INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE FÍSICA Y MATEMÁTICAS

CÓDIGOS ASOCIADOS A ALGUNAS MATRICES

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN FÍSICA Y MATEMÁTICAS

PRESENTA:

ELISEO SARMIENTO ROSALES

ASESOR:

DR. CARLOS RENTERÍA MARQUEZ

ASESOR EXTERNO:

DR. MANUEL GONZALEZ SARABIA

Índice general

Introducción

La Teoría de códigos es una rama de las matemáticas y de la computación que se ocupa de la transmisión de información y posteriormente detectar errores en la información recibida. Sus inicios datan de 1948 cuando Claude Shannon, trabajando en los Laboratorios Bell (Estados Unidos), inauguró la disciplina publicando un trabajo llamado A Mathematical Theory of Communication, donde sentó las bases para la corrección de errores, supresión de ruidos y redundancia.

En 1950 Richard Hamming, también de los Laboratorios Bell, publicó detalles de su trabajo sobre códigos de corrección de errores explícitos con tasas de transmisión de información más eficientes que la simple repetición. Se dice que Hamming inventó este código después de varios intentos de perforar un mensaje en una cinta de papel usando el código de paridad.

Mientras Shannon y Hamming trabajaban sobre la transmisión de la información en los Estados Unidos, John Leech ideó códigos similares al investigar sobre teoría de grupos en Cambridge (Reino Unido).

El trabajo aquí presentado es sobre códigos que se pueden obtener a través de una función evaluación y que se asocian a matrices particulares. Es importante decir que se ha dividido en tres partes, comenzando por el primer y segundo capítulo que trata sobre teoría que nos ayudará a comprender los resultados posteriores; el primer capítulo trata sobre Variedades Algebraicas y algunas variedades particulares, y aunque no es el objetivo prioritario se han resuelto algunos ejercicios importantes. En el segundo capítulo se definen los códigos que usaremos, sus parámetros básicos y se definen funciones para los cálculos; al final hablamos sobre los ideales tóricos asociados a matrices.

La segunda parte es el tercer capítulo de la tesis, donde se enumeran los resultados que se obtuvieron a lo largo de una investigación de los doctores

Manuel González Sarabia y Carlos Rentería Márquez; pero se les da una explicación mas amplia a los detalles para que cualquier alumno con los conceptos básicos sea capaz de comprenderlo. En la última parte y en este caso el último capítulo se describe un programa en Macaulay que sirvió para encontrar los resultados a lo largo de la investigación arriba mencionada y se dan dos ejemplos de matrices usando primero el programa y luego verificando los resultados principales.

Agradecimientos

Comenzaré agradeciendo a mis padres: Amelia Rosales Flores y Pablo Sarmiento Morales, ya que fueron las personas que creyeron en mi desde el inicio de mi vida y con este proyecto de estudiar Matemáticas. También a mis hermanos Moisés y Noé ya que son y seguirán siendo mis amigos.

A mis tías, mis tíos y a mis primos, los cuales me han adoptado en su familia y se que siempre están dandome consejos para ser una mejor persona.

A mi mejor amiga, mi inspiración y la chica que me ayudó a poner mi vida en total equilibrio, a mi novia Mayra Itandehui Aguilera.

A mis amigos, a las personas que han sido capaces de soportarme sin tener ningún vínculo familiar, pero sobre todo de los que me he ganado su confianza, su respeto y saben que cuentan conmigo en cualquier situación, en especial a los que me han ayudado a lo largo de mi carrera.

Al final, las dos personalidades de las que más he recibido ayuda como alumno, pero también como futuro investigador. Comienzo con la persona que me ayudó en la primera mitad de la licenciatura, el profesor que notó un poco (espero que no sea tan poco) de talento en mí, también es la persona que me ayudó a tomar la difícil decisión de no salirme de la Licenciatura, el Dr. Manuel González Sarabia que aunque sólo tomé dos cursos con él fueron suficientes para que jamás dejara el área de las matemáticas que más me gusta: Álgebra.

Y la segunda personalidad es actualmente casi mi guía intelectual, el cual me ha ayudado a tomar decisiones académicas a lo largo de los últimos semestres, pero sobre todo se que tengo su apoyo incondicional y más aún, el tener un investigador de su nivel apoyando mi carrera habla muy bien de mi: Dr. Carlos Rentería Márquez.

Gracias a todas las personas que me han ayudado, pero más en especial a las últimas dos personas que mencioné, ya que espero algún día ser (como cualquier buen alumno) mejor que ellos; aunque se que es casi imposible.

Capítulo 1

Variedades afines y proyectivas

En este capítulo estudiaremos las definiciones más importantes sobre variedades afines y proyectivas, revisaremos algunos de los ejemplos más comunes que nos ayudarán en resultados posteriores.

1.1. Variedades Afines

Sea K un campo algebraicamente cerrado, definimos al n-espacio afín sobre K como el conjunto de las n-adas de elementos de K y lo denotamos como $\mathbb{A}^n_k$ o simplemente $\mathbb{A}^n$. Un elemento $\mathrm{P} \in \mathbb{A}^n$ se llamará *punto* y si $\mathrm{P} = (a_1, a_2, a_3, \ldots, a_n)$ con $a_i \in K$ entonces los a_i se llamarán *coordenadas* de P.

Sea $A = K[x_1, x_2, \ldots, x_n]$ el anillo de polinomios en n variables sobre K. Veremos a los elementos de A como funciones del n-espacio afín de K y definiendo $f(\mathrm{P}) = f(a_1, a_2, a_3, \ldots, a_n)$, $f \in A$ y $\mathrm{P} \in \mathbb{A}^n$. Así si $f \in A$ es un polinomio, podremos tomar el conjunto de ceros de f, y lo denotaremos por: $\mathbf{Z}(f) = \{\ \mathrm{P} \in \mathbb{A}^n \mid f(\mathrm{P}) = 0\ \}$. En general si T es un subconjunto de A, definiremos al *conjunto de ceros* de T como:

$$\mathbf{Z}(\mathrm{T}) = \{\ \mathrm{P} \in \mathbb{A}^n \mid f(\mathrm{P}) = 0, \text{ para todo } f \in \mathrm{T}\ \}$$

Es fácil ver que si a es el ideal de A generado por T, entonces $\mathbf{Z}(\mathrm{T}) = \mathbf{Z}(a)$. Además como A es un anillo noetheriano, todo ideal a tiene un conjunto finito de generadores $f_1, f_2, \ldots, f_r$. Así, $\mathbf{Z}(\mathrm{T})$ puede ser expresado como los ceros comunes de un conjunto finito de polinomios $f_1, f_2, \ldots, f_r$.

Definición* 1.1** *Un subconjunto Y de $\mathbb{A}^n$ es un* ***conjunto algebraico *si hay un subconjunto $T \subseteq A$ tal que $Y = \boldsymbol{Z}(T)$.*

***Proposición* 1.1** *La unión de dos conjuntos algebraicos es un conjunto algebraico. La intersección de cualquier familia de conjuntos algebraicos es un conjunto algebraico. El conjunto vacío y el total son conjuntos algebraicos.*

Demostración. Si $Y_1 = \mathbf{Z}(T_1)$ y $Y_2 = \mathbf{Z}(T_2)$, entonces $Y_1 \cup Y_2 = \mathbf{Z}(T_1T_2)$ ya que si P $\in Y_1 \cup Y_2$ entonces P es cero de cualquier producto de elementos de T_1 y T_2. Recíprocamente si P $\in$ $\mathbf{Z}(T_1T_2)$ y P$\notin Y_1$ entonces existe un f $\in T_1$ tal que f (P) $= 0$, pero como (fg) (P)$= 0$ con $g \in T_2$ entonces g (P) $=$ 0 y P $\in Y_2$.

Si $Y_\alpha = \mathbf{Z}(T_\alpha)$ es cualquier familia de conjuntos algebraicos es evidente que $\bigcap Y_\alpha = \mathbf{Z}(\bigcup T_\alpha)$, entonces $\bigcap Y_\alpha$ es también un conjunto algebraico. Para terminar, $\emptyset = \mathbf{Z}(1)$, $\mathbb{A}^n = \mathbf{Z}(0)$. ■

***Definición* 1.2** *Definimos la* **Topología de Zariski** *en $\mathbb{A}^n$ tomando a los subconjuntos abiertos como los complementos de los conjuntos algebraicos. Es fácil ver que, por la proposición anterior, es un topología.*

Ejemplo 1.1 *Consideremos la Topología de Zariski en la recta afín $\mathbb{A}^1$. Como $K[x]$ es un Dominio de Ideales Principales (DIP), luego todo ideal en $A = K[x]$ es principal, lo que significa que cualquier conjunto algebraico al ser el conjunto de ceros de algún ideal, será el conjunto de ceros de un único polinomio. Como pedimos que k fuera un campo algebraicamente cerrado, luego cualquier polinomio se puede escribir de la siguiente manera: $f(x) = c(x-a_1)\dots(x-a_n)$ con $c, a_1, \dots, a_n \in k$; lo que significa que $Z(f) = \{a_1, \dots, a_n\}$. Así los conjuntos algebraicos de $\mathbb{A}^1$ son solamente los conjuntos finitos, el vacío y el total, entonces los abiertos son los complementos de los conjuntos finitos, el vacío y el total; dicha topología es la Topología cofinita. Es importante darse cuenta que dados dos puntos en $\mathbb{A}^1$ no existen dos abiertos disjuntos que lo contengan respectivamente, luego nuestra Topología no es Hausdorff.*

Definición* 1.3** *Un subconjunto Y no vacío de un espacio topológico* `X` *es* ***irreducible *si no puede ser expresado como la unión de dos subconjuntos propios, cada uno cerrado en Y. El vacío no es considerado como irreducible.*

Ejemplo 1.2 $\mathbb{A}^1$ *es un conjunto irreducible, ya que sus únicos cerrados distintos del total son finitos, luego no puede ser unión de dos cerrados ya que k es un campo algebraicamente cerrado, entonces infinito.*

Ejemplo 1.3 *Todo subconjunto abierto no vacío de un espacio irreducible es denso e irreducible.*

Sea X un espacio irreducible, tomemos un subconjunto propio abierto O $\subset X$ *distinto del vacío, primero demostremos que O es irreducible por contraposición. Supongamos que O no es irreducible, luego existen F y G cerrados de X, tales que* $O = (O \cap F) \cup (O \cap G)$*, como X es irreducible* $F \cup G \neq X$*, luego* O^c *es un subconjunto propio cerrado de X, luego es fácil ver:* $X = (F \cup G) \cup O^c$*, lo que es una contradicción, luego se concluye que O es irreducible.*

Ahora demostremos la densidad de O, sea U un abierto de X distinto del vacío, si $U = X$ *tenemos:* $O \cap U \neq \emptyset$*. Ahora si* $U \neq X$*, como X es irreducible* $O^c \cup U^c \neq X \Rightarrow (O^c \cup U^c)^c \neq \emptyset \Rightarrow (O \cap U) \neq \emptyset$*, luego O tiene intersección distinta del vacío con cualquier abierto de X, entonces O es denso en X.*

Ejemplo 1.4 *Si Y es un subconjunto irreducible de X, entonces su cerradura* $\overline{Y}$ *en X es también irreducible.*

Supongamos que Y es un subconjunto irreducible de X, y supongamos que $\overline{Y}$ *no es irreducible, luego existen F y G cerrados en X, tales que si* $U = F \cap \overline{Y}$ *y* $V = G \cap \overline{Y}$*, entonces:* $Y \subset \overline{Y} = U \cup V$*, entonces veamos que si* $U \cap Y = \emptyset$*, luego* $Y \subset V$*, pero como V es cerrado se tiene* $\overline{Y} \subset V \subset G$*, luego es una contradicción por la forma en que definimos a G, entonces:* $U \cap Y \neq \emptyset$*, de la misma forma se demuestra que* $V \cap Y \neq \emptyset$*, entonces se tiene que* $Y = (U \cap Y) \cup (V \cap Y)$*, lo que es una contradicción por la irreducibilidad de Y. Por lo tanto* $\overline{Y}$ *es irreducible.*

Definición* 1.4** *Una* ***Variedad Algebraica Afín *o simplemente* ***Variedad Afín*** *es un subconjunto cerrado e irreducible de* $\mathbb{A}^n$ *con la topología inducida. Un subconjunto abierto de una variedad afín es una* ***variedad quasi-afín****.*

Ahora podemos explorar un poco mas las relaciones entre subconjuntos de $\mathbb{A}^n$ e ideales en A. Para cualquier subconjunto $\mathrm{Y} \subseteq \mathbb{A}^n$ definimos el *ideal* de Y en A por:

$$\mathbf{I}(\mathrm{Y}) = \{\ f \in A \mid f\ (\mathrm{P}) = 0 \quad \forall\ \mathrm{P} \in Y\}$$

Ahora tenemos una función Z la cual mapea subconjuntos de A en conjuntos algebraicos y una función $\mathbf{I}$ la cual mapea subconjuntos de $\mathbb{A}^n$ en ideales. Y sus propiedades son:

***Proposición* 1.2**

1. *Si $T_1 \subseteq T_2$ son subconjuntos de A, entonces $\boldsymbol{Z}(T_2) \subseteq \boldsymbol{Z}(T_1)$*
2. *Si $Y_1 \subseteq Y_2$ son subconjuntos de $\mathbb{A}^n$, entonces $\boldsymbol{I}(Y_2) \subseteq \boldsymbol{I}(Y_1)$*
3. *Para cualquiera dos subconjuntos $Y_1, Y_2 \subseteq \mathbb{A}^n$ se cumple que $\boldsymbol{I}(Y_1 \cup Y_2) = \boldsymbol{I}(Y_1) \cap \boldsymbol{I}(Y_2)$*
4. *Para todo ideal $a \subseteq A$, $\boldsymbol{I}(\boldsymbol{Z}(a)) = \sqrt{a}$, donde $\sqrt{a}$ es el radical de a.*
5. *Para todo subconjunto $Y \subseteq \mathbb{A}^n$, $\boldsymbol{Z}(\boldsymbol{I}(Y)) = \overline{Y}$, cerrradura de Y.*

Demostración. Los puntos 1,2 y 3 son obvios, el punto 4 es consecuencia del Teorema de los ceros de Hilbert (el cual se enunciará enseguida).

Para demostrar el punto 5 tomemos Y $\subseteq \mathbf{Z}(\mathbf{I}(\mathrm{Y}))$, como es un conjunto cerrado se cumple que $\overline{Y} \subseteq \mathbf{Z}(\mathbf{I}(\mathrm{Y}))$. Por otra parte sea W un conjunto cerrado que contiene a Y, entonces W $= \mathbf{Z}(a)$, para algún a ideal, pero Y $\subseteq \mathbf{Z}(a)$, y por el punto 2 se tiene que: $\mathbf{I}(\mathbf{Z}(a)) \subseteq \mathbf{I}(\mathrm{Y})$, pero $a \subseteq \mathbf{I}(\mathbf{Z}(a))$ y usando el punto 1 de la proposición se sigue que $\mathbf{Z}(\mathbf{I}(\mathrm{Y})) \subseteq \mathbf{Z}(a)$. ■

***Teorema* 1** *(de los ceros de Hilbert). Sea K un campo algebraicamente cerrado, sea a un ideal en $A = K[x_1, x_2, \ldots, x_n]$, y sea $f \in A$ un polinomio el cual se escinde en $\boldsymbol{Z}(a)$. Entonces $f^r \in a$ para algún entero $r \geq 1$.*

Demostración. M.F.Atiyah-I.G.Macdonald, Introducción al álgebra conmutativa, página 95. ■

***Corolario* 1** *Hay una correspondencia entre los conjuntos algebraicos de $\mathbb{A}^n$ e ideales radicales de A (aquellos ideales que son iguales a sus propios radicales) dado por $Y \mapsto \boldsymbol{I}(Y)$ y $a \mapsto \boldsymbol{Z}(a)$. Además un conjunto algebraico en $\mathbb{A}^n$ es irreducible si y solo si su ideal asociado en A es un ideal primo.*

Demostración. La parte de la correspondecia ya se demostró anteriormente, sólo falta verificar la última parte. Tomamos un Y irreducible y mostraremos que $\mathbf{I}(\mathrm{Y})$ es un ideal primo. Note que si $f\,g \in \mathbf{I}(\mathrm{Y})$, entonces Y $\subseteq \mathbf{Z}(f\,g) = \mathbf{Z}(f) \cup \mathbf{Z}(g)$. Así si Y $= (\ \mathrm{Y} \cap \mathbf{Z}(f)\ ) \cup (\ \mathrm{Y} \cap \mathbf{Z}(g)\ )$, los cuales

son subconjuntos cerrados en Y, pero como Y es irreducible se tiene que para alguno, digamos $\mathbf{Z}(f)$ se tiene que $\mathrm{Y} = \mathrm{Y} \cap \mathbf{Z}(f)$, en cuyo caso $\mathrm{Y} \subseteq \mathbf{Z}(f)$; en caso contrario se debe tener $\mathrm{Y} \subseteq \mathbf{Z}(g)$. Entonces se tiene que $f \subseteq \mathbf{I}(\mathrm{Y})$ o $g \subseteq \mathbf{I}(\mathrm{Y})$, lo que implica que $\mathbf{I}(\mathrm{Y})$ es primo.

Para la otra contención se tiene que si p es un ideal primo, entonces suponemos que $\mathbf{Z}(p) = Y_1 \cup Y_2$, entonces se tiene $p = \mathbf{I}(Y_1) \cap \mathbf{I}(Y_2)$ lo que implica $p = \mathbf{I}(Y_1)$ o $p = \mathbf{I}(Y_2)$. Así $\mathbf{Z}(p) = Y_1$ o $\mathbf{Z}(p) = Y_2$, así $\mathbf{Z}(p)$ es irreducible. ■

Ejemplo 1.5 *$\mathbb{A}^n$ es irreducible, ya que el ideal que le corresponde es el ideal cero en A, el cual es primo.*

Ejemplo 1.6 *Sea f un polinomio irreducible en $A = K[x, y]$, entonces el ideal generado por f es un ideal primo en A, luego como A es un Dominio de Factorización Única el conjunto de ceros $Y = Z(f)$ es irreducible. A Y le llamaremos la curva afín defnida por $f(x, y) = 0$. Si f tiene grado d diremos que Y es una curva de grado d.*

Ejemplo 1.7 *En el caso general sea f un polinomio irreducible en $A = K[x_1, x_2, \ldots, x_n]$, obtendremos una variedad afín $Y = Z(f)$ llamada superficie si $n = 3$, o hypersuperficie si $n \geq 4$.*

Ejemplo 1.8 *Un ideal maximal $\boldsymbol{m}$ de $A = K[x_1, x_2, \ldots, x_n]$ se corresponde con un subconjunto cerrado minimal de $\mathbb{A}^n$, dicho subconjunto solo puede ser un punto $P = (a_1, \ldots, a_n)$, ya que los puntos son los únicos conjuntos cerrados que no contienen subconjuntos propios cerrados. Lo que significa que todo ideal maximal de A es de la forma: $\boldsymbol{m} = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$, para algunos $a_1, \ldots, a_n \in k$.*

Definición* 1.5** *Si $Y \subseteq \mathbb{A}^n$ es un conjunto algebraico afín, definamos al* ***Anillo afín de coordenadas A*(Y) de Y como el cociente A/****I****(Y).*

Notemos que si Y es una variedad afín, entonces $\mathbf{I}(\mathrm{Y})$ será un ideal primo, por lo tanto $A(\mathrm{Y})$ será un dominio entero. Además $A(\mathrm{Y})$ es una K-álgebra finitamente generada. Recíprocamente, toda K-álgebra finitamente generada B que sea un dominio, es el anillo afín de coordenadas de alguna variedad afín J. De hecho B se puede escribir como el cociente de algún anillo de polinomios $A = K[x_1, x_2, \ldots, x_n]$ y algún ideal primo a, entonces $\mathrm{J} = \mathbf{Z}(a)$.

***Definición* 1.6** *Un espacio topológico* $\boldsymbol{X}$ *es llamado noetheriano si satisface la condición de cadena descendente para subconjuntos cerrados: para cualquier sucesión* $Y_1 \supseteq Y_2 \supseteq Y_3 \ldots$ *de subconjuntos cerrados, existe un entero* r *tal que* $Y_r = Y_{r+1} = Y_{r+2} \ldots$

Un ejemplo de un espacio topológico noetheriano es $\mathbb{A}^n$. De hecho si $Y_1 \supseteq Y_2 \supseteq Y_3 \ldots$ es una cadena descendente de subconjuntos cerrados, entonces $\mathbf{I}(Y_1) \subseteq \mathbf{I}(Y_2) \subseteq \ldots$ es una cadena ascendente de ideales en $A = K[x_1, x_2, \ldots, x_n]$. Como A es noetheriano, entonces dicha cadena de ideales es también estacionaria, pero para todo i, $Y_i = \mathbf{Z}(\mathbf{I}(Y_i))$, entonces formando esta nueva cadena será estacionaria.

Proposición* 1.3** *En un espacio topológico noetheriano* $\boldsymbol{X}$*, todo subconjunto cerrado no vacío* Y *puede ser expresado como unión finita* $Y{=}Y_1 \cup Y_2 \cup Y_3 \ldots$ *de subconjuntos cerrados irreducibles* Y_i*. Si además pedimos que* $Y_i \nsubseteq Y_j$ *para todo* $i{\neq}j$*, entonces los* Y_i *están singularmente determinados y se llaman las* ***componentes irreducibles *de* Y*.*

***Demostración*.** Primero mostremos que cualquier Y subconjunto cerrado no vacío se puede escribir como unión de subconjuntos cerrados irreducibles. Sea Ω el conjunto de subconjuntos cerrados no vacíos de $\mathbf{X}$ que no se pueden escribir como unión finita de subconjuntos cerrados irreducibles. Si Ω es no vacío, entonces como $\mathbf{X}$ es noetheriano, debe existir un elemento mínimo, digamos Z. Como Z no puede ser irreducible por construccion de Ω, entonces lo podemos escribir como $Z = Z' \cup Z''$ con Z' y Z'' subconjuntos propios cerrados de Z. Pero por la minimalidad de Z, Z' y Z'' no pueden estar en Ω, o sea se pueden escribir como unión finita de subconjuntos cerrados irreducibles, así Z también es unión finita de subconjuntos cerrados irreducibles lo que es una contradicción. Entonces Ω es vacío, luego todo subconjunto cerrado no vacío cumple la primera parte de la proposición.

Ahora supongamos que existe Y subconjunto cerrado que tiene dos representaciones de sunconjuntos maximales diferentes: $Y{=}Y_1 \cup Y_2 \cup Y_3 \ldots Y_n$, $Y{=}Y_1' \cup Y_2' \cup Y_3' \ldots Y_r'$. Entonces $Y_1' \subseteq Y{=}Y_1 \cup Y_2 \cup Y_3 \ldots Y_n$, entonces $Y_1' = \bigcup(Y_1' \cap Y_i)$. Luego por ser Y_1' irreducible se tiene que $Y_1' \subseteq Y_i$ para algún i. Sin pérdida de generalidad supongamos que es para $i{=}1$. Procediendo de la misma manera podemos llegar a $Y_1 \subseteq Y_j'$, luego usando la transitividad de las contenciones $Y_1' \subseteq Y_j'$ y por la maximalidad de los conjuntos $j{=}1$. De donde encontramos que $Y_1 = Y_1'$. Por último sea $Z = (Y - Y_1) = (Y - Y_1')$,

de donde se tiene la siguiente igualdad $Z = Y_2 \cup Y_3 \ldots Y_n = Y_2' \cup Y_3' \ldots Y_r'$ y procediendo por inducción sobre n se tiene que cada Y_i es único. ■

***Corolario* 2** *Todo conjunto algebraico en $\mathbb{A}^n$ se puede escribir de manera única como unión de variedades no contenidas unas en otras.*

***Definición* 1.7** *Si X es un espacio topológico, definimos la dimensión de X (que denotaremos por dim X) como el supremo de todos los enteros n tal que exista una cadena $Z_0 \subset Z_1 \ldots \subset Z_n$ de subconjuntos cerrados irreducibles distintos de X. Definimos la dimensión de una variedad afín o quasi-afín con la definición anterior tomando a la variedad como espacio topológico.*

Ejemplo 1.9 *La dimensión de $\mathbb{A}^1$ es 1, ya que los únicos subconjuntos cerrados e irreducibles son los unipuntuales, que son los conjuntos que constan únicamente de un punto, y el total.*

***Definición* 1.8** *En un anillo A la altura de un ideal primo p es el supremo de todos los n tales que existe una cadena de ideales $p_0 \subset p_1 \ldots \subset p_n = p$ de ideales primos distintos. Definimos la dimensión de Krull o simplemente dimensión de A como el supremo de todas las alturas de todos sus ideales primos.*

***Proposición* 1.4** *Si Y es un conjunto algebraico afín, entonces la dimensión de Y es igual a la dimensión de su anillo afín de coordenadas $A(Y)$.*

***Demostración*.** Si Y es un conjunto algebraico afín de $\mathbb{A}^n$, entonces los subconjuntos cerrados irreducibles se corresponden con los ideales primos de $A = K[x_1, x_2, \ldots, x_n]$ contenidos en $I(Y)$, y estos corresponden a su vez a los ideales primos de $A(Y)$. Luego la dimensión de Y es la longitud de la cadena de primos mas grande en $A(Y)$, la cual es su dimensión. ■

La proposición anterior nos permite aplicar los resultados de la teoría de la dimensión para anillos noetherianos en la geometría algebraica.

***Teorema* 2** *Sea k un campo, y sea B un dominio entero el cual es finitamente generado como una k-álgebra. Entonces:*

- *La dimensión de B es igual al grado de trascendencia del campo de cocientes $K(B)$ de B sobre k.*
- *Para cualquier ideal primo p en B se tiene:*

$$altura\ p\ +\ dim\ B/p\ =\ dim\ B$$

***Proposición* 1.5** *La dimensión de $\mathbb{A}^n$ es n.*

Demostración. Recordando la última proposición se tiene que $\mathbb{A}^n$ tiene la misma dimensión que su anillo afín de coordenadas $K[x_1, x_2, \ldots, x_n]$, ahora como $K[x_1, x_2, \ldots, x_n]$ se puede ver como una k-álgebra finitamente generada usamos el primer punto del teorema anterior y llegamos a que tiene dimensión n, luego el resultado. ■

***Proposición* 1.6** *Si $\mathbf{Y}$ es una variedad quasi-afín, entonces dim$\mathbf{Y}$ = dim$\overline{Y}$*

Demostración. Es fácil ver que si $Z_0 \subset Z_1 \ldots \subset Z_n$ es una suceción de subconjuntos cerrados e irreducibles de $\mathbf{Y}$, entonces $\overline{Z}_0 \subset \overline{Z}_1 \ldots \subset \overline{Z}_n$ es una sucesión de subconjuntos cerrados e irreducibles de $\overline{Y}$, luego dim$\mathbf{Y} \leq$ dim$\overline{Y}$. En particular si la dim$\mathbf{Y}$ es finita, entonces podemos elegir una cadena maximal de cerrados irreducibles $Z_0 \subset Z_1 \ldots \subset Z_n$, tal que dim$\mathbf{Y}$ = n. En este caso Z_0 debe ser igual a un punto P del espacio afín, luego es evidente que $\overline{Z}_0 \subset \overline{Z}_1 \ldots \subset \overline{Z}_n$ es también una cadena maximal, ahora P tiene una correspondencia con un ideal maximal m del anillo afín de coordenadas A($\overline{Y}$) de $\overline{Y}$. Luego los primos que se correponden con los $\overline{Z}_i$ están contenidos en m, entonces la altura de m es n, pero como P es un punto del espacio afín entoces A($\overline{Y}$)/$m \cong k$, lo que significa entonces que n = dim A($\overline{Y}$) = dim $\overline{Y}$ ■

***Teorema* 3** *(Krull's Hauptidealsatz). Sea A un anillo noetheriano, y sea $f \in$ A el cual no es divisor de cero ni unidad. Entonces todo ideal primo minimal que contenga a f tiene altura 1.*

***Proposición* 1.7** *Un dominio entero noetheriano D es un dominio de factorización única si y solo si todo ideal primo de altura 1 es principal.*

***Proposición* 1.8** *Una variedad Y de $\mathbb{A}^n$ tiene dimensión n-1 si y solo si es el conjunto de ceros $Z(f)$ de un solo polinomio irreducible no constante en $A = K[x_1, x_2, \ldots, x_n]$.*

Demostración. Si f es un polinomio irreducible, es fácil ver que Z(f) = Z(p) es una variedad, con $p = (f)$ un ideal primo. Por el Teorema de Krull's Hauptidealsatz p tiene altura 1, luego por el Teorema 10 se tiene que Z(f) tiene dimensión n-1. Recíprocamente a una variedad de dimensión

n-1 le corresponde un ideal primo p de altura 1, pero por la proposición anterior como A es un dominio de factorización única, luego p es principal, de donde $p = (f)$, para algún f polinomio irreducible de A, de donde se sigue la conclusión. ■

1.2. Variedades Proyectivas

Para definir las variedades proyectivas seguiremos los razonamientos anteriores, y obviaremos las partes que sean solamente repetitivas.

Sea k un campo algebraicamente cerrado, definamos el *n-espacio proyectivo* $\mathbb{P}^n_k$ o simplemente $\mathbb{P}^n$ como el conjunto de clases de equivalencia de las (n + 1)- entradas de elementos de k no todos cero, bajo la siguiente relación de equivalencia:

$(a_0, a_1 \ldots, a_n) \sim (\lambda a_0, \lambda a_1 \ldots, \lambda a_n)$, para todo $\lambda \in k$ distinta de cero

Otra forma de ver al espacio proyectivo $\mathbb{P}^n$ a nivel de conjuntos es viendolo como el cociente de A^{n+1} - (0, 0, ... , 0) con la relación de equivalencia que identifica a cada punto con la recta que pasa por el origen y por ese punto. Un elemento P en $\mathbb{P}^n$ es llamado punto, luego el conjunto de las (n + 1)- entradas que pertenecen a P son llamadas el *conjunto de coordenadas homegeneas de P.*

Un anillo R es graduado si se puede ver como suma directa de grupos abelianos R_d, o sea: R = $\bigoplus_{d\geq 0} R_d$, tal que para todo $d,e \geq 0$ se tiene que $R_d \cdot R_e \subseteq R_{d+e}$. Luego a un elemento de R_d es llamado un *elemento homogeneo de grado d.* De esta forma todo elemento de R puede ser escrito de una única forma como suma de elementos homogeneos. Un ideal $a \subseteq$ R es un ideal homogeneo si $a = \bigoplus_{d\geq 0} (a \cap R_d)$. Recordemos también algunos resultados de ideales homogeneos: un ideal es homogeneo si y solo si se puede generar por elementos homogeneos; la suma, la intersección, el producto y el radical de ideales homogeneos es homogeneo y por último para saber si un ideal homogeneo a es primo, es suficiente mostrar que para cualquiera dos elementos homogeneos f y g tal que $fg \in a$, entonces $f \in a$ o $g \in a$.

Ahora tomemos a R = $K[x_0, x_1, \ldots, x_n]$, y tomemos a R_d como el conjunto de todas las combinaciones lineales de monomios en R de grado d. Si f es

un polinomio de R, no podría definir una función en $\mathbb{P}^n$ ya que no estaría bien definida, pero si f es un polinomio homogeneo de grado d, entonces se tiene que $f(\lambda a_0, \lambda a_1 \ldots, \lambda a_n) = \lambda^d f(a_0, a_1 \ldots, a_n)$, lo que significa que si f es cero en un punto, entonces será cero en toda la clase de equivalencia. Así f dará una función entre el espacio $\mathbb{P}^n$ y el conjunto formado por el cero y el uno; dicha función estará definida de la siguiente forma: $f(\mathrm{P})=0$ si $f(a_0, a_1 \ldots, a_n)=0$, y $f(\mathrm{P})=1$ si $f(a_0, a_1 \ldots, a_n)\neq 0$.

Ahora podremos hablar sobre los ceros de un polinomio homogeneo, llamado $\mathbf{Z}(f) = \{\ \mathrm{P} \in \mathbb{P}^n \mid f(\mathrm{P}) = 0\ \}$. Si T es cualquier conjunto de polinomios homogeneos de S, definiremos a los ceros de T por:

$$\mathbf{Z}(\mathrm{T}) = \{\ \mathrm{P} \in \mathbb{P}^n \mid f(\mathrm{P}) = 0, \forall f \in \mathrm{T}\ \}$$

Si a es un ideal homogeneo de R, definamos $\mathbf{Z}(a)=\mathbf{Z}(\mathrm{T})$, donde T es el conjunto de todos los elementos homogeneos de a. Como R es un anillo noetheriano, cualquier conjunto de elementos homogeneos tiene un subconjutno finito $f_1, f_2, \ldots, f_r$, tal que $\mathbf{Z}(\mathrm{T})=\mathbf{Z}(f_1, f_2, \ldots, f_r)$.

***Definición* 1.9** *Un subconjunto* $\boldsymbol{Y}$ *de* $\mathbb{P}^n$ *es un conjunto algebraico si existe un conjunto* T *de elementos homogeneos de* R*, tal que* $Y = Z(T)$*.*

***Proposición* 1.9** *La unión de dos conjuntos algebraicos es algebraico. La intersección de cualquier familia de conjuntos algebraicos es algebraico. El conjunto vacío y el espacio total son conjuntos algebraicos.*

Demostración. Similar a la demostración de la proposición 1 ■

***Definición* 1.10** *Se define la Topología de Zariski en* $\mathbb{P}^n$ *tomando a los abiertos como los complementos de los conjuntos algebraicos.*

Ahora solamente ampliaremos las definiciones de irreducibilidad y de dimensión que definimos en la sección anterior.

***Definición* 1.11** *Una variedad algebraica proyectiva (o simplemente variedad proyectiva) es un conjunto algebraico irreducible en* $\mathbb{P}^n$*, con la topología inducida. Un subconjunto abierto de una variedad proyectiva es una variedad quasi-proyectiva. La dimensión de una variedad proyectiva o quasi-proyectiva es su dimensión como espacio topológico.*

Si Y es cualquier subconjunto de $\mathbb{P}^n$, definimos el ideal homogeneo de Y en S, denotado por $I(Y)$, como el ideal generado por $\{ f \in R \mid f$ es homogeneo y $f(P) = 0, \forall P \in Y\}$. Si Y es un conjunto algebraico, definimos al anillo homogeneo de coordenadas de Y por $R(Y) = R/I(Y)$.

Nuestro siguiente objetivo es mostrar que el espacio n-proyectivo tiene una cubierta abierta de n-espacios afines, y luego que cada variedad proyectiva tiene una cubierta abierta de variedades afines. Pero antes introduzcamos mas notación.

Si $f \in$ S es un polinomio lineal homogeneo, entonces el conjunto de ceros de f es llamado un *hiperplano*. En particular denotamos al conjunto de ceros del polinomio x_i por H_i, para i=0, ... ,n. Sea U_i el conjunto abierto $\mathbb{P}^n$ - H_i. Entonces $\mathbb{P}^n$ está cubierto por los conjuntos abiertos U_i, ya que si P=$(a_0, a_1, \ldots, a_n)$ es un punto del $n-$espacio proyectivo, luego hay al menos algún $a_i \neq 0$, luego P$\in U_i$. Ahora definamos una mapeo φ_i:$U_i \to \mathbb{A}^n$ de la siguiente manera: si P=$(a_0, a_1, \ldots, a_n) \in U_i$, entonces φ_i(P) = Q, donde Q es el punto con coordenadas afines:

$$\left(\frac{a_0}{a_i}, \ldots, \frac{a_n}{a_i}\right),$$

quitando la entrada $\frac{a_i}{a_i}$. Es fácil ver que φ_i está bien definida ya que las coordenadas $\frac{a_j}{a_i}$ son independientes de las coordenadas homogeneas que escojamos.

***Proposición* 1.10** *El mapeo φ_i es un homeomorfismo de U_i con la topología inducida hacia $\mathbb{A}^n$ con la topología de Zariski.*

***Demostración*.** Claramente φ_i es biyectiva, luego solo resta demostrar que los conjuntos cerrados de U_i están identificados con los conjuntos cerrados de $\mathbb{A}^n$ por medio de φ_i. Sin pérdida de generalidad podemos suponer i=0 y escribiremos U por U_0 y φ en lugar de φ_0.

Sea $A = K[y_1, y_2, \ldots, y_n]$, definamos un mapeo α de R^h (el conjunto de elementos homogeneos de R) en A, y un mapeo β de A a R^h. Sea $f \in R^h$, entonces definimos $\alpha(f) = f(1, y_1, y_2, \ldots, y_n)$. Ahora para definir β tomo $g \in A$ y supongamos que es de grado e, luego defino $\beta(g) = x_0^e g\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right)$ que es un polinomio homogeneo de grado e y que está en R^h.

Primero vamos a demostrar que la imagen bajo φ de cualquier subconjunto cerrado U en $\mathbb{A}^n$ es cerrado. Así sea $Y \subseteq U$ un subconjunto cerrado, y sea $\overline{Y}$ su cerradura en $\mathbb{P}^n$, lo que significa que existe un conjunto $T \subseteq R^h$, tal que $Z(T) = \overline{Y}$, entonces podremos escribir a T de la siguiente manera: $T = I(Y)$. Ahora recordando que estamos en un anillo noetheriano se tiene que $I(Y) = \langle f_1, f_2, \ldots, f_r \rangle$, entonces definimos a $T' = \alpha(T) = \alpha(I(Y)) = \alpha(\langle f_1, f_2, \ldots, f_r \rangle)$, ahora llamemos $g_i = \alpha(f_i)$ y notemos lo siguiente: $P \in \varphi(Y) \Leftrightarrow f_i(1, a_1, \ldots, a_n) = 0, \forall i = 1, \ldots, r \Leftrightarrow g_i(a_1, \ldots, a_n) = 0, \forall i = 1, \ldots, r$, lo que concluye esta parte de la demostración, ya que: $\varphi(Y) = Z(g_1, g_2, \ldots, g_r) = Z(T')$.

Recíprocamente demostraremos que para cada cerrado de $\mathbb{A}^n$ al aplicarle φ^{-1} define un conjunto en el proyectivo que es cerrado en U con la topología inducida. Sea W un conjunto cerrado de $\mathbb{A}^n$, entonces existe un T' tal que $W = Z(T') = Z(f_1, f_2, \ldots, f_n)$, para algún $T' = \langle f_1, f_2, \ldots, f_n \rangle \subseteq A$. Ahora llamemos $g_i = \beta(f_i)$, tomemos $P \in \varphi^{-1}(W) \subseteq U$, luego es fácil ver: $g_i(P) = f_i(\varphi(P)) = 0$, luego $\varphi^{-1}(W) \subseteq (U \cap Z(g_1, g_2, \ldots, g_n)) = ((U \cap X(\beta(T'))))$, ahora para demostrar la igualdad tomo $P \in (U \cap Z(g_1, g_2, \ldots, g_n)) = ((U \cap Z(\beta(T'))))$, luego $0 = g_i(P) = f_i(\varphi(P))$, entonces: $P \in \varphi^{-1}(W)$, lo que nos dice: $\varphi^{-1}(W) = ((U \cap Z(\beta(T'))))$. De lo anterior concluimos que φ y φ^{-1} son funciones cerradas, luego φ es un homeomorfismo. ■

Corolario 3 *Si Y es una variedad proyectiva (quasi-proyectiva), entonces Y puede ser cubierta por conjuntos abiertos $Y \cap U_i, i = 0, \ldots, n$, los cuales son homeomorfos a variedades afines (quasi-afines),vía el homeomorfismo φ_i definido arriba.*

Demostración. Se sigue de la proposición anterior ■

1.3. Ejemplos

Para terminar este capítulo se expondrán de manera breve ejemplos de variedades algebraicas, pero al no ser el objetivo de esta tesis el estudio de éstos, solo se expondrán de manera general algunos detalles de las demostraciones.

Ejemplo 1.10 *Cerradura Proyectiva de una Variedad Afín.*

Si $Y \subseteq \mathbb{A}^n$ es una veriedad afín, identificamos a $\mathbb{A}^n$ con un abierto $U_0 \subseteq P^n$ vía el homeomorfismo φ_0. Ahora denotaremos por $\overline{Y}$ a la cerradura de Y en $\mathbb{P}^n$ y le llamaremos la ***cerradura proyectiva*** *de Y.*

Uno puede probar que $\boldsymbol{I}(\overline{Y})$ es el ideal generado por $\beta(\boldsymbol{I}(Y))$, con β definido como en la última proposición (aquí solo se dará una de las contenciones). Primero uno debe demostrar que si a *es un ideal radical, entonces* β(a) *vuelve a ser un ideal radical. Luego uno puede verificar las contenciones de la siguiente manera:*

Sea $f \in a$ el ideal generado por $\beta(\boldsymbol{I}(Y))$, entonces:

$$f(x_0, x_1, \ldots, x_n) = \sum x_0^k g_k \left(\tfrac{x_1}{x_0}, \ldots, \tfrac{x_n}{x_0}\right), \text{ con } g_k \in \boldsymbol{I}(Y) \text{ de grado } k$$

Por lo que: $f(1, x_1, \ldots, x_n) = \sum g_k(x_1, \ldots, x_n) = h$ un polinomio en $\boldsymbol{I}(Y)$, ahora como $U_0 = \mathbb{P}^n - Z(x_0)$, se tiene que f restringido a U_0 es h, luego f se anula en $Y = \overline{Y} \cap U_0$, luego $Y \subseteq Z(a)$ que es un conjunto cerrado, entonces: $\overline{Y} \subseteq Z(a)$, de donde se sigue una de las contenciones.

Ejemplo 1.11 *El Cono Afín*

Un subconjunto algebraico afín $X \subseteq \mathbb{A}^n$ es llamado ***cono afín*** *si: $\forall$ $(a_1, \ldots, a_n) \in X$ y $\forall$ $\lambda \in k$ se tiene que $(\lambda a_1 \ldots, \lambda a_n) \in X$. Para darnos una idea de lo que sucede, es fácil ver que el cero del espacio afín siempre será un elemento del cono, y además que si un punto P está en el cono, luego toda recta que toca al punto P y pasa por el origen está en X, luego cualquier cono se puede escribir como unión de rectas que pasan por el origen.*

Ejemplo 1.12 *El Cono sobre una Variedad Proyectiva.*

Sea $Y \subseteq \mathbb{P}^n$ un conjunto algebraico, sea θ:$A^{n+1} - \{\hat{0}\} \longrightarrow \mathbb{P}^n$ el mapeo que envía a un punto $(a_0, a_1, \ldots, a_n)$ de coordenadas afines al punto $(a_0, a_1, \ldots, a_n)$ con coordenadas homogeneas. Definimos el ***Cono Afín*** *sobre Y de la siguiente forma:*

$$C(Y) = \theta^{-1}(Y) \cup \{\hat{0}\}$$

En este caso el cono afín sobre una variedad proyectiva Y es el conjunto formado por el cero y el conjunto de puntos en el espacio afín tales que sus respectivas clases en el espacio proyectivo están en Y. Entre las observaciones que podemos hacer es que el cono $C(Y)$ será un conjunto algebraico en el afín, y que Y será irreducible si y solo si $C(Y)$ es irreducible, luego si Y es una variedad proyectiva, entonces $C(Y)$ será una variedad afín.

Ejemplo 1.13 *El mapeo de Veronese*

Este es un ejemplo que mostrará como inyectar de manera no trivial un espacio proyectivo como un subconjunto algebraico de otro espacio proyectivo de mayor dimensión. Pero antes revisaremos un resultado para que sea más fácil su comprensión.

Dados n,d > 0, hay $\binom{n+d}{n}$ *monomios de grado d en las n+1 variables* $x_0, x_1, \ldots, x_n$*. La demostración se hace por inducción sobre d y n; se empieza con el caso d = n = 0 que es trivial, luego se toma a f el polinomio que es la suma de todos los monomios de grado d en las n+1 variables y nos damos cuenta que es un polinomio homogeneo que se puede ver como:*

$$f(x_0, x_1, \ldots, x_n) = f_1(x_1, \ldots, x_n) + x_0 f_2(x_0, x_1, \ldots, x_n)$$

donde f_1 *es la suma de todos los polinomio de grado d que no tienen a la variable* x_0*, luego es la suma de todos los monomios de grado d en las n variables* $x_1, \ldots, x_n$*, luego por la hipótesis de inducción tiene* $\binom{n-1+d}{n-1}$ *elementos. También podemos notar que* f_2 *es la suma de todos los monomios de grado* $d-1$ *en las* $n+1$ *variables* $x_0, x_1, \ldots, x_n$*, usando nuevamente nuestra hipótesis de inducción nos queda que tiene* $\binom{n+d-1}{n}$ *elementos. Por último sumando los elementos de* f_1 *y* f_2 *nos queda:*

$$\binom{n-1+d}{n-1} + \binom{n+d-1}{n} = \binom{n+d}{n}$$

que son los elementos de f y es lo que se quería demostrar.

Ahora sean $M_0, M_1, \ldots, M_N$ *todos los monomios de grado d en las* $n+1$ *variables* $x_0, x_1, \ldots, x_n$*, con* $N = \binom{n+d}{n} - 1$ *y definimos el siguiente mapeo:*

$$\rho_d : \mathbb{P}^n \to \mathbb{P}^N$$
$$\rho_d(P) = (M_0(P), M_1(P), \ldots, M_N(P))$$

Algo que es fácil de verificar es que ρ_d *está bien definida. El mapeo anterior es llamado la* ***d-ésima inmersión*** *de* $\mathbb{P}^n$ *en* $\mathbb{P}^N$ *y a cualquier mapeo que difiera de* ρ_d *por automorfismos de* $\mathbb{P}^N$ *le llamaremos un* ***mapeo de Veronese****.*

Sea $\theta : K[y_0, y_1, \ldots, y_N] \to K[x_0, x_1, \ldots, x_n]$ *el homomorfismo que a cada* y_i *lo envía a* M_i*. Ahora sea* $a = \ker(\theta)$*, entonces a será un ideal primo homogeneo, luego* $Z(a)$ *es una variedad proyectiva de* $\mathbb{P}^N$ *llamada la* ***Variedad de Veronese****; más aún uno puede demostrar que* $Im(\rho_d) = Z(a)$ *y que entonces* ρ_d *es un homeomorfismo sobre la variedad proyectiva* $Z(a)$*.*

Geométricamente, el mapeo de Veronese está caracterizado por la propiedad de que las hypersuperficies de grado d en $\mathbb{P}^n$ *son las secciones de los hyperplanos de la imagen* $\rho_d(\mathbb{P}^n) \subset \mathbb{P}^N$*.*

Ejemplo 1.14 *La Superficie de Veronesse*

Sea Y la imagen de ρ_2 la 2-ésima inmersión de $\mathbb{P}^2$ en $\mathbb{P}^5$ dada de la siguiente forma:

$$\rho_2 : \mathbb{P}^2 \to \mathbb{P}^5$$
$$\rho_2 : [X_0, X_1, X_2] \to [X_0^2, X_1^2, X_2^2, X_0X_1, X_1X_2, X_0X_2]$$

Entonces a la imagen de este mapeo lo llamaremos la ***superficie de Veronese****.*

Capítulo 2

Conceptos generales

2.1. Códigos lineales

En este capítulo cambiaremos la notación de los puntos del espacio proyectivo por la siguiente: $(0, \ldots, 0, 1, a_1, a_2, \ldots, a_l)$, donde la primer entrada no cero del punto en cuestión es 1. Esto es para garantizar que los mapeos de evaluación dados más adelante estén bien definidos.

Notación

Si X es un conjunto denotaremos por $|X|$ la cardinalidad de X. Si $x \in \mathbb{R}$ pondremos $[x]$ para denotar la parte entera de x. En este trabajo, a menos que se diga lo contrario, denotaremos por K el campo finito con $q = p^r$ elementos, donde p es primo arbitrario, esto es $K := \mathbb{F}_q$. Por $\mathbb{P}^n(K)$ denotaremos el n-ésimo espacio proyectivo definido sobre $K = \mathbb{F}_q$.

En esta sección inicial se introducirán algunas de las nociones básicas de la teoría de códigos lineales. Consideremos el K-espacio vectorial $K^n = (\mathbb{F}_q)^n$.

***Definición* 2.1** *La distancia de Hamming sobre K^n es la función:*

$$\delta : K^n \times K^n \to \mathbb{N} \cup \{0\}$$

$$\delta\left((a_1, \ldots, a_n), (b_1, \ldots, b_n)\right) := |\{i : a_i \neq b_i\}|.$$

La distancia de Hamming es una métrica en K^n como puede verificarse fácilmente.

***Definición* 2.2** *El peso de Hamming de un elemento $a = (a_1, \ldots, a_n) \in K^n$ se define como*

$$w(a) := \delta(a, 0) = |\{i : a_i \neq 0\}|.$$

***Definición* 2.3** *Un código lineal C (sobre el alfabeto K) es un subespacio lineal de K^n. Los elementos de C serán las palabras del código. Llamaremos a n la longitud del código y a su dimensión $k := \dim_K C$, como $K-$espacio vectorial, la dimensión de C. En este caso, un $[n, k]-$código es un código de longitud n y dimensión k.*

***Definición* 2.4** *La distancia mínima, $\delta(C)$, de un código no trivial C se define como*

$$\delta(C) := \text{mín}\{\delta(a, b) : a, b \in C \quad y \quad a \neq b\}.$$

Por las definiciones anteriores se tiene que $\delta(a, b) = \delta(a-b, 0) = w(a-b)$, por lo que

$$\delta(C) = \text{mín}\{w(a) : 0 \neq a \in C\}$$

***Definición* 2.5** *Un $[n, k]-$código C, con distancia mínima δ se denota como un $[n, k, \delta]-$código. A los enteros n, k, δ les llamaremos parámetros básicos del código correspondiente.*

Para un código C con distancia mínima δ sea $t := \left[\frac{\delta-1}{2}\right]$. Si $a \in K^n$ y $\delta(a, c) \leq t$ para algún $c \in C$, entonces c es la única palabra con $\delta(a, c) \leq t$.

Lo anterior significa que si al transmitir información, se recibe el vector a, y este difiere de c en a lo más t componentes, entonces se acepta a c como la palabra transmitida. Por este hecho se dice que C es un código corrector de t errores.

***Definición* 2.6** *El producto interno canónico sobre K^n está definido por*

$$\langle (a_1, \ldots, a_n), (b_1, \ldots, b_n) \rangle := \sum_{i=1}^{n} a_i b_i.$$

***Definición* 2.7** *Si $C \subseteq K^n$ es un código lineal, entonces el código dual de C es*

$$C^{\perp} := \{u \in K^n : \langle u, a \rangle = 0 \quad \textit{para todo} \quad a \in C\}.$$

Uno de los más importantes problemas de la teoría de códigos es construir códigos con dimensión y distancia mínima grandes, en comparación con su longitud, debido a que la capacidad de corrección de errores depende de la distancia mínima. Sin embargo hay ciertas limitaciones en este sentido, una de ellas, la más sencilla, es la cota de Singleton:

***Proposición* 2.1 (Singleton)** *Para un* $[n, k, \delta]-$*código lineal* C *se cumple que*

$$k + \delta \leq n + 1$$

***Demostración*.** [31], página 41. ■

***Definición* 2.8** *Los códigos con* $k + \delta = n + 1$ *son llamados códigos MDS (códigos de máxima distancia separable).*

2.2. Función de Hilbert y $a-$invariante

En esta sección definiremos la función de Hilbert y algunos resultados que serán importantes en el desarrollo de este trabajo.

Sean $K = \mathbb{F}_q$ y $A := K[x_0, \ldots, x_n] = \bigoplus_{i \geq 0} A_i$ el anillo de polinomios en las indeterminadas $x_0, \ldots, x_n$ con coeficientes en K, con la graduación natural, es decir, A_i consta de todos los polinomios homegéneos de grado i y el cero.

Sea X un subconjunto no vacío de $\mathbb{P}^n(K)$. Sea $I_X := < f \in A : f$ es homogéneo y $f(P) = 0$ para todo $P \in X > = \bigoplus_{i \geq 0} I_X(i)$, donde $I_X(i)$ significa la parte homogénea de grado i de I_X, el ideal anulador graduado de X en A. De igual manera, consideremos $R := A/I_X$ como el anillo coordenado del conjunto X.

***Definición* 2.9** *La función de Hilbert del anillo coordenado* $R = A/I_X$ *se define como*

$$H_X : \mathbb{N} \cup 0 \to \mathbb{N} \cup 0$$

$$H_X(d) := \dim_K A_d/I_X(d) = \dim_K A_d - \dim_K I_X(d).$$

***Proposición* 2.2** *Usemos la notación anterior y sea* $\gamma_X := \min\{i \geq 0 : I_X(i) \neq 0\}$*, entonces existe un entero* a_X *de tal forma que:*

(I) $H_X(d) = \dim_K A_d = \binom{n+d}{n}$ *si y sólo si* $d < \gamma_X$*.*

(II) $H_X(d) < H_X(d+1) < |X|$ *si* $0 \leq d < a_X$*.*

(III) $H_X(d) = |X|$ *para* $d \geq a_X + 1$*.*

***Demostración*.** [29], página 166. ■

***Definición* 2.10** *El entero* a_X *de la Proposición anterior se llama el* $a-$*invariante de* R*, o el* $a-$*invariante de* I*, o incluso el* $a-$*invariante de* X*.*

***Definición* 2.11** *Puesto que el valor de la función de Hilbert a partir de* $a_X + 1$ *es constante (igual a la cardinalidad de* X*), este número,* $a_X + 1$*, se llama índice de regularidad de* R *o* I_X*. Más aún, el ideal* I_X *está dado por:*

$$I_X = \langle I_X(\gamma_X), I_X(\gamma_X + 1), \ldots, I_X(a_X + 2)\rangle$$

2.3. Códigos Reed-Muller

En esta sección se introducen los códigos de evaluación cuyas características se estudiarán y analizarán. Estos códigos son una generalización de los originales códigos Reed-Muller introducidos en 1954 (cf. [**?**], [**?**]).

Sea $K = \mathbb{F}_q$ y $A_d \subseteq K[x_0, \ldots, x_n]$ la colección de todos los polinomios homogéneos de grado d, y el cero.

***Definición* 2.12** *Sean* $d \in \mathbb{N} \cup \{0\}$ *y* $X = \{P_1, \ldots, P_m\} \subseteq \mathbb{P}^n(K)$*. Definimos el mapeo evaluación siguiente:*

$$\begin{aligned} ev_d : A_d &\rightarrow K^m \\ ev_d(f) &= (f(P_1), \ldots, f(P_m)). \end{aligned} \tag{2.1}$$

Es claro que este mapeo es $K-$lineal. Además el núcleo de esta aplicación es $I_X(d)$.

***Definición* 2.13** *El código de evaluación de orden d sobre el conjunto X, el cual se denota por $C_X(d)$, se define como la imagen del mapeo evaluación ev_d.*

De lo anterior se sigue que $C_X(d)$ es isomorfo a $A_d/I_X(d)$, luego por la definición de función de Hilbert:

$$\dim_K C_X(d) = H_X(d).$$

A continuación se da un ejemplo de aplicación de un código de evaluación de una variedad donde se han estudiado algunos códigos lineales ([18], [22]).

Como ya vimos, el mapeo de Veronese ν_n de grado n, está dado por

$$\nu_n : \mathbb{P}^m(K) \to \mathbb{P}^N(K),$$
$$\nu_n(\underline{z}) = (\ldots, M(\underline{z}), \ldots)$$

donde $\underline{z} = (z_0, \ldots, z_m) \in \mathbb{P}^m(K)$ y $M(\underline{z})$ corre sobre todos los monomios de grado n en las variables $Z_0, \ldots, Z_m$ y $N = \binom{n+m}{n} - 1$.

La imagen del mapeo ν_n es la variedad de Veronese (se acostumbra decir de grado n, pero por comodidad usaremos de manera implícita el valor de n y nos referiremos a ella simplemente como la variedad de Veronese), la cual se denotó anteriormente por V. En este caso, $C_V(d)$ es la imagen del mapeo siguiente

$$K[Y_0, \ldots, Y_N]_d \to K^{|V|},$$
$$f \to (f(\ldots, M, \ldots)(Q_1), \ldots, f(\ldots, M, \ldots)(Q_{k_2}))$$

donde $k_2 = |\mathbb{P}^m(K)|$ y $\mathbb{P}^m(K) = \{Q_1, \ldots, Q_{k_2}\}$.

***Definición* 2.14** *Al código $C_V(d)$ le llamaremos el código de evaluación de orden d sobre la variedad de Veronese.*

Para los códigos de evaluación asociados a la variedad de Veronese sobre el campo K ya se han calculado los parámetros principales ([22], Lema 2 y Teorema 1, página 4).

2.4. Ideales tóricos

Sea $\mathbf{A} = \{a_1, \ldots, a_n\}$ un subconjunto de $\mathbf{N}^d \backslash \{\mathbf{0}\}$, y sea A la matriz con columnas a_i y supongamos que rank(A) = d. Consideremos el anillo de polinomios S = $k[x_1, x_2, \ldots, x_n]$ y definamos el siguiente homomorfismo:

$$\pi : \mathbf{N}^n \longrightarrow \mathbf{N}^d$$
$$\pi(\mathbf{u}) = \pi(u_1, \ldots, u_n) = u_1 a_1 + \ldots + u_n a_n$$

Donde la imagen de π es el semigrupo:

$$\mathbf{NA} = \{\lambda_1 a_1 + \ldots + \lambda_n a_n \mid \lambda_1, \ldots, \lambda_n \in \mathbf{N}\}$$

y donde π se puede extender a un homomorfismo:

$$\varphi : k[x_1, x_2, \ldots, x_n] \longrightarrow k[t_1, t_2, \ldots, t_d]$$
$$\varphi(x_i) = \mathbf{t}^{a_i} = t_1^{a_{i1}} \ldots t_d^{a_{id}}.$$

El Kernel de φ es denotado por $I_\mathbf{A}$ el cual es un ideal primo y es llamado el **ideal tórico** asociado a la matriz A. La forma de ver a φ explícitamente como la extensión de π y también ver como actúa la matriz A sobre cualquier monomio de S es tomando a $\mathbf{u} = (u_1, \ldots, u_n)$, y sea $\mathbf{x^u} = x_1^{u_1} \ldots x_n^{u_n}$, entonces se tiene:

$$\mathbf{x^u} \longrightarrow \mathbf{t}^{\pi(\mathbf{u})} = \mathbf{t}^{A\mathbf{u}}$$

***Definición* 2.15** *El **anillo tórico** es:*

$$S/I_{\boldsymbol{A}} \cong k[\boldsymbol{t}^{a_1}, \ldots, \boldsymbol{t}^{a_n}] \cong \boldsymbol{NA}$$

donde el segundo isomorfismo está dado por $\boldsymbol{t^a} \longmapsto \boldsymbol{a}$.

Una **variedad tórica** es una variedad parametrizada por un número finito de monomios, luego podremos escribir una variedad tórica como $V(I_\mathbf{A})$ = Z($I_\mathbf{A}$).

La palabra tórico es usada porque existe una acción toro en la variedad tórica: el toro d-dimensional $(k^*)^d$ actuando diagonalmente en k^n e interpretando $\mathbf{A}$ como el conjunto de pesos. La órbita de un punto $(\alpha_1, \ldots, \alpha_n) \in k^n$ es:

$$(k^*)^d(\alpha_1, \ldots, \alpha_n) = \left\{(\mathbf{t}^{a_1}\alpha_1, \ldots, \mathbf{t}^{a_n}\alpha_n) \mid \mathbf{t} \in (k^*)^d\right\}$$

***Teorema* 4** *La dimensión de Krull del anillo tórico $S/I_{\boldsymbol{A}}$ es d=dim A.*

Demostración. Recordemos que por la defínción anterior el anillo tórico $S/I_{\mathbf{A}}$ es isomorfo al subanillo $k[\mathbf{t}^{a_1}, \ldots, \mathbf{t}^{a_n}]$, pero la dimensión de Krull en este dominio entero es el máximo número de monomios algebraicamente independientes $\mathbf{t}^{a_i}$, y solo tenemos que darnos cuenta que dos monomios son independientes si y sólo si sus vectores exponentes son linealmente independientes, luego la dimensión del anillo tórico es igual al rango de A que es d ■

***Definición* 2.16** *Si $\boldsymbol{u} \in Z^m$, definimos al **soporte** de $\boldsymbol{u}$ por:*

$$supp(\boldsymbol{u}) = \{i \mid \boldsymbol{u}_i \neq 0\}$$

Para todo $\mathbf{u}$ definimos a $\mathbf{u}_+$ como el vector que en la i-ésima coordenada es u_i si $u_i > 0$ y es igual a 0 en cualquier otra entrada, y definimos a $\mathbf{u}_-$ como el vector que en la i-ésima coordenada es $-u_i$ si $u_i < 0$ y es igual a 0 en cualquier otra entrada. Así es fácil ver que entonces siempre se puede escribir $\mathbf{u} = \mathbf{u}_+ - \mathbf{u}_-$, donde $\mathbf{u}_+$ y $\mathbf{u}_-$ tienen entradas no negativas y además se cumple: $\text{supp}(\mathbf{u}_+) \cap \text{supp}(\mathbf{u}_-) = \emptyset$.

***Definición* 2.17** *Definimos a un **término** como un múltiplo escalar de un monomio. Un **binomio** de un anillo de polinomios será una diferncia de monomios y a un ideal generado por binomios será llamado un **ideal binomial**.*

De ahora en adelante la matriz A se considerará como la matriz de un mapeo de $\mathbf{Z}^n$ en $\mathbf{Z}^d$.

***Definición* 2.18** *Definimos al kernel de A como:* $\ker A = \{\boldsymbol{u} \in \boldsymbol{Z}^n \mid A\boldsymbol{u} = 0\}$

Antes de comenzar el siguiente teorema es importante darnos cuenta de que las matrices como mapeos son transformaciones lineales, luego en nuestro caso como A tiene entradas en los naturales unión el cero, si A no es la matriz con todas las entradas cero, entonces para cualquier $\mathbf{u} \in \mathbf{N}^n$ distinto del vector cero se tendrá $A\mathbf{u} \neq 0$. Por lo tanto los elementos distintos de cero que estén en el kernel de A necesariamente tendrán entradas negativas.

Como dijimos anteriormente las matrices funcionan como transformaciones lineales, luego tomemos $\mathbf{u} \in \ker A$ distinto del vector cero, como ya vimos existen dos vectores con entradas no negativas y soporte disjunto tales que:$\mathbf{u}_+ - \mathbf{u}_- = \mathbf{u}$, entonces se tiene que:

$$\mathrm{A}\mathbf{u} = 0 \Rightarrow \mathrm{A}\,(\mathbf{u}_+ - \mathbf{u}_-) = 0 \Rightarrow \mathrm{A}\mathbf{u}_+ - \mathrm{A}\mathbf{u}_- = 0 \Rightarrow \mathrm{A}\mathbf{u}_+ = \mathrm{A}\mathbf{u}_-$$

Con las observaciones anteriores tenemos el siguiente:

***Lema* 1** *Para todo* $\boldsymbol{u} \in \ker A$ *se tiene:*

$$\varphi\left(\boldsymbol{x}^{\boldsymbol{u}_+}\right) = \varphi\left(\boldsymbol{x}^{\boldsymbol{u}_-}\right)$$

De donde se concluye que $\boldsymbol{x}^{\boldsymbol{u}_+} - \boldsymbol{x}^{\boldsymbol{u}_-} \in I_{\boldsymbol{A}}$.

Demostración. Solo tenemos que usar las observaciones anteriores ya que si tomamos $\mathbf{u} \in \ker A$:

$$\mathrm{A}\mathbf{u}_+ = \mathrm{A}\mathbf{u}_- \Rightarrow \mathbf{t}^{A\mathbf{u}_+} = \mathbf{t}^{A\mathbf{u}_-} \Rightarrow \varphi\left(\mathbf{x}^{\mathbf{u}_+}\right) = \varphi\left(\mathbf{x}^{\mathbf{u}_-}\right)$$

La última parte es evidente ■

***Teorema* 5** *Todo binomio de* $I_{\boldsymbol{A}}$ *es de la forma* $\mathrm{m}(\boldsymbol{x}^{\boldsymbol{u}_+} - \boldsymbol{x}^{\boldsymbol{u}_-})$ *para algún monomio* m *y algún* $\boldsymbol{u} \in \ker A$. *Además el ideal tórico está generado por el conjunto de binomios:*

$$I_{\boldsymbol{A}} = \langle \{\boldsymbol{x}^{\boldsymbol{u}_+} - \boldsymbol{x}^{\boldsymbol{u}_-} \mid \boldsymbol{u} \in \ker A\} \rangle$$

Así el ideal $I_{\boldsymbol{A}}$ *tendrá un sistema minimal de generadores que consistirá de binomios.*

Demostración. Denotemos por $I' = \langle \{\mathbf{x}^{\mathbf{u}_+} - \mathbf{x}^{\mathbf{u}_-} \mid \mathbf{u} \in \ker A\} \rangle$. Por el lema anterior como todos los binomios están en $I_{\mathbf{A}}$, se tiene la siguiente contensión: $I' \subseteq I_{\mathbf{A}}$. Ahora supongamos que $I' \neq I_{\mathbf{A}}$, luego fijamos un orden monomial $<$ en S, tal que el ideal inicial de $I_{\mathbf{A}}$ es monomial. Luego como existe un $f \in I_{\mathbf{A}}$, tal que $f \notin I'$ (o sea que no puede ser generados por binomios); de todos los polinomios que cumplan la condición anterior tomamos el polinomio cuyo término líder $lt(f) = g$ sea minimal con respecto al orden monomial fijo. Como sabemos que los monomios forman una base de $k[t_1, t_2, \ldots, t_d]$, f está en el ideal tórico $I_{\mathbf{A}}$, se sigue: $\varphi(f) = 0$, entonces existe un término g' de f tal que g y g' son mapeados bajo φ a algún múltimplo escalar de un mismo monomio. Entonces tenemos $g = \alpha\mathbf{x}^{\mathbf{v}}$ y $g' = \beta\mathbf{x}^{\mathbf{w}}$,con $\alpha, \beta \in k^*$. Abajo mostraremos que lo anterior implica que $\mathbf{x}^{\mathbf{v}} - \mathbf{x}^{\mathbf{w}} \in I'$, luego existe $\widetilde{f} = f - \alpha\left(\mathbf{x}^{\mathbf{v}} - \mathbf{x}^{\mathbf{w}}\right)$, el cual no puede estar en I', ya que de no ser así: $f \in I'$; luego como evidentemente: $lt(\widetilde{f}) < lt(f)$, esto nos lleva a una contradicción y tenemos que $I' = I_{\mathbf{A}}$.

Para finalizar demostremos lo que dejamos pendiente, sean $\mathbf{x}^{\mathbf{v}}$ y $\mathbf{x}^{\mathbf{w}}$ dos monomios mapeados bajo φ al mismo monomio, demostraremos que $\mathbf{x}^{\mathbf{v}} - \mathbf{x}^{\mathbf{w}} \in I'$. Sea $\mathbf{x}^{\mathbf{q}} = \gcd(\mathbf{x}^{\mathbf{v}}, \mathbf{x}^{\mathbf{w}})$, ahora definimos: $\mathbf{u}_+ = \mathbf{v} - \mathbf{q}$ y a $\mathbf{u}_- = \mathbf{w} - \mathbf{q}$. De donde se tiene: $\mathbf{x}^{\mathbf{v}} - \mathbf{x}^{\mathbf{w}} = \mathbf{x}^{\mathbf{q}}(\mathbf{x}^{\mathbf{u}_+} - \mathbf{x}^{\mathbf{u}_-})$ y es obvio que $\operatorname{supp}(\mathbf{u}_+) \cap \operatorname{supp}(\mathbf{u}_-) = \emptyset$. Claramente $\mathbf{x}^{\mathbf{u}_+}$ y $\mathbf{x}^{\mathbf{u}_-}$ son mapeados bajo φ al mismo monomio; lo que significa: $\mathrm{A}\mathbf{u}_+ = \mathrm{A}\mathbf{u}_-$, luego tomando $\mathbf{u} = \mathbf{u}_+ - \mathbf{u}_-$, se concluye $\mathbf{u} \in \ker A$, y llegamos a lo que queríamos demostrar: $\mathbf{x}^{\mathbf{v}} - \mathbf{x}^{\mathbf{w}} \in I'$ ■

***Corolario* 4** *Toda base de Grobner reducida de $I_{\boldsymbol{A}}$ consiste únicamente de binomios.*

***Demostración*.** Como ya vimos en el Teorema anterior, podemos elegir un sistema minimal de binomios que generen a $I_{\mathbf{A}}$, luego aplicamos el algoritmo de Buchberger lo que significa que aplicaremos solamente operaciones de reducción y los S-polinomios seguirán siendo binomios, luego tenemos el resultado. ■

***Corolario* 5** *Dos matrices enteras A y A' determinan el mismo ideal tórico si $A' \in SL_d(\boldsymbol{Z})A$.*

***Demostración*.** Es fácil ver que la siguiente igualdad:

$$\{\mathbf{u} \mid \mathbf{u} \in \mathbf{Z}^n, \mathbf{u} \in \ker A\} = \{\mathbf{u} \mid \mathbf{u} \in \mathbf{Z}^n, \mathbf{u} \in \ker TA\}$$

se cumple siempre que $\det T = \pm 1$ ■

***Proposición* 2.3** *Los siguientes enunciados son equivalentes:*

(*a*) *$I_{\boldsymbol{A}}$ define una variedad tórica proyectiva.*

(*b*) *$I_{\boldsymbol{A}}$ es homogeneneo con respecto a los grados $deg(x_i) = 1$.*

(*c*) *Los puntos $a_1, \ldots, a_n$ están en algún hyperplano en $\boldsymbol{R}^d$ que no pasa a través del origen.*

(*d*) *A puede escojerse de tal forma que $a_1, \ldots, a_n$ estén en el hyperplano $v_1 = 1$, donde $(v_1, \ldots, v_d)$ son las coordenadas en $\boldsymbol{R}^d$.*

Capítulo 3

Códigos Asociados a Matrices

3.1. Preliminares

En el capítulo pasado revisamos las definiciones de códigos de evaluación y de ideales tóricos. En este capítulo definiremos algunos códigos asociados a algunas matrices específicas y trabajeremos alrededor de dichos códigos encontrando su: longitud, distancia mínima y dimensión. Es importante decir que estos códigos son códigos MDS, definidos también en el capítulo pasado.

Sea $A = (a_{ij})$ una matriz $m \times (n+1)$ con entradas enteras no negativas a_{ij} y columnas no cero. Sean $K[X_0, \ldots, X_n]$ y $K[t_1, \ldots, t_m]$ dos anillos de polinomios sobre K. Entonces como vimos en la última sección, tomamos φ un homomorfismo de $K-$algebras:

$$\varphi : K[X_0, \ldots, X_n] \to K[t_1, \ldots, t_m]$$
$$\varphi(X_i) = t_1^{a_{1i}} \cdots t_m^{a_{mi}}$$

Sea I_A el ideal tórico asociado a nuestra matriz A

***Observación* 1** *Como vimos en la última sección podemos usar bases de Gröbner para calcular I_A, luego podemos usar Macaulay 2 para calcularlo [6].*

La variedad tórica determinada por la matriz A es el subconjunto del espacio proyectivo $\mathbb{P}_K^n$ dado por

$$X = \{(t_1^{a_{11}} \cdots t_m^{a_{m1}}, \ldots, t_1^{a_{1(n+1)}} \cdots t_m^{a_{m(n+1)}}) \in \mathbb{P}_K^n | \, t_1, \ldots, t_m \in K\}$$

Tomando siempre los valores $t_1, \ldots, t_m \in K$ de tal forma que definan un punto de $\mathbb{P}^n_K$.

Observación 2 *Este estudio generaliza muchos códigos de evaluación que han sido estudiados anteriormente. Por ejemplo, si tomamos la matriz identidad $(n+1) \times (n+1)$, tendremos que la variedad asociada a dicha matriz es todo el espacio proyectivo, luego los correspondientes códigos de evaluación son los códigos proyectivos Reed-Muller, los cuales son muy conocidos(cf. [17], [30]).*

Por otro lado , si consideramos la matriz $(n+1) \times (n+1)$ de la siguiente forma:

$$\begin{pmatrix} 1 & 1 & 1 & \ldots & 1 & 1 \\ 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 \end{pmatrix}$$

la variedad correspondiente a esta matriz es la que nos regresa al espacio afín (inmerso en el espacio proyectivo), y los códigos de evaluación son los Códigos Reed Muller generalizados, los cuales son también muy conocidos (cf. [4], [17]).

De esta forma, muchos de los casos particulares de códigos de evaluación trabajados con anterioridad (cf. [5], [24], [25], [26], [27],[16]) pueden ser descritos desde este punto de vista.

En particular, los códigos de evaluación que resultan de la Variedad de Segre, de la variedad de Veronesse y los códigos Generalizados Reed-Solomon pueden ser estudiados con este tipo de conceptos.

En las siguientes secciones trabajaremos algunas matrices, las cuales sólo tendrán 1's en el primer renglón y sus elementos en las otras entradas estarán en progresión aritmética. Los 1's en el primer renglón implican que el ideal tórico es homogeneo con la graduación usual.

3.2. Resultados principales

De ahora en adelante trabajaremos con matrices $m \times (n+1)$ que sean de la siguiente forma

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ a_2 & a_2+c_2 & a_2+2c_2 & \dots & a_2+nc_2 \\ a_3 & a_3+c_3 & a_3+2c_3 & \dots & a_3+nc_3 \\ \dots & \dots & \dots & \dots & \dots \\ a_m & a_m+c_m & a_m+2c_m & \dots & a_m+nc_m \end{pmatrix}$$

Donde $a_2, \dots, a_m, c_2, \dots, c_m$ son enteros positivos.

Con las condiciones anteriores, el conjunto X que se tiene, y que es una Variedad Tórica Proyectiva, está dado por:

$$X = \{(1, t_2^{c_2} \cdots t_m^{c_m}, t_2^{2c_2} \cdots t_m^{2c_m}, \dots, t_2^{nc_2} \cdots t_m^{nc_m}) |\, t_2, \dots, t_m \in K^*\}$$

Si $X = \{P_1, \dots, P_s\} \subset \mathbb{P}_K^n$, definamos el mapeo de evaluación, que esta dado de la siguiente forma:

$$ev_d : K[X_0, \dots, X_n]_d \to K^s,$$
$$ev_d(f) = (f(P_1), \dots, f(P_s))$$

Sea $C_X(d)$ el código lineal, el cual es la imagen de el mapeo de evaluación anterior, llamado el código de evaluación de orden d definido sobre la variedad tórica X, o asociado a la matriz A.

En la siguiente sección describimos el primer parámetro de este tipo de códigos.

3.2.1. La longitud del código $C_X(d)$

Con la notación usada anteriormene, la longitud del código de evaluación definido sobre la variedad tórica X se puede obtener con la ayuda del siguiente teorema:

Teorema 6 *La longitud s del código de evaluación $C_X(d)$ está dado por:*

$$s = \frac{q-1}{gcd(q-1,c_2,c_3,\ldots,c_m)}$$

Demostración.

Sea $K^* = \langle a \rangle$ y $t_i = a^{j_i}$ para toda $i = 1, \ldots, m$. Si tomamos $c := gcd(q-1, c_2, \ldots, c_m)$, entonce se tiene:

$$t_2^{c_2} \cdots t_m^{c_m} = a^{j_2c_2+\cdots+j_mc_m} = (a^c)^l$$

donde $j_2c_2 + \cdots + j_mc_m = cl$.

Más aún, el orden de el elemento a^c vienen dado por:

$$\circ(a^c) = \frac{q-1}{c}$$

De donde si tomamos $\alpha = a^c$ se tiene:

$$X = \{(1, \alpha^l, \alpha^{2l}, \ldots, \alpha^{nl}) : l = 1, \ldots, \tfrac{q-1}{c}\}$$

Por lo tanto:

$$\#X = \frac{q-1}{c}$$

que es lo que se quería demostrar. ■

3.2.2. La dimensión del código $C_X(d)$ y el $a-$invariante del ideal anulador I_X

En esta sección encontraremos la dimensión de los códigos de evaluación asociados a las matrices definidas anteriormente y el $a-$invariante de su correspondiente ideal anulador I_X. Usando la notación del teorema anterior se tiene:

$$X = \{(1, \alpha^l, \alpha^{2l}, \ldots, \alpha^{nl}) : l = 1, \ldots, \tfrac{q-1}{c}\}$$

donde $\alpha = a^c$, $K^* = \langle a \rangle$, $c = \gcd(q-1, c_2, \ldots, c_m)$ y $s = \#X = \frac{q-1}{c}$.

Por otro lado, trabajaremos con el conjunto Y dado por:

$$Y = \{(1, \alpha^l) \in \mathbb{P}^1_K : l = 1, \ldots, s\}$$

Entonces $s = \#X = \#Y$. Ahora usamos la siguiente notación: $S = K[X_0, \ldots, X_n]$, $S_1 = K[Y_0, Y_1]$, y

$$I_X = \langle f \in S : f(P) = 0 \text{ for all } P \in X \rangle$$

$$I_Y = \langle g \in S_1 : g(Q) = 0 \text{ for all } Q \in Y \rangle$$

los correspondientes ideales anuladores homogeneos asociados a X y Y.

Lema 2 *El ideal anulador I_Y viene dado por:*

$$I_Y = \langle Y_1^s - Y_0^s \rangle$$

Demostración. Sea F un polinomio homogeneo del ideal I_Y. Tomando el orden lexicográfico $Y_1 > Y_0$ aplicamos el algoritmo de la división de la siguiente forma:

$$F = G \cdot (Y_1^s - Y_0^s) + r$$

donde $G, r \in S_1$ y $r = 0$ o r es una combinación $K-$lineal de momomios ninguno de los cuales es divisible por Y_1^s.

Por lo tanto, $\deg_{Y_1} r < s$. Pero $0 = F(1, \alpha^l) = r(1, \alpha^l)$ para todo $l = 1, \ldots, s$ lo que significa que r tiene al menos s raices (visto como un polinomio en la variable Y_1). Luego se contradice que $\deg_{Y_1} r < s$. ■

Lema 3 *El $a-$invariante del ideal anulador I_Y es:*

$$a_Y = s - 2$$

Demostración. Del lema anterior sabemos que s es el menor grado de una componente homogenea no trivial del ideal I_Y , y recordando la proposición 2.2: $H_Y(d) = \binom{d+1}{1} = d+1$ si $d < s$. Luego $H_Y(s-2) = s-1 < \#Y$ y $H_Y(s-1) = s = \#Y$. De donde se concluye $a_Y = s - 2$. ■

Teorema 7 *La dimensión del código evaluación $C_X(d)$ está dado por:*

$$\dim_K C_X(d) = nd + 1 \quad si \quad nd < s$$

Demostración. Comencemos por definir el siguiente mapeo

$$\psi : S_d \longrightarrow S_1(nd)$$
$$f(X_0, \ldots, X_n) \longrightarrow f(Y_0^n, Y_0^{n-1}Y_1, \ldots, Y_1^n)$$

Donde $S_1(nd)$ es el conjunto de polinomios homogeneos de grado nd en el anillo S_1. Ahora mostremos que nuestro mapeo es suprayectivo, de donde será suficiente encontrar los monomios de la forma $Y_0^{nd-i}Y_1^i$ para $i = 0, \ldots, nd$. Si $i \leq d$ tomemos

$$\psi(X_0^{d-i}X_1^i) = Y_0^{n(d-i)}Y_0^{(n-1)i}Y_1^i = Y_0^{nd}Y_0^{-ni}Y_0^{ni}Y_0^iY_1^i = Y_0^{nd-i}Y_1^i$$

Así si $i > d$, con el algoritmo de la división se tiene: $i = dq_1 + r_1$, con $0 \leq r_1 < d$ de donde:

$$\psi(X_{q_1}^{d-r_1}X_{q_1+1}^{r_1}) = (Y_0^{n-q_1}Y_1^{q_1})^{d-r_1}(Y_0^{n-q_1-1}Y_1^{q_1+1})^{r_1} =$$

$$Y_0^{nd-nr_1-q_1d+q_1r_1}Y_1^{q_1d-q_1r_1}Y_0^{nr_1-q_1r_1-r_1}Y_1^{q_1r_1+r_1} =$$

$$Y_0^{nd-dq_1-r_1}Y_1^{dq_1+r_1} = Y_0^{nd-i}Y_1^i.$$

Luego ψ es un mapeo suprayectivo.
También es fácil ver que $\operatorname{Ker}\psi = I_X(d)$ y se tiene

$$S_d/I_X(d) \cong S_1(nd)$$

Por lo tanto $H_X(d) = H_Y(nd) = nd + 1$. Finalmente si $nd < s$ se tiene: $\dim_K C_X(d) = nd + 1$. ■

Observación 3 *En la demostración del teorema anterior mostramos que si $nd < s$ entonces $S_d/I_X(d) \cong S_1(nd)$, pero es obvio ver que como $I_Y(nd) = \{0\}$ (gracias a que sabemos que s es el menor grado de cualquier componente homegenea no trivial del ideal I_Y) se tiene: $S_d/I_X(d) \cong S_1(nd)/I_Y(nd)$ lo que prueba $H_X(d) = H_Y(nd)$ si $nd < s$. Más aún, el isomorfismo inducido entre $C_X(d)$ y $C_Y(nd)$ preserva el peso de las palabras del código, luego la distancia mínima de $C_X(d)$ es igual a la distancia mínima de $C_Y(nd)$.*

***Corolario* 6** *El $a-$invariante del ideal I_X está dado por:*

$$a_X = \begin{cases} j-1 & \text{if } r = 0 \\ j & \text{if } 0 < r < n \end{cases}$$

donde j es el cociente y r es el residuo cuando dividimos $s-1$ sobre n, luego $s-1 = nj+r$ con $0 \leq r < n$.

***Demostración*.** Si $0 < r < n$ entonces $H_X(j+1) = H_Y(nj+n) = H_Y(s+n-r-1)$. Pero $n-r-1 \geq 0$ y luego $H_X(j+1) = s$. Además, $H_X(j) = H_Y(nj) = H_Y(s-r-1)$. Pero como ya sabemos, por el lema anterior $s-r-1 \leq s-2 = a_Y$ se tiene $H_X(j) < s$. Lo que prueba $a_X = j$ si $0 < r < n$.

Si $r = 0$, $H_X(j) = H_Y(nj) = H_Y(s-1) = s$. Por otro lado, $H_X(j-1) = H_Y(nj-n) = H_Y(s-n-1) < s$. Por lo tanto $a_X = j-1$ si $r = 0$. ■

3.2.3. La distancia mínima del código $C_X(d)$

En esta sección encontraremos las distancia mínima del código $C_X(d)$ y veremos que el código será un código MDS.

***Teorema* 8** *Si $nd < s$ entonces las distancia mínima δ del código $C_X(d)$ viene dado por:*

$$\delta = s - nd$$

***Demostración*.** Comencemos por recordar que por la cota de Singleton se tiene: $(nd+1) + \delta \leq s+1$; lo que significa que $\delta \leq s - nd$.

Por otro lado, de la observacion 3 se sabe que δ también es la distancia mínima del código $C_Y(nd)$. Así es suficienete demostrar que cualquier palabra del código $C_Y(nd)$ tiene un peso de Hamming de al menos $s-nd$. Ahora sea $G(Y_0, Y_1) \in S_1(nd)$. Entonces $G(1, X_1)$ tiene grado $g \leq nd$ y por lo tanto tiene g o menos raices. Si Λ es la palabra asociada al polinomio $G(Y_0, Y_1)$, tenemos:

$$\Lambda = (G(1,\alpha), G(1,\alpha^2), \ldots, G(1,\alpha^s))$$

entonces:

$$w(\Lambda) \geq s - g \geq s - nd$$

Donde $w(\Lambda)$ es el peso de Hamming de la palabra Λ. De donde se concluye: $\delta \geq s - nd$. ■

Capítulo 4

Ejemplos con Macaulay

En este capítulo estudiaremos algunos ejemplos específicos de los códigos de evaluación definidos anteriormente, pero el aporte especial es que generaremos programas en Macaulay 2 (cf. [13]), de donde encontraremos los parámetros básicos de dichos códigos (longitud, dimensión y distancia mínima) y otras características de la variedad tórica X ($a-$invariante, series de Hilbert, ideal anulador).

4.1. Construcción del programa

Aquí construiremos paso a paso el programa que se usó para encontrar los resultados del capítulo anterior, dada una matriz iremos construyendo el programa alrededor de dicha matriz.

Sea la siguiente matriz 3×6 con $q = 81$, $c_2 = 8$, $c_3 = 28$, como se definió en la sección 3.2:

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 10 & 18 & 26 & 34 & 42 \\ 5 & 33 & 61 & 89 & 117 & 145 \end{pmatrix}$$

y trabajaremos con $K = GF(3^4) = \{0, 1, a, a^2, \ldots, a^{79}\}$ el campo con 81 elementos.

Primero declaramos el campo finito donde trabajaremos dando el número de elementos de nuestro campo como 3^4, ponemos a $q = 81$ para poder trabajar a q como el número de elementos del campo.

```
K=GF(3,4,Variable=>a);
q=81;
```

Luego definimos una función que nos proporcione el representante principal de cada clase de equivalencia en nuestro campo (recordando que estamos trabajando en $\mathbb{Z}_{3^4}$).

```
e:=method()
e(ZZ):=n->mod(n,p);
```

Ahora declaramos el anillo de polinomios $K[x_0, x_1, \ldots, x_5]$, y declararemos nuestra matriz; (es importante observar que cuando se declara una matriz en Macaulay cambia los renglones por las columnas y las columnas por renglones y comienza desde la entrada $(0, 0)$).

```
R=K[x_0..x_5];
A=matrix{{1,1,1,1,1,1},{2,10,18,26,34,42},
{5,33,61,89,117,145}};
```

Ahora declaramos una función que nos ayudará a encontrar los elementos de la variedad proyectiva asociada a la matriz A, recordemos que solo es necesario obtener los c_i's, que en este caso sería $5-2$ y $33-5$ o las entradas: $a_{11} - a_{01}$ y $a_{12} - a_{02}$:

```
f=(x,y)->x^(A_1_1-A_0_1)*y^(A_1_2-A_0_2);
```

X será nuestra variedad asociada a A, por lo tanto debemos declarar a ese conjunto inicialmente como conjunto vacío; ahora para obtener los elementos de X solo recordemos que para un elemento de X su primer entrada sera 1 y las demás potencias de los c_i's, así solo debemos recorrerlos valores por todos los elementos del campo $(q-1)$; luego escribimos una función que deje sólo un representante por cada elemento de X, y por último contamos los elementos de X:

```
X={};
i=0;
while i<q-1 do(j=0; while j<q-1 do (X=append(X,1,f(a^i,a^j),
(f(a^i,a^j))^2,(f(a^i,a^j))^3,(f(a^i,a^j))^4,
(f(a^i,a^j))^5);j=j+1);i=i+1)
```

```
X=unique X
#X
```

Ahora calcularemos el ideal asociado a la variedad X, esto se hará recordando rápidamente la forma en que se calcula el ideal asociado a un punto proyectivo, primero declararemos una función llamada *ide*, que nos dará los polinomios que anulan a cada punto de la variedad X.

Si nos damos cuenta primero buscará la primer entrada no cero del punto, y luego simplemente calculará los polinomios que anularán a las demás entradas, ésta es la razón por la cual se tienen 5 distintas opciones. Por último los ideales generados por cada punto estarán en una lista llamada *id*3.

```
ide=method ()

ide(List):= t ->(i=0;id3=; while i<#t do (if
t_i_0!=0 then id3=append(id3,ideal(t_i_0 * x_1-t_i_1 * x_0,
t_i_0 * x_2-t_i_2 * x_0, t_i_0*x_3 - t_i_3 * x_0,
t_i_0 * x_4 - t_i_4 * x_0 , t_i_0 * x_5 - t_i_5 * x_0))

else if t_i_1!=0 then id3=append(id3,ideal
(x_0, t_i_1 * x_2 - t_i_2 * x_1, t_i_1 * x_3 - t_i_3 * x_1,
t_i_1 * x_4 - t_i_4 * x_1, t_i_1 * x_5 - t_i_5 * x_1))

else if t_i_2!=0 then id3=append(id3,ideal(x_0,
x_1, t_i_2 * x_3 - t_i_3 * x_2, t_i_2 * x_4 - t_i_4 * x_2,
t_i_2 * x_5 - t_i_5 * x_2))

else if t_i_3!=0 then id3=append(id3,ideal(x_0, x_1, x_2,
t_i_3 * x_4 - t_i_4 * x_3, t_i_3 * x_5 - t_i_5 * x_3))

else if t_i_4!=0 then id3=append(id3,ideal(x_0, x_1, x_2,
x_3, t_i_4 * x_5 - t_i_5 * x_4))

else id3=append(id3,ideal(x_0, x_1, x_2, x_3, x_4));i=i+1))

ide(X)

id3
```

Como sabemos el ideal que anulará a X será la intersección de los ideales que anulan a cada punto de X. Entonces describimos la función $int3$ y luego se la aplicamos a $id3$ y la intesección se llamará J:

```
int3=method()
int3(List):=t->(i=0;J=ideal(x_0,x_1,x_2,x_3,x_4,x_5);
while i<#t do (J=intersect(J,t_i);i=i+1))
int3(id3)
J
```

Para conocer la dimensión del código y el $a-$invariante podemos usar la funciónde Hilbert, aquí calculamos dicha función para todos los códigos de orden menor que quince, y como sabemos el último lugar antes de que la función se empiece a repetir será el $a-$invariante.

```
toString J
cJ=coker gens J
i=0;
while i <15 do (print(hilbertFunction(i,cJ));i=i+1)
```

Por último calculamos la serie de Hilbert para el ideal J

```
hilbertSeries J
```

Y terminamos nuestro programa. A continuación expondremos los resultados de dos ejemplos, los cuales pueden ser obtenidos directamente del programa anterior o de los resultados de esta tesis.

4.2. Ejemplo I

Este ejemplo será con la matriz anterior y ya que tenemos el programa, será muy simple:

Sea $K = GF(3^4) = \{0, 1, a, a^2, \ldots, a^{79}\}$ el campo con 81 elementos y consideremos la siguiente matriz:

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 10 & 18 & 26 & 34 & 42 \\ 5 & 33 & 61 & 89 & 117 & 145 \end{pmatrix}$$

En este caso, $q = 81$, $c_2 = 8$, $c_3 = 28$ y entonces:

$$s = \#X = \frac{80}{gcd(80,8,28)} = 20$$

Además, la veriedad tórica proyectiva $X \subset \mathbb{P}^5_K$ es:

$$\begin{array}{l} X = \{(1,1,1,1,1,1), (1, a^{28}, a^{56}, a^4, a^{32}, a^{60}), \\ (1, a^{56}, a^{32}, a^8, a^{64}, a^{40}), (1, a^4, a^8, a^{12}, a^{16}, a^{20}), \\ (1, a^{32}, a^{64}, a^{16}, a^{48}, 1), (1, a^{60}, a^{40}, a^{20}, 1, a^{60}), \\ (1, a^8, a^{16}, a^{24}, a^{32}, a^{40}), (1, a^{36}, a^{72}, a^{28}, a^{64}, a^{20}), \\ (1, a^{64}, a^{48}, a^{32}, a^{16}, 1), (1, a^{12}, a^{24}, a^{36}, a^{48}, a^{60}), \\ (1, a^{40}, 1, a^{40}, 1, a^{40}), (1, a^{68}, a^{56}, a^{44}, a^{32}, a^{20}), \\ (1, a^{16}, a^{32}, a^{48}, a^{64}, 1), (1, a^{44}, a^8, a^{52}, a^{16}, a^{60}), \\ (1, a^{72}, a^{64}, a^{56}, a^{48}, a^{40}), (1, a^{20}, a^{40}, a^{60}, 1, a^{20}), \\ (1, a^{48}, a^{16}, a^{64}, a^{32}, 1), (1, a^{76}, a^{72}, a^{68}, a^{64}, a^{60}), \\ (1, a^{24}, a^{48}, a^{72}, a^{16}, a^{40}), (1, a^{52}, a^{24}, a^{76}, a^{48}, a^{20})\} \end{array}$$

Luego tenemos, $n = 5$, $s - 1 = 19 = 5(3) + 4$ de donde: $j = 3$ y $r = 4$. Por lo tanto el $a-$invariante es $j = 3$, entonces podemos trabajar con los códigos $C_X(2)$ y $C_X(3)$ con dimensiones $H_X(2) = 5(2)+1 = 11$ y $H_X(3) = 5(3)+1 = 16$, respectivamente.

Por nuestros resultados tenemos que la distancia mínima del código $C_X(2)$ es $\delta = 20 - 5(2) = 10$ y para el código de $C_X(3)$ es $\delta = 20 - 5(3) = 5$.

De hecho, la Serie de Hilbert viene dada por:

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

Ahora, si aplicamos el algoritmo usado en [6], pp. 179-182, se tiene que:

$$\begin{array}{l} I_{\overline{A}} = \langle X_4^2 - X_3X_5, X_3X_4 - X_2X_5, X_2X_4 - X_1X_5, X_1X_4 - X_0X_5, X_3^2 - \\ X_1X_5, X_2X_3 - X_0X_5, X_1X_3 - X_0X_4, X_2^2 - X_0X_4, X_1X_2 - X_0X_3, X_1^2 - X_0X_2\rangle \end{array}$$

Donde $I_{\overline{A}}$ es el ideal tórico sobre la matriz A, si trabajamos con la cerradura algebraica $\overline{K}$, del campo K.

Finalmente, el Ideal anulador del anillo de coordenadas de la variedad tórica X está dada por:

$$I_X = \langle I_{\overline{A}}, \{X_0^4 - X_5^4\}\rangle$$

4.3. Ejemplo II

Para éste ejemplo escribiremos primero la matriz y el campo, después el programa en Macaulay y por último los resultados.

Sea un campo con 32 elementos y con una matriz 3×4. Sea $K = GF(2^5) = \{0, 1, a, a^2, \ldots, a^{30}\}$ un campo con 32 elementos y la matriz A dada por:

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 7 & 13 & 19 & 25 \\ 4 & 14 & 24 & 34 \end{pmatrix}$$

En este caso $q = 32$, $c_2 = 6$, $c_3 = 10$. El programa asociado será:

```
K=GF(2,5,Variable=>a);
q=32;

R=K[x_0..x_3];
A=matrix{{1,1,1,1},{7,13,19,25},{4,14,24,34}};

f=(x,y)->x^(A_1_1-A_0_1)*y^(A_1_2-A_0_2);

X={};
i=0;
while i<q-1 do(j=0; while j<q-1 do (X = append(X,
{1, f(a^i,a^j), (f(a^i,a^j))^2, (f(a^i,a^j))^3})
;j=j+1);i=i+1)
X=unique X
toString X
#X

ide=method ()
ide(List):= t ->(i=0;id3={}; while
i<#t do (if t_i_0!=0 then id3 = append(id3, ideal gens
gb ideal (t_i_0 * x_1 - t_i_1 * x_0, t_i_0 * x_2
- t_i_2 * x_0, t_i_0 * x_3 - t_i_3 * x_0))

else if t_i_1!=0 then id3=append(id3, ideal gens gb ideal
(x_0, t_i_1 * x_2 - t_i_2 * x_1, t_i_1 * x_3 - t_i_3 * x_1))
```

```
else if t_i_2!=0 then id3=append(id3, ideal gens gb ideal
(x_0, x_1, t_i_2 * x_3 - t_i_3 * x_2))

else id3=append(id3,ideal gens gb ideal(x_0,x_1,x_2));i=i+1))
ide(X)
id3

int3=method()
int3(List):=t->
(i=0;J=ideal(x_0,x_1,x_2,x_3);while i<#t do
(J=intersect(J,t_i);i=i+1))
int3(id3)
J

cJ=coker gens J
i=0;
while i <15 do (print(hilbertFunction(i,cJ));i=i+1)
hilbertSeries J
```

Ahora según el programa y nuestros resultados tenemos:

$$s = \#X = \frac{31}{gcd(31,6,10)} = 31$$

Así la variedad tórica $X \subset \mathbb{P}^3_K$ es:

$$\begin{aligned} X = \{&(1,1,1,1),(1,a^{10},a^{20},a^{30}),(1,a^{20},a^{9},a^{29}),\\ &(1,a^{29},a^{27},a^{25}),(1,a^{8},a^{16},a^{24}),(1,a^{18},a^{5},a^{23}),\\ &(1,a^{28},a^{25},a^{22}),(1,a^{7},a^{14},a^{21}),(1,a^{17},a^{3},a^{20}),\\ &(1,a^{27},a^{23},a^{19}),(1,a^{6},a^{12},a^{18}),(1,a^{16},a,a^{17}),\\ &(1,a^{23},a^{15},a^{7}),(1,a^{2},a^{4},a^{6}),(1,a^{12},a^{24},a^{5}),\\ &(1,a^{22},a^{13},a^{4}),(1,a,a^{2},a^{3}),(1,a^{11},a^{22},a^{2}),\\ &(1,a^{24},a^{17},a^{10}),(1,a^{3},a^{6},a^{9}),(1,a^{13},a^{26},a^{8}),\\ &(1,a^{30},a^{29},a^{28}),(1,a^{9},a^{18},a^{27}),(1,a^{19},a^{7},a^{26}),\\ &(1,a^{25},a^{19},a^{13}),(1,a^{4},a^{8},a^{12}),(1,a^{14},a^{28},a^{11}),\\ &(1,a^{26},a^{21},a^{16}),(1,a^{5},a^{10},a^{15}),(1,a^{15},a^{30},a^{14}),\\ &(1,a^{21},a^{11},a)\} \end{aligned}$$

Por otro lado, $n = 3$, $s - 1 = 30 = 3(10)$ y entonces: $j = 10$ y $r = 0$. Por lo tanto el $a-$invariante es $j - 1 = 9$, por lo que podemos trabajar con los códigos $C_X(i)$ con dimensiones $H_X(i) = 3i + 1$ para $i = 2, \ldots, 9$.

La distancia mínima de los códigos $C_X(i)$ estándo dados por $\delta_i = 31 - 3i$ para $i = 2, \ldots, 9$ y todods ellos son códigos MDS.

También podemos encontrar la Serie de Hilbert:

$$F_X(t) = \frac{1+2t-3t^{11}}{(1-t)^2}$$

De la misma forma que en el ejemplo anterior obtenemos que el ideal tórico asociado a la matriz A para la cerradura algebraica del campo K:

$$I_{\overline{A}} = \{X_2^2 - X_1X_3, X_1X_2 - X_0X_3, X_1^2 - X_0X_2\}$$

Además obtenemos el ideal anulador del anillo de coordenadas de la variedad tórica X está dado por:

$$I_X = \langle I_{\overline{A}}, \{X_0^{11} - X_1X_3^{10}, X_0^{10}X_1 - X_2X_3^{10}, X_0^{10}X_2 - X_3^{11}\}\rangle$$

Bibliografía

[1] M. Boguslavsky, *On the Number of Solutions of Polynomial Systems*. Finite Fields and their Aplicattions, Vol. **3**, No. 4, pp. 287-299, Oct. (1997).

[2] B. Cooke. *Reed-Muller Error Correcting Codes*. MIT Undergraduate Journal of Mathematics, pp. 21-26, (1995).

[3] D. Cox, J. Little, D. O'Shea. *Ideals, Varieties and Algorithms*. UTM, Springer-Verlag, (1992).

[4] P. Delsarte, J.M. Goethals, F.J. MacWilliams. *On generalized Reed-Muller codes and their relatives*. Inform. and Control, Vol. **16**, pp. 403-422, (1970).

[5] I. Duursma, C. Rentería and H. Tapia-Recillas. *Reed-Muller codes on complete intersections*. Applicable Algebra in Engineering, Communication and Computting, AAECC **11**, 455-462 (2001).

[6] D. Eisenbud, D.R Grayson, M. Stillman, B. Sturmfels. Computations in Algebraic Geometry with Macaulay 2. *Springer Verlag* (2002).

[7] W. Fulton. *Algebraic curves: An introduction to algebraic geometry*. W.A. Benjamin, Inc. New York, Amsterdam, (1969).

[8] J.P. Hansen. *Points in Uniform Position and Maximum Distance Separable Codes, Zero Dimensional schemes*. Proc. Int. Conf., Ravello, 1992, Walter de Gruyter, Berlin, pp. 205-211, (1994).

[9] J. Harris. *Algebraic Geometry: A First Course*. Springer-Verlag, GTM, No. 133, (1992).

[10] R. Hartshorne. *Algebraic Geometry*. Springer-Verlag, (1977).

[11] T. Kasami, S. Lin, and W.W. Peterson. *New generalizations of the Reed-Muller codes. Part I: Primitive codes*. IEEE Trans. Inform. Theory, Vol. **IT-14, no. 2**, pp. 189-199, (1968).

[12] G. Lachaud. *The parameters of the projective Reed-Muller codes*. Discrete Mathematics **81**, pp. 217-221, (1990).

[13] D.R. Grayson, M. Stillman. *Macaulay 2*,(1999).

[14] F.J. MacWilliams and J.A. Sloane. *The theory of Error-Correcting Codes*. North-Holland Publ. Co., Amsterdam, New York, Oxford, (1977).

[15] M.A. Hernández de la Torre. *Aplicaciones del Algebra Conmutativa y la Geometría Algebraica a la Teoría de Códigos Algebraicos*. ESFM del IPN, Tesis de Maestría, (2000).

[16] C. Rentería, H. Tapia-Recillas, The $a-$ invariant of some Reed-Muller Codes, *Applicable Algebra in Engineering, Communication and Computing, AAECC, Springer* vol. **10**, No. 1, pp. 33-40 (1999).

[17] C. Rentería, H. Tapia-Recillas, Reed-Muller codes: An ideal Theory Approach, *Communications in Algebra*, **25** (2), pp. 401-413 (1997).

[18] C. Rentería, H. Tapia-Recillas. *A connection between the Veronese Map and Reed-Muller codes*. C. Numerantium Vol. **102**, pp. 175-181, (1994).

[19] C. Rentería, H. Tapia-Recillas. *Linear codes associated to the ideal of points in $\mathbb{P}^d$ and its canonical module*. Communications in Algebra **24 (3)**, pp. 1083-1090, (1996).

[20] C. Rentería, H. Tapia-Recillas. *Reed-Muller codes: An ideal theory approach*. Communications in Algebra **25 (2)**, pp. 401-413, (1997).

[21] C. Rentería, H. Tapia-Recillas. *The a-invariant of some Reed-Muller Codes*. Applicable Algebra in Engineering, Communications and Computing, (AAECC), Springer-Verlag, Vol. **10**, No. 1 (1999).

[22] C. Rentería, H. Tapia-Recillas. *Reed-Muller Type Codes on the Veronese Variety over Finite Fields*. Coding Theory, Cryptography and Related Areas (J. Buchmann, T. Hoholdt, H. Stichtenoth, H. Tapia-Recillas, eds.), ISBN 3-540-66248-0, Springer-Verlag, pp. 237-243, (2000).

[23] D.J. Mercier, R. Rolland. *Polynômes homogènes qui sánnulent sur léspace projectif* $\mathbb{P}^m(\mathbb{F}_q)$. Journal of Pure and Applied Algebra. Elsevier Science, Vol. **124 (1-3)**, pp. 227-240, (1998).

[24] M. González-Sarabia, C. Rentería and H. Tapia-Recillas. *Reed-Muller-Type Codes Over the Segre Variety*. Finite Fields and their Applications, Vol 8, No. 4, pp. 511-518, October (2002).

[25] M. González-Sarabia, C. Rentería. *The dual code of some Reed-Muller-type codes*. AAECC, Vol. 14, Number 5, pp. 329-333. Springer-Verlag, Berlín, (2004).

[26] M. González-Sarabia, C. Rentería and M.A. Hernández de la Torre. *Minimum distance and second generalized Hamming weight of two particular linear codes*. Congressus Numerantium Vols. 161 (2003), pp. 105-116.

[27] M. González-Sarabia, C. Rentería. *The Dual Code Arising From Segre's Variety*, Congressus Numerantium **174**, pp. 199-205 (2005).

[28] C.E. Shannon. *The Mathematical Theory of Communications*. Bell System Technical Journal 27, pp. 379-423, 623-656, (1948).

[29] A.V. Geramita, M. Kreuzer and L. Robbiano. *Cayley-Bacharach schemes and their canonical modules*. Transactions of the AMS, Vol. **339**, number 1, pp. 163-189, sept. (1993).

[30] A.B. Sörensen. *Projective Reed-Muller codes*. IEEE Trans. on Inform. Theory. vol. 37, **no. 6**, pp. 1567-1576, (1991).

[31] H. Stichtenoth. *Algebraic Function Fields and codes*. University Text, Springer-Verlag, (1993).

[32] M. Tsfasman and S. Vladut. *Algebraic-geometric codes*. Kluwer Academic Pub., Math. and its Appl. **58**, (1991).

[33] E.J. Weldon. *New Generalizations of the Reed-Muller codes. Part II: Nonprimitive codes*. Trans. Inform. Theory, Vol. **IT-14**, pp. 199-205, (1968).

[34] X. Youxin, C. Jin, F. Changgeng. *Implementation of coding and encryption in satellite channel*. Communication Technology Procedings, ICCT'96, Vol. **1**, pp. 31-34, (1996).