Universidad
de La Laguna

Usando bases de Gröbner en teoría de códigos

Using Gröbner Bases in coding theory

Adrián Cruz Guerra

Trabajo de Fin de Grado

Álgebra

Sección de Matemáticas

Facultad de Ciencias

Universidad de La Laguna

La Laguna, 16 de junio de 2016

Dra. Dña. **Evelia Rosa García Barroso**, con N.I.F. 42.851.422-F y Dra. Dña. **María Victoria Reyes Sánchez** con N.I.F. 42.040.774-V profesoras titulares de Álgebra adscritas al Departamento de Matemáticas, Estadística e Investigación Operativa de la Universidad de La Laguna.

C E R T I F I C A N

Que la presente memoria titulada:

"*Usando bases de Gröbner en teoría de códigos.*"

ha sido realizada bajo su dirección por D. **Adrián Cruz Guerra**, con N.I.F. 54.135.823-X.

Y para que así conste, en cumplimiento de la legislación vigente y a los efectos oportunos firman la presente en La Laguna a 16 de junio de 2016

Agradecimientos

A Evelia R. García Barroso
y Mª Victoria Reyes Sánchez,
por su inconmensurable ayuda,
trato cercano e impecable trabajo.

A mi familia y amigos, por
apoyarme en mi paso por la universidad.

Resumen

La finalidad principal de esta memoria es el estudio de la descodificación de algunos códigos correctores de errores mediante el uso de bases de Gröbner. Para ello se necesitará realizar un estudio previo de los códigos correctores de errores, algunas familias de éstos, así como algunas de sus propiedades y resultados más importantes.

En primer lugar se trabajará con el concepto de código corrector de error, de los que desarrollaremos el estudio de los códigos lineales. Asimismo se estudiarán algunas características de éstos y se señalarán algunos resultados de relevancia. A continuación estudiaremos algunas familias de códigos lineales, de los que distinguiremos los códicos cíclicos, y algunas particularizaciones de éstos, además de los códigos de evaluación sobre variedades afines. Por último, abordaremos el estudio de descodificación mediante el uso de bases de Gröbner, tanto de códigos cíclicos como de códigos de evaluación sobre variedades afines.

Palabras clave: Códigos lineales, Códigos cíclicos, Códigos de evaluación sobre variedades afines, Bases de Gröbner.

Abstract

This essay aims at the studying of some error-correcting codes through the Gröbner Bases. For this purpose, we need a preliminary study of error correcting codes, some families of them, as well as some properties and important results.

We first work with the concept of error correcting code, highlighting the linear codes. Additionally, we study some of their characteristics and we show some relevant results. Following, we study some families of linear codes, emphasising cyclic codes, and some particular cases, along with affine variety codes. Finally, we approach the study of decoding cyclic codes and affine variety codes, using Gröbner bases.

Keywords: *Linear codes, Cyclic codes, Affine variety codes, Gröbner bases.*

Índice general

Introducción

La Teoría de Códigos Correctores forma parte de una de las recientes disciplinas de las Matemáticas. Surge en los años 50, de la necesidad del manejo y la transmisión de información de una forma fiable y segura. Hasta entonces, la transmisión de información era deficiente pues cualquier tipo de *ruido*, debido al soporte o al medio de transmisión, podía perturbar la información que se quería transmitir. Es el uso de la Teoría de Códigos, y en particular el nacimiento de los códigos correctores de errores, lo que permitió aumentar la probabilidad de éxito en la transmisión de un mensaje.

La idea que fundamenta los códigos correctores de errores consiste en reescribir el mensaje que se desea transmitir añadiéndole información redudante que de alguna forma, controle el mensaje durante la transmisión. De este modo, si no han ocurrido muchos errores, el receptor podrá descodificar correctamente el mensaje enviado. Un ejemplo de codifiación se encuentra en el D.N.I., donde la letra es la información redundante que se ha añadido y determina si el número es correcto o no.

Aún siendo una teoría joven, diferentes áreas de las Matemáticas, como pueden ser el Álgebra Lineal y la Geometría Algebraica, han contribuido en su crecimiento. Por un lado, los *códigos lineales* aprovechan las propiedades de los espacios vectoriales y los resultados del Álgebra Lineal y el calculo matricial. Por otra parte, los *códigos de evaluación*, definidos a partir de los puntos de una variedad algebraica afín, incluyen a determinados códigos lineales como los Reed-Solomon que, bajo este punto de vista pueden ser descodificados mediante el uso de las conocidas como *bases de Gröbner*.

Esta memoria, basada en [6], está dividida en tres capítulos. En el primer capítulo se pretende introducir al lector en el campo de los códigos correctores de errores, destacando los denominados códigos lineales, que tienen estructura de espacio vectorial. Además se darán a conocer propiedades y resultados en relación a estos, como son la matriz generatriz y de control y la descodificación mediante el método síndrome-líder.

En el segundo capítulo se trabaja con diferentes familias de códigos lineales, en particular, con los códigos cíclicos, particularizaciones de estos como son los códigos BCH y Reed-Solomon, y los códigos por evaluación. Del mismo modo que en el primer capítulo, se presentan propiedades y resultados de estos códigos, donde se incluyen diferentes métodos de captura de error.

El tercer y último capítulo, comienza con una breve introducción a las bases de Gröbner. Para la preparación de la memoria hemos realizado un estudio sobre las bases de Gröbner que incluye desde el algoritmo de la división en varias variables hasta el algoritmo de Buchberger, pasando por las bases e Gröbner minimales y reducidas y los teoremas de eliminación y extensión, recogidos en [5].Sin emabrgo no se han incluido en el texto debido a la limitación de espacio, ya que nuestro objetivo principal es presentar el uso de las bases de Gröbner para la descodificación de códigos cíclicos y de evaluación. Así, las secciones de estos capítulos están dedicadas a explicar de forma detallada el método usado en ambos casos, donde se pone de manifiesto la importancia y necesidad de las bases de Gröbner.

Se completa toda la memoria con ejemplos de los métodos de codificación y descodificación presentados.

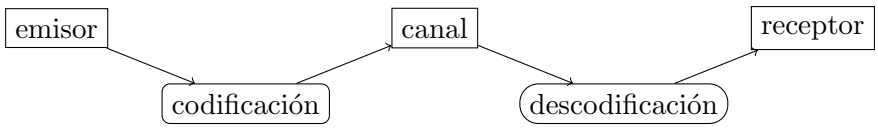
Capítulo 1

Códigos correctores de errores

En este primer capítulo introduciremos el concepto de *código corrector de errores* y destacaremos aquellos que son *lineales* mostrando algún ejemplo.

En primer lugar, y antes de empezar con la teoría de códigos correctores, es preciso destacar la importancia de dichos códigos y su funcionalidad. Supongamos que tenemos un mensaje, como una canción o un libro, que queremos codificar para posteriormente poder ser transmitido y leído. Una vez codificado el mensaje, en el momento de transmisión, puede sufrir algún cambio debido al soporte de transmisión, como por ejemplo un rayón en un CD, en este momento es cuando los códigos correctores realizan un papel fundamental a la hora de descodificar pues son capaces de detectar el error producido y corregirlo. Es por esto que los códigos correctores son tan importantes en la teoría de códigos pues no solo codifican un mensaje sino que muchas veces son capaces de corregir errores producidos en la transmisión para asegurar así que el mensaje recibido es el correcto.

Es preciso conocer que para la transmisión de información mediante la codificación se ha de tomar un conjunto finito, $\mathcal{A}$, o *alfabeto* y el conjunto de secuencias finitas de elementos de dicho alfabeto, que denotaremos por $\mathcal{A}^*$. En lo que sigue se tomará como alfabeto el cuerpo finito $\mathbb{F}_q$, siendo q una potencia de un número primo. Una vez determinado el alfabeto correspondiente y el método de codificación, la transmisión del mensaje quedará regida por el siguiente diagrama:



El proceso general de la codificación en estos tipos de códigos se basa en la toma de un mensaje $m = (x_1, x_2, ..., x_l) \in \mathcal{A}^l$ y elección de dos enteros $k < n$, con l múltiplo de k. Una vez llegados a este punto, dividiremos el mensaje en submensajes de longitud k que codificaremos por separado mediante la aplicación:

$$c : \mathcal{A}^k \longrightarrow \mathcal{A}^n$$

$$(x_1, ..., x_k) \longmapsto c(x_1, ..., x_k)$$

Así, el conjunto $\mathcal{C} = Im(c)$ es denominado código. Formalmente se tiene la siguiente definición:

Definición 1.1. Un código corrector de errores es un subconjunto $\mathcal{C} \subseteq \mathcal{A}^n$, siendo $\mathcal{A}$ un alfabeto finito y n un entero positivo. Los elementos de $\mathcal{C}$ son llamados palabra y n es su longitud.

Ejemplo 1.1. Uno de los alfabetos más conocidos es el binario, esto es, $\mathcal{A} = \mathbb{F}_2 = \{0, 1\}$. En dicho alfabeto podemos tomar códigos como:

$$\mathcal{C} =< \{(0, 0, 1, 0), (1, 0, 0, 1)\} >\subset \mathbb{F}_2^4,$$

donde $< F >$ denota el subespacio generado por F

Observaciones 1.1. Cada palabra de $\mathcal{C}$ contendrá k símbolos de información y $n - k$ símbolos redundantes, siendo así k/n la *tasa de transmisión* de $\mathcal{C}$.

Notamos que si $c \notin \mathcal{C}$ se ha cometido algún error en la transmisión e incluso cuando $c \in \mathcal{C}$ no estamos seguros de que el mensaje sea el correcto. Es por ello que a un código bien diseñado se le exige que contenga palabras muy diferentes entre sí. Para medir esta diferencia se define el siguiente concepto.

Definición 1.2. Dados $x, y \in \mathcal{A}^n$, llamamos distancia de Hamming entre x e y al número de coordenadas distintas que poseen, esto es:

$$d(x, y) = \#\{i/x_i \neq y_i\},$$

siedo x_i e y_i i-ésimas coordenadas de x e y respectivamente.

Ejemplo 1.2. Tomando el código descrito en el Ejemplo 1.1, tenemos que, las palabras

$$x = (1, 0, 0, 1) \text{ e } y = (1, 0, 1, 1)$$

verifican, bajo la distancia Hamming, que $d(x, y) = 1$.

Se comprueba que la función $d : \mathcal{A}^n \text{ x} \mathcal{A}^n \to \mathbb{N}$ tal que $d(x, y) = \#\{i/x_i \neq y_i\}$ es una distancia en $\mathcal{A}^n$. Notamos que la capacidad correctora vendrá dada por la *distancia mínima del código*, es decir, por:

$$d = d(\mathcal{C}) = min\, d(x, y) = min\#\{i/x_i \neq y_i\},$$

pues recibido un vector $x \in \mathcal{A}^n$ será descodificado por la palabra $c \in \mathcal{C}$ que minimice la distancia entre ellos. Si el número de errores no supera $\lfloor (d-1)/2 \rfloor$ la palabra corregida coincide con la realmente enviada. Esto nos indica que nuestro código será capaz de corregir $\lfloor (d-1)/2 \rfloor$ errores y detectar $d - 1$.

Uno de los objetivos de la teoría de códigos es encontrar un código que maximice k/n (tasa de transmisión) y d/n, o encuentre un equilibrio entre ellos. Una de las familias de códigos más conocidos es la de *códigos lineales*.

1.1. Códigos lineales

Definición 1.3. Un código lineal q-ario de longitud n es un subespacio vectorial $\mathcal{C} \subseteq \mathbb{F}_q^n$. Se denotará como código lineal del tipo $[n, k, d]$, esto es, de longitud n, dimension k y distancia mínima d.

Ejemplo 1.3. El código del Ejemplo 1.1 es un código lineal, pues $\mathcal{C}$ es subespacio vectorial de $\mathbb{F}_2^4$.

Ejemplo 1.4. Tomando el cuerpo $\mathbb{F}_2^4$, el subespacio vectorial generado por

$$\mathcal{B} = \{(0,0,0,1), (0,0,1,0)\}$$

es un código lineal de longitud 4 y dimensión 2.

Los códigos lineales, al igual que los subespacios vectoriales pueden ser descritos de dos maneras diferentes, mediante la matriz generatriz o mediante una matriz de control.

1.1.1. Matriz generatriz y matriz de control

Sabemos que todo subespacio vectorial posee una base y, asociada a ésta, una matriz que lo determina. Esta matriz será la denominada *matriz generatriz* de un código.

Definición 1.4. Llamaremos matriz generatriz de $\mathcal{C}$ a la matriz de una aplicación lineal inyectiva $c : \mathbb{F}_q^k \to \mathcal{C} \subset \mathbb{F}_q^n$, es decir, a una matriz de tamaño $k \times n$ y rango k, cuyas filas son una base de $\mathcal{C}$.

Ejemplo 1.5. El código lineal $\mathcal{C}_1$ descrito en el Ejemplo 1.4 tiene como matriz generatriz

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

Notemos que la dimensión de la matriz es 2×4.

Una vez obtenida la matriz generatriz G, para codificar un mensaje $a \in \mathbb{F}_q^k$ bastará con multiplicar el mensaje por dicha matriz, esto es, aG.

Ejemplo 1.6. Tomando $\mathcal{C}$ el código del Ejemplo 1.5 cuya matriz de generatriz es

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

queda claro, que

$$\mathcal{C} = \{(x_1, x_2)G = (0, 0, x_1, x_2) / x_1, x_2 \in \mathbb{F}_2\}.$$

Sabemos, que la base de un subespacio vectorial no es única, es por ello que la matriz generatriz de un código tampoco lo será, luego, atendiendo a lo anterior, se pueden obtener diferentes presentaciones de un mismo código según la matriz escogida. Una de las más

usadas es la *codificación sistemática*, la cual genera un código de la forma $(a, z) \in \mathbb{F}_q^k \times \mathbb{F}_q^{n-k}$, siendo a el mensaje. Es evidente que la codificación será sistemática si la matriz generatriz es de la forma $G = (I_k, C)$, donde I_k denota la matriz identidad $k \times k$. A la forma (I_k, C) de la matriz generatriz G se la denomina forma *estándar*.

Definición 1.5. Diremos que dos códigos $\mathcal{C}_1$, $\mathcal{C}_2$ de la misma longitud n, sobre $\mathbb{F}_q$ son equivalentes si existe una permutación $\sigma \in S_n$ tal que:

$$\mathcal{C}_2 = \{\sigma(c) = (c_{\sigma(0)}, ..., c_{\sigma(n-1)}) / \, c = (c_0, ..., c_{n-1}) \in \mathcal{C}_1\},$$

siendo S_n el grupo de permutaciones de n elementos.

Se puede probar que todo código es equivalente a uno sistemático.

Ejemplo 1.7. Tomando el código $\mathcal{C}_1$ del Ejemplo 1.5, con base del subespacio vectorial $\mathcal{B} = \{(0,0,0,1), (0,0,1,0)\}$ y aplicando la permutación σ a la base, de modo que

$$\sigma(\beta_1) = (0,1,0,0) \text{ y } \sigma(\beta_2) = (1,0,0,0)$$

se tiene el código $\mathcal{C}_2$ con matriz generatriz

$$G_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

en su forma sitemática, esto es

$$\mathcal{C}_2 = \{(x_1, x_2)G_2 = (x_1, x_2, 0, 0) / x_1, x_2 \in \mathbb{F}_2\}.$$

Como se ha destacado anteriormente, al igual que los subespacios vectoriales, existe otra forma de describir a los códigos lineales y es mediante su *matriz de control*. Esta matriz surge de la idea de describrir los subespacios vectoriales mediante ecuaciones implícitas.

Definición 1.6. Diremos que una matriz H es una matriz de control del código $\mathcal{C}$ si para todo vector $x \in \mathbb{F}_q^n$ se verifica que $x \in \mathcal{C}$ si y sólo si $Hx^t = 0$.

Observaciones 1.2. Notemos que si $\mathcal{C}$ es del tipo $[n, k, d]$, la matriz de control tendrá tamaño $(n-k) \times n$ y rango $n - k$.

Proposición 1.1. *Si G y H son matrices generatriz y de control de $\mathcal{C}$ respectivamente, entonces $GH^t = 0$.*

Demostración. En primer lugar observamos que

$$GH^t = 0 \iff HG^t = 0.$$

Y esto se comprueba de una manera sencilla, pues las columna de G^t forman una base de $\mathcal{C}$ y por tanto al multiplicarlas por la matriz de control G se obtiene un cero, por definición. □

Ejemplo 1.8. La matriz de control del código $\mathcal{C}_1$ del Ejemplo 1.5 es

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

Observamos que se verifica la Proposición 1.1, pues, efectivamente $GH^t = 0$.

Además, se cumple el siguiente resultado.

Proposición 1.2. *Sean $\mathcal{C}$ un código y $G = (I_k, C)$ una matriz generatriz. La matriz $H = (-C^t, I_{n-k})$ es una matriz de control para $\mathcal{C}$, y diremos que es una matriz de control que está en su forma estándar.*

Una de las aplicaciones de la matriz de control es la de ayudar en el cálculo de la distancia mínima. Veamos con los siguientes conceptos como es esto posible.

Definición 1.7. Sea $x = (x_1, \cdots, x_n) \in \mathbb{F}_q^n$. Llamaremos soporte de x al conjunto

$$sop(x) = \{i/1 \leq i \leq n, x_i \neq 0\}.$$

Además, denominaremos peso de Hamming de x a $w(x) = \#sop(x) = d(x, 0)$.

Observaciones 1.3. La aplicación w, así definida, es una norma en $\mathbb{F}_q^n$, cuya distancia asociada es d.

Definición 1.8. El peso mínimo de un código se define por

$$w(\mathcal{C}) = min\{w(c)/c \in \mathcal{C}, c \neq 0\}.$$

Lema 1.3. *En un código lineal, la distancia mínima es igual al peso mínimo.*

Demostración. Sea $\mathcal{C}$ un código, notamos que

$$d(x, y) = w(x - y) \tag{1.1}$$

para cualquier $x, y \in \mathcal{C}$. Por tanto, supongamos $d(\mathcal{C})$ la distancia mínima del código, entonces existe $x, y \in \mathcal{C}$ tal que $d(x, y) = d(\mathcal{C})$. Al tratarse de un subespacio vectorial $x - y \in \mathcal{C}$ y por (1.1) se tiene que $d(\mathcal{C}) = w(x - y)$, por tanto $d(\mathcal{C}) \leq w(\mathcal{C})$.

Supongamos $x \in \mathcal{C}$ tal que $w(x) = w(\mathcal{C})$. Entonces $d(x, 0) = w(x) = w(\mathcal{C})$, luego $d(\mathcal{C}) \leq w(\mathcal{C})$. Con esto podemos concluir que $d(\mathcal{C}) = w(\mathcal{C})$. □

Proposición 1.4. *Sea $\mathcal{C}$ un código lineal de matriz de control H y distancia mínima d y sea $r \in \mathbb{N}$. Entonces $r < d$ si, y solo si, cualesquieras r columnas de H son linealmente independientes. Por tanto, la distancia mínima de $\mathcal{C}$ coincide con el menor cardinal de un conjunto de columnas linealmente dependientes de H.*

Demostración. Veamos que cualesquiera r columnas de H son linealmente independientes, si y solo si, para ningún vector de peso menor o igual a r sucede que $Hx^t = 0$, con esto quedaría probada la proposición.

Sea x un vector de peso menor o igual a r, entonces, por definición, tiene a lo sumo r componentes distintas de cero. Supongamos que $Hx^t = 0$, entonces existe una combinación lineal de al menos r columnas de H que da cero, esto es, existen r columnas de H dependientes.

Supongamos que existen r columnas de H que son dependientes. Entonces, podemos encontrar un vector x de peso $w(x) = r$ tal que $Hx^t = 0$.

□

Corolario 1.5. *(Cota de Singleton). La distancia mínima de un código lineal* $[n, k]$*, verifica* $d \leq n - k + 1$*.*

Definición 1.9. Los códigos que alcanzan la cota de Singleton son llamados de máxima distancia de separación (MDS).

1.1.2. Dualidad

En el apartado anterior hemos visto cómo la matriz de control y la matriz generatriz determinan un mismo código de forma distinta. Lo natural sería preguntarse qué ocurriría si tomáramos la matriz de control como matriz generatriz de un código. Es así como se origina el concepto de *código dual*.

Definición 1.10. Sea $\mathcal{C}$ un código cuyas matrices generatriz y de control son G y H respectivamente. Se denomina código dual de $\mathcal{C}$ al código cuya matriz generatriz es H. Se denotará por $\mathcal{C}^{\perp}$.

Ejemplo 1.9. Como adelantamos en el Ejemplo 1.8, el código $\mathcal{C}_2$ es el dual del código $\mathcal{C}_1$.

Observaciones 1.4. Sea $\mathcal{C}$ un código con matriz generatriz G y matriz de control H, entonces:

1. Podemos apreciar que si H, matriz de control de $\mathcal{C}$ de dimensión k, es la matriz generatriz de $\mathcal{C}^{\perp}$, la dimensión de $\mathcal{C}^{\perp}$ será $n - k$.

2. Por otro lado, G tomará el papel de matriz de control pues la igualdad $GH^t = 0$ implica que $HG^t = 0$.

A continuación veamos cómo caracterizar dichos códigos en el caso de los códigos lineales.

Proposición 1.6. *Si* $\mathcal{C}$ *es un código lineal, entonces su dual* $\mathcal{C}^{\perp}$ *es el espacio ortogonal de* $\mathcal{C}$ *con respecto a la forma bilineal*

$$< u, v >= \sum u_i v_i \in \mathbb{F}_q.$$

1.1.3. Descodificación

Una vez introducidos los códigos lineales y algunas de sus propiedades, pasamos a mostrar un método de descodificación de los mismos. En este apartado introduciremos algunos conceptos necesarios para la descodificación así como daremos a conocer el *método del líder*.

En primer lugar es importante tener claro qué idea seguirá nuestro método de descodificación para posteriormente adentrarnos en él. Sea $\mathcal{C}$ un código lineal $[n, k, d]$ sobre $\mathbb{F}_q^n$, como se dijo al inicio del capítulo la idea que seguiremos será la de tomar nuestro mensaje $y = c + e$, donde c denota el mensaje original y e el error, y descodificarlo por la palabra más cercana de $\mathcal{C}$.

Definición 1.11. Llamaremos síndrome de y al vector $s(y) = Hy^t \in \mathbb{F}_q^{n-k}$, donde H denota a la matriz de control.

Observaciones 1.5.

1. Notamos que $y \in \mathcal{C}$ si, y solo si, $s(y) = 0$ por la definición de la matriz de control.

2. En caso de tener $y = c + e$, entonces $s(y) = s(c + e) = s(c) + s(e) = s(e)$. Luego una vez conocido el síndrome del mensaje conocemos el síndrome del error.

Proposición 1.7. *El síndrome del vector recibido y es una combinación lineal de las columnas de H correspondientes a las posiciones de error.*

Para desarrollar el algoritmo del líder vamos a tomar el espacio vectorial cociente $\mathbb{F}_q^n/\mathcal{C}$. Observamos que los elementos de $\mathbb{F}_q^n/\mathcal{C}$ son clases de equivalencia, donde cada clase posee $\#\mathcal{C} = q^{n-k}$ elementos, ya que la dimensión del espacio vectorial cociente es $n - k$.

Observaciones 1.6. Nótese que $u - v \in \mathcal{C}$ si, y solo si, $s(u) = s(v)$, por tanto recibido y se conoce la clase a la que pertenece el error.

Definición 1.12. Si en una clase existe un elemento de peso mínimo, éste recibirá el nombre de líder de la clase cuando su peso sea menor o igual que t (considerando t la capacidad correctora del código).

Proposición 1.8. *Cada clase de $\mathbb{F}_q^n/\mathcal{C}$ posee a lo más un elemento de peso $\leq t$.*

Demostración. Sea $\mathcal{C}$ un código con capacidad correctora $\frac{d(\mathcal{C})-1}{2}$. Supongamo que existe u y v, de peso menor o igual a t,en la misma clase. Entonces $u - v \in \mathcal{C}$ y además $w(u - v) \leq w(u) + w(v) \leq 2t < d(\mathcal{C})$.

□

Nos encontramos en disposición de describir el algoritmo del líder. Sea y el vector recibido, deseamos encontrar la palabra del código que minimice la distancia a y, entonces sabiendo que la clase de y es

$$[y] = \{y - c, c \in \mathcal{C}\},$$

una vez calculado el líder de la clase, es decir, aquel que minimice $d(y, c)$, no tenemos más que tomarlo como error y descodificarlo escogiendo como mensaje la diferencia $c = y - e$. Observamos que esta descodificación requiere de la existencia del elemento líder pues en caso contrario fallaría.

Para llevar a cabo el proceso debemos construir una tabla síndrome-líder, con dos columnas y tantas filas como clases haya en $\mathbb{F}_q^n/\mathcal{C}$. Entonces, calculamos el síndrome de nuestro vector recibido y y lo buscamos en la tabla, el vector líder que lo acompaña será el que tome el papel de error, descodificando el vector de la forma $c = y - e$.

Ejemplo 1.10. Sea el cuerpo $\mathbb{F}_2$. Tomamos el código

$$\mathcal{C} =< (1,1,1,0,0,0), (0,0,0,1,1,1) >\subset \mathbb{F}_2^6.$$

Se comprueba que se trata de un código de dimensión 2 y matriz de generatriz y de control

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

respectivamente. Además, el subespacio vectorial cociente $\mathbb{F}_2^6/\mathcal{C}$ tiene dimensión 4 y la tabla síndrome-líder obtenida es la siguiente:

Síndrome	Líder	Síndrome	Líder
(0, 0, 0, 0)	(0, 0, 0, 0, 0, 0)	(1, 0, 0, 1)	
(1, 0, 0, 0)	(1, 0, 0, 0, 0, 0)	(1, 1, 0, 1)	
(0, 1, 0, 0)	(0, 1, 0, 0, 0, 0)	(0, 1, 1, 0)	
(1, 1, 0, 0)	(0, 0, 1, 0, 0, 0)	(0, 1, 0, 1)	
(0, 0, 1, 0)	(0, 0, 0, 1, 0, 0)	(0, 1, 1, 1)	
(0, 0, 0, 1)	(0, 0, 0, 0, 1, 0)	(1, 1, 1, 0)	
(0, 0, 1, 1)	(0, 0, 0, 0, 0, 1)	(1, 1, 0, 1)	
(1, 0, 1, 0)		(1, 1, 1, 1)	

Cuadro 1.1: Tabla Síndrome-Líder

Supongamos recibido el mensaje $y = (0, 0, 1, 1, 1, 1)$, su síndrome es $s(y) = (1, 1, 0, 0)$, que aparece en la cuarta fila de la primera columna de síndromes. Por tanto, asumimos por error el vector $e = (0, 0, 1, 0, 0, 0)$ y como consecuencia otenemos que $c = y - e = (0, 0, 0, 1, 1, 1)$.

Capítulo 2

Familias de códigos correctores de errores

En este capítulo mostraremos algunas familias de códigos lineales. En primer lugar estudiaremos los códigos *cíclicos* y algunas de sus propiedades, a continuación nos centraremos en el estudio de los *códigos BCH*, que son un caso particular de los códigos cíclicos. Por último, analizaremos un tipo de códigos BCH, los denominados códigos *Reed-Solomon*.

2.1. Códigos cíclicos

Los códigos cíclicos surgen en el año 1957 con un artículo de E. Prange. Su riqueza y enormes propiedades hacen interesante el estudio de estos códigos, obteniendo así, hoy en día, numerosos artículos que giran en torno a ellos. Para empezar a estudiarlos, veamos cuál es su definición formal.

Definición 2.1. Un código lineal $\mathcal{C}$ de longitud n sobre $\mathbb{F}_q$, es cíclico si para cada $(c_0, c_1, ...c_{n-1}) \in \mathcal{C}$, se verifica que $(c_1, c_2, ...c_{n-1}, c_0) \in \mathcal{C}$.

Ejemplo 2.1. El código

$$\mathcal{C} = \{(0,0), (0,1)\} \subset \mathbb{F}_2^2$$

no es un código cíclico, pues $(1,0) \notin \mathcal{C}$.

Ejemplo 2.2. El código

$$\mathcal{C} = \{(0,0,0), (0,1,1), (1,1,0), (1,0,1)\} \subset \mathbb{F}_2^3$$

es un código cíclico con matriz generatriz

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

En el estudio de los códigos cíclicos vamos a tomar el espacio vectorial de los polinomios con coeficientes en $\mathbb{F}_q$ y grado menor que n, denotado por $\mathbb{F}_q[X]_{n-1}$, y el anillo cociente $A_{q,n} = \mathbb{F}_q[X]/(X^n - 1)$. Observamos que ambos espacios son isomorfos a $\mathbb{F}_q^n$, y podremos interpretar los elementos del código, indistintamente, como vectores, polinomios o clases de equivalencia. Además impondremos que $m.c.d(q, n) = 1$ para garantizar de este modo que $X^n - 1$ no tenga raíces múltiples.

Para caracterizar los códigos cíclicos y trabajar con ellos de una manera más sencilla se presenta el siguiente resultado que relaciona esta familia de códigos con los ideales del anillo cociente $A_{q,n} = \mathbb{F}_q[X]/(X^n - 1)$.

Teorema 2.1. *Sea $\mathcal{C}$ un código lineal no nulo de longitud n sobre el cuerpo finito $\mathbb{F}_q$. Diremos que el código $\mathcal{C}$ es cíclico si, y solo si, considerado incluido en el anillo $A_{q,n}$, es un ideal.*

Teniendo en cuenta el resultado anterior y que el anillo cociente $A_{q,n} = \mathbb{F}_q[X]/(X^n - 1)$ es un dominio de ideales principales surge el siguiente corolario.

Corolario 2.2. *Dado un código cíclico no nulo $\mathcal{C}$ de longitud n, existe un único polinomio mónico $g(X) \in \mathbb{F}_q[X]$, divisor de $X^n - 1$, tal que $\mathcal{C} = (g(X))$. En consecuencia, los elementos de $\mathcal{C}$ pueden identificarse con los polinomios de grado menor que n y múltiplos de $g(X)$.*

2.1.1. Matriz generatriz y matriz de control

Como los códigos cíclicos son una subfamilia de los códigos lineales, podremos definirlos mediante, la matriz de control y la matriz generatriz. Recordemos que la matriz generatriz es aquella cuyas filas conforman una base del espacio, es por ello que el siguiente resultado nos resultará muy útil.

Proposición 2.3. *Sea $\mathcal{C}$ un código cíclico de longitud n sobre $\mathbb{F}_q$ con polinomio generador $g(X)$ de grado $n - k$. El conjunto*

$$\{g(X), Xg(X), ...X^{k-1}g(X)\} \tag{2.1}$$

es una base de $\mathcal{C}$.

Demostración. En primer lugar veamos que se trata de un conjunto generador de $\mathcal{C}$. Para ello tomamos $g(X)f(X) \in \mathcal{C}$, por el Corolario 2.2, podemos suponer sin pérdida de generalidad que $deg(f(X)) < k$. Escribimos entonces

$$f(X) = a_0 + a_1X + \ldots + a_{k-1}X^{k-1}.$$

Por tanto, tenemos que

$$g(X)f(X) = a_0g(X) + a_1Xg(X) + \ldots + a_{k-1}X^{k-1}g(X).$$

Notamos que para cualquier elemento del código hemos encontrado una combinación lineal del conjunto (2.1) que lo genera.

Veamos ahora que se trata de un conjunto libre. Para ello tomamos

$$b_0 g(X) + b_1 X g(X) + \ldots + b_{k-1} X^{k-1} g(X) = 0.$$

Si $b(X) = b_0 + b_1 X + \ldots + b_{k-1} X^{k-1}$, entonces $b(X)g(X) = 0$ si, y solo si, $b(X) = 0$, pues $A_{q,n}$ es un dominio de integridad y $g(X) \neq 0$. □

Corolario 2.4. *Un código cíclico de longitud n y polinomio generador* $g(X) = g_0 + g_1 X + ... + g_{n-k} X^{n-k}$ *tiene matriz generatriz:*

$$\begin{pmatrix} g_0 & g_1 & g_2 & ... & g_{n-k} & 0 & 0 & 0 & ... & 0 \\ 0 & g_0 & g_1 & g_2 & ... & g_{n-k} & 0 & 0 & ... & 0 \\ & 0 & . & . & . & & . & & & \\ & & & . & . & . & & . & & \\ & & & & . & . & . & & . & 0 \\ 0 & 0 & ... & 0 & 0 & g_0 & g_1 & g_2 & ... & g_{n-k} \end{pmatrix}.$$

Ejemplo 2.3. Sean el cuerpo $\mathbb{F}_2$ y el anillo de polinomios $\mathbb{F}_2[X]$. Tomemos $g(X) = X + 1$, divisor de $X^3 - 1$ en $\mathbb{F}_2[X]$ y definimos el código cíclico de longitud $n = 3$, dimensión $k = 2$ y polinomio generador $g(X)$. Una matriz generatriz será

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

Notemos que tal código coincide con el código descrito en el Ejemplo 2.2.

Una vez obtenida la matriz generatriz del código es sencillo codificar un mensaje. En este caso, la codificación de un mensaje, que será interpretado como un polinomio $a(X)$ de grado menor que k, se podrá hacer mediante la matriz generatriz del código o simplemente tomando

$$c(X) = g(X)a(X) \in \mathcal{C},$$

siendo $g(X)$ el polinomio generador de $\mathcal{C}$.

Como se ha tratado en la Subsección 1.1.1, para cualquier código lineal es posible realizar una codificación sistemática, por lo tanto, en particular para cualquier código cíclico. En este caso su codificación será tan sencilla como realizar la siguiente división euclídea:

$$X^{n-k} a(X) = g(X)q(X) + r(X),$$

con $deg(r(X)) \lneq deg(g(X)) = n - k$. Ell mensaje codificado es precisamente:

$$X^{n-k}a(X) - r(X),$$

notando que el mensaje original aparece en las últimas k posiciones.

Ejemplo 2.4. Tomando el código del Ejemplo 2.3, y el mensaje $a(X) = 1$, codificaremos sistemáticamente de la siguiente forma:

$$X^2 = (X+1)(X+1) + 1.$$

Entonces el mensaje queda codificado por

$$c(X) = X^2 + 1.$$

Para introducir la matriz de control de $\mathcal{C}$ es preciso presentar un nuevo concepto que nos facilitará el manejo de la misma.

Definición 2.2. Si $\mathcal{C}$ es un código cíclico de longitud n, con polinomio generador $g(X)$ de grado $n-k$, llamaremos polinomio de control de $\mathcal{C}$ a

$$h(X) = \tfrac{X^n-1}{g(X)} = h_0 + h_1X + ... + h_kX^k.$$

Observamos que para cualquier elemento de la forma $f(X)g(X) \in \mathcal{C} = (g(X))$ se tiene que

$$h(X)f(X)g(X) = \tfrac{X^n-1}{g(X)}g(X)f(X) = (X^n-1)f(X).$$

Luego en el cociente $A_{q,n}$ se cumple que $h(X)(f(X)g(X)) = 0$, para cualquier $f(X)g(X) \in \mathcal{C}$.

Proposición 2.5. *Con la notación de la Definición 2.2, la matriz*

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

es una matriz de control de $\mathcal{C}$, cuyo tamaño es $(n-k) \times n$.

Ejemplo 2.5. Tomando el Ejemplo 2.3, tenemos que

$$h(X) = \frac{X^3-1}{X+1} = X^2 + X + 1.$$

Por tanto la matriz de control queda

$$H = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}.$$

Observaciones 2.1. Es preciso notar que el polinomio generador del código dual de $\mathcal{C}$ no será $h(X)$, sino $h'(X) = h_0^{-1}X^k h(X^{-1}) = h_0^{-1}(h_0X^k + h_1X^{k-1} + ... + h_k)$. Además $h'(X)$ es un divisor de $X^n - 1$ pues multiplicando por X^n la igualdad

$$h(X^{-1})g(X^{-1}) = X^{-n} - 1$$

deducimos

$$X^k h(X^{-1})X^{n-k}g(X^{-1}) = 1 - X^n,$$

y apreciamos que el dual de un código cíclico es también cíclico.

2.1.2. Ceros de un código cíclico

Una de las características principales de los códigos cíclicos es que pueden definirse o bien a partir de un polinomio, como hemos visto anteriormente, o bien a partir de una serie de ceros.

Sea $X^n - 1 = f_1(X)\cdots f_m(X)$ su descomposición en factores irreducibles, y sea α_i raíz de $f_i(X)$. Tomemos el código generado por $f_i(X)$.

Observamos que $\mathcal{C} = (f_i(X)) = \{c(X)/c(\alpha_i) = 0\}$ y en general para un $g(X) = f_1(X)\cdots f_r(X)$ se tiene que

$$\mathcal{C} = (g(X)) = (f_1(X)\cdots f_r(X)) = \{c(X)/c(\alpha_1) = ... = c(\alpha_r) = 0\}.$$

Nótese entonces que, como se señaló anteriormente, los códigos cíclicos pueden definirse a partir de una serie de raíces n-ésimas de la unidad adecuadas. Por ejemplo, si tomamos un conjunto de elementos $\{\alpha_1, ..., \alpha_r\}$ raíces n-ésimas de la unidad, en una extensión finita $\mathbb{F}_{q^e}$ de $\mathbb{F}_q$ podemos definir:

$$\mathcal{C} = \{c(X) \in A/c(\alpha_1) = \ldots = c(\alpha_r) = 0\},$$

que será cíclico pues, si $f_i(X)$ es el polinomio mínimo de α_i para todo $i \in \{1, ..., r\}$, se verifica que $\mathcal{C} = (g(X)) = (m.c.m(f_1, ..., f_r))$. Además, se comprueba que $g(x)$ divide a $X^n - 1$.

De este modo se simplifica el proceso que nos permite comprobar si un elemento está o no en el código pues solo hará falta evaluar el polinomio en las raíces convenientes para determinar su pertenencia al código. Si tomamos la matriz

$$H' = \begin{pmatrix} 1 & \alpha_1 & ... & \alpha_1^{n-1} \\ 1 & \alpha_2 & ... & \alpha_2^{n-1} \\ . & . & & . \\ . & . & & . \\ . & . & & . \\ 1 & \alpha_r & ... & \alpha_r^{n-1} \end{pmatrix}$$

y denotamos $H'f(X) = (f(\alpha_1), ..., f(\alpha_r))$, se puede observar cómo la matriz H' desempeña el papel de matriz de control, pero sin embargo no tiene coeficientes en $\mathbb{F}_q$, en general, ni dimensión $(n-k) \times n$.

Ejemplo 2.6. Tomando el código del Ejemplo 2.3 tenemos que el único cero de $g(X) = X + 1$ es $X = 1$ y la longitud del código es $n = 3$. Por tanto la matriz de control obtenida por sus ceros queda

$$H' = (1\,1\,1).$$

Todos los elementos de $\mathcal{C} = (g(X))$ tienen como cero, al menos a $X = 1$.

Ejemplo 2.7. Tomamos el cuerpo $\mathbb{F}_2$ y la extensión $\mathbb{F}_{2^4}$ del mismo. Sean α y α^3 raíces quinceavas de la unidad cuyos polinomios mínimos sobre $\mathbb{F}_2$ son:

$$g_1(X) = X^4 + X^3 + 1 \text{ y } g_2(X) = X^4 + X^3 + X^2 + X + 1$$

respectivamente. Se comprueba que

$$g(X) = m.c.m.(g_1, g_2) = X^8 + X^4 + X^3 + X + 1.$$

Por tanto, podemos determinar el código cíclico $\mathcal{C} = (g(X))$ de longitud $n = 15$ y matriz de control

$$H' = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \dots & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \dots & \alpha^9 & \alpha^{12} \end{pmatrix}.$$

2.1.3. Descodificación de los códigos cíclicos

Una vez definidas sus correspondientes matrices generatriz y de control, es hora de pasar a la descodificación de los códigos cíclicos. Al tratarse de un código lineal, el método síndrome-líder es totalmente aplicable para los códigos cíclicos. Sin embargo estos códigos permiten una reducción notable en el momento de su descodificación, pues al tratarse de códigos que presentan ciertas propiedades con respecto a la permutación de sus elementos, bastará con centrarnos en corregir el error de una posición fija, en general la posición $n-1$. Para ello crearemos una tabla síndrome-líder reducida, donde pondremos aquellos síndromes cuyo líder tenga componente $n-1$ no nula. A partir de ahí se procede de una forma totalmente análoga a la del método clásico. Se calcula el síndrome de nuestro vector y se busca en la tabla reducida. Si está, se corrige el error como en el método original, en caso contrario la componente $n-1$ del vector y es correcta. Una vez realizado este paso se tomará el vector $y^{(1)} = (y_{n-1}, y_0, ..., y_{n-2})$ y se aplica el proceso anterior. Se repetirá dicho proceso hasta llegar al vector $y^{(n-1)}$.

Ejemplo 2.8. Sea $\mathcal{C}$ un código sobre $\mathbb{F}_2$, de longitud 3 y polinomio generador $g(X) = X^2 + X + 1$. Se obtiene que sus matrices generatriz y de control son

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

respectivamente. Además obtenemos

$$\mathbb{F}_2^3/\mathcal{C} = \{[(0,0,0)],\ [(0,0,1)],\ [(0,1,0)],\ [(1,0,0)]\}.$$

Construimos la tabla síndrome-líder y su reducida, para poder apreciar la diferencia.

Tabla síndrome-líder	
Síndrome	Líder
(0,0)	(0,0,0)
(0,1)	(0,1,0)
(1,0)	(1,0,0)
(1,1)	(0,0,1)

Tabla síndrome-líder reducida	
Síndrome	Líder
(1,1)	(0,0,1)

Cuadro 2.1: Tabla Síndrome-líder

Entonces, recibido el mensaje $y = (0,1,0)$ realizamos el proceso descrito. En primer lugar calculamos su síndrome $s = (0,1)$, notamos que no aparece en la tabla reducida, por lo tanto podemos concluir que la última coordenada es correcta. Calculamos ahora el síndrome de la permutación $y^{(1)} = (0,0,1)$ la cual es $s^{(1)} = (1,1)$. Aparece en la tabla reducida, acompañada del líder $(0,0,1)$, por tanto corregimos la segunda componente de y de la forma usual. Por último observamos que el síndrome de $y^{(2)} = (1,0,0)$ no aparece en la tabla, luego el mensaje queda descodificado por $c = (0,0,0)$.

2.1.4. Captura del error. Errores a ráfaga

Otra técnica utilizada a la hora de descodificar es la de *captura del error*. Para este método, y notando la facilidad que nos ofrece el manejo de mensajes como polinomios, vamos a introducir el siguiente concepto.

Definición 2.3. Sea $\mathcal{C}$ un código cíclico generado por el polinomio $g(X)$. Recibido el vector y, llamaremos polinomio síndrome de y, y lo representamos por $s[y](X)$, al resto de la división de $y(X)$ entre $g(X)$.

Haciendo uso de este concepto, podemos presentar un método de descodificación más rápido, ligado a la siguiente proposición.

Proposición 2.6. *Sea $\mathcal{C}$ un código cíclico que corrige a lo sumo t errores. Si recibido el mensaje $y = c + e$ han ocurrido a lo sumo t errores y si el polinomio síndrome $s[y](X)$ tiene, como mucho, peso t, entonces $e(X) = s[y](X)$.*

Demostración. Observamos que $\mathcal{C}$ corrige, como máximo, t errores, por tanto $d > 2t$. Supongamos recibido el mensaje $y(X) = c(X) + e(X)$, por definición tenemos que

$$s[y](X) = y(X) - g(X)q(X) = c(x) + e(X) + g(X)q(X),$$

entonces se tiene naturalmente que $s[y](X) - e(X) = c(X) + g(X)q(X) \in \mathcal{C}$. Por hipótesis el peso de $s[y](X)$ y el número de errores cometidos es menor o igual que t, por tanto el peso de $s[y](X) - e(X)$ será a lo sumo $2t < d$, luego $s[y](X) = e(X)$.

□

Ejemplo 2.9. Sea el cuerpo $\mathbb{F}_4$, consideramos el anillo de polinomios $\mathbb{F}_4[X]$ y el código cíclico de longiud 5 y dimensión 1 generado por el polinomio $g(X) = X^4+X^3+X^2+X+1$. Notemos que $g(X)$ divide a $X^5 - 1$. La distancia mínima del código es 5, por tanto su capacidad correctora será $t = 2$.

Supongamos recibido el mensaje $y(X) = \alpha X^2 + \alpha X^3 + \alpha X^4$, su síndrome será

$$s[y](X) = \alpha + X\alpha.$$

Por tanto, atendiendo a la Proposición 2.6 se tiene que, como $w(s[y](X)) = 2$, podemos tomar el síndrome como error y descodificar de la siguiente forma:

$$c(X) = y(X) - s[y](X) = \alpha X^4 + \alpha X^3 + \alpha X^2 + \alpha X + \alpha.$$

Observaciones 2.2. Este método requiere que el síndrome tenga un peso menor o igual a t, lo que no tiene por qué suceder siempre. Es por ello que en algunos casos se prueba con $s[y^{(j)}](X)$, pues si tiene peso menor a t se verifica que:

$$e(X) = s[y^{(j)}]^{(n-j)}(X).$$

Un caso particular de la producción de errores es el que se genera de forma consecutiva, en el proceso de transmisión de un mensaje, como ocurrió en el Ejemplo 2.9. Para introducir esta nueva idea hará falta la siguiente definición.

Definición 2.4. Una ráfaga es un vector $x \in \mathbb{F}_q^n$ tal que todas sus coordenadas no nulas son consecutivas. Se llama longitud de la ráfaga a $w(x)$.

Observamos entonces que el tipo de error descrito anteriormente corresponderá a un vector ráfaga. Por su estructura, los códigos cíclicos son especialmente eficaces a la hora de detectar y corregir estos tipos de errores. Así lo demuestra la siguiente proposición.

Proposición 2.7. *Un código cíclico $\mathcal{C}$ de parámetros $[n, k]$ no contiene ninguna ráfaga de longitud $l \leq n - k$ y por lo tanto detecta cualquier error ráfaga de longitud $l \leq n - k$.*

Demostración. Sea $X^i l(X)$ una ráfaga de longitud l, por tanto $deg(l(X)) < l$. Sabemos que $l(X) \notin \mathcal{C}$ pues $deg(l(X)) < deg(g(X))$. Consecuentemente $X^i l(X) \notin \mathcal{C}$, luego en $\mathcal{C}$ no hay ninguna ráfaga de longitud $l \leq n-k$. Supongamos ahora recibida la palabra $y = c+e$, con e una ráfaga de longitud l. Se tiene que $c + e \notin \mathcal{C}$, pues en caso contrario $e \in \mathcal{C}$. □

Anteriormente vimos que podíamos descodificar un código mediante el método de la captura de error utilizando el síndrome del mensaje recibido y. Si el error producido es un error ráfaga se prueba que siempre se podrá encontrar una permutación cíclica de nuestro mensaje que verifique que $e(X) = s[y](X)$, esto es, podremos utilizar siempre el método de captura de error.

Proposición 2.8. *Sea $\mathcal{C}$ un código cíclico de parámetros $[n, k]$. Si los errores de un vector recibido y constituye una ráfaga de longitud a lo sumo $n - k$, entonces existe j tal que $e^{(j)}(X) = s[y^{(j)}](X)$.*

Demostración. Por hipótesis existe un $y^{(j)}$ en el que se han producido errores en las coordenadas $0, 1, \ldots, n-k-1$, por tanto $deg(e^{(j)}) < n-k$. Además,

$$y^{(j)}(X) = c(X) + e^{(j)}(X) = g(X)h(X) + s[y^{(j)}](X),$$

luego $e^{(j)}(X) = g(X)h'(X) + s[y^{(j)}](X)$ y en consecuencia

$$s[y^{(j)}](X) = s[e^{(j)}](X) = e^{(j)}(X).$$

□

Ejemplo 2.10. Tomemos el código desarrollado en el Ejemplo 2.9. Atendiendo a la Proposición 2.7 sabemos que el código no contiene ninguna ráfaga de longitud $n-k = 5-1 = 4$. Supongamos recibido el mensaje $y(X) = (\alpha+1)X^4+(\alpha+1)X^3+X^2+X+1$, notamos que posee una ráfaga de longitud 2. Tomemos $y^{(4)}(X) = X^4 + X^3 + X^2 + (\alpha+1)X + (\alpha+1)$ y calculamos su síndrome

$$y^{(4)}(X) = g(X)h(X) + s[y^{(4)}](X) = (X^4 + X^3 + X^2 + X + 1) + ((\alpha)X + (\alpha)).$$

Por tanto, podemos asumir como error $s[y^{(4)}](X)$ y descodificar obteniendo

$$c(X) = y(X) - s[y](X) = (\alpha+1)X^4 + (\alpha+1)X^3 + (\alpha+1)X^2 + (\alpha+1)X + (\alpha+1).$$

2.2. Códigos BCH

Como caso particular de los códigos cíclicos se originan los códigos BCH. En la Subsección 2.1.2 estudiamos que los códigos cíclicos son fácilmente descritos mediante una serie de ceros, utilizando así la matriz

$$H' = \begin{pmatrix} 1 & \alpha_1 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \ldots & \alpha_2^{n-1} \\ . & . & & . \\ . & . & & . \\ . & . & & . \\ 1 & \alpha_r & \ldots & \alpha_r^{n-1} \end{pmatrix}$$

como matriz de control. Usando esta matriz vimos que la distancia mínima del código cíclico $\mathcal{C}$ verificaba que $d(\mathcal{C}) \geq d$ si cualesquiera $d-1$ columnas de H' son linealmente independientes. Sin embargo no es fácil conocer esta cota para una serie de raíces arbitrarias. Es la necesidad de diseñar un código con una cota prefijada de la distancia mínima la que genera los códigos BCH (Bose, Chaudhuri y Hocquenghem). Estos códigos se basan en la toma de raíces primitivas n-ésimas de la unidad como raíces que determinarán al código. De esta forma cualquier menor de la matriz H' es del tipo Vandermonde, luego $d(\mathcal{C}) \geq r+1$.

En lo que sigue fijaremos como alfabeto el conjunto $\mathbb{F}_q$ y denotaremos por n a la longitud del código. Además denotaremos por m al orden multiplicativo de q módulo n y $\alpha \in \mathbb{F}_{q^m}$ una raíz primitiva n-ésima de la unidad. Teniendo en cuenta esta notación obtenemos la siguiente definición.

Definición 2.5. Llamaremos código BCH de longitud n y distancia mínima prevista δ, al código cíclico de longitud n cuyo polinomio generador tiene por raíces $\alpha^b, ..., \alpha^{b+\delta-2}$, con $b \geq 0$ y $\delta \geq 1$.

Ejemplo 2.11. El código construido en el Ejemplo 2.7 no es un código BCH pues, aunque α y α^3 sean raíces del polinomio generador, α^2 no lo es.

En la familia de códigos BCH distinguimos diferentes tipos:

1. Si $b = 1$ el código se denomina en sentido estricto.
2. Si $n = q^m - 1$ lo llamaremos código BCH primitivo.
3. Si además $m = 1$, esto es, $n = q - 1$, el código se denomina Reed-Solomon.

Como se citó anteriomente, los códigos BCH se caracterizan por tener una distancia mínima prevista δ, que será una cota de la distancia mínima real.

Proposición 2.9. *Si $\mathcal{C}$ es un código BCH de distancia mínima prevista δ, posee distancia mínima $d \geq \delta$.*

Demostración. Tomando la matriz de control

$$H' = \begin{pmatrix} 1 & \alpha_1 & ... & \alpha_1^{n-1} \\ 1 & \alpha_2 & ... & \alpha_2^{n-1} \\ . & . & & . \\ . & . & & . \\ . & . & & . \\ 1 & \alpha_r & ... & \alpha_r^{n-1} \end{pmatrix}$$

cualquier menor $(\delta-1)\times(\delta-1)$ es una matriz del tipo Vandermonde, luego cualesquiera $\delta-1$ de sus columnas son linealmente independientes y por tanto atendiendo a la Proposición 1.4 se prueba el resultado. □

Al tratarse de códigos cíclicos podremos trabajar con ellos a partir del polinomio generador. Para calcular dicho polinomio, como hemos visto en la Sección 2.2, debemos obtener para cada raíz su polinomio mínimo sobre $\mathbb{F}_q$, esto es, para todo $i \in \{b, ..., b + \delta - 2\}$, debemos calcular $g_i = Irr(\alpha, \mathbb{F}_q)$. Entonces tenemos que

$$g(X) = m.c.m.\{g_b(X), ..., g_{b+\delta-2}(X)\}$$

es el polinomio generador del código.

Ejemplo 2.12. Sea $\mathbb{F}_{2^3}$ una extensión del cuerpo $\mathbb{F}_2$. Tenemos que $m = 3$ por lo tanto, $2^3 \equiv 1$ (mód n) con $n = 7$. Tomemos $\alpha \in \mathbb{F}_{2^3}$ una raíz primitiva séptima de la unidad. Sean $n = 7$, $b = 2$ y $\delta = 3$, se tiene que

$$f_1 = Irr(\alpha^2, \mathbb{F}_2) = X^3 + X + 1,\ f_2 = Irr(\alpha^3, \mathbb{F}_2) = X^3 + X^2 + 1.$$

Denotamos por $g(X) = m.c.m\{f_1,\, f_2\} = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$. Entonces el código $\mathcal{C} = (g(X))$ es un código BCH con parámetros $n = 7$, $b = 2$ y $\delta = 3$. Su matriz de control y generatriz son las siguiente:

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \text{ y } H = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Y su matriz de control tomada a partir de los ceros es

$$H' = \begin{pmatrix} 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \end{pmatrix}.$$

2.3. Códigos Reed-Solomon

En esta sección trataremos los *códigos de Reed-Solomon*, uno de los casos particulares de los códigos BCH citados en la Sección 2.2. Para empezar veamos cuál es, formalmente, su definición.

Definición 2.6. Un código Reed-Solomon sobre $\mathbb{F}_q$ es un código BCH primitivo de longitud $n = q - 1$.

Debido a su naturaleza, los procesos de codificación y descodificación de los códigos de Reed-Solomon son análogos a los estudiados en los códigos BCH. Sin embargo, la raíz α, que determina a los códigos Reed-Solomon pertenecen al cuerpo $\mathbb{F}_q$, por ello se trabajará siempre dentro de dicho cuerpo.

Ejemplo 2.13. Sea el cuerpo $\mathbb{F}_{2^4}$, y sea $n = 15$. Tomemos $g(X) = X^4 + X + 1$ que divide a $X^{15} - 1$.

Además, si α es raíz de $g(X)$, lo es de $X^{15} - 1$ y consecuentemente $\alpha \in \mathbb{F}_{2^3}$. Por tanto el código cíclico generado por g(X) es un código Reed-Solomon de longitud 15 y dimensión 11.

A continuación se presenta una propiedad de los códigos Reed-Solomon.

Proposición 2.10. *Los códigos Reed-Solomon son códigos de máxima distancia de separación (MDS).*

Demostración. Tomemos $\mathcal{C}$ un código Reed-Solomon. Al tratarse de un caso particular de los códigos BCH, se cumple, como en estos, que fijada una distancia mínima prevista δ y α una raíz n-ésima de la unidad y siendo $g(X)$ el polinomio generador del código, la distancia

mínima del código y su dimensión verifican $d \geq \delta$ y $k = n - deg(g(X))$, respectivamente. Se tiene que

$$g(X) = m.c.m.\{Irr(\alpha^i, \mathbb{F}_q)/i = 1, \ldots, \delta - 1\}.$$

Además para todo $i \in \{1, \ldots, n\}$ se cumple que $\alpha^i \in \mathbb{F}_q$. Consecuentemente es natural que $deg(g(X)) = \delta - 1$. Teniendo en cuenta esto, tenemos que $\delta = n - k + 1$ y por tanto, haciendo uso de la cota de Singleton

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

Por tanto $d = n - k + 1$ y $\mathcal{C}$ es de máxima distancia de separación. □

2.3.1. Descenso de cuerpo

Uno de los mayores inconvenientes de los códigos de Reed-Solomon es que presentan una restricción en su longitud, la cual quedará limitada a $q - 1$ sobre el cuerpo $\mathbb{F}_q$. Por fortuna, la *estrategia de descenso de cuerpo* sirve para solventar este inconveniente.

Para poder llevar a cabo la *estrategia de descenso de cuerpo*, tomaremos una extensión del cuerpo finito $\mathbb{F}_q$ de la forma $\mathbb{F}_{q^r}$, con $r \in \mathbb{N}$. El objetivo primordial del proceso es tomar un código $\mathcal{C}$ de longitud n sobre el cuerpo $\mathbb{F}_{q^r}$ y transformarlo en un código de longitud nr sobre el cuerpo $\mathbb{F}_q$. Aprovechando que $\mathbb{F}_{q^r}$ es isomorfo a $\mathbb{F}_q^r$, para todo

$$c = (c_0, ..., c_{n-1}) \in \mathcal{C} \subset \mathbb{F}_{q^r}^n$$

podremos identificar cada componente c_i con un vector de $\mathbb{F}_q^r$ e $i \in \{0, ..., n-1\}$. Por tanto cada palabra del código podrá ser escrita como

$$c = (c_{01}, \ldots, c_{0r}, \ldots, c_{j1}, \ldots, c_{jr}, \ldots, c_{(n-1)1}, \ldots, c_{(n-1)r}) \in \mathcal{C} \subset \mathbb{F}_q^{nr}.$$

Nótese que de esta forma conseguimos un código sobre el cuerpo $\mathbb{F}_q$ de longitud nr. Gracias a esta construcción surge el siguiente resultado.

Proposición 2.11. *Sea $\mathcal{C}$ un código de Reed-Solomon sobre $\mathbb{F}_{2^r}$ con distancia $d = 2t+1$. Entonces, el código binario obtenido por descenso de cuerpo sobre $\mathbb{F}_2$ corrige todos los errores a ráfaga de longitud $l \leq (t-1)r + 1$.*

Demostración. En primer lugar, observamos que como la distancia mínima de $\mathcal{C}$ es $d = 2t+1$, la capacidad correctora será t. Tomemos un vector de $\mathcal{C} \subset \mathbb{F}_{2^r}$ y mediante un proceso inverso al del descenso de cuerpo lo transformaremos en un vector de $\mathbb{F}_2$. Suponemos que el vector error forma una ráfaga de longitud, a lo sumo, $(t-1)r + 1$. Es por ello que la palabra transformada, al colapsar r símbolos binarios en uno, contendrá, como máximo, t componenetes erróneas. Como t es la capacidad correctora del código, el resultado queda probado. □

2.4. Códigos de evaluación sobre variedades afines

Una vez estudiadas algunas familias de códigos lineales generales podemos abordar el estudio de los *códigos de evaluación sobre variedades afines*. Para determinar dichos códigos necesitaremos un espacio vectorial de funciones, un conjunto de puntos, que vendrán dados por la *variedad* de un ideal, y una aplicación, que denotaremos por ev.

Empezaremos por conocer el concepto de *variedad*, que pasamos a definir formalmente.

Definición 2.7. Sea K un cuerpo y sean $f_1, ..., f_s$ polinomios de $K[X_1, ..., X_n]$. El conjunto

$$V(f_1, ..., f_s) = \{(a_1, ..., a_n) \in K^n : f_i(a_1, ..., a_n) = 0, \textit{para todo}\, 1 \leq i \leq s\}$$

es la variedad afín del conjunto de polinomios $\{f_1, ..., f_s\}$.

Obsérvese que

$$V(f_1, \ldots, f_s) = V(f_1) \cap \ldots \cap V(f_s).$$

Para trabajar con los *códigos de evaluación sobre variedades afines*, consideraremos el cuerpo finito $\mathbb{F}_q$, donde $q = p^n$, y n, $p \in \mathbb{N}$, siendo p primo; $\mathbb{F}_q[X_1, ..., X_s]$ el anillo de polinomios en las variables $\{X_1, \ldots, X_s\}$, con coeficientes en $\mathbb{F}_q$, y un ideal $I \subset \mathbb{F}_q[X_1, ..., X_s]$. Denotemos:

$$I_q = I + (X_1^q - X_1, ..., X_s^q - X_s).$$

Nos proponemos analizar la variedad de I_q, sobre la clausura algebraica de $\mathbb{F}_q$. Atendiendo a lo anterior concluimos que

$$V(I_q) = V(I + (X_1^q - X_1, ..., X_s^q - X_s)) = V(I) \cap V((X_1^q - X_1, ..., X_s^q - X_s)).$$

Además notamos que $V((X_1^q - X_1, ..., X_s^q - X_s)) = \mathbb{F}_q^s$. Por lo tanto, tenemos que $V(I_q) = V(I) \cap \mathbb{F}_q^s = \{\mathbf{P}_1, ..., \mathbf{P}_n\}$, esto es, la variedad del ideal I_q es finita. Con esto, ya hemos determinado el conjunto de puntos necesarios para definir los *códigos de evaluación sobre variedades afines*.

Nuestro próximo objetivo es encontrar el espacio vectorial de funciones que utilizaremos para la definición de dichos códigos. En primer lugar comprobamos que el ideal I_q es un ideal radical. Para ello haremos uso de los siguientes resultados.

Lema 2.12. *Sean K cuerpo, $K[X_1, \ldots, X_n]$ e $I \subset K[X_1, \ldots, X_n]$ un ideal. Sea $g_1 \in (I \bigcap K[X_1]) \backslash \{0\}$ y $g_1 = h_1 \ldots h_t$ su descomposición en irreducibles, entonces se tiene que*

$$I = \bigcap_{i=1}^{t} (I + h_i).$$

Demostración.
Para todo $f \in \bigcap_{i=1}^{t}(I+(h_i))$, existe $r_i \in I$ y $q_i \in K[X_1,\ldots,X_n]$ tal que $f = r_i + q_i h_i$ con $i = 1,\ldots,t$. Observamos que

$$f\prod_{j\neq i} h_j = r_i \prod_{j\neq i} h_j + q_i g_1 \text{ con } i = 1,\ldots,t.$$

Además como $m.c.d.(\prod_{j\neq 1} h_j,\ldots,\prod_{j\neq t} h_j) = 1$ podemos encontrar, $l_1,\ldots,l_t \in K[X_1]$ tal que

$$l_1\prod_{j\neq 1} h_j + \ldots + l_t\prod_{j\neq t} h_t = 1.$$

Por tanto:

$$f = \sum_{i}^{t} l_i f \prod_{j\neq i} h_j \in I.$$

Luego $I \supseteq \bigcap_{i=1}^{t}(I+(h_i))$.
Trivialmente se se cumple la otra inclusión. □

La prueba del siguiente resultado está basada en la demostración que se puede leer en [4], página 150. Para consultar una prueba alternativa véase [7], página 310.

Lema 2.13. *(Lema de Seidenberg) Sea K un cuerpo, $K[X_1,\ldots,X_n]$ y sea $I \subset K[X_1,\ldots,X_n]$ un ideal cuya variedad es finta. Si para todo $i \in \{1,\ldots,n\}$, existe un polinomio $g_i \in (I \cap K[X_i])\backslash\{0\}$ tal que $m.c.d.(g_i, g_i') = 1$, entonces I es un ideal radical.*

Demostración. En primer lugar, observamos que g_i es un polinomio libre de cuadrados para todo $i \in \{1,\ldots,n\}$. Para realizar la demostración vamos a proceder por inducción sobre n.

Sea $n = 1$. El anillo de polinomios $K[X_1]$ es un dominio de ideales principales. Sea un ideal $I \subset K[X_1]$ tal que existe un $g_1(X_1) \in I$ libre de cuadrados. El generador de I será libre de cuadrados y en consecuencia el ideal radical.

Supongamos cierto el resultado para $n-1$, esto es, si para todo $i \in \{1,\ldots,n-1\}$, existe un polinomio $g_i \in (I \cap K[X_i])\backslash\{0\}$ tal que $m.c.d.(g_i, g_i') = 1$, entonces I es un ideal radical.

Probemos el resultado para n. En primer lugar supongamos g_1 irreducible. Tomamos el epimorfimo canónico entre anillos:

$$\begin{array}{rcl} \varphi:\ K[X_1,\ldots X_n] & \longrightarrow & K[X_1]/(g_1)\,[X_2,\ldots,X_n] \\ f & \longmapsto & \varphi(f) = f + (g_1) \end{array}$$

cuyo núcleo es $Ker\,\varphi = (g_1) \subset I$. Denotamos por $J = \varphi(I)$ y definimos la siguiente correspondencia entre anillos:

$$\begin{array}{rcl} \sigma:\ K[X_1,\ldots,X_n]/I & \longrightarrow & ((K[X_1]/(g))\,[X_2,\ldots,X_n])/\varphi(I) \\ h+I & \longmapsto & \sigma(h+I) = \varphi(h) + \varphi(I) \end{array}$$

Comprobemos que se trata de un isomorfimo. En primer lugar veamos que es una aplicación. Sea

$$h_1 + I = h_2 + I \Rightarrow h_1 - h_2 \in I \Rightarrow \varphi(h_1 - h_2) = 0 \Rightarrow$$

$$\Rightarrow \varphi(h_1) = \varphi(h_2) \Rightarrow \sigma(h_1 + I) = \sigma(h_2 + I).$$

Veamos ahora que es inyectiva, para ello tomamos

$$h_1 + I \in K[X_1, \ldots, X_n]/I \text{ tal que } \varphi(h_1) \in \varphi(I) \Rightarrow \varphi(h_1) = \varphi(h_2),\ h_2 \in I \Rightarrow$$

$$\Rightarrow \varphi(h_1 - h_2) = 0 \Rightarrow h_1 - h_2 \in Ker\,\varphi \subseteq I \Rightarrow h_1 - h_2 \in I \Rightarrow h_1 \in I.$$

Por último, se tiene de forma natural que σ es una aplicación sobreyectiva y lineal pues φ lo es. Luego se sigue que

$$((K[X_1]/(g_1))\,[X_2, \ldots, X_n])/\varphi(I) \cong K[X_1, \ldots, X_n]/I$$

y por lo tanto la variedad asociada a $J = \varphi(I)$ es finita. Por hipótesis se tiene que para todo $i = 2, \ldots, n$ el $m.c.d(g_i, g_i') = 1$ y satisfacen que $\varphi(g_i) = g_i \in ((K[X_1]/(g_1))\,[X_2, \ldots, X_n])$ por lo tanto J es un ideal radical por hipótesis de inducción.

En consecuencia $((K[X_1]/(g_1))\,[X_2, \ldots, X_n])/\varphi(I)$ no tiene elementos nilpotentes no nulos y debido al isomorfimo $K[X_1, \ldots, X_n]/I$ tampoco, luego I es radical.

Supongamos que g no es irreducible y sea $g = f_1 \ldots f_t$ su factorización en irreducibles. Por el Lema 2.12 tenemos que $I = \bigcap_{i=1}^{t}(I + (h_i))$, y como la intersección de ideales radicales es radical solo quedaría proceder, con cada h_i como en el caso anterior. □

Aplicando el Lema 2.13 podemos afirmar que I_q es un ideal radical, luego, por el Teorema de los ceros de Hilbert (ver [2], pag. 175, The Strong Nullstellensatz),

$$I(V(I_q)) = I_q \quad .$$

y por ello

$$R = \mathbb{F}_q[X_1, ..., X_s]/I(V(I_q)) = \mathbb{F}_q[X_1, ..., X_s]/I_q.$$

Además, como hemos considerado anteriormente $V(I_q) = \{\mathbf{P}_1, ..., \mathbf{P}_n\}$, luego $dim\,R = \#V(I_q) = n$.

Por último presentamos una proposición que servirá para determinar la aplicación asociada a los códigos de evaluación sobre variedades afines.

Proposición 2.14. *La correspondencia*

$$\begin{array}{rcl} ev: R & \longrightarrow & \mathbb{F}_q^n \\ f + I_q & \longmapsto & ev(f + I_q) = (f(\boldsymbol{P}_1), \ldots, f(\boldsymbol{P}_n)) \end{array}$$

es un isomorfimo de $\mathbb{F}_q$-espacios vectoriales.

Demostración. En primer lugar veamos que se trata de una aplicación. Sean $f+I_q, g+I_q \in R = \mathbb{F}_q[X_1, ..., X_s]/I_q$, entonces si

$f + I_q = g + I_q \Rightarrow f - g \in I_q$, y por lo tanto, $(f(P_1), ..., f(P_n)) - (g(P_1), ..., g(P_n)) = 0$.

A continuación comprobemos que se trata de un homomorfismo:

1. Sea $f + I_q, g + I_q \in \mathbb{F}_q[X_1, ..., X_s]/I_q$, entonces :

$$ev((f + I_q) + (g + I_q)) = ev((f + g) + I_q) = ((f + g)(P_1), ..., (f + g)(P_n)) = (f(P_1) + g(P_1), ..., f(P_n) + f(P_n)) = (f(P_1), ..., f(P_n)) + (g(P_1), ..., g(P_n)).$$

2. Sea $\lambda \in \mathbb{F}_q$, entonces:

$$ev(\lambda(f + I_q)) = ev(\lambda f + I_q) = (\lambda f(P_1), ..., \lambda f(P_n)) = \lambda(f(P_1), ..., f(P_n)).$$

Veamos por último que ev es una biyección. En primer lugar comprobamos que la aplicación ev es inyectiva. Para ello supongamos que:

$$f + I_q \in Ker(ev) \Rightarrow ev(f + I_q) = (f(P_1), ..., f(P_n)) = 0 \Rightarrow f \in I_q.$$

Y teniendo en cuenta que

$$dim(\mathbb{F}_q[X_1, ..., X_s]/I_q) = dim(\mathbb{F}_q^n)$$

podemos concluir que la aplicación ev es un isomorfimo. □

Estamos en disposición de definir los *códigos de evaluación sobre variedades afines.*

Definición 2.8. Sea L un $\mathbb{F}_q$-subespacio vectorial de $\mathbb{F}_q[X_1, ..., X_s]/I_q$. Definimos el código evaluación $C(I_q, L)$ sobre la variedad afín $V(I_q)$ como la imagen de L por la aplicación ev. Denotaremos por $C^{\perp}(I_q, L)$ a su código dual.

Observaciones 2.3.

1. Notamos que una permutación en los puntos de $V(I_q)$ proporciona un código equivalente.

2. Si $\{f_1+I_q, ..., f_k+I_q\}$ es una base de L, la matriz $[f_i(P_j)]$ con $i = 1, ..., k$ y $j = 1, ..., n$ es la matriz generatriz del código evaluación $C(I_q, L)$ y la matriz control de su dual.

Proposición 2.15. *Los códigos Reed-Solomon son códigos de evaluación sobre variedades afines.*

Demostración. Tomemos α una raíz primitiva n-ésima de la unidad, y sea $g(X)$ raíz de $\mathcal{P} = \{1, \alpha, \ldots, \alpha^{q-1}\}$. Si escogemos el espacio vectorial de funciones $V = \{f(X) \in \mathbb{F}_q | deg(f) \leq \delta - 2\}$, tenemos que una base de dicho subespacio vectorial sobre $\mathbb{F}_q$ es $\{1, X, ..., X^{n-1}\}$. Por tanto, determinando $V(I_q) = \{1, \alpha, \ldots, \alpha^{q-1}\}$, tenemos que una base del subespacio vectorial determinado a partir de la evaluación de V por la aplicación ev es

$$\{(1, \ldots, 1), (1, \alpha, \ldots, \alpha^{q-1}), \ldots, (1, \alpha^{\delta-2}, \ldots, \alpha^{(q-1)(\delta-2)}\}.$$

Esto es, la matriz generatriz del código definido a partir de la evaluación es

$$H = \begin{pmatrix} 1 & 1 & . & . & . & 1 \\ 1 & \alpha & . & . & . & \alpha^{q-1} \\ . & . & & & & . \\ . & . & & & & . \\ . & . & & & & . \\ 1 & \alpha^{\delta-2} & . & . & . & \alpha^{(q-1)(\delta-2)} \end{pmatrix}.$$

El código dual $\mathcal{C}^{\perp}$ tendrá como matriz de control a H, luego podemos afirmar que se trata de un código Reed-Solomon de distancia δ y longitud $n = q - 1$, donde el polinomio generador de dicho código será

$$g(X) = \prod_{i=0}^{\delta-2} (X - \alpha^i).$$

□

Ejemplo 2.14. Tomamos el cuerpo $\mathbb{F}_4$, el anillo de polinomios $\mathbb{F}_4[X, Y, Z]$ y el ideal $I = (X^2 + Y^2 + Z, X + Y)$. Calculamos la variedad del ideal I_q y obtenemos

$$V(I_q) = \{(0, 0, 0), (1, 1, 0), (\alpha, \alpha, 0), (\alpha + 1, \alpha + 1, 0)\}.$$

Tomamos ahora el subespacio vectorial $L =< \{x + I_q, y + 1 + I_q\} > .\mathbb{F}_4$. Mediante la aplicación ev generamos el subespacio vectorial de base $\mathcal{B} = \{(0, 1, \alpha, \alpha+1), (1, 0, \alpha+1, \alpha)\}$ que puede ser interpretado como un código lineal, de longitud 4 y dimensión 2, cuya matriz generatriz es

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

Se comprueba que la matriz de control es

$$H = \begin{pmatrix} 1 & 0 & \alpha + 1 & \alpha \\ 0 & 1 & \alpha & \alpha + 1 \end{pmatrix}$$

y la distancia mínima del código es 3.

Capítulo 3

Descodificación usando bases de Gröbner

Una vez estudiadas algunas familias de códigos correctores de errores y sus propiedades, nos proponemos analizar la descodificación de algunos de estos códigos mediante las *bases de Gröbner*. Trataremos, de una forma breve, la descodificación de dos familias de códigos, los códigos cíclicos y los códigos de evaluación sobre variedades afines. Para realizar un estudio más detallado de ambos procesos véase [1] y [3] respectivamente.

Antes de comenzar, es preciso definir formalmente algunos conceptos que nos ayudarán a entender mejor la descodificación de códigos mediante bases de Gröbner.

Definición 3.1. Sea $\mathbb{T}^n = \{X^\alpha = X_1^{\alpha_1} \dots X_n^{\alpha_n} | \alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n\}$. Se define un orden monomial sobre $\mathbb{T}^n$ como un orden total $\prec$ que satisface:

1. $1 \prec X^\alpha$ para todo $X^\alpha \in \mathbb{T}^n$ distinto de 1.

2. Si $X^\alpha \prec X^\beta$ entonces $X^\gamma X^\alpha \prec X^\gamma X^\beta$ para todo $X^\gamma \in \mathbb{T}^n$.

Si $f \in K[X_1, \dots, X_n]$ denotamos por $lt_\succ(f)$ a $c_\beta X^\beta$ siendo X^β el mayor monomio de f con respecto al orden monomial $\succ$ y c_β su coeficiente.

Definición 3.2. Dado un orden monomial $\succ$ y un ideal $I \subset K[X_1, \dots, X_n]$ diremos que el conjunto $\{f_1, \dots, f_s\} \subset K[X_1, \dots, X_n]$ es una base de Gröbner de I para $\succ$ si se cumple:

$$(lt_\succ(f_1), \dots, lt_\succ(f_s)) = (lt_\succ(I)),$$

donde $lt_\succ(I) = \{lt_\succ(f) | f \in I\}$.

La existencia de bases de Gröbner para cualquier ideal está garantizado por el siguiente teorema, cuya demostración puede verse en [5, Chapter 5].

Teorema 3.1. *Dado un orden monomial $\succ$ y un ideal $I \subset R$ existe una base de Gröbner de I y es un sistema generador del ideal I.*

3.1. Descodificación de códigos cíclicos

En la descodificación de códigos cíclicos mediante el uso de bases de Gröbner, se determinará la matriz de control de los códigos atendiendo a las raíces del polinomio generador. Sea $\mathcal{C}$ un código cíclico $[n, k, d]$ sobre el cuerpo $\mathbb{F}_q$, generado por el polinomio $g(X)$ de grado $r = n - k$. Tomemos $\mathbb{F}_{q^l}$ una extensión de $\mathbb{F}_q$ que contiene a las raíces de $g(X)$ y sea α una raíz n-ésima primitiva de la unidad sobre $\mathbb{F}_{q^l}$ tal que tal que para todo $i \in J(\mathcal{C}) = \{j_1, ..., j_r\}$, α^i es raíz de $g(X)$. Por tanto, la matriz de control del código generado por $g(X)$ es

$$H = \begin{pmatrix} 1 & \alpha^{j_1} & \alpha^{2j_1} & ... & \alpha^{(n-1)j_1} \\ 1 & \alpha^{j_2} & \alpha^{2j_2} & ... & \alpha^{(n-1)j_2} \\ . & . & . & & . \\ . & . & . & & . \\ . & . & . & & . \\ 1 & \alpha^{j_r} & \alpha^{2j_r} & ... & \alpha^{(n-1)j_r} \end{pmatrix}.$$

Recibido el vector $y = c + e$, o en notación polinómica $y(X) = c(X) + e(X)$, lo que nos interesa es conocer el error cometido durante la transmisión. El primer paso para esto, como hasta ahora, será calcular el síndrome $s = Hy^t$, en particular,

$$s_i = y(\alpha^{j_i}) = e(\alpha^{j_i}) \text{ con } i = 1, \ldots, r.$$

Si se han cometido t errores en las posiciones $i_1, \ldots, i_t$, con valores del error $e_{i_1}, \ldots, e_{i_t}$, el síndrome vendrá dado por

$$s_j = \sum_{m=1}^{t} e_{i_m} (\alpha^{i_m})^j, \text{ con } j = j_1, \ldots, j_r.$$

Así, si consideramos el siguiente sistema de ecuaciones sobre $\mathbb{F}_{q^l}[X_1, ..., X_t, E_1, ..., E_t]$

$$[S] \begin{cases} \sum_{m=1}^{t} E_m X_m^j = s_j, & j \in \{j_1, \ldots, j_r\} \\ E_m^q = E_m, & m = 1, \ldots, t \\ X_m^n = 1, & m = 1, \ldots, t \end{cases}.$$

Notamos que $X_m = \alpha^{i_m}$, $E_m = e_{i_m}$, con $m = 1, \ldots, t$ es una solución del sistema y además la única solución, salvo permutaciones, pues en caso contrario no se daría la unicidad del vector error. Es por ello que tomaremos el sistema [S] como el ideal generado por los polinomios que lo conforma en $\mathbb{F}_{q^l}[X_1, ..., X_t, E_1, ..., E_t]$, que denotaremos por (S) y nuestro objetivo será calcular la variedad de dicho ideal, es decir, los ceros de las ecuaciones que nos proporcionarán el vector error buscado. A partir de esta idea surge la siguiente proposición.

Proposición 3.2. *Si suponemos que han ocurrido exactamente t errores en las posiciones $i_1, ..., i_t \in \{1, ..., n\}$ con valor de error $e_{i_1}, ..., e_{i_t}$, entonces existen $t!$ puntos en $V(E_y)$, los cuales serán de la forma:*

$$\{(\alpha^{i_{\sigma(1)}}, \ldots, \alpha^{i_{\sigma(t)}}, e_{i_{\sigma(1)}}, \ldots, e_{i_{\sigma(t)}}) \in \mathbb{F}_{q^l}^{2t} / \sigma \in S_t\}, \tag{3.1}$$

con S_t grupo simétrico de las permutaciones de t elementos.

Demostración. Como consecuencia de la simetría de los polinomios de (S), todos los puntos del conjunto (3.1) están en la variedad de (S). Además, por unicidad del vector error son los únicos puntos de $V(S)$.

□

Antes de continuar, veamos un resultado que resulta fundamental a la hora de relacionar las bases de Gröbner con este método de descodificación.

Teorema 3.3. *Sea $I \subset K[X_1, ..., X_n]$ un ideal y sea G una base de Gröbner de I con respecto al orden lexicográfico, donde $X_n > X_{n-1} > ... > X_1$. Entonces, para cada $1 \leq k \leq n$, el conjunto*

$$G_k = G \cap K[X_1, ..., X_k]$$

es una base de Gröbner del k-ésimo ideal de eliminación $I_k = I \cap K[X_1, ..., X_k]$.

Si definimos el orden lexicográfico $\prec$ donde

$$X_1 \prec E_1 \prec \ldots \prec X_t \prec E_t,$$

podemos observar que se trata de un orden monomial que satisface el Teorema 3.3. Por lo tanto, si $\mathcal{G}$ es una base de Gröbner del ideal (S), atendiendo al Teorema 3.3, tenemos que el conjunto $\mathcal{G}_1 = \mathcal{G} \cap F_q[X_1]$ es una base de Gröbner del ideal $(S_1) = (S) \cap F_q[X_1]$, la cual estará compuesta por un unico elemento, pues el anillo de polinomios $F_q[X_1]$ es un dominio de ideales principales.

Con las variables X_1 y E_1 obtenemos los errores: primero localizamos su posición con X_1 mientras que sus valores los obtenemos con E_1. Más concretamente, como consecuencia del Teorema de Extensión (ver [2, Chapter 3, Theorem 3]), que generaliza a sistemas polinomiales el proceso de resolución de sistemas triangulares de ecuaciones, podemos afirmar que las posiciones de los errores se obtienen al calcular la variedad asociada a (S_1). Teniendo en cuenta que $\mathcal{G}_1 = \{g_1(X)\}$, calcular dicha variedad no es más que resolver una ecuación con una incógnita.

El siguiente paso en la descodificación es considerar $(S_2) = (S) \cap \mathbb{F}_q[X_1, E_1]$, la base de Gröbner $\mathcal{G}_2 = \mathcal{G} \cap F_q[X_1, E_1]$ y sustituir en ella los valores de X_1 obtenidos en el paso anterior. De esta forma nos encontramos de nuevo en el caso de una única variable E_1 que proporcionará para cada valor de X_1 el valor del error en dicha posición.

Ejemplo 3.1. Sea el cuerpo $\mathbb{F}_2$, $\alpha \in \mathbb{F}_{2^4}$ una raíz quinceava de la unidad y el polinomio $g(X) = X^8 + X^4 + X^2 + X + 1 \in \mathbb{F}_2[X]$. Se comprueba que $g(X)$ divide a $X^{15} - 1$, por tanto genera un código cíclico que denotaremos por $\mathcal{C} = (g(X))$.

Obtenemos que $g(X)$ tiene por raíces a $\alpha^3, \alpha^6, \alpha^7, \alpha^9, \alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14}$. A continuación se presenta una matriz de control del código:

$$H = \begin{pmatrix} 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^{15} & \alpha^{18} & \alpha^{21} & \alpha^{24} & \alpha^{27} & \alpha^{30} & \alpha^{33} & \alpha^{36} & \alpha^{39} & \alpha^{42} \\ 1 & \alpha^6 & \alpha^{12} & \alpha^{18} & \alpha^{24} & \alpha^{30} & \alpha^{36} & \alpha^{42} & \alpha^{48} & \alpha^{54} & \alpha^{60} & \alpha^{66} & \alpha^{72} & \alpha^{78} & \alpha^{84} \\ 1 & \alpha^7 & \alpha^{14} & \alpha^{21} & \alpha^{28} & \alpha^{35} & \alpha^{42} & \alpha^{49} & \alpha^{56} & \alpha^{63} & \alpha^{70} & \alpha^{77} & \alpha^{84} & \alpha^{91} & \alpha^{98} \\ 1 & \alpha^9 & \alpha^{18} & \alpha^{27} & \alpha^{36} & \alpha^{45} & \alpha^{54} & \alpha^{63} & \alpha^{72} & \alpha^{81} & \alpha^{90} & \alpha^{99} & \alpha^{108} & \alpha^{117} & \alpha^{126} \\ 1 & \alpha^{11} & \alpha^{22} & \alpha^{33} & \alpha^{44} & \alpha^{55} & \alpha^{66} & \alpha^{77} & \alpha^{88} & \alpha^{99} & \alpha^{110} & \alpha^{121} & \alpha^{132} & \alpha^{143} & \alpha^{154} \\ 1 & \alpha^{12} & \alpha^{24} & \alpha^{36} & \alpha^{48} & \alpha^{60} & \alpha^{72} & \alpha^{84} & \alpha^{96} & \alpha^{108} & \alpha^{120} & \alpha^{132} & \alpha^{144} & \alpha^{156} & \alpha^{168} \\ 1 & \alpha^{13} & \alpha^{26} & \alpha^{39} & \alpha^{52} & \alpha^{65} & \alpha^{78} & \alpha^{91} & \alpha^{104} & \alpha^{117} & \alpha^{130} & \alpha^{143} & \alpha^{156} & \alpha^{169} & \alpha^{182} \\ 1 & \alpha^{14} & \alpha^{28} & \alpha^{42} & \alpha^{56} & \alpha^{70} & \alpha^{84} & \alpha^{98} & \alpha^{112} & \alpha^{126} & \alpha^{140} & \alpha^{154} & \alpha^{168} & \alpha^{182} & \alpha^{196} \end{pmatrix}.$$

Supongamos recibido el vector $y = (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$, el síndrome de dicho vector es $s = (\alpha^3+\alpha+1, \alpha^3+1, \alpha^3+\alpha, \alpha^3+\alpha^2+\alpha, \alpha^3+\alpha^2+\alpha+1, \alpha^3+\alpha^2+1, \alpha^3+\alpha^2, \alpha^3)$. Denotaremos por s_j a cada componente del vector síndrome con $j = 3, 6, 7, 9, 11, 12, 13, 14$.

Si se han cometido $t = 2$ errores tomamos el anillo de polinomios $\mathbb{F}_{2^4}[X_1, X_2, E_1, E_2]$ y determinaremos el sistema

$$\begin{cases} E_1X_1^3 + E_2X_2^3 - (\alpha^3 + \alpha + 1) = 0; E_1X_1^6 + E_2X_2^6 - (\alpha^3 + 1) = 0 \\ E_1X_1^7 + E_2X_2^7 - (\alpha^3 + \alpha) = 0; E_1X_1^9 + E_2X_2^9 - (\alpha^3 + \alpha^2 + \alpha) = 0 \\ E_1X_1^{11} + E_2X_2^{11} - (\alpha^3 + \alpha^2 + \alpha + 1) = 0; E_1X_1^{12} + E_2X_2^{12} - (\alpha^3 + \alpha^2 + 1) = 0 \\ E_1X_1^{13} + E_2X_2^{13} - (\alpha^3 + \alpha^2) = 0; E_1X_1^{14} + E_2X_2^{14} - \alpha^3 = 0 \\ E_1^2 - E_1 = 0; E_2^2 - E_2 = 0 \\ X_1^{15} - 1 = 0; X_2^{15} - 1 = 0 \end{cases}$$

Una vez obtenido el sistema, tomamos el ideal (S) generado por los polinomios que conforman el sistema. Se comprueba, mediante el sistema algebraico computacional SageMath, que una base de Gröbner de dicho ideal es

$$\mathcal{B} = \{X_2^2 + (\alpha^3 + \alpha^2 + \alpha)X_2 + (\alpha^2 + 1), X_1 + X_2 + (\alpha^3 + \alpha^2 + \alpha), E_1 + 1, E_2 + 1\}.$$

Entonces tomamos

$$(S_1) = (S) \cap \mathbb{F}_{2^4}[X_2] = (X_2^2 + (\alpha^3 + \alpha^2 + \alpha)X_2 + (\alpha^2 + 1)),$$

y calculamos su variedad sobre $\mathbb{F}_{2^4}$, obteniendo que $V(S_1) = \{\alpha^3, \alpha^5\}$. Por tanto determinamos que los errores se han producido en las posiciones 3 y 5. Tomemos ahora el ideal

$$(S_2) = (S) \cap \mathbb{F}_{2^4}[X_2, E_1] = (X_2^2 + (\alpha^3 + \alpha^2 + \alpha)X_2 + (\alpha^2 + 1), E_1 + 1).$$

Notamos que los puntos de la variedad del nuevo ideal serán $V(S_2) = \{(\alpha^3, 1), (\alpha^5, 1)\}$. Por tanto el valor del error es 1 en ambos casos. Por último, podemos descodificar nuestro mensaje de la siguiente forma

$$\begin{aligned} c &= (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1) - (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) = \\ &= (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1). \end{aligned}$$

3.2. Descodificación de códigos de evaluación

Para la descodificación en este tipo de códigos utilizaremos un proceso de descodificación similar al anteriormente explicado.

En primer lugar vamos a definir el código de evaluación sobre una variedad afín $C(I_q, L)$. Para ello tomaremos el ideal $I = (g_1, ..., g_m) \subseteq \mathbb{F}_q[X_1, ..., X_s]$, el cual nos proporcionará al ideal

$$I_q = I + (X_1^q - X_1, ..., X_s^q - X_s).$$

Además tomaremos el $\mathbb{F}_q$-subespacio vectorial $L =< \{f_1 + I_q, ..., f_r + I_q\} >$, con $f_i \in \mathbb{F}_q[X_1, ..., X_s], i = 1, ..., r$. Y por último calculamos la variedad de I_q, $V(I_q) = \{\mathbf{P}_1, ..., \mathbf{P}_n\} \subset \mathbb{F}_q^s$.

Consideramos el código dual $\mathcal{C} = C(I_q, L)^\perp$. Apreciamos que una base del código $C(I_q, L)$ proporciona una matriz de control del código dual. Por lo tanto, si recibimos la palabra $y = (y_1, ..., y_n)$, su síndrome vendrá dado por

$$s_i = \sum_{j=1}^n y_j f_i(\mathbf{P}_j),\ i = 1, ..., r.$$

Sabemos que $y = c + e, c \in \mathcal{C}$ y si suponemos que se han producido t errores en las posiciones $k_1, \ldots, k_t$, con valores $e_{k_1}, \ldots, e_{k_t}$, entonces se tiene que:

$$s_i = \sum_{m=1}^t e_{k_m} f_i(\mathbf{P}_{k_m}),\ i = 1, ..., r.$$

El siguiente paso en el proceso de descodificación será tomar las s variables $\{X_1, ..., X_s\}$ y crear t réplicas de éstas (siendo $w(e) = t$), proporcionando así t paquetes de nuevas variables que denotaremos por $\{X_{i1}, ..., X_{is}\}$, con $i = 1, ..., t$. Observamos que el primer subíndice denota el paquete al que pertenece la variable, y el segundo subíndice denota de qué variable original es réplica. Además añadiremos t variables nuevas que denotaremos por $E_1, ..., E_t$. Una vez hecho esto denotamos por T al anillo de polinomios

$$T = \mathbb{F}_q[X_{11}, ..., X_{1s}, ..., X_{i1}, ..., X_{is}, ..., X_{t1}, ..., X_{ts}, E_1, ..., E_t].$$

El objetivo fundamental que abordaremos será el de calcular la variedad de un ideal muy similar al propuesto en la Sección 3.1, que denotaremos por E_y y estará generado por tres tipos de polinomios que pasamos a definir a continuación.

Polinomios del tipo 1.

La creación de los polinomios del primer tipo se fundamenta en el proceso que realizamos anteriormente para replicar las variables. En este caso, vamos a crear réplicas de los polinomios generadores del ideal $I = (g_1, ..., g_m) \subseteq \mathbb{F}_q[X_1, ..., X_s]$ de la siguiente forma:

$$g_1 \begin{cases} g_{11}(X_{11}, ..., X_{1s}) \in \mathbb{F}_q[X_{11}, ..., X_{1s}] \\ g_{21}(X_{21}, ..., X_{2s}) \in \mathbb{F}_q[X_{21}, ..., X_{2s}] \\ ... \\ g_{t1}(X_{t1}, ..., X_{ts}) \in \mathbb{F}_q[X_{t1}, ..., X_{ts}] \end{cases}$$

$$
\begin{array}{l}
\cdot \\
\cdot \\
\cdot \\
g_m \begin{cases} g_{1m}(X_{11},...,X_{1s}) \in \mathbb{F}_q[X_{11},...,X_{1s}] \\ g_{2m}(X_{21},...,X_{2s}) \in \mathbb{F}_q[X_{21},...,X_{2s}] \\ ... \\ g_{tm}(X_{t1},...,X_{ts}) \in \mathbb{F}_q[X_{t1},...,X_{ts}] \end{cases}
\end{array}
$$

Notamos nuevamente que el primer subíndice de los nuevos polinomios denota en qué paquete de variables está evaluado, mientras que el segundo denota de qué polinomio es réplica. Además es importante observar que dichos polinomios tendrán como raíces al menos a los puntos de $V(I_q)$, pues, en esencia, son los polinomios generadores de I evaluados en otras variables.

Polinomios del tipo 2.

Los polinomios de la segunda categoría son creados de una forma simple, los denotaremos por p_j y serán

$$p_j(E_j) = E_j^{q-1} - 1 \text{ con } j = 1, ..., t.$$

Observamos que para todo $a \in \mathbb{F}_q \backslash \{0\}$ se cumple que $p(a) = 0$. Podemos adelantar que dicho polinomio servirá para mantener los valores del error en el cuerpo $\mathbb{F}_q$.

Polinomios del tipo 3.

Por último, y teniendo en cuenta que $s_i = \sum_{m=1}^{t} e_{k_m} f_i(\mathbf{P}_{k_m})$, $i = 1, ..., r$, denotamos por h_i a

$$h_i = \sum_{j=1}^{t} E_j f_i(X_{j1}, ..., X_{js}) - s_i, \ i = 1, ..., r,$$

los cuales supondrán los polinomios del tercer tipo.

Es preciso observar alguna característica que presentan estos polinomios. En primer lugar notamos que cada polinomio h_i depende de un solo f_i y que tendremos tantos polinomios h_i como generadores del subespacio vectorial L. Nuevamente podemos observar que se han creado t réplicas de los polinomios f_i de una forma análoga a la anterior y que escribimos como:

$$
f_i \begin{cases} f_i(X_{11},...,X_{1s}) \in \mathbb{F}_q[X_{11},...,X_{1s}] \\ f_i(X_{21},...,X_{2s}) \in \mathbb{F}_q[X_{21},...,X_{2s}] \\ ... \\ f_i(X_{t1},...,X_{ts}) \in \mathbb{F}_q[X_{t1},...,X_{ts}] \end{cases}
$$

Además observamos que en cada polinomio h_i actúan las t réplicas del polinomio f_i, cada una de estas multiplicadas por un respectivo E_j, por tanto

$h_i = \sum_{j=1}^{t} E_j f_i(X_{j1}, ..., X_{js}) - s_i \in \mathbb{F}_q[X_{11}, ..., X_{1s}, ..., X_{t1}, ..., X_{ts}, ...E_1, ..., E_t]$, $i = 1, ..., r$.

Por último, es importante destacar que para un i fijo, el polinomio h_i es simétrico para cualquier permutación de j.

Una vez detallados estos polinomios consideraremos el ideal

$$E_y = (\{g_{jl}, E_j^{q-1} - 1, h_i / j = 1, ..., t,\ l = 1, ..., m \text{ e } i = 1, ..., r\})_q$$

en el anillo de polinomios $\subseteq \mathbb{F}_q[X_{11}, ..., X_{1s}, ..., X_{t1}, ..., X_{ts}, ...E_1, ..., E_t]$.

Observaciones 3.1. El ideal E_y contiene también a los polinomios de la forma $X_{jk}^{q-1} - X_{jk}$ con $j = 1, ..., t$ y $k = 1, ..., s$.

Una vez generado el ideal, estamos en disposición de calcular la variedad del ideal E_y. Para ello notamos que la variedad del ideal E_y es

$$V(\{g_{jl} : (j,l) \in \{1, \ldots, t\} \times \{1, \ldots, m\}\}) \cap V(\{p_j : j \in \{1, \ldots, t\}\}) \cap V(\{h_i : i \in \{1, \ldots, r\}\}).$$

Es por ello que iremos analizando cada uno de estos conjuntos por separado.

Variedad del ideal $(\{g_{jl} : (j,l) \in \{1, \ldots, t\} \times \{1, \ldots, m\}\})$

En primer lugar observamos que naturalmente se tiene que

$$V(\{g_{jl} : (j,l) \in \{1, \ldots, t\} \times \{1, \ldots, m\}\}) =$$

$$= \left\{a \in \mathbb{F}_q^{ts} : \forall (j,l) \in \{1, ..., t\} \times \{1, ..., m\}\, g_{jl}(a) = 0\right\} =$$

$$= \{(P_{1i_1}, ..., P_{si_1}, P_{1i_2}, ..., P_{si_2}, ..., P_{1i_t}, ..., P_{si_t}) / i_1, ..., i_t \in \{1, 2, ..., n\}\},$$

donde el segundo subíndice de cada punto denota de qué punto de la variedad original es réplica, mientras que el primer subíndice marca la coordenada de la que es réplica. Es preciso observar que dentro de los puntos de la variedad $V(E_y)$, la variedad $V(\{g_{jl} : (j,l) \in \{1, \ldots, t\} \times \{1, \ldots, m\}\})$ impone condiciones sobre las primeras ts coordenadas.

Variedad del ideal $(\{p_j : j \in \{1, \ldots, t\}\})$

A continuación analizaremos los puntos correspondientes a $V(\{p_j : j \in \{1, \ldots, t\}\})$, variedad que impondrá condiciones sobre las t últimas coordenadas de los puntos de la variedad E_y. Veamos de qué forma:

$$V(\{p_j : j \in \{1, \ldots, t\}\}) = \left\{a \in \mathbb{F}_q^t : \forall j \in \{1, ..., t\}\, p_j(a) = 0\right\} =$$

$$= \left\{ a \in \mathbb{F}_q^t : \forall j \in \{1, ..., t\}\, ,\, a_j^{q-1} - 1 = 0 \right\} =$$
$$= \left\{ (a_1, ..., a_t) \in \mathbb{F}_q^t : \forall j \in \{1, ..., t\}\, a_j \in \mathbb{F} \backslash \{0\} \right\} = \mathbb{F}_q^t \backslash \{0\}$$

Por lo tanto, las t últimas coordenadas permanecerán en el cuerpo $\mathbb{F}_q$ y serán no nulas.

Variedad del ideal E_y

Para finalizar, analicemos como son los puntos de la variedad E_y. Para ello estudiaremos la variedad del ideal $(\{h_i : i \in \{1, \ldots, r\}\})$ restringida a las dos variedades obtenidas anteriormente. Tomamos un polinomio, para un i fijo,

$$h_i = \sum_{j=1}^{t} E_j f_i(X_{j1}, ..., X_{js}) - s_i,$$

y lo evaluaremos en un punto arbitrario $a \in V(\{g_{jl} : (j, l) \in \{1, \ldots, t\} \times \{1, \ldots, m\}\}) \cap V((\{p_j : j \in \{1, \ldots, t\}\})$. Recordemos que $s_i = \sum_{m=1}^{t} e_{k_m} f_i(\mathbf{P}_{k_m})$, $i = 1, ..., r$. Por tanto, tendremos que $h_i(a) = 0$ si y solo si $\sum_{m=1}^{t} \alpha_{k_m} f_i(\mathbf{P}_{k_j}) = s_i$, con $\alpha_{k_m} \in \mathbb{F}_q - \{0\}$ y $k_m \in \{1, ..., n\}$.

Una vez analizada por partes la variedad del ideal E_y podemos escribir el siguiente resultado.

Teorema 3.4. *Si han ocurrido exactamente t errores (siendo t la capacidad correctora del código) en las posiciones $i_1, ..., i_t \in \{1, ..., n\}$ con valor de error $e_{i_1}, ..., e_{i_t}$, entonces existen exactamente $t!$ puntos en $V(E_y)$, los cuales serán de la forma:*

$$\left\{ (P_{1\sigma(i_1)}, ..., P_{s\sigma(i_1)}, ..., P_{1\sigma(i_t)}, ..., P_{s\sigma(i_t)}, e_{\sigma(i_1)}, ..., e_{\sigma(i_t)}) / i_1, ..., i_t \in \{1, 2, ..., n\} \right\},$$

siendo $\sigma \in S_t$ el grupo simétrico de de permutaciones de t elementos.

Demostración. La demostración es análoga a la realizada para la Proposición 3.2 □

Observamos entonces que solo bastará con conocer uno de los puntos de la variedad del ideal E_y para conseguir obtener el error producido en el mensaje. Es aquí donde entra en juego el papel de las bases de Gröbner. Para ello es necesario en primer lugar definir un orden monomial basado en la extensión del orden lexicográfico. El orden lexicográfico que tomaremos implica a las variables del primer paquete junto con el primer error donde

$$X_{11} \prec_1 X_{12} \prec_1 ... \prec_1 X_{1s} \prec_1 E_1. \tag{3.2}$$

En dicho orden monomial tomaremos los monomios en T y los escribiremos como MN de tal manera que M implique a las variables de (3.2) mientras que la segunda parte del elemento implica al resto de variables. Entonces sean M_1N_1 y M_2N_2 elementos de nuestra anillo de polinomios T, se define el orden de eliminación $\prec$ como:

$$M_1N_1 \prec M_2N_2 \iff \begin{cases} M_1 \prec_1 M_2 \\ Si\, M_1 = M_2,\, entonces\, N_1 \prec_2 N_2 \end{cases},$$

siendo $\prec_2$ cualquier otro orden monomial que implica al resto de variables que no están en (3.2).

Una vez llegados a este punto, es natural plantearse desarrollar el mismo procedimiento que el visto en la Sección 3.1. El desarrollo del método deberá determinar las posibles soluciones para las variables $X_{11}, \ldots, X_{s1}$, las cuales determinarán los localizadores de errores, y de la variable E_1 que nos dará el valor del error cometido en cada posición.

Una vez definido tal orden monomial, suponemos $\mathcal{G}$ una base de Gröbner del ideal E_y. Entonces, atendiendo al Teorema 3.3 podemos determinar para cada ideal

$$I_i = E_y \cap \mathbb{F}_q[x_{11}, \ldots, x_{qi}],\ i = 1, \ldots, s,$$

una base de Gröbner $\mathcal{G}_i = \mathcal{G} \cap \mathbb{F}_q[x_{11}, \ldots, x_{1i}]$, $i = 1, \ldots, s$. Es entonces cuando, teniendo en cuenta nuevamente el ya citado Teorema de Extensión, podemos obtener las soluciones buscadas bajo un método de sustitución.

En primer lugar determinaremos $I_1 = E_y \cap \mathbb{F}_q[X_{11}]$, el cual será un ideal principal por la naturaleza del anillo $\mathbb{F}_q[X_{11}]$. Un generador de dicho ideal será $\mathcal{G}_1 = (g_{11}[X_{11}])$. Determinando los ceros del polinomio generador, obtenemos todos los posibles valores para X_{11}. A continuación, repetimos el proceso sobre $I_2 = E_y \cap \mathbb{F}_q[X_{11}, X_{12}]$ y sustituyendo en los polinomios que generan $\mathcal{G}_2 = \mathcal{G} \cap \mathbb{F}_q[X_{11}, X_{12}]$ los valores obtenidos anteriormente para X_{11} obtenemos, determinando las raíces de los polinomios que conforman la base de Gröbner de I_2, los pares (α, β) que determinan las dos primeras componentes de los puntos de $V(E_y)$. Repitiendo el proceso obtenemos todas los posibles valores para las s primeras componentes, que determinarán las posiciones del error, y la componente marcada por la variable E_1 que proporcionará los posibles valores de los errores.

Ejemplo 3.2. Para desarrollar este ejemplo, haremos uso del código dual del código descrito en el Ejemplo 2.14. Recordemos que el código que obtuvimos, que denotaremos por $C(I, L)$, con $I = (X^2+Y^2+Z, X+Y)$, $V(I_q) = \{(0,0,0), (1,1,0), (\alpha,\alpha,0), (\alpha+1, \alpha+1, 0)\}$ y $L =< \{X + I_4, Y + 1 + I_4\} >$, era un código de dimensión 2, longitud 4 y distancia mínima 3, luego su capacidad correctora es 1. Además las matrices generatriz y de control del código son

$$G = \begin{pmatrix} 0 & 1 & \alpha & \alpha+1 \\ 1 & 0 & \alpha+1 & \alpha \end{pmatrix} \text{ y } H = \begin{pmatrix} 1 & 0 & \alpha+1 & \alpha \\ 0 & 1 & \alpha & \alpha+1 \end{pmatrix}$$

respectivamente. Por lo tanto, el código que usaremos en el ejemplo tendrá por matriz generatriz H, mientras que G cumple el papel de matriz de control. Supongamos recibido el mensaje $y = (1, 1, \alpha + 1, \alpha)$, y supongamos cometido 1 error durante la transmisión del mensaje, esto es $t = 1$, . El vector síndrome del mensaje es $s = (1, 0)$. Observamos que al tratarse de un solo error no hará falta replicar las variables. Consideremos el ideal $E_y \subseteq \mathbb{F}_q[X, Y, Z, E]$ generado por los siguientes polinomios.

Polinomios del tipo 1

$$g_1(X,Y,Z) = X^2 + Y^2 + Z \text{ y } g_2(X,Y,Z) = X + Y.$$

Polinomios del tipo 2

$$p(E) = E^3 - 1.$$

Polinomios del tipo 3

$$h_1(X,Y,Z,E) = EX - 1 \text{ y } h_2(X,Y,Z,E) = E(Y+1).$$

Recordemos que, por definición, el ideal E_y contiene también a los polinomios $X^4 - X$, $Y^4 - Y$ y $Z^4 - Z$. Para calcular la variedad de E_y, obtenemos una base de Gröbner de dicho ideal, nuevamente haciendo uso del sistema algebraico computacional SageMath:

$$\mathcal{G} = \{X+1, Y+1, Z, E+1\}.$$

Siguiendo el procedimiento descrito obtenemos que los localizadores de errores son las raíces de los polinomios $X+1$, $Y+1$ y Z, que son, respectivamente, 1, 1, 0, esto conforma el punto (1,1,0), lo que nos indica que el error se ha cometido en la segunda posición. Además, resolviendo el polinomio $E_1 + 1$, obtenemos que el valor del error es 1, luego el mensaje corregido quedaría

$$c = (1, 1, \alpha+1, \alpha) - (0, 1, 0, 0) = (1, 0, \alpha+1, \alpha).$$

Ejemplo 3.3. Sea $\mathbb{F}_4[X,Y]$ el anillo de polinomios e $I = (Y^2 + Y - X^3) \subset \mathbb{F}_4[X,Y]$ un ideal. Se comprueba que

$$V(I_4) = \{(0,0), (0,1), (1,\alpha), (1,\alpha^2), (\alpha,\alpha), (\alpha,\alpha^2), (\alpha^2,\alpha), (\alpha^2,\alpha^2)\}.$$

Tomaremos el subespacio vectorial

$$L = < \{1 + I_4, X + I_4, Y + I_4, XY + I_4\} > .$$

y consideramos el código $\mathcal{C} = C(L, I_4)$, cuya matriz de control es

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \alpha & \alpha & \alpha^2 & \alpha^2 \\ 0 & 1 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha & \alpha^2 \\ 0 & 0 & 1 & 1 & \alpha^2 & \alpha^2 & \alpha & \alpha \\ 0 & 0 & \alpha & \alpha^2 & \alpha^2 & 1 & 1 & \alpha \end{pmatrix}.$$

Obtenemos que se trata de un código de longitud 8, dimensión 5 y distancia mínima 5, por ello tiene capacidad correctora $t = 2$. Supongamos recibido el mensaje

$$y = (\alpha+1, 0, \alpha+1, 1, \alpha+1, 1, \alpha, 1).$$

Se comprueba que su síndrome es

$$s(y) = (0, \alpha+1, 0, \alpha, 1).$$

Una vez obtenido, podemos calcular los polinomios que generarán el ideal E_y.

Polinomios del tipo 1

$$g_{11}(X_1, Y_1) = Y_1^2 + Y_1 - X_1^3 \text{ y } g_{21}(X_2, Y_2) = Y_2^2 + Y_2 - X_2.$$

Polinomios del tipo 2

$$p_1(E_1) = E_1^3 - 1 \text{ y } p_2(E_2) = E_2^3 - 1.$$

Polinomios del tipo 3
$h_1(X_1, Y_1, X_2, Y_2, E_1, E_2) = E_1 + E_2$
$h_2(X_1, Y_1, X_2, Y_2, E_1, E_2) = E_1X_1 + E_2 + X_2 - (\alpha + 1)$,
$h_3(X_1, Y_1, X_2, Y_2, E_1, E_2) = E_1Y_1 + E_2Y_2$
$h_4(X_1, Y_1, X_2, Y_2, E_1, E_2) = E_1X_1^2 + E_2X_2^2 - a$
$h_5(X_1, Y_1, X_2, Y_2, E_1, E_2) = E_1X_1Y_1 + E_2X_2Y_2 - 1$.

Recordemos que el ideal E_y contiene a los polinomios

$$X_1^4 - X_1,\ X_2^4 - X_2,\ Y_1^4 - Y_1, \text{ y } Y_2^4 - Y_2.$$

Obtenemos que una base de Gröbner del ideal E_y es

$$\mathcal{B} = \{X_2^2 + (\alpha + 1)X_2 + \alpha, X_1 + X_2 + (\alpha + 1), Y_1 + \alpha, Y_2 + \alpha, E_1 + 1, E_2 + 1\}.$$

Observamos que una base del ideal $(S_1) = E_y \cap \mathbb{F}_4[Y_1]$ es

$$\mathcal{B}_1 = \{Y_1 + \alpha\}$$

cuya variedad es $V(S_1) = \{\alpha\}$. A constinuación, obtenemos $(S_2) = E_y \cap \mathbb{F}_4[Y_1, X_1]$, de donde podemos calcular los localizadores de errores

$$(1, \alpha),\ (\alpha, \alpha).$$

Por tanto podemos determinar que los errores se produjeron en la tercera y la quinta posición. Por último mediante el ideal de eliminación $(S_3) = E_y \cap \mathbb{F}_4[Y_1, X_1, E_1]$ podemos determinar que los valores del error fue, en ambos casos, $e_3 = 1$ y $e_5 = 1$. Una vez acabado este proceso, podemos concluir que el mensaje enviado fue

$$(\alpha + 1, 0, \alpha, 1, \alpha, 1, \alpha, 1).$$

Conclusiones

En esta memoria se ha presentado una introducción a la teoría de códigos correctores. En primer lugar, se ha hecho una breve introducción a la teoría de códigos correctores tratando, de un modo más específico, los códigos lineales y algunas familias de estos. A continuación, se han analizado los códigos de evaluación sobre variedades afines y se ha mostrado un algoritmo de descodificación mediante el uso de bases de Gröbner para códigos cíclicos y códigos de evaluación sobre variedades afines a una variedad.

La teoría de códigos correctores es una herramienta fundamental en el manejo y transmisión de información. Actualmente, nuevos sistemas de comunicaciones inalámbricos, como el Li-Fi, depende de este tipo de códigos para su evolución. Este tipo de sistema de comunicación es un sistema de bajo costo que ha probado ser hasta cien veces más rápido que la tecnología Wi-Fi. Sin embargo, es más vulnerable a la generación de errores, y es aquí donde la teoría de códigos correctores juega un papel importante. Por ello el avance en el estudio de esta teoría ayudaría a garantizar el buen funcionamiento de nuevas tecnologías.

No obstante, el avance en la descodificación de los códigos correctores de errores perjudicaría a lo que hoy se conoce como *Criptografía basada en códigos.* que nació ante la amenaza que representa la aparición de los ordenadores cuánticos.

Durante la elaboración de esta memoria se ha podido calcular el método de descodificación mediante el uso de bases de Gröbner en algunos ejemplos concretos. Sin embargo, al aumentar el número de variables, o la capacidad correctora del código, la descodificación se vuelve casi impracticable, debido a la magnitud de las bases de Gröbner, implicando esto una búsqueda casi exhaustiva. Aun así la existencia de este método de descodificación para algunos códigos concretos supone un éxito en tanto que el problema general de descodificación, como se mencionó anteriormente, es un problema NP-completo.

Los ejemplos propuestos en el texto utilizan como alfabeto, en la mayoría de los casos, los cuerpos finitos $\mathbb{F}_2$ y $\mathbb{F}_4$, pues son los más usados en la actualidad en este campo. No obstante, todos los resultados incluidos se generalizan para cualquiera cuerpo de la forma $\mathbb{F}_q$ siendo q potencia de un número primo.

Bibliografía

[1] Boer M., y Pellikaan R. (1995) *Gröbner bases for error-correcting codes and their decoding*. Eindhoven.

[2] Cox D., Little J., y O'Shea D. (1992). *Ideal, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. New York: Springer-Verlag.

[3] Fitzgerald, J., y Lax R. (1998). Designs, Codes and Cryptography, 13, 147-158, (1998) *Decoding affine variety bodes using Göbner base*

[4] Kreuzer, M., y Robbiano L. (2000). *Computational Commutative Algebra 1*. Springer.

[5] Lauritzen N. (2005). *Concrete abstract algebra: from numbers to Gröbner bases*. United Kingdom: Cambridge University Press

[6] Martínez Moro, E., Munuera Gómez C., y Ruano Benito D. (2007). *Bases de Gröbner: aplicaciones a la codificación algebraica*. Caracas, Venezuela.

[7] Seidenberg A. (1974). *Construction in algebra*. America Mathematical Society, 97.

Using Gröbner bases in coding theory

Adrián Cruz Guerra
University of La Laguna

Linear codes

Let $\mathbb{F}_q$ a finite field with q elements. A q-ary linear code of length n is a linear subspace $\mathcal{C} \subseteq \mathbb{F}_q^n$. We say it is a $[n, k, d]$ linear code, where d is the minimum distance of the code and t=$\lfloor (d-1)/2 \rfloor$ its correcting capacity. The basis of this linear subspace will form what we call the generator matrix G. Therefore,

$$\mathcal{C} = \{aG | a \in \mathbb{F}^n\}.$$

The orthogonal linear subspace, $\mathcal{C}^\perp$, is the dual code, and its generator matrix H verifies

$$Ha^t = 0 \text{ for all } a \in \mathcal{C}$$

Thereby, $s = Hy^t$ is the syndrome and with the relation $u \sim v \iff s(u) = s(v)$ we obtain $\mathbb{F}_q^n/\mathcal{C}$, where the class leader is the element of weight less than or equal to t.

Syndrome-leader algorithm

input(y);
$s := Hy^t$;
if $s_j = 0$ for all j
  then output(y);stop;{no errors occurred}
else;
  Look for the class leader;
    If such leader doesn't exist, the decodification fails;
    Otherwise, the leader is the error; output($y - e$)

Cyclic codes

A linear code $\mathcal{C}$ of length n over $\mathbb{F}_q$, is a cyclic code if for every $(c_0, c_1, ...c_{n-1}) \in \mathcal{C}$, then $(c_1, c_2, ...c_{n-1}, c_0) \in \mathcal{C}$.

Theroem: Let $\mathcal{C}$ a nonzero linear code of length n over the finite field $\mathbb{F}_q$. We say that $\mathcal{C}$ is cyclic if, and only if, seen in the ring $A_{q,n}$, is an ideal generated by a polynomial $g(X)$ divisor of $X^n - 1$.

This codes may be defined from the zeroes of the generator polynomial, taking as control matrix

$$H' = \begin{pmatrix} 1 & \alpha_1 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \dots & \alpha_2^{n-1} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ 1 & \alpha_r & \dots & \alpha_r^{n-1} \end{pmatrix}$$

with $\alpha_1, \dots, \alpha_r$ roots of $g(X)$.

BCH Codes

We call BCH code of length n and minimum distance δ, a cyclic code of length n and the roots of its generator polynomial are $\alpha^b, ..., \alpha^{b+\delta-2}$, with $b \geq 0$ and $\delta \geq 1$.

The BCH codes may be distinguished attending the next classification:

1. If $b = 1$ we call BCH code in the strict sense.
2. If $n = q^m - 1$ we call primitive BCH code.
3. If, moreover, $m = 1$, that is, $n = q - 1$, we call it Reed-Solomon code.

Affine variety codes

Let $I \subset \mathbb{F}_q[X_1, \dots, X_s]$ be an ideal, we denote

$$I_q = I + (X_1^q - X_1, ..., X_s^q - X_s).$$

So we have $V(I_q) = \{P_1, \dots, P_n\}$. Thus, we define an affine variety code as it follows.

Definition Let the map

$$ev : R \longrightarrow \mathbb{F}_q^n$$
$$f + I_q \longmapsto ev(f + I_q) = (f(P_1), \dots, f(P_n))$$

$L =< \{f_1 + I_q, \dots, f_s + I_q > a \mathbb{F}_q$-linear subspace of $\mathbb{F}_q[X_1, ..., X_s]/I_q$. We define the affine variety code $C(I_q, L)$ to be $ev(L)$, the image of L under the map ev.

Groebner Bases

Let a monomial order $\succ$ and an ideal $I \subset R$. We say that the set $\{f_1, \dots, f_s\} \subset R$ is a Groebner Bases of I for $\succ$ if it satisfies

$$(lt_\succ(f_1), \dots, lt_\succ(f_s)) = (lt_\succ(I))$$

where $lt_\succ(I) = \{lt_\succ(f) | f \in I\}$.

Theorem:Given a monomial order $\succ$ and an ideal $I \subset R$, it exists a Groebner bases of I and it is a generator set of the ideal I.

Decoding cyclic codes

Let $\mathcal{C}$ be a $[n, k, d]$ cyclic code over the field $\mathbb{F}_q$, generated by the polynomial $g(X)$ of degree $r = n - k$. Let us take $\mathbb{F}_{q^l}$ an extension of $\mathbb{F}_q$ such that, all root of $g(X)$. is in $\mathbb{F}_{q^l}$. Now, we take a nth primitive root of the unit, α, over $\mathbb{F}_{q^l}$, and let $J(\mathcal{C}) = \{j_1, ..., j_r\}$ such that for all $i \in J(\mathcal{C})$, α^i is root of $g(X)$. We denote by H its control matrix, and let us suppose that t errors have occured. Then the decoding algorithm is the following one:

Algorithm

input(y);
$s := Hy^t$;
if $s_j = 0$ for all j
  then output(y);stop;{no errors occurred}
else;
  $S := (\{\sum_{m=1}^{t} Y_m X_m^j - s_j, j \in J\} \cup$
  $\cup \{Y_m^q - Y_m, X_m^n - 1, m = 1, \dots t\})$
  $\mathcal{G} := Groebner(S)$;
  $\{g_1(X_1)\} := \mathcal{G} \cap \mathbb{F}_{q^l}[X_1]$;
  error.locators:={zero of $g(X_1)$};
  $\mathcal{G}_2 := \mathcal{G} \cap \mathbb{F}_{q^l}[X_1, X_2]$;
  error.value:= {zero of $\mathcal{G}_2/X_1$ is an error-locator}

Decoding affine variety codes

Let $\mathcal{C} \subset \mathbb{F}_q^n$ be an affine variety code and H the control matrix of that code. Let t be the number of errors made and $\mathbb{F}_q[X_{11}, ..., X_{1s}, ..., X_{t1}, ..., X_{ts}, ...E_1, ..., E_t]$ the polynomial ring. Then the decoding algorithm is the following one:

Algorithm

input(y);
$s := Hy^t$;
if $s_j = 0$ for all j
  then output(y);stop;{no errors occurred}
else;
  $E_y := (\{g_{jl}, E_j^{q-1} - 1, h_i/j = 1, ..., t,\ l = 1, ..., m \in i = 1, ..., r\})_q$
  $\mathcal{G} := Groebner(E_y)$;
  for j=1 to s
    $I_j = E_y \cap \mathbb{F}_q[x_{11}, \dots, x_{qj}]$
    $\mathcal{G}_j = \mathcal{G} \cap \mathbb{F}_q[x_{11}, \dots, x_{1j}]$
    $e.I_j$:={zero of $\mathcal{G}_j/(X_1, \dots, X_{j-1}) \in e.I_{j-1}$};
  $I_{s+1} = E_y \cap \mathbb{F}_q[x_{11}, \dots, x_{qs}, E_1]$
  $\mathcal{G}_{s+1} = \mathcal{G} \cap \mathbb{F}_q[x_{11}, \dots, x_{1s}, E_1]$
  error.value:= {zero of $\mathcal{G}_{s+1}/(X_1, \dots, X_s) \in e.I_s$};

References

[1] Martnez Moro, E., Munuera Gmez C., y Ruano Benito D. (2007). *Bases de Grbner: aplicaciones a la codificacin algebraica*. Caracas, Venezuela.

[2] Boer M., y Pellikaan R. (1995) *Grbner bases for error-correcting codes and their decoding*. Eindhoven.

[3] Fitzgerald, J.. y Lax R. (1998). Designs, Codes and Cryptography, 13, 147-158, (1998) *Decoding affine variety bodes using Gbner base*