UNIVERSIDAD MICHOACANA DE SAN NICOLÁS DE HIDALGO

INSTITUTO DE FÍSICA Y MATEMÁTICAS

SOBRE LOS PARÁMETROS DE LOS CÓDIGOS Y LOS ANILLOS DE COX DE SUPERFICIES RACIONALES

TESIS PARA OBTENER EL GRADO DE

MAESTRA EN CS. MATEMÁTICAS

PRESENTA

BRENDA LETICIA DE LA ROSA NAVARRO

ASESOR

DR. MUSTAPHA LAHYANE

CO-ASESOR

DR. ISRAEL MORENO MEJÍA

AGOSTO, 2009

Índice General

Agradecimientos

A toda mi familia por su apoyo incondicional.

A mis asesores Mustapha Lahyane e Israel Moreno, por todas sus enseñanzas durante mi trabajo de tesis.

A los miembros de mi comité: Dr. Abel Castorena, Dr. Osvaldo Osuna y Dr. Elmar Wagner, por sus observaciones y recomendaciones.

A mis amigos por toda su ayuda brindada desde que llegue a Morelia.

Introducción General

Este trabajo se consta de dos partes. La primera parte tiene como objetivo construir códigos utilizando las geometrías de superficies racionales lisas, en esta parte utilizaremos la superficie que esta dada por la explosión del plano proyectivo de puntos que estan sobre una recta, nuestra contribución original es el Teorema 68.

En la segunda parte daremos la teoría de anillos de Cox ofreciendo una conjetura acerca de la finitud de estos anillos.

Para mayor información del contenido de las dos partes ver las introducciones de cada una.

Parte I

Sobre los Parámetros de los Códigos

Introducción

La Teoría de Códigos se encarga de estudiar métodos para transmitir información eficaz y precisa de un lugar a otro. Esta teoría se ha desarrollado para distintas aplicaciones, algunas de ellas son la utilización de un celular, transmisión de información financiera a través de lineas telefónicas, transmitir información de una computadora a otra, entre otros. Esto puede llevarse a cabo mediante una codificación de la información que se requiere enviar.

La Teoría de Códigos es una parte de la Teoría de la Información igual que la Criptografía. La Teoría de Códigos complementa a la Criptografía, ya que el interés de esta ultima es codificar la información que se desea enviar, de tal manera que si alguien intersecta esta información no la pueda leer. Una vez que la criptografía hace su trabajo interviene la Teoría de Códigos.

Uno de los principales problemas a los que un código se enfrenta son los errores. Hay códigos llamados detectores de errores, estos permiten detectar cambios en un mensaje. También existen códigos llamados correctores de errores, los cuales pueden corregir los errores ocurridos.

El medio por el cual la información es transmitida se llama canal. Algunos

ejemplos de canales pueden ser los satélites, lineas telefónicas, fibras ópticas y cualquier otro medio físico por donde se pueda enviar información. A la hora de que la información pasa por el canal pueden ocurrir errores a causa de algún tipo de interferencia en el canal, esta interferencia es llamada ruido.

Debido al ruido originado en el canal, la información se transforma agregando cierta redundancia, a esto se le llama codificación. Luego el emisor envía la información codificada a través del canal. En base a esta codificación el receptor puede detectar, y posiblemente corregir, los errores producidos y finalmente obtener la información original, a este proceso se le llama descodificación.

El objetivo principal de la Teoría de Códigos es construir códigos con la propiedad de detectar y corregir errores originados durante la transmisión de información por ruido en el canal. El siguiente diagrama muestra una idea del modelo general de un sistema de transmisión de información con una protección contra los errores.

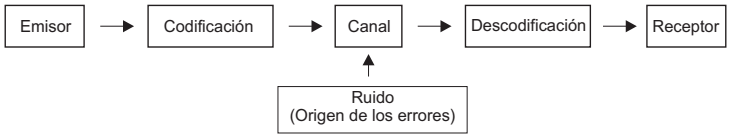


Figura 1: Esquema de transmisión de información codificada con protección.

Veamos un ejemplo para visualizar el esquema. Supongamos que deseamos recargar nuestro celular, para esto llamamos a atención a clientes de nuestra compañía de celular, entonces escuchamos una grabación que dice lo siguiente: si desea recargar presione 1, si desea escuchar su saldo presione 2,

si desea hablar con un operador presione 3, si desea escuchar nuevamente el menú presione 4. Los mensajes posible a enviar son recargar, saldo, operador y menú, y están codificados como 1, 2, 3 y 4, respectivamente. En este caso, el canal es un satélite.

Figura 2: Proceso de recarga de celular.

Puesto que Rebeca desea recargar su celular presiona el 2, entonces ella envia el mensaje de recargar codificado como 2, este mensaje pasa por el satélite, luego el receptor recibe la información, en este caso es Loco-cel, como Loco-cel sabe que 2 significa recarga, entonces descodifica el mensaje y finalmente Rebeca tiene lo que queria. En este ejemplo considere que en el satélite no ocurre ruido, pero esto no sucede, en la practica siempre ocurren errores en el canal, para solucionar esto se construyen códigos que puedan detectar y corregir errores. A continuación se procedera a dar la descripción del contenido de esta parte de la tesis.

Esta parte del trabajo se divide en 6 capítulos:

Capítulo 1: Se presentan nociones generales para el estudio de los parámetros de un código.

Capítulo 2: En este capítulo se define la noción de un código detector y corrector de errores.

Capítulo 3: Se definen los conceptos generales para estudiar un código lineal, además se muestra la manera de generarlos a partir de una matriz con renglones linealmente independientes, esta matriz es llamada matriz generadora. Además se presenta un método para descodificar un código lineal.

Capítulo 4: Se muestra que los parámetros de un código no son arbitrarios, están restringidos por ciertas cotas, en este trabajo la cota de interés es la cota de Singleton.

Capítulo 5: Se definen conceptos generales para construir códigos cíclicos. Se muestra que un código cíclico puede ser generado a partir de un único polinomio mónico en $\mathbb{F}[x]$, donde $\mathbb{F}$ es un campo finito.

Capítulo 6: En este capítulo se presentan conceptos fundamentales, por ejemplo la explosión del plano afín y presentamos nuestro resultado original (ver Teorema 68), donde hemos construido códigos utilizando la geometría de las superficies racionales obtenidas como explosión del plano proyectivo en un número finito de puntos de una recta.

Capítulo 1

Nociones Básicas

Introducción

1.1 Códigos

Se tomará un conjunto finito $\mathbb{F}$, el cual será llamado *alfabeto*. Los elementos del alfabeto $\mathbb{F}$ se llamarán *símbolos* o *dígitos* (cuando los elementos son números). Se dirá que una *palabra* es una secuencia finita de símbolos del alfabeto $\mathbb{F}$. Luego, la *longitud* de una palabra está dada por el número de símbolos o dígitos que forman dicha palabra.

Definición 1 *Sea* $\mathbb{F}$ *un alfabeto. Un* código C *es un conjunto finito de palabras sobre* $\mathbb{F}$*. Los elementos de* C *son llamados* palabras código*. El* tamaño T *del código* C *es el número de palabras código de* C*, es decir* $T = |C|$*. Por otro lado, si* $|\mathbb{F}| = q$ *se dirá que* C *es un* código $q-ario$*, en el caso*

cuando $q = 2$ *el código* C *será llamado* código binario.

Cuando todas las palabras de un código tienen la misma longitud n , este código será llamado *código bloque de longitud* n, de otra manera se tendrá que el código es un *código de longitud variable*. Los enteros n y T serán llamados unos *parámetros del código*.

Observación 2 *Si la palabra* x *tiene longitud* n $(x = x_1x_2 \cdots x_n)$*, es equivalente decir que* $x \in \mathbb{F}^n$*. Entonces un código bloque de longitud* n *es un subconjunto de* $\mathbb{F}^n$*.*

Si C es un código bloque de longitud n y tamaño T, se dirá que es un $(n, T) - código$, donde n y T son parámetros del código.

1.2 Tasa de información

Definición 3 *Sea* C *un* $(n, T) - código\ q - ario$*, entonces el porcentaje de símbolos que guardan la información del mensaje original sobre el total de símbolos del mensaje transmitido se conoce como* tasa de información *dada por*

$$R(C) = \frac{\log_q(T)}{n}.$$

Obviamente $R(C)$ *es un elemento del intervalo* $[0, 1]$.

1.3 Distancia de Hamming

Para poder comparar una palabra con otra se va a definir una distancia conocida como distancia de Hamming. La importancia de definir una distancia es el poder medir la cantidad de errores que ocurren durante la transmisión de información. En el siguiente capítulo, se muestra la capacidad que tiene un código para detectar y corregir errors. Esta capacidad esta dada en relación con la distancia que se va a definir a continuación.

Definición 4 *La* distancia de Hamming *está dada de la siguiente manera:*

$$\delta : \mathbb{F}^n \times \mathbb{F}^n \longrightarrow \mathbb{R}^+$$

$$\delta((x_1, ..., x_n), (y_1, ..., y_n)) = |\{i \mid x_i \neq y_i, \ con \ i \in \{1, ..., n\}\}| .$$

De esta definición se puede observar que $0 \leq d(x, y) \leq n$ para todo $(x, y) \in \mathbb{F}^n \times \mathbb{F}^n$.

Ejemplo 5 *Si tenemos las palabras* 010301 *y* 103011 *en* $\mathbb{F}_4^6$*, entonces su distancia es* $\delta(010301, 103011) = 5$.

En la siguiente proposición se demostrará que esta distancia da una estructura de espacio métrico al conjunto $\mathbb{F}^n$.

Proposición 6 $(\mathbb{F}^n, \delta)$ *es un espacio métrico, donde* δ *es la distancia de Hamming.*

Demostración. Veamos que δ satisface las tres propiedades de una métrica.

(i) Inmediatamente de la definición de δ se tiene que $\delta(x,y) \geq 0$ para todo $(x,y) \in \mathbb{F}^n \times \mathbb{F}^n$. Por otro lado, se tiene que $\delta(x,y) = 0$ si y sólo si

$$\{i \mid x_i \neq y_i, \ con\ i \in \{1,...,n\}\} = \varnothing,$$

si y sólo si $x_i = y_i$ para todo $i \in \{1,...,n\}$. Por lo tanto $x = y$.

(ii) Simetría: Sea $(x,y) \in \mathbb{F}^n \times \mathbb{F}^n$, por definición

$$\begin{aligned} \delta(x,y) &= |\{i \mid x_i \neq y_i, \ con\ i \in \{1,...,n\}\}| \\ &= |\{i \mid y_i \neq x_i, \ con\ i \in \{1,...,n\}\}| = \delta(y,x). \end{aligned}$$

(iii) Desigualdad del Triángulo: Sean $x, y, z \in \mathbb{F}^n$. Consideremos los conjuntos

$$A_1 = \{i \mid x_i \neq y_i, con\ i \in \{1,...,n\}\},$$

$$A_2 = \{i \mid x_i \neq y_i\ y\ x_i \neq z_i, con\ i \in \{1,...,n\}\},$$

$$A_3 = \{i \mid x_i \neq y_i\ y\ x_i = z_i, con\ i \in \{1,...,n\}\}.$$

Luego, se tiene que A_1 es la unión disjunta de $A_2 \cup A_3$, entonces $\delta(x,y) = |A_1| = |A_2| + |A_3|$. Por otro lado, $|A_2| \leq \delta(x,z)$ y $|A_3| \leq \delta(z,y)$. Por lo tanto, $\delta(x,y) \leq \delta(x,z) + \delta(z,y)$.

■

Ahora se define otro parámetro del código que se llamará distancia mínima de un código C.

Definición 7 *Sea C un código, la* distancia mínima *de C se define como*

$$d = \delta(C) = \min\{\delta(x,y) \mid x, y \in C, \ x \neq y\}. \tag{1.1}$$

Ejemplo 8 *Si tenemos el código*

$$C = \{0123, 2223, 1133, 2201\},$$

su distancia mínima es $d = 2$.

La distancia mínima se toma mayor que cero ya que más adelante se mostrará un hecho que permite detectar a un código un cierto número de errores, ocurridos durante la transmisión de información, en base a la distancia mínima.

Así definimos los parámetros del código C como la longitud n, tamaño T y distancia mínima d, y códificamos esta información diciendo que C es un $(n, T, d) - código$.

Como $\mathbb{F}^n$ tiene estructura de espacio métrico se puede hablar de la noción de bolas.

Definición 9 *Sean* $x \in \mathbb{F}^n$ *y* $r \geq 0$, *se define la* bola *de radio* r *centrada en* x *como*

$$B(x, r) = \{y \in \mathbb{F}^n \mid \delta(x, y) \leq r\}.$$

Estas definiciones ayudarán a que cuando se recibe una palabra y que no está en el código, se puede descodificar por la palabra código más cercana a y.

Lema 10 *Sea* C *un código con distancia mínima* $d = 2t + 1$ *ó* $d = 2t + 2$, *entonces*

$$B(a, t) \cap B(b, t) = \varnothing,$$

para cualesquiera $a, b \in C$ *y* $a \neq b$.

Demostración. Se proseguirá por contradicción. Sean $a, b \in C$ con $a \neq b$. Supongamos que existe $z \in B(a,t) \cap B(b,t)$, entonces

$$\delta(a,b) \leq \delta(a,z) + \delta(z,b) \leq t + t = 2t < d,$$

lo cual contradice que d es la distancia mínima de C. ■

Para ahorrar casos, en lugar de considerar $d = 2t+1$ ó $d = 2t+2$ se tomará $t = \left\lfloor \frac{d-1}{2} \right\rfloor$, se puede ver de forma fácil que son equivalentes.

Capítulo 2

Detección y Corrección de Errores de un Código

Consideraremos al alfabero $\mathbb{F}$ como un campo finito de q elementos. En este capítulo veremos que la distancia mínima da una cota superior para el número de errores que puede detectar y corregir un código (ver [3] y [7]).

2.1 Detección de errores

Para empezar a hablar de como un código puede detectar errores, primero supongamos que tenemos un $(n, T, d) - \textit{código } C$. Ahora, cuando se envia una palabra código $x \in C$ y se recibe una palabra $z \in \mathbb{F}^n$, se dice que C puede detectar errores si $z \notin C$. Luego, se va a decir que ocurrieron s errores en la transmisión si $\delta(x, z) = s$. Por otro lado, se llamará patrón de error a la palabra $e \in \mathbb{F}^n$, donde $e = z - x$.

Entonces, se dirá que C detectará el patrón de error e si y sólo si $e+x \notin C$ para todo $x \in C$.

Veamos algunos ejemplos para visualizar lo anterior.

Ejemplo 11 *Consideremos el código*

$$C = \{000000, 000111, 111000, 111111\},$$

donde $\mathbb{F} = \mathbb{F}_2$, *y el cual es un* $(6, 4, 3) -$ *código. Supongamos que se envia la palabra código* 111111 *y se recibe la palabra* $111011 \in \mathbb{F}^6$, *puesto que* $111011 \notin C$ *se tiene que* C *puede detectar errores, además tenemos que ocurrio un error, ya que* $d\,(111111, 111011) = 1$. *Luego el patrón de error es* $e = 000100$. *Como* $e + x \notin C$ *para cualquier palabra código* x *de* C, *entonces* C *puede detectar el patrón de error* e.

Ejemplo 12 *Si tomamos un código* C *igual al conjunto* $\mathbb{F}^n$, *¿puede este código detectar algún patrón de error?. La respuesta es no, ya que si se envia la palabra código* $aa \cdots aa \in C$, *suponiendo que solo ocurre un error, y se recibe* $ba \cdots aa$, *esta palabra también pertene a* C. *Por lo tanto* C *no puede detectar errores.*

Ejemplo 13 *Sean* $\mathbb{F} = \mathbb{F}_4$ *y* $C = \{0011, 1122, 2233\}$. *Ahora consideremos los patrones de errores* $e_1 = 1100$ *y* $e_2 = 2222$, *se tiene que* C *puede detectar* e_1, *pero no a* e_2, *ya que* $e_2 + 0011 = 2233 \in C$.

Definición 14 *Se dice que un código* detecta *hasta* r *errores si al enviar palabras código ocurren* s *errores durante la transmisión, con* $1 \leq s \leq r$, *y la*

palabra recibida no es una palabra código. Un código detecta exactamente s errores si no detecta $s+1$ errores.

Ejemplo 15 *Consideremos el código*

$$C = \{0000, 1100, 0011, 1111\} \subset \mathbb{F}_2^4,$$

este código puede detectar un error, ya que si al enviar 0000 *se recibe* 1000*, la palabra recibida no pertenece al código y la* $\min\{\delta(1000, x) \mid x \in C\} = 1$*. Por otro lado, si ocurren dos errores y se recibe* 1100*, el código no puede detectar que ocurren dos errores, ya que* $1100 \in C$*. Por lo tanto, C detecta un error.*

Teorema 16 *Sea $C \subset \mathbb{F}^n$ un código con distancia mínima d, entonces C puede detectar a lo más $d-1$ errores.*

Demostración. Si suponemos que se envia la palabra código $x \in C$, entonces la bola $B(x, d-1)$ contiene todas las posibles palabras recibidas en las que ocurren a lo mas $d-1$ errores durante la transmisión. Luego, la bola $B(x, d-1)$ no contiene otras palabras código, ya que la distancia mínima entre cada palabra código es d. De esto, si no ocurren más de $d-1$ errores la palabra recibida no es una palabra código. Por lo tanto C puede detectar a lo más $d-1$ errores. ■

Ejemplo 17 *Si tenemos el código*

$$C = \{00000, 11110, 01111, 10001\} \subset \mathbb{F}_2^5,$$

su distancia mínima es $d = 2$. Por el teorema anterior C detecta un error.

2.2 Corrección de errores

Si se envia un palabra código x de un código $C \subseteq \mathbb{F}^n$ y se recibe una palabra z de $\mathbb{F}^n$ teniendo como resultado que el patrón de error $e = z - x$, entonces se puede concluir que x fue la palabra enviada por ser z la palabra más cercana a x que a cualquier otra palabra código. Si esto sucede cada vez que una palabra código es transmitida, entonces podemos decir que C corrige el patrón de error e.

Definición 18 *Un código C* corrige *s errores si corrige todos los patrones de error de distancia a lo más s y no corrige al menos un patrón de error de distancia $s+1$.*

Ejemplo 19 *Si consideramos el código*

$$C = \{000, 111\} \subseteq \mathbb{F}_2^6,$$

si enviamos la palabra código 000 *y ocurre un error durante la transmisión, entonces las posibles palabras recibidas son* $\{100, 010, 001\}$*, puesto que estas palabras son más cercanas a la palabra código* 000*, se tiene que C puede corregir un error y descodificar como* 000*. De manera analoga, si al enviar la palabra código* 111 *ocurre un error, entonces el código puede corregir el error y obtener finalmente la palabra enviada. Ahora si suponemos que ocurren dos errores, por ejemplo si se envia* 000 *y se recibe* 101*, el código decodificaría a* 101 *como* 111*, por ser* 101 *más cercana a* 111*. Por lo tanto C solo puede corregir un error.*

Teorema 20 *Sea $C \subseteq \mathbb{F}^n$ un código con distancia mínima d, entonces C puede corregir $t = \left\lfloor \frac{d-1}{2} \right\rfloor$.*

Demostración. Si al enviar una palabra código se recibe la palabra $z \in \mathbb{F}^n$, y ocurren a lo más t errores, entonces por el Lema 10 el error puede ser corregido y z se descodifica por la palabra código $c \in C$ tal que $z \in B(c,t)$.

■

Ejemplo 21 *Se tiene que el código*

$$C = \{000000, 101001, 111111\}$$

tiene distancia mínima $d = 3$, entonce C puede corregir $t = 1$ error.

Capítulo 3

Códigos Lineales

De ahora en adelante se tomará al alfabeto $\mathbb{F}$ como un campo finito de q elementos, entonces $\mathbb{F}^n$ tiene una estructura de espacio vectorial sobre el campo $\mathbb{F}$.

3.1 Código lineal

Definición 22 *Un* código lineal C *se define como un subespacio vectorial de* $\mathbb{F}^n$ *de dimensión* $k \leq n$.

Ahora se tiene que el tamaño de C es $T = q^k$, de esto en lugar de tomar el tamaño del código lineal como parámetro se considerará su dimensión. Entonces un código lineal será codificado como $(n, k, d) - \textit{código lineal}$. Los enteros $n,\ k$ y d serán llamados los parámetros de un código lineal C. Además, en este caso la tasa de información de C será exactamente $\frac{k}{n}$.

De otro lado, como $\mathbb{F}^n$ es un espacio vectorial, podemos definir la función w llamada peso de Hamming.

Definición 23 *El* peso de Hamming *está dado por*

$$w : \mathbb{F}^n \longrightarrow \mathbb{R}^+,$$

donde

$$w(x_1, \ldots, x_n) = |\{i \mid x_i \neq 0,\ 1 \leq i \leq n\}|,$$

para todo $(x_1, \ldots, x_n) \in \mathbb{F}^n$.

El *peso de un código lineal* se define como

$$w(C) = \min\{w(x) \mid x \in C,\ x \neq 0\}.$$

De esta definición y de la igualdad (1.1), se tiene el siguiente resultado.

Proposición 24 *Sea* C *un código lineal, entonces* $\delta(C) = w(C)$,

Demostración. De (1.1) se tiene que,

$$\begin{aligned} \delta(C) &= \min\{\delta(x, y) \mid x, y \in C,\ x \neq y\} \\ &= \min\{\delta(x - y, 0) \mid x, y \in C,\ x \neq y\} \\ &= \min\{w(x - y, 0) \mid x, y \in C,\ x - y \neq 0\}. \end{aligned}$$

Por ser C un subespacio, se tiene que $x - y \in C$ para todo $x, y \in C$, entonces

$$\begin{aligned} d(C) &= \min\{w(x - y) \mid x, y \in C,\ x - y \neq 0\} \\ &= \min\{w(z) \mid z \in C,\ z \neq 0\} = w(C). \end{aligned}$$

■

La importancia de esta función es la manera práctica de calcularse, ya que en códigos grandes el calcular su distancia mínima será más tardado. Por la proposición anterior calcular la distancia mínima es lo mismo que calcular el peso de un código lineal.

3.2 Matriz generadora

La noción de matriz generadora se debe a que existe una transformación lineal de $\mathbb{F}^k$ a $\mathbb{F}^n$ tal que cada elemento de una base de $\mathbb{F}^k$ lo envia a un elemento de $\mathbb{F}^n$, de manera que los elementos obtenidos sean linealmente independientes. Entonces podemos formar una matriz donde estos elementos sean sus renglones. Como veremos a continuación, una matriz con k renglones linealmente independientes generara un código lineal de dimensión k.

Definición 25 *Sea $C \subseteq \mathbb{F}^n$ un código lineal de dimensión k y longitud n. Una* matriz generadora *de C, es una matriz G de tamaño $k \times n$ cuyos renglones forman una base de C.*

Como una base de un código lineal C no es única, tampoco lo es la matriz generadora, esto es, para cada base de C se tiene una matriz generadora.

Observación 26 *Sea C un código lineal y G una matriz generadora de C, entonces G genera a C, es decir*

$$C = \left\{ uG \mid u \in \mathbb{F}^k \right\}.$$

Demostración. Sea $\{c_1, \ldots, c_k\}$ una base de C.

($\subseteq$) Sea $x \in C$, entonces existen únicos $u_1, \ldots, u_k \in \mathbb{F}$ tal que $x = \sum_{i=1}^{k} u_i c_i$.

Luego, tomando

$$u = (u_1, \ldots, u_k) \in \mathbb{F}^k \text{ y } G = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{pmatrix}.$$

Por lo tanto, $c = uG$.

($\supseteq$) Sea $u \in \mathbb{F}^k$, se tiene que $uG = u_1 c_1 + \cdots + u_k c_k = \sum_{i=1}^{k} u_i c_i \in C$.

■

De lo anterior se puede ver fácilmente que, si se tiene un código lineal C se puede obtener una matriz generadora a partir de encontrar una base de C. Por otro lado, si se tiene una matriz G de tamaño $k \times n$, con entradas en $\mathbb{F}$, de rango $k \leq n$, entonces G genera a un código lineal.

Observación 27 *Sean $u, v \in \mathbb{F}^k$, entonces $uG = vG$ si y sólo si $u = v$.*

Demostración. Sea

$$G = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{pmatrix},$$

una matriz generadora.

($\Rightarrow$) Si $uG = vG$, donde $u = (u_1, \ldots, u_k)$ y $v = (v_1, \ldots, v_k)$, entonces

$$\begin{aligned} uG &= u_1c_1 + \cdots + u_kc_k \\ &= v_1c_1 + \cdots + v_kc_k \\ &= vG, \end{aligned}$$

luego

$$(u_1 - v_1)\, c_1 + \cdots + (u_k - v_k)\, c_k = 0.$$

Como $c_1, \ldots, c_k$ son linealmente independientes implica que $(u_i - v_i) = 0$ para todo $i \in \{1, \ldots, k\}$. Por lo tanto $u = v$.

($\Leftarrow$) Si $u = v$ implica que $uG = vG$.

■

Por otro lado, se puede decir que un código lineal C es la imagen de una transformación lineal inyectiva dada por

$$T : \mathbb{F}^k \longrightarrow \mathbb{F}^n,$$

$$u \longmapsto uG,$$

donde G es una matriz generadora de C.

Definición 28 *Una matriz generadora G es llamada en* forma estándar *si es de la forma $G = (I_k, A)$, donde I_k es la matriz identidad $k \times k$ y A es una matriz de tamaño $k \times (n - k)$.*

Definición 29 *Se dice que un código lineal C es un* código sistemático *si es generado por una matriz en forma estándar.*

Definición 30 *Dos códigos C_1 y C_2, de misma longitud n, son* equivalentes *si existe una permutación $\sigma \in S_n$ tal que*

$$C_2 = \{\sigma(x) \mid x \in C_1\},$$

donde $\sigma(x) = \left(x_{\sigma(1)}, \ldots, x_{\sigma(n)}\right)$ y $x = (x_1, \ldots, x_n)$.

Los códigos equivalentes tienen los mismos parámetros k y d. Por otra parte, no todo código lineal es generado por una matriz en forma estándar, por ejemplo el código lineal generado por $G = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Pero se tiene el siguiente resultado:

Proposición 31 *Todo código lineal C es equivalente a un código sistemático C'.*

Demostración. Sea G la matriz generadora de C y sea $\overline{G}$ la matriz escalonada reducida de G. Luego, se toma a (j, i_j) como la posición de los $1's$ líderes en el $j-ésimo$ renglón y en la $i_j - ésima$ columna de $\overline{G}$. Si $\overline{G} = (g_1, g_2, \ldots, g_n)$ y tomando la permutación $\sigma = (k\ i_k) \cdots (2\ i_2)(1\ i_1) \in S_n$, entonces $G' = \left(g_{\sigma(1)}, g_{\sigma(2)}, \ldots, g_{\sigma(n)}\right)$ es una matriz en forma estándar. Como

$$C = \left\{u\overline{G} \ : \ u \in \mathbb{F}^k\right\},$$

de esto se tiene que

$$\left\{\sigma\left(u\overline{G}\right) : \ u \in \mathbb{F}^k\right\} = \left\{uG' : \ u \in \mathbb{F}^k\right\} = C',$$

donde $\sigma\left(u\overline{G}\right) = \left(ug_{\sigma(1)}, ug_{\sigma(2)}, \ldots, ug_{\sigma(n)}\right)$. ■

Ejemplo 32 *Consideremos el código lineal*

$$C = \{000, 001, 010, 011\} \subseteq \mathbb{F}_2^3,$$

una base para C *es* $\{001, 010\}$*, entonces una matriz generadora de* C *es*

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

luego se toma $\sigma = (1\ 3)\,(2)$ *y se tiene que*

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

Por lo tanto C *es equivalente al código sistemático* $C' = \{000, 100, 010, 110\}$.

3.3 Matriz de control

Definición 33 *Se dirá que* H *es una* matriz de control *del código* C*, si para todo* $x \in \mathbb{F}^n$ *se cumple que* $x \in C$ *si y sólo si* $Hx^t = 0$.

Para un $(n, k) - \textit{código lineal}$ la matriz de control H tiene tamaño $(n-k) \times n$ y rango $n-k$ (ver [4]).

Proposición 34 *Si* G *y* H *son las matrices generadora y de control de* C*, respectivamente, entonces* $GH^t = 0$.

Demostración. Si

$$G = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{pmatrix},$$

entonces $\{c_1, c_2, \ldots, c_k\}$ es una base de C. Luego, $Hc_j^t = 0$, ya que $c_j \in C$ para toda $j \in \{1, \ldots, k\}$. Además, $0 = Hc_j^t = \left(Hc_j^t\right)^t = c_j H^t$, con $1 \leq j \leq k$. Por otro lado,

$$GH^t = \begin{pmatrix} c_1 H^t \\ c_2 H^t \\ \vdots \\ c_k H^t \end{pmatrix} = 0_{k\times(n-k)},$$

donde $0_{k\times(n-k)}$ es la matriz cero de tamaño $k \times (n-k)$. ■

Definición 35 *Una matriz de control es de la* forma estándar *si es de la forma* $H = (B, I_{n-k})$, *donde* I_{n-k} *es la matriz identidad* $(n-k)\times(n-k)$ *y* B *es un matriz de tamaño* $(n-k)\times k$.

Teorema 36 *Sea* H *una matriz de control del* $(n,k)-$*código lineal* C. *Entonces* C *tiene distancia* d *si y sólo si cualquier conjunto de* $d-1$ *columnas de* H *son linealmente independientes, y al menos un conjunto de* d *columnas de* H *es linealmente dependiente.*

Demostración.

($\Rightarrow$) Sea d la distancia de C, entonces existe $z \in C$ tal que $w(z) = d$, donde $z = (z_1, z_2, ..., z_n)$. Como

$$0 = Hz^t = zH^t = z_1 h_1^t + \cdots + z_n h_n^t = z_{i_1} h_{i_1}^t + \cdots + z_{i_d} h_{i_d},$$

con $z_{i_1}, ..., z_{i_d}$ las coordenadas de z distintas de cero, esto implica que H tiene un conjunto de d columnas linealmente dependientes. Ahora,

supongamos que existe $h_{i_1}, h_{i_2}, ..., h_{i_{d-1}}$ un conjunto de columnas de H linealmente dependientes, entonces existen $d-1$ escalares $a_{i_1}, ..., a_{i_{d-1}} \in \mathbb{F}$ no todos ceros tales que $a_{i_1}h_{i_1}^t + \cdots + a_{i_{d-1}}h_{i_{d-1}}^t = 0$. Si tomamos $a = (a_1, ..., a_n)$ con $a_j = 0$ para todo $j \notin \{i_1, ..., i_{d-1}\}$, luego

$$aH^t = a_1h_1^t + \cdots + a_nh_n^t = a_{i_1}h_{i_1}^t + \cdots + a_{i_{d-1}}h_{i_{d-1}}^t = 0,$$

lo cual implica que $a \in C$, ya que $Ha^t = aH^t = 0$, pero $w(a) \leq d-1$ lo que contradice que C tenga distancia d.

($\Leftarrow$) Sea $s = \min\{w(x) \mid x \in C, x \neq 0\}$. Primero demostraremos que $s \geq d$. Por contradicción, sea $x \in C$ distinto de cero, supongamos que $s \leq d-1$, sean $x_{i_1}, x_{i_2}, ..., x_{i_s}$ las coordenadas de x distintas de cero. Luego, sean $h_1, h_2, ..., h_n$ las columnas de H, entonces

$$0 = Hx^t = xH^t = x_1h_1^t + x_2h_2^t + \cdots + x_nh_n^t = x_{i_1}h_{i_1}^t + x_{i_2}h_{i_2}^t + \cdots + x_{i_t}h_{i_s}^t,$$

pero esto contradice que H tenga $d-1$ columnas linealmente independientes. De esto se tiene que $s \geq d$. Falta demostrar que $s \leq d$. Por contradicción, supongamos que para todo $z \in C$ el peso de z es mayor que d. Luego, existe un conjunto $\{h_{i_1}, h_{i_2}, ..., h_{i_d}\}$ de d columnas de H linealmente dependientes, entonces existe $v \in \mathbb{F}^n \backslash C$ con coordenadas $v_j = 0$ para todo $j \notin \{i_1, ..., i_d\}$ con $w(v) \leq d$, entonces $Hv^t = 0$ e implica que $v \in C$, esto es una contradicción, por lo tanto $s \leq d$. Finalmente se tiene lo deseado.

■

3.4 Código dual

El espacio vectorial $\mathbb{F}^n$ sobre el campo finito $\mathbb{F}$ tiene un producto interno canónico dado por $\langle x, y\rangle = \sum_{i=1}^{n} x_i y_i$ con $x, y \in \mathbb{F}^n$.

Definición 37 *Si C es un $(n, k, d) -$ código lineal entonces su* código dual *$C^{\perp}$ de C es el conjunto*

$$C^{\perp} = \{x \in \mathbb{F}^n : \ \langle x, c\rangle = 0 \ \forall \ c \in C\} .$$

Teorema 38 *Sea C un $(n, k, d) -$ código lineal.*

(i) Si G es una matriz generadora de C entonces

$$C^{\perp} = \left\{x \in \mathbb{F}^n : \ xG^t = 0\right\} .$$

(ii) $C^{\perp}$ es un código lineal.

(iii) La dimensión de $C^{\perp}$ es $n - k$.

(iv) $\left(C^{\perp}\right)^{\perp} = C$.

Demostración.

(i) Sea $x \in C^{\perp}$, entonces $\langle x, c\rangle = xc^t = 0$ para todo $c \in C$, en particular si $\{e_1, e_2, ..., e_k\}$ es la base canónica de $\mathbb{F}^k$ se tiene que $e_i G \in C$ para todo $1 \leq i \leq k$, de esto $x\left(e_i G\right)^t = xG^t e_i^t = 0$. Si $G = [G_1, G_2, ..., G_n]$ entonces

$$xG^t e_i^t = \left(x_1 G_1, x_2 G_2, ..., x_n G_n\right) e_i^t = x_i G_i = 0 \, , \ \forall \ 1 \leq i \leq k \, .$$

Luego, $xG^t = 0$ y de esto $x \in \{x \in \mathbb{F}^n : \ xG^t = 0\}$. Reciprocamente, sea $x \in \{x \in \mathbb{F}^n : \ xG^t = 0\}$ y sea $c \in C$. Por demostrar que $xc^t = 0$. Luego, existe $u \in \mathbb{F}^k$ tal que $c = uG$, de esto

$$xc^t = xG^t u^t = (0, ..., 0)\, u^t = 0.$$

Por lo tanto, $C^\perp = \{x \in \mathbb{F}^n : \ xG^t = 0\}$.

(ii) Como C es un subespacio de $\mathbb{F}^n$ también lo es $C^\perp$ (ver Proposición 5.31 de [4]).

(iii) Existe un resultado que dice que si $C \subseteq \mathbb{F}^n$ entonces

$$\dim(\langle C \rangle) + \dim\left(C^\perp\right) = n$$

(ver Proposición 5.32 de [4]), en nuestro caso $C = \langle C \rangle$, ya que C es un subespacio de $\mathbb{F}^n$. Por lo tanto se tiene que $\dim\left(C^\perp\right) = n - k$.

(iv) Si en $\dim(C) + \dim\left(C^\perp\right) = n$ hacemos $C = C^\perp$, tenemos que

$$\dim\left(\left(C^\perp\right)^\perp\right) = k = \dim(C),$$

entonces es suficiente probar que $C \subseteq \left(C^\perp\right)^\perp$. Sea $c \in C$ y sea $z \in C^\perp$. Luego, para todo $b \in C$ se tiene que $zb^t = 0$, en particular $zc^t = 0$, de esto $cz^t = zc^t = 0$, lo que implica que $c \in \left(C^\perp\right)^\perp$.

■

Observación 39 *Si G es una matriz generadora del $(n, k) - $ código lineal C. Entonces G es una matriz de control del $(n, n-k) - $ código lineal $C^\perp$.*

Demostración. Por demostrar que $C^{\perp} = \{x \in \mathbb{F}^n \ : \ Gx^t = 0\}$. Esto se tiene del Teorema 38 (i), ya que $Gx^t = xG^t = 0$. ■

Observación 40 *Sea H una matriz de control de C un $(n,k)-$código lineal. Entonces H es una matriz generadora del código dual $C^{\perp}$, es decir*

$$C^{\perp} = \left\{vH \ : v \in \mathbb{F}^{n-k}\right\}.$$

Demostración.

$(\supseteq)$ Sea $v \in \mathbb{F}^{n-k}$ y sea $c \in C$. Por definición de H se tiene que $Hc^t = 0$, luego $(vH)\, c^t = v\,(Hc^t) = 0$. Por lo tanto, $vH \in C^{\perp}$.

$(\subseteq)$ Sea $z \in C^{\perp}$. Si

$$H = \begin{pmatrix} h_1 \\ h_2 \\ \vdots \\ h_{n-k} \end{pmatrix},$$

luego de la Proposición 34 y de la observación anterior, tenemos que $h_i \in C^{\perp}$ para todo $1 \leq i \leq n-k$. Además el conjunto $\{h_1, h_2, ..., h_{n-k}\}$ forma una base para $C^{\perp}$, ya que H tiene rango $n-k$. Entonces existen únicos $v_1, v_2, ..., v_{n-k} \in \mathbb{F}$ tal que $z = vH$, donde $v = (v_1, v_2, ..., v_{n-k})$.

■

3.5 Decodificación de un código lineal

Ahora daremos un método para la descodificación de un código lineal. Sea C un $(n,k,d) - \textit{código lineal}$ de $\mathbb{F}^n$. Sea $x \in C$ una palabra enviada y sea

$y \in \mathbb{F}^n$ la palabra recibida, entonces consideremos el subconjunto

$$y - C = \{y - \beta \mid \beta \in C\}$$

de $\mathbb{F}^n$, luego existe un $z_0 \in \mathbb{F}^n$ tal que $w(z_0) = \min\{w(z) \mid z \in y - C\}$, el proposito de esta descodificación es de decir que la palabra código $y - z_0$ es la palabra que hemos enviado, osea $y - z_0 = x$.

Capítulo 4

Cotas de un Código

Como ya se definio antes, los parámetros para el estudio de un código C, son la longitud n, el tamaño T y la distancia mínima d. Estos enteros, en general, no son arbitrarios, por ejemplo el tamaño de C no puede ser mayor que $|\mathbb{F}^n|$, ya que $C \subseteq \mathbb{F}^n$ y también se tiene que $1 \leq d \leq n$. Pero estas no son las únicas restricciones para estos parámetros, acontinuación se mostrarán algunas cotas para los parámetros, por mencionar algunas se tiene la cota de Griesmer, la cota de Plotkin, la cota de Hamming y la cota de Singleton (ver [6]).

4.1 Cota de Hamming

Antes de probar la *cota de Hamming*, para un $(n, T, d) - código\ q - ario$, veamos que

$$|B(x,r)| = \sum_{i=0}^{\lfloor r \rfloor} \binom{n}{i} (q-1)^i,$$

para todo $x \in \mathbb{F}^n$, y $r \geq 0$. Se tiene que

$$B(x,r) = \{y \in \mathbb{F}^n \mid \delta(x,y) \leq r\} = \bigcup_{l=0}^{\lfloor r \rfloor} \{y \in \mathbb{F}^n \mid \delta(x,y) = l\}.$$

De esto $|B(x,r)| = \sum_{i=0}^{\lfloor r \rfloor} |\{y \in \mathbb{F}^n \mid \delta(x,y) = l\}|$. Por demostrar que

$$|\{y \in \mathbb{F}^n \mid \delta(x,y) = l\}| = \binom{n}{l} (q-1)^l.$$

Sea $y \in \{y \in \mathbb{F}^n \mid \delta(x,y) = l\}$, entonces si $x = (x_1, \ldots, x_n)$ existen i_1, $i_2, \ldots, i_l$ tal que $x_{i_j} \neq y_{i_j}$, con $1 \leq j \leq l$, y $x_i = y_i$ para toda $i \in \{1, \ldots, n\} \setminus \{i_1, \ldots, i_l\}$. Sin perdida de generalidad se puede suponer que

$$x = (x_1, \ldots, x_l, a_1, \ldots, a_{n-l}) \text{ y } y = (y_1, \ldots, y_l, a_1, \ldots, a_{n-l})$$

con $x_i \neq y_i$ para toda $i \in \{1, \ldots, l\}$. Luego, se tiene que hay $\binom{n}{l}$ posibles maneras de tomar a y. Ahora, para elegir a $y_i \neq x_i$ hay $q-1$ elementos de $\mathbb{F}$ para toda $i \in \{1, \ldots, l\}$. Por lo tanto

$$|\{y \in \mathbb{F}^n \mid \delta(x,y) = l\}| = \binom{n}{l} (q-1)^l.$$

Proposición 41 (Cota de Hamming) *Sea C un $(n, T, d)-$código $q-$ario con $t = \left\lfloor \frac{d-1}{2} \right\rfloor$, entonces*

$$T \cdot \sum_{i=0}^{t} \binom{n}{i} (q-1)^i \leq q^n. \tag{4.1}$$

Demostración. Por el Lema 10, se tiene que las bolas de radio t centradas en palabras código de C distintas son disjuntas, entonces $T \cdot |B(x,t)| \leq q^n$ para todo $x \in C$. De la observación anterior se tiene la desigualdad (4.1). ■

4.2 Cota de Singleton

Proposición 42 (Cota de Singleton) *Sea C un $(n,T,d)-$código $q-$ario, entonces*

$$T \leq q^{n-d+1}.$$

En particular, si C es un $(n.k,d)-$código lineal $q-$ario, entonces

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

Demostración. Sea $\mathbb{F}$ un alfabeto de q elementos, entonces $C \subseteq \mathbb{F}^n$. Si a cada palabra código de C eliminamos las últimas $d-1$ coordenadas, entonces las palabras resultantes son de longitud $n-(d-1)$ y estas son todas distintas, ya que la distancia mínima de C es d. Luego, si D es el conjunto formado por las palabras de longitud $n-(d-1)$, entonces $D \subseteq \mathbb{F}^{n-(d-1)}$. Por otro lado se tiene que D tiene T elementos, de esto $T = |D| \leq q^{n-d+1}$.

Ahora, para el caso de un $(n,k,d)-$*código lineal* se tiene que $T = q^k$, luego $q^k \leq q^{n-d+1}$, lo que implica que $k \leq n-d+1$. ■

Definición 43 *Los códigos lineales que satifacen la cota de Singleton son llamados* códigos de máxima distancia de separación *(o MDS).*

Por ejemplo, un código

$$C = \{(\alpha, ..., \alpha) \in \mathbb{F}^n | \ \alpha \in \mathbb{F}\},$$

donde el campo $\mathbb{F}$ tiene q símbolos, es un $(n, 1, n) - \textit{código lineal}$ y satisface la cota de Singleton, entonces es un MDS. Existen otros códigos lineales llamados Reed-Solomon, estos serán definidos más adelante, que satisfacen la igualdad de esta cota. De lo cual se tiene que, en general, la cota no puede ser mejorada.

Proposición 44 *Si C es un $(n, k, d) - \textit{código lineal de máxima distancia de separación (MDS), entonces su código dual } C^{\perp}$ es un $(n, n-k, k+1) - \textit{código lineal de MDS.}$*

Demostración. Del Teorema 38 se tiene que $C^{\perp}$ es un código lineal de dimensión $n - k$, entonces lo que queda por demostrar es que la distancia de $C^{\perp}$ es $k + 1$. Si G es la matriz generadora de C, la cual tiene rango k, implica que G es la matriz de control de $C^{\perp}$. Luego, si d' es la distancia de $C^{\perp}$ entonces $d' - 1 = k$ por el Teorema 36. Por lo tanto, $d' = k + 1$. ■

Capítulo 5

Códigos Cíclicos

Como los códigos cíclicos son códigos lineales, seguiremos considerando un alfabeto $\mathbb{F}$ como un campo finito de q elementos. Nuestro interés en estos códigos es para definir los códigos Reed-Solomon, los códigos cíclicos son los pilares para construir los códigos Reed-Solomon ([6]).

5.1 Código cíclico

Definición 45 *Un* $(n,k)-$*código lineal* C *sobre* $\mathbb{F}$*, es un* código cíclico *si para cada* $c=(c_0,c_1,...,c_{n-1})\in C$ *se cumple que* $\widehat{c}=(c_{n-1},c_0,...,c_{n-2})\in C$*.*

Ejemplo 46 *Consideremos el código*

$$C=\{0000,1010,0101,1111\}\subseteq\mathbb{F}_2^4,$$

es es un $(4,2)-$*código lineal. Ahora veamos que es cíclico, para* 1010 *en* C *se tiene que* $0101\in C$ *y para* $0101\in C$ *tenemos que* 1010 *es un elemento*

de C. Para los dos elementos restantes de C es obvio que al mover el ultimo dígito al inicio la palabra resultante sigue siendo una palabra código. Por lo tanto C es un código cíclico.

Ejemplo 47 *Tomemos el código lineal*

$$C = \{000, 100, 011, 111\} \subseteq \mathbb{F}_2^3,$$

luego para 011 *en* C *se tiene que* 101 *no es un elemento del código, por lo que implica que* C *no es un código cíclico.*

Consideremos el anillo de polinomios $\mathbb{F}[x]$, luego existe una correspondencia entre la palabra $c = (c_0, c_1, ..., c_{n-1}) \in \mathbb{F}^n$ y el polinomio $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \in \mathbb{F}[x]$ (ver [8]). Por otro lado, si $A = \mathbb{F}[x] / \langle x^n - 1 \rangle$ podemos identificar el polinomio $c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ en $\mathbb{F}[x]$ con la clase $c_0 + c_1x + \cdots + c_{n-1}x^{n-1} + \langle x^n - 1 \rangle$ en A. Entonces, para $\widehat{c} = (c_{n-1}, c_0, ..., c_{n-2})$ su polinomio correspondiente es

$$\begin{aligned} \widehat{c}(x) &= c_{n-1} + c_0x + \cdots + c_{n-2}x^{n-1} \\ &= x\left(c_0 + c_1x + \cdots + c_{n-1}x^{n-1}\right) - c_{n-1}(x^n - 1) \\ &= xc(x) - c_{n-1}(x^n - 1), \end{aligned}$$

de esto, $\widehat{c}(x) = xc(x) + \langle x^n - 1 \rangle$.

En consecuencia de lo anterior,

$$\pi : \mathbb{F}^n \longrightarrow A,$$

es una transformación lineal de espacios vectoriales sobre $\mathbb{F}$, dada por

$$\pi(a_0, a_1, ..., a_{n-1}) := a(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1},$$

donde $a = (a_0, a_1, ..., a_{n-1})$. Entonces un código en $\mathbb{F}^n$ puede considerarse como un subconjunto en A. En el transcurso de este capítulo, identificaremos algunas veces a $\mathbb{F}^n$ con A.

Ejemplo 48 *Tomemos el código cíclico*

$$C = \{0000, 1010, 0101, 1111\} \subseteq \mathbb{F}_2^4;$$

entonces $\pi(0000) = 0$, $\pi(1010) = 1 + x^2$, $\pi(0101) = x + x$ *y* $\pi(1111) = 1 + x + x^2 + x^3$. *Por lo tanto,*

$$\pi(C) = \left\{0, 1 + x^2, x + x^3, 1 + x + x^2 + x^3\right\} \subset \mathbb{F}_2[x] / \left\langle x^4 - 1 \right\rangle.$$

Antes de continuar introduciremos una nociones básicas para el estudio de códigos cíclicos.

Definición 49 *Sea R un anillo conmutativo. Sea I un subconjunto de R, se dice que I es un* ideal *de R, si:*

(i) Para todo $a, b \in I$, se tiene que $a + b \in I$

(ii) Para todo $r \in R$ y $a \in I$, se cumple que $ra \in I$.

Teorema 50 *Un código lineal C en $\mathbb{F}^n$ es cíclico si y sólo si $\pi(C)$ es un ideal en A.*

Demostración.

($\Rightarrow$) Sean $c_1 = (u_0, u_1, ..., u_{n-1}), c_2 = (v_0, v_1, ..., v_{n-1}) \in C$, entonces $\pi(c_1) = u_0 + u_1 x + \cdots + u_{n-1}x^{n-1}$ y $\pi(c_2) = v_0 + v_1 x + \cdots + v_{n-1}x^{n-1}$, luego

$$\pi(c_1) + \pi(c_2) = (u_0 + v_0) + (u_1 + v_1)x + \cdots + (u_{n-1} + v_{n-1})x^{n-1} \in \pi(C).$$

Ahora sea $r(x) \in A$, donde $r(x) = p(x) + \langle x^n - 1 \rangle$, con $p(x) \in \mathbb{F}[x]$ y sea $c = (z_0, z_1, ..., z_{n-1}) \in C$. Por demostrar que $r(x)\pi(c) \in \pi(C)$. Puesto que $xc(x)$ corresponde a $(z_{n-1}, z_0, ..., z_{n-2})$ y es un elemento de C, ya que C es cíclico, entonces $xc(x) = x\pi(c) \in \pi(C)$, luego $x^2c(x)$ corresponde a $(z_{n-2}, z_{n-1}, ..., z_{n-3}) \in C$, entonces $x^2c(x) \in \pi(C)$, de manera analoga se tiene que $x^ic(x) \in \pi(C)$ para todo i. Por otro lado, $r(x) = r_0 + r_1 x + \cdots + r_{n-1}x^{n-1}$ para algún $(r_0, r_1, ..., r_{n-1}) \in \mathbb{F}^n$, y de lo anterior se tiene que

$$r(x)c(x) = r_0 c(x) + r_1 xc(x) + \cdots + r_{n-1}x^{n-1}c(x) \in \pi(C).$$

Por lo tanto, $\pi(C)$ es un ideal en A.

($\Leftarrow$) Sea $(c_0, c_1, ..., c_{n-1}) \in C$, entonces $\pi(c_0, c_1, ..., c_{n-1})$ es un elemento del ideal $\pi(C)$, luego $x\pi(c_0, c_1, ..., c_{n-1}) \in \pi(C)$ y esto corresponde a la palabra código $(c_{n-1}, c_0, ..., c_{n-2})$. Por lo tanto, C es cíclico.

■

Definición 51 *Un ideal I de un anillo conmutativo R es llamado* ideal principal *si existe $a \in I$ tal que $I = \langle a \rangle$, donde $\langle a \rangle = \{ra \ : \ r \in R\}$. Luego, a es llamado el elemento generador de I.*

Observación 52 *Todo ideal I del anillo A es un ideal principal.*

Demostración. Una demostración esta en el Teorema 5.2 en la página 151 de [11] ■

Corolario 53 *Sea C un código cíclico en $\mathbb{F}^n$, existe un único polinomio mónico $g(x) \in \mathbb{F}[x]$ que divide a $x^n - 1$, tal que $\pi(C) = \langle g(x) + \langle x^n - 1 \rangle \rangle$.*

Demostración. Por el Teorema de la Correspondencia existe un ideal I de $\mathbb{F}[x]$, con $\langle x^n - 1 \rangle \subseteq I$, tal que $\pi(C) = I \diagup \langle x^n - 1 \rangle$. Luego existe $g(x) \in I$ polinomio mónico tal que $I = \langle g(x) \rangle$, como $x^n - 1 \in I$ se tiene que $g(x)$ divide a $x^n - 1$. Ahora, sea $f(x) + \langle x^n - 1 \rangle \in \pi(C)$, como $f(x) \in I$ existe $p(x) \in \mathbb{F}[x]$ tal que $f(x) = p(x) g(x)$. De esto

$$\begin{aligned} f(x) + \langle x^n - 1 \rangle &= p(x) g(x) + \langle x^n - 1 \rangle \\ &= (p(x) + \langle x^n - 1 \rangle)(g(x) + \langle x^n - 1 \rangle). \end{aligned}$$

Lo anterior implica que $\pi(C) = \langle g(x) + \langle x^n - 1 \rangle \rangle$. Solo falta mostrar la unicidad. Supongamos que existen $q(x), h(x) \in \mathbb{F}[x]$ polinomios mónicos de grando más pequeño que dividen a $x^n - 1$, tal que sus clases generan a $\pi(C)$. Luego $\deg(q(x)) = \deg(h(x))$. Entonces $q(x) - h(x)$ es un polinomio distinto de cero de grado más pequeño que el grado de $q(x)$ en $\pi(C)$, esto es una contradicción. Por lo tanto $g(x)$ es único. ■

Definición 54 *Si C es un código cíclico, el* polinomio generador *de $\pi(C)$ también es llamado el polinomio generador de C.*

Teorema 55 *Sea C un código cíclico en $\mathbb{F}^n$ y sea $g(x)$ el polinomio generador de C. Si $\deg(g(x)) = n-k$ entonces*

(i) C tiene dimensión k.

(ii) Las palabras código correspondientes a $g(x), xg(x), ..., x^{k-1}g(x)$ forman una base para C.

Demostración. Una prueba a este teorema se encuentra en el Teorema 4.2.13 en la página 105 de [3]. ■

Ejemplo 56 *Sea $n = 5$, $g(x) = x+1$ el polinomio generador para el código cíclico C en $\mathbb{F}_2^5$. Entonces una base para C es*

$$\left\{x+1, x^2+x, x^3+x^2, x^4+x^3\right\},$$

donde esta base corresponde a las palabras código $11000, 01100, 00110, 00011$, *respectivamente.*

5.2 Matriz Generadora y Matriz de Control

Corolario 57 *Sea C un código cíclico en $\mathbb{F}^n$, con polinomio generador*

$$g(x) = g_0 + g_1 x + \cdots + g_{n-k}x^{n-k},$$

entonces tiene matriz generadora

$$G = \begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ & & & \vdots & & & & \\ 0 & \cdots & 0 & 0 & g_0 & g_1 & \cdots & g_{n-k} \end{pmatrix}.$$

Demostración. Del teorema anterior los renglones de la matriz G forman una base para C. De esto se tiene que G es una matriz generadora. ■

Definición 58 *Sea C un código cíclico en $\mathbb{F}^n$, con polinomio generador $g(x)$ de grado $n-k$, llamaremos* polinomio de control *de C a*

$$h(x) = \frac{x^n - 1}{g(x)} = h_0 + h_1 x + \cdots + h_k x^k. \tag{5.1}$$

Proposición 59 *Para un código cíclico C en $\mathbb{F}^n$, con polinomio de control dado por* (5.1)*, entonces la matriz de control H, de tamaño $(n-k) \times n$, es de la forma*

$$H = \begin{pmatrix} 0 & 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & h_1 & h_0 \\ 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & h_1 & h_0 & 0 \\ & & & & \vdots & & & & \\ h_k & h_{k-1} & \cdots & h_1 & h_0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Demostración. Solo se necesita probar que $GH^t = 0$. ■

5.3 Ceros de un código cíclico

Supongamos que $f_1(x), ..., f_r(x)$ son los factores irreducibles del polinomio generador de C, y $\{\alpha_1, ..., \alpha_s\}$ el conjunto de todas las raices de los f_i, con $1 \leq i \leq r$, que están en una extensión finita $\mathbb{F}'$, donde $\mathbb{F}$ tiene q^m elementos, de $x^n - 1$ sobre $\mathbb{F}$. Entonces,

$$\pi(C) = \langle g(x) \rangle = \{c(x) \in A | c(\alpha_1) = c(\alpha_2) = \cdots = c(\alpha_s) = 0 + \langle x^n - 1 \rangle\}.$$

Ahora consideremos la matriz

$$\overline{H} = \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_r & \cdots & \alpha_r^{n-1} \end{pmatrix}$$

de tamaño $r \times n$. Además, $c = (c_0, c_1, ..., c_{n-1}) \in C$ si y sólo si $\overline{H}c^t = 0$, es decir, $c \in C$ si y sólo si el polinomio $g(x)$ divide al polinomio $c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$. Luego, los renglones de $\overline{H}$ pueden ser linealmente dependientes, o sea, una matriz de control de C puede ser obtenida de $\overline{H}$ borrando renglones si es necesario.

5.4 Códigos BCH y Códigos Reed-Solomon

Fijamos un campo $\mathbb{F}$ de q elementos, y números naturales n, b y ρ con $2 \leq \rho \leq n$. Sea m el menor número natural tal que $q^m \equiv 1 \bmod n$, y sea $\alpha \in \mathbb{F}'$ una $n - ésima$ raíz primitiva de la unidad.

Definición 60 *Un* código BCH *de longitud n y distancia designada ρ, es el código cíclico con polinomio generador que tiene por raíces $\alpha^b, \alpha^{b+1}, ..., \alpha^{b+\rho-2}$.*

Cuando se toma $b = 1$ el código BCH es llamado en sentido estricto. Si la longitud es $n = q^m - 1$ el código es llamado un código BCH primitivo.

Definición 61 *Se dice que un código BCH primitivo es un código* Reed-Solomon *si su longitud es $n = q - 1$.*

Proposición 62 *Un código BCH de distancia designada ρ tiene distancia mínima $d \geq \rho$. En general no se conoce el valor exacto de la distancia mínima.*

Demostración. Una demostración se encuentra en el Teorema 6.2 de la página 206 de [11]. ■

Teorema 63 *Un código Reed-Solomon de longitud n, dimensión k, y distancia designada ρ satisface la distancia mínima es $d = \rho = n - k + 1$ y por lo tanto tiene parámetros $(n, k, n - k + 1)$. Esta es la razón por la cual estos código son de MDS.*

Demostración. Una demostración se encuentra en el Teorema 7.1 en la página 239 de [11]. ■

Capítulo 6

Códigos bajo la Restricción de Colinealidad

6.1 Códigos Algebraico Geométricos

Ahora consideremos un objeto geométrico $\mathcal{X}$, por ejemplo una recta o una superficie o cualquier variedad de cualquier dimensión, con un subconjunto $\mathcal{P}$ que consiste de n puntos $P_1, ..., P_n$. Supongamos que tenemos un espacio vectorial $\mathcal{L}$ sobre un campo $\mathbb{F}$ de funciones en $\mathcal{X}$ con valores en $\mathbb{F}$. Tomemos la aplicación evaluación

$$ev_{\mathcal{P}} : \mathcal{L} \longrightarrow \mathbb{F}^n,$$

dada por

$$f \longmapsto (f(P_1), ..., f(P_n)).$$

Esta aplicación es $\mathbb{F}-$*lineal* y por lo tanto su imagen es un código lineal. Este tipo de códigos son llamados generalmente códigos **Algebraico Geométrico**.

Ejemplo 64 (Construcción del Código Reed-Solomon) *Vamos a tomar como nuestro objeto geométrico $\mathcal{X}$ la linea afín sobre $\mathbb{F}$, campo finito con q elementos. Sean $n = q-1$ y $\mathcal{P} = \mathbb{F} \setminus \{0\} = \{\alpha_1, ..., \alpha_n\}$. Para un entero k con $1 \leq k \leq n$, el espacio vectorial $\mathcal{L}$ sobre $\mathbb{F}$ será el conjunto*

$$L_k = \{f \in \mathbb{F}[x] \mid \deg(f) \leq k-1\}.$$

Luego la dimensión de L_k es k.

Ahora consideremos la aplicación evaluación

$$\begin{array}{rcl} ev_{\mathcal{P}} & : & L_k \longrightarrow \mathbb{F}^n \\ f & \longmapsto & (f(\alpha_1), f(\alpha_2), ..., f(\alpha_n)) \end{array}$$

La aplicación es $\mathbb{F}-$lineal e inyectiva. De esto $\dim_{\mathbb{F}}(\operatorname{Im} ev_{\mathcal{P}}) = \dim_{\mathbb{F}}(L_k) = k$. Por lo tanto

$$C_k := \operatorname{Im} ev_{\mathcal{P}} = \{(f(\alpha_1), f(\alpha_2), ..., f(\alpha_n)) \mid f \in L_k\},$$

es un $(n,k)-$código lineal sobre $\mathbb{F}$.

Lo que sigue es calcular la distancia mínima de C_k: Sea $ev_{\mathcal{P}}(f) \in C_k$ distinto de cero, entonces su peso es

$$\begin{array}{rcl} w(ev_{\mathcal{P}}(f)) & = & |\{i \in \{1, ..., n\} \mid f(\alpha_i) \neq 0\}| \\ & = & n - |\{i \in \{1, .., n\} \mid f(\alpha_i) = 0\}| \\ & \geq & n - (k-1) = n - k + 1 \end{array}$$

De esto la distancia minima d de C_k satisface $d \geq n-k+1$. Por otro lado, la cota de Singleton nos dice que $d \leq n-k+1$. Esto implica que $d = n-k+1$. De lo anterior C_k es un $(n, k, n-k+1) - código\ lineal$. Este código es llamado ***Reed-Solomon****, que además es un código de Máxima Distancia de Separación.*

6.2 Explosión del plano afín

Las explosiones se pueden definir localmente y ya que nos interesan los superficies racionales, consideremos ahora la explosión del plano afín $\mathbb{A}^2_k$ en el punto $(0,0)$, por simplicidad denotaremos $\mathbb{A}^2_k$ como $\mathbb{A}^2$ y a $\mathbb{P}^1_k$ como $\mathbb{P}^1$. Tomemos el producto $\mathbb{A}^2 \times \mathbb{P}^1$, el cual es una variedad cuasi-proyectiva. Sean u, v las coordenadas en $\mathbb{A}^2$ y sean w, z las coordenadas homogéneas en $\mathbb{P}^1$, entonces los subconjuntos cerrados de $\mathbb{A}^2 \times \mathbb{P}^1$ estan definidos por polinomios en las variables u, v, w, z, los cuales son polinomios homogéneos con respecto a w, z.

Ahora definamos la explosión $\mathbb{A}^2$ en $(0,0)$ como el subconjunto cerrado X de $\mathbb{A}^2 \times \mathbb{P}^1$ definido por la ecuación $uz = vw$. Luego se tiene un morfismo natural $\varphi : X \longrightarrow \mathbb{A}^2$ dado por restringir el mapeo proyección de $\mathbb{A}^2 \times \mathbb{P}^1$ en el primer factor. A continuación estudiaremos las propiedades de X :

(i) $\varphi^{-1}(0,0) \cong \mathbb{P}^1$. Sea $((u,v),(w:z)) \in X$ tal que $\varphi((u,v),(w:z)) = (0,0)$, por definición de φ se tiene que $(u,v) = (0,0)$, entonces $(w:z)$ no tiene restricciones. Por lo tanto $\varphi^{-1}(0,0) = \{(0,0)\} \times \mathbb{P}^1$ y de esto

$\varphi^{-1}(0,0) \cong \mathbb{P}^1$. Llamaremos **divisor excepcional** a $\varphi^{-1}(0,0)$ y lo denotaremos por E.

(ii) Sea $P = (p_1, p_2)$ en $\mathbb{A}^2$ distinto de $(0,0)$, entonces el conjunto $\varphi^{-1}(P)$ consiste de un solo punto. Sea $((u,v),(w:z)) \in X$, tal que

$$\varphi((u,v),(w:z)) = (p_1,p_2),$$

luego tenemos que $(u,v) = (p_1,p_2)$. De la definición de X se tiene que $p_1 z = p_2 w$, sin perdida de generalidad podemos suponer que $p_1 \neq 0$ lo que implica que $z = \frac{p_2}{p_1} w$, de esto se obtiene que

$$\begin{aligned} ((u,v),(w:z)) &= \left((p_1,p_2),\left(w:\frac{p_2}{p_1}w\right)\right) \\ &= \left((p_1,p_2),\left(1:\frac{p_1}{p_2}\right)\right) \\ &= ((p_1,p_2),(p_1:p_2)). \end{aligned}$$

Finalmente, $\varphi^{-1}(P) = \{((p_1,p_2),(p_1:p_2))\}$.

(iii) φ induce un isomorfismo de $X - \varphi^{-1}(0,0)$ sobre $\mathbb{A}^2 - \{(0,0)\}$. Si tomamos

$$\psi : \mathbb{A}^2 - \{(0,0)\} \longrightarrow X - \varphi^{-1}(0,0),$$

dada por

$$(p_1,p_2) \longmapsto ((p_1,p_2),(p_1:p_2)),$$

esta función define el morfismo inverso de φ, esto es para $(p_1,p_2) \in \mathbb{A}^2 - \{(0,0)\}$ se tiene que

$$\varphi \circ \psi(p_1,p_2) = \varphi((p_1,p_2),(p_1:p_2)) = (p_1,p_2),$$

entonces $\varphi \circ \psi = id_{\mathbb{A}^2 - \{(0,0)\}}$. Ahora para $((p_1, p_2), (q_1 : q_2)) \in X - \varphi^{-1}(0,0)$ tenemos

$$\psi \circ \varphi ((p_1, p_2), (q_1 : q_2)) = \psi (p_1, p_2) = ((p_1, p_2), (p_1 : p_2)),$$

pero $p_1 q_2 = p_2 q_1$, lo cual implica que

$$((p_1, p_2), (q_1 : q_2)) = ((p_1, p_2), (p_1 : p_2)),$$

por lo tanto $\psi \circ \varphi = id_{X - \varphi^{-1}(0,0)}$.

(iv) Consideremos todas las lineas en $\mathbb{A}^2$ que pasan por el punto $(0,0)$, el cual es el conjunto

$$L = \left\{ \left\{ (x,y) \in \mathbb{A}^2 \mid y = \lambda x \right\} \mid \lambda \in k \right\} \cup \left\{ \left\{ (0,y) \in \mathbb{A}^2 \mid y \in k \right\} \right\}.$$

Sea $L_\lambda := \{(x,y) \in \mathbb{A}^2 \mid y = \lambda x\} \in L$ con $\lambda \in k$, veamos quien es $\varphi^{-1}(L_\lambda)$. Sea $((x,y), (w : z)) \in X$ tal que $\varphi ((x,y), (w : z)) \in L_\lambda$, entonces $(x,y) \in L_\lambda$, luego $y = \lambda x$, de esto

$$((x,y), (w : z)) = ((x, \lambda x), (w : z)).$$

Si $x = 0$, obtenemos que $((x,y), (w : z)) = ((0,0), (w : z))$. Si $x \neq 0$ implica que

$$z = \frac{y}{x} w = \frac{\lambda x}{x} w = \lambda w,$$

de lo cual se tiene que

$$((x,y), (w : z)) = ((x, \lambda x), (w : \lambda w)) = ((x, \lambda x), (1 : \lambda)).$$

Por lo anterior tenemos que

$$\varphi^{-1}(L_\lambda) = \left\{((x,y),(1:\lambda)) \in \mathbb{A}^2 \times \mathbb{P}^1 \mid y = \lambda x\right\} \cup \left(\{(0,0)\} \times \mathbb{P}^1\right).$$

Para la recta definida por $x = 0$, sea $L^0 := \{(0,y) \in \mathbb{A}^2 \mid y \in k\} \in L$, y sea $((x,y),(w:z)) \in X$ tal que $\varphi((x,y),(w:z)) \in L^0$, entonces $(x,y) = (0,y)$, luego

$$\varphi^{-1}\left(L^0\right) = \left\{((0,y),(0:z)) \in \mathbb{A}^2 \times \mathbb{P}^1 \mid y \neq 0\right\} \cup \left(\{(0,0)\} \times \mathbb{P}^1\right).$$

(v) X es irreducible. Vamos a trabajar con la Topología de Zariski para demostrar que X es irreducible. Podemos ver X es la unión de $X - \varphi^{-1}(0,0)$ y $\varphi^{-1}(0,0)$. Como $X - \varphi^{-1}(0,0)$ es isomorfo a $\mathbb{A}^2 - \{(0,0)\}$, se tiene que $X - \varphi^{-1}(0,0)$ es irreducible. Cada punto de $\varphi^{-1}(0,0)$ está en la cerradura de algún subconjunto de $X - \varphi^{-1}(0,0)$, esto implica que $X - \varphi^{-1}(0,0)$ es denso en X. Por lo tanto, X es irreducible.

Si C es una curva $\mathbb{A}^2$ que pasa por $(0,0)$, se tiene que $\varphi^{-1}(C)$ es la unión del divisor excepcional E y la curva irreducible $\widetilde{C}$, donde $\widetilde{C}$ se conoce como la **Transformada Estricta** de C. La **Transformada Total** de C, se denota por $\varphi^*(C)$ y está dada por $\varphi^*(C) = E + \widetilde{C}$.

Un caso particular de la Proposición 3.2 de la página 386 de [2] nos da el siguiente resultado:

Lema 65 *Sea X la explosión del plano proyectivo en el punto P, entonces $Pic(X) = \mathbb{Z}\mathcal{E}_0 \oplus \mathbb{Z}\mathcal{E}_1$ y la forma de intersección de $Pic(X)$ está dada por*

$$(a,b)(\alpha,\beta) = a\alpha - b\beta,$$

donde $(a,b) = a\mathcal{E}_0 - b\mathcal{E}_1$ *y* $(\alpha,\beta) = \alpha\mathcal{E}_0 - \beta\mathcal{E}_1$*, con* $\mathcal{E}_0 = \varphi^*(L)$ *(donde* L *es una recta general) y* $\mathcal{E}_1$ *es la clase en* $Pic(X)$ *del divisor excepcional de la explosión.*

6.3 Nociones Fundamentales

Utilizaremos libremente las nociones de divisores y propiedades de los mismo, una referencia es el capítulo II y V de [2], o bien, en la parte II de esta tesis se encuentra una breve introducción.

Definición 66 *Un divisor* D *de una superficie proyectiva lisa* X *es numéricamente efectivo si el número de intersección de* D *con cualquier curva* C *en* X *es mayor o igual a cero.*

Consideremos la superficie racional X como la explosión del plano proyectivo en r puntos $P_1, P_2, ..., P_r$ de una recta, su geometría que nos interesa está dada por el siguiente resultado, es decir calcular la dimensión de las secciones globales de un divisor en X:

Lema 67 *Sea* D *un divisor numéricamente efectivo en* X *entonces la dimensión del espacio vectorial de secciones globales de* D*, donde* D *es de la forma*

$$D = a\mathcal{E}_0 - \mu_1\mathcal{E}_1 - \cdots - \mu_r\mathcal{E}_r,$$

esta dada por

$$\frac{a^2 + 3a + 2 - \sum_{j=1}^{r} \mu_j\left(\mu_j - 1\right)}{2},$$

donde $\mathcal{E}_0 = \varphi^*(L)$, *aqui* L *es una recta general del plano proyectivo, y* $\mathcal{E}_j = \varphi^*(P_j)$ *para cada* $j = 1, .., r$, *y donde* $a, \mu_1, ..., \mu_r$ *son números enteros.*

Demostración. Es una consecuencia del Teorema de Riemann-Roch y de la Dualidad de Serre (ver el Teorema 1.6 de la página 362 y el Corolario 7.7 de la página 244 de [2]). ■

6.4 Códigos bajo la restricción de colinealidad

Un código se considera bueno si corrige la mayor cantidad posible de errores ocurridos durante la transmisión de información. Lo interesante del siguiente Teorema es que nos proporciona una cota inferior para la distancia mínima de un código Algebraico Geométrico. Este Teorema es nuestro resultado principal, el cual es un resultado nuevo.

Teorema 68 *Sea* q *una potencia de un número primo y sean* $a, \mu_1, ..., \mu_r$ *(con* $r \in \mathbb{Z}^+$*) enteros positivos de modo que:*

(i) $a \leq q - 2$,

(ii) $\mu_1 + \cdots + \mu_r \leq a$.

Entonces existe un código lineal de longitud $(q-1)^2$, *de dimensión*

$$\frac{a^2 + 3a + 2 - \sum_{j=1}^{r} \mu_j \left(\mu_j - 1\right)}{2},$$

y con distancia mínima $d \geq (q-1)(q-1-a)$.

Demostración. Tomemos la descomposición del plano proyectivo $\mathbb{P}^2_{\mathbb{F}_q}$ sobre el campo finito $\mathbb{F}_q$ forma siguiente

$$\mathbb{P}^2_{\mathbb{F}_q} = \mathbb{A}^2_{\mathbb{F}_q} \cup \mathbb{P}^1_{\mathbb{F}_q},$$

donde $\mathbb{P}^1_{\mathbb{F}_q} = C(x_0)$, con $(x_0 : x_1 : x_2)$ son las coordenadas homogéneas de $\mathbb{P}^2_{\mathbb{F}_q}$ y para cualquier ideal I del anillo de polinomios $K[x_0, x_1, x_2, ..., x_n]$ en $n+1$ variables con coeficientes en el campo K, $C(I)$ denotará el subconjunto de K^{n+1} de ceros de los elementos de I. En particular, si I esta generado por $f_1, f_2, ..., f_s$, denotaremos $C(I)$ por simplicidad $C(f_1, f_2, .., f_s)$.

Por otro lado, fijemos r puntos $P_1, ..., P_r$ que están sobre la recta $C(x_2)$ de $\mathbb{A}^2_{\mathbb{F}_q}$. Consideremos el conjunto de todas las curvas proyectivas de grado a y que pasan por P_j con una multiplicidad al menos μ_j para cada $j = 1, ..., r$. Esto es un espacio vectorial sobre $\mathbb{F}_q$ isomorfo a las secciones globales del elemento $\mathcal{D} = O_X(D)$ de $Pic(X)$ donde X es la explosión del plano proyectivo de $\mathbb{P}^2_{\mathbb{F}_q}$ en todos los puntos $P_1, P_2, ..., P_r$ y $\mathcal{D} = a\mathcal{E}_0 - \mu_1\mathcal{E}_1 - \cdots - \mu_r\mathcal{E}_r$, ver notación en el Lema anterior. Ahora tomemos la siguiente aplicación

$$\Psi : E(a, \mu_1, ..., \mu_r) \longrightarrow \mathbb{F}_q^{(q-1)^2}$$

dada por

$$f \longmapsto \Psi(f) = \left(\frac{f}{x_0^a}(Q_1), \frac{f}{x_0^a}(Q_2), ..., \frac{f}{x_0^a}\left(Q_{(q-1)^2}\right) \right),$$

donde

$$E(a, \mu_1, ..., \mu_r) = \left\{ f \in \mathbb{F}_q[x_0, x_1, x_2]_h^a \mid m_{p_i}(C(f)) \geq \mu_i \ \forall\ i = 1, ..., r \right\},$$

$\mathbb{F}_q[x_0, x_1, x_2]_h^a$ es el anillo de polinomios homogéneos en las variables x_0, x_1, x_2 de grado a y $\left\{Q_1, Q_2, ..., Q_{(q-1)^2}\right\} = \mathbb{A}^2_{\mathbb{F}_q} - C(x_1x_2)$.

Esta es una aplicación lineal inyectiva. Entonces define un código lineal en $\mathbb{F}_q^{(q-1)^2}$ con longitud $(q-1)^2$ y con dimensión $k = \dim_{\mathbb{F}_q} E(a, \mu_1, ..., \mu_r)$. De otro lado, $E(a, \mu_1, ..., \mu_r)$ es isomorfo a $H^0(X, \mathcal{D})$, dado por el isomorfismo $\Phi : E(a, \mu_1, ..., \mu_r) \longrightarrow H^0(X, \mathcal{D})$ de manera que $\Phi(f) = \frac{f}{x_0^a}$. De las condiciones (i) y (ii) deducimos que D es númericamente efectivo, por lo tanto por el Teorema de Riemann-Roch obtenemos que

$$\dim_{\mathbb{F}_q} H^0(X, \mathcal{D}) = \frac{a^2 + 3a + 2 - \sum_{j=1}^{r} \mu_j (\mu_j - 1)}{2}.$$

Luego, se tiene que el número de puntos de $\left\{Q_1, Q_2, ..., Q_{(q-1)^2}\right\}$ que están en la curva definida por f $(f \in E(a, \mu_1, ..., \mu_r))$ está acotado por $a(q-1)$, lo cual implica que la distancia mínima

$$d \geq (q-1)^2 - a(q-1) = (q-1)(q-1-a).$$

■

Este resultado nos dá la existencia de un código Algebraico Geométrico. Además, como ya se menciono antes, se tiene una cota inferior para la distancia mínima, lo cual es de gran interés, ya que entre más grande posible sea la distancia mínima el código puede detectar y corregir más errores.

Del Teorema 68 se tiene el siguiente Corolario:

Corolario 69 *Sea q una pontencia de un número primo y sean a y μ enteros positivos tales que $\mu \leq a \leq q-2$. Entonces existe un código Algebraico*

Geométrico de longitud $(q-1)^2$*, de dimensión*

$$\frac{a^2+3a+2-\mu(\mu-1)}{2},$$

y con distancia mínima $d \geq (q-1)(q-1-a)$.

Este Corolario contiene resultados de códigos ya existentes los cuales se pueden ver en la Tabla 2.

A continuación tenemos una tabla donde se muestran algunos parámetros de algunos códigos, donde q, a, r, μ_i, k y d son como en el Teorema 68 y $n = (q-1)^2$. En la última columna se muestra el número de errores que puede corregir cada código en el caso de tener como distancia mínima la cota inferior que se está dando. La cota superior de la distancia mínima está dada por la cota de Singleton.

q	a	r	μ_i	(n,k)	Cota Inferior d	Cota Superior d	Cota Inferior $\lfloor \frac{d-1}{2} \rfloor$
3	1	1	$\mu_1 = 1$	$(4,3)$	2	2	0
4	1	1	$\mu_1 = 1$	$(9,3)$	6	7	2
4	2	2	$\mu_1 = 1, \mu_2 = 1$	$(9,6)$	3	4	1
5	1	1	$\mu_1 = 1$	$(16,3)$	12	14	5
5	3	2	$\mu_1 = 1, \mu_2 = 2$	$(16,9)$	4	8	1
7	1	1	$\mu_1 = 1$	$(36,3)$	30	34	14
7	3	2	$\mu_1 = 1, \mu_2 = 2$	$(36,9)$	18	28	8
7	5	5	$\mu_1 = 1, \mu_2 = 1$ $\mu_3 = 1, \mu_4 = 1$ $\mu_5 = 1$	$(36,21)$	6	16	2
9	1	1	$\mu_1 = 1$	$(64,3)$	56	62	27
9	2	1	$\mu_1 = 1$	$(64,6)$	48	60	23
17	2	1	$\mu_1 = 2$	$(256,5)$	224	252	111

Tabla 1: Datos obtenidos del Teorema 68.

Podemos observar en esta tabla que entre más pequeña es a la cota inferior de d es más grande, lo que nos dice que nuestro código de tales parámetros puede corregir más errores.

Los datos de la siguiente tabla fueron obtenidos en www.codetables.de:

q	(n,k)	d	Cota Inferior d	Cota Superior d
3	$(4,3)$	2	2	2
4	$(9,3)$	6	6	6
4	$(9,6)$	3	3	3
5	$(16,3)$	12	12	12
5	$(16,9)$	6	6	6
7	$(36,3)$	30	30	30
7	$(36,9)$	21	21	24
7	$(36,21)$	10	10	13
9	$(64,3)$	56	56	56
9	$(64,6)$	49	49	53

Tabla 2: Datos obtenidos de www.codetables.de.

Tomemos $n = 36$ y $k = 3$. De la Tabla 1 se tiene que existe un $(36,3)-$ *código Algebraico Geométrico* con cota inferior de la distancia mínima 30, este código tiene la posibilidad de que su distancia mínima sea estrictamente mayor que 30, mientras que en la Tabla 2 se muestra que existe un $(36,3)-$ *código lineal* con distancia mínima 30, para este código la distancia mínima ya no puede ser mejorada.

Parte II

Sobre los Anillos de Cox de Superficies

Introducción

Esta parte de mi tesis se refiere a los anillos de Cox de variedades proyectivas lisas, en particular el espacio proyectivo de dimensión arbitraria. Este ha sido un tema en el que me he interesado recientemente. La idea es dar una introducción breve de la noción de anillo de Cox, que es un tema de interés actual, y presentar un problema en el que me interesaría trabajar proximamente. Los anillos de Cox fueron considerados primero por David A. Cox en su artículo [9] para variedades toricas, probando en particular, que el anillo de Cox, denotado por $Cox\,(X)$, de X es una $k-$álgebra finitamente generada, donde k es el campo de definción de la variedad torica X. Posteriormente este concepto se extendio a cualquier variedad por Hu-Keel (ver [10]) en donde plantean el problema sobre la finitud de $Cox\,(X)$ como $k-$álgebra, esto es, ¿para cuales X, $Cox\,(X)$ es finitamente generado?. Ellos han utilizado un ejemplo de Nagata para mostrar que si X es la explosión de $\mathbb{P}^2$ en r puntos en posición general, con $r \geq 9$, entonces $Cox\,(X)$ no es finitamente generado, dejando abierto el problema de clasificar las superficies racionales proyectivas lisas Y tales que $Cox\,(Y)$ es finitamente generado. Hasta ahora se sabe

que si Y es la explosión de r puntos en posición general con $r \leq 8$, $Cox\,(Y)$ es finitamente generado (este tipo de superficies se conocen usualemte como superficies de Del Pezzo), quedando pendiente el problema de las superficies que son explosiones de r puntos no necesariamente en posición general, con $r \leq 8$. En esta dirección, proponemos una conjetura (ver conjetura 119), que se refiere al caso $r \leq 10$.

Esta segunda parte del trabajo se divide en cuatro capítulos.

Capítulo 7: Se presentan nociones generales que se necesitan para definir un divisor de un esquema y se da una relación de equivalencia entre divisores.

Capítulo 8: Se define el anillo de Cox de una variedad proyectiva no singular.

Capítulo 9: Se determina el anillo de Cox del espacio proyectivo de dimensión n y se propone una conjetura sobre la finitud del anillo de Cox de algunas superficies racionales.

Capítulo 7

Divisores y Equivalencia Lineal

En este capítulo introduciremos brevemente las nociones de divisor de un esquema algebraico X y la relación de equivalencia lineal entre divisores, que nos servirán para definir el anillo de Cox en el siguiente capítulo. Iniciaremos explicando la terminología y las técnicas que emplearemos.

7.1 Anillos de valoración discreta

Definición 70 *Sea K un campo, una valoración discreta v de K es una función*

$$v : K^* \longrightarrow \mathbb{Z},$$

donde $K^* = K \setminus \{0\}$, que satisface:

(i) $v(a+b) \geq \min\{v(a), v(b)\}$.

(ii) $v(ab) = v(a) + v(b)$.

Luego, el siguiente Lema muestra que para cada valoración discreta de K es posible asociarle un subanillo de K:

Lema 71 *Sea v una valoración discreta de K, el conjunto R_v definido por:*

$$R_v = \{0\} \cup \{f \in K^* \mid v(f) \geq 0\},$$

es un subanillo de K. Además es un anillo local. Más aun es un anillo de ideales principales.

Demostración. Un bosquejo de la demostración se encuentra en las páginas 94 y 95 de [1]. ■

Definición 72 *Si R es un dominio entero, se dice que R es un anillo de valoración discreta si existe una valoración v, para el campo de fracciones $Q(R)$ de R tal que $R_v = R$.*

Notese que si R es un anillo de valoración discreta cuya valoración es v, entonces el ideal maximal de R_v es de la forma

$$\mathfrak{M} = \{0\} \cup \{f \in R_v \mid v(f) \geq 1\}$$

y todos los ideales de R_v tienen la forma

$$I_n = \{0\} \cup \{f \in R_v \mid v(f) \geq n\}$$

con $n \geq 1$.

Además, $f \in R_v$ es unidad si y sólo si $v(f) = 0$.

7.2 Gavillas

Se puede definir gavillas sobre espacios topológicos de la manera siguiente:

Definición 73 *Una gavilla $\mathcal{F}$ sobre un espacio topológico X es una asignación $U \longmapsto \mathcal{F}(U)$, para cada abierto U de X, de un conjunto de funciones $\mathcal{F}(U)$, de manera que estas funciones estan definidas sobre U y su codominio es un conjunto fijo para toda U. Además se debe satisfacer lo siguiente:*

(i) Para cada subconjunto abierto V de U, la aplicación restricción

$$res_V^U : \mathcal{F}(U) \longrightarrow \mathcal{F}(V),$$

dada por $res_V^U(\sigma) := \sigma|_V$ esta bien definida.

(ii) Si $\{U_i\}_{i\in I}$ es una familia de abiertos de X, dada $\sigma_i \in \mathcal{F}(U_i)$ para todo $i \in I$ tal que $\sigma_i|_{U_i\cap U_j} = \sigma_j|_{U_i\cap U_j}$, entonces existe $\sigma \in \mathcal{F}\left(\bigcup_{i\in I} U_i\right)$ tal que $\sigma|_{U_i} = \sigma_i$ para todo $i \in I$.

Observación 74 *Los elementos de $\mathcal{F}(U)$ se llaman secciones de $\mathcal{F}$ sobre U. Generalmente $\mathcal{F}(U)$ tienen una estructura adicional, por ejemplo grupos, anillos, etc., y hablamos de gavillas de grupos, anillos, respectivamente. En estas situaciones se pide que las restricciones res_V^U sean morfismos de grupos, anillos, respectivamente.*

Definición 75 *Sean $\mathcal{F}$ y $\mathcal{G}$ gavillas sobre un espacio topologico X. Un morfismo de gavillas $\Psi : \mathcal{F} \longrightarrow \mathcal{G}$ es una familia de morfismos $\Psi[U]$:*

$\mathcal{F}(U) \longrightarrow \mathcal{G}(U)$, *para cada abierto* $U \subset X$, *tal que si* $V \subset U$ *es otro abierto, el siguiente diagrama conmuta*

$$\begin{array}{ccc} \mathcal{F}(U) & \xrightarrow{\Psi[U]} & \mathcal{G}(U) \\ \downarrow \ res_V^U & & \downarrow \ res_V^U \\ \mathcal{F}(V) & \xrightarrow{\Psi[V]} & \mathcal{G}(V) \end{array}$$

Definición 76 *Sea* $\mathcal{F}$ *una gavilla y sea* $p \in X$. *El tallo* $\mathcal{F}_p$ *se puede definir como sigue: sean* $\sigma \in \mathcal{F}(U)$, $\sigma' \in \mathcal{F}(U')$, *donde* U *y* U' *son abiertos de* X *tal que* $p \in U \cap U'$. *Decimos que* $\sigma \sim \sigma'$ *si y sólo si existe* $U'' \subseteq U \cap U'$ *tal que* $\sigma|_{U''} = \sigma'|_{U''}$ *con* $p \in U''$. *Entonces*

$$\mathcal{F}_p = \frac{\bigsqcup_{p \in U} \mathcal{F}(U)}{\sim},$$

donde $\bigsqcup$ *denota unión disjunta.*

Definición 77 *Los elementos de* $\mathcal{F}_p$ *se llaman gérmenes. Sea* $\sigma \in \mathcal{F}(U)$, $p \in U$, *el germen de* σ *en* p *es la clase de* σ *en* $\mathcal{F}_p$ *y se denota por* σ_p.

7.3 Esquemas

A continuación se construirá el espacio espectro asociado a un anillo R, usualmente denotado por *Spec* R. El *Spec* R se define como el conjunto de todos los ideales primos de R. Si I es cualquier ideal de R, entonces definimos el subconjunto $V(I) \subseteq Spec\ R$ a ser el conjunto de todos los ideales primos que contienen a I. El radical de un ideal I de un anillo R se define como el conjunto

$$Rad(I) = \{x \in R \mid \exists\ r \in \mathbb{N} \text{ tal que } x^r \in I\}.$$

El siguiente lema es fácil de verificar.

Lema 78 *Sea R un anillo.*

(i) Si I y J son dos ideales de R, entonces $V(IJ) = V(I) \cup V(J)$.

(ii) Si $\{I_j\}$ es cualquier conjunto de ideales de R, entonces

$$V\left(\sum I_j\right) = \bigcap V(I_j).$$

(iii) Si I y J son dos ideales de R, se tiene que $V(I) \subseteq V(J)$ si y sólo si $Rad\ (J) \subseteq Rad\ (I)$.

Ahora definiremos una topología sobre $Spec\ R$, definida por: tomando como subconjuntos cerrados a los subconjuntos $V(I)$ donde I es un ideal de R.

Es obvio que $V(R) = \varnothing$ y $V((0)) = Spec\ R$. El lema anterior muestra que estos subconjuntos cerrados definen una topología sobre $Spec\ R$, llamada topología de Zariski.

Lo siguiente es definir una gavilla de anillos O sobre $Spec\ R$. Para cada ideal primo $P \subseteq R$, sea R_P la localización de R en P. Para un conjunto abierto $U \subseteq Spec\ R$, se define $O(U)$ como el conjunto de funciones

$$\sigma : U \longrightarrow \bigsqcup_{P \in U} R_P,$$

de modo que $\sigma(P)$ es un elemento de R_P para cada P en U, y tal que σ es localmente un cociente de elementos de R, es decir, se requiere que para cada

$P \in U$, exista una vecindad $V \subseteq U$ de P, y elementos $a, f \in R$, tal que para cada $Q \in V$, $f \notin Q$, y $\sigma(Q) = \frac{a}{f}$ en R_P.

Es claro que la suma y el producto de tales funciones son de nuevo este tipo de funciones, y que el elemento 1 el cual da 1 en cada R_P es la identidad de $O(U)$. De esto $O(U)$ es un anillo conmutativo con identidad. Además, si $V \subseteq U$ son dos conjuntos abiertos, el mapeo natural restricción $O(U) \longrightarrow O(V)$ es un homomorfismo de anillos. Se puede verificar que O es una gavilla sobre $Spec\ R$ que se llama la gavilla estructural de R.

Definición 79 *Sea R un anillo. El espectro de R es el par $(Spec\ R, O)$ consistiendo del espacio topologico Spec R junto con la gavilla de anillos O anteriormente definida.*

Definición 80 *Un espacio anillado es un par (X, O_X), donde X es un espacio topológico y O_X es una gavilla de anillos sobre X. Dado $U \subset X$ abierto tenemos un espacio anillado $\left(U, O_{X|_U}\right)$, donde $O_{X|_U}(V) := O_X(V)$ para todo abierto $V \subset U$. Un esquema es un espacio anillado (X, O_X), de manera que X tiene una cubierta abierta $\{U_i\}_{i \in I}$ tal que $\left(U_i, O_{X|_{U_i}}\right)$ es el espectro de $O_X(U_i)$. Por simplicidad nos referiremos al esquema (X, O_X) simplemente como X.*

Ejemplo 81 *El primer ejemplo de esquema que tenemos es el espectro de un anillo. De hecho, los espectros de anillos se conocen como esquemas afines.*

Lema 82 *Dado un punto x de un esquema X, el tallo $O_{X,x}$ es un anillo local, al que nos referiremos como el anillo local de x.*

Demostración. Ver capítulo II Proposición 2.3 página 73 de [2]. ■

Definición 83 *Sea $f : X \longrightarrow Y$ una función continua sobre espacios topológicos. Dada $\mathcal{F}$ una gavilla sobre X, se puede definir una gavilla sobre Y, denotada por $f_*\mathcal{F}$, la imagen directa de $\mathcal{F}$ bajo f, definiendo*

$$(f_*\mathcal{F})(V) = \mathcal{F}\left(f^{-1}(V)\right),$$

para todo $V \subset Y$ abierto.

Definición 84 *Sean (X, O_X), (Y, O_Y) esquemas, un morfismo de esquemas $F : (X, O_X) \longrightarrow (Y, O_Y)$ consiste de una función continua $f : X \longrightarrow Y$ y morfismo de gavillas $f^{\#} : O_Y \longrightarrow f_*O_X$ tal que el morfismo inducido en los tallos $f_p : O_{Y,f(p)} \longrightarrow O_{X,p}$ para todo $p \in X$ es un morfismo local (esto es, la imagen inversa del ideal máximo de $O_{X,p}$ es el ideal máximo de $O_{Y,f(p)}$).*

Por simplicidad vamos a denotar el morfismo de esquemas F simplemente por $f : X \longrightarrow Y$.

Definición 85 *Un morfismo de esquemas $f : X \longrightarrow Y$ es una inmersión cerrada si como función continua es inmersión cerrada y además se tiene que el morfismo $f^{\#} : O_Y \longrightarrow f_*O_X$ es suprayectivo, esto es que los morfismos inducidos en los tallos sean suprayectivos.*

La siguiente noción que necesitamos es la de dimensión de un espacio topológico X.

Definición 86 *Un conjunto $Y \subseteq X$ es irreducible si y sólo si $Y = Y_1 \cup Y_2$, donde Y_1, Y_2 son subconjuntos cerrados no vacios, entonces $Y = Y_1$ o $Y = Y_2$.*

Definición 87 *Si* $\varnothing \neq Y_0 \subsetneq Y_1 \subsetneq \cdots \subsetneq Y_n \subseteq X$ *es una cadena de conjuntos irreducibles, decimos que la cadena tiene longitud* n.

Definición 88 *Sea* X *un espacio topológico. La dimensión de* X *se define por el supremo de las longitudes de cadenas de longitudes finitas de subconjuntos cerrados irreducibles de* X.

Ahora continuaremos con algunas propiedades de esquema que serán de gran utilidad.

Definición 89 *Un esquema* X *es conexo, si como espacio topológico es conexo. Un esquema* X *es irreducible si lo es como espacio topológico.*

Definición 90 *Un esquema* X *es reducido si para cada conjunto abierto* U, *el anillo* $O_X(U)$ *no tiene elementos nilpotentes. Equivalentemente,* X *es reducido si y sólo si los anillos locales* $O_{X,p}$, *para todo* $p \in X$, *no tienen elementos nilpotentes.*

Definición 91 *Un esquema* X *es entero si para cada conjunto abierto* U *en* X, *el anillo* $O_X(U)$ *es un dominio entero.*

Proposición 92 *Un esquema* X *es entero si y sólo si es reducido e irreducible.*

Demostración. Una demostración a esta Proposición se puede encontrar en el capítulo II sección 3 en la Proposición 3.1 de [2]. ■

Definición 93 *Si Y es un subconjunto irreducible cerrado, entonces un punto genérico de Y es un punto $y \in Y$ tal que $\overline{\{y\}} = Y$. Si X es un esquema, entonces todo subconjunto cerrado irreducible $Y \neq \varnothing$ tiene un único punto genérico.*

Definición 94 *Un espacio topológico X es Noetheriano si toda cada descendente de subconjuntos cerrados se estaciona.*

Definición 95 *Un esquema X es localmente Noetheriano, si dado $U \subset X$ abierto tal que $\left(U, O_{X|_U}\right)$ es el espectro de $O_X(U)$, entonces $O_X(U)$ es un anillo noetheriano.*

Definición 96 *Se dice que un esquema X es noetheriano si, es localmente noetheriano y como espacio topologico es cuasi-compacto (para nosotros cuasi-compacto quiere decir que toda cubierta abierta admite una subcubierta finita).*

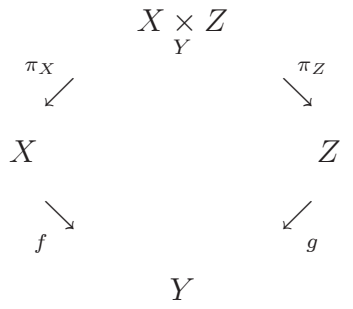
Definición 97 *Un esquema sobre Y consiste de un esquema X, y un morfismo de esquemas $f : X \longrightarrow Y$, y se denota por (X, f).*

Definición 98 *Si (X, f), (Z, g) son esquemas sobre Y, entonces un morfismo $H : (X, f) \longrightarrow (Z, g)$, es un morfismo de esquemas $h : X \longrightarrow Z$, que es compatible con la estructura de esquemas sobre Y, esto es $f = g \circ h$.*

En la categoría de esquemas algebraicos existen los productos fibrados, esto es, dados $f : X \longrightarrow Y$, $g : Z \longrightarrow Y$ dos morfismos de esquemas existe un esquema $X \underset{Y}{\times} Z$, equipado con morfismos

$$\pi_X : X \underset{Y}{\times} Z \longrightarrow X, \ \ \pi_Y : X \underset{Y}{\times} Z \longrightarrow Z,$$

tales que el siguiente diagrama conmuta

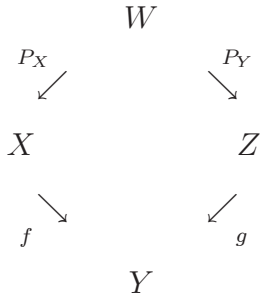


y además se satisface la propiedad universal del producto fibrado:

dados morfismos de esquemas

$$P_X : W \longrightarrow X,\ P_Z : W \longrightarrow Z,$$

tales que el siguiente diagrama conmuta



entonces existe un único morfismo $\varphi : W \longrightarrow X \underset{Y}{\times} Z$ tal que $P_X = \pi_X \circ \varphi$ y $P_Z = \pi_Z \circ \varphi$, para una prueba de estos hechos ver capítulo II Teorema 3.3 de [2].

Entonces, dado un morfismo $f : X \longrightarrow Y$ podemos construir el producto fibrado $X \underset{Y}{\times} X$ tomando $g = f$. Además podemos construir un morfismo

$\Delta : X \longrightarrow X \underset{Y}{\times} X$ tal que (tomando $P_X : X \longrightarrow X$, $P_Z : X \longrightarrow X$ como la identidad), $\pi_X \circ \Delta = id_X$, $\pi_Z \circ \Delta = id_X$. Luego, Δ se conoce como e l **morfismo diagonal** de f.

Definición 99 *Sea $f : X \longrightarrow Y$ un morfismo de esquemas. Sea*

$$\Delta : X \longrightarrow X \underset{Y}{\times} X,$$

el morfismo diagonal, f es separado si Δ es una inmersion cerrada. Se dice que un esquema X es separado si X es separado sobre el espectro de $\mathbb{Z}$ (Spec $\mathbb{Z}$). Por ejemplo, los esquemas proyectivos sobre el espectro de un anillo son esquemas separados (ver [2]).

7.4 Divisores de Weil

Ahora asumiremos que nuestro esquema X es noetheriano, entero y separado.

Definición 100 *Un esquema X es regular en codimensión* 1 *si para todo $p \in X$ tal que* $\dim(O_{X,p}) = 1$ *se tiene que $O_{X,p}$ es un anillo de valoración discreta (esto es equivalente a que $O_{X,p}$ sea regular, ver Teorema 6.2A, página 40 de [2]).*

Definición 101 *Sea X esquema. Vamos a definir el campo de funciones $K(X)$ de X como sigue: sea x el punto genérico de X, el anillo local de $x, O_{X,x}$ es un dominio entero, entonces podemos tomar $K(X)$ como el campo de fracciones de $O_{X,x}$.*

Definición 102 *Sea X un esquema. Un subesquema cerrado entero Y de X, (notese que Y es irreducible), es un divisor primo de X si* $\dim(Y) = \dim(X) - 1$. *Se define el grupo de divisores de X, $Div(X)$ como el grupo abeliano libre generado por todos los divisores primos de X. Esto es, dado $D \in Div(X)$ tenemos que D se escribre de manera unica como*

$$D = \sum_{i=1}^{k} a_i Y_i,$$

con Y_i divisor primo y $a_i \in \mathbb{Z}$.

Definición 103 *Un divisor $\sum_{i=1}^{k} a_i Y_i$ en $Div(X)$ se llama efectivo si los $a_i \geq 0$ para todo $1 \leq i \leq k$.*

Ahora vamos a pedir que nuestro esquema X sea regular en codimensión 1. Sea Y un divisor primo de X. Sea $y \in Y$ el punto genérico de Y. Entonces el anillo local de y, $O_{X,y}$ tiene dimensión 1, ya que Y tiene codimensión 1, por lo tanto es un anillo de valoración discreta y podemos hablar de la valoración v_Y de Y.

Definición 104 *Dada $f \in K(X)^*$, el divisor asociado a f se define como*

$$(f) := \sum_{Y \subset X} v_Y(f)\, Y,$$

donde la suma corre sobre todos los divisores primos Y de X.

Lema 105 *Sea $f \in K(X)^*$, se tiene que $v_Y(f) = 0$ excepto para un número finito de divisores primos Y de X.*

Demostración. Una demostración se encuentra en el capítulo II Lema 6.1 de [2]. ■

Por lo tanto (f) es un elemento de $Div(X)$.

Definición 106 *Sean* $D_1,\ D_2 \in Div(X)$, *decimos que* D_1 *y* D_2 *son linealmente equivalentes,* $D_1 \sim D_2$ *si y solo si existe* $f \in K(X)^*$ *tal que* $D_1 - D_2 = (f)$.

Veamos que esta relación $\sim$ define una relación de equivalencia:

(i) Sea $D \in Div(X)$, si tomamos $1 \in K(X)$, entonces el divisor asociado a 1 es

$$(1) = \sum_{Y \subset X} v_Y(1)\, Y,$$

de las propiedades de la valoración se tiene que $v_Y(1) = 0$, lo que implica que $D - D = (1) = 0$. Por lo tanto $D \sim D$.

(ii) Sean $D_1, D_2 \in Div(X)$, si $D_1 \sim D_2$, por demostrar que $D_2 \sim D_1$. Luego, existe $f \in K(X)^*$ tal que $D_1 - D_2 = (f)$, de esto $D_2 - D_1 = -(f) = \left(\frac{1}{f}\right)$.

(iii) Sean $D_1, D_2, D_3 \in Div(X)$. Si $D_1 \sim D_2$ y $D_2 \sim D_3$, entonces debe pasar que $D_1 \sim D_3$. Se tiene que existen $f, g \in K(X)^*$ tales que $D_1 - D_2 = (f)$ y $D_2 - D_3 = (g)$, luego $D_1 - D_3 = (f) + (g)$. Por otro

lado

$$\begin{aligned}(f)+(g) &= \sum_{Y\subset X} v_Y(f)\,Y + \sum_{Y\subset X} v_Y(g)\,Y \\ &= \sum_{Y\subset X} \left(v_Y(f)+v_y(g)\right)Y \\ &= \sum_{Y\subset X} v_Y(fg)\,Y,\end{aligned}$$

por lo tanto $D_1 - D_3 = (fg)$.

De ahora en adelante vamos a suponer que nuestro esquema X es no singular (regular). De este modo el grupo de divisores de X módulo la relación de equivalencia lineal coincide con el grupo de Picard de X, $Pic(X)$. Y esta será la definición de grupo de Picard que adoptaremos nosotros, esto es

$$Pic(X) = \frac{Div(X)}{\sim}.$$

Notación 107 *Si $D \in Div(X)$, entonces denotaremos la clase de D en $Pic(X)$ por $O_X(D)$. Además consideraremos a $Pic(X)$ como un grupo multiplicativo bajo la operación de producto tensorial, esto es*

$$O_X(D_1+D_2) = O_X(D_1)\otimes O_X(D_2),$$

$$O_X(-D_1) = O_X(D_1)^{-1},$$

$$O_X(0) = O_X,$$

donde $D_1, D_2 \in Div(X)$.

Capítulo 8

Anillos de Cox

Estamos casi listos para definir el anillo de Cox de una variedad. Ahora vamos a suponer que nuestro esquema X es una variedad proyectiva no singular definida sobre un campo algebraicamente cerrado k. Notese que $K(X)$ es una extensión de k, más aún $k \subset O_{X,x}$ para todo $x \in X$.

8.1 Sistemas lineales de divisores

Primero necesitamos la siguiente definición:

Definición 108 *Dado $\ell \in Pic(X)$, sea $D \in Div(X)$ un representante, esto es $\ell = O_X(D)$, a (ℓ, D) le vamos a asociar un espacio vectorial $H^0(X, \ell) \subset K(X)$, dado por*

$$H^0(X,\ell) := \{f \in K(X)^* \mid D + (f) \text{ es un divisor efectivo}\} \cup \{0\}.$$

Lema 109 *Para cada* $\ell \in Pic(X)$, *se tiene que* $H^0(X,\ell)$ *es un espacio vectorial sobre* k.

Demostración. Por definición $0 \in H^0(X,\ell)$. Ahora sean $f, g \in H^0(X,\ell)$, primero vamos a ver que si $\alpha \in k^*$, entonces $\alpha f \in H^0(X,\ell)$, esto se sigue de que $(\alpha f) = (f)$, pues $v_Y(\alpha f) = v_Y(\alpha) + v_Y(f) = v_Y(f)$, ya que α es una unidad en $O_{X,y}$. Falta ver que $f + g \in H^0(X,\ell)$. Por demostrar que $D + (f+g)$ es un divisor efectivo, supongamos que $D = \sum a_Y Y$, entonces $D + (f+g) = \sum (a_Y + v_Y(f+g)) Y$, y por las propiedades de valoración tenemos que, podemos suponer que $a_Y + v_Y(f+g) \geq a_Y + v_Y(f) \geq 0$, entonces $D + (f+g)$ es efectivo. ■

Observación 110 *En la prueba anterior vimos que* $(\alpha f) = (f)$, *para* $\alpha \in k^*$, *de hecho se tiene que* $(f) = (g)$ *si y sólo si existe* $\alpha \in k^*$ *tal que* $g = \alpha f$ *(ver [2]).*

8.2 Anillo de Cox de variedades

Es el momento de definir el anillo de Cox.

Definición 111 *Para cada* $\ell \in Pic(X)$, *tomemos un representante* $D_\ell \in Div(X)$, $\ell = O_X(D_\ell)$. *Sea* $Cox(X)$ *el grupo abeliano dado por*

$$Cox(X) = \bigoplus_{\ell \in Pic(X)} H^0(X,\ell).$$

Lema 112 $Cox(X)$ *esta equipado con una estructura de anillo.*

Demostración. Consideremos el neutro O_X de $Pic(X)$, para O_X tomamos a $0 \in Div(X)$ como representante, entonces notemos que para toda $f \in k^*$, se tiene que $(f) = 0$. Entonces $k \subset H^0(X, O_X)$ (de hecho $k = H^0(X, O_X)$), en particular tenemos que $1 \in Cox(X)$, y que $Cox(X)$ resultará ser una $k-$álgebra. Para definir el producto, basta definirlo para los elementos de $H^0(X, \ell)$ para todo $\ell \in Pic(X)$. Sean $x_{\ell_i} \in H^0(X, \ell_i)$ con $i = 1, 2$. Ahora consideramos a x_{ℓ_1},x_{ℓ_2} como elementos de $K(X)$, y los multiplicamos usando el producto de $K(X)$. Luego, este producto va a determinar un elemento de $H^0(X, \ell_1 \otimes \ell_2)$, como $\ell_1 \otimes \ell_2 = O_X(D_{\ell_1} + D_{\ell_2})$ solo se necesita mostrar que $D_{\ell_1} + D_{\ell_2} + (x_{\ell_1} \cdot x_{\ell_2})$ es efectivo. Por la propiedades de valoración y la forma de escribir a D_{ℓ_1}, D_{ℓ_2}, se tiene que

$$\begin{aligned} D_{\ell_1} + D_{\ell_2} + (x_{\ell_1} \cdot x_{\ell_2}) &= \sum_{Y \subset X} a_Y Y + \sum_{Y \subset X} b_Y Y + \sum_{Y \subset X} v_Y(x_{\ell_1} \cdot x_{\ell_2}) Y \\ &= \sum_{Y \subset X} (a_Y + b_Y) Y + \sum_{Y \subset X} v_Y(x_{\ell_1}) Y + \sum_{Y \subset X} v_Y(x_{\ell_2}) Y \\ &= \sum_{Y \subset X} (a_Y + b_Y + v_Y(x_{\ell_1}) + v_Y(x_{\ell_2})) Y, \end{aligned}$$

donde $a_Y, b_Y \in \mathbb{Z}$, además como $D_{\ell_1} + (x_{\ell_1})$ y $D_{\ell_2} + (x_{\ell_2})$ son efectivos implica que $a_Y + v_Y(x_{\ell_1}) \geq 0$ y $b_Y + v_Y(x_{\ell_2}) \geq 0$, entonces $D_{\ell_1} + D_{\ell_2} + (x_{\ell_1} \cdot x_{\ell_2}) \in H^0(X, \ell_1 \otimes \ell_2)$. ■

Definición 113 *Sea G un semigrupo abeliano. Un anillo R esta graduado por G si pasa lo siguiente: consideremos a R como un $\mathbb{Z} - módulo$ y supongamos que para todo $g \in G$ existe un $\mathbb{Z} - submódulo$ R_g de R, de manera que $R = \bigoplus_{g \in G} R_g$ y se debe satisfacer que dados $r_{g_1} \in R_{g_1}$ y $r_{g_2} \in R_{g_2}$, el producto $r_{g_1} r_{g_2} \in R_{g_1 g_2}$.*

Notese que $Cox\,(X)$ es una $k-$álgebra graduada sobre $Pic\,(X)$. Como mencionamos antes el problema que nos interesa es estudiar si dado X el anillo de Cox de X es finitamente generado como $k-$álgebra.

Capítulo 9

Anillos de Cox de Superficies Racionales

El objetivo de este capítulo es de probar que el anillo de Cox del espacio proyectivo es un anillo de polinomios y sugerir una conjetura sobre la finitud de los anillos de Cox de algunas superficies racionales obtenidas como explosiones del plano proyectivo en r puntos con $r \leq 10$.

9.1 Anillo de Cox del espacio proyectivo $\mathbb{P}^n$

Por definición tenemos que

$$Cox\left(\mathbb{P}^n\right) = \bigoplus_{O_{\mathbb{P}^n}(D) \in Pic(\mathbb{P}^n)} H^0\left(\mathbb{P}^n, O_{\mathbb{P}^n}\left(D\right)\right).$$

Esto sugiere que antes de todo debemos determinar $Pic\left(\mathbb{P}^n\right)$. En efecto, sea $x \in Pic\left(\mathbb{P}^n\right)$, entonces existe $D \in Div\left(\mathbb{P}^n\right)$ tal que $x = O_{\mathbb{P}^n}\left(D\right)$. Como

$D \in Div(\mathbb{P}^n)$, $D = \sum_{i=1}^{r} n_i \Gamma_i$, con $n_i \in \mathbb{Z}$ para $i = 1, ..., r$ y Γ_i un divisor primo de $\mathbb{P}^n$, en este caso cada divisor primo Γ_i es el conjunto de ceros de un polinomio homogeneo irreducible $f_i \in k[x_0, ..., x_n]$ de grado d_i, para toda $i = 1, ..., r$.

Es fácil verificar el siguiente lema.

Lema 114 *$Rank(Pic(\mathbb{P}^n)) = 1$.*

Demostración. Para una demostración de este Lema ver el capítulo II Proposición 6.4 de [2]. ■

En particular podemos decir que $Pic(\mathbb{P}^n) = \mathbb{Z}L$ donde $L = O_{\mathbb{P}^n}(\Gamma_0)$ y Γ_0 es el divisor asociado al polinomio x_0. Si denotamos $O_{\mathbb{P}^n}(m) := O_{\mathbb{P}^n}(m\Gamma_0)$ con $m \in \mathbb{Z}$, entonces dado un divisor arbitrario D podemos escribir $O_{\mathbb{P}^n}(D) = O_{\mathbb{P}^n}(m)$ para algún $m \in \mathbb{Z}$. De esto tenemos que $Cox(\mathbb{P}^n) = \bigoplus_{m \in \mathbb{Z}} H^0(\mathbb{P}^n, O_{\mathbb{P}^n}(m))$.

Lema 115

(*a*) *Si $m = 0$ tenemos que $H^0(\mathbb{P}^n, O_{\mathbb{P}^n}) = k$.*

(*b*) *Si $m < 0$ se tiene que $H^0(\mathbb{P}^n, O_{\mathbb{P}^n}(m)) = \{0\}$.*

Demostración.

(*a*) Esto es porque $\mathbb{P}^n$ es una variedad proyectiva.

(*b*) Puesto que el grado de (f) para todo $f \in K(\mathbb{P}^n)^*$ es cero tenemos que $m\Gamma_0 + (f)$ no puede ser efectivo.

■

Por lo anterior podemos considerar $Cox\left(\mathbb{P}^n\right) = \underset{m\in\mathbb{N}}{\oplus} H^0\left(\mathbb{P}^n, O_{\mathbb{P}^n}\left(m\right)\right)$.

Lema 116 $\underset{m\in\mathbb{N}}{\oplus} H^0\left(\mathbb{P}^n, O_{\mathbb{P}^n}\left(m\right)\right) \cong k\left[x_0, ..., x_n\right]$

Demostración. La desmostración se tiene de que $H^0\left(\mathbb{P}^n, O_{\mathbb{P}^n}\left(m\right)\right)$ es isomorfo al espacio de polinomios homogéneos de grado m, bajo el mapeo $f \longmapsto x_0^m f$. ■

Teorema 117 $Cox\left(\mathbb{P}^n\right) \cong k\left[x_0, ..., x_n\right]$.

Demostración. Por los dos Lemas anteriores se tiene la demostración. ■

Corolario 118 $Cox\left(\mathbb{P}^2\right) \cong k\left[x_0, x_1, x_2\right]$.

9.2 Anillos de Cox de superficies racionales

De este hecho queremos estudiar $Cox\left(X\right)$, donde X es una explosión de un número finito de puntos de $\mathbb{P}^2$. Denotemos por $Bl_n\left(\mathbb{P}^2\right)$ a la explosión de n puntos en $\mathbb{P}^2$. En esta dirección daremos la siguiente conjutura:

Conjetura 119 *Sea* $X = Bl_{10}\left(\mathbb{P}^2\right)$. $Cox\left(X\right)$ *es finitamente generado si y solo el número de todas las curvas* (-1) *y de todas las curvas* (-2) *en* X *es finito, donde una curva* (-1) *(resp. una curva* (-2)*) es un divisor primo regular racional* Γ *en* X *de auto-intersección -1 (resp. -2).*

Notese que si X es una superficie obtenida como explosiones del plano proyectivo en r puntos con $r \leq 8$, el número total de curvas (-1) y de curvas (-2) es finito. Entonces, de nuestra conjetura, en caso de ser verdadera, se deduce inmediatamente el hecho de que los anillos de Cox de superficies de Del Pezzo son finitamente generados.

Conclusiones

Este trabajo me ha permitido construir un código utilizando la geometría de una superficie racional. Me gustaría dedicarme a constuir otros códigos utilizando superficies que no son solamente obtenidas por explosines del plano proyectivo. Y también me gustaría dedicarme a dar una prueba a mi Conjetura 119 presentada en el capítulo 9.

Bibliografía

[1] M. F. Atiyah, I. G. Macdonald. Introduction to Commutative Algebra. Addison-wesley, 1969.

[2] R. Hartshorne. Algebraic Geometry. Springer Verlag, 1977.

[3] D. G. Hoffman, D. A. Leonard, C. C. Lindner, K. T. Phelps, C. A. Rodger, J. R. Wall. Coding Theory. The Essentials. Marcel Dekker, 1991.

[4] R. Kaye, R. Wilson. Linear Algebra. Oxford University Press, 1998.

[5] S. Ling, C. Xing. Coding Theory. A First Course. Cambridge University Press, 2004.

[6] J. H. van Lint. Introduction to Coding Theory. Springer Verlag, 1999.

[7] O. Pretzel. Error-Correcting Codes and Finite Fields. Oxford University Press, 1992.

[8] J. J. Rotman. Advanced Modern Algebra. Prentice Hall, 2002.

[9] Cox, David A.(1-AMH-MC). The homogeneous coordinate ring of a toric variety. J. Algebraic Geom. 4 (1995), no. 1, 17–50.

[10] Hu, Yi; Keel, Sean Mori dream spaces and GIT. Dedicated to William Fulton on the occasion of his 60th birthday. Michigan Math. J. 48 (2000), 331–348.

[11] S. A. Vanstone, P. C. van Oorshot. An introduction to error correcting codes with applications. Kluwer Academic Publishers, 1989.