq 0} H_i(t) t^i \end{aligned}$$

Teorema 1.4.2 (Teorema de Hilbert-Serre)

$$\text{Hilbert}_I(t) = \frac{h(t)}{(1-t)^s}$$

donde $s = \dim(R/I) - 1$ y $h(t) \in \mathbb{Q}[t]$ y $\deg(h) \leq n$.

Definición 1.4.5

Se define el grado de multiplicidad de R/I por:

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

con h dada en la función anterior.

Ejemplo 1.4.1

Considere el anillo $R = K[x, y]$ y el ideal $I = \langle x^2, xy^2, y^4 \rangle$. Queremos calcular $e(R/I)$. Se tiene el anillo graduado:

$$R/I = \bigoplus_{n \geq 0} (R/I)_n$$

se tiene que:

Grado	Graduado	Base	Valor Hilbert $H_I(n)$
$n = 0$	$(R/I)_0 = \mathbb{K}$	$\{1\}$	1
$n = 1$	$(R/I)_1$	$\{x, y\}$	2
$n = 2$	$(R/I)_2$	$\{xy, y^2\}$	2
$n = 3$	$(R/I)_3$	$\{y^3\}$	1
$n \geq 4$	$(R/I)_4 = \langle 0 \rangle$	\emptyset	0

(todas estas son bases sobre el campo \mathbb{K}). Por lo cual tenemos las anteriores funciones de Hilbert, con lo que se genera la siguiente serie de Hilbert:

$$\text{Hilbert}_I(t) = 1t^0 + 2t^1 + 2t^2 + 1t^3$$

por lo cual:

$$e(R/I) = h(1) = 6$$

Ejemplo 1.4.2

Considere el anillo $R = \mathbb{K}[x, y, z]$ y al ideal $I = \langle x^2, xy^2, y^3 \rangle$. Tomamemos:

$$M = R/I = \mathbb{K}[x, y, z] / \langle x^2, xy^2, y^3 \rangle$$

se tiene:

Grado	Graduado	Base	Valor Hilbert $H_M(n)$
$n = 0$	$M_0 = \mathbb{K}$	$\{1\}$	1
$n = 1$	M_1	$\{x, y, z\}$	3
$n = 2$	M_2	$\{y^2, z^2, xz, yz, xy\}$	5
$n = 3$	M_3	$\{z^3, xz^2, yz^2, y^2z, xyz, \}$	5
$n = 4$	M_4	$\{z^4, xz^3, yz^3, xyz^2, y^2z^2\}$	5
\vdots	\vdots	\vdots	\vdots
$n = i$	M_i	$\{z^i, xz^{i-1}, yz^{i-1}, xyz^{i-2}, y^2z^{i-2}\}$	5
\vdots	\vdots	\vdots	\vdots

entonces, la serie de Hilbert es infinita y es:

$$Hilbert_M(t) = 1 + 3t + 5t^2 + 5t^3 + 5t^4 + \cdots = \frac{1 + 2t + 2t^2}{1 - t}$$

(ejercicio) por tanto:

$$\deg(M) = e(M) = 1 + 2 + 2 = 5$$

En general, todo lo anterior que hemos hecho se puede definir para cualquier R -módulo graduado.

Proposición 1.4.2 (Propiedad Aditiva de $e(R/I)$)

Si $I = q_1 \cap \cdots \cap q_l$ es una descomposición primaria de I , entonces

$$e(R/I) = \sum_{\text{height}(Q_i)=ht(I)} e(R/q_i)$$

Continuamos ahora con los códigos evaluación. Recordemos que fijamos puntos en el espacio:

$$x = \{p_1, \dots, p_n\} \subseteq \mathbb{P}^{k-1}$$

y formábamos una función $ev_t : R_t \rightarrow \mathbb{K}^n$ dada por:

$$f \mapsto (f(p_1), \dots, f(p_n))$$

hacíamos $\mathcal{C} = ev_t(R_t)$ el código evaluación. Se tiene que ev_t es un mapeo lineal. Se tiene:

$$\begin{aligned} \ker(ev_t) &= \left\{ f \in R_t \mid ev_t(f) = 0 \right\} \\ &= \left\{ f \in R_t \mid f(p_i) = 0, \quad \forall i = 1, \dots, n \right\} \\ &= I(X)_t \end{aligned}$$

siendo $I(X)_t$ el ideal de anulación de todos los polinomios de grado t .

Por el primer teorema de isomorfismo se sigue que:

$$R_t/I(X)_t \cong ev_t(R_t) = \mathcal{C}$$

como todo código lineal es un código evaluación.

Recordemos que para un código \mathcal{C} se tiene que su longitud es $|X| = e(R/I(X))$. En la clase pasada se dijo que:

$$I(X) = I(p_1) \cap \cdots \cap I(p_n)$$

es una descomposición primaria del ideal $I(X)$. Se puede probar que:

- $ht(I(X)) = ht(I(p_i))$ para todo i .

$$\blacksquare \quad e(R/I(p_i)) = 1.$$

en particular, por la propiedad aditiva de $e(R/I)$ se sigue que:

$$e(R/I(X)) = \sum_{ht(I(X))=ht(I(p_i))} e(R/I(p_i)) = n = |X|$$

por lo que tenemos ahora una forma únicamente algebraica para interpretar la longitud de un código.

Para el código \mathcal{C} , se tiene que:

$$\dim_{\mathbb{K}}(\mathcal{C}) = \dim([R/I(X)]_t) = H_{I(X)}(t)$$

considerando el anillo graduado $R/I = \bigoplus_{t \geq 1} (R/I)_t$.

Proposición 1.4.3

La distancia mínima del código $\mathcal{C}(X, t)$ está dada por:

$$d(X)_t = m - \max_{X' \subseteq X} \left\{ |X'| \mid \dim_{\mathbb{K}}(I(X')) > \dim_{\mathbb{K}}(I(X)_t) \right\}$$

Demostración:

Sea $w \in \mathcal{C}(X, t)$ palabra de peso de Hamming $s \geq 1$ que alcanza la distancia mínima, luego w es de la forma:

$$w = (f(p_1), \dots, f(p_m))$$

donde el grado del polinomio es t (todo esto ya hace sentido). En particular, podemos elegir i_1, \dots, i_s tales que

$$f(p_{i_1}), \dots, f(p_{i_s}) \neq 0$$

y, $f(p_j) = 0$ para todo $j \in \{1, \dots, n\} \setminus \{i_1, \dots, i_s\}$. Sea

$$X' = \{p_j \mid j \in \{1, \dots, n\} \setminus \{i_1, \dots, i_s\}\}$$

es claro que $X' \subseteq X$, en particular $I(X)_t \subseteq I(X')_t$, luego

$$\dim_{\mathbb{K}}(I(X')_t) > \dim_{\mathbb{K}}(I(X)_t)$$

y es estricta ya que $f \in I(X')_t \setminus I(X)_t$. Se tiene también que

$$s = m - |X'|$$

por lo que X' es tal que:

$$d(X)_t = m - \max_{X' \subseteq X} \left\{ |X'| \mid \dots \right\}$$

lo cual prueba el resultado. ■

Definición 1.4.6

El **grado inicial** de un ideal homogéneo $\alpha(I(\mathcal{Z}_c)) = \min \{t \mid (I(\mathcal{Z}_c))_t \neq 0\}$. Lo denotaremos por

$$\alpha(\mathcal{Z}) = \alpha(I(\mathcal{Z}_c))$$

Proposición 1.4.4

Sea $1 \leq t \leq \alpha(X) - 1$, entonces

$$d(X)_t + u \geq (k - 1)(\alpha(X) - t)$$

para algún $u \in \{0, \dots, k - 2\}$, con $X \subseteq \mathbb{P}^{k-1}$.

Demostración:

Supongamos que $X = \{p_1, \dots, p_m\}$. Denotemos por:

$$d = d(X)_t \geq 1$$

Sea $X' \subseteq X$ tal que

$$d = m - |X'| \Rightarrow |X'| = m - d$$

(por la proposición anterior). Sea

$$Y = X \setminus X' = \{Q_1, \dots, Q_d\}$$

y sea $f \in I(X')_t$.

$$f(Q_i) \neq 0$$

para todo $j = 1, \dots, d$. Si $d \leq k - 1$, entonces Y están contenido en un hiperplano definido por $V(L)$ (ceros de L), donde L es una forma lineal (esto es que $\deg(L) = 1$) y entonces $f \cdot L \in I(X)$, entonces

$$\alpha(X) \leq t + 1$$

por lo que:

$$\alpha(X) - t \leq 1 \Rightarrow (k - 1)(\alpha(X) - t) \leq k - 1 = d + (k - 1) - d$$

por lo que tomando $u = (k - 1) - d$ se tiene el resultado (esto si $d \leq k - 1$).

Si $d \geq k$, tomemos $\delta = \lceil \frac{d}{k-1} \rceil$, entonces,

$$\delta \cdot (k - 1) = d \cdot u$$

con $u \in \{0, \dots, k - 2\}$, entonces cualquier conjunto Y de $k - 1$ puntos pertenece a un hiperplano. Podemos considerar la unión de δ -hiperplanos:

$$V(L_1), \dots, V(L_\delta) \subseteq \mathbb{P}^{k-1}$$

que contine a los puntos de Y siendo cada L_i una forma lineal de grado uno, entonces

$$L_1 \cdots L_\delta \cdot f \in I(X)$$

por lo que $\alpha(X) \leq \delta + t$. De forma inmediata se sigue que:

$$d + u \geq (k - 1)(\alpha(X) - t)$$

■