Métodos del Álgebra Conmutativa en la Teoría de Códigos

Cristo Daniel Alvarado

13 de noviembre de 2024

Índice general

Capítulo 1

Preeliminares

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:

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

si consideramos la base estándar de $\mathbb{K}^n$, entonces podemos pensar en $\mathcal{C}$ como la imagen de una función lineal lineal $\phi : \mathbb{K}^k \to \mathbb{K}^n$, 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 $v \in \mathcal{K}^n$ es una palabra de $\mathcal{C}$?

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

$$\phi(v) = vG = vw_1 + \cdots + v_k w_k$$

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:

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

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

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

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:

$$d(\mathcal{C}) = \text{mín} \left\{ w(v) \,\middle|\, v \in \mathcal{C} \setminus \{0\} \right\}$$

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 Haming 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:

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

Definición 1.2.2
Un ideal Q de R es **ideal primario de** R, si siempre que $f \cdot g \in Q$ con $f \notin Q$, enotnces $q \in \sqrt{Q}$.

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 $f_1, ..., f_l \in R$ tales que

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

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

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

con $r_i \in R$.

Teorema 1.2.1
Podemos expresar a $I \subseteq R$ como:

$$I = Q_1 \cap \cdots \cap Q_s$$

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 algún libro de álgebra conmutativa. ■

Definición 1.2.5
Dado un ideal $I \subseteq R$, el conjunto formado a partir del teorema anterior:

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

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:

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

denotado por $\text{ht}\,(P)$.

Definición 1.2.7
Sea $I \subseteq R$. Se define la **altura de** I, como:

$$\text{ht}\,(I) = \text{mín}\left\{ht(P)\middle| I \subseteq P\right\}$$

Definición 1.2.8
La **dimensión de Krull de** R es el máximo de $\text{ht}\,(P)$ tal que P es ideal primo de R. En este caso, la dimensión de Krull de R se denota por $\dim(R)$.

Cuando $R = K[x_1, ..., x_n]$, 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,

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

Por el hecho anterior, se tiene que

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

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 $\mathbb{A}^k \setminus \{(0, ..., 0)\}$ y definir una equivalencia sobre este conjunto dada como sigue:

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

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

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

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

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

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 $[a_1, ..., a_k] \in \mathbb{P}^{k-1}$ es un **punto proyectivo**, $a_1, ..., a_k$ 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:

$$[0, ..., 0, 1, a_i, ..., a_k]$$

Definición 1.3.2
Consideremos el anillo $R = K[x_1, ..., x_n]$. 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 anulación** o **ideal de definición de** X, denotado por $I(X)$, es el conjunto de todos los polinomios que se anulan en todos los puntos de X.

Definición 1.3.3
Una **hipersuperficie** es una variedad generada por una sola variedad polinomial.

Definición 1.3.4
La **dimensión** de una variedad proyectiva $X \subseteq \mathbb{P}^{k-1}$ es m si $k-1-m$ es el número más pequeño de hiperplanos genéricos que tienen intersección con X en un conjunto finito de puntos.

El número 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 $Q = [a_1, ..., a_k]$, entonces

$$I(Q) = \langle \left\{ a_i x_j - a_j x_i \middle| 1 \leq i \leq j \leq k \right\} \rangle$$

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

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

para cada punto $P_i \in X$.

Definición 1.3.5
En lo anterior, tenemos que se denomina un **esquema de puntos reducidos**.

Definición 1.3.6
Sea $X = \{P_1, ..., P_m\} \subseteq \mathbb{P}^{k-1}$ un conjunto finito y $n_1, ..., n_m$ enteros positivos. Un **esquema de puntos gordos**, es un esquema de puntos proyectivos con ideal de definición:

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

Observación 1.3.1
En notación de *divisores*, escribimos:

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

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

Definición 1.3.7
Sea $X = \{P_1, ..., P_n\} \subseteq \mathbb{P}^{k-1}$. Si consideramos a G como la matriz $k \times n$ con columnas las coordenadas homogéneas de algún representante de P_i.

Decimos que X están en **posición general** si y sólo 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 $p = [a_1, ..., a_k] \in \mathbb{P}^k$ es un punto, entonces podemos asociar una forma lineal $l_p = a_1x_1 + \cdots + a_kx_k \in R = K[x_1, ..., x_n]$.

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

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:

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

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 incluídos 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:

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

Si la matriz G tiene columnas proporcionales, consideremos:

$$\mathcal{Z}_c = m_1p_q + \cdots + m_sp_s$$

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:

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

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 $p_1, ..., p_4$ no colineales y $p_2, ..., p_4$ 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:

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

Demostración:

Por definición, la distancia de mínima d de código lineal, existe una palabra no cero $v = (v_1, ..., v_n) \in \mathcal{C}$ 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 $\alpha = (\alpha_1, ..., \alpha_k) \in \mathbb{K}^k$ tal que

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

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

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

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

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

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

Pero, como

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

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

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

donde

$$L(x_1, ..., x_k) = \alpha_1 x_1 + \cdots + \alpha_k x_k$$

siendo $P_i = [a_{1i}, ..., a_{ki}] \in \mathbb{P}^{k-1}$ 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:

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

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 $\mathcal{Z}_c = m_1p_1 + \cdots + m_sp_s \subseteq \mathbb{P}^{k-1}$ no todos colineales, si

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

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

Sea $\mathcal{Z} = m_1p_1 + \cdots + m_sp_s \subseteq \mathbb{P}^{k-1}$ 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:

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

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

$$A(X) = (c_1, ..., c_s)$$

y,

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

Teorema 1.3.1
Si $d = d(X)$, entonces

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

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 $hyp(\mathcal{Z}) = 5$. 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 $hyp(X) = 3$.

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

$$\alpha(\mathcal{Z}) = \alpha(I(\mathcal{Z})) = \text{mín}\left\{t \middle| I(\mathcal{Z})_t \neq 0\right\}$$

(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 $X = \{p_1, ..., p_n\} \subseteq \mathbb{P}^{k-1}$ un conjunto finito. Se tiene que

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

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

Definimos un mapeo lineal

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

dado por:

$$ev_t(f) = (f(p_1), ..., f(p_n))$$

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 evaluacón tiene los parámetros básicos que cumplen las igualdades:

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

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

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:

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

Teorema 1.4.2 (**Teorema de Hilbert-Serre**)

$$Hilbert_I(t) = \frac{h(t)}{(1-t)^s}$$

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:

$$R/I = \bigoplus_{n \geq 1} (R/I)_n$$

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:

$$Hilbert_I(t) = 1t^0 + 2t^1 + 2t^3 + 1t^3$$

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

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

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

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

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

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

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

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

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 evaluacíon.

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.

- $e(R/I(p_i)) = 1$.

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 lóngitud de un código.

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

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

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:

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

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:

$$w = (f(p_1), ..., f(p_m))$$

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

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

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

$$X' = \left\{p_j \,\middle|\, j \in \{1, ..., n\} \setminus \{i_1, ..., i_s\}\right\}$$

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:

$$d(X)_t = m - \max_{X'\subseteq X}\left\{|X'| \,\middle|\, ...\right\}$$

lo cual prueba el resultado. ■

Definición 1.4.6
El **grado inicial** de un ideal homogéneo $\alpha(I(\mathcal{Z}_c)) = \text{mín}\left\{t \middle| (I(\mathcal{Z}_c))_t \neq 0\right\}$. 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 $u \in \{0, ..., k-2\}$, con $X \subseteq \mathbb{P}^{k-1}$.

Demostración:

Supongamos que $X = \{p_1, ..., p_m\}$. 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

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

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

$$f(Q_i) \neq 0$$

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

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

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:

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

■

Ejemplo 1.4.3

Sea $\mathcal{C}$ un código con matriz generadora

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

el esquema de puntos (reducido/gordos) está dado por:

$$X = \{p_1 = [1,0,0], p_2 = [0,1,0], p_3 = [0,0,1], p_4 = [1,-1,0], p_5 = [1,0,-1]\} \subseteq \mathbb{P}^2$$

Se tiene el ideal de definición:

$$\begin{aligned} I(X) &= I(p_1) \cap \cdots \cap I(p_5) \\ &= \langle x_2, x_3 \rangle \cap \langle x_1, x_3 \rangle \cap \langle x_1, x_2 \rangle \cap \langle x_1 + x_2, x_3 \rangle \cap \langle x_1 + x_3, x_2 \rangle \end{aligned}$$

(nomás basta ver como son los puntos para ver como se generan los ideales). Notemos que $p_1, p_2, p_4 \in V(x_3)$ y $p_1, p_3, p_5 \in V(x_2)$. Por ende, $x_2 x_3 \in I(X)$.

Así, $\alpha(X) \leq 2$. Afirmamos que $\alpha(X) = 2$ ya que no hay una forma lineal que se vaya a anular en todos.

$$hyp(X) = 3$$

Por lo cual,

$$d(X) = 5 - hyp(X) = 5 - 3 = 2$$

Si $t = 1$ con $u = 0$, tenemos que:

$$\begin{aligned} d(X)_1 + u &= 2 + 0 \\ &= (3-1)(2-1) \\ &= (k-1)(\alpha(X) - t) \end{aligned}$$

para $t = 2$, necesitamos exhibir un polinomio de grado 2 que anule a la mayor cantidad de puntos de X, pero no a todos, elegimos x_1x_3 ya que $p_1, p_2, p_3, p_4 \in V(x_1x_3)$. En este caso,

$$d(X)_t = |X| - \max_{X' \subseteq X} \left\{ |X'| \,\middle|\, \cdots \right\}$$

note que $X' = \{p_1, ..., p_4\}$ y $p_5 \notin V(x_1x_3)$, por lo que

$$d(X)_2 = 5 - 4 = 1$$

(esto por el hecho de que $\alpha(X) = 2$).

Corolario 1.4.1
Sea $X \subseteq \mathbb{P}^{k-1}$ con $k \geq 3$ es un conjunto de n puntos reducidos no todos contenidos en un mismo hiperplano. Sea $t \geq 1$ un entero, entonces:

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

Demostración:
No se verá. ■

Corolario 1.4.2
Sea $X \subseteq \mathbb{P}^{k-1}$ con $k \geq 3$ es un conjunto de n puntos reducidos no todos contenidos en un mismo hiperplano. Sea $d(X)$ la distancia mínima del esquema X. Entonces,

$$d(X) = \alpha(X) - 1 \iff hyp(X) = n - 1 \iff d = 1$$

Demostración:
Si $t = 1$, del corolario anteriror tenemos que

$$d(X)_t \geq (k-1)(\alpha(X) - 2) + 1$$

- Si $d(X) = \alpha(X) - 1$, se tiene que:

$$\begin{aligned} \alpha(X) - 1 &\geq (k-1)(\alpha(X) - 2) + 1 \\ &\Rightarrow 0 \geq (k-1)(\alpha(X) - 2) + 2 - \alpha(X) \\ &\Rightarrow 0 \geq (k-2)(\alpha(X) - 2) \end{aligned}$$

como $k \geq 3$, entonces $\alpha(X) - 2 \leq 0$, luego al tenerse que el grado inicial es un número positivo, debe tenerse que $1 \leq \alpha(X) \leq 2$, pero como no todos están en un mismo hiperplano, se sigue

que $\alpha(X) = 2$ (en caso que fuese 1, habría una forma lineal que se anulase en todos, luego todos están en un mismo hiperplano, cosa que no puede suceder).

Luego, $d(X) = \alpha(X) - 1 = 1$, lo cual implica que:

$$hyp(X) = n - d(X) = n - 1$$

- Si $d(X) = 1$, entonces del corolario anterior se sigue que:

$$\begin{aligned} 1 &\leq (k-1)(\alpha(X) - 2) + 1 \\ \Rightarrow 0 &\geq (k-1)(\alpha(X) - 2) \end{aligned}$$

como en el caso anterior, se sigue que $\alpha(X) = 2$. Luego $d(X) = 2 - 1 = \alpha(X) - 1 \iff hyp(X) = n - 1$.

■

Todas estás preguntas las hemos respondido en un esquema de puntos reducidos, pero ¿qué sucede en el caso de esquema de puntos gordos (es decir, con multiplicidad)?

1.5. El caso de puntos gordos

Sea $\mathcal{Z} = m_1 p_1 + \cdots + m_s p_s$ y $m_1, ..., m_s \geq 1$ es un esquema de puntos gordos no todos contenidos en un hiperplano y además,

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

sea $X = supp(\mathcal{Z}) = \{p_1, ..., p_s\}$. Denotemos por

$$m = m(\mathcal{Z}) = \text{máx}\{m_1, ..., m_s\}$$

Teorema 1.5.1
Sea $\mathcal{Z}$ un esquema de puntos gordos, entonces

$$d(\mathcal{Z}) \geq \alpha(\mathcal{Z}) - m$$

Demostración:
No se hará. ■

Ahora hablaremos de más parámetros sobre los códigos, en particular de lo siguiente:

- Pesos generalizados de Hamming.
- Códigos evaluación.
- Como una función sobre ideales graduados/función de Hilbert.

Definición 1.5.1
Sea $\mathcal{C} \subseteq \mathbb{K}^n$ un $[n, k, d]$ un código lineal. Considere $\mathcal{D} \subseteq \mathcal{C}$ un subcódigo (subespacio) de $\mathcal{C}$.

El **soporte de** $\mathcal{D}$ se define por:

$$supp(\mathcal{D}) = \left\{ i \in \{1, ..., n\} \,\middle|\, \exists (x_1, ..., x_n) \in D \text{ con } x_i \neq 0 \right\}$$

y sea $m(D) = |supp(D)|$.

Observación 1.5.1
Para $c = (c_1, ..., c_n) \in \mathcal{C}$:

$$supp(c) = \left\{ i \in \{1, ..., n\} \,\middle|\, c_i \neq 0 \right\} = w(c)$$

recordemos que esto es el peso de Hamming de una palabra.

Definición 1.5.2
Sea $\mathcal{C} \subseteq \mathbb{K}^n$ un $[n, k, d]$ un código lineal. Para $r \in \{1, ..., k\}$, definimos el **r-ésimo peso generalizado de Hamming de $\mathcal{C}$** por:

$$d_r(\mathcal{C}) = \min_{\mathcal{D} \subseteq \mathcal{C}} \left\{ m(\mathcal{D}) \,\middle|\, \dim_{\mathbb{K}}(\mathcal{D}) = r \right\}$$

Observación 1.5.2
Veamos quién es uno por uno:

$$d_1(\mathcal{C}) = \min_{\mathcal{D} \subseteq \mathcal{C}} \left\{ m(\mathcal{D}) \,\middle|\, \dim_{\mathbb{K}}(\mathcal{D}) = 1 \right\}$$

entonces, $\mathcal{D}$ es un subespacio de $\mathcal{C}$ generado por un único elemento, digamos $D = \mathcal{L}(c)$ con $c \in \mathcal{C}$. Por lo que:

$$\begin{aligned} d_1(\mathcal{C}) &= \min_{c \in \mathcal{C}} \left\{ w(c) \,\middle|\, c \in \mathcal{C} \setminus \{0\} \right\} \\ &= d(\mathcal{C}) \end{aligned}$$

es decir que recuperamos el peso de Hamming original.

Consideremos ahora $X0\,\{p_1, ..., p_m\} \subseteq \mathbb{P}^{k-1}$ y tomemos el anillo de polinomios $R = \mathbb{K}[x_1, ..., x_m] = \bigoplus_{t \geq 1} R_t$ con la graduación estándar.

Se definió la función evaluacíon:

$$\begin{aligned} ev_t : R_t &\to \mathbb{K}^m \\ f &\mapsto (f(p_1), ..., f(p_m)) \end{aligned}$$

se tomó el código evaluación con parámetro t por $\mathcal{C}(X, t) = ev_t(R_t)$. Se sabe además que:

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

El peso de Hamming de una palabra c cuenta el número de entradas no cero de una palabra, lo cual lo podemos ver coom elnúmero de no raíces de un polinomio f en X, el cual es

$$|X| - |\{\text{raíces de } f\}| = |X| - |V_X(f)|$$

entonces,

$$\begin{aligned} d(\mathcal{C}) &= \min \left\{ |X| - |V_X(f)| \,\middle|\, f \in \mathbb{K}[x_1, ..., x_m] \text{ es tal que } f \notin I(X)_t \right\} \\ &= \deg(R_t / I(X)_t) - \max \left\{ |V_X(f)| \,\middle|\, f \notin I(X)_t \right\} \end{aligned}$$

¿Cómo calcular la cardinalidad de $|V_X(f)|$ donde f es un polinomio homogéneo de grado t y $X \subseteq \mathbb{P}^{k-1}$?

En 2018 se encontró lo siguiente: bajo las condiciones anteriores:

$$|V_X(f)| = \begin{cases} \deg\left(R/(I(X), f)\right) & \text{si} \quad (I(X) : f) \neq I(X) \\ 0 & \text{si} \quad (I(X) : f) = I(X) \end{cases}$$

el ideal $(I : f)$ es llamado **ideal colon/cociente**, formado por:

$$(I : f) = \left\{ h \in R \middle| hf \in I \right\}$$

por lo cual,

$$d(\mathcal{C}) = \deg(R_t/I(X)_t) - \text{máx}\left\{ \deg(R_t/(I(X)_t : f)) \middle| (I(X) : f) \neq I(X) \right\}$$

Ahora, para los pesos generalizados. En el caso en que $r = 1$, solamente necesitamos un polinomio. Considere el conjunto de polinomios:

$$\mathcal{F}_{t,r} = \left\{ \{f_1, ..., f_r\} \subseteq R_t \middle| ((I(X)_t : \langle f_1, ..., f_r \rangle)) \neq I(X)_t \right\}$$

donde ahora el ideal colon/cociente es:

$$(I : J) = \left\{ h \in R \middle| hJ \subseteq I \right\}$$

Con lo cual, la forma de calcular el r-ésimo grado generalizado se convierte en computar:

$$d_r(\mathcal{C}) = \deg\left(R_t/I(X)_t\right) - \text{máx}\left\{ \deg\left(R_t/(I(X)_t, f_1, ..., f_r)\right) \middle| \{f_1, ..., f_r\} \in \mathcal{F}_{t,r} \neq \emptyset \right\}$$

1.6. Ejercicios

Ejercicio 1.6.1
Muestre que para $f \notin I$:

$$(I : f) \neq I \iff f \text{ es divisor de cero de } R/I$$

Demostración:
$\Rightarrow$) : Como $(I : f) \neq I$ entonces existe $g \in (I : f)$ tal que $gf \in I$, luego $(I + g)(I + f) = I$ con $g, f \notin I$, luego f es divisor de cero en R/I. $\Leftarrow$) : Suponga que f es divisor de cero de R/I, entonces existe $g \in R \setminus I$ tal que

$$(I + g)(I + f) = I + gf = I$$

luego, $g \in (I : f)$, por lo que $(I : f) \neq I$. ■

Ejercicio 1.6.2
Si $\mathcal{C}$ es un $[n, k]$ código lineal, y H su matriz de paridad, entonces $d(\mathcal{C}) = d$ si y sólo si d es el entero máximo tal que cualesquiera $d - 1$ columnas de H son l.i.

Demostración:
$\Rightarrow$) : Suponga que $d(\mathcal{C}) = d$. Considere $d-1$ columnas de H, obtenida a partir de la función lineal $H : \mathbb{K}^k \to \mathbb{K}^n$ Sea $c \in \mathbb{K}^n$ tal que $d(\mathcal{C}) = w(c) = d$. Entonces,

$$cH = 0$$

(viendo a la función lineal $H : \mathbb{K}^k \to \mathbb{K}^n$ y al código como el kernel de H). Como a lo más c tiene exactamente d entradas no cero, entonces existen $c_1, c_2, ..., c_d \in \mathbb{K} \setminus \{0\}$ y vectores columna de H, $w_{i_1}, ..., w_{i_d}$ tales que

$$c_1 w_{i_1} + \cdots + c_d w_{i_d} = 0$$

para cualquier vector en $\mathcal{C}$. Por ende, todo espacio generado por más de $d - 1$ vectores es l.d. y no puede suceder que haya $d-1$ vectores l.d. ya que en tal caso podremos encontrar un elemento $c \in \mathbb{K}^n$ tal que

$$cH = 0$$

con $c \in \mathcal{C}$ (pues $\mathcal{C}$ es el subespacio del kernel de $\mathcal{C}$). Por tanto, $d - 1$ columnas de H son l.d.

La vuelta es inmediata comprendiendo lo anterior y procediendo por contradicción. (el peso de Hamming nunca va a poder ser menor que $d - 1$ ya que siempre va a haber $d - 1$ vectores columna l.i. de la matriz H). ■

Ejercicio 1.6.3
Sea $\mathcal{C}$ un $[n, k, d]$ código lineal. Entonces:

$$d \leq n - k + 1$$

Demostración:
Recordemos que

$$d(\mathcal{C}) = \text{mín}\left\{ w(c) \middle| c \in \mathcal{C} \setminus \{0\} \right\}$$

a lo más, $d(\mathcal{C})$ puede tener n entradas cero, esto es que:

$$d(\mathcal{C}) \leq n$$

acortemos más la distancia. Como $\dim_{\mathbb{K}}(\mathcal{C}) = k$, entonces a lo menos, un vector $c \in \mathcal{C}$ no cero tiene $k-1$ entradas no cero, por lo que

$$w(c) \leq n - (k-1) = n - k + 1$$

así que,

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

■

Ejercicio 1.6.4
$\mathcal{C}$ es degenerado si y sólo si $d(\mathcal{C}^{\perp}) = 1$.

Demostración:
Suponga que $\mathcal{C}$ es degenerado, entonces una columna de la una matriz generadora es 0, digamos la entrada i-ésima, luego el vector: ■

Ejercicio 1.6.5
Los pesos generalizados se relacionan de la siguiente forma:

$$d_1(\mathcal{C}) < d_2(\mathcal{C}) < \cdots < d_k(\mathcal{C}) \leq n$$

Demostración:

■

Ejercicio 1.6.6
Calcular la descomposición primaria del ideal:

$$I = \langle x_1x_2, x_2x_3, x_2x_5, x_4x_5, x_5x_6 \rangle$$

Veamos que:

$$I =$$