Códigos de subespacios y algunas implementaciones

Universidad del Norte

División de Ciencias Básicas
Departamento de Matemáticas y Estadística

Códigos de subespacios y algunas implementaciones

Darling Vasquez Cassis

Trabajo presentado como requisito parcial para optar al título de Magíster en Matemáticas

Director: Prof. Dr. Ismael S. Gutiérrez García

Barranquilla, Julio de 2013

Agradecimientos

Inicialmente doy gracias a Dios, por estar conmigo en cada paso que doy, por fortalecerme e iluminar mi mente con entendimiento y fe, por haber puesto en mi camino a aquellas personas que han sido soporte y compañía durante este proceso.

Al finalizar esta etapa de realizar una tesis de maestría llena de alegrías, dificultades, ansiedad y la satisfacción de un logro más, es consecuente pensar que esto no hubiese sido posible sin la participación de personas que han facilitado las cosas para que este proyecto llegue a un feliz término. Es por esta razón que es para mí un placer expresarles mis agradecimientos.

A mis padres, hermana y a mi tía Hortensia Cassis, a ellos gracias por creer en mí, por su amor y comprensión constante.

De manera especial agradezco a mi profesor, Dr. Ismael Gutiérrez García, por aceptarme para realizar esta tesis bajo su dirección. Su apoyo, confianza en mí y su capacidad para guiarme ha sido un aporte invaluable, no sólo en el desarrollo del trabajo, sino también en mi formación profesional y personal.

Quiero expresar mi más sincero agradecimiento al profesor Antálcides Olivo y a Alfredo Bayuelo, quienes tuvieron participación activa y un importante aporte en esta tesis. Destaco la disponibilidad, paciencia y ayuda desinteresada de ambos.

A mi novio, mis amigos, mis demás familiares y profesores que de una u otra manera me llenaron de impulso para concluir esta etapa.

A todos, muchas gracias.

Introducción

El presente trabajo de tesis está dividido en tres capítulos. En el primer capítulo presentamos algunos aspectos elementales de la teoría clásica de los códigos lineales. La idea de este es tener la posibilidad posterior de comparar ciertos resultados de la nueva teoría de códigos de red.

En el capítulo siguiente introducimos los códigos de red. Esta nueva rama de las matemáticas discretas es relativamente nueva. Los trabajos mas importantes y los cuales inspiran el presente trabajo de maestría son los realizados por R. Koetter, D. Silva y F. Kschischang [6].

La organización de este capítulo contempla una introducción del modelo de canal operador como una abstracción concisa y consciente del canal encontrado en la codificación en red aleatoria lineal cuando el transmisor ni el receptor conocen las características de transferencia del canal. Posteriormente definimos la métrica de subespacios, la cual es natural y conveniente en el contexto de la codificación en red aleatoria lineal.

Un tema central, tanto en la teoría clásica como en la de red es el estudio de algunas cotas, tales como la del empaquetamiento esférico y de la cobertura esférica, análogas a la cota de Hamming y la cota de Gilbert-Varshamov. Consideramos también el estudio de la cota de Singleton para códigos de dimensión constante. Finalmente, se construye un código de Reed-Solomon bajo el contexto de los códigos de subespacios.

En el tercer capítulo se muestra la construcción de un código tipo Reed-Solomon de red, utilizando el software MAPLE como herramienta computacional. Esta implementación puede considerarse como un aporte personal y original en el trabajo. La importancia radica en que a pesar de la existencia de ciertos algoritmos estos carecen aún de implementaciones eficientes debido a los grandes costos computacionales.

Índice general

Capítulo 1

Teoría clásica de códigos

En este primer capítulo se destacan algunos resultados importantes de la teoría de códigos, particularmente los códigos lineales, los cuales son subespacios de espacios vectoriales sobre un cuerpo finito.

Cabe resaltar algunas ventajas que ofrece trabajar con este tipo de códigos, como por ejemplo, el no necesitar almacenar todos los *codewords* (palabras código), sino una base de dicho subespacio.

Por otro lado, el costo de calcular la distancia mínima de un código disminuirá, debido a que esta se podrá encontrar utilizando el concepto de peso de un vector. Sin embargo la propiedad de linealidad afecta otros parámetros como lo es el orden del código, regularmente para los códigos lineales, si la distancia mínima es "grande", entonces no se cuenta con muchos codewords, y si se quiere tener un código lineal con muchos elementos, entonces se debe trabajar con una distancia mínima pequeña, lo cual limita la corrección y detección de errores.

1.1 Códigos lineales

A lo largo de esta sección K denota siempre un cuerpo finito con q elementos.

1.1.1 Definición. Sea A un alfabeto finito y $n \in \mathbb{N}$. Un subconjunto no vacío C de A^n se denomina código de **longitud** n sobre el alfabeto A. Los elementos de C son llamados **codewords**. Si $|A| = 2$, entonces llamamos a C un código binario.

En este trabajo se considerará siempre como alfabeto el cuerpo finito K y q es potencia de algún número primo. Es decir $K \cong \mathbb{F}_q$, entonces un código

binario es un código definido sobre el cuerpo $\mathbb{F}_2$.

1.1.2 Definición. Sea $n \in \mathbb{N}$. Definimos la función **distancia de Hamming**

$$\mathrm{d} : K^n \times K^n \longrightarrow \mathbb{N}$$

de la siguiente manera: Para $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n) \in K^n$

$$\mathrm{d}(u, v) := |\{j \mid u_j \neq v_j, j = 1, \ldots n\}|.$$

Es decir, d cuenta el número de coordenadas en las que u y v difieren.

1.1.3 Teorema. La distancia de Hamming define una métrica sobre K^n. Es decir, para todo $u, v, w \in K^n$ se verifican
(a) $\mathrm{d}(u, v) \geq 0$ y $\mathrm{d}(u, v) = 0$ si y sólo si $u = v$.
(b) $\mathrm{d}(u, v) = \mathrm{d}(v, u)$, es decir d es simétrica.
(c) $\mathrm{d}(u, v) \leq \mathrm{d}(u, w) + \mathrm{d}(w, v)$. (Desigualdad triangular).

Demostración. La no negatividad y la simetría son inmediatas.

Para la desigualdad triangular, sean $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n)$ y $w = (w_1, \ldots, w_n) \in K^n$. Si $u_j \neq v_j$, entonces $u_j \neq w_j$ o $v_j \neq w_j$, de lo cual se sigue

$$\mathrm{d}(u, v) \leq \mathrm{d}(u, w) + \mathrm{d}(w, v).$$

□

1.1.4 Corolario. La distancia de Hamming es invariante bajo traslaciones. Es decir para todo $u, v, w \in K^n$ se verifica que

$$\mathrm{d}(u + w, v + w) = \mathrm{d}(u, v).$$

Demostración.

$$\begin{aligned} \mathrm{d}(u, v) =& |\{j \mid u_j \neq v_j, j = 1, \ldots n\}| \\ =& |\{j \mid u_j + w_j \neq v_j + w_j, j = 1, \ldots n\}| \\ =& \mathrm{d}(u + w, v + w). \end{aligned}$$

□

Antes de presentar la definición formal de códigos lineales definimos los parámetros de un código en general.

1.1.5 Definición. Sea C un código de longitud n sobre K.

(a) Si $|C| > 1$, entonces llamamos a

$$\mathrm{d}(C) := \mín\{\mathrm{d}(c, c') \mid c, c' \in C, c \neq c'\}$$

la **distancia mínima** de C y si $|C| = 1$, entonces $\mathrm{d}(C) := 0$.

(b) Si $\mathrm{d}(C) = d$ y $M = |C|$, entonces decimos que C es un (n, M, d)-código sobre K. Llamamos a (n, M, d) los **parámetros** de C.

1.1.6 Definición. Sea C un código sobre K, con distancia mínima d y $t \in \mathbb{N}_0$.

(a) C se denomina un código t**-detector**. Es decir, C detecta hasta t errores, si y solo si $d \geq t + 1$.

(b) C se denomina un código t**-corrector**. Es decir, C corrige hasta t errores, si y solo si $d \geq 2t + 1$.

Un problema muy importante en la teoría clásica de códigos es la determinación y clasificación de los códigos perfectos. Presentamos a continuación la defínción y algunas caracterizaciones de estos.

1.1.7 Definición. Sea C un código de longitud n sobre K. Decimos que C es un código perfecto, si existe $r \in \mathbb{N}_0$ tal que

$$K^n = \bigcup_{c \in C} B_r(c)$$

es la union disyunta de las esferas $B_r(c)$.

1.1.8 Teorema. (Cota de Singleton)

Sea C un código de longitud n sobre K, con distancia mínima d. Entonces

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

Demostración. Considere la función

$$f : \ K^n \longrightarrow K^{n-d+1}$$

definida por

$$f(x_1, ..., x_n) := (x_1, ..., x_{n-d+1}).$$

Se verifica que la restricción de f a C es inyectiva, para esta prueba, tome $x, y \in C$ digamos $x = (x_1, ..., x_n)$ y $y = (y_1, ..., y_n)$.

Supongamos que $f(x) = f(y)$, esto es,

$$(x_1, ..., x_{n-d+1}) = (y_1, ..., y_{n-d+1})$$

entonces necesariamente

$$(x_1, ..., x_n) = (y_1, ..., y_n),$$

pues de no ser así, cualquier par de codewords, digamos x, y difieren en máximo $n-(n-d+1) = d-1$ coordenadas. Esto es, $\mathrm{d}(x, y) \leq d-1$, lo cual es absurdo debido a la minimalidad de d. Por tanto se afirma que

$$|C| = |f(C)| \leq |K^{n-d+1}| = q^{n-d+1}.$$

□

1.1.9 Definición. Sea C un código de longitud n, sobre K y distancia mínima d. Decimos que C es un **MDS-código**, si C alcanza la cota de Singleton. Es decir, si

$$|C| = q^{n-d+1}.$$

El nombre de MDS-código se debe a sus siglas en inglés *Maximum Distance Separable*.

1.1.10 Definición. Sea $n \in \mathbb{N}$. Un subespacio vectorial C del espacio K^n, se denomina un **código lineal** de longitud n sobre K. Notamos esto con $C \leq K^n$. Si $\dim_K(C) = k$ y distancia mínima $\mathrm{d}(C) = d$, entonces decimos que C es un $[n, k, d]$-código o también que C es un $[n, k, d]_q$-código. Si en el enunciado de un resultado la distancia mínima de C no juega un papel alguno, entonces decimos simplemente que C es un $[n, k]$-código.

1.1.11 Definición. El **peso** de un vector de K^n se define como el número de coordenadas no nulas de este. Formalmente, si $x = (x_1, ..., x_n) \in K^n$, definimos el peso de x notado $\mathrm{wt}(x)$, como

$$\mathrm{wt}(x) := \mathrm{d}(x, 0) = |\{j \mid x_j \neq 0\}|$$

y la función wt: $K^n \longrightarrow \mathbb{N}_0$, se denomina función peso sobre K^n.

Es común definir también el peso de un vector con el orden de su soporte, el **soporte** de un vector x se define y se nota mediante

$$\mathrm{sop}(x) := \{j \mid \ x_j \neq 0\}.$$

A continuación también se define un concepto que será de gran utilidad en el cálculo de la distancia mínima de un código, dado que más adelante se

mostrará que el peso mínimo y la distancia mínima de un código lineal son iguales. Si $C \neq \{0\}$, entonces el **peso mínimo** de C se define:

$$\mathrm{wt}(C) := \mathrm{mín}\{\mathrm{wt}(x) \mid 0 \neq x \in C\}.$$

Si $C = \{0\}$, entonces se define $\mathrm{wt}(C) = 0$.

1.1.12 Teorema. Sea $n \in \mathbb{N}$. Si $C \leqslant K^n$, entonces

$$\mathrm{d}(C) = \mathrm{wt}(C).$$

Demostración. Si $C = \{0\}$, la afirmación se obtiene trivialmente, en efecto $\mathrm{d}(C) = 0 = \mathrm{wt}(C)$. Supongamos entonces que $C \neq \{0\}$, de la invariancia bajo traslaciones de d y por ser C un espacio vectorial, se sigue

$$\begin{aligned}\mathrm{d}(C) =& \mathrm{mín}\{\mathrm{d}(x, x') \mid x, x' \in C, x \neq x'\}\\ =& \mathrm{mín}\{\mathrm{d}(x - x', 0) \mid x, x' \in C, x \neq x'\}\\ =& \mathrm{mín}\{\mathrm{d}(c, 0) \mid c \in C, c \neq 0\}\\ =& \mathrm{wt}(C).\end{aligned}$$

□

Notamos en lo que sigue con $\mathrm{Mat}(k \times n, K)$ al conjunto de todas las matrices de tamaño $k \times n$ con entradas en K.

1.1.13 Definición. Sea C un $[n, k]$-código sobre K y sean $g_1 = (g_{11}, \ldots, g_{1n})$, ..., $g_k = (g_{k1}, ..., g_{kn}) \in K^n$ filas de una matriz G. Si $B = (g_1, ..., g_n)$ es una base para C, entonces se dice que

$$G = \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix} = \begin{pmatrix} g_{11} & \cdots & g_{1n} \\ \vdots & & \vdots \\ g_{k1} & \cdots & g_{kn} \end{pmatrix} \in \mathrm{Mat}(k \times n, K)$$

es una **matriz generadora** de C.

1.1.14 Teorema. Sea C un $[n, k]$-código sobre K. $G \in \mathrm{Mat}(k \times n, K)$ es una matriz generadora de C, si y sólo si

$$C = \{uG \mid u \in K^k\}.$$

Demostración. Suponga que

$$G = \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix} = \begin{pmatrix} g_{11} & \cdots & g_{1n} \\ \vdots & & \vdots \\ g_{k1} & \cdots & g_{kn} \end{pmatrix} \in \mathrm{Mat}(k \times n, K)$$

es una matriz generadora de C. Si $u = (u_1, u_2, ..., u_k) \in K^k$, entonces

$$\begin{aligned} uG =& (u_1g_{11} + ... + u_kg_{k1}, ..., u_1g_{1n} + ... + u_kg_{kn}) \\ =& (u_1g_{11}, ..., u_1g_{1n}) + ... + (u_kg_{k1}, ..., u_kg_{kn}) \\ =& u_1(g_{11}, ..., g_{1n}) + ... + u_k(g_{k1}, ..., g_{kn}) \\ =& u_1g_1 + ... + u_kg_k \in C. \end{aligned}$$

Lo anterior muestra que $\{uG \mid u \in K^k\} \subseteq C$, y para la otra contenencia es fácil ver que si $c \in C$, entonces por ser G una matriz generadora de C, se tiene que $c = x_1g_1 + ... + x_kg_k$ para cualquier $x \in K^k$, esto es $C \subseteq \{uG \mid u \in K^k\}$.

Recíprocamente, si se cumple que $C = \{uG \mid u \in K^k\}$ y tomamos los vectores de la base canónica de K^k, notados por e_j con $1 \leq j \leq k$, obtenemos lo siguiente,

$$\begin{aligned} e_1G &= g_1 \\ &\vdots \\ e_kG &= g_k. \end{aligned}$$

Es decir las filas de G son codewords de C y además

$$C = \{u_1g_1 + ... + u_kg_k \mid u_j \in K\} = \langle g_1, ..., g_k \rangle.$$

Como la $\dim_K C = k$, entonces $B = (g_1, ..., g_k)$ es una base para C, luego G es una matriz generadora de C. □

1.1.15 Definición. Sea C un $[n, k]$-código sobre un cuerpo finito K, con $k < n$. Se denomina $H \in \text{Mat}(n - k \times n, K)$ una **matriz de control** de C, si

$$C = \{u \in K^n \mid Hu^t = 0\}.$$

El siguiente teorema proporciona un procedimiento para hallar una matriz de control para un $[n, k]$-código C, a partir de una matriz generadora del mismo.

1.1.16 Teorema. Sea C un $[n, k]$-código sobre un cuerpo finito K, con $k < n$. Entonces existe una matriz $H \in \text{Mat}(n - k \times n, K)$ tal que para $x \in K^n$ se verifica que

$$Hx^t = 0 \Leftrightarrow x \in C.$$

Además el rango de H, notado por $\text{Rang}(H) = n - k$. Luego si G es una matriz generadora para C, entonces $HG^t = 0$.

Demostración. Sean $u = (u_1, ..., u_n) \in K^n$, $B = (g_1, ..., g_k)$ una base para C, donde cada $g_j = (g_{j1}, ..., g_{jn})$ es una fila de una matriz generadora G, con $1 \leq j \leq k$, esto es

$$G = \begin{pmatrix} g_{11} & \cdots & g_{1n} \\ \vdots & & \vdots \\ g_{k1} & \cdots & g_{kn} \end{pmatrix}.$$

Entonces calculemos $Gu^t = 0$, el cual es un sistema de ecuaciones lineales homogéneo

$$\begin{aligned} g_{11}u_1 \quad &+\cdots+ \quad g_{1n}u_n \quad = 0 \\ & \qquad\qquad\qquad\quad \vdots \\ g_{k1}u_1 \quad &+\cdots+ \quad g_{kn}u_n \quad = 0. \end{aligned}$$

Como el $\text{Rang}(G) = k$, y del álgebra lineal se tiene para el anterior sistema

$$\text{Rang}(G) + \dim(\ker(G)) = n,$$

entonces $\dim(\ker(G)) = n - k$, es decir la dimensión del espacio solución es $n - k$. Si definimos para dicho espacio una base $B' = (h_1, ..., h_{n-k})$, donde cada $h_j = (h_{j1}, ..., h_{jn})$ es una fila de una matriz $H \in \text{Mat}(n - k \times n, K)$, con $1 \leq j \leq n - k$, definida como

$$H := \begin{pmatrix} h_{11} & \cdots & h_{1n} \\ \vdots & & \vdots \\ h_{n-k,1} & \cdots & h_{n-k,n} \end{pmatrix}.$$

Luego $Hg_i^t = 0$ para todo $i \in \{1, ..., k\}$, por lo tanto $Hx^t = 0$ para todo $x \in C$.

Análogamente se obtiene el siguiente resultado del álgebra lineal, como el $\text{Rang}(H) = n - k$ y equivalentemente

$$\text{Rang}(H) = n - \dim(\ker(H)).$$

Entonces

$$\dim(\ker(H)) = k = \dim_K(C).$$

Esto es, $C = \ker(H)$. □

Ahora se mostrará la ventaja de poder hallar la distancia mínima de un código a partir de una matriz de control asociada a este, a través del siguiente teorema, del cual omitimos su prueba.

1.1.17 Teorema. Sea C un $[n, k]$-código sobre un cuerpo finito K, con $k > 1$ y $H \in \text{Mat}(n-k\times n, K)$ una matriz de control para C. Se definen los siguientes conjuntos:

- $A(r)$= $\{r \in \mathbb{N} \mid r$ columnas de H son linealmente dependientes$\}$.
- $B(r) = \{r \in \mathbb{N} \mid r-1$ columnas de H son linealmente independientes$\}$.

Entonces

$$\mathrm{d}(C) = \mathrm{wt}(C) = \min_{1 \leq r \leq n} A(r) = \max_{1 \leq r \leq n} B(r).$$

Demostración. Ver [5]. □

1.2 Decodificación

A lo largo de esta sección K denota siempre un cuerpo finito con q elementos.

En el proceso de comunicación, se transmite un mensaje sobre un canal expuesto a ruidos, un mensaje x no es mas que un elemento de K^n, para algún número natural n.

El mensaje debe ser transformado, para tratar de protegerlo contra posibles alteraciones, generalmente esta transformación se hace de modo digital, para obtener así una palabra código o codeword. Este proceso se conoce como codificación. Una vez el mensaje pasa por el canal, es probable que este se reciba en forma distorsionada, entonces se procede a decodificarlo. Es decir, tratar de obtener el mensaje original.

La decodificación se define como el proceso mediante el cual se convierten símbolos en información entendible para el receptor. El objetivo principal de la teoría de códigos consiste en codificar y decodificar un mensaje, además de protegerlo de posibles errores y si es el caso, tratar de detectarlos y corregirlos.

Para transformar la información codificada en la información original existen diversos métodos. A manera de ilustración, presentamos dos ejemplos.

La decodificación de máxima verosimilitud.

Esta también se llama **decodificación ML**, denominada así por sus siglas en inglés *Maximum Likelihood Decoding*. Sea $C \leqslant K^n$ y notemos con $P(v|c)$ la probabilidad condicional que se recibió el vector $v \in K^n$, dado que fue enviado $c \in C$. Una decodificación de máxima verosimilitud, decodifica el vector v mediante el codeword c, para el cual se verifica que

$$P(v|c) = \max_{c' \in C} P(v|c').$$

Esto es, mediante el codeword con mayor probabilidad de haber sido enviado. Si existe otro codeword con la misma probabilidad, entonces se elige uno aleatoriamente.

En resumen, la decodificación ML asigna a un vector recibido el codeword más cercano. Es decir, el codeword para el cual la distancia de Hamming con el vector recibido sea mínima. Este método es sencillo de aplicar, pero costoso si C es grande.

Decodificación del síndrome.

Este método de decodificación para códigos lineales hace uso de las clases laterales de espacios vectoriales y algunas de sus propiedades, las cuales son presentadas en el siguiente teorema.

1.2.1 Teorema. Sean $C \leqslant V \leqslant K^n$ y $v_1, v_2 \in V$.
(a) $v_1 + C = v_2 + C$ o $(v_1 + C) \cap (v_2 + C) = \emptyset$.
(b) $v_1 + C = v_2 + C$ si y sólo si $v_1 - v_2 \in C$.
(c) Si $v_1 \in v_2 + C$, entonces $v_1 + C = v_2 + C$.
(d) Si de cada clase lateral elegimos un representante v_j, entonces

$$V = \dot{\bigcup_{j \in J}} (v_j + C).$$

(e) $|C| = |v + C|$, para todo $v \in V$.
(f) Si C es un $[n, k]$-código sobre K, entonces C tiene q^{n-k} clases laterales.

Demostración. Las pruebas de la (a) a la (d) son inmediatas.
(e) Definamos la función $f : C \longrightarrow v + C$ mediante

$$f(x) = v + x,$$

con $v \in V$ fijo. Entonces Si para $x, y \in C$ se tiene que $f(x) = f(y)$, es decir, $v + x = v + y$, y como v es fijo, $x = y$, luego f es inyectiva.
Por otro lado, si $b \in v + C$, entonces existe $x \in C$ tal que $b = v + x$, es decir $b - v = x$, y $f(x) = f(b - v) = v + (b - v) = b$, luego f es sobreyectiva, por tanto, biyectiva y se tiene que $|C| = |v + C|$.
(f) Usando las dos últimas propiedades

$$q^n = |V| = \sum_{j \in I} |v_j + C| = \sum_{j \in I} |C| = |I||C| = |I|q^k,$$

con lo cual se tiene que

$$|I| = \frac{q^n}{q^k} = q^{n-k}.$$

□

El siguiente método de decodificación, es denominado decodificación del síndrome.

1.2.2 Definición. Dados un $[n, k]$-código C sobre K y una matriz de control $H \in \mathrm{Mat}(n-k \times n, K)$. Suponiendo que un codeword $c \in C$ fue enviado y que es recibido un vector $v \in K^n$, se define el vector de error de la siguiente manera:

$$e := v - c.$$

Note además que $e \in v + C$. El **síndrome** de v es un vector $s_v \in K^{n-k}$, definido por

$$s_v := Hv^t.$$

Note que todo $c \in C$ tiene síndrome 0.

1.2.3 Observación. El síndrome de un vector recibido $v \in K^n$ y el síndrome del error e coinciden. En efecto,

$$s_v = Hv^t = H(c+e)^t = Hc^t + He^t = He^t = s_e.$$

1.2.4 Lema. Sea K un cuerpo finito y $n \in \mathbb{N}$. Entonces $x, y \in K^n$ tienen el mismo síndrome, si y sólo si $x + C = y + C$.

Demostración. Para $x, y \in K^n$,

$$\begin{aligned} s_x = s_y &\Leftrightarrow Hx^t = Hy^t \\ &\Leftrightarrow H(x-y)^t = 0 \\ &\Leftrightarrow x - y \in C \\ &\Leftrightarrow x + C = y + C. \end{aligned}$$

□

La aplicación del anterior lema es la siguiente, si c es un *codeword* enviado y se recibe v con posibles alteraciones como e, entonces $v = c + e$, y como v y e tienen el mismo síndrome, pertenecen a la misma clase lateral, la idea de la decodificación del síndrome es asignar al vector recibido v el codeword $v - e_v$, es decir buscar el representante de la clase $e_v \in v + C$ que tenga el mismo síndrome de v.

1.2.5 Ejemplo. Sea C un $[5, 3]$- código binario (sobre $\mathbb{F}_2$), con matriz generadora

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

Aplicando el teorema 1.1.16 es posible hallar una matriz de control correspondiente, para esto resolvamos el sistema de ecuaciones lineales

$$Gu^t = 0,$$

donde $u = (u_1, u_2, u_3, u_4, u_5) \in \mathbb{F}_2^5$, entonces

$$Gu^t = 0 \Leftrightarrow \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \\ u_5 \end{pmatrix} = 0$$

$$\Leftrightarrow \begin{cases} u_1 + u_2 + u_3 = 0 \\ u_1 + u_4 = 0 \\ u_2 + u_5 = 0. \end{cases}$$

Para $u = (u_1, u_2, u_3, u_4, u_5)$ el conjunto solución de $Gu^t = 0$ es dado por

$$S = \{(u_4, u_5, u_4 + u_5, u_4, u_5) \mid u_4, u_5 \in \mathbb{F}_2\}$$

y hallando una base para S, obtenemos una matriz de control para C, digamos

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

Así también, como G es una matriz generadora, del teorema 1.1.14 se tiene

$$C = \{uG \mid u \in \mathbb{F}_2^3\}$$
$$C = u_1 g_1 + u_2 g_2 + u_3 g_3,$$

donde $u_j \in \mathbb{F}_2$ y g_1, g_2, g_3 son las filas de G, Entonces

$$C = \{(11100), (10010), (01001), (01110), (11011), (10101), (00111), (00000)\}$$

y las $q^{n-k} = 2^{5-3} = 4$ clases laterales de C están dadas por $v + C$, con $v \in \mathbb{F}_2^5$. Esto es

$$00000 + C = C$$
$$10000 + C = \{(01100), (00010), (11001), (11110), (01011), (00101), (10111), (10000)\}$$
$$01000 + C = \{(10100), (11010), (00001), (00110), (10011), (11101), (01111), (01000)\}$$
$$00100 + C = \{(11000), (10110), (01101), (01010), (11111), (10001), (00011), (00100)\}.$$

Ahora suponga que se recibió el vector $v = (01101)$. Entonces este tiene el mismo síndrome que $e = (00100)$ (representante de la cuarta clase lateral de C). Por lo tanto la decodificación del síndrome le asigna el codeword

$$c = v - e = (01101) - (00100) = (01001).$$

Representante de la clase lateral	Síndrome
$e_0 = 00000$	$He_0^t = (0,0)^t$
$e_1 = 01000$	$He_1^t = (0,1)^t$
$e_2 = 00100$	$He_2^t = (1,0)^t$
$e_3 = 00010$	$He_3^t = (1,1)^t$

1.3 Los códigos de Hamming

A lo largo de esta sección K denota siempre un cuerpo finito con q elementos.

Ahora consideramos una familia de códigos perfectos, recordemos que los códigos perfectos son aquellos que a partir de un radio fijo r, las esferas centradas en los *codewords* con radio r logran cubrir todo el espacio K^n, a través de una union disjunta.

Es también conocido que dado un código $C \neq \{0\}$ de longitud n sobre K y $\mathrm{d}(C) = 2r + 1$, con $r \in \mathbb{N}_0$, entonces C es perfecto si y sólo si se verifica la igualdad en la cota del empaquetamiento esférico. Es decir, si y solo si,

$$|C| = \frac{q^n}{\sum_{j=0}^{r} \binom{n}{j}(q-1)^j}.$$

1.3.1 Teorema. Sean $k \in \mathbb{N}$ con $k \geq 2$ y $n = \frac{q^k-1}{q-1}$. Entonces existe un $[n, n-k, 3]$-código perfecto sobre K, el cual denominamos **código de Hamming.**

Demostración. Cada vector $v \in K^k$, $v \neq 0$, determina un subespacio vectorial de dimensión uno, esto es, una recta generada por v, la cual está dada por

$$\langle v \rangle = \{kv \mid k \in K\}.$$

El espacio vectorial K^k tiene $q^k - 1$ vectores no nulos y para cada $v \in K^k$ no nulo existen $q - 1$ múltiplos escalares no nulos.

Para $k \in K^\times$, cualquier vector de la forma kv, define la misma recta que v, debido a que $kv \in \langle v \rangle$, luego se sigue que existen

$$n = \frac{q^k - 1}{q - 1}$$

rectas distintas en K^k.
Sean $\langle h_1 \rangle, ..., \langle h_n \rangle$ dichas rectas y sea $H \in \mathrm{Mat}(k \times n, K)$ la matriz cuyas columnas son exactamente los vectores h_j. Es decir, $H = (h_1 ... h_n)$.

El código C con matriz de control H, es llamado **código de Hamming**. De las n columnas de H, pueden elegirse k, tales que una base para K^k sea $B = (h_1, ..., h_k)$. Entonces el $\text{Rang}(H) = k$ y se tiene que $\dim_K(C) = n - k$, luego $|C| = q^{n-k}$.

Además, como cualquier par de columnas distintas son linealmente independientes, convenientemente podemos elegir tres columnas linealmente dependientes, y del teorema 1.1.17 resulta

$$\text{wt}(C) = \text{d}(C) = 3,$$

es decir, C puede corregir 1 error.

Verifiquemos ahora que C es perfecto, utilizando la igualdad que se enunció al comenzar la sección, C es perfecto si y sólo si $|C| = \frac{q^n}{\sum_{j=0}^{r} \binom{n}{j}(q-1)^j}$.

Entonces,

$$\begin{aligned} |C| &= \frac{q^n}{\sum_{j=0}^{1} \binom{n}{j}(q-1)^j} \\ &= \frac{q^n}{1 + n(q-1)} \\ &= \frac{q^n}{1 + \frac{q^k-1}{q-1}(q-1)} \\ &= \frac{q^n}{q^k}. \end{aligned}$$

Para denotar los códigos de Hamming usaremos $\text{Ham}_q(k)$.

1.3.2 Ejemplo. Para $q = 2$, $k = 3$ el código $\text{Ham}_2(3)$ es un $[7, 4]$-código binario de Hamming. Una matriz de control es

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

Observe que las columnas 3, 4 y 7 (de izquierda a derecha) son linealmente dependientes, entonces por teorema 1.1.17 la distancia mínima para el $\text{Ham}_2(3)$ es 3, luego es un $[7, 4, 3]$- código binario de Hamming.

1.4 Los códigos de Reed-Solomon

En el año de 1960 fueron presentados los códigos de Reed-Solomon, los cuales deben su nombre a sus creadores, Irving S. Reed y Gustave Solomon. Actualmente, estos códigos tienen muchas aplicaciones en áreas como la telefonía

móvil, en los CDs y sondas espaciales, por ejemplo la sonda Galileo enviada a Júpiter en 1989, la sonda Magallanes enviada a Venus ese mismo año o la sonda Ulises al Sol en 1990. Se destaca además el uso de los códigos de Reed-Solomon en las comunicaciones por satélite en la radiodifusion de video digital (DVB), en la transmisión digital de televisión ISDB-T, así como en los sistemas xDSL de comunicación por cable.

1.4.1 Definición. Sean $k, n \in \mathbb{N}$, con $1 \leq k \leq n \leq q$. El conjunto de todos los polinomios con coeficientes en K, de grado estrictamente menor que k, se notará con $K[x]_k$. Esto es,

$$K[x]_k := \{f \in K[x] \mid \text{grad}(f) < k\}.$$

Sea $A = \{a_1, ..., a_n\} \subseteq K$, con $a_i \neq a_j$, para $i \neq j$. Se define

$$C(A) := \{(f(a_1), ..., f(a_n)) \mid f \in K[x]_k\} \subseteq K^n.$$

De la definición del conjunto $C(A)$ se sigue fácilmente que $C(A) \leqslant K^n$. Este subespacio es llamado **código de Reed-Solomon** o **RS-código**.

En el siguiente teorema se verifican los parámetros de un código de Reed-Solomon, y se muestra además que este es un MDS-código (*Maximum Distance Separable*), es decir que alcanza la cota de Singleton.

1.4.2 Teorema. Sean $k, n \in \mathbb{N}$ con $1 \leq k \leq n \leq q$. Entonces $C(A)$ es un $[n, k, n-k+1]$-código sobre K.

Demostración. Recuerde cómo se definió el RS-código,

$$C(A) := \{(f(a_1), ..., f(a_n)) \mid f \in K[x]_k\} \subseteq K^n,$$

entonces claramente $C(A)$ tiene longitud n.

Por otra parte, considere la función

$$\alpha : K[x]_k \longrightarrow C(A)$$

definida por

$$\alpha(f) := (f(a_1), ..., f(a_n))$$

y veamos que α es un homomorfismo entre espacios vectoriales, en efecto, sean $f, g \in K[x]_k$ y $z \in K$

$$\begin{aligned}
\alpha(f+g) =& ((f+g)(a_1), ..., (f+g)(a_n)) \\
=& (f(a_1) + g(a_1), ..., f(a_n) + g(a_n)) \\
=& (f(a_1), ..., f(a_n)) + (g(a_1), ..., g(a_n)) \\
=& \alpha(f) + \alpha(g).
\end{aligned}$$

y también

$$\begin{aligned}\alpha(zf) =&(zf(a_1), ..., zf(a_n))\\ =&z(f(a_1), ..., f(a_n))\\ =&z\alpha(f).\end{aligned}$$

Note que si $b \in C(A)$, entonces existe $f \in K[x]_k$ tal que $b = (f(a_1), ..., f(a_n))$, con $a_j \in K$, luego $b = \alpha(f)$ lo que indica que α es un epimorfismo.

Demostamos ahora que α es inyectiva, si $f \in \ker(\alpha)$, entonces

$$\alpha(f) = (f(a_1), ..., f(a_n)) = (0, 0, ..., 0).$$

Como el grado de f es estrictamente menor que k y este a su vez es menor o igual que n, del álgebra se sigue que f tiene a lo más $k-1$ raíces distintas, por tanto la igualdad anterior se verifica para $f = 0$. Con esto hemos probado que α es un isomorfismo. Observe también que $B = (1, x, x^2, ..., x^{k-1})$ es una base para $K[x]_k$, luego

$$\dim_K K[x]_k = k = \dim_K C(A).$$

Calculemos ahora la distancia mínima, tomando cualesquiera par de elementos en $C(A)$, sean estos c_f y c_g, entonces por la invariancia bajo traslaciones y ser $C(A)$ un espacio vectorial, se tiene lo siguiente

$$\mathrm{d}(c_f, c_g) = \mathrm{d}(c_f - c_g, 0) = \mathrm{wt}(c_h)$$

con $c_h \in C(A)$, como grad $c_h < k$, entonces $\mathrm{wt}(c_h) \leq k-1$, si $\mathrm{d}(c_f, c_g) = t$, esto es, c_f y c_g sólo coinciden en $n-t$ posiciones, entonces el polinomio $c_f - c_g$ tiene $n-t$ raíces, luego tenemos que $n-t \leq k-1$, es decir

$$t \geq n - k + 1.$$

Entonces $n-k+1$ es una cota inferior para el conjunto distancias entre polinomios de $K[x]_k$, si tomamos la mayor de esas cotas como $\mathrm{d}(C(A))$, entonces $n-k+1 \leq \mathrm{d}(C(A))$. De esta manera, para el polinomio

$$f = \prod_{j=1}^{k-1}(x - a_j)$$

se verifica que $\mathrm{wt}(c_f) = n-k+1$, por tanto $\mathrm{d}(C(A)) = n-k+1$. Y concluimos que $C(A)$ es un $[n, k, n-k+1]$-código sobre K.□

1.4.3 Ejemplo. Construyamos un $[3,2]$-código ternario de Reed-Solomon.
Sea $A = \mathbb{F}_3$. Note que:

$$K[x]_2 := \{0, 1, 2, x, 2x, x+1, x+2, 2x+1, 2x+2\}.$$

Por lo tanto

$$\begin{aligned} C(A) =& \{(f(0), f(1), f(2)) \mid f \in K[x]_2\} \\ =& \{000, 111, 222, 012, 021, 120, 201, 102, 210\}. \end{aligned}$$

Observe que

$$\mathrm{d}(C(A)) = n - k + 1 = 3 - 2 + 1 = 2.$$

Otra forma de calcular o hallar los codewords de un RS-código, es a través de una matriz generadora. Como veremos en el siguiente teorema, la forma de esta es muy simple, es una matriz de Vandermonde.

1.4.4 Teorema. Sea $A = \{a_1, \ldots, a_n\} \subseteq K$, con $a_i \neq a_j$ para $i \neq j$ y $1 \leq k \leq n \leq q$. Entonces la matriz generadora de un $[n,k]$-código de Reed-Solomon está dada por la matriz de Vandermonde.

$$G = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & \vdots & & \vdots \\ a_1^{k-1} & a_2^{k-1} & \cdots & a_n^{k-1} \end{pmatrix}.$$

Demostración.

$$\begin{aligned} c_f \in C(A) \Leftrightarrow & \exists f \in K[x]_k \text{ tal que } c_f = (f(a_1), ..., f(a_n)) \\ \Leftrightarrow & \exists c_0, ..., c_{k-1} \in K \text{tales que } c_f = \left(\sum_{j=0}^{k-1} c_j a_1^j, ..., \sum_{j=0}^{k-1} c_j a_n^j \right) \\ \Leftrightarrow & c_f = (c_0, ..., c_{k-1})G \\ \Leftrightarrow & c_f \in K^k G. \end{aligned}$$

Finalmente del teorema 1.1.14 se tiene la afirmación.□

Para el ejemplo anterior, una matriz generadora es:

$$G = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \end{pmatrix}.$$

1.5 El código dual

Se define el código dual a partir de una forma bilineal no degenerada, utilizando la estructura del producto escalar euclidiano.

Sean K un cuerpo finito, $n \in \mathbb{N}$ y se define la forma

$$(\cdot \mid \cdot) : K^n \times K^n \longrightarrow K$$

mediante

$$(u \mid v) := \sum_{j=1}^{n} u_j v_j$$

con $u = (u_1, ..., u_n)$ y $v = (v_1, ..., v_n)$.

1.5.1 Lema. Sean $u, v, w \in K^n$ y $a, b \in K$. Entonces
(a) $(u + v \mid w) = (u \mid w) + (v \mid w)$.
(b) $(au \mid v) = a(u \mid v)$.
(c) $(\cdot \mid \cdot)$ es una forma bilineal simétrica, esto es, $(u \mid v) = (v \mid u)$.
(d) $(0 \mid v) = (v \mid 0) = 0$
(e) Si $(u \mid v) = 0$, para todo $v \in K^n$, entonces $u = 0$. Luego $(\cdot \mid \cdot)$ es una forma bilineal simétrica no degenerada.

Demostración. Sean $u = (u_1, ..., u_n)$, $v = (v_1, ..., v_n)$, $w = (w_1, ..., w_n)$ en K^n y $a, b \in K$.
(a)

$$\begin{aligned}(u + v \mid w) =& \sum_{j=1}^{n} (u_j + v_j) w_j \\ =& \sum_{j=1}^{n} u_j w_j + \sum_{j=1}^{n} v_j w_j \\ =& (u \mid w) + (v \mid w).\end{aligned}$$

(b) $(au \mid v) = \sum_{j=1}^{n} a u_j v_j = a \sum_{j=1}^{n} u_j v_j = a(u \mid v)$.
(c) $(u \mid v) = \sum_{j=1}^{n} u_j v_j = \sum_{j=1}^{n} v_j u_j = (v \mid u)$.
(d) $(0 \mid v) = \sum_{j=1}^{n} 0 v_j = \sum_{j=1}^{n} 0 = 0$.
(e) Sea e_j el j-ésimo vector de la base canónica de K^n. Entonces $0 = (u \mid e_j) = u_j$. Por tanto $u = 0$.
□

1.5.2 Definición. Sea C un $[n,k]$-código sobre un cuerpo finito K.
(a) El **código dual** de C, notado por $C^{\perp}$, se define como:

$$C^{\perp} := \{u \in K^n \mid (u \mid c) = 0, \forall c \in C\}$$

(b) C se denomina **auto-ortogonal**, si $C \subseteq C^{\perp}$.
(c) C se denomina **auto-dual**, si $C = C^{\perp}$.

Por medio de las propiedades vistas en el teorema anterior es fácil verificar que $C^{\perp}$ es siempre un espacio vectorial de K^n.

Ahora veremos la relación de parámetros entre un código y su código dual, así también se mostrará que una matriz generadora de C será una matriz de control para $C^{\perp}$ y viceversa, una matriz de control para C será una matriz generadora para $C^{\perp}$.

1.5.3 Teorema. Sea C un $[n,k]$-código sobre un cuerpo finito K, $|K| = q$. Entonces
(a) $C^{\perp}$ es un $[n, n-k]$-código sobre K.
(b) $(C^{\perp})^{\perp} = C$.
(c) G es una matriz generadora de C si y sólo si G es una matriz de control para $C^{\perp}$.
(d) H es una matriz de control de C si y sólo si H es una matriz generadora para $C^{\perp}$.
(e) Si $(I_k \mid A)$ es una matriz generadora de C (en forma estándar), entonces $(-A^t \mid I_{n-k})$ es una matriz generadora de $C^{\perp}$, por tanto es una matriz de control para C.
(f) Si C es auto-dual, entonces $n = 2k$. En particular, todo código auto-dual tiene longitud par.

Demostración.
(a) Sea G una matriz generadora de C, cuyas filas se denotan como

$$g_j = (g_{j1}, \ldots, g_{jn}), j = 1, \ldots, k.$$

Entonces

$$\begin{aligned} x \in C^{\perp} &\Leftrightarrow (x \mid c) = 0, \forall c \in C. \\ &\Leftrightarrow (x \mid v_j) = 0, \text{ para una base } B = (v_1, \cdots, v_k) \text{ de } C. \\ &\Leftrightarrow (x \mid g_j) = 0. \\ &\Leftrightarrow Gx^t = 0 \end{aligned}$$

Esto demuestra que G es una matriz de control para $C^{\perp}$, y del álgebra lineal se obtiene

$$n = \text{Rang}(G) + \dim_K \ker(G).$$

En consecuencia,

$$n = \text{Rang}(G) + \dim_K C^{\perp}.$$

Entonces $\dim_K C^{\perp} = n - k$.

(b) Si $x \in C$ y $v \in C^{\perp}$, entonces $(x \mid v_j) = 0$. Por tanto $x \in (C^{\perp})^{\perp}$, es decir $C \subseteq (C^{\perp})^{\perp}$. Y del inciso (a) se tiene

$$\dim_K (C^{\perp})^{\perp} = n - (n-k) = k = \dim_K C.$$

Entonces se tiene un conjunto contenido en otro, y los dos tienen la misma dimensión, con lo cual se concluye que son iguales, es decir $(C^{\perp})^{\perp} = C$.

(c) En la parte (a) se mostró que si G es una matriz generadora de C, entonces es una matriz de control para $C^{\perp}$. Ahora veamos la recíproca, es decir, si G es una matriz de control para $C^{\perp}$, entonces como $C^{\perp}$ es un $[n, n-k]$-código sobre K, se verifica que cualquier matriz generadora de $C^{\perp}$ tiene $n-k$ filas. Luego cualquier matriz de control de $C^{\perp}$ tendrá $n-(n-k) = k$ filas, sean estas filas notadas por

$$g_j = (g_{j1}, \ldots, g_{jn}), j = 1, \ldots, k.$$

Entonces $(x \mid g_j) = 0$, para todo $x \in C^{\perp}$ y todo $j = 1, \ldots, k$. es decir, $g_j \in (C^{\perp})^{\perp} = C$ para todo $j = 1, \ldots, k$. Como las filas de G son linealmente independientes y $\dim_K C = k$, con k el número de filas de G, se tiene que G es una matriz generadora de C.

(d) De los incisos (b) y (c) se tiene lo siguiente, H es matriz generadora de $C^{\perp}$ si y solo si H es matriz de control de $(C^{\perp})^{\perp} = C$.

(e) Para mostrar que $(-A^t \mid I_{n-k})$ es una matriz generadora de $C^{\perp}$, por tanto es una matriz de control para C, se verifica que

$$\begin{aligned}(-A^t \mid I_{n-k})(I_k \mid A)^t &= (-A^t \mid I_{n-k})\begin{pmatrix} I_k \\ A^t \end{pmatrix} \\ &= -A^t I_k + I_{n-k} A^t \\ &= 0.\end{aligned}$$

(f) Si C es auto-dual, entonces C y $C^{\perp}$ tienen la misma dimensión sobre K. Luego $k = n - k$, es decir, $n = 2k$.□

1.5.4 Definición. El código dual del código de Hamming se denomina **código simplex**, y se denota como $\mathrm{Sim}_q(k)$.

1.5.5 Lema. Sea K un cuerpo finito, con $|K| = q$.
(a) Si $0 \neq c \in \mathrm{Sim}_q k$, entonces $\mathrm{wt}(c) = q^{k-1}$. Es decir, todos los codewords no nulos del código simplex tienen el mismo peso.
(b) $\mathrm{Sim}_q(k)$ es un $[\frac{q^k-1}{q-1}, k, q^{k-1}]$-código sobre K.

Demostración. Sea H una matriz de control para $\mathrm{Ham}_q(k)$, con filas $f_1, \ldots, f_k$, entonces H es una matriz generadora para $\mathrm{Sim}_q(k)$.

Sea $0 \neq c = (c_1, \ldots, c_n) \in \mathrm{Sim}_q(k)$. Entonces $B = (f_1, \ldots, f_k)$ es una base para $\mathrm{Sim}_q(k)$. Por tanto

$$c = \sum_{j=1}^{k} a_j f_j = \sum_{j=1}^{k} a_j (f_{j1}, \ldots, f_{jn}), a_j \in K.$$

Sea $h_i := (f_{1i}, \ldots, f_{ki})$ la i-ésima columna de H, $a := (a_1, \ldots, a_k) \in K^k$ y se define el conjunto

$$U(a) := \{\ (b_1, \ldots, b_k)^t \mid b_j \in K,\ \sum_{j=1}^{k} a_j b_j = 0\ \} \subseteq K^k.$$

Esto es, $U(a) = \langle a \rangle^{\perp}$. Por tanto

$$\begin{aligned} \dim_K U(a) &= \dim_K \langle a \rangle^{\perp} \\ &= k - \dim_K \langle a \rangle \\ &= k - 1. \end{aligned}$$

Luego $U(a)$ tiene $\frac{q^{k-1}-1}{q-1}$ columnas h_i de H. Además

$$\begin{aligned} c_i = 0 &\Leftrightarrow \sum_{j=1}^{k} a_j f_{ji} = 0 \\ &\Leftrightarrow (f_{1i}, \ldots, f_{ki})^t \in U(a). \end{aligned}$$

Lo cual demuestra que hay $\frac{q^{k-1}-1}{q-1}$ ceros. Entonces

$$\begin{aligned} \mathrm{wt}(c) &= n - \frac{q^{k-1}-1}{q-1} \\ &= \frac{q^k - 1}{q-1} - \frac{q^{k-1}-1}{q-1} \\ &= q^{k-1}. \end{aligned}$$

Como es conocido, la distancia mínima es igual al peso mínimo, y dado que todos los pesos son iguales se tiene que $d(\mathrm{Sim}_q(k)) = q^{k-1}$.$\square$

Capítulo 2

Códigos de red

En este segundo capítulo, estudiamos los códigos de red y la codificación en red aleatoria. Esta última es una herramienta para la difusión de información en redes, la cual como en el caso clásico, también es susceptible a errores en la transmisión de paquetes causados por ruido o por interferencia intencional. Cabe anotar que en la más sencilla implementación un sólo error en un paquete recibido haría inservible toda la transmisión cuando el paquete adulterado se combina con otros paquetes recibidos para deducir el mensaje transmitido. También es posible que algunos paquetes insuficientes de alguna generación, alcancen el receptor destinado, razón por la cual el problema de deducir la información no pueda completarse.

2.1 Generalidades de la teoría de códigos de red

A diferencia de los códigos lineales clásicos donde los codewords son vectores de K^n, en la teoría de códigos de red el alfabeto de entrada y salida es tomado de la geometría proyectiva. Es decir, estos son conjuntos cuyos elementos son subespacios de K^n, donde K es como siempre el cuerpo finito $\mathbb{F}_q$.

En este trabajo se formula una teoría de códigos en el contexto de un modelo de transmisión de un canal de poca memoria para codificación en red aleatoria lineal, el cual captura tanto *errores*, es decir, paquetes recibidos erróneamente, como *borraduras*, paquetes recibidos con insuficiencia. La transmisión por medio de una red es una técnica que en lugar de limitarse a emitir los paquetes de información que se reciben, envía varios paquetes a través de los nodos de una red y los mezcla para la transmisión. En este contexto *mezclar* significa hacer combinaciones lineales de los paquetes recibidos. Esto puede ser utilizado para transmitir un mayor flujo de información.

La situación a modo general es la siguiente: simultáneamente el nodo T_1 envía el bit b_1 y el nodo T_2 envía el bit b_2. La idea es que los dos receptores R_1 y R_2 reciban ambos bits. El nodo intermedio I, es decir, un nodo entre el transmisor y el receptor, no puede mandar simultáneamente el bit b_1 o el bit b_2, entonces R_1 o R_2 reciben la información requerida con algún retraso. Lo anterior se ilustra en la figura 2.1

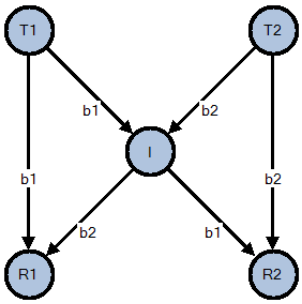

Figura 2.1: Envío de información a través de una red.

La codificación en red admite que los nodos intermedios pueden *mezclar* información entrante antes de enviarlos a una tasa de información mayor. En nuestra red el nodo I combina b_1 y b_2 y transmite b_1+b_2, y así R_1 y R_2 obtienen simultáneamente la información requerida, como se ilustra en la figura 2.2

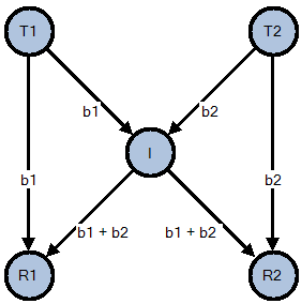

Figura 2.2: Envío por combinación de información.

Note que R_1 puede obtener b_2 de

$$b_1 + (b_1 + b_2) = b_2.$$

Este método tiene una gran ventaja sobre la decodificación convencional, porque se reduce notablemente la pérdida de tiempo.

2.2 El canal operador

Iniciamos la formulación del problema para el caso de un simple *unicast*, esto es, el envío de información desde un único emisor a un único receptor. Para entender la esencia de la codificación en red aleatoria recuerde que la comunicación entre transmisor y receptor ocurre en una serie de rondas o generaciones, durante cada generación, el transmisor inyecta en la red una serie de paquetes de longitud fija, cada uno de los cuales puede ser considerado como un vector fila de longitud N, es decir, un elemento de $\mathbb{F}_q^N$.

Estos paquetes se propagan por medio de la red, pasando posiblemente a través de nodos intermedios. Siempre que un nodo intermedio tenga la oportunidad de enviar un paquete, este crea aleatoriamente una combinación lineal sobre $\mathbb{F}_q$, de los paquetes disponibles y la transmite. Finalmente el receptor recoge tales paquetes generados aleatoriamente y trata de inferir los paquetes inyectados en la red. Aquí no hay suposición alguna de que la red opera sincrónicamente o que la red sea acíclica, es decir que el nodo inicial no coincida con el nodo final.

El conjunto de transmisiones exitosas de paquetes en una generación, induce un grafo dirigido conformado por el mismo conjunto de vértices de la red, en el cual los bordes o aristas denotan transmisiones exitosas de paquetes. La tasa de transmisión de información (paquetes por generación) entre el transmisor y el receptor está acotada superiormente por el min-cut entre estos nodos, esto es, el mínimo número de aristas borradas en el grafo, las cuales podrían causar corte o separación entre el emisor y receptor (este tipo de red es notada en inglés como network min-cut). Es conocido que la codificación lineal en red aleatoria en $\mathbb{F}_q$ es capaz de lograr una tasa de transmisión que alcanza la tasa min-cut, con una probabilidad cercana a uno cuando $q \to \infty$ (ver [9]).

Sea $\{p_1, \ldots, p_M\} \subseteq \mathbb{F}_q^N$ el conjunto de vectores inyectados. En caso que no se produzcan errores durante la transmisión, el receptor recibe los paquetes y_j, con $j \in \{1, \ldots, L\}$, donde cada y_j es formado de la siguiente manera:

$$y_j = \sum_{i=1}^{M} h_{ji} p_i,$$

con $h_{ji} \in \mathbb{F}_q$ elegidos aleatoriamente. Note que a priori el número L no está fijo, y que el receptor normalmente recoge tantos paquetes como le sea posible. No obstante como se señaló arriba, propiedades de la red tales como el min-cut entre el emisor y el receptor pueden influir en la distribución de los h_{ji}, y en algún punto no habría beneficio alguno de la información redundante adicional.

Debido a que el medio para transmitir información está expuesto a ruidos o alteraciones que puedan dañar o anular la información, es posible recibir datos erróneos, lo cual alteraría el número L de vectores recibidos, si escogemos para considerar la inyección de T paquetes erróneos, entonces el modelo anterior se amplía para incluir los paquetes de error e_k, con $k \in \{1, \ldots, T\}$ para dar

$$y_j = \sum_{i=1}^{M} h_{ji} p_i + \sum_{k=1}^{T} g_{jk} e_k,$$

donde nuevamente $g_{jk} \in \mathbb{F}_q$ y son escogidos aleatoriamente.

Notese que, dado que estos paquetes erróneos pueden inyectarse en cualquier lugar de la red, estos pueden causar la propagación grande del error. En particular, si $g_{j1} \neq 0$ para todo $j \in \{1, \ldots, L\}$, un simple paquete erróneo e_1 tiene el potencial para corromper cada uno de los paquetes recibidos.

En forma matricial, el modelo de transmisión descrito puede escribirse de la siguiente manera:

$$y = Hp + Ge, \tag{2.1}$$

donde $H \in \mathrm{Mat}(L \times M, \mathbb{F}_q)$, $G \in \mathrm{Mat}(L \times T, \mathbb{F}_q)$ son escogidas aleatoriamente, $p \in \mathrm{Mat}(M \times N, \mathbb{F}_q)$ es la matriz cuyas filas son los vectores transmitidos, $y \in \mathrm{Mat}(L \times N, \mathbb{F}_q)$ es la matriz cuyas filas son los vectores recibidos, y $e \in \mathrm{Mat}(T \times N, \mathbb{F}_q)$ cuyas filas son los vectores con error.

En este punto, dado que H es elegida aleatoriamente, podemos preguntarnos: ¿Qué propiedad de la sucesión de paquetes inyectados permanece invariante en el canal descrito por (2.1), incluida la posibilidad de ausencia de ruido, es decir, $e = 0$?

Dado que H es una matriz aleatoria, todo lo que se fija por el producto Hp es el espacio de filas de p. En efecto, en cuanto al receptor se refiere, cualquiera de los posibles conjuntos generadores para este espacio son equivalentes. Esto nos lleva por lo tanto, a considerar la transmisión de la información no a través de la escogencia de p, sino más bien por la elección del espacio vectorial generado por las filas de p.

Esta simple observación es el centro de los modelos de canales y de las estrategias de transmisión consideradas en este trabajo. En efecto, con relación

al espacio vectorial seleccionado por el transmisor, el único efecto nocivo que una multiplicación por H puede causar es que Hp tenga un rango menor que el de p, debido a, por ejemplo, borraduras o a un min-cut insuficiente, en cuyo caso Hp genera un subespacio generado por las filas de p, es decir, ahora nuestro objetivo será identificar p a partir de su generado, digamos

$$\widetilde{V} := \langle p_1, \ldots, p_M \rangle.$$

Esta es la razón por la cual ahora se consideran subespacios como elementos de los códigos de red.

Fijamos a continuación algunas notaciones que serán de gran importancia a lo largo del presente capítulo. Sea W un espacio vectorial N-dimensional sobre $\mathbb{F}_q$, fijo. Todos los paquetes enviados y recibidos son elementos de W, sin embargo se describe un modelo de transmisión en términos de subespacios de W generados por estos paquetes.

Sea $\mathcal{P}(W)$ el conjunto de todos los subespacios de W, usualmente denominado la geometría proyectiva de W. La dimensión de un elemento $V \in \mathcal{P}(W)$ se notará con $\dim_{\mathbb{F}_q}(V)$ o simplemente $\dim(V)$ si no hay lugar a confusión. La suma de dos subespacios $U, V \in \mathcal{P}(W)$ se nota y define así

$$U + V = \{u + v \mid u \in U, v \in V\}.$$

Equivalentemente $U + V$ es el subespacio más pequeño de W que contiene tanto a U como a V. Si $U \cap V = \{0\}$, entonces la suma anterior se convierte en una suma directa, la cual notamos como $U \oplus V$.

Del álgebra lineal es conocido que

$$\dim(U + V) = \dim(U) + \dim(V) - \dim(U \cap V)$$

y si $U \cap V = \{0\}$, entonces

$$\dim(U \oplus V) = \dim(U) + \dim(V).$$

Para cualquier par de subespacios U y V de W, se tiene que $V = (U \cap V) \oplus V'$, para algún V' isomorfo al espacio cociente $V/(U \cap V)$.

En este caso,

$$U + V = U + ((U \cap V) \oplus V') = U \oplus V'.$$

A continuación se define un operador estocástico o de probabilidad $\mathcal{S}_k$, llamado operador de borrado, de la siguiente manera: Para cada $k \in \mathbb{N}_0$

$$\mathcal{S}_k : \mathcal{P}(W) \longrightarrow \mathcal{P}(W)$$

donde para cada $V \in \mathcal{P}(W)$

$$\mathcal{S}_k(V) = \begin{cases} T \leqslant V, & \text{si } \dim(V) > k \ ; \\ V, & \text{otro caso.} \end{cases}$$

Note que si $\dim(V) > k$, entonces $\mathcal{S}_k(V)$ devuelve cualquier subespacio T de V con dimensión k. En otro caso $\mathcal{S}_k(V)$ devuelve V.

Para los propósitos de este trabajo la distribución de $\mathcal{S}_k(V)$ no es importante, por ejemplo, pudiese ser escogida de manera uniforme. Finalmente, dados dos subespacios U y V de W, siempre es posible expresar U de la forma

$$U = \mathcal{S}_k(V) \oplus E,$$

para algún $E \leqslant W$, asumiendo que $k = \dim(U \cap V)$ y que $\mathcal{S}_k(V) = U \cap V$.

La descripción anterior del canal operador como un modelo conciso de transmisión para codificación en red puede formalizarse en la siguiente definición.

2.2.1 Definición. Un canal operador asociado a un espacio ambiente W es un canal con alfabeto de entrada y salida $\mathcal{P}(W)$. Una entrada V y una salida U pueden relacionarse siempre en la forma

$$U = \mathcal{S}_k(V) \oplus E, \tag{2.2}$$

donde $k = \dim(U \cap V)$ y E es un espacio de error. Decimos que en el proceso de transformar V en U el canal comete ρ borraduras u omisiones, donde

$$\rho = \dim(V/(U \cap V)) = \dim(V) - k$$

y comete t errores, con

$$t = \dim(E).$$

Note que hemos elegido para modelar el espacio de errores E uno que tiene intersección trivial con el espacio transmitido V. En efecto, dado que $E \leqslant U$ y $E \cap (U \cap V) = \{0\}$, se tiene que

$$(E \cap U) \cap V = E \cap V = \{0\}.$$

En consecuencia la escogencia de E no es independiente de V. Sin embargo si tuviésemos que modelar el espacio recibido U de la forma

$$U = \mathcal{S}_k(V) + E$$

para un espacio de error arbitrario E, entonces dado que E puede descomponerse en la forma

$$E = (E \cap V) \oplus E'$$

obtendríamos que

$$U = \mathcal{S}_k(V) + ((E \cap V) \oplus E') = \mathcal{S}_{k'}(V) \oplus E',$$

para algún $k' \geq k$. En otras palabras, componentes de un espacio de errores que tienen intersección no trivial con el espacio transmitido V sólo sería útil, posiblemente, para disminuir el número de borraduras vistas por el receptor.

En resumen, un canal operador recibe un espacio vectorial y coloca un nuevo espacio con posibles borraduras, es decir, eliminación de información, supresión de vectores o parte de vectores en el espacio transmitido, o errores, esto es, adición de vectores al espacio transmitido.

2.3 La métrica de subespacios, códigos de dimensión constante y cotas superiores

La definición 2.2.1 presenta de manera concisa el efecto de la codificación en red aleatoria lineal en la presencia de redes con borraduras, variación del min-cut o errores en los paquetes. La idea ahora es construir códigos para este canal que estén en capacidad de corregir combinaciones de borraduras y errores. Antes de dar tal construcción necesitamos construir una métrica adecuada.

2.3.1 Una métrica sobre $\mathcal{P}(W)$

Sean W un espacio vectorial N-dimensional sobre $\mathbb{F}_q$ y $\mathcal{P}(W)$ el conjunto de todos los subespacios de W. Definamos una distancia entre subespacios de W, notada con d_S de la siguiente manera:

$$d_S : \mathcal{P}(W) \times \mathcal{P}(W) \longrightarrow \mathbb{N}_0$$

donde para $U, V \in \mathcal{P}(W)$

$$d_S(U, V) = \dim(U + V) - \dim(U \cap V). \tag{2.3}$$

Dado que $\dim(U + V) = \dim(U) + \dim(V) - \dim(U \cap V)$ se sigue que

$$\begin{aligned} d_S(U, V) &= \dim(U) + \dim(V) - 2\dim(U \cap V) \\ &= 2\dim(U + V) - \dim(U) - \dim(V) \end{aligned}$$

El siguiente lema es fundamental para describir el tipo de codificación que hace uso del canal operador descrito en la definición 2.2.1.

2.3.1 Lema. La función d_S anterior define una métrica sobre $\mathcal{P}(W)$. Es decir, para todo $U, V, X \in \mathcal{P}(W)$ se verifican
(a) $d_S(U,V) \geq 0$ y $d_S(U,V) = 0$ si y sólo si $U = V$.
(b) $d_S(U,V) = d_S(V,U)$.
(c) $d_S(U,V) \leq d_S(U,X) + d_S(X,V)$. (Desigualdad triangular)

Demostración. Las afirmaciones (a) y (b) son inmediatas. Nos concentramos en demostrar la desigualdad triangular.

$$\begin{aligned}
&\frac{1}{2}[d_S(U,V) - d_S(U,X) - d_S(X,V))] = \\
&\quad \frac{1}{2}[\dim(U) + \dim(V) - 2\dim(U \cap V) - \dim(U) - \dim(X) + 2\dim(U \cap X) \\
&\quad - \dim(X) - \dim(V) + 2\dim(X \cap V)] \\
&\quad = \frac{1}{2}[2\dim(U \cap X) + 2\dim(X \cap V) - 2\dim(U \cap V) - 2\dim(X)] \\
&\quad = \dim(U \cap X) + \dim(X \cap V) - \dim(U \cap V) - \dim(X) \\
&\quad = \underbrace{\dim(U \cap X + V \cap X) - \dim(X)} + \underbrace{\dim(U \cap X \cap V) - \dim(U \cap V)}.
\end{aligned}$$

Dado que $(U \cap X + V \cap X) \leqslant X$ y $(U \cap X \cap V) \leqslant (U \cap V)$ se tiene que

$$\frac{1}{2}[d_S(U,V) - d_S(U,X) - d_S(X,V))] \leq 0.$$

En consecuencia $d_S(U,V) \leq d_S(U,X) + d_S(X,V)$. $\square$

Si fijamos una base para W, entonces los elementos de W pueden verse como N-tuplas con entradas en $\mathbb{F}_q$. Tomemos ahora el producto interno usual entre vectores

$$(\cdot,\cdot) : W \times W \longrightarrow \mathbb{F}_q,$$

esto es, si $u = (u_1, \ldots, u_N)$ y $v = (v_1, \ldots, v_N)$, entonces

$$(u,v) = \sum_{i=1}^{N} u_i v_i.$$

Si U es un subespacio k-dimensional de W, entonces el subespacio ortogonal de U definido por

$$U^{\perp} := \{v \in W \mid (u,v) = 0, \forall u \in U\}$$

es un espacio vectorial sobre $\mathbb{F}_q$ de dimensión $N - k$.

Es bien conocido del álgebra lineal que si $U, V \leqslant W$, entonces
(a) $(U^\perp)^\perp = U$.
(b) $(U + V)^\perp = U^\perp \cap V^\perp$.
(c) $(U \cap V)^\perp = U^\perp + V^\perp$.

2.3.2 Teorema. Sean $U, V \in \mathcal{P}(W)$. Entonces $d_S(U^\perp, V^\perp) = d_S(U, V)$.

Demostración. Se sigue que

$$\begin{aligned} d_S(U^\perp, V^\perp) &= \dim(U^\perp + V^\perp) - \dim(U^\perp \cap V^\perp) \\ &= \dim((U \cap V)^\perp) - \dim((U + V)^\perp) \\ &= (N - \dim(U \cap V)) - (N - \dim(U + V)) \\ &= \dim(U + V) - \dim(U \cap V) \\ &= d_S(U, V). \end{aligned} \tag{2.4}$$

Así, entonces la distancia entre subespacios queda reflejada por la distancia entre los subespacios ortogonales correspondientes.

2.3.2 Los parámetros de los códigos de red

Sea nuevamente W un espacio vectorial N-dimensional sobre $\mathbb{F}_q$, el cual llamamos espacio ambiente para el canal operador. Un **código de red** para un canal operador con espacio ambiente W es simplemente un subconjunto no vacío de $\mathcal{P}(W)$. Es decir, un conjunto no vacío de subespacios de W.

El tamaño de un código $\mathcal{C}$, llamado también orden de $\mathcal{C}$ es denotado por $|\mathcal{C}|$. La distancia mínima de $\mathcal{C}$ se nota y define de la siguiente manera:

$$D_S(\mathcal{C}) := \text{mín}\{d_S(U, V) \mid U, V \in \mathcal{C}, U \neq V\}.$$

La dimensión máxima de $\mathcal{C}$ se define así:

$$l(\mathcal{C}) = \dim(\mathcal{C}) := \text{máx}\{\dim(V) \mid V \in \mathcal{C}\}.$$

Si la dimensión de cada codeword de $\mathcal{C}$ es la misma, entonces se dice que $\mathcal{C}$ es un código de **dimensión constante**.

Análogo como se definieron en el capítulo anterior los parámetros de un código lineal C, un código de red $\mathcal{C}$ para un canal operador con espacio ambiente N-dimensional W, se denomina un código de red de tipo

$$[N, l(\mathcal{C}), |\mathcal{C}|, D_S(\mathcal{C})].$$

El código complementario correspondiente a un código de red $\mathcal{C}$ se nota y define como se sigue:

$$\mathcal{C}^{\perp} = \{U^{\perp} \mid U \in \mathcal{C}\}.$$

Es decir, $\mathcal{C}^{\perp}$ es el conjunto de todos los subespacios ortogonales de los codewords de $\mathcal{C}$. Del teorema 2.3.2 se sigue inmediatamente que $D_S(\mathcal{C}^{\perp}) = D_S(\mathcal{C})$.

Ahora, si $\mathcal{C}$ es un código de dimensión constante con parámetros $[N, l, |\mathcal{C}|, D_S]$, entonces $\mathcal{C}^{\perp}$ es también un código de dimensión constante con parámetros $[N, N-l, |\mathcal{C}|, D_S]$.

Presentamos ahora una definición adecuada de tasa de transmisión, es decir para $\mathcal{C} \subseteq \mathcal{P}(W)$, un código del tipo $[N, l, |\mathcal{C}|, D_S]$ si se quiere transmitir un subespacio $V \in \mathcal{C}$, el transmisor requerirá inyectar hasta l vectores de una base de V en la red, lo cual corresponde a la transmisión de Nl símbolos q-arios, esto motiva la siguiente definición.

2.3.3 Definición. Sea $\mathcal{C} \subseteq \mathcal{P}(W)$ un código del tipo $[N, l, |\mathcal{C}|, D_S]$. Definimos el peso normalizado λ, la tasa R y la mínima distancia normalizada δ de $\mathcal{C}$ de la siguiente manera:

$$\lambda = \frac{l}{N}, \quad R = \frac{\log_q |\mathcal{C}|}{Nl}, \quad \text{y} \quad \delta = \frac{D_S}{2l}.$$

Los parámetros λ, R y δ son bastante naturales. El peso normalizado λ toma el papel del parámetro de peso equivalente a los códigos con peso constante. El rango de valores que puede tomar λ es $[0, 1]$. Para códigos de dimensión constante, así como en el caso de códigos de peso constante es interesante ver que el rango puede estar limitado a valores de $[0, \frac{1}{2}]$.

La definición de δ también se mueve en un rango de $[0, 1]$, en efecto, una distancia normalizada de 1 sólo puede ser obtenida por espacios que tienen intersección trivial. La tasa R de un código está restringida al intervalo $[0, 1]$, con una tasa de 1 sólo cuando $\lambda \to 0$.

El problema fundamental para la construcción de códigos de red para el canal operador de la definición 2.2.1, se convierte por lo tanto en la determinación de tuplas alcanzables $[\lambda, R, \delta]$, cuando la dimensión N del espacio ambiente se hace arbitrariamente grande. Tenga en cuenta que esta configuración puede carecer de realidad física, ya que asume que la red puede operar con paquetes arbitrariamente largos, por ello es necesario obtener resultados para un N finito, siempre que sea posible.

2.3.3 Corrección de errores y borraduras

En la teoría de códigos de red establecemos diferencia entre dos tipos de adulteración que pueden presentarse a la hora de transmitir información por la red, la borraduras y los errores. Las borraduras corresponden a eliminación de información debido a, por ejemplo, insuficiente min-cut en la red o una escogencia inadecuada de los coeficientes en la codificación lineal aleatoria de red. Por su parte los errores son inserción en la dimensión debido a errores o deliberada fraudulencia.

Un decodificador de distancia mínima para un código $\mathcal{C}$, es aquel que toma el espacio recibido U y devuelve un codeword $V \in \mathcal{C}$ que sea más cercano a U. Esto es, un codeword $V \in \mathcal{C}$ tal que para cualquier $V' \in \mathcal{C}$ se tenga

$$d_S(U, V) \leq d_S(U, V').$$

2.3.4 Definición. Sea $\mathcal{C} \subseteq \mathcal{P}(W)$ un código. Supongamos $V \in \mathcal{C}$ es transmitido a través de un canal operador y $U \in \mathcal{P}(W)$ es recibido. Se dice que el canal comete

$$t = \dim(U/U \cap V) \text{ errores.}$$
$$\rho = \dim(V/U \cap V) \text{ borraduras.}$$

La importancia de la distancia mínima $D_S(\mathcal{C})$ para un código $\mathcal{C} \subseteq \mathcal{P}(W)$ es evidenciada en el siguiente teorema, el cual proporciona la capacidad de un código $\mathcal{C}$ para combinar la corrección de errores y borraduras bajo la decodificación de distancia mínima.

Notación. Usaremos $(x)_+$ para denotar

$$(x)_+ := \text{máx}\{0, x\}.$$

2.3.5 Teorema. Sean $\mathcal{C} \subseteq \mathcal{P}(W)$ un código del tipo $[N, l, |\mathcal{C}|, D_S]$ y $V \in \mathcal{C}$ transmitido a través del canal operador con t errores y ρ borraduras, con $\rho = (l(\mathcal{C}) - k)_+$ el número máximo de borraduras inducidas por el canal. Si $U = \mathcal{S}_k(V) \oplus E$ es el codeword recibido, donde $\dim(E) = t$, y

$$2(t + \rho) < D_S(\mathcal{C}), \tag{2.5}$$

entonces el decodificador de mínima distancia puede obtener V dado que se recibió U.

Demostración. Sea $V' = \mathcal{S}_k(V) = U \cap V$. Note que

$$\begin{aligned} d_S(V, V') &= \dim V + \dim V' - 2\dim(V \cap V') \\ &= \dim V + \dim(U \cap V) - 2\dim(U \cap V) \\ &= \dim V - k \text{ (número de borraduras, ver definición 2.2.1)} \\ &\leq \rho. \end{aligned}$$

Y también

$$\begin{aligned} d_S(V', U) &= \dim V' + \dim U - 2\dim(V' \cap U) \\ &= \dim U - \dim(U \cap V) \\ &= \dim E \\ &= t. \end{aligned}$$

Usando la desigualdad triangular se tiene

$$d_S(V, U) \leq d_S(V, V') + d_S(V', U) \leq \rho + t. \quad (*)$$

Si $T \neq V$ es otro codeword en $\mathcal{C}$, entonces

$$D_S(\mathcal{C}) \leq d_S(V, T) \leq d_S(V, U) + d_S(U, T)$$

suponiendo la validez de $(*)$, se sigue que

$$d_S(U, T) \geq D_S(\mathcal{C}) - d_S(V, U) \geq D_S(\mathcal{C}) - (\rho + t).$$

Y por hipótesis, aplicando (2.5) en la última desigualdad se tiene

$$d_S(U, T) > 2(t + \rho) - (\rho + t) = t + \rho \geq d_S(V, U)$$

luego, el decodificador de mínima distancia puede obtener V de U. □

No es de extrañar, dada la simetría en esta configuración, entre borraduras y errores, que estos sean igualmente costosos al momento de decodificar. Esto contrasta aparentemente con la corrección tradicional de errores (donde borraduras cuestan menos que los errores), sin embargo esta diferencia no es más que un accidente de terminología. Un concepto tal vez más estrechamente relacionado (clásicamente) sería el de "inserción" y "eliminación".

Si pudiéramos asegurarnos que el operador proyección es elegido convenientemente (por ejemplo, una opción sería el operador $\mathcal{S}_N$, donde $N = \dim(W)$, el cual actúa como el operador identidad sobre cada subespacio de W) o que la red no produzca errores, es decir que el espacio $E = \{0\}$, entonces tendríamos el siguiente corolario.

2.3.6 Corolario. Sea W el espacio ambiente con $\dim W = N$. Asuma que se usa un código $\mathcal{C}$ para transmitir sobre un canal operador y $V \in \mathcal{C}$ es transmitido. Si

$$U = \mathcal{S}_N(V) \oplus E = V \oplus E$$

es recibido, y si $2t < D_S(\mathcal{C})$ donde $\dim E = t$, entonces un decodificador de distancia mínima para $\mathcal{C}$ reproduce exitosamente a V. Análogamente, si

$$U = \mathcal{S}_k(V) \oplus \{0\} = \mathcal{S}_k(V)$$

es recibido, y si $2\rho < D_S(\mathcal{C})$ donde $\rho = (l(\mathcal{C}) - k)_+$, entonces el decodificador de distancia mínima para $\mathcal{C}$ reproduce exitosamente a V.

En otras palabras, la primera parte del corolario establece que en ausencia de borraduras un decodificador de distancia mínima está en capacidad de corregir errores hasta la dimensión

$$t \leq \left\lfloor \frac{D_S(\mathcal{C}) - 1}{2} \right\rfloor.$$

Similar como sucede en la teoría clásica de códigos correctores.

2.3.4 Códigos con dimensión constante

En el contexto de la codificación de red, es natural considerar códigos en los cuales todos los codewords tengan la misma dimensión. Ya que el conocimiento de la dimensión del codeword puede ser explotada por el decodificador para iniciar el proceso de decodificación. Los códigos de dimensión constante son similares a los códigos de peso constante, como lo es por ejemplo el código Simplex.

Como se señaló anteriormente, cuando consideramos códigos de dimensión constante, podemos limitarnos a códigos del tipo

$$[N, l, |\mathcal{C}|, D_S]$$

con $l \leq N - l$, dado que un código $\mathcal{C}$ del tipo $[N, l, |\mathcal{C}|, D_S]$ con $l > N - l$ puede ser sustituido por su código complementario $\mathcal{C}^{\perp}$, manteniendo al mismo tiempo todas las propiedades de distancia (por lo tanto manteniendo toda la capacidad para corregir errores y borraduras).

2.3.7 Definición. Sea W el espacio ambiente con $\dim W = N$. Denotemos con $\mathcal{P}(W, l)$ el conjunto de todos los subespacios de W de dimensión constante l. Este conjunto es conocido como la l-**Grassmanniana**. Esto es,

$$\mathcal{P}(W, l) = \{V \mid V \in \mathcal{P}(W), \dim(V) = l\}$$

El grafo de Grassmann $G(W, l)$ tiene como conjunto de vértices a $\mathcal{P}(W, l)$ donde dos vértices U y V son adyacentes si y sólo si $d_S(U, V) = 2$.

Asumiremos que un codeword $V \in \mathcal{C}$ fue enviado. En esta situación, un receptor podrá recolectar paquetes hasta que estos paquetes (vectores) generen un espacio de dimensión l.

2.3.8 Observaciones. Sea W el espacio ambiente con $\dim W = N$.

(a) Si $\mathcal{C} \subseteq \mathcal{P}(W, l)$, entonces para todo $U, V \in \mathcal{C}$ se verifica que $2 \mid d_S(U, V)$. En efecto,

$$\begin{aligned} d_S(U, V) &= \dim U + \dim V - 2\dim(U \cap V) \\ &= l + l - 2\dim(U \cap V) \\ &= 2l - 2\dim(U \cap V)). \end{aligned}$$

(b) Si $\mathcal{C} \subseteq \mathcal{P}(W, l)$, entonces de ($a$) se sigue que

- $d_S(\mathcal{C}) \leq 2l$ ó
- $d_S(\mathcal{C}) = 2l$ si y solo si $\dim(U \cap V) = \{0\}$.

2.3.5 Algunos ejemplos de códigos de red

Concluimos esta sección con la construcción de dos ejemplos de códigos de dimensión constante.

2.3.9 Ejemplo. Sea $W = \mathbb{F}_q^N$. Considere el conjunto $\mathcal{C} \subseteq \mathcal{P}(W, l)$ de subespacios U_i, $i = 1, 2, \ldots, |\mathcal{C}|$ con matriz generadora

$$G(U_i) = (I_l \mid A_i),$$

donde I_l es la matriz identidad de tamaño $l \times l$ con entradas en $\mathbb{F}_q$ y las A_i recorren el conjunto $\mathrm{Mat}(l \times (N - l), \mathbb{F}_q)$. Es fácil ver que cada matriz $G(U_i)$ genera espacios diferentes, cuyas intersecciones son subespacios de dimensión a lo más $l - 1$ y que en consecuencia la distancia mínima de $\mathcal{C}$ es

$$2l - 2(l - 1) = 2.$$

Este es un código de dimensión constante de tipo

$$[N, l, l(N - l), 2],$$

con peso normalizado $\lambda = \frac{l}{N}$, tasa $R = 1 - \lambda$ y distancia normalizada $\delta = \frac{1}{\lambda N}$.

Este primer ejemplo corresponde a un código trivial que no ofrece protección contra errores en lo absoluto. Este código no es óptimo para una distancia dada $D_S(\mathcal{C}) = 2$, como puede verse en el siguiente ejemplo.

2.3.10 Ejemplo. Sea nuevamente $W = \mathbb{F}_q^N$. Sea $\mathcal{C}_1 = \mathcal{P}(W, l)$ código de dimensión constante de tipo

$$[N, l, \begin{bmatrix} N \\ l \end{bmatrix}_q, 2],$$

donde $\begin{bmatrix} N \\ l \end{bmatrix}_q$ es el q-ésimo coeficiente de Gauss que veremos en la próxima sección. Sea ahora $\mathcal{C}_2$ definido de la siguiente manera:

$$\mathcal{C}_2 = \bigcup_{i=1}^{l} \mathcal{P}(W, i),$$

(note que $\mathcal{C}_2$ ya no es un código de dimensión constante) $\mathcal{C}_2$ es un código más grande que $\mathcal{C}_1$ (aunque con $D_S(\mathcal{C}_2) = 1$) que puede ser utilizado para la codificación lineal de red de $\mathcal{C}$ y $\mathcal{C}_1$. Sin embargo, a diferencia de $\mathcal{C}_1$, el receptor debe ser capaz de determinar en qué momento la transmisión del código es completa. Esta información está implícita en $\mathcal{C}$ y $\mathcal{C}_1$ dado que la dimensión del espacio transmitido es fijada de antemano.

2.3.11 Teorema. Si $\mathcal{C} \subseteq \mathcal{P}(W, l)$ y $D_S(\mathcal{C}) = 2l$, entonces $|\mathcal{C}| \leq \dfrac{q^N - 1}{q^l - 1}$.
En particular, si se cumple la igualdad $|\mathcal{C}| = \dfrac{q^N - 1}{q^l - 1}$, entonces $l \mid N$.

Demostración. Si $\mathcal{C} = \{V_i \mid i = 1, 2, ..., r\}$ entonces

$$\bigcup_{i=1}^{r} V_i^{\times} \subseteq W^{\times}$$

donde $V_i^{\times} = V_i \backslash \{0\}$ y $W^{\times} = W \backslash \{0\}$. Por lo tanto $r(q^l - 1) \leq q^N - 1$, de donde se obtiene

$$|\mathcal{C}| \leq \frac{q^N - 1}{q^l - 1}.$$

Ahora, si $|\mathcal{C}| = \dfrac{q^N - 1}{q^l - 1} \in \mathbb{N}$, entonces $l \mid N$. $\square$

2.3.12 Ejemplo. (Código de extensión.) Sea $l \mid N$. Entonces a partir de un cuerpo $W = \mathbb{F}_{q^N}$ construimos un subcuerpo $L = \mathbb{F}_{q^l}$, esto es W es una extensión de L y notamos

$$L = \mathbb{F}_{q^l} \leqslant E = \mathbb{F}_{q^N} = W.$$

Por tanto, como grupos se tiene que

$$L^{\times} = \mathbb{F}_{q^l}^{\times} \leqslant E^{\times} = \mathbb{F}_{q^N}^{\times}.$$

Ahora podemos hacer una partición en clases laterales disyuntas por medio de un transversal T del subgrupo $L^{\times}$ sobre el grupo $E^{\times}$. Es decir, sean $T = \{a_1, ..., a_r\}$ y $E^{\times} = \bigcup_{i=1}^{r} a_i L^{\times}$ donde $r = \dfrac{q^N - 1}{q^l - 1}$.

Ahora se puede verificar que $V_i = a_i L^{\times} \cup \{0\}$ es un espacio vectorial de dimensión l sobre el cuerpo $\mathbb{K} = \mathbb{F}_q$ y $V_i \cap V_j = \{0\}$ para $i \neq j$, luego

$$\mathcal{C} = \{V_i \mid i = 1, 2, ..., r\} \subseteq \mathcal{P}(W, l),$$

$D_S(\mathcal{C}) = 2l$ y $|\mathcal{C}| = \dfrac{q^N - 1}{q^l - 1}$.

2.4 Algunas cotas superiores

2.4.1 El q-ésimo coeficiente de Gauss

Iniciamos esta sección introduciendo algunas notaciones que serán de gran importancia para el empaquetamiento en $\mathcal{P}(W, l)$, donde $W = \mathbb{F}_q^N$. El q-ésimo coeficiente de Gauss, el cual por simplicidad sólo llamamos el coeficiente de Gauss es análogo al coeficiente binomial. Este es definido para los enteros no negativos l y n con $l \leq n$ por

$$\begin{bmatrix} n \\ l \end{bmatrix}_q := \frac{(q^n - 1)(q^{n-1} - 1) \dots (q^{n-(l-1)} - 1)}{(q^l - 1)(q^{l-1} - 1) \dots (q - 1)} = \prod_{i=0}^{l-1} \frac{q^{n-i} - 1}{q^{l-i} - 1}.$$

para el caso en que $l = 0$, entonces el coeficiente se interpreta como 1.

Es bien conocido que $\begin{bmatrix} N \\ l \end{bmatrix}_q$ suministra el número de subespacios distintos de dimensión l que tiene un espacio vectorial de dimensión N sobre $\mathbb{F}_q$ (Ver [13]. Cap 4).

Para $q > 1$, el comportamiento asintótico de $\begin{bmatrix} N \\ l \end{bmatrix}_q$ se presenta en el siguiente lema.

2.4.1 Lema. El coeficiente de Gauss $\begin{bmatrix} n \\ l \end{bmatrix}_q$ satisface

$$q^{l(n-l)} < \begin{bmatrix} n \\ l \end{bmatrix}_q < 4q^{l(n-l)}$$

para $0 < l < n$.

Demostración. La cantidad $q^{l(n-l)}$ es el número de subespacios l-dimensionales de $\mathbb{F}_q^n$ cuyos elementos son generados por las filas de una matriz de la forma $(I \mid A)$, donde I es la matriz identidad de tamaño $l \times l$ y A es una matriz arbitraria de $l \times (n-l)$ con entradas en $\mathbb{F}_q$ (note que este es el número de codewords en el código $\mathcal{C}$ del ejemplo 2.3.9, tomando $n = N$). Como $l > 0$, este conjunto no contiene todos los subespacios l- dimensionales de $\mathbb{F}_q^n$, por lo cual se tiene el lado izquierdo de la desigualdad.

Para el lado derecho de la desigualdad observe que $\begin{bmatrix} n \\ l \end{bmatrix}_q$ puede ser escrito como se sigue:

$$\begin{aligned}
\begin{bmatrix} n \\ l \end{bmatrix}_q =& \frac{(q^n-1)(q^{n-1}-1)\dots(q^{n-l+1}-1)}{(q^l-1)(q^{l-1}-1)\dots(q-1)} \\
=& \frac{q^n(1-q^{-n})q^{n-1}(1-q^{-n+1})\dots q^{n-l+1}(1-q^{-n+l-1})}{q^l(1-q^{-l})q^{l-1}(1-q^{-l+1})\dots q(1-q^{-1})} \\
=& \frac{q^{l(n-l)}(1-q^{-n})(1-q^{-n+1})\dots(1-q^{-n+l-1})}{(1-q^{-l})(1-q^{-l+1})\dots(1-q^{-1})} \\
<& q^{l(n-l)} \frac{1}{(1-q^{-l})(1-q^{-l+1})\dots(1-q^{-1})} \\
<& q^{l(n-l)} \prod_{j=1}^{\infty} \frac{1}{1-q^{-j}}.
\end{aligned}$$

La función $f(x) = \prod_{j=1}^{\infty} \frac{1}{1-x^j}$ genera la función partición de enteros, [ver [13]. Cap 15] la cual es creciente en x. Como nos interesa el caso $f(\frac{1}{q})$ para $q \geq 2$, tenemos que

$$\prod_{j=1}^{\infty} \frac{1}{1-q^{-j}} \leq \prod_{j=1}^{\infty} \frac{1}{1-2^{-j}} \leq \frac{1}{Q_0} < 4$$

donde $Q_0 = 0,288788095$ es una constante de probabilidad combinatoria [2]. □

Algunas propiedades referentes al coeficiente gaussiano las notamos a continuación:

(a) $\begin{bmatrix} n \\ l \end{bmatrix}_q = \begin{bmatrix} n \\ n-l \end{bmatrix}_q$. En particular $\begin{bmatrix} n \\ 0 \end{bmatrix}_q = \begin{bmatrix} n \\ n \end{bmatrix}_q = 1$.

(b) $\begin{bmatrix} n \\ 1 \end{bmatrix}_q = \begin{bmatrix} n \\ n-1 \end{bmatrix}_q = 1 + \ldots + q^{n-1}$ con $n \geq 1$.

(c) $\begin{bmatrix} n \\ l \end{bmatrix}_q = q^l \begin{bmatrix} n-1 \\ l \end{bmatrix}_q + \begin{bmatrix} n-1 \\ l-1 \end{bmatrix}_q$.

(d) $\begin{bmatrix} n \\ l \end{bmatrix}_q = \begin{bmatrix} n-1 \\ l \end{bmatrix}_q + q^{n-1} \begin{bmatrix} n-1 \\ l-1 \end{bmatrix}_q$.

2.4.2 Definición. Sean W un espacio vectorial de dimensión N y $V \in \mathcal{P}(W,l)$. La esfera $S(V,l,t)$ de radio t y centro en V se define de la siguiente manera:

$$S(V,l,t) = \{U \in \mathcal{P}(W,l) \mid d_S(U,V) \leq 2t\}.$$

Observe que se prefirió definir el radio en términos de la distancia del grafo en el grafo de Grassmann. El radio por lo tanto puede tomar cualquier valor entero no negativo.

2.4.3 Teorema. El número de espacios en una esfera $S(V,l,t)$ no depende de su centro V, y además cumple con la siguiente igualdad

$$|S(V,l,t)| = \sum_{i=0}^{t} q^{i^2} \begin{bmatrix} l \\ i \end{bmatrix} \begin{bmatrix} N-l \\ i \end{bmatrix},$$

para $t \leq l$.

Demostración. Dado que $\mathcal{P}(W,l)$ constituye un grafo de distancia regular, es decir, un grafo donde cada vértice tiene el mismo grado o número de aristas adyacentes, (ver [3]), se tiene que $|S(V,l,t)|$ es independiente de V.

Damos ahora una expresión para el número de subespacios U que intersecan a V en un subespacio de dimensión $l-i$. Podemos elegir los subespacios intersección con dimensión $l-i$ en $\begin{bmatrix} l \\ i \end{bmatrix} = \begin{bmatrix} l \\ l-i \end{bmatrix}$ formas.

Una vez hecho esto, podemos completar el subespacio en

$$\frac{(q^N - q^l)(q^N - q^{l+1}) \dots (q^N - q^{l+i-1})}{(q^l - q^{l-i})(q^l - q^{l-i+1}) \dots (q^l - q^{l-1})} = q^{i^2} \frac{(q^{N-l}-1)(q^{N-l-1}-1) \dots (q^{N-l-i+1}-1)}{(q^i-1)(q^{i-1}-1) \dots (q-1)} = q^{i^2} \begin{bmatrix} N-l \\ i \end{bmatrix}$$

maneras. Luego, la cardinalidad de una capa de espacios a una distancia $2i$ de V es igual a

$$q^{i^2} \begin{bmatrix} N-l \\ i \end{bmatrix} \begin{bmatrix} l \\ i \end{bmatrix}.$$

Sumando las cardinalidades de las distintas capas se tiene la afirmación. □

Note que del teorema 2.3.2 se obtiene $|S(V,l,t)| = |S(V,N-l,t)|$.

2.4.2 Cotas de empaquetamiento esférico y de cobertura esférica

Ahora podemos establecer cotas para el ampaquetamiento esférico y cobertura esférica de la siguiente manera

2.4.4 Teorema. Sea $\mathcal{C} \subseteq \mathcal{P}(W,l)$ con $D_S(\mathcal{C}) \geq 2t$ y sea $s = \left\lfloor \frac{t-1}{2} \right\rfloor$. Entonces

$$|\mathcal{C}| \leq \frac{|\mathcal{P}(W,l)|}{|S(V,l,s)|} = \frac{\begin{bmatrix} N \\ l \end{bmatrix}_q}{|S(V,l,s)|} < \frac{\begin{bmatrix} N \\ l \end{bmatrix}_q}{q^{s^2} \begin{bmatrix} l \\ s \end{bmatrix}_q \begin{bmatrix} N-l \\ s \end{bmatrix}_q} < 4q^{(l-s)(N-s-l)}.$$

Por otro lado, existe un código $\mathcal{C}'$ con $D_S(\mathcal{C}') \geq 2t$ tal que $|\mathcal{C}'|$ está acotado inferiormente por

$$\begin{aligned} |\mathcal{C}'| \geq \frac{|\mathcal{P}(W,l)|}{|S(V,l,t-1)|} = \frac{\begin{bmatrix} N \\ l \end{bmatrix}_q}{|S(V,l,t-1)|} &> \frac{\begin{bmatrix} N \\ l \end{bmatrix}_q}{(t-1)q^{(t-1)^2} \begin{bmatrix} l \\ t \end{bmatrix}_q \begin{bmatrix} N-l \\ t-1 \end{bmatrix}_q} \\ &> \frac{1}{16t} q^{(l-t+1)(N-t-l+1)}. \end{aligned}$$

Demostración. Teniendo en cuenta la expresión para el número de elementos de una esfera en $\mathcal{P}(W,l)$, las cotas superiores e inferiores son exactamente las cotas conocidas para empaquetamiento y cubrimiento esféricos para códigos en grafos con distancia regular.□

Nuevamente como consecuencia del teorema 2.3.2, para $U, V \in \mathcal{C}$, las cotas del teorema anterior son simétricas en un espacio de dimensión l y su espacio complementario de dimensión $N-l$.

A continuación obtenemos una cota superior tipo Singleton para paquetes en el grafo de Grassmann.

2.4.3 La cota de Singleton

Comenzamos definiendo una adecuada operación de perforación de un código. Supongamos que $\mathcal{C} \subseteq \mathcal{P}(W,l)$ donde $\dim W = N$. Sea W' el hiperplano de W, esto es $W' \leqslant W$ y $\dim W' = N-1$.

Un código perforado $\mathcal{C}'$ es obtenido a partir de $\mathcal{C}$, mediante la sustitución de cada espacio $V \in \mathcal{C}$, por $V' = \mathcal{S}_{l-1}(V \cap W')$, donde $\mathcal{S}_{l-1}$ denota el operador de borrado definido anteriormente.

En otras palabras V es reemplazado por $V \cap W'$, si $\dim V \cap W' = l - 1$; en otro caso V se sustituye por algún subespacio de V que tenga dimensión $l-1$.

Aunque esta operación de perforación no suministra en general un único código, denotamos cualquiera de los códigos perforados resultantes por $\mathcal{C}|_{W'}$.

2.4.5 Teorema. Si $\mathcal{C} \subseteq \mathcal{P}(W, l)$ es un código de tipo

$$[N, l, |\mathcal{C}|, D_S]$$

con $D_S > 2$ y W' es un hiperplano de W, entonces $\mathcal{C}' := \mathcal{C}|_{W'}$ es un código de tipo $[N-1, l-1, |\mathcal{C}|, D'_S]$ con $D'_S \geq D_S - 2$.

Demostración. Sólo resta probar la cardinalidad de $\mathcal{C}'$ y su distancia mínima, los otros parámetros se obtienen fácilmente de la definición.

Verifiquemos primero que $D'_S \geq D_S - 2$.

Sean $U, V \in \mathcal{C}$ con $U \neq V$. Supongamos que

$$U' = \mathcal{S}_{l-1}(U \cap W') \quad \text{y} \quad V' = \mathcal{S}_{l-1}(V \cap W').$$

son los correspondientes codewords en $\mathcal{C}'$.

Como $U' \subseteq U$ y $V' \subseteq V$, entonces $U' \cap V' \subseteq U \cap V$, luego

$$2\dim(U' \cap V') \leq 2\dim(U \cap V) \leq 2l - D_S,$$

la última desigualdad se obtiene de

$$d_S(U, V) = 2l - 2\dim(U \cap V) \geq D_S.$$

Ahora en $\mathcal{C}'$ tenemos:

$$\begin{aligned} d_S(U', V') &= \dim(U') + \dim(V') - 2\dim(U' \cap V') \\ &= 2(l-1) - 2\dim(U' \cap V') \\ &\geq 2(l-1) - (2l - D_S) \\ &= D_S - 2. \end{aligned}$$

Ahora, dado que $D_S > 2$, se verifica que $d_S(U', V') > 0$, así $U' \neq V'$ (con U' y V' definidos a partir de U y V respectivamente), esto demuestra que $\mathcal{C}'$ tiene tantos codewords como $\mathcal{C}$. $\square$

Ahora podemos presentar la cota de Singleton.

2.4.6 Teorema. (Cota de Singleton)
Sea $\mathcal{C} \subseteq \mathcal{P}(W, l)$ de tipo $[N, l, |\mathcal{C}|, D_S]$. Entonces

$$|\mathcal{C}| \leq \begin{bmatrix} N - (D_S - 2)/2 \\ \text{máx}\{l, N - l\} \end{bmatrix}_q .$$

Demostración. Si $\mathcal{C}$ es perforado $(D_S - 2)/2$ veces, entonces obtenemos un código $\mathcal{C}'$ de tipo

$$[N - (D_S - 2)/2, l - (D_S - 2)/2, |\mathcal{C}|, D'_S]$$

esto es, cada codeword de $\mathcal{C}'$ tiene dimensión $l - (D_S - 2)/2$ y $D'_S \geq 2$. Note que la distancia mínima se obtiene fácilmente del teorema anterior, en efecto,

$$\begin{aligned} d_S(U', V') =& \dim(U') + \dim(V') - 2\dim(U' \cap V') \\ =& 2(l - (D_S - 2)/2) - 2\dim(U' \cap V') \\ =& 2l - D_S + 2 - 2\dim(U' \cap V') \\ \geq& 2l - D_S + 2 - (2l - D_S) \\ =& 2. \end{aligned}$$

Tal código no puede tener más codewords que la correspondiente Grassmanniana, la cual tiene a elementos, donde:

$$|\mathcal{C}| = |\mathcal{C}'| \leq |\mathcal{P}(W')| = \begin{bmatrix} N - (D_S - 2)/2 \\ l - (D_S - 2)/2 \end{bmatrix}_q = \begin{bmatrix} N - (D_S - 2)/2 \\ N - l \end{bmatrix}_q = a$$

Aplicando el mismo argumento a $\mathcal{C}^{\perp}$ se tiene la cota superior

$$b = \begin{bmatrix} N - (D_S - 2)/2 \\ l \end{bmatrix}_q .$$

Ahora, $a < b$ si y solo si $l < N - l$, con lo cual tenemos

$$|\mathcal{C}| \leq \begin{bmatrix} N - (D_S - 2)/2 \\ \text{máx}\{l, N - l\} \end{bmatrix}_q .$$

□

2.5 Construcción de un código tipo Reed-Solomon

Regresamos al problema de construir un código que esté en capacidad de corregir errores y borraduras en el espacio de salida de un canal operador definido anteriormente.

La construcción de nuestro código es equivalente a la citada por Wang, Xing y Safavi-Naini [14] en el contexto de los códigos lineales de autenticación, que a su vez pueden ser considerados como una aplicación de la construcción de Gabidulin del máximo rango [4]. (La conexión entre los códigos de dimensión constante y códigos con la métrica del rango es estudiada en detalle en [11].)

2.5.1 Polinomios Linealizados

Sea $\mathbb{F}_q$ un cuerpo finito y $\mathbb{F}_{q^m}$ una extensión de cuerpos.

Un polinomio $L(x)$ se denomina polinomio linealizado sobre $\mathbb{F}_{q^m}$ si tiene la forma

$$L(x) = \sum_{i=0}^{d} a_i x^{q^i} \tag{2.6}$$

con coeficientes $a_i \in \mathbb{F}_{q^m}$, $0 \leq i \leq d$.

Si $a_i = 0$ para cualquier $i \in \{0, \ldots, d\}$, se define $L(x)$ como el polinomio cero y lo escribimos $L(x) \equiv 0$.

En general, se tiene

$$L_1(x) \equiv L_2(x), \text{ si } \; L_1(x) - L_2(x) \equiv 0.$$

Sin lugar a confusión sustituimos x^{q^i} por $x^{[i]}$, teniendo fijo a q. Luego bajo esta notación, un polinomio linealizado sobre $\mathbb{F}_{q^m}$ puede ser escrito como

$$L(x) = \sum_{i=0}^{d} a_i x^{[i]}.$$

Algunas de las propiedades de los polinomios linealizados se presentan a continuación.

Si $L_1(x)$ y $L_2(x)$ son polinomios linealizados sobre $\mathbb{F}_{q^m}$, entonces su combinación lineal

$$\alpha_1 L_1(x) + \alpha_2 L_2(x),$$

para todo $\alpha_1, \alpha_2 \in \mathbb{F}_{q^m}$, también es un polinomio linealizado. En efecto, supongamos que $L_1(x) = \sum_{i=0}^{d} a_i x^{[i]}$ y $L_2(x) = \sum_{i=0}^{t} b_i x^{[i]}$. Entonces

$$\alpha_1 L_1(x) + \alpha_2 L_2(x) = \sum_{i=0}^{d} \alpha_1 a_i x^{[i]} + \sum_{i=0}^{t} \alpha_2 b_i x^{[i]} = \sum_{i=0}^{r} h_i x^{[i]}.$$

Con h_i adecuado.

El producto usual de polinomios linealizados no es en general un polinomio linealizado, sin embargo la composición $L_1 \circ L_2$, escrita usualmente como $L_1(x) \otimes L_2(x)$, de dos polinomios linealizados sobre $\mathbb{F}_{q^m}$ es un polinomio linealizado. Note además que esta operación no es conmutativa, esto es

$$L_1(x) \otimes L_2(x) \neq L_2(x) \otimes L_1(x)$$

Explícitamente, para calcular la composición de polinomios linealizados

$$L_1(x) = \sum_{i \geq 0} a_i x^{[i]} \quad \text{y} \quad L_2(x) = \sum_{j \geq 0} b_j x^{[j]}$$

tenemos

$$\begin{aligned} L_1(x) \otimes L_2(x) &= L_1(L_2(x)) \\ &= \sum_{i \geq 0} a_i (L_2(x))^{[i]} \\ &= \sum_{i \geq 0} a_i \left(\sum_{j \geq 0} b_j x^{[j]} \right)^{[i]} \\ &= \sum_{i \geq 0} \sum_{j \geq 0} a_i b_j^{[i]} x^{[j+i]} \\ &= \sum_{k \geq 0} c_k x^{[k]}, \end{aligned}$$

donde

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}^{[i]}.$$

Por lo tanto, los coeficientes de $L_1(x) \otimes L_2(x)$ se obtienen de $L_1(x)$ y $L_2(x)$ por medio de una operación de convolución modificada.

2.5.1 Observación. Si notamos el grado de $L_1(x)$ y el grado de $L_2(x)$ respectivamente con $\text{grad}(L_1(x))$ y $\text{grad}(L_2(x))$, entonces si

$$\text{grad}(L_1(x)) = q^{d_1} \quad \text{y } \text{grad}(L_2(x)) = q^{d_2}$$

se afirma que

$$\text{grad}(L_1(x) \otimes L_2(x)) = \text{grad}(L_2(x) \otimes L_1(x)) = q^{d_1 + d_2}.$$

Bajo estas condiciones, afirmamos que con las operaciones de suma + y composición $\otimes$, el conjunto de los polinomios linealizados sobre $\mathbb{F}_{q^m}$ forman un anillo no conmutativo con elemento identidad.

Aunque este anillo no es conmutativo, tiene muchas de las propiedades de un dominio entero euclidiano, incluyendo por ejemplo, la no existencia de divisores de cero. El grado de un elemento no nulo forma una norma natural.

Existen también dos algoritmos de la división: la división a izquierda y división a derecha, es decir dados dos polinomios linealizados $a(x)$ y $b(x)$, no es difícil probar por inducción, que existen polinomios únicos linealizados $q_L(x)$, $q_R(x)$, $r_L(x)$, $r_R(x)$ tales que

$$\begin{aligned} a(x) =& b(x) \otimes q_R(x) + r_R(x) \\ a(x) =& q_L(x) \otimes b(x) + r_L(x) \end{aligned}$$

donde

$$\begin{aligned} r_R(x) \equiv 0 \quad \text{ó} \quad \text{grad}(r_R(x)) < \text{grad}(b(x)) \text{ y} \\ r_L(x) \equiv 0 \quad \text{ó} \quad \text{grad}(r_L(x)) < \text{grad}(b(x)). \end{aligned}$$

Los polinomios $q_R(x)$ y $r_R(x)$ pueden ser determinados fácilmente por el siguiente algoritmo, el cual es una variación del algoritmo de la división larga.

Sea $lc(a(x))$ el coeficiente principal de $a(x)$, esto es el coeficiente de la indeterminada x con mayor exponente, luego si $\text{grad}(a(x)) = q^d$, es decir

$$a(x) = a_d x^{[d]} + a_{d-1} x^{[d-1]} + \ldots + a_0 x^{[0]} \quad \text{con} \quad a_d \neq 0$$

entonces $lc(a(x)) = a_d$.

Procedimiento: división a derecha de los polinomios $a(x)$ y $b(x)$.

Procedure RDiv$(a(x), b(x))$

entrada: un par de polinomios linealizados $a(x)$, $b(x)$ sobre $\mathbb{F}_{q^m}$ con $b(x) \not\equiv 0$.
salida: un par de polinomios linealizados $q(x)$, $r(x)$ sobre $\mathbb{F}_{q^m}$.

Inicio
si $\text{grad}(a(x)) < \text{grad}(b(x))$ **entonces**
return $(0, a(x))$
si no $d := \log_q \text{grad}(a(x))$, $e := \log_q \text{grad}(b(x))$, $a_d := lc(a(x))$, $b_e := lc(b(x))$.

$t(x) := (a_d/b_e)^{[m-e]}x^{[d-e]}$ (I)
return $(t(x), 0)$+**RDiv**$(a(x) - b(x) \otimes t(x), b(x))$ (II)
fin si
fin

Note que el parámetro m en el paso (I), es igual a la dimensión de $\mathbb{F}_{q^m}$ como espacio vectorial sobre $\mathbb{F}_q$.

El algoritmo termina cuando produce los polinomios $q(x)$ y $r(x)$ con la propiedad

$$a(x) = b(x) \otimes q(x) + r(x)$$

y se verifica que $r(x) \equiv 0$ ó $\text{grad}(r(x)) < \text{grad}(b(x))$.

El procedimiento para la división a izquierda es esencialmente el mismo, simplemente se reemplaza **RDiv** por **LDiv** y los pasos (I) y (II) son sustituidos por

$t(x) := (a_d/(b_e^{[d-e]}))x^{[d-e]}$
return $(t(x), 0)$+**LDiv**$(a(x) - t(x) \otimes b(x), b(x))$

Nuevamente el algoritmo termina cuando encuentre los polinomios $q(x)$ y $r(x)$ tales que $a(x) = q(x) \otimes b(x) + r(x)$ con $r(x) \equiv 0$ ó $\text{grad}(r(x)) < \text{grad}(b(x))$.

Estos polinomios reciben el nombre de linealizados por la siguiente propiedad:

Sea $L(x)$ un polinomio linealizado sobre $\mathbb{F}_{q^m}$ y K una extensión cualquiera de $\mathbb{F}_{q^m}$, entonces K puede ser considerado como espacio vectorial sobre $\mathbb{F}_q$. La función $K \ni \beta \mapsto L(\beta) \in K$ es lineal sobre $\mathbb{F}_q$, es decir para todo β_1, $\beta_2 \in K$ y λ_1, $\lambda_2 \in \mathbb{F}_q$, se verifica que

$$L(\lambda_1\beta_1 + \lambda_2\beta_2) = \lambda_1 L(\beta_1) + \lambda_2 L(\beta_2).$$

Suponga que K es escogido lo suficientemente grande, como para incluir todos los ceros de $L(x)$.

Los ceros de $L(x)$ corresponden al kernel de $L(x)$, cuando este es considerado como un operador lineal, estos ceros forman un espacio vectorial sobre $\mathbb{F}_q$.

Si $L(x)$ tiene grado q^d, entonces este espacio vectorial tiene dimensión a lo más d, pero esta dimensión puede ser menor que d si $L(x)$ tiene raíces múltiples (lo que ocurre si y sólo si $a_0 = 0$ en 2.6).

El siguiente lema muestra que si dos polinomios linealizados de grado a lo más q^{d-1} coinciden en al menos d puntos linealmente independientes, los dos polinomios coinciden.

2.5.2 Lema. Sea d un entero positivo y sean $f(x)$ y $g(x)$ dos polinomios linealizados sobre $\mathbb{F}_{q^m}$ con grados menores que q^d. Si $\{\alpha_1, \ldots, \alpha_d\}$ es un conjunto linealmente independiente de elementos de K tales que $f(\alpha_i) = g(\alpha_i)$ para $i = 1, \ldots, d$ entonces $f(x) \equiv g(x)$.

Demostración. Definamos el polinomio $h(x) = f(x) - g(x)$. Note que $h(\alpha_i) = 0$ para todo $i = 1, \ldots, d$, esto es h tiene d ceros, y además todas las q^d combinaciones lineales de estos, son ceros de h.

Entonces h tiene por lo menos q^d ceros distintos. Sin embargo, como

$$\text{grad}(h(x)) < q^d,$$

entonces la única posibilidad es que $h(x) \equiv 0$. □

2.5.2 Construcción del código

Así como tradicionalmente son obtenidas las componentes de un codeword en un código de Reed-Solomon mediante la evaluación de un polinomio, podemos obtener una base para el espacio vectorial transmitido via la evaluación de un polinomio linealizado.

Sea $\mathbb{F}_q$ un cuerpo finito y $\mathbb{F}_{q^m}$ una extensión finita del cuerpo $\mathbb{F}_q$, como vimos en la sección 2.5.1, podemos considerar $\mathbb{F}_{q^m}$ como un espacio vectorial de dimensión m sobre $\mathbb{F}_q$.

Sea $A = \{\alpha_1, \ldots, \alpha_l\} \subset \mathbb{F}_{q^m}$ un conjunto de elementos linealmente independientes en este espacio vectorial. Los elementos de este conjunto generan un espacio vectorial l-dimensional sobre $\mathbb{F}_q$, esto es $\langle A \rangle \subseteq \mathbb{F}_{q^m}$, claramente $l \leq m$. Tomamos como espacio ambiente W, la suma directa

$$W = \langle A \rangle \oplus \mathbb{F}_{q^m} = \{(\alpha, \beta) \mid \alpha \in \langle A \rangle, \beta \in \mathbb{F}_{q^m}\},$$

el cual es un espacio vectorial sobre $\mathbb{F}_q$ con dimensión $l + m$.

Sea $u = (u_0, \ldots, u_{k-1}) \in \mathbb{F}_{q^m}^k$ un mensaje de bloque consistente en k símbolos sobre $\mathbb{F}_{q^m}$, o equivalentemente mk símbolos sobre $\mathbb{F}_q$.

Denotemos con $\mathbb{F}_{q^m}^k[x]$ el conjunto de todos los polinomios linealizados sobre $\mathbb{F}_{q^m}$ de grado a lo más q^{k-1}, es decir

$$\mathbb{F}_{q^m}^k[x] = \{f(x) \mid \text{grad}(f) \leq q^{k-1}\}$$

donde

$$f(x) = \sum_{i=0}^{k-1} u_i x^{[i]}$$

es un polinomio linealizado con coeficientes u_i correspondientes a $u \in \mathbb{F}_{q^m}^k$. Finalmente, dado $\beta_i = f(\alpha_i)$, cada par ordenado (α_i, β_i) con $i = 1, \ldots, l$ puede ser considerado un vector en W. Ahora, como $A = \{\alpha_1, \ldots, \alpha_l\}$ es un conjunto linealmente independiente, se tiene que el conjunto

$$\{(\alpha_1, \beta_1), \ldots, (\alpha_l, \beta_l)\}$$

también lo es, en efecto, supongamos que para $\gamma_1, \ldots, \gamma_l \in \mathbb{F}_q$ se tiene $\sum_{i=1}^{l} \gamma_i(\alpha_i, \beta_i) = 0$. Entonces tendríamos

$$\sum_{i=1}^{l} \gamma_i(\alpha_i, \beta_i) = \left(\sum_{i=0}^{l} \gamma_i \alpha_i, \sum_{i=0}^{l} \gamma_i \beta_i \right) = (0, 0).$$

Lo anterior se sigue únicamente de la independencia lineal del conjunto A, es decir, sólo si $\gamma_1, \ldots, \gamma_l = 0$, dado que los α_i, son linealmente independientes.

por lo tanto este conjunto genera un espacio $V \in \mathcal{P}(W, l)$.

Notamos con $\mathtt{ev}_A$ la función que envía un polinomio $f(x) \in \mathbb{F}_{q^m}^k[x]$ a un espacio vectorial $V \in \mathcal{P}(W, l)$, con $l = |A|$.

2.5.3 Lema. Si $|A| \geq k$, entonces la función

$$\mathtt{ev}_A : \mathbb{F}_{q^m}^k[x] \longrightarrow \mathcal{P}(W, |A|)$$

es inyectiva.

Demostración. Supongamos $|A| \geq k$ y $\mathtt{ev}_A(f) = \mathtt{ev}_A(g)$ para $f, g \in \mathbb{F}_{q^m}^k[x]$. Sea $h(x) = f(x) - g(x)$, es claro que $h(\alpha_i) = 0$ para todo $i = 1, \ldots, l$. Dado que $h(x)$ es un polinomio linealizado, se sigue que para todo $x \in \langle A \rangle$, $h(x) = 0$, luego $h(x)$ tiene por lo menos

$$q^{|A|} \geq q^k$$

raíces, y como $\text{grad}(h(x)) \leq q^{k-1}$, entonces la única posibilidad para $h(x)$ es que $h(x) \equiv 0$, en consecuencia $f(x) \equiv g(x)$. $\square$

En lo que sigue asumimos que $l \geq k$. El lema anterior asegura que si se mantiene esta condición, entonces $\text{Im}(\mathtt{ev}_A)$ es un código $\mathcal{C} \in \mathcal{P}(W, l)$ con q^{mk} codewords, y cuya distancia mínima será definida en el próximo teorema, pero antes necesitamos del siguiente lema.

2.5.4 Lema. Si $\{(\alpha_1, \beta_1), \ldots, (\alpha_r, \beta_r)\} \subseteq W$ es un conjunto de r vectores linealmente independientes, que satisfacen

$$\beta_i = f(\alpha_i)$$

para algún polinomio linealizado f sobre $\mathbb{F}_{q^m}$, entonces $\{\alpha_1, \ldots, \alpha_r\}$ es un conjunto linealmente independiente.

Demostración. Supongamos que para $\gamma_1, \ldots, \gamma_r \in \mathbb{F}_q$ se tiene $\sum_{i=1}^{r} \gamma_i \alpha_i = 0$. Entonces en el espacio W, tendríamos

$$\begin{aligned}\sum_{i=1}^{r} \gamma_i(\alpha_i, \beta_i) &= \left(\sum_{i=0}^{r} \gamma_i \alpha_i, \sum_{i=0}^{r} \gamma_i \beta_i\right) = \left(0, \sum_{i=0}^{r} \gamma_i f(\alpha_i)\right) \\ &= \left(0, f\left(\sum_{i=0}^{r} \gamma_i \alpha_i\right)\right) = (0, f(0)) = (0, 0).\end{aligned}$$

Lo anterior es posible sólo si $\gamma_1, \ldots, \gamma_r = 0$, dado que los pares (α_i, β_i) son linealmente independientes. □

2.5.5 Teorema. Sea $\mathcal{C} = \mathrm{Im}(\mathtt{ev}_A) = \mathtt{ev}_A(\mathbb{F}_{q^m}^k[x])$ con $l = |A| \geq k$. Entonces $\mathcal{C}$ es un código de tipo

$$[l + m, l, q^{mk}, 2(l - k + 1)].$$

Demostración. Dado que $\mathtt{ev}_A$ es inyectiva, se tiene que $|\mathcal{C}| = q^{mk}$. Entonces sólo resta probar que la distancia mínima de $\mathcal{C}$ es $2(l - k + 1)$.

Para ello sean $f(x)$, $g(x) \in \mathbb{F}_{q^m}^k[x]$, con $f(x) \not\equiv g(x)$, además

$$U = \mathtt{ev}_A(f) \qquad \text{y} \qquad V = \mathtt{ev}_A(g)$$

Supongamos también que $\dim(U \cap V) = r$, esto significa que es posible hallar r elementos linealmente independientes, digamos $(\alpha'_1, \beta'_1), \ldots, (\alpha'_r, \beta'_r)$ tales que

$$f(\alpha'_i) = g(\alpha'_i) = \beta'_i \qquad \text{con} \quad i = 1, \ldots, r.$$

Por el lema anterior, $\{\alpha'_1, \ldots, \alpha'_r\}$ es un conjunto linealmente independiente y por lo tanto generan un espacio B, r-dimensional con la propiedad que

$$f(b) - g(b) = 0$$

para todo $b \in B$.

En efecto, si $b \in B$, entonces $b = \sum_{j=1}^{r} b_j \alpha'_j$, en consecuencia

$$f(b) = \sum_{j=1}^{r} b_j f(\alpha'_j) = \sum_{j=1}^{r} b_j \beta'_j = g(b).$$

Si $r \geq k$, entonces $f(x)$ y $g(x)$ serían dos polinomios linealizados de grado menor que q^k que coinciden en al menos k puntos linealmente independientes y aplicando el lema 2.5.2 obtendríamos $f(x) \equiv g(x)$.

Dado que este no es el caso, debemos considerar $r \leq k-1$, luego

$$\begin{aligned} d_S(U,V) =& \dim(U) + \dim(V) - 2\dim(U \cap V) \\ =& l + l - 2r = 2(l-r) \geq 2(l-k+1). \end{aligned}$$

Es fácil encontrar dos codewords U y V que satisfagan la igualdad, para lo cual $D_S(\mathcal{C}) = 2(l-k+1)$. □

2.5.6 Ejemplo. Construyamos un código Reed-Solomon de red tomando $\mathbb{F}_{q^m} = \mathbb{F}_4$, extensión finita del cuerpo $\mathbb{F}_2$.

Dado $\mathbb{F}_4 = \{\bar{0}, \bar{1}, \bar{\omega}, \overline{\omega+1}\}$, el cual puede ser visto como un espacio vectorial de dimensión 2 sobre el cuerpo $\mathbb{F}_2$, como

$$\mathbb{F}_4 = \mathbb{F}_2^2 = \{(0,0), (0,1), (1,0), (1,1)\}$$

Donde cada clase en $\mathbb{F}_4$ puede ser representada por un vector en $\mathbb{F}_2^2$, así por ejemplo podemos identificar la clase $\bar{\omega}$ con el vector $(1,0)$.

Paso 1: Elijamos un conjunto $A \subset \mathbb{F}_4$ cuyos l elementos (con $l < 2 = m$) sean linealmente independientes en este espacio vectorial, es decir,

$$A = \{(1,1)\},$$

entonces el generado es el conjunto

$$\langle A \rangle = \{(0,0), (1,1)\}.$$

El espacio ambiente sobre el cual construiremos el código es el siguiente

$$W = \langle A \rangle \oplus \mathbb{F}_4 = \{(\alpha, \beta) \mid \alpha \in \langle A \rangle, \beta \in \mathbb{F}_4\}$$

luego

$$\dim_{\mathbb{F}_2} W = \underbrace{\dim_{\mathbb{F}_2} \langle A \rangle}_{l} + \underbrace{\dim_{\mathbb{F}_2} \mathbb{F}_4}_{m} = 1 + 2 = 3$$

Paso 2: A continuación se hallan todos los polinomios linealizados sobre $\mathbb{F}_4$ de grado a lo más q^{k-1}, donde $q = 2$ y para garantizar la existencia del código $|A| = l \geq k$, dado que $l = 1$ la única opción para k es $k = 1$,

$$\begin{aligned} \mathbb{F}_4^k[x] = \mathbb{F}_4[x] &= \{a_i x \mid a_i \in \mathbb{F}_4\} \\ &= \{0, x, \omega x, (\omega+1)x\}. \end{aligned}$$

A través de la función inyectiva descrita en el lema 2.5.3

$$\mathtt{ev}_A : \mathbb{F}_{q^m}^k[x] \longrightarrow \mathcal{P}(W, l)$$

se genera un RS-código del tipo $[l+m, l, q^{mk}, 2(l-k+1)]$, es decir, nuestro ejemplo es un código del tipo $[3, 1, 4, 2]$.

Paso 3: Ahora hallemos los codewords del código generados por la evaluación de cada polinomio en $\mathbb{F}_4[x]$.
Sea $\beta_i = f(\alpha_i)$ con $f \in \mathbb{F}_4[x]$, cada par (α_i, β_i), para $i = 1, \ldots, l$ es un vector en W. Además como $A = \{\alpha_1, \ldots, \alpha_l\}$ es un conjunto con elementos linealmente independientes, entonces $\{(\alpha_1, \beta_1), \ldots, (\alpha_l, \beta_l)\}$ también lo es y genera un subespacio V de dimensión l en W. En consecuencia, para nuestro ejemplo $l = 1$ y definiendo los polinomios como

$$f_1 = 0, \quad f_2 = x, \quad f_3 = \omega x, \quad f_4 = (\omega + 1)x$$

evaluemos $\alpha_1 = (1, 1)$ para obtener lo siguiente

$f_1(\alpha_1) = (0, 0) = \beta_1 \longrightarrow (\alpha_1, \beta_1) = 1100$
$f_2(\alpha_1) = (1, 1) = \beta_1 \longrightarrow (\alpha_1, \beta_1) = 1111$
$f_3(\alpha_1) = \omega(1, 1) = \omega(\omega + 1) = 1 = (0, 1) = \beta_1 \longrightarrow (\alpha_1, \beta_1) = 1101$
$f_4(\alpha_1) = (\omega + 1)(1, 1) = (\omega + 1)(\omega + 1) = \omega = (1, 0) = \beta_1 \rightarrow (\alpha_1, \beta_1) = 1110$

Paso 4: Finalmente concluimos que los codewords para este código Reed Solomon tipo $[3, 1, 4, 2]$, son cuatro subespacios (rectas) generados por los conjuntos

$$\{1100\}, \{1111\}, \{1101\}, \{1110\}.$$

La cota de Singleton evaluada con los parámetros del código del teorema anterior establece que

$$|\mathcal{C}| \leq \begin{bmatrix} N - (D_S - 2)/2 \\ \text{máx } \{l, N - l\} \end{bmatrix}_q = \begin{bmatrix} l + m - (2(l - k + 1) - 2)/2 \\ \text{máx } \{l, l + m - l\} \end{bmatrix}_q = \begin{bmatrix} m + k \\ m \end{bmatrix}_q$$

esto es,

$$|\mathcal{C}| \leq \begin{bmatrix} m + k \\ m \end{bmatrix}_q = \begin{bmatrix} m + k \\ (m + k) - m \end{bmatrix}_q = \begin{bmatrix} m + k \\ k \end{bmatrix}_q < 4q^{mk}.$$

Esto significa que un código que alcance la cota de Singleton no podría tener más que cuatro veces la cantidad de codewords que $\mathcal{C}$ (el código de Reed-Solomon construido antes).

Cuando N es suficientemente grande, la diferencia entre la tasa de un código que alcance la cota de Singleton y $\mathcal{C}$ resulta insignificante, en efecto, en términos de los parámetros normalizados, tenemos

$$R = (1 - \lambda)\left(1 - \delta + \frac{1}{\lambda N}\right),$$

el cual tiene el mismo comportamiento asintótico que tiene la cota de Singleton cuando $N \to \infty$.

Estos códigos de Reed-Solomon se comportan muy bien en el sentido que están muy cerca de alcanzar la cota de Singleton.

Observe también que el código de red del ejemplo 2.3.9, un código del tipo $[m + l, l, q^{ml}, 2]$ se obtiene como un caso particular del código Reed-Solomon, cuando $k = l$.

La construcción de este código supone que la evaluación de polinomios linealizados está íntimamente relacionada con la construcción de la métrica del rango de Gabidulin [4].

Sin embargo en nuestro sistema, los codewords no son arreglos, pero los espacios vectoriales son generados por las filas de los arreglos y la correspondiente métrica relacionada con la decodificación no es la métrica del rango, sino más bien la distancia definida entre subespacios (2.1).

Capítulo 3

Construcción de un código Reed-Solomon usando Maple

En este capítulo mostraremos cómo utilizamos el programa Maple para generar los codewords de un código de red de dimensión constante del tipo Reed-Solomon. En esta oportunidad implementamos el código sobre el cuerpo finito $\mathbb{F}_4$ construido en el ejemplo 2.5.6, un código sencillo de desarrollar sin ayuda de una herramienta computacional, debido a su tamaño. Luego mostramos un código un poco más robusto sobre $\mathbb{F}_8$, en este último se aprecia mucho más la necesidad de utilizar un software para tal objetivo. Ambos códigos resultaron de los polinomios irreducibles $x^2 + x + 1$ sobre $\mathbb{F}_4$ y $x^3 + x^2 + 1$ sobre $\mathbb{F}_8$.

3.1 Generalidades sobre cuerpos finitos

Recordemos que un cuerpo es una terna $(K, +, \cdot)$, de forma que $(K, +)$ es un grupo abeliano y $(K^*, \cdot)$ (donde $K^* = K \setminus \{0\}$) es un semigrupo abeliano, junto con la propiedad distributiva:

$$\text{para todo } x, y, z \in K, \quad z \cdot (x + y) = z \cdot x + z \cdot y$$

Ya conocemos tres ejemplos básicos de cuerpos $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, la cuestión es que no son los únicos cuerpos posibles; por ejemplo $\mathbb{Q}[i]$ es otro cuerpo. Nótese que, en realidad es posible escribir $\mathbb{Q}[i]$ como

$$\mathbb{Q}[i] = \mathbb{Q}[x]/(x^2 + 1).$$

Antes de abordar el ejemplo de cuerpo que nos interesa, es preciso recordar los cuerpos $\mathbb{Z}/\mathbb{Z}_p = \mathbb{F}_p$, donde p es un número entero primo

$$\mathbb{Z}/\mathbb{Z}_p = \mathbb{F}_p = \{[0], [1], \ldots, [p-1]\},$$

de forma que

$$[a] + [b] = [a + b]$$
$$[a] \cdot [b] = [a \cdot b]$$

Generalmente se abusa de la notación y se escribe a en lugar de $[a]$.

No es difícil demostrar que efectivamente, $\mathbb{F}_p$ es cuerpo para cualquier p primo, y que, de hecho $\mathbb{Z}/\mathbb{Z}_n$ para n arbitrario es un anillo. Sin embargo, consideremos con cierto detalle el cuerpo $\mathbb{F}_5$, cuyas tablas de sumar y multiplicar se muestran a continuación.

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[0]$	$[1]$	$[2]$	$[3]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[0]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[0]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[0]$	$[4]$	$[3]$	$[2]$	$[1]$

Los cuerpos de este tipo, por obvia razón, se llaman cuerpos finitos. Más a delante veremos que no todos los cuerpos finitos son de este tipo.

Un concepto muy importante sobre un cuerpo es su característica. Supongamos un cuerpo K, y consideremos la sucesión de elementos de K

$$1, 1+1, 1+1+1, 1+1+1+1, \ldots$$

Para la cual se tienen dos posibilidades:

- La sucesión nunca es cero: lo que ocurre en cuerpos como $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}[i]$,...
- Existe un mínimo entero $p > 0$ tal que en K la siguiente suma es cero

$$\underbrace{1 + 1 + \ldots + 1}_{p \text{ veces}}$$

El ejemplo para este es $\mathbb{F}_p$.

En el primer caso, se dice que la característica es cero, y en el segundo, que la característica es p. En ambos casos se denota la característica de K por $\text{char}(K)$.

Obsérvese que si $\text{char}(K) = p > 0$, entonces p es un número primo; en efecto, si suponemos que p no es primo, entonces $p = 0$ y se expresaría como $p = p_1 p_2 = 0$, de forma que uno de los factores, digamos p_1 (sin perder generalidad) es cero, y esto contradice la minimalidad de p.

Otras conclusiones inmediatas que obtenemos son:

(i) Todo cuerpo finito K verifica $\text{char}(K) > 0$.

(ii) Si $\text{char}(K) = p > 0$, $K \supseteq \mathbb{F}_p$ como subcuerpo. (Basta considerar el homomorfismo $j : \mathbb{Z} \longrightarrow K$, y ver que $\mathbb{Z}/\ker(j)$ es un subcuerpo de K)

Dado un cuerpo K es posible obtener un cuerpo más grande adjuntando raíces de polinomios, a la manera que se obtiene $\mathbb{C}$ de $\mathbb{R}$ adjuntando i. En general se considera un cuerpo cualquiera, K, y el anillo de los polinomios sobre K, que denotamos $K[x]$. Sea $f(x)$ un polinomio irreducible, y consideremos el conjunto

$$K[x]/(f(x)) = \{\text{polinomios módulo} f(x)\}.$$

En este caso $K[x]/(f(x))$ es un cuerpo con las operaciones similares al caso de $\mathbb{Z}/\mathbb{Z}_5$ que vimos antes:

$$\begin{aligned}[h(x)] + [g(x)] =& [h(x) + g(x)] \\ [h(x)] \cdot [g(x)] =& [h(x) \cdot g(x)]\end{aligned}$$

Otra manera de pensar en este cuerpo es como el conjunto de polinomios de grado estrictamente menor que el grado del polinomio irreducible $f(x)$, es decir, los restos de las divisiones por $f(x)$, o mejor aún, como la extensión algebraica $K[x]/(f(x)) = K[\alpha]$, con $f(\alpha) = 0$. Veamos un ejemplo, sea $K = \mathbb{F}_2$ y el polinomio irreducible $f(x) = x^2 + x + 1$. En este caso,

$$\mathbb{F}_2[x]/(x^2 + x + 1) = \{0, 1, x, x + 1\}.$$

(Note que abusamos de la notación y escribimos x en lugar de $[x]$.) Estos son todos los elementos de $\mathbb{F}_2[x]/(x^2 + x + 1)$. También podemos concebir este cuerpo como $\mathbb{F}_2[\alpha]$, donde α es raíz del polinomio irreducible $x^2 + x + 1$, es decir, α verifica la ecuación $\alpha^2 + \alpha + 1 = 0$. De esta forma y dado que $[-1] = [1]$ es fácil calcular

$$\begin{aligned}\alpha^3 =& \alpha^2 \alpha \\ =& (\alpha + 1)\alpha \\ =& \alpha + 1 + \alpha \\ =& 1\end{aligned}$$

Se escribe $[\alpha^3] = [1]$ o simplemente $\alpha^3 = 1$. Escrito de esta forma,

$$\mathbb{F}_2[\alpha] = \{0, 1, \alpha, \alpha + 1\}.$$

Para finalizar este ejemplo se pueden calcular las tablas de sumar y multiplicar de $\mathbb{F}_2[\alpha]$.

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

Una observación trivial sobre los cuerpos finitos es que si $\deg f(x) = n$, con $f(x)$ irreducible sobre $\mathbb{F}_p[x]$, el cardinal de $\mathbb{F}_p[\alpha] = p^n$. Estos son los hechos básicos de los cuerpos finitos. Necesitaremos unos cuantos hechos no tan básicos, pero cuya demostración omitimos. El primero de ellos, es que los cuerpos finitos son todos de este tipo.

3.1.1 Teorema. Sea $q \in \mathbb{Z}^+$. Existe un cuerpo con q elementos si y sólo si $q = p^n$ para algún primo p y algún $n > 0$. Más aún, salvo isomorfismo, existe un único cuerpo con q elementos, y es de la forma $\mathbb{F}_p[x]/f(x)$ para algún polinomio irreducible de grado n.

3.1.2 Teorema. Sea $\mathbb{F}$ un cuerpo finito con p^n elementos. Entonces $\mathbb{F}^*$ es un grupo cíclico de orden $p^n - 1$; es decir, existe un cierto $\beta \in \mathbb{F}^*$ y tal que

$$\mathbb{F}^* = \{\beta, \beta^2, \ldots, \beta^{n-1}\}.$$

Donde β se denomina raíz primitiva de $\mathbb{F}$.

3.1.3 Teorema. (i) $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ si y sólo si $m \mid n$.
(ii) En $\mathbb{F}_q$, se verifica que $(x + y)^p = x^p + y^p$.

3.2 Algunos cálculos con Maple

En maple es posible calcular directamente sobre cuerpos finitos, usando varias de las funciones predefinidas. Comenzaremos por lo más sencillo. La función `mod` permite hacer cálculos en $\mathbb{F}_p$. Como ejemplo veamos quién es el inverso de 6 en $\mathbb{F}_{11}$.

```
> 6^(-1) mod 11;
```

$$2$$

La tabla de multiplicar de $\mathbb{F}_{11}$ la podemos calcular haciendo la siguiente secuencia por filas y columnas, de la siguiente manera:

```
> A := array( [seq([seq(i*j mod 11, j = 1..10) ], i = 1..10)]);
```

$$A := \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 4 & 6 & 8 & 10 & 1 & 3 & 5 & 7 & 9 \\ 3 & 6 & 9 & 1 & 4 & 7 & 10 & 2 & 5 & 8 \\ 4 & 8 & 1 & 5 & 9 & 2 & 6 & 10 & 3 & 7 \\ 5 & 10 & 4 & 9 & 3 & 8 & 2 & 7 & 1 & 6 \\ 6 & 1 & 7 & 2 & 8 & 3 & 9 & 4 & 10 & 5 \\ 7 & 3 & 10 & 6 & 2 & 9 & 5 & 1 & 8 & 4 \\ 8 & 5 & 2 & 10 & 7 & 4 & 1 & 9 & 6 & 3 \\ 9 & 7 & 5 & 3 & 1 & 10 & 8 & 6 & 4 & 2 \\ 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{bmatrix}$$

Para cálculos sobre $\mathbb{F}_p^n$, necesitamos fijar una extensión algebraica de grado n sobre $\mathbb{F}_p$. Para maple, esto se hace definiendo un polinomio irreducible sobre $\mathbb{F}_p$ de grado n.

Supongamos que queremos realizar cálculos sobre $\mathbb{F}_8 = \mathbb{F}_2^3$. Necesitamos un polinomio de grado 3 sobre $\mathbb{F}_2$, por ejemplo $f(x) = x^3 + x^2 + 1$. Llamamos α a una raíz de $f(x)$. Por definición se tiene que verificar que $\alpha^3 = \alpha^2 + 1$. En efecto,

```
> Factor(α^3 + α^2 + 1) mod 2;
```

$$\alpha^3 + \alpha^2 + 1$$

```
> alias(alpha = RootOf(α^3 + α^2 + 1)):
> Normal(α^3) mod 2;
```

$$\alpha^2 + 1$$

La combinación `Factor... mod` verifica si un polinomio es irreducible sobre $\mathbb{F}_p$. A continuación hacemos que maple sustituya `RootOf`(x^3+x^2+1) por α para que los resultados sean legibles. Por último normalizamos la expresión x^3 en $\mathbb{F}_8=\mathbb{F}_2[\alpha]$, dando como solución α^2+1.

Ahora veremos de qué forma podemos listar los elementos del cuerpo $\mathbb{F}_8$, esto se puede hacer utilizando la función `polinum()`. Una vez que tenemos esta función auxiliar, podemos enumerar los elementos de $\mathbb{F}_8$ con la función `FF(2,`α`)`.

```
> polinum := proc(i, p, alpha)
      local n, k;
      n := convert(i, base, p);
      return sum(n[k]*alpha^(k-1), k=1..nops(n))
  end:
  FF := proc(p, alpha)
     return [seq(polinum(i, p, alpha), i=0..p^(degree(op(1, alpha)))-1)]
  end:
> FF(2, alpha);
```

$$[0,\ 1,\ \alpha,\ 1+\alpha,\ \alpha^2,\ 1+\alpha^2,\ \alpha+\alpha^2,\ 1+\alpha+\alpha^2]$$

Ahora podemos hacer la tabla de multiplicación para $\mathbb{F}_8$ como se sigue:

```
> array([seq([seq(Normal(polinum(i, 2, alpha)*polinum(j, 2, alpha)) mod 2, i=1..7)], j=1..7)]);
```

$$\begin{bmatrix}
1 & \alpha & 1+\alpha & \alpha^2 & 1+\alpha^2 & \alpha+\alpha^2 & 1+\alpha+\alpha^2 \\
\alpha & \alpha^2 & \alpha+\alpha^2 & 1+\alpha^2 & 1+\alpha+\alpha^2 & 1 & 1+\alpha \\
1+\alpha & \alpha+\alpha^2 & 1+\alpha^2 & 1 & \alpha & 1+\alpha+\alpha^2 & \alpha^2 \\
\alpha^2 & 1+\alpha^2 & 1 & 1+\alpha+\alpha^2 & 1+\alpha & \alpha & \alpha+\alpha^2 \\
1+\alpha^2 & 1+\alpha+\alpha^2 & \alpha & 1+\alpha & \alpha+\alpha^2 & \alpha^2 & 1 \\
\alpha+\alpha^2 & 1 & 1+\alpha+\alpha^2 & \alpha & \alpha^2 & 1+\alpha & 1+\alpha^2 \\
1+\alpha+\alpha^2 & 1+\alpha & \alpha^2 & \alpha+\alpha^2 & 1 & 1+\alpha^2 & \alpha
\end{bmatrix}$$

Cuando se quiere buscar un polinomio irreducible de grado adecuado, podemos pedir a maple que lo calcule. Veamos un polinomio que define a $\mathbb{F}_{16}$.

```
> G := GF(2, 4) : G[extension];
```

$$(T^4+T^3+1) \bmod 2$$

```
> alias(alpha = RootOf(alpha^4+alpha^3+1)) :
> FF(2, alpha);
```

$$[0,\ 1,\ \alpha,\ 1+\alpha,\ \alpha^2,\ 1+\alpha^2,\ \alpha+\alpha^2,\ 1+\alpha+\alpha^2,\ \alpha^3,\ 1+\alpha^3,\ \alpha+\alpha^3,\ 1+\alpha+\alpha^3,\ \alpha^2+\alpha^3,\ 1+\alpha^2+\alpha^3,\ \alpha+\alpha^2+\alpha^3,\ 1+\alpha+\alpha^2]$$

Es preferible copiar a mano el polinomio irreducible que maple devuelve, en lugar de usarlo directamente, porque la indeterminada que aparece (en este caso T), el programa no la "entiende" como variable global T.

3.2.1 Construcción

En lo que sigue se muestran exclusivamente los resultados de la implementación del código de red tipo Reed-Solomon sobre $\mathbb{F}_4$, dado que su construcción fue explicada en detalle en el ejemplo 2.5.6.

Creación del cuerpo F4

$G := GF(2, 2) : G[extension];$

$$(T^2 + T + 1) \bmod 2$$

$alias(\alpha = RootOf(x^2 + x + 1)) :$

$polinun := \mathbf{proc}(i, p, \alpha)\mathbf{local}\ n, k; n := convert(i, base, p);$
$\mathbf{return}\ sum(n[k] \cdot \alpha^{(k-1)}, k = 1 .. nops(n))\ \mathbf{end\ proc}:$

$FF := \mathbf{proc}(p, \alpha)\mathbf{return}\ [seq(polinun(i, p, \alpha), i = 0 .. p^{degree(op(1, \alpha))} - 1)]\ \mathbf{end\ proc}:$
$FF(2, \alpha);$

$$[0, 1, \alpha, 1 + \alpha]$$

Simbolizamos con H al cuerpo $\mathbb{F}_4$ visto como espacio vectorial sobre $\mathbb{F}_2$:

$with(PolynomialTools) :$
$T := [seq(Vector_{row}(2, CoefficientVector(W[i], x)), i = 1 .. 4)];$

$$[[0\ 0], [1\ 0], [0\ 1], [1\ 1]]$$

$H := convert(T, set);$

$$\{[0\ 0], [1\ 1], [1\ 0], [0\ 1]\}$$

Todos los posibles subconjuntos de H formados por un vector:

$with(combinat) :$
$with(LinearAlgebra) :$
$choose(H, 1);$

$$\{\{[0\ 0]\}, \{[1\ 1]\}, \{[1\ 0]\}, \{[0\ 1]\}\}$$

enumeramos de la lista anterior los subconjuntos de vectores linealmente independientes y elegimos uno de los subconjuntos aleatoriamente:

$LI(H, 1)$

$$[2, 3, 4]$$

$luplas := LI(H, 1)$

$$[2, 3, 4]$$

$ind := choose(nops(H), 1);$

$$[[1], [2], [3], [4]]$$

$aleatorio := rand(nops(luplas)) :$
$aleatorio := aleatorio( ) + 1;$

$$3$$

el elemento correspondiente es el tercero de la lista denominada como *luplas*, es decir, este corresponde al cuarto conjunto de H.

```
H[ind[luplas[aleatorio]][1]]
```

$$[\,0\ 1\,]$$

Ahora creamos la lista de los polinomios linealizados

```
linealizados2 := proc(B, p, k) local i, O, m, todoscero;
 O := [ ];
 for i from 1 by 1 to nops(B) do
     todoscero := true;
     for m from 1 by 1 to k do
         if B[i] ≠ 0 then
            todoscero := true;
         end if;
     end do;
     if (N[i] ≠ 0 or todoscero = true) then
         O := [op(O), op([[(sum(B[i]·x^(p^j), j = 0 .. k - 1))]])]
     end if;
 end do;
end proc:
poly := linealizados2(B, 2, 1);
```

$$[0, x, \alpha x, (1+\alpha)\,x]$$

Evaluación del vector $(0,1)$ en cada polinomio

$$[0, \alpha, 1+\alpha, 1]$$

Finalmente creamos todos los codewords haciendo una suma directa entre el conjunto $\{(0,1)\}$ y el conjunto imágen bajo los cuatro polinomios linealizados de grado uno encontrados.

```
cartesiano := proc(A :: set, B :: set)
local i, j, C :
C := { } :
for i from 1 to nops(A) do
  for j from 1 to nops(B) do
  C := C union {[[op(A)][i], [op(B)][j]]}
 od:
 od: C; end:
SSS := cartesiano({[ 0 1 ]}, AA) :
a1 := convert(SSS, list) :
Subespacios := [seq({a1[i]}, i = 1 ..nops(a1))];
                [{[[ 0 1 ], [ 0 1 ]]}, {[[ 0 1 ], [ 1 1 ]]}, {[[ 0 1 ], [ 1 0 ]]}, {[[ 0 1 ], [ 0 0 ]]}]
```

Luego los codewords son cuatro subespacios generados por los conjuntos de la lista anterior, los cuales conforman un código con parámetros $[3, 1, 4, 2]$.

A continuación abordamos la construcción de un código Reed-Solomon de subespacios sobre el cuerpo finito $\mathbb{F}_8 = \mathbb{F}_2^3$. De los cálculos hechos en la sección anterior, sabemos que los elementos de $\mathbb{F}_2^3$ son

```
> FF(2, alpha);
        [0, 1, α, 1 + α, α^2, 1 + α^2, α + α^2, 1 + α + α^2]
```

El cual, puede verse como un espacio vectorial de dimensión tres sobre el cuerpo $\mathbb{F}_2$, para esto debemos convertir cada elemento del cuerpo a un polinomio con indeterminada x y luego utilizar el paquete de maple `PolynomialTools` y la función auxiliar `CoefficientVector`, esta función arroja el vector de coeficientes de un polinomio en la indeterminada x.

```
W := subs(α = x, B) :
with(PolynomialTools) :
T := [seq(Vector_row(3, CoefficientVector(W[i], x)), i = 1 ..8)] :
H := convert(T, set);
        H := {[ 0 1 1 ], [ 1 0 1 ], [ 0 0 1 ], [ 0 1 0 ], [ 1 1 0 ], [ 0 0 0 ], [ 1 0 0 ], [ 1 1 1 ]}
```

Ahora debemos generar un subconjunto de l vectores linealmente independientes a partir del espacio vectorial $\mathbb{F}_2^3$, donde el número l debe ser estrictamente menor que la dimensión de $\mathbb{F}_2^3$ (tomaremos $l = 2$), es decir, ahora vamos a crear todos los posibles subconjuntos de dos vectores, para esto primero hacemos uso del paquete `LinearAlgebra` y el comando `choose` para mostrar los 28 posibles

```
with(combinat) :
with(LinearAlgebra) :
choose(H, 2);
```

$$\{\{[0\ 1\ 1], [0\ 1\ 0]\}, \{[0\ 1\ 1], [0\ 0\ 0]\}, \{[0\ 1\ 1], [1\ 0\ 1]\}, \{[0\ 1\ 1], [1\ 1\ 0]\}, \{[0\ 1\ 1], [1\ 1\ 1]\}, \{[0\ 1\ 1], [0\ 0\ 1]\}, \{[0\ 1\ 1], [1\ 0\ 0]\}, \{[0\ 1\ 0], [0\ 0\ 0]\}, \{[0\ 1\ 0], [1\ 0\ 1]\}, \{[0\ 1\ 0], [1\ 1\ 0]\}, \{[0\ 1\ 0], [1\ 1\ 1]\}, \{[0\ 1\ 0], [0\ 0\ 1]\}, \{[0\ 1\ 0], [1\ 0\ 0]\}, \{[0\ 0\ 0], [1\ 0\ 1]\}, \{[0\ 0\ 0], [1\ 1\ 0]\}, \{[0\ 0\ 0], [1\ 1\ 1]\}, \{[0\ 0\ 0], [0\ 0\ 1]\}, \{[0\ 0\ 0], [1\ 0\ 0]\}, \{[1\ 0\ 1], [1\ 1\ 0]\}, \{[1\ 0\ 1], [1\ 1\ 1]\}, \{[1\ 0\ 1], [0\ 0\ 1]\}, \{[1\ 0\ 1], [1\ 0\ 0]\}, \{[1\ 1\ 0], [1\ 1\ 1]\}, \{[1\ 1\ 0], [0\ 0\ 1]\}, \{[1\ 1\ 0], [1\ 0\ 0]\}, \{[1\ 1\ 1], [0\ 0\ 1]\}, \{[1\ 1\ 1], [1\ 0\ 0]\}, \{[0\ 0\ 1], [1\ 0\ 0]\}\}$$

Lo siguiente es crear un procedimiento que de la lista anterior elija los subconjuntos de dos vectores linealmente independientes y enumere estos subconjuntos, finalmente que en cada subconjunto identifique el vector con el elemento asociado del cuerpo de ocho elementos.

```
LI := proc(H, l)
    local i, O, Q;
    with(combinat);
    with(LinearAlgebra) :
    O := choose(H, l) :
    Q := [ ] :
    for i from 1 by 1 to nops(O) do
        if nops(Basis(O[i])) = l then;
           Q := [op(Q), i] :
        end if;
     end do;
 end proc:
LI(H, 2)
```

$$[1, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28]$$

```
luplas := LI(H, 2)
```

$$[1, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28]$$

```
ind := choose(nops(H), 2);
```

$$[[1, 2], [1, 3], [1, 4], [1, 5], [1, 6], [1, 7], [1, 8], [2, 3], [2, 4], [2, 5], [2, 6], [2, 7], [2, 8], [3, 4], [3, 5], [3, 6], [3, 7], [3, 8], [4, 5], [4, 6], [4, 7], [4, 8], [5, 6], [5, 7], [5, 8], [6, 7], [6, 8], [7, 8]]$$

Ahora se elige con el comando `rand()` uno de los subconjuntos linealmente independientes aleatoriamente

```
aleatorio := rand(nops(luplas)) :
aleatorio := aleatorio( ) + 1;
```

$$3$$

```
H[ind[luplas[aleatorio]][1]]
```

$$[\,0\ 1\ 1\,]$$

```
H[ind[luplas[aleatorio]][2]]
```

$$[\,1\ 1\ 0\,]$$

De lo anterior se entiende que el elemento aleatorio es el tercero de la lista de `luplas`, es decir, la cuarta pareja en la lista `ind`, esta es la formada por el primer y quinto elemento del conjunto H que representa el espacio vectorial de la página 63. Estos dos últimos vectores $v_1 = (0,1,1)$ y $v_2 = (1,1,0)$ son de gran importancia para generar el código, pero antes debemos crear los polinomios linealizados (definidos en el capítulo anterior) a partir de los cuales se construyen los codewords.

Como se explicó en el capítulo anterior, en el lema 2.5.3, para garantizar la existencia del código se debe verificar que $l \geq k$, donde l es el número de vectores linealmente independientes, en este caso $l = 2$, y k se define a partir de que los polinomios linealizados son de grado a lo más q^{k-1} (teniendo en cuenta que estamos trabajando sobre $q = 2$). En este orden de ideas, para nuestro código, $1 \leq k \leq 2$, tomaremos $k = 2$ en la fórmula $\sum_{i=0}^{k-1} a_i x^{2^i}$, donde $a_i \in \mathbb{F}_2^3$, esto es, los posibles polinomios linealizados son de grado 2:

$$\sum_{i=0}^{1} a_i x^{2^i} = a_0 x + a_1 x^2.$$

El siguiente paso en la construcción es crear todas las parejas de coeficientes $[a_0, a_1]$ de los polinomios, para esto se utiliza el paquete `combinat` y crear combinaciones de dos con los elementos de $\mathbb{F}_2^3$.

pero antes se realiza una lista escribiendo dos veces los elementos del cuerpo, esto para permitir las parejas con coeficientes repetidos

```
B := FF(2, α) :
k := 2 :
A := B :
for i from 1 by 1 to (k − 1) do
  A := [op(A), op(B)]
end do
```

$$[0, 1, \alpha, 1+\alpha, \alpha^2, 1+\alpha^2, \alpha+\alpha^2, 1+\alpha+\alpha^2, 0, 1, \alpha, 1+\alpha, \alpha^2, 1+\alpha^2, \alpha+\alpha^2, 1+\alpha+\alpha^2]$$

```
with(combinat) :
N := permute(A, 2);
```

$$[[0,1],[0,\alpha],[0,1+\alpha],[0,\alpha^2],[0,1+\alpha^2],[0,\alpha+\alpha^2],[0,1+\alpha+\alpha^2],[0,0],[1,0],[1,\alpha],$$
$$[1,1+\alpha],[1,\alpha^2],[1,1+\alpha^2],[1,\alpha+\alpha^2],[1,1+\alpha+\alpha^2],[1,1],[\alpha,0],[\alpha,1],[\alpha,1+\alpha],$$
$$[\alpha,\alpha^2],[\alpha,1+\alpha^2],[\alpha,\alpha+\alpha^2],[\alpha,1+\alpha+\alpha^2],[\alpha,\alpha],[1+\alpha,0],[1+\alpha,1],[1+\alpha,\alpha],$$
$$[1+\alpha,\alpha^2],[1+\alpha,1+\alpha^2],[1+\alpha,\alpha+\alpha^2],[1+\alpha,1+\alpha+\alpha^2],[1+\alpha,1+\alpha],[\alpha^2,0],$$
$$[\alpha^2,1],[\alpha^2,\alpha],[\alpha^2,1+\alpha],[\alpha^2,1+\alpha^2],[\alpha^2,\alpha+\alpha^2],[\alpha^2,1+\alpha+\alpha^2],[\alpha^2,\alpha^2],[1+\alpha^2,$$
$$0],[1+\alpha^2,1],[1+\alpha^2,\alpha],[1+\alpha^2,1+\alpha],[1+\alpha^2,\alpha^2],[1+\alpha^2,\alpha+\alpha^2],[1+\alpha^2,1+\alpha$$
$$+\alpha^2],[1+\alpha^2,1+\alpha^2],[\alpha+\alpha^2,0],[\alpha+\alpha^2,1],[\alpha+\alpha^2,\alpha],[\alpha+\alpha^2,1+\alpha],[\alpha+\alpha^2,\alpha^2],$$
$$[\alpha+\alpha^2,1+\alpha^2],[\alpha+\alpha^2,1+\alpha+\alpha^2],[\alpha+\alpha^2,\alpha+\alpha^2],[1+\alpha+\alpha^2,0],[1+\alpha+\alpha^2,1],[1$$
$$+\alpha+\alpha^2,\alpha],[1+\alpha+\alpha^2,1+\alpha],[1+\alpha+\alpha^2,\alpha^2],[1+\alpha+\alpha^2,1+\alpha^2],[1+\alpha+\alpha^2,\alpha$$
$$+\alpha^2],[1+\alpha+\alpha^2,1+\alpha+\alpha^2]]$$

Lo siguiente es recorrer la lista anterior, multiplicando cada coeficiente encontrado por x^{p^j}, donde $p = 2$ para $j = 0, 1$.

Más exactamente multiplicar por x y x^2 y luego crear la sumatoria

```
linealizados2 := proc(N, p, k) local i, O, m, todoscero;
 O := [ ];
 for i from 1 by 1 to nops(N) do
     todoscero := true;
     for m from 1 by 1 to k do
         if N[i][m] ≠ 0 then
            todoscero := true;
         end if;
      end do;
      if (N[i][k] ≠ 0 or todoscero = true) then
         O := [op(O), op([[(sum(N[i][j+1]·x^(p·j), j = 0 .. k-1))]])]
      end if;
 end do;
 end proc:
poly := linealizados2(N, 2, 2);
```

$$[x^2, \alpha x^2, (1+\alpha) x^2, \alpha^2 x^2, (1+\alpha^2) x^2, (\alpha+\alpha^2) x^2, (1+\alpha+\alpha^2) x^2, 0, x, x+\alpha x^2, x+(1+\alpha) x^2, x + \alpha^2 x^2, x+(1+\alpha^2) x^2, x+(\alpha+\alpha^2) x^2, x+(1+\alpha+\alpha^2) x^2, x+x^2, \alpha x, \alpha x+x^2, \alpha x+(1+\alpha) x^2, \alpha x+\alpha^2 x^2, \alpha x+(1+\alpha^2) x^2, \alpha x+(\alpha+\alpha^2) x^2, \alpha x+(1+\alpha+\alpha^2) x^2, \alpha x+\alpha x^2, (1+\alpha) x, (1+\alpha) x+x^2, (1+\alpha) x+\alpha x^2, (1+\alpha) x+\alpha^2 x^2, (1+\alpha) x+(1+\alpha^2) x^2, (1+\alpha) x+(\alpha+\alpha^2) x^2, (1+\alpha) x+(1+\alpha+\alpha^2) x^2, (1+\alpha) x+(1+\alpha) x^2, \alpha^2 x, \alpha^2 x+x^2, \alpha^2 x+\alpha x^2, \alpha^2 x+(1+\alpha) x^2, \alpha^2 x+(1+\alpha^2) x^2, \alpha^2 x+(\alpha+\alpha^2) x^2, \alpha^2 x+(1+\alpha+\alpha^2) x^2, \alpha^2 x+\alpha^2 x^2, (1+\alpha^2) x, (1+\alpha^2) x+x^2, (1+\alpha^2) x+\alpha x^2, (1+\alpha^2) x+(1+\alpha) x^2, (1+\alpha^2) x+\alpha^2 x^2, (1+\alpha^2) x+(\alpha+\alpha^2) x^2, (1+\alpha^2) x+(1+\alpha+\alpha^2) x^2, (1+\alpha^2) x+(1+\alpha^2) x^2, (\alpha+\alpha^2) x, (\alpha+\alpha^2) x+x^2, (\alpha+\alpha^2) x+\alpha x^2, (\alpha+\alpha^2) x+(1+\alpha) x^2, (\alpha+\alpha^2) x+\alpha^2 x^2, (\alpha+\alpha^2) x+(1+\alpha^2) x^2, (\alpha+\alpha^2) x+(1+\alpha+\alpha^2) x^2, (\alpha+\alpha^2) x+(\alpha+\alpha^2) x^2, (1+\alpha+\alpha^2) x, (1+\alpha+\alpha^2) x+x^2, (1+\alpha+\alpha^2) x+\alpha x^2, (1+\alpha+\alpha^2) x+(1+\alpha) x^2, (1+\alpha+\alpha^2) x+\alpha^2 x^2, (1+\alpha+\alpha^2) x+(1+\alpha^2) x^2, (1+\alpha+\alpha^2) x+(\alpha+\alpha^2) x^2, (1+\alpha+\alpha^2) x+(1+\alpha+\alpha^2) x^2]$$

Ahora cada uno de los 64 polinomios linealizados de la lista anterior debe evaluar los dos vectores linealmente independientes mencionados antes. Primero es evaluado el vector $(0,1,1)$, cuyo equivalente en el cuerpo es el escalar $\alpha^2+\alpha$, y luego el vector $(1,1,0)$, correspondiente al elemento $1+\alpha$.

$$HH := \left[seq\left(expand\left(\left(eval\left(poly[i], x = \alpha^2 + \alpha \right) \right) \bmod 2 \right) \bmod 2,\ i = 1 \ldots nops(poly) \right) \right]:$$

```
KK := proc(n, x);
        x^n = expand((x^2 + 1)·x^(n - 3));
  end proc:
```

$$SS := seq(KK(j, \alpha), j = 3 \ldots 6):$$

$$\#DD := (subs(SS, HH)) \bmod 2;$$

$$DD := \left(subs\left(\alpha^3 = \alpha^2 + 1, \alpha^4 = \alpha^2 + \alpha^1 + 1, \alpha^5 = \alpha + 1, \alpha^6 = \alpha^2 + \alpha, HH \right) \right) \bmod 2$$

$$\left[1+\alpha,\ \alpha+\alpha^2,\ 1+\alpha^2,\ 1,\ \alpha,\ 1+\alpha+\alpha^2,\ \alpha^2,\ 0,\ \alpha+\alpha^2,\ 0,\ 1+\alpha,\ 1+\alpha+\alpha^2,\ \alpha^2,\ 1,\ \alpha,\ 1+\alpha^2,\ 1,\ \alpha,\ \alpha^2,\ 0,\ 1+\alpha,\ \alpha+\alpha^2,\ 1+\alpha^2,\ 1+\alpha+\alpha^2,\ 1+\alpha+\alpha^2,\ \alpha^2,\ 1,\ \alpha+\alpha^2,\ 1+\alpha^2,\ 0,\ 1+\alpha,\ \alpha,\ \alpha,\ 1,\ \alpha^2,\ 1+\alpha+\alpha^2,\ 0,\ 1+\alpha^2,\ \alpha+\alpha^2,\ 1+\alpha,\ \alpha^2,\ 1+\alpha+\alpha^2,\ \alpha,\ 1,\ 1+\alpha^2,\ 1+\alpha,\ 0,\ \alpha+\alpha^2,\ 1+\alpha,\ 0,\ 1+\alpha^2,\ \alpha+\alpha^2,\ \alpha,\ 1,\ 1+\alpha+\alpha^2,\ \alpha^2,\ 1+\alpha^2,\ \alpha+\alpha^2,\ 1+\alpha,\ 0,\ \alpha^2,\ 1+\alpha+\alpha^2,\ \alpha,\ 1 \right]$$

$$HHH := \left[seq\left(expand\left(\left(eval\left(poly[i], x = 1 + \alpha \right) \right) \bmod 2 \right) \bmod 2,\ i = 1 \ldots nops(poly) \right) \right]:$$

$$DDD := \left(subs\left(\alpha^3 = \alpha^2 + 1, \alpha^4 = \alpha^2 + \alpha^1 + 1, \alpha^5 = \alpha + 1, \alpha^6 = \alpha^2 + \alpha, HHH \right) \right) \bmod 2$$

$$\left[1+\alpha^2,\ 1+\alpha+\alpha^2,\ \alpha,\ 1+\alpha,\ \alpha+\alpha^2,\ \alpha^2,\ 1,\ 0,\ 1+\alpha,\ \alpha^2,\ 1,\ 0,\ 1+\alpha^2,\ 1+\alpha+\alpha^2,\ \alpha,\ \alpha+\alpha^2,\ \alpha+\alpha^2,\ 1+\alpha,\ \alpha^2,\ 1+\alpha^2,\ 0,\ \alpha,\ 1+\alpha+\alpha^2,\ 1,\ 1+\alpha^2,\ 0,\ \alpha,\ \alpha+\alpha^2,\ 1+\alpha,\ 1,\ \alpha^2,\ 1+\alpha+\alpha^2,\ 1,\ \alpha^2,\ \alpha+\alpha^2,\ 1+\alpha,\ 1+\alpha+\alpha^2,\ 1+\alpha^2,\ 0,\ \alpha,\ \alpha,\ 1+\alpha+\alpha^2,\ 1+\alpha^2,\ 0,\ 1,\ \alpha+\alpha^2,\ 1+\alpha,\ \alpha^2,\ 1+\alpha+\alpha^2,\ \alpha,\ 0,\ 1+\alpha^2,\ \alpha^2,\ 1,\ \alpha+\alpha^2,\ 1+\alpha,\ \alpha^2,\ 1,\ 1+\alpha,\ \alpha+\alpha^2,\ 1+\alpha+\alpha^2,\ \alpha,\ 0,\ 1+\alpha^2 \right]$$

Estas dos últimas listas son las imágenes a través de los polinomios linealizados f_i, de los dos vectores linealmente independientes, $v_1 = (0,1,1)$ y $v_2 = (1,1,0)$, ahora lo que queremos es crear los conjuntos de la forma $\{(v_1, f_i(v_1)), (v_2, f_i(v_2))\}$ donde $i = 1, \ldots, 64$.

Para este último paso volvemos a convertir cada elemento en un vector y realizamos una suma externa entre el conjunto $\{v_1, v_2\}$ y el conjunto de imágenes bajo los polinomios $\{f_1, \ldots, f_{64}\}$, para así concluir que cada conjunto $\{(v_1, f_i(v_1)), (v_2, f_i(v_2))\}$ genera un subespacio, es decir, un codeword del código Reed-Solomon sobre $\mathbb{F}_2^3$ con parámetros $[m+l, l, q^{mk}, 2(l-k+1)]$, esto es, un $[5, 2, 64, 2]$-código

```
MM := [seq(subs(α=x, DDD[i]), i=1..nops(DDD))]:
with(PolynomialTools):
VLL := [seq(Vector[row](3, CoefficientVector(MM[i], x)), i=1..nops(MM))]:
AAA := convert(VLL, set):
cartesiano :=proc(A::set, B::set)
local i, j, C:
C := {}:
for i from 1 to nops(A) do
  for j from 1 to nops(B) do
  C := C union {[[op(A)][i], [op(B)][j]]}
 od:
od: C; end:
SSS := cartesiano({[0 1 1]}, AA): SSSS := cartesiano({[1 1 0]}, AAA):
a1 := convert(SSS, list): a2 := convert(SSSS, list):
Subespacios := [seq({a1[i], a2[i]}, i=1..nops(a1))];
```

```
[{[[0 1 1], [0 1 0]], [[1 1 0], [1 1 0]]}, {[[0 1 1], [1 0 0]], [[1 1 0],
  [1 0 1]]}, {[[0 1 1], [1 1 0]], [[1 1 0], [0 0 1]]}, {[[0 1 1], [0 1 1]],
  [[1 1 0], [1 1 1]]}, {[[0 1 1], [1 1 0]], [[1 1 0], [1 0 1]]}, {[[0 1 1],
  [1 0 0]], [[1 1 0], [1 0 0]]}, {[[0 1 1], [0 0 0]], [[1 1 0], [0 1 1]]},
  {[[0 1 1], [1 1 0]], [[1 1 0], [0 1 0]]}, {[[0 1 1], [1 0 1]], [[1 1 0],
  [1 1 0]]}, {[[0 1 1], [1 1 1]], [[1 1 0], [0 0 1]]}, {[[0 1 1], [0 1 0]],
  [[1 1 0], [1 0 1]]}, {[[0 1 1], [0 0 1]], [[1 1 0], [0 0 0]]}, {[[0 1 1],
  [0 1 0]], [[1 1 0], [0 1 1]]}, {[[0 1 1], [0 0 0]], [[1 1 0], [0 0 0]]},
  {[[0 1 1], [0 1 1]], [[1 1 0], [0 0 0]]}, {[[0 1 1], [0 1 1]], [[1 1 0],
  [1 0 1]]}, {[[0 1 1], [0 0 1]], [[1 1 0], [0 1 1]]}, {[[0 1 1], [0 1 1]],
```

$$[[1\ 1\ 0],[1\ 0\ 0]]\},\{[[0\ 1\ 1],[0\ 1\ 0]],[[1\ 1\ 0],[0\ 0\ 0]]\},\{[[0\ 1\ 1],$$
$$[1\ 0\ 1]],[[1\ 1\ 0],[0\ 1\ 1]]\},\{[[0\ 1\ 1],[1\ 1\ 1]],[[1\ 1\ 0],[0\ 1\ 1]]\},$$
$$\{[[0\ 1\ 1],[1\ 1\ 1]],[[1\ 1\ 0],[0\ 0\ 1]]\},\{[[0\ 1\ 1],[1\ 1\ 0]],[[1\ 1\ 0],$$
$$[0\ 1\ 0]]\},\{[[0\ 1\ 1],[1\ 0\ 0]],[[1\ 1\ 0],[0\ 1\ 0]]\},\{[[0\ 1\ 1],[1\ 1\ 0]],$$
$$[[1\ 1\ 0],[1\ 0\ 0]]\},\{[[0\ 1\ 1],[0\ 1\ 0]],[[1\ 1\ 0],[0\ 0\ 0]]\},\{[[0\ 1\ 1],$$
$$[0\ 0\ 0]],[[1\ 1\ 0],[0\ 0\ 0]]\},\{[[0\ 1\ 1],[1\ 0\ 0]],[[1\ 1\ 0],[0\ 0\ 0]]\},$$
$$\{[[0\ 1\ 1],[0\ 0\ 0]],[[1\ 1\ 0],[0\ 1\ 1]]\},\{[[0\ 1\ 1],[1\ 0\ 0]],[[1\ 1\ 0],$$
$$[1\ 1\ 1]]\},\{[[0\ 1\ 1],[1\ 1\ 0]],[[1\ 1\ 0],[0\ 1\ 0]]\},\{[[0\ 1\ 1],[0\ 0\ 0]],$$
$$[[1\ 1\ 0],[1\ 0\ 1]]\},\{[[0\ 1\ 1],[1\ 0\ 1]],[[1\ 1\ 0],[1\ 1\ 1]]\},\{[[0\ 1\ 1],$$
$$[1\ 1\ 1]],[[1\ 1\ 0],[0\ 1\ 0]]\},\{[[0\ 1\ 1],[0\ 0\ 1]],[[1\ 1\ 0],[1\ 0\ 0]]\},$$

$$\{[[0\ 1\ 1],[1\ 0\ 0]],[[1\ 1\ 0],[0\ 0\ 1]]\},\{[[0\ 1\ 1],[0\ 0\ 1]],[[1\ 1\ 0],$$
$$[0\ 0\ 1]]\},\{[[0\ 1\ 1],[1\ 1\ 1]],[[1\ 1\ 0],[1\ 0\ 0]]\},\{[[0\ 1\ 1],[0\ 1\ 0]],$$
$$[[1\ 1\ 0],[1\ 0\ 1]]\},\{[[0\ 1\ 1],[1\ 0\ 0]],[[1\ 1\ 0],[1\ 1\ 0]]\},\{[[0\ 1\ 1],$$
$$[0\ 0\ 0]],[[1\ 1\ 0],[1\ 1\ 0]]\},\{[[0\ 1\ 1],[1\ 0\ 1]],[[1\ 1\ 0],[1\ 1\ 1]]\},$$
$$\{[[0\ 1\ 1],[0\ 1\ 1]],[[1\ 1\ 0],[0\ 1\ 0]]\},\{[[0\ 1\ 1],[0\ 0\ 0]],[[1\ 1\ 0],$$
$$[0\ 1\ 1]]\},\{[[0\ 1\ 1],[1\ 1\ 0]],[[1\ 1\ 0],[1\ 1\ 1]]\},\{[[0\ 1\ 1],[1\ 0\ 1]],$$
$$[[1\ 1\ 0],[1\ 0\ 1]]\},\{[[0\ 1\ 1],[0\ 0\ 1]],[[1\ 1\ 0],[0\ 0\ 0]]\},\{[[0\ 1\ 1],$$
$$[0\ 0\ 1]],[[1\ 1\ 0],[1\ 1\ 1]]\},\{[[0\ 1\ 1],[1\ 1\ 1]],[[1\ 1\ 0],[1\ 0\ 0]]\},$$
$$\{[[0\ 1\ 1],[1\ 0\ 0]],[[1\ 1\ 0],[1\ 1\ 0]]\},\{[[0\ 1\ 1],[1\ 0\ 1]],[[1\ 1\ 0],$$
$$[1\ 0\ 0]]\},\{[[0\ 1\ 1],[1\ 1\ 1]],[[1\ 1\ 0],[1\ 0\ 0]]\},\{[[0\ 1\ 1],[1\ 1\ 0]],$$

$$[[1\ 1\ 0],[1\ 1\ 0]]\},\{[[0\ 1\ 1],[0\ 1\ 0]],[[1\ 1\ 0],[0\ 1\ 0]]\},\{[[0\ 1\ 1],$$
$$[0\ 0\ 1]],[[1\ 1\ 0],[0\ 0\ 1]]\},\{[[0\ 1\ 1],[0\ 1\ 1]],[[1\ 1\ 0],[0\ 1\ 1]]\},$$
$$\{[[0\ 1\ 1],[0\ 1\ 0]],[[1\ 1\ 0],[1\ 1\ 0]]\},\{[[0\ 1\ 1],[0\ 1\ 1]],[[1\ 1\ 0],$$
$$[0\ 1\ 0]]\},\{[[0\ 1\ 1],[1\ 0\ 1]],[[1\ 1\ 0],[0\ 0\ 1]]\},\{[[0\ 1\ 1],[1\ 0\ 1]],$$
$$[[1\ 1\ 0],[1\ 0\ 1]]\},\{[[0\ 1\ 1],[0\ 0\ 0]],[[1\ 1\ 0],[1\ 1\ 0]]\},\{[[0\ 1\ 1],$$
$$[1\ 1\ 1]],[[1\ 1\ 0],[0\ 0\ 1]]\},\{[[0\ 1\ 1],[0\ 0\ 1]],[[1\ 1\ 0],[1\ 1\ 1]]\},$$
$$\{[[0\ 1\ 1],[0\ 1\ 1]],[[1\ 1\ 0],[1\ 1\ 1]]\}]$$

Bibliografía & Referencias

[1] E. R. Berlekamp. *Algebraic Coding Theory.*New York: McGrawHill, (1968).

[2] E. R. Berlekamp. *The technology of error-correcting codes.*IEEE, vol. 68, 564-593,May (1980).

[3] E. A. Brouwer, A. M. Cohen y A. Neumaier. *Distance-regular graph.*New York: Springer-Verlag, (1989).

[4] E.M. Gabidulin. *Theory of codes with maximum rank distance.* Probl. Inform. Transm., vol 21, 1-12, Julio (1985).

[5] I. Gutiérrez. *Teoría de códigos, Notas de clase,* 15-66, 71-79, (2011).

[6] R. Koetter, F. R. Kschischang. A *Coding for Errors and Erasures in Random Network Coding,* IEEE Transactions on Information Theory, Volumen 54, (2008).

[7] R. Lidl y H. Niederreiter. *Finite Fields.* in the encyclopedia of mathematics, G.-C. Rota, Ed. Reading, MA: Addison-Wesley, 1983, vol 20.

[8] F. J. MacWilliams y N. J. A. Sloane. *Tje theory of error-correcting codes.*New York: North-Holland, (1977).

[9] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong. *A random linear network coding approach to multicast,* IEEE Trans. Inf. Theory, vol. 52, no. 10, 4413-4430,Oct. (2006).

[10] R. M. Roth. *Introduction to coding theory* .Cambridge Univ. (2006).

[11] D. Silva and F. R. Kschischang y R. Koetter*A rank-metric approach to error-control in random network coding.*IEEE Trans, inf. Theory[Online]. Available: http://arxiv.org/abs/0711.0708.

[12] M. J. Soto. *Notas preliminares del master en estudios avanzados de matemáticas.* Curvas y códigos algebraicos, Universidad de Sevilla (2009).

[13] J. H. van Lint y R. M. Wilson. *A course in combinatorics,* 2da ed. Cambridge, U.K.:Cambridge Univ, (2001).

[14] H. Wang, C. Xing y R. Safavi-Naini. *Linear authentication codes:*

bounds and constructions.IEEE trans. inf. Theory, vol. 49, no. 4, 866-872, Abril (2003).