Métodos del Álgebra Conmutativa en la Teoría de Códigos

Cristo Daniel Alvarado

11 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
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 1.2.2
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 1.2.3
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 Hungerford. ■

Definición 1.2.4
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 1.2.5
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 $ht(P)$.

Definición 1.2.6
Sea $I \subseteq R$. Se define la **altura de** I, como:

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

Definición 1.2.7
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 $R = K[x_1, ..., x_n]$, 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 $l_p = a_1 x_1 + \cdots + a_k x_k \in R = K[x_1, ..., x_n]$.

Inversamente, para cualquier forma lineal $l = b_1 x_1 + \cdots + b_k x_k$ 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:

$$\mathcal{Z}_c = m_1 p_q + \cdots + m_s p_s$$

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:

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

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

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