Construcción de Códigos Lineales Proyectivos que alcanzan la cota de Griesmer.

Tesis
entregada a la
Universidad de Chile
en cumplimiento parcial de los requisitos
para optar al grado de
Magíster en Ciencias con mención en Matemáticas

Facultad de Ciencias
por

Vania Ramírez Bustamante

Enero, 2010

Director de Tesis: Dr. Antonio Behn

FACULTAD DE CIENCIAS

UNIVERSIDAD DE CHILE

INFORME DE APROBACIÓN

TESIS DE MAGISTER

Se informa a la Escuela de Postgrado de la Facultad de Ciencias que la Tesis de Magíster presentada por el candidato

Vania Ramírez Bustamante

Ha sido aprobada por la Comisión de Evaluación de la tesis como requisito para optar al grado de Magíster en Ciencias con mención en Matemáticas, en el examen de Defensa de Tesis rendido el día 27 de enero de 2010 .

Director de Tesis:

Dr. Antonio Behn .....

Comisión de Evaluación de la Tesis

Dr. Anita Rojas .....

Dr. Víctor González-Aguilera .....

A mi Mami.

Agradecimientos

Agradezco a mis padres y hermanos por todo el amor que desde siempre me han brindado, por esa fe ciega que tiene en mi, y ese apoyo incondicional.

También quero agradecer a mi esposo, que ha estado en las buenas y las malas siempre a mi lado, que ha sabido sostenerme y aguantarme en esos momentos en que todo sale mal y lo más importante que ha llenado mi corazón de alegrías y amor.

No puedo dejar de agradecer a los profesores que han estado presentes en todo este proceso de aprendizaje. Muy especialmente, quiero agradecer a Renato Lewin y Angel Carocca que estuvieron siempre guiándome y apoyandome en mi etapa de licenciatura, y también a mi tutor Antonio Behn que supo guiarme en este largo trabajo.

Quero agradecer a todos mis amigos, del colegio, de la iglesia, de la universidad, que a pesar de que en este largo proceso aveces me he "desaparecido" me han hecho sentir que siempre van a estar a mi lado.

Y sobre todo quero dar gracias a Dios que me ha dado la oportunidad de conocer lo que son las Matemáticas.

Índice general

Resumen

Uno de los objetivos que se busca en la teoría de códigos es encontrar un $[n, k, d]_q$-código tal que la longitud de éste sea mínima con respecto a los parámetros fijos k,d y q.

En esta tésis estudiaremos algoritmos para la construcción de $[n, k, d]_q$-códigos donde k, d y q están fijos. Esto con el fin de encontrar todos los posibles n, de modo que dicho código exista. Procederemos relacionando la búsqueda de matrices generadoras de $[n, k, d]_q$- códigos con estructuras definidas en la geometría proyectiva finita. En particular estudiaremos los llamados minihypers.

Nuestro objetivo es utilizar estos algoritmos para mostrar $[n, k, d]_q$-códigos que alcanzen la cota de Griesmer.

Summary

One of the goals in the theory of codes is to find $[n, k, d]_q$-codes with minimal length n for fixed values of the parameters k, d and q.

In this tesis we study algorithms to construct the $[n, k, d]_q$-codes, where k,d, and q are fixed. This has the purpose of finding every possible n, such that this code exist. We will proceed relating the search of matrix generator of $[n, k, d]_q$-codes with defined structures, in the finite projective geometry. In particular, we will study what it are called minihypers.

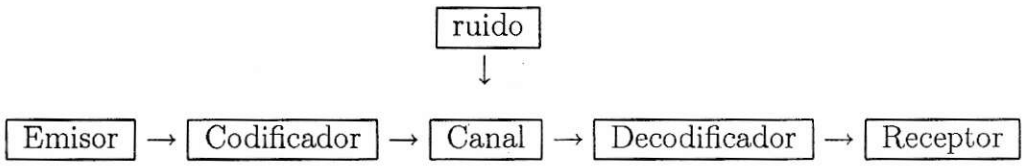
Our objetive is to use these algorithms for showing $[n, k, d]_q$-codes that reach Greismer's bound.

Introducción

Uno de los objetivos de la teoría de códigos es la construcción de códigos para:

- La transmisión de información.
- Detectar errores en la transmisión.
- Corregir el mayor número posible de éstos.

En este trabajo nos centraremos en estudiar cuál es la mejor manera de codificar para poder detectar la mayor cantidad de errores que se producen en la transmisión, y para poder corregir el mayor número posible de éstos.
Con el objetivo de corregir o detectar errores en la transmisión, a los códigos se les añade redundancia con lo que se pierde eficiencia. Pero esta es la manera natural de conseguir este fin. Por ejemplo, los lenguajes naturales tienen una gran cantidad de redundancia, lo que permite entender una conversación telefónica a pesar de que haya errores en la transmisión.
Esta forma de codificación se usa cuando se realiza una transmisión por un canal ruidoso, es decir un canal que está sujeto a perturbaciones y que genera alteraciones en el mensaje (ejemplos de canales: atmósfera, línea telefónica,etc.), y funcionan de tal forma que cuando se produzca un error, la palabra resultante no sea una palabra del código y que la palabra real sea la más próxima a la palabra recibida.



En particular, nos restringiremos al estudio de códigos lineales. Un **código lineal** C corresponde a un subespacio de $\mathbb{F}_q^n$ sobre $\mathbb{F}_q$, y es denotado por $[n,k]_q$-código, donde k es la dimensión de C sobre $\mathbb{F}_q$. A los elementos de C

los llamaremos **palabras**.

Debido a que estos códigos son subespacios de dimensión finita, los podemos caracterizar a través de cualquiera de sus bases. De este modo, un código lineal C se puede representar por medio de una matriz Γ tal que el conjunto de filas de ésta, sea una base sobre $\mathbb{F}_q$ del subsepacio C. A esta matriz la llamamos **matriz generadora** de C. Si la matriz generadora de un código no posee columnas de ceros, a este código se le llama **código proyectivo**.

Dotaremos al espacio $\mathbb{F}_q^n$ de una distancia llamada **distancia de Hamming**. Se define como el número de coordenadas en que dos elementos $x, y \in \mathbb{F}_q^n$ difieren. Una característica importante a destacar es la distancia más pequeña entre dos palabras distintas de C, la cual es muy importante para la detección de errores. A esta distancia la llamamos **distancia mínima** de C. Si d es la distancia mínima de C, lo llamamos $[n, k, d]_q$**-código**.

Como ya mencionamos al comienzo de la introducción, la forma que ocuparemos para decodificar una palabra es escoger la palabra $c \in C$ más cercana a la palabra recibida, con respecto a la métrica de Hamming, es decir, y es decodificado en una palabra $c \in C$, si

$$d(c, y) \leq d(c', y) \qquad \forall \quad c' \in C$$

El problema se produce cuando la palabra más cercana a y no es la palabra enviada. Es por este motivo que estudiaremos cuantos son los errores que se pueden cometer en la transmisión de un mensaje para poder detectar o corregir éstos; es aquí donde nos ayuda el conocimiento de la distancia mínima del código.
Debido a que las bolas centradas en cada palabra $c \in C$ con radio $t = \frac{d-1}{2}$ son disjuntas, si el vector $y \in F_q^n$ recibido tiene a lo más t errores, podemos decodificarlo sin dificultades.

Este es el problema que nos motiva, ya que si la distancia mínima de un código lineal es mayor, podremos detectar o corregir mayor cantidad de errores en los mensajes recibidos.

Es por esto que nosostros estamos en búsqueda de códigos optimales, donde C es un $[n, k, d]_q$**- código optimal** si no existe un $[n, k, d']_q$-código con $d' > d$. Existen resultados teóricos que dan cotas a los diferentes parámetros

de un $[n, k, d]_q$-código, como lo es la **cota de Griesmer** dada por

$$n \geqslant \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil$$

donde $\lceil x \rceil$ denota la función que asigna a x el mayor entero más cercano a x.
Tal como su nombre lo dice, este trabajo representa un estudio sobre la construcción de códigos lineales proyectivos, siendo nuestro principal objetivo estudiar la construcción de códigos que alcanzen la cota de Griesmer, que podemos encontrar en [3].

Los párrafos siguientes describen los principales temas a tratar en este trabajo.

Comenzamos en el capítulo 1 mostrando los conceptos básicos utilizados en la teoría de códigos [1], y las diferentes cotas que existen para los parámetros de un $[n, k, d]_q$-código [2].

En el capítulo 2 estudiamos las isometías lineales entre códigos lineales y mostramos como contar las clases de isometría lineal para n, k y q fijos [2].

En el capítulo 3 analizamos las características que posee la matriz generadora de un código lineal de distancia mínima d fija e introducimos los conceptos de minihypers, t-bloques y grafos que son necesarios para construirlas [2].

Finalmente en el capítulo 4, con la ayuda de la Geometría proyectiva finita estudiaremos algunos teoremas [10] que nos servirán para demostrar la existencia de códigos lineales que alcanzen la cota de Griesmer, y la no existencia en ciertos casos de códigos que la alcanzen.

Capítulo 1

Conceptos Básicos

1.1. Codificación

Definición 1.1.1. Un alfabeto es un conjunto finito $A = \{a_1, ..., a_q\}$. Una palabra de longitud n sobre A es una sucesión de n elementos de A, que denotaremos por

$$a = a_{i_1} a_{i_2} ... a_{i_n} \quad \text{con} \quad a_{i_j} \in A$$

Al conjunto de tales palabras lo denotaremos por A^n y por A^* al conjunto de todas las palabras sobre A.

Definición 1.1.2. Si $A = \{a_1, ..., a_q\}$ es un alfabeto, un código q-ario sobre A es un subconjunto C de A^* . Si el tamaño de C es $\mid C \mid = M$ y todas las palabras de C tienen longitud fija n decimos que C es un (n, M)-código.

Nosotros sabemos que en realidad cuando enviamos un mensaje a través de un canal, es casi imposible que este no posea ruidos, es decir que no se produzcan errores de transmisión, en estos casos hay que utilizar alguna técnica para poder saber cuál fue el mensaje enviado. Con este objetivo, vamos a definir una distancia para A^n.

Definición 1.1.3. (Distancia de Hamming) Sean x e $y \in A^n$, la distancia de Hamming entre x e y, denotada por $d(x, y)$, se define como el número de coordenadas en que x e y difieren, es decir

$$\begin{aligned} d: \quad A^n \times A^n &\longrightarrow \{1, 2, ..., n\} \\ (x, y) &\longmapsto |\{i \in \{1, 2, ..., n\} \mid x_i \neq y_i\}| \end{aligned}$$

Proposición 1.1.4. *La función d es una distancia en A^n.*

DEMOSTRACIÓN: Es claro que $d(x,y) \geqslant 0$ y $d(x,y) = 0$ si y sólo si $x = y$, también que $d(x,y) = d(y,x)$ para todo x e $y \in A^n$. Lo que nos falta demostrar es $d(x,y) \leqslant d(x,z) + d(z,y)$ para todo x, z e $y \in A^n$.

Sean $T_1 = \{i \mid x_i \neq y_i\}$, $T_2 = \{i \mid x_i \neq z_i\}$, $T_3 = \{i \mid z_i \neq y_i\}$,
$V_1 = \{i \mid x_i \neq y_i \text{ y } x_i = z_i\}$ y $V_2 = \{i \mid x_i \neq y_i \text{ y } x_i \neq z_i\}$ notemos que $d(x,y) = \mid T_1 \mid$, $d(x,z) = \mid T_2 \mid$ y $d(z,y) = \mid T_3 \mid$, además
$T_1 = V_1 \cup V_2$, $V_2 \subseteq T_2$ y $V_1 \subseteq T_3$, por lo cual $V_1 \cup V_2 \subseteq T_2 \cup T_3$ lo que implica

$$\mid V_1 + V_2 \mid = d(x,y) \leqslant \mid T_2 \cup T_3 \mid \leqslant \mid T_2 \mid + \mid T_3 \mid = d(x,z) + d(z,y)$$

□

Definición 1.1.5. Dado un código C se define la distancia mínima de C, denotada por $d(C)$,como la menor distancia no-nula entre sus palabras.
Un (n, M, d)-código es un código de longitud n, tamaño M y distancia mínima d.

Para codificar y decodificar de manera más práctica y eficiente es útil dotar al alfabeto A de cierta estructura algebraica. Es común considerar a A como un cuerpo finito aunque también se lo puede considerar como un anillo. De ahora en adelante, fijamos $A = \mathbb{F}_q$, el cuerpo finito de q elementos.

Definición 1.1.6. Un código lineal q-ario de longitud n y rango k es un subespacio $C \leq \mathbb{F}_q^n$ de dimensión k. En este caso decimos que C es un $[n,k]_q$ -código. Si C tiene distancia mínima $d(C) = d$, entonces decimos que C es un $[n,k,d]_q$ -código.

Definición 1.1.7. Dado $x \in \mathbb{F}_q$ se define el peso de x, denotado por $w(x)$, como el número de coordenadas no-nulas de x. Se define el peso mínimo de C denotado por $w(C)$, como el mínimo de los pesos de las palabra no-nulas de C.

Proposición 1.1.8. *Si C es un código lineal entonces $d(C) = w(C)$.*

DEMOSTRACIÓN: Como C es lineal, tenemos

$$d(C) = \min_{x \neq y \in C} d(x,y) = \min_{x \neq y \in C} w(x-y) = \min_{x \neq 0 \in C} w(x) = w(C)$$

□

Proposición 1.1.9. *El codificador de un $[n,k]_q-$código, es una función lineal e inyectiva $\gamma : \mathbb{F}^k \longrightarrow \mathbb{F}^n$. Esta función puede ser representada por una matriz Γ de rango k, la cual no está únicamente determinada, ya que depende de la base en la que trabajemos.*

Definición 1.1.10. Sea C un $[n,k]_q$-código, llamamos matriz generadora de C a una $(k \times n)$-matriz Γ, tal que

$$C = \{v\Gamma \mid v \in \mathbb{F}^k\}$$

Teorema 1.1.11. *El conjunto de todas las matrices generadoras de un $[n,k]_q$-código, con matriz generadora Γ es*

$$\{B\Gamma \mid B \in GL_k(q)\}$$

donde $GL_k(q)$ es el conjunto de todas la $k \times k$-matrices invertibles sobre $\mathbb{F}_q$.

Otra manera de caracterizar un $[n,k]_q$-código C es a través de la **matriz de control**, que se define como la matriz asociada a la transformación lineal, que posee como núcleo al código C. Al igual que la matriz generadora, la $(n-k) \times n$ - matriz de control no esta únicamente determinada.

Definición 1.1.12. Sea C un $[n,k]_q$-código, llamamos matriz de control de C a una matriz H, tal que

$$C = \{x \in \mathbb{F}_q^n \mid Hx^t = 0\}$$

Definición 1.1.13. Al conjunto de todos los $[n,k]_q$- códigos lo denotaremos por

$$U[n,k]_q = \{U \leq \mathbb{F}_q^n \mid dim(U) = k\}, \text{ con } 1 \leq k \leq n$$

Al espacio métrico $(\mathbb{F}_q^n, d)$ lo llamaremos espacio métrico de Hamming de dimensión n sobre $\mathbb{F}_q$ y lo denotaremos por $\mathbb{H}[n,q]$.

Observación 1.1.14. Recordemos que la **Grassmanniana** se define como el conjunto que contiene todos los subespacios lineales, de un espacio vectorial V de una dimensión fija k, y se denota por $Gr_k(V)$. En particular el conjunto $U[n,k]_q$ coincide con la grassmanniana $Gr_k(\mathbb{F}_q^n)$.

1.2. Decodificación

Al enviar una palabra de un código a través de un canal, esta palabra puede perturbarse, lo cual trae como consecuencia que la palabra recibida

posea algún error. Nuestro objetivo es detectar o corregir estos errores, es por esta razón que en esta sección estudiaremos de qué factores depende el que podamos detectar que se produjo algún error o el que podamos corregir estos errores.

Si $D \subseteq \mathbb{F}_q^n$ es un conjunto de palabras de un código lineal C enviados a través de un canal, podemos encontrar algunas palabras que sufrieron perturbación, ocupando la matriz de control de C. Es importante notar que con este procedimiento no encontramos todas las palabras que tuvieron alguna perturbación al enviarlas, ya que la palabra recibida, aunque posea errores, puede pertenecer al código C.

Definición 1.2.1. Sea C un $[n,k]_q$-código, y sea $y \in \mathbb{F}_q^n$ el vector recibido al enviar una palabra $c \in C$ a través de un canal, decimos que y posee r errores si $d(c,y) = r$.

La forma más natural de corregir errores, es que si $y \in \mathbb{F}_q^n$ es el vector recibido buscamos una de las palabras $c \in C$ más cercanas a y, con respecto a la métrica de Hamming, es decir, y es decodificado en una palabra $c \in C$, si

$$d(c,y) \leq d(c',y) \qquad \forall \quad c' \in C$$

A esta forma de decodificar se le llama **decodificación por distancia mínima**. Los problemas se producen cuando hay más de una palabra $c \in C$ que cumple con que $d(c,y) \leq d(c',y)$ para todo $c' \in C$ y cuando la palabra más cercana a y no es la palabra enviada.

Es por este motivo que estudiaremos cuantos son los errores que se pueden cometer en la transmisión de un mensaje para poder detectar o corregir éstos; es aquí donde nos ayuda el conocimiento de la distancia mínima del código.

Definición 1.2.2. Dado $x \in A^n$, con $|A| = q$ y $r \geqslant 0$, se define la esfera de radio r centrada en x como

$$S_q(x,r) = \{y \in A^n \mid d(x,y) = r\}$$

y la bola de radio r centrada en x como

$$B_q(x,r) = \{y \in A^n :| \, d(x,y) \leqslant r\} = \bigcup_{i=0}^{r} S_q(x,i)$$

Se define el volumen $V_q(n,r)$ como el cardinal de una bola de radio r en A^n . Luego

$$V_q(n,r) = \mid B_q(n,r) \mid = \sum_{i=0}^{r} \mid S_q(x,i) \mid = \sum_{i=0}^{r} \binom{n}{k} (q-1)^i$$

Veamos que las bolas de radio $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ centradas en palabras del códigos son disjuntas.

Teorema 1.2.3. *Sea C un $[n,k,d]_q$-código y sea $t = \left\lfloor \frac{d-1}{2} \right\rfloor$, entonces las bolas $B_q(c,r)$ son disjuntas $\forall\ c \in C$, donde $\lfloor x \rfloor$ denota la función parte entera de x.*

DEMOSTRACIÓN: Sea $z \in B_q(c_1,t) \cap B_q(c_2,t)$ con c_1 y $c_2 \in C$, luego

$$d(c_1,c_2) \leq d(c_1,z) + d(c_2,z) \leq 2t < d$$

pero como d es la distancia mínima entre dos palabras de C, podemos concluir que $c_1 = c_2$, y así $B_q(c_1,t) = B_q(c_2,t)$.

□

Como las bolas $B_q(c,t)$ son disjuntas para todo $c \in C$, tenemos que si el vector $y \in F_q^n$ recibido tiene a lo más t errores, podemos decodificarlo sin problema.

Corolario 1.2.4. *Si C es un $[n,k,d]_q$ código :*

(i) Podemos detectar si una palabra $c \in C$ al enviarla a través de un canal tuvo perturbaciones si la palabra recibida posee a lo más $d-1$ errores.

(ii) Si una palabra $c \in C$ al enviarla a través de un canal tuvo perturbaciones podemos corregirla si esta posee a lo más $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ errores. Es por esta razón que un código a veces es llamado código t-corrector de errores.

DEMOSTRACIÓN:

(i) Sea $c \in C$ el mensaje enviado e $y \in \mathbb{F}_q^n$ el mensaje recibido, si suponemos que a lo más se produjeron $d-1$ errores tenemos que $d(c,y) < d$, lo que implica que $y \notin C$, por lo tanto podemos detectar que se produjeron errores en la transmisión. Mientras si suponemos que se produjeron más de $d-1$ errores tenemos que $d(c,y) \geqslant d$, lo que implica que y puede pertenecer al código C y en este caso no podríamos siempre detectar que se produjeron errores en la transmisión.

(ii) Sea $c \in C$ el mensaje enviado e $y \in \mathbb{F}_q^n$ el mensaje recibido, si suponemos que a lo más se produjeron $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ errores, tenemos por el teorema anterior que las bolas de radio t centradas en palabras del códigos son disjuntas, lo que implica que la palabra del código más cercana a y es c, por lo cual podemos corregir los errores que se produjeron en la transmisión. Mientras si suponemos que se produjeron más de t errores tenemos que $y \notin B_q(c,t)$, lo que implica que la palabra del código más cercana a y no es c, por lo cual si corrigiéramos los errores que se produjieron en la transmisión, no decodificaríamos correctamente.

□

Es importante notar que (i) y (ii) no se pueden hacer simultáneamente, sino que tenemos que decidir si vamos a detectar errores o los vamos a corregir.

Ejemplo 1.2.5. *Sea* $C = \{000000, 111111\}$ *el código lineal sobre* $\mathbb{F}_2$ *generado por la matriz* $\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$. *Este es un* $[6,2,5]_2$*-código, por la proposición anterior el puede detectar 4 errores o puede corregir 2 errores.*

1. *Si al enviar una palabra de* C *recibimos la palabra* (111000)*,como*

$$d(111000, 000000) = d(111000, 111111) = 3$$

sólo podemos detectar que esta palabra posee 3 errores.

2. *Si al enviar una palabra de* C *recibimos la palabra* (110000)*,como*

$$d(110000, 000000) = 2 \leqslant d(110000, 111111) = 4$$

podemos detectar que esta palabra posee 2 o 4 errores. También podemos decidir corregirla, pero en este caso asumimos que son 2 los errores que se cometieron, corrigiéndola como la palabra (000000).

3. *Si al enviar una palabra de C recibimos la palabra* (100000), *como*

$$d(100000, 000000) = 1 \leqslant d(100000, 111111) = 5$$

podemos detectar que esta palabra posee 1 o 5 errores. También podemos decidir corregirla, pero en este caso asumimos que es 1 el error que se cometió, corrigiéndola como la palabra (000000).

Estos son los problemas que nos motivan, ya que si la distancia mínima de un código es mayor podremos detectar o corregir mayor cantidad de errores. Es por esto que nosotros estamos en búsqueda de códigos que posean la mayor distancia mínima posible, para parámetros fijos n, k, q.
La siguiente proposición nos ayudará a definir lo que es un código optimal.

Proposición 1.2.6. *Si existe un $[n, k, d]_q$-código con $1 < d$, entonces para todo $1 < d' < d$ existe un $[n, k, d']_q$-código.*

DEMOSTRACIÓN: Sea C un $[n, k, d]_q$-código con $1 < d$ y sea Γ una matriz generadora de C de la forma, $\Gamma = (I_k \mid u_1^t \mid ... \mid u_{n-k}^t)$ donde I_k es la matriz identidad de orden k y $u_j \in \mathbb{F}_q^k$, si reemplazamos cualquier columna u_j^t por una columna de ceros, tenemos que el código generado por esta nueva matriz es un $[n, k, d]_q$-código o un $[n, k, d-1]_q$-código. Si vamos reemplazando una por una cada columna de Γ por columnas de ceros, paso a paso la distancia mínima se conserva o disminuye en 1, hasta llegar a obtener una matriz de la forma $\Gamma = (I_k \mid 0)$, la cual genera un $[n, k, 1]_q$-código.

□

Así llegamos a la definición de código optimal

Definición 1.2.7. Sea C un $[n, k, d]_q$- código, decimos que C es un código optimal si no existe un $[n, k, d+1]_q$-código.

Existen resultados teóricos que dan cotas para

$$d_{max}[n, k, q] = \text{máx}\{d \mid \text{ exista un } [n, k, d]_q\text{- código}\}$$

$$n_{min}[k, d, q] = \text{mín}\{n \mid \text{ exista un } [n, k, d]_q\text{- código}\}$$

En general se busca maximar la distancia del código, es decir se busca $d_{max}[n, k, q]$, pero una condición más fuerte es minimizar la longitud de éste.

Proposición 1.2.8. *Si C es un $[n, k, d]_q$-código con $n = n_{min}[k, d, q]$ entonces $d = d_{max}[n, k, q]$.*

DEMOSTRACIÓN: Sea C un $[n,k,d]_q$-código con $n = n_{min}[k,d,q]$ y supongamos que $d \neq d_{max}[n,k,q]$, es decir existe un $[n,k,d+1]_q$-código C'.

Sea $\Gamma' = (\gamma_i^t)$ con $i \in \{1...n\}$, la matriz generadora de C', sin perdida de generalidad podemos suponer que γ_1 es un vector con coordenadas distintas de cero, luego si formamos la matriz $\Gamma = (\gamma_i^t)$ con $i \in \{2...n\}$ ésta genera un $[n-1,k,d]_q$-código lo que contradice, que $n = n_{min}[k,d,q]$.

□

Es por este motivo que en este trabajo siempre buscaremos al $n_{min}[k,d,q]$.

Las cotas que estudiaremos son

Teorema 1.2.9. *(Cota de Singleton)[2] Si C es un $[n,k,d]_q$-código, se cumple*

$$d \leqslant n - k + 1$$

Los $[n,k,d]_q$-códigos que alcanzan esta cota se les llaman **códigos** MDS.

Teorema 1.2.10. *(Cota de Plotkin)[2] Si C es un $[n,k,d]_q$ código, se cumple*

$$d \leqslant \frac{nq^{k-1}(q-1)}{q^k - 1}$$

Teorema 1.2.11. *(Cota de Hamming)[2] Si C es un $[n,k,d]_q$-código y sea $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ entonces*

$$q^k \sum_{i=0}^{t} \binom{n}{i} (q-1)^i \leqslant q^n$$

A esta cota también se le llama **Cota de empaquetamiento de esferas.** Cuando un $[n,k,d]_q$-código alcanza esta cota se le llama **código perfecto.**

Teorema 1.2.12. *(Cota de Griesmer)[2] Todo $[n,k,d]_q-$código, satisface que:*

$$n \geqslant \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil$$

donde $\lceil x \rceil$ denota la función que asigna a x el mayor entero más cercano a x.

Existen algunos casos en que se ha demostrado que no existen códigos que alcancen estas cotas, como por ejemplo en [5] se demuestra que no existe un $[116, 5, 85]_4$-código, es decir para $q = 4$, $k = 5$ y $d = 85$ no se alcanza la cota de Griesmer dada por

$$\sum_{i=0}^{4} \left\lceil \frac{85}{4^i} \right\rceil = 85 + \left\lceil \frac{85}{4} \right\rceil + \left\lceil \frac{85}{16} \right\rceil + \left\lceil \frac{85}{64} \right\rceil + \left\lceil \frac{85}{256} \right\rceil = 85 + 22 + 6 + 2 + 1 = 116.$$

También existen casos en que aún no se conoce algún código que las alcance, que podemos encontrar en [3]. Es por este motivo que estudiaremos las maneras de construir $[n, k, d]_q$-códigos con k y q fijos, para luego fijar nuestro objetivo en encontrar $[n_{min}[k, d, q], k, d]_q$-códigos.
Si comparamos la cota de Singleton con la cota de Griesmer notamos que

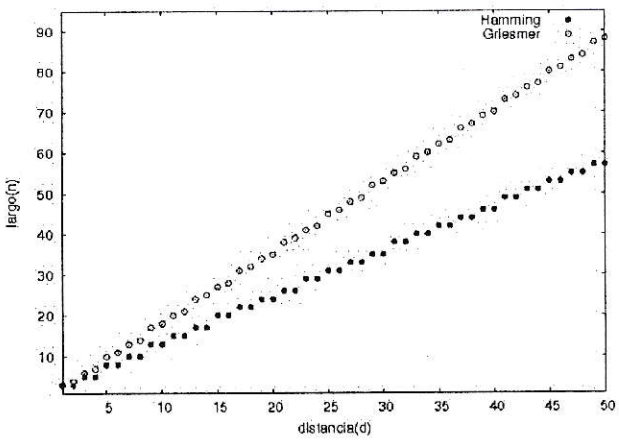
$$n \geqslant \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil \geqslant d + (k-1) \left\lceil \frac{d}{q^i} \right\rceil \geqslant d + k - 1$$

la cota de Singleton está por abajo de la cota Griesmer. Al igual que la cota de Plotkin, ya que

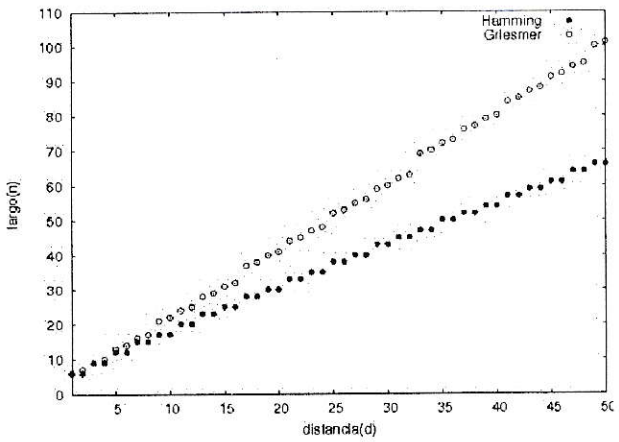
$$n \geqslant \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil \geqslant \sum_{i=0}^{k-1} \frac{d}{q^i} = \frac{d(q^k - 1)}{q^{k-1}(q-1)}.$$

Ahora lo que nos falta, es ver como se comporta la cota de Hamming con respecto a la de Griesmer, y esto lo haremos a través de gráficos.

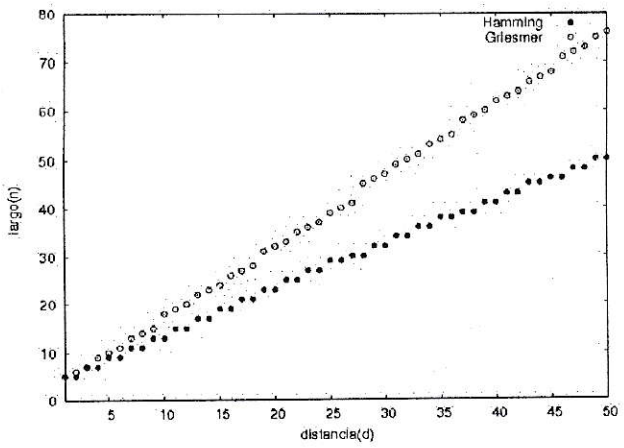
$q = 2,\ k = 3$



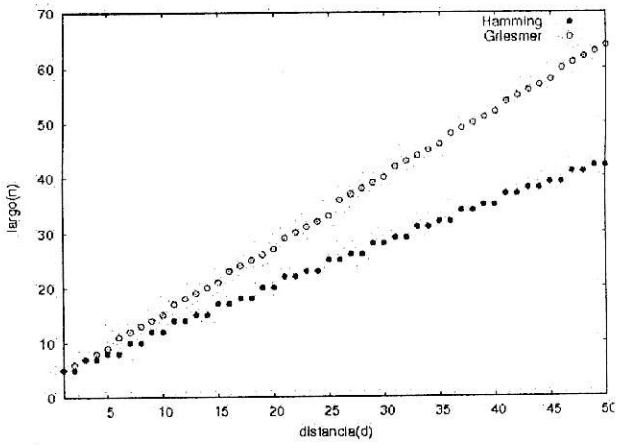
$q = 2,\ k = 6$



$q = 3,\ k = 5$



$q = 5,\ k = 5$



En estos gráficos podemos notar que la cota de Hamming también en la mayoría de los casos va por debajo que la cota de Griesmer. Es por este motivo que la cota que mayormente nos servirá para encontrar este $n_{min}[k, d, q]$ es la cota de Griesmer, y ésta será con la que trabajaremos.

Capítulo 2

Isometrías Lineales

2.1. Caracterización

Antés de comenzar con la construcción de $[n,k]_q$-códigos, nos centraremos en estudiar cuando dos códigos lineales son esencialmente el mismo, para que en el proceso de construir códigos veamos si podemos descartar algunos códigos que posean las mismas características, o bien distinguir cuando construimos códigos nuevos.

Con este propósito estudiaremos isomorfismos de espacios vectoriales, pero no olvidemos que los espacios vectoriales en los cuales estamos trabajando ya los dotamos de una métrica, dándoles una estructura de espacio métrico, por lo cual también debemos respetar la distancia en este espacio. Es por esto que las funciones que vamos a estudiar son las isometrías lineales en el espacio métrico $(\mathbb{F}_q^n, d)$, denotado por $\mathbb{H}[n,q]$.

Definición 2.1.1. Dos $[n,k]_q$- códigos lineales $C, C' \subseteq \mathbb{H}[n,q]$ son isométricos si existe una función $\tau : \mathbb{H}[n,q] \longrightarrow \mathbb{H}[n,q]$ tal que $\tau(C) = C'$ y

$$d(u,v) = d(\tau(u), \tau(v)) \qquad \forall\, u, v \in \mathbb{H}[n,q]$$

esta función τ la llamamos isometría en $\mathbb{H}[n,q]$.

Un tipo de isometría en $\mathbb{H}[n,q]$, son las isometrías lineales.

Definición 2.1.2. Dos $[n,k]_q$-códigos $C, C' \subseteq \mathbb{H}[n,q]$ son linealmente isométricos, si existe una isometría lineal $\tau : \mathbb{H}[n,q] \longrightarrow \mathbb{H}[n,q]$ tal que $\tau(C) = C'$.

Un ejemplo de éstas son las llamadas isometrías permutacionales, las cuales sólo permutan las coordenadas de cada palabra $c \in C$, y se definen como sigue.

Definición 2.1.3. Dos $[n,k]_q$-códigos $C, C' \subseteq \mathbb{H}[n,q]$ son permutacionalmente isométricos, si existe una permutación $\sigma \in S_n$ tal que $C' = P_\sigma(C)$ donde

$$P_\sigma(C) = \{P_\sigma(c) = (c_{\sigma^{-1}(0)}, ..., c_{\sigma^{-1}(n-1)}) \mid c \in C\}$$

esta función $P_\sigma : \mathbb{H}[n,q] \longrightarrow \mathbb{H}[n,q]$ es llamada isometría permutacional.

Observación 2.1.4. Como las isometrías a las que dedicaremos nuestra atención son las isometrías lineales en $\mathbb{H}[n,q]$, siempre que en nuestro trabajo, digamos que dos $[n,k]_q$-códigos son isométricos, nos referimos a que son linealmente isométricos en $\mathbb{H}[n,q]$

Así como las isometrías permutacionales las pudimos caracterizar, ahora intentaremos caracterizar las isometrías lineales en $\mathbb{H}[n,q]$ en general .
Para caracterizar estas isometrías, tenemos que estudiar las funciones lineales del espacio vectorial $\mathbb{F}_q^n$ y analizar sus efectos en la distancia de Hamming, es decir estudiar las funciones lineales en $\mathbb{H}[n,q]$.

Observación 2.1.5. Si $\tau : \mathbb{H}[n,q] \longrightarrow \mathbb{H}[n,q]$ es una isometría lineal, tenemos que

$$w(v) = d(v,0) = d(\tau(v),\tau(0)) = d(\tau(v),0) = w(\tau(v)) \quad \forall\, v \in \mathbb{H}[n,q]$$

es decir la isometría lineal τ **preserva el peso.**

De la observación anterior se desprende:

Si e_i es un vector unitario entonces

$$\tau(e_i) = K_l e_l \qquad \text{con} \quad K_l \in \mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\} \quad \text{y} \quad l \in \{1,2,...,n\}$$

Más aún, como la suma de dos vectores unitarios diferentes tiene peso dos, tenemos que

$$2 = w(e_i + e_j) = w(\tau(e_i + e_j)) = w(\tau(e_i) + \tau(e_j)) = w(K_l e_l + K_m e_m)$$

luego si $e_i \neq e_j$ entonces $e_l \neq e_m$.

Con estos resultados podemos concluir que dada una isometría lineal $\tau : \mathbb{H}[n,q] \longrightarrow \mathbb{H}[n,q]$, esta tiene asociada un único vector $\varphi \in (\mathbb{F}_q^*)^n$, y una única permutación $\sigma \in S_n$ tal que

$$\tau(e_i) = \varphi_{\sigma(i)}\, e_{\sigma(i)} \qquad \forall\, i \in \{1,2,...,n\}$$

Recíprocamente, cualquier función lineal que se pueda expresar como

$$\tau(e_i) = \varphi_{\sigma(i)}\, e_{\sigma(i)} \qquad \text{con} \quad \varphi \in (\mathbb{F}_q^*)^n \quad \text{y} \quad \sigma \in S_n$$

es una isometría lineal en $\mathbb{H}[n,q]$. Es por esto que en general denotaremos

$$\tau = (\varphi, \sigma)$$

Es claro que el conjunto de isometrías lineales sobre el espacio $\mathbb{H}[n,q]$ forma un grupo. Donde el producto de este grupo es la composición, denotada por

$$\begin{aligned}(\psi,\delta)(\varphi,\sigma)(e_i) &= (\psi,\delta)(\varphi_{\sigma(i)}\, e_{\sigma(i)}) \\ &= \varphi_{\sigma(i)}\psi_{\delta\sigma(i)}\, e_{\delta\sigma(i)} \\ &= \varphi_{\delta^{-1}\delta\sigma(i)}\psi_{\delta\sigma(i)}\, e_{\delta\sigma(i)} \\ &= (\psi\varphi_\delta, \delta\sigma)(e_i)\end{aligned}$$

Ocupando la notación antes definida, sigue que.

Corolario 2.1.6. *Las isometrías lineales en $\mathbb{H}[n,q]$ forman el grupo*

$$I = \{(\varphi,\sigma) \mid \varphi \in (\mathbb{F}_q^*)^n, \sigma \in S_n\}$$

Donde el producto esta dado por

$$(\psi,\delta)(\varphi,\sigma) = (\psi\varphi_\delta, \delta\sigma) \quad \textit{con} \quad \psi\varphi_\delta(i) = \psi_i\varphi_{\delta^{-1}(i)} \quad \forall\, i \in \{1,2,...,n\}$$

el elemento neutro es

$$1_I = (\xi, id) \quad \textit{donde} \quad \xi_i = 1 \ \ \forall\, i \in \{1,2,..n\}$$

y el inverso es

$$(\varphi,\sigma)^{-1} = (\varphi^{-1}_{\sigma^{-1}}, \sigma^{-1})$$

A continuación recordamos la definición del producto trenzado pues el grupo I corresponde al producto trenzado de dos grupos conocidos. Esta caracterización nos será de mucha utilidad para la próxima sección.

Definición 2.1.7. Sea H un grupo y sea G un subgrupo de S_n. Se define el producto trenzado (wreath product) de H y G , denotado por $H \wr_n G$, como el producto semidirecto de los grupos H^n y G

$$H \wr_n G = H^n \rtimes G = \{(\varphi,\sigma)/\varphi \in H^n, \sigma \in G\}$$

con la multiplicación definida por

$$(\psi,\delta)(\varphi,\sigma) = (\psi\varphi_\delta, \delta\sigma) \quad \text{donde} \quad \psi\varphi_\delta(i) = \psi_i\varphi_{\delta^{-1}(i)} \quad \forall\ i \in \{1,2,...,n\}$$

por lo cual el elemento neutro

$$1_{H\wr_n G} = (\xi, 1_G) \quad \text{donde} \quad \xi_i = 1 \ \ \forall\, i \in \{1, 2, ..., n\}$$

y el inverso

$$(\varphi, \sigma)^{-1} = (\varphi_{\sigma^{-1}}^{-1}, \sigma^{-1}) \quad \text{donde} \quad \varphi_{\sigma^{-1}}^{-1}(i) = \varphi_{\sigma(i)}^{-1} \ \ \forall\, i \in \{1, 2, ..., n\}$$

Observación 2.1.8. [2] Tomemos H como el grupo multiplicativo $\mathbb{F}_q^*$ y G el grupo de permutaciones S_n, entonces

$$H \wr_n G = \mathbb{F}_q^* \wr_n S_n = \{(\varphi, \sigma) \mid \varphi \in (\mathbb{F}_q^*)^n, \sigma \in S_n\}$$

Con lo cual obtenemos que $I \simeq \mathbb{F}_q^* \wr_n S_n$.

Otra caracterización que veremos del grupo de isometrías lineales, es su representación en forma matricial. Esta caracterización la utilizaremos en el siguiente capítulo.

Observación 2.1.9. Si τ es una isometría, tenemos que:

$$\tau(e_i) = \varphi_{\sigma(i)}\ e_{\sigma(i)} = e_i M_{(\varphi,\sigma)}^t$$

donde la (n, n)-matriz $M_{\varphi,\sigma} = (a_{i,j})$ es de la forma,

$$a_{i,j} = \begin{cases} \varphi_{\sigma(i)} & \text{si } j = \sigma(i) \\ 0 & \text{en otro caso} \end{cases}$$

Y al igual que la forma anteriormente descrita, para estas isometrías.

Corolario 2.1.10. *Las matrices representantes de los elementos del grupo de isometrías, forman el grupo*

$$M_n(q) = \{M_{(\varphi,\sigma)} / \varphi \in (\mathbb{F}_q^*)^n, \sigma \in S_n\}$$

Donde el producto matricial coincide con

$$M_{(\psi,\delta)} M_{(\varphi,\sigma)} = M_{(\psi\varphi_\delta, \delta\sigma)}$$

Observación 2.1.11. El homomorfismo

$$\begin{aligned} \theta : \ I &\longrightarrow M_n(q) \\ (\varphi, \sigma) &\longmapsto M_{(\varphi,\sigma)} \end{aligned}$$

corresponde a un isomorfismo entre estos dos grupos.

2.2. Clases de Isometría Lineal

Como nuestro propósito es saber cuando dos $[n,k]_q$-códigos son isométricos, vamos a definir una acción del grupo $\mathbb{F}_q^* \wr_n S_n$ en el conjunto de todos los $[n,k]_q$-códigos denotado en 1.1.13 por $U[n,k]_q$.

Con este motivo primero definiremos una acción del grupo trenzado $H \wr_n G$ sobre un conjunto Y^n,

Definición 2.2.1. Sea H un grupo que actúa en un conjunto Y y G un subgrupo de S_n. Se define una función ϵ, como sigue

$$\begin{aligned} \epsilon: \quad H \wr_n G \times Y^n &\longrightarrow Y^n \\ ((\varphi,\sigma)\ ,\ f) &\longmapsto (\varphi,\sigma)f \end{aligned}$$

donde $((\varphi,\sigma)f)_i = \varphi_i f_{\sigma^{-1}(i)}$

Dado que el grupo H actúa en el conjunto Y y el grupo G es un subgrupo de S_n, tenemos que

Lema 2.2.2. *La función ϵ definida anteriormente, es una acción del grupo trenzado $H \wr_n G$ sobre un conjunto Y^n*

DEMOSTRACIÓN: Tenemos que $1_{H\wr_n G} = (\xi, id)$ donde $\xi_i = 1 \quad \forall\ i \in \{1,2..n\}$ y id es la permutación identidad. Sea $f \in Y^n$ luego

$$((\xi,id)f)_i = 1 f_{id^{-1}(i)} = f_i \ \ \forall\, i \in \{1,2,...,n\}$$

Sea (ψ,δ) y $(\varphi,\sigma) \in H \wr_n G$, luego

$$\begin{aligned} ((\psi,\delta)((\varphi,\sigma)f))_i &= \psi_i((\varphi,\sigma)f)_{\delta^{-1}(i)} \\ &= \psi_i \varphi_{\delta^{-1}(i)} f_{\sigma^{-1}(\delta^{-1}(i))} \\ &= \psi_i \varphi_{\delta^{-1}(i)} f_{(\delta\sigma)^{-1}(i)} \\ &= ((\psi\varphi_\delta, \delta\sigma)f)_i \\ &= ((\psi,\delta)(\varphi,\sigma)f)_i \ \ \forall\, i \in \{1,2...n\} \end{aligned}$$

□

Observación 2.2.3. Ahora como el grupo $\mathbb{F}_q^*$ actúa en el conjunto $\mathbb{F}_q$, tenemos por el lema anterior una acción de $\mathbb{F}_q^* \wr_n S_n$ en $\mathbb{F}_q^n$ definida por

$$\begin{array}{rcl} \mathbb{F}_q^* \wr_n S_n \times \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ ((\varphi,\sigma)\ ,\ v) & \longmapsto & (\varphi,\sigma)v \end{array}$$

donde $((\varphi,\sigma)v)_i = \varphi_i v_{\sigma^{-1}(i)}$.

Teorema 2.2.4. *El grupo de isometrías lineales $\mathbb{F}_q^* \wr_n S_n$ actúa en $U[n,k]_q$ como sigue*

$$\begin{array}{rcl} \mathbb{F}_q^* \wr_n S_n \times U[n,k]_q & \longrightarrow & U[n,k]_q \\ ((\varphi,\sigma)\,,\,C) & \longmapsto & (\varphi,\sigma)\cdot C = \{(\varphi,\sigma)c \mid c \in C\} \end{array}$$

Llamaremos clase de isometría del $[n,k]_q$-código C a la órbita

$$\mathbb{F}_q^* \wr_n S_n(C) = \{(\varphi,\sigma)\cdot C \mid (\varphi,\sigma) \in \mathbb{F}_q^* \wr_n S_n\}$$

Luego el conjunto de clases de isometría de $[n,k]_q$-códigos es

$$U[n,k]_q/\mathbb{F}_q^* \wr_n S_n$$

el conjunto de todas las $\mathbb{F}_q^* \wr_n S_n$-órbitas en $U[n,k]_q$.

DEMOSTRACIÓN: Queremos demostrar que la función definida corresponde a una acción del grupo $\mathbb{F}_q^* \wr_n S_n$ en el conjunto $U[n,k]_q$ .Para esto primero demostraremos que si $(\varphi,\sigma) \in \mathbb{F}_q^* \wr_n S_n$,entonces $(\varphi,\sigma)\cdot C \in U[n,k]_q$ para todo $C \in U[n,k]_q$.
Sea $(\varphi,\sigma) \in \mathbb{F}_q^* \wr_n S_n$, como (φ,σ) representa una isometría en particular define un isomorfismo en el espacio $\mathbb{F}_q^n$, dado por

$$\begin{array}{rccc} T_{(\varphi,\sigma)}: & \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ & v & \longmapsto & (\varphi,\sigma)v \end{array}$$

Sea $C \in U[n,k]_q$, luego como $C \leqslant \mathbb{F}_q^n$ de dimensión k, la imagen de C bajo el isomorfismo antes definido es un subespacio de $\mathbb{F}_q^n$ de dimensión k, es decir que

$$T_{(\varphi,\sigma)}(C) = (\varphi,\sigma)\cdot C \in U[n,k]_q \qquad \forall\ C \in U[n,k]_q$$

Ahora nos falta demostrar las dos propiedades que debe cumplir esta función para definir una acción . Es claro que si (ξ, id) representa la identidad del grupo $\mathbb{F}_q^* \wr_n S_n$, luego

$$(\xi,id)\cdot C = C \qquad \forall\ C \in U[n,k]_q.$$

Sea (ψ, δ) y$(\varphi, \sigma) \in \mathbb{F}_q^* \wr_n S_n$, luego

$$\begin{aligned}(\psi, \delta) \cdot ((\varphi, \sigma) \cdot C) &= (\psi, \delta) \cdot (\{(\varphi, \sigma)c \mid c \in C\}) \\ &= \{(\psi, \delta)((\varphi, \sigma)c) \mid c \in C\} \\ &= \{(\psi, \delta)(\varphi, \sigma)c \mid c \in C\} \\ &= (\psi, \delta)(\varphi, \sigma) \cdot C\end{aligned}$$

□

En términos de matrices

Teorema 2.2.5. *El grupo de isometrías $M_n(q)$ actúa en $U[n,k]_q$ como sigue*

$$\begin{aligned}M_n(q) \times U[n,k]_q &\longrightarrow U[n,k]_q \\ (M_{(\varphi,\sigma)}, C) &\longmapsto M_{(\varphi,\sigma)} \cdot C = \{cM_{(\varphi,\sigma)}^t \mid c \in C\}\end{aligned}$$

Así la clase de isometría del $[n,k]_q$-código C, también puede ser descrita como

$$M_n(q)(C) = \{M_{(\varphi,\sigma)} \cdot C \mid M_{(\varphi,\sigma)} \in M_n(q)\}$$

y el conjunto de clases de isometría de $[n,k]_q$-códigos como

$$U[n,k]_q / M_n(q)$$

el conjunto de todas las $M_n(q)$-órbitas en $U[n,k]_q$.

DEMOSTRACIÓN: Es claro que si I representa la isometría identidad en $M_n(q)$, luego

$$I \cdot C = C \qquad \forall\ C \in U(n,k,q).$$

Sea $M_{(\psi,\tau)}$ y$M_{(\varphi,\sigma)} \in M_n(q)$, luego

$$\begin{aligned}M_{(\varphi,\sigma)} \cdot (M_{(\psi,\tau)} \cdot C) &= M_{(\varphi,\sigma)} \cdot (\{cM_{(\psi,\tau)}^t \mid c \in C\}) \\ &= \{cM_{(\psi,\tau))}^t M_{(\varphi,\sigma)}^t \mid c \in C\} \\ &= \{c(M_{(\varphi,\sigma)} M_{(\psi,\tau)})^t \mid c \in C\} \\ &= M_{(\varphi,\sigma)} M_{(\psi,\tau)} \cdot C\end{aligned}$$

□

Como en el próximo capítulo queremos construir códigos lineales, y estos se construyen a través de sus matrices generadoras, veremos como actúa el grupo de isometrías en el conjunto de matrices generadoras.

Definición 2.2.6. Denotamos por $\mathbb{F}_q^{k\times n,k}$ al conjunto de $k \times n$-matrices de rango k sobre $\mathbb{F}_q$, es decir el conjunto de matrices generadoras de $[n,k]_q$-códigos.

Observación 2.2.7. Del teorema 2.2.5 se desprende la acción del grupo de isometrías lineales $M_n(q)$ en el conjunto $\mathbb{F}_q^{k\times n,k}$, como sigue

$$\begin{aligned} M_n(q) \times \mathbb{F}_q^{k\times n,k} &\longrightarrow \mathbb{F}_q^{k\times n,k} \\ (M_{(\varphi,\sigma)} \ , \ \Gamma) &\longmapsto \Gamma \ M_{(\varphi,\sigma)}^t \end{aligned}$$

donde es importante notar que $\mathbb{F}_q^{k\times n,k}/M_n(q)$ hace una partición en el conjunto de matrices generadoras, pero no en $U[n,k]_q$. Si dos matrices cualesquiera petenecen a distintas órbitas no quiere decir que generen distintos códigos lineales, pero si dos matrices pertenecen a la misma órbita tenemos que estas generan códigos lineales isométricos.

Ejemplo 2.2.8. *Sea $q = 3$, $k = 2$ y $n = 3$, luego el conjunto $\mathbb{F}_3^{2\times 3,2}$ de todas las matrices generadoras de $[3,2]_3$-códigos tiene cardinalidad 624, mientras que el conjunto $U[3,2]_3$ de todos los $[3,2]_q$-códigos tiene cardinalidad 13. Al hacer actuar al grupo $M_3(3)$ sobre $\mathbb{F}_3^{2\times 3,2}$, notamos que $\mid \mathbb{F}_3^{2\times 3,2}/M_3(3) \mid = 22$. Con sólo esta información ya sabemos que existen matrices generadoras que generan al mismo código lineal y pertenecen a distintas órbitas. Un ejemplo de estas son las matrices*

$$\Gamma_1 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 2 & 1 \end{pmatrix} \quad y \quad \Gamma_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 2 & 0 \end{pmatrix}$$

las que claramente generan el mismo código lineal pero $M_3(3)(\Gamma_1) \neq M_3(3)(\Gamma_2)$

Esto ocurre por lo descrito en el teorema 1.1.11, ya que antes de actuar con el grupo $M_n(q)$, debemos actuar con el grupo $GL_k(q)$ sobre el conjunto $\mathbb{F}_q^{k\times n,k}$.

Corolario 2.2.9. *El producto directo $GL_k(q) \times M_n(q)$ actúa en el conjunto $\mathbb{F}_q^{k\times n,k}$ como sigue*

$$\begin{aligned}(GL_k(q) \times M_n(q)) \times \mathbb{F}_q^{k\times n,k} &\longrightarrow \mathbb{F}_q^{k\times n,k}\\ ((B \ , \ M_{(\varphi,\sigma)}) \ , \ \Gamma) &\longmapsto B\Gamma M_{(\varphi,\sigma)}^t\end{aligned}$$

Así el conjunto de clases de isometría de $[n,k]_q$-códigos puede ser identificado

$$\mathbb{F}_q^{k\times n,k}/(GL_k(q) \times M_n(q))$$

el conjunto de todas las $GL_k(q) \times M_n(q)$-órbitas en $\mathbb{F}_q^{k\times n,k}$.

Ejemplo 2.2.10. *Sea $k = 2$, $n = 3$, $q = 2$. Luego el conjunto*

$$\mathbb{F}_2^{2\times 3,2} = \left\{ \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \right.$$
$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$
$$\begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix},$$
$$\left. \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix} \right\}$$

y el grupo

$$GL_2(2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$$

Por último debemos conocer el conjunto

$$(\mathbb{F}_2^*)^3 = \{(111)\} \quad \textit{llamemos} \quad \varphi = (111)$$

y el grupo de simetría,

$$S_3 = \{\sigma_1 = id., \sigma_2 = (12), \sigma_3 = (13), \sigma_4 = (23), \sigma_5 = (123), \sigma_6 = (132)\}$$

Para formar el grupo,

$$M_3(2) = \left\{ M_{(\varphi,\sigma_1)} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, M_{(\varphi,\sigma_2)} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, M_{(\varphi,\sigma_3)} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \right.$$
$$\left. M_{(\varphi,\sigma_4)} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, M_{(\varphi,\sigma_5)} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, M_{(\varphi,\sigma_6)} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \right\}$$

Primero mostraremos las órbitas formadas por la acción de el grupo $GL_2(2)$ *en el conjunto* $\mathbb{F}_2^{2\times 3,2}$*:*

$$GL_2(2)\left(\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}\right) = \left\{\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}\right\}$$

$$GL_2(2)\left(\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}\right) = \left\{\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}\right\}$$

$$GL_2(2)\left(\begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}\right) = \left\{\begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}\right\}$$

$$GL_2(2)\left(\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}\right) = \left\{\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}\right\}$$

$$GL_2(2)\left(\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}\right) = \left\{\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}\right\}$$

$$GL_2(2)\left(\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}\right) = \left\{\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}\right\}$$

$$GL_2(2)\left(\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}\right) = \left\{\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}\right\}$$

Así $|\mathbb{F}_2^{2\times 3,2}/GL_2(2)| = 7$*, lo que significa que existen 7* $[3,2]_2$*-códigos diferentes. Ahora mostraremos las órbitas producidas por la acción del grupo* $(GL_2(2) \times M_3(2))$ *en el conjunto* $\mathbb{F}_2^{2\times 3,2}$*.*

$$(GL_2(2)\times M_3(2))\left(\begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}\right) = \left\{\begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \right.$$
$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$
$$\left. \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix} \right\}$$

$$(GL_2(2)\times M_3(2))\left(\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}\right) = \left\{\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \right.$$
$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix},$$
$$\left. \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \right\}$$

$$(GL_2(2)\times M_3(2))\left(\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}\right) = \left\{\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \right\}$$

Así $|(GL_2(2) \times M_3(2))/\mathbb{F}_2^{2\times 3,2}| = 3$*, lo que significa que existen 3 clases de isometría lineal de* $[3,2]_2$*-códigos .*

2.3. Enumeración de Clases de Isometría Lineal.

Ya habiendo particionado el conjunto de todos los $[n,k]_q$-códigos, denotado por $U[n,k]_q$ en órbitas producidas por la acción del grupo de isometrías, nuestro estudio se enfocará en contar estas órbitas y así saber cuantos $[n,k]_q$-códigos lineales no isométricos existen.

Con este fin estudiaremos como actúa el grupo trenzado $\mathbb{F}_q^* \wr_n S_n$ en el conjunto de $GL_k(q)$-órbitas en $\mathbb{F}_q^{k\times n,k}$, el cual representa al conjunto $U[n,k]_q$, y ocuparemos elementos del álgebra abstracta, en particular de la teoría de grupos, para poder contar las órbitas producidas por esta acción, que como ya vimos en el teorema 2.2.4 corresponden a las clases de isometría de $[n,k]_q$-códigos .

Debido a la condición en el rango, el conjunto $\mathbb{F}_q^{k\times n,k}$ no es fácil de manejar, es por esto que preferiremos trabajar con el conjunto de $(k\times n)-$matrices sobre $\mathbb{F}_q$, que es denotado por $\mathbb{F}_q^{k\times n}$. Es claro que este conjunto contiene al conjunto de matrices generadoras de $[n,l]_q$-códigos lineales sobre $\mathbb{F}_q$, con $l \leqslant k$.

Así también las matrices que contienen columnas de ceros no son de nuestro interés, así que sólo estudiaremos códigos lineales generados por matrices que no contengan columnas de ceros, estos códigos son llamados **códigos lineales no redundantes**.

Observación 2.3.1. Si $\Gamma = (\gamma_1^t \mid \gamma_2^t \mid ... \mid \gamma_n^t)$ con $\gamma_i \in \mathbb{F}_q^k$, $i \in \{1,2,..,n\}$ es una matriz generadora de de un $[n,k]_q$-código no redundante, esta puede ser identificada con el vector $\gamma = (\gamma_1, \gamma_2 ... \gamma_n) \in (\mathbb{F}_q^k \setminus \{0\})^n$.

Teniendo en cuenta que la acción del grupo $GL_k(q)$ en el conjunto $(\mathbb{F}_q^k \setminus \{0\})^n$ está dada por:

$$\begin{array}{ccc} GL_k(q) \times (\mathbb{F}_q^k \setminus \{0\})^n & \longrightarrow & (\mathbb{F}_q^k \setminus \{0\})^n \\ (A\ ,\ f) & \longmapsto & A \cdot f \end{array}$$

donde $(A \cdot f)_i = f_i A^t$, podemos reescribir nuestro problema para códigos lineales no redundantes, de la siguiente manera

Lema 2.3.2. *Sea la acción del grupo $\mathbb{F}_q^* \wr_n S_n$ en el conjunto de órbitas $((\mathbb{F}_q^k \setminus \{0\})^n / GL_k(q))$ como sigue*

$$\begin{aligned} \mathbb{F}_q^* \wr_n S_n \times ((\mathbb{F}_q^k \setminus \{0\})^n / GL_k(q)) &\longrightarrow (\mathbb{F}_q^k \setminus \{0\})^n / GL_k(q) \\ ((\varphi, \sigma)\ ,\ GL_k(q)(f)) &\longmapsto (\varphi, \sigma) \cdot GL_k(q)(f) = GL_k(q)((\varphi, \sigma)f) \end{aligned}$$

Luego el conjunto

$$((\mathbb{F}_q^k \setminus \{0\})^n / GL_k(q)) / \mathbb{F}_q^* \wr_n S_n$$

es el conjunto de clases de isometría de $[n, l]_q$-códigos no redundantes, para todo $l \leq k$.

DEMOSTRACIÓN: Primero queremos demostrar que esta función está bien definida. Sean f y $g \in (\mathbb{F}_q^k \setminus \{0\})^n$, tales que $GL_k(q)(f) = GL_k(q)(g)$, entonces

$$fA^t = g \qquad \text{para algún} \quad A \in GL_k(q)$$

lo que implica

$$f_i A^t = g_i \quad \text{para algún} \quad A \in GL_k(q) \quad \text{y} \quad \forall\, i \in \{1, 2..n\}$$

luego para todo $(\varphi, \sigma) \in \mathbb{F}_q^* \wr_n S_n$

$$((\varphi, \sigma)g)_i = \varphi_i g_{\sigma^{-1}(i)} = \varphi_i f_{\sigma^{-1}(i)} A^t = \varphi_i (Af)_{\sigma^{-1}(i)} = ((\varphi, \sigma)Af)_i$$

para algún $A \in GL_k(q)$ y $\forall\, i \in \{1, 2..n\}$ y así demostramos que para todo $(\varphi, \sigma) \in \mathbb{F}_q^* \wr_n S_n$

$$GL_k(q)((\varphi, \sigma)f) = GL_q(k)((\varphi, \sigma)g)$$

Ahora demostraremos que esta función define una acción por la izquierda. Claramente si (ξ, id) representa la identidad de $\mathbb{F}_q^* \wr_n S_n$

$$(\xi, id) \cdot GL_k(q)(f) = GL_k(q)((\xi, id)f) = GL_k(q)(f)\ \forall\ f \in (\mathbb{F}_q^k \setminus \{0\})^n$$

Ahora si (φ, σ) y $(\psi, \delta) \in \mathbb{F}_q^* \wr_n S_n$, tenemos que

$$\begin{aligned} (\varphi, \sigma) \cdot ((\psi, \delta) \cdot GL_k(q)(f)) &= (\varphi, \sigma) \cdot GL_k(q)((\psi, \delta) \cdot f) \\ &= GL_k(q)((\varphi, \sigma) \cdot ((\psi, \delta) \cdot f)) \\ &= GL_k(q)((\varphi, \sigma)(\psi, \delta) \cdot f) \\ &= (\varphi, \sigma)(\psi, \delta) \cdot GL_k(q)(f) \end{aligned}$$

□

Lema 2.3.3. $((\mathbb{F}_q^k \setminus \{0\})^n / GL_k(q))/\mathbb{F}_q^* \wr_n S_n = ((\mathbb{F}_q^k \setminus \{0\})^n / \mathbb{F}_q^* \wr_n S_n)/GL_k(q)$

DEMOSTRACIÓN: Sea $f \in (\mathbb{F}_q^k \setminus \{0\})^n$,luego

$$\begin{aligned}
\mathbb{F}_q^* \wr_n S_n(GL_k(q))(f)) &= \{\mathbb{F}_q^* \wr_n S_n(A \cdot f) \mid A \in GL_k(q)\} \\
&= \{\mathbb{F}_q^* \wr_n S_n(f_1 A^t, ..., f_n A^t) \mid A \in GL_k(q)\} \\
&= \{(\varphi, \sigma) \cdot (f_1 A^t, ..., f_n A^t) \mid (\varphi, \sigma) \in \mathbb{F}_q^* \wr_n S_n \text{ y } A \in GL_k(q)\} \\
&= \{(\varphi_1 f_{\sigma^{-1}(1)} A^t, ..., \varphi_n f_{\sigma^{-1}(n)} A^t) \mid (\varphi, \sigma) \in \mathbb{F}_q^* \wr_n S_n \text{ y } A \in GL_k(q)\} \\
&= \{A \cdot (\varphi_1 f_{\sigma^{-1}(1)}, ..., \varphi_n f_{\sigma^{-1}(n)}) \mid (\varphi, \sigma) \in \mathbb{F}_q^* \wr_n S_n \text{ y } A \in GL_k(q)\} \\
&= \{A \cdot ((\varphi, \sigma) \cdot f) \mid (\varphi, \sigma) \in \mathbb{F}_q^* \wr_n S_n \text{ y } A \in GL_k(q)\} \\
&= GL_k(q)(\mathbb{F}_q^* \wr_n S_n(f))
\end{aligned}$$

□

Y así por los lemas 2.3.2 y 2.3.3, podemos concluir que el conjunto $((\mathbb{F}_q^k \setminus \{0\})^n / \mathbb{F}_q^* \wr_n S_n)/GL_k(q)$ corresponde con el conjunto de clases de isometría de $[n, l]_q$-códigos no redundantes, para todo $l \leq k$.

Ahora definiremos un espacio, que nos facilitará nuestro estudio.

Definición 2.3.4. El espacio proyectivo correspondiente a $\mathbb{F}_q^k$ se define como sigue

$$\mathbb{F}_q\mathbb{P}^{k-1} = (\mathbb{F}_q^k \setminus \{0\})/\sim$$

donde la relación $\sim$ esta definida por: $v \sim w$ si y sólo si existe $\lambda \in \mathbb{F}_q^*$ tal que $v = \lambda w$. También denotado por

$$\mathbb{F}_q\mathbb{P}^{k-1} = (\mathbb{F}_q^k \setminus \{0\})/\mathbb{F}_q^*$$

El orden $\theta_{k-1}(q)$ de este grupo es

$$\theta_{k-1}(q) = \mid \mathbb{F}_q\mathbb{P}^{k-1} \mid = \frac{q^k - 1}{q - 1} = q^{k-1} + q^k + ... + q + 1$$

El siguiente lema nos será de mucha utilidad, ya que muestra una biyección entre las órbitas de la acción del grupo trenzado $H \wr_n G$ en el conjunto Y^n y las órbitas de otra acción más fácil de manejar.

Lema 2.3.5. *Sea H un grupo que actúa en un conjunto Y y sea G un subgrupo de S_n. Si definimos la acción del grupo $H \wr_n G$ en Y^n como en la observación 2.2.1, la función $\phi : Y^n \longrightarrow (Y/H)^n$, donde $(\phi(f))_i = Hf_i$, y la acción de el grupo G en el conjunto $(Y/H)^n$ como*

$$\begin{array}{ccc} G \times (Y/H)^n & \longrightarrow & (Y/H)^n \\ (\sigma\ ,\ \bar{f}) & \longmapsto & \sigma\bar{f} \end{array}$$

donde $(\sigma\bar{f})_i = \bar{f}_{\sigma^{-1}(i)}$ tenemos que

(i) La función

$$\begin{array}{rccc} \psi: & Y^n/(H \wr_n G) & \longrightarrow & (Y/H)^n/G \\ & H \wr_n G(f) & \longmapsto & G(\phi(f)) \end{array}$$

es biyectiva.

(ii) $H \wr_n G(f) = \phi^{-1}(\psi(H \wr_n G(f))) = \phi^{-1}(G(\phi(f)))\ \forall\ f \in Y^n$

DEMOSTRACIÓN:

(i) Primero queremos demostrar que la función ψ está bien definida y es inyectiva. Sean f y $g \in Y^n$, tales que

$\psi(H \wr_n G(f)) = \psi(H \wr_n G(g))$

$\Leftrightarrow G(\phi(f)) = G(\phi(g))$

$\Leftrightarrow \phi(f) \in G(\phi(g))$

$\Leftrightarrow \phi(f) = \sigma\phi(g)$ para algún $\sigma \in G$

$\Leftrightarrow Hf_i = Hg_{\sigma^{-1}(i)}$ para algún $\sigma \in G$ y $\forall\ i \in \{1, 2.., n\}$

$\Leftrightarrow f_i \in Hg_{\sigma^{-1}(i)}$ para algún $\sigma \in G$ y $\forall\ i \in \{1, 2.., n\}$

$\Leftrightarrow f_i = hg_{\sigma^{-1}(i)}$ para algún $h \in H$ algún $\sigma \in G$ y $\forall\ i \in \{1, 2.., n\}$

$\Leftrightarrow f = g(\varphi, \sigma)$ para algún $(\varphi, \sigma) \in H \wr_n G$

$\Leftrightarrow f \in H \wr_n G(g)$

$\Leftrightarrow H \wr_n G(f) = H \wr_n G(g)$

Ahora para demostrar que la función ψ es sobreyectiva, primero demostraremos que la función ϕ es sobreyectiva.
Sean $F \in (Y/H)^n$ y $f^F \in Y^n$ tal que $f_i^F \in F_i$, luego

$$(\phi(f^F))_i = Hf_i^F = F_i$$

lo que demuestra que ϕ es una función sobreyectiva. Así para todo $F \in (Y/H)^n$ tenemos que existe $f^F \in Y^n$ tal que

$\psi(H \wr_n G(f^F)) = G(\phi(f^F)) = G(F)$ por lo tanto ψ es sobreyectiva.

(ii) Primero notemos que, si $F \in (Y/H)^n$ existe $f \in Y^n$ tal que $\phi(f) = F$, ya que ϕ es una función sobreyectiva. Entonces

$$\begin{aligned}
\phi^{-1}(F) &= \phi^{-1}(\{\phi(f)\}) \\
&= \{\tau \in Y^n \mid \tau_i \in Hf_i \quad \forall\, i \in \{1,2..n\}\} \\
&= \{\tau \in Y^n \mid \tau_i = \psi_i f_i \text{ con } \psi \in H^n \text{ y } \forall\, i \in \{1,2..n\}\} \\
&= \{(\psi,1)f \mid \psi \in H^n\} \\
&= H \wr_n \{1\}(f)
\end{aligned}$$

y $(\phi(\sigma f))_i = H(\sigma f)_i = Hf_{\sigma^{-1}(i)} = (\sigma(\phi(f)))_i \quad \forall\, i \in \{1,2..n\}$

$$\begin{aligned}
\text{Luego} \quad H \wr_n G(f) &= \{(\varphi,\sigma)f \mid \varphi \in H^n, \sigma \in G\} \\
&= \{\tilde{f} \mid \tilde{f}_i = \varphi_i f_{\sigma^{-1}(i)} \text{ con } \varphi \in H^n, \sigma \in G\} \\
&= \bigcup_{\sigma \in G} \{\tilde{f} \mid \tilde{f}_i = \varphi_i f_{\sigma^{-1}(i)} \text{ con } \varphi \in H^n\} \\
&= \bigcup_{\sigma \in G} H \wr_n \{1\}(\sigma f) \\
&= \bigcup_{\sigma \in G} \phi^{-1}(\{\phi(\sigma f)\}) \\
&= \bigcup_{\sigma \in G} \phi^{-1}(\{\sigma\phi(f)\}) \\
&= \phi^{-1}(\bigcup_{\sigma \in G} \{\sigma\phi(f)\}) \\
&= \phi^{-1}(\{\sigma\phi(f)/\sigma \in G\})
\end{aligned}$$

$$= \phi^{-1}(G(\phi(f)))$$

$$= \phi^{-1}(\psi(H \wr_n G(f))$$

□

Si aplicamos el lema anterior parte (i), al grupo trenzado $\mathbb{F}_q^* \wr_n S_n$ actuando en $(\mathbb{F}_q^k \setminus \{0\})^n$, podremos reescribir las órbitas estudiadas, tal que esta nueva forma de construir estas órbitas, nos facilitará el cálculo de ellas.

$$\begin{aligned} \phi: \quad (\mathbb{F}_q^k \setminus \{0\})^n &\longrightarrow ((\mathbb{F}_q^k \setminus \{0\})/\mathbb{F}_q^*)^n \\ f &\longmapsto \phi(f) \end{aligned}$$

donde $(\phi(f))_i = \mathbb{F}_q^*(f_i)$, entonces la función

$$\begin{aligned} \psi: \quad (\mathbb{F}_q^k \setminus \{0\})^n/\mathbb{F}_q^* \wr_n S_n &\longrightarrow ((\mathbb{F}_q^k \setminus \{0\})/\mathbb{F}_q^*)^n/S_n \\ \mathbb{F}_q^* \wr_n S_n(f) &\longmapsto S_n(\phi(f)) \end{aligned}$$

es una biyección.
Por lo cual

$$((\mathbb{F}_q^k \setminus \{0\})^n/\mathbb{F}_q^* \wr_n S_n)/GL_k(q)$$

lo podemos reescribir de la siguiente manera.

$$(((\mathbb{F}_q^k \setminus \{0\})/\mathbb{F}_q^*)^n/S_n)/GL_k(q)$$

Más aún como el espacio proyectivo $\mathbb{F}_q\mathbb{P}^{k-1}$ es $(\mathbb{F}_q^k \setminus \{0\})/\mathbb{F}_q^*$, como lo vimos en la definición 2.3.4,tenemos que

Corolario 2.3.6. *El conjunto de clases de isometría lineal de (n,l)-códigos lineales no redundantes, para todo $l \leq k$ puede ser descrito*

$$((\mathbb{F}_q\mathbb{P}^{k-1})^n/S_n)/GL_k(q)$$

Donde la acción del grupo S_n en el espacio $\mathbb{F}_q\mathbb{P}^{k-1}$, esta dada por

$$\begin{aligned} S_n \times (\mathbb{F}_q\mathbb{P}^{k-1})^n &\longrightarrow (\mathbb{F}_q\mathbb{P}^{k-1})^n \\ (\sigma\,,\, f) &\longmapsto \sigma \cdot f \end{aligned}$$

donde $(\sigma \cdot f)_i = \sigma f_i = [v_{\sigma^{-1}(i)}]$ entendiendo que $f_i = [v_i]$.

Y la acción del grupo $GL_k(q)$ en el conjunto $((\mathbb{F}_q\mathbb{P}^{k-1})^n/S_n)$ se desprende del lema 2.3.3, de la siguiente manera

$$\begin{aligned} GL_k(q) \times (\mathbb{F}_q\mathbb{P}^{k-1})^n)/S_n &\longrightarrow ((\mathbb{F}_q\mathbb{P}^{k-1})^n)/S_n \\ (A\,,\,\sigma \cdot f) &\longmapsto A \cdot (\sigma \cdot f) \end{aligned}$$

donde $(A \cdot (\sigma \cdot f))_i = [v_{\sigma^{-1}(i)}A^t]$ entendiendo que $f_i = [v_i]$

La definición que sigue a continuación, nos servirá para reducir tiempo al momento de calcular estar órbitas.

Definición 2.3.7. Sea $f \in (\mathbb{F}_q\mathbb{P}^{k-1})^n$, definimos el contenido de f como la siguiente función

$$\begin{aligned} c(f): \ \mathbb{F}_q\mathbb{P}^{k-1} &\longrightarrow \mathbb{N} \\ y &\longmapsto |\,\{i \mid f_i = y\}\,| \end{aligned}$$

Teorema 2.3.8. *Sean f y $g \in (\mathbb{F}_q\mathbb{P}^{k-1})^n$, entonces $S_n(f) = S_n(g)$ si y sólo si $c(f) = c(g)$*

DEMOSTRACIÓN: Sean f y $g \in (\mathbb{F}_q\mathbb{P}^{k-1})^n$ tal que $c(f) = c(g)$, luego

$$|\,\{i \mid f_i = y\}\,| = |\,\{i \mid g_i = y\}\,| \ \ \forall\, y \in \mathbb{F}_q\mathbb{P}^{k-1}$$

lo que implica que existe una permutación $\sigma \in S_n$ tal que

$$f_{\sigma(i)} = g_i \quad \forall\, i \in \{1, 2..n\}$$

y así $\sigma^{-1} \cdot f = g$, por lo cual $f \in S_n(g)$ concluyendo que $S_n(f) = S_n(g)$.

Recíprocamente, sean f y $g \in (\mathbb{F}_q\mathbb{P}^{k-1})^n$ tal que $S_n(f) = S_n(g)$, entonces $f \in S_n(g)$, es decir

$$f_{\sigma^{-1}(i)} = g_i \quad \text{para algún} \ \ \sigma \in S_n$$

Luego

$$c(g) = |\,\{i \mid g_i = y\}\,| = |\,\{i \mid f_{\sigma^{-1}(i)} = y\}\,| = |\,\{i \mid f_i = y\}\,| = c(f)$$

□

Corolario 2.3.9. *El conjunto de órbitas $(\mathbb{F}_q\mathbb{P}^{k-1})^n/S_n$ puede ser representado por un sistema completo de n-tuplas $f \in (\mathbb{F}_q\mathbb{P}^{k-1})^n$ con contenidos diferentes.*

Ejemplo 2.3.10. *(1) En el espíritu del corolario anterior, buscaremos quienes son los representantes de las órbitas $(\mathbb{F}_2\mathbb{P}^1)^3/S_3$. Donde*

$$\mathbb{F}_2\mathbb{P}^1 = \{[0,1],[1,0],[1,1]\}$$

Así $|\ (\mathbb{F}_2\mathbb{P}^1)^3 \ | = 27$. Luego aplicando la función contenido a cada elemento de $(\mathbb{F}_2\mathbb{P}^1)^3$ encontramos los representantes buscados, escogiendo los elementos que tienen diferentes contenidos

$$\begin{array}{ll}
c(([0,1],[0,1],[0,1])) = [3,0,0], & c(([0,1],[0,1],[1,0])) = [2,1,0],\\
c(([0,1],[0,1],[1,1])) = [2,0,1], & c(([0,1],[1,0],[1,0])) = [1,2,0],\\
c(([0,1],[1,0],[1,1])) = [1,1,1], & c(([0,1],[1,1],[1,1])) = [1,0,2],\\
c(([1,0],[1,0],[1,0])) = [0,3,0], & c(([1,0],[1,0],[1,1])) = [0,2,1],\\
c(([1,0],[1,1],[1,1])) = [0,1,2], & c(([1,1],[1,1],[1,1])) = [0,0,3].
\end{array}$$

Con esto redujimos el problema de aplicar la acción a 27 elementos, a aplicarla a sólo 10 elementos.

(2) Ahora buscaremos quienes son los representantes de las órbitas $(\mathbb{F}_3\mathbb{P}^1)^3/S_3$. Donde

$$\mathbb{F}_3\mathbb{P}^1 = \{[0,1],[1,0],[1,1],[1,2]\}$$

Así $|\ (\mathbb{F}_3\mathbb{P}^1)^3 \ | = 64$. Luego aplicando la función contenido a cada elemento de $(\mathbb{F}_3\mathbb{P}^1)^3$ encontramos los representantes buscados, escogiendo los elementos que tiene diferentes contenidos, cuáles son

$$\begin{array}{ll}
c(([0,1],[0,1],[0,1])) = [3,0,0,0], & c(([0,1],[0,1],[1,0])) = [2,1,0,0],\\
c(([0,1],[0,1],[1,1])) = [2,0,1,0], & c(([0,1],[0,1],[1,2])) = [2,0,0,1],\\
c(([0,1],[1,0],[1,0])) = [1,2,0,0], & c(([0,1],[1,0],[1,1])) = [1,1,1,0],\\
c(([0,1],[1,0],[1,2])) = [1,1,0,1], & c(([0,1],[1,1],[1,1])) = [1,0,2,0],\\
c(([0,1],[1,1],[1,2])) = [1,0,1,1], & c(([0,1],[1,2],[1,2])) = [1,0,0,2],\\
c(([1,0],[1,0],[1,0])) = [0,3,0,0], & c(([1,0],[1,0],[1,1])) = [0,2,1,0],\\
c(([1,0],[1,0],[1,2])) = [0,2,0,1], & c(([1,0],[1,1],[1,1])) = [0,1,2,0],\\
c(([1,0],[1,1],[1,2])) = [0,1,1,1], & c(([1,0],[1,2],[1,2])) = [0,1,0,2],\\
c(([1,1],[1,1],[1,1])) = [0,0,3,0], & c(([1,1],[1,1],[1,2])) = [0,0,2,1],
\end{array}$$

$$c(([1,1],[1,2],[1,2])) = [0,0,1,2], \quad c(([1,2],[1,2],[1,2])) = [0,0,0,3].$$

Con esto redujimos el problema de aplicar la acción a 64 elementos, a aplicarla a sólo 20 elementos.

(3) Para casos en que n y k son mayores como por ejemplo:

(i) El conjunto $(\mathbb{F}_3\mathbb{P}^2)^5$ el que tiene cardinalidad 371.293, los elementos que representan la órbita $(\mathbb{F}_3\mathbb{P}^2)^5/S_5$ son sólo 6.188.

(ii) El conjunto $(\mathbb{F}_4\mathbb{P}^1)^3$ el que tiene cardinalidad 125, los elementos que representan la órbita $(\mathbb{F}_4\mathbb{P}^1)^3/S_3$ son sólo 35.

(iii) El conjunto $(\mathbb{F}_5\mathbb{P}^1)^3$ el que tiene cardinalidad 216, los elementos que representan la órbita $(\mathbb{F}_4\mathbb{P}^1)^3/S_3$ son sólo 56.

Ahora del lema 2.3.5 parte (ii) aplicado al grupo trenzado $\mathbb{F}_q^* \wr_n S_n$ actuando en $(\mathbb{F}_q^k \setminus \{0\})^n$, se desprende el siguiente lema,el cual nos proporcionara la última forma que mostraremos de reescribir las órbitas que estamos estudiando. Esta nueva forma de construir estas órbitas nos servirá para contarlas.

Lema 2.3.11. *Sean $A \in GL_k(q)$ y ϕ como en el lema 2.3.5*

$$\begin{array}{rccc} \phi: & (\mathbb{F}_q^k \setminus \{0\})^n & \longrightarrow & (\mathbb{F}_q\mathbb{P}^{k-1})^n \\ & f & \longmapsto & \phi(f) \end{array}$$

donde $(\phi(f))_i = [f_i]$. Entonces

$$\phi(\mathbb{F}_q^* \wr_n S_n(Af)) = A(Sn(\phi(f))) \quad \forall\ f \in (\mathbb{F}_q^k \setminus \{0\})^n$$

DEMOSTRACIÓN: Del lema 2.3.5,ii obtenemos que

$$\mathbb{F}_q^* \wr_n S_n(Af) = \phi^{-1}(\psi(\mathbb{F}_q^* \wr_n S_n(Af))) = \phi^{-1}(S_n(\phi(Af)))$$

es decir

$$\phi(\mathbb{F}_q^* \wr_n S_n(Af)) = S_n(\phi(Af)$$

por otro lado tenemos que

$$(\phi(Af))_i = [f_i A^t] = A[f_i] = A(\phi(f))_i \quad \forall\ i \in \{1, 2..n\}$$

por lo cual $\phi(Af) = A\phi(f)$, entonces

$$\phi(\mathbb{F}_q^* \wr_n S_n(Af)) = S_n(\phi(Af)) = S_n(A\phi(f)) = A(S_n(\phi(f)))$$

□

De esta manera acabamos de sustituir la acción del grupo $GL_k(q) \times \mathbb{F}_q^* \wr_n S_n$ en el conjunto $(\mathbb{F}_q^k \setminus \{0\})^n$ por la acción de el grupo $GL_k(q) \times S_n$ en el conjunto $(\mathbb{F}_q\mathbb{P}^{k-1})^n$ dada por

$$\begin{array}{lll} (GL_k(q) \times S_n) \times (\mathbb{F}_q\mathbb{P}^{k-1})^n & \longrightarrow & (\mathbb{F}_q\mathbb{P}^{k-1})^n \\ ((A,\sigma), f) & \longmapsto & (A,\sigma)f \end{array} \tag{2.1}$$

donde $((A,\sigma)f)_i = Af_{\sigma^{-1}(i)} = [f_{\sigma^{-1}(i)}A^t]$

Y así llegamos a nuestro teorema principal.

Teorema 2.3.12. *El conjunto de clases de isometría de $[n,l]_q$-códigos no redundantes, para todo $l \leq k$ puede ser descrito como*

$$(\mathbb{F}_q\mathbb{P}^{k-1})^n/(GL_k(q) \times S_n)$$

con la acción descrita en (2.1), o bien

$$((\mathbb{F}_q\mathbb{P}^{k-1})^n/S_n)/GL_k(q)$$

donde el conjunto de órbitas $(\mathbb{F}_q\mathbb{P}^{k-1})^n/S_n$ puede ser representado por cualquier sistema completo de n-tuplas $f \in (\mathbb{F}_q\mathbb{P}^{k-1})^n$ con contenidos diferentes.

Ejemplo 2.3.13. *Sea $q=2$, $k=1$ y $n=3$, tenemos que $(\mathbb{F}_2\mathbb{P}^0)^3 = \{[111]\}$, es decir tenemos una sola clase de $[3,1]_2$-códigos lineales no redundantes sobre $\mathbb{F}_2$. Ahora si tomamos $q=2$, $k=2$ y $n=3$, como ya vimos en el ejemplo 2.3.10 los representantes de la órbita*

$\mathbb{F}_2\mathbb{P}^1/S_3 = \{([0,1],[0,1],[0,1]),([0,1],[0,1],[1,0]),([0,1],[0,1],[1,1]),([0,1],[1,0],[1,0]),$
$([0,1],[1,0],[1,1]),([0,1],[1,1],[1,1]),([1,0],[1,0],[1,0]),([1,0],[1,0],[1,1]),([1,0],[1,1],[1,1]),$
$([1,1],[1,1],[1,1])\}$

Así si le aplicamos a estos representantes la acción de $GL_2(2) \times S_3$ tenemos que las órbitas que se forman son

$GL_2(2) \times S_3(([0,1],[0,1],[0,1])) = \{([0,1],[0,1],[0,1]),([1,0],[1,0],[1,0]),([1,1],[1,1],[1,1])\}$

$GL_2(2) \times S_3\,(([0,1],[0,1],[1,0])) = \{([0,1],[0,1],[1,0]),([0,1],[0,1],[1,1]),([0,1],[1,0],[0,1]),$
$([0,1],[1,0],[1,0]),([0,1],[1,1],[0,1]),([0,1],[1,1],[1,1]),([1,0],[0,1],[0,1]),([1,0],[0,1],[1,0]),$
$([1,0],[1,0],[0,1]),([1,0],[1,0],[1,1]),([1,0],[1,1],[1,0]),([1,0],[1,1],[1,1]),([1,1],[0,1],[0,1]),$

$([1,1],[0,1],[1,1]),([1,1],[1,0],[1,0]),([1,1],[1,0],[1,1]),([1,1],[1,1],[0,1]),([1,1],[1,1],[1,0])\}$

$GL_2(2)\times S_3(([0,1],[1,0],[1,1])) = \{([0,1],[1,0],[1,1]),([0,1],[1,1],[1,0]),([1,0],[0,1],[1,1]),$
$([1,0],[1,1],[0,1]),([1,1],[0,1],[1,0]),([1,1],[1,0],[0,1])\}$

Luego son 3 los $[3,l]_2$-código no redundantes no isométricos, para $l \leqslant 2$. Juntando nuestros dos resultados tenemos que son 2 los $[3,2]_2$-códigos no redundantes no isométricos, este resultado coincide con el del ejemplo 2.2.10 ya que la primera órbita que se muestra en este ejemplo posee soló códigos redundantes.

Para facilitar nuestro trabajo, vamos a usar una notación mas abreviada para los conjuntos y valores que utilizaremos.

Definición 2.3.14. Denotamos por

(i) $V[n,k]_q$ al conjunto de todos los $[n,k]_q$-códigos no redundantes

(ii) $U_{[n,k]_q}$ al conjunto de clases de isometría en $U[n,k]_q$, es decir $U_{[n,k]_q} = U[n,k]_q/M_n(q)$

(iii) $V_{[n,k]_q}$ al conjunto de clases de isometría en $V[n,k]_q$, es decir $V_{[n,k]_q} = V[n,k]_q/M_n(q)$

(iv) $T_{[n,k]_q}$ al conjunto de clases de isometría de $[n,l]_q$-códigos no redundantes para todo $l \leq k$, es decir $T_{[n,k]_q} = \bigcup_{l\leq k} V_{[n,l]_q}$

Corolario 2.3.15. *Veamos relaciones entre los números* $\mid T_{[n,k]_q} \mid, \mid V_{[n,k]_q} \mid, \mid U_{[n,k]_q} \mid$

(i) $\mid T_{[n,k]_q} \mid = \mid (\mathbb{F}_q\mathbb{P}^{k-1})^n/(GL_k(q)\times S_n) \mid$

(ii) $\mid V_{[n,k]_q} \mid = \mid T_{[n,k]_q} \mid - \mid T_{[n,k-1]_q} \mid$ *para* $1 < k \leq n$

(iii) $\mid U_{[n,k]_q} \mid = \sum_{k\leq i\leq n} \mid V_{[n,i]_q} \mid$

Así tenemos expresado $\mid V_{[n,k]_q} \mid$ y $\mid U_{[n,k]_q} \mid$ en términos de $\mid T_{[n,k]_q} \mid$, luego lo que nos resta es calcular el valor de $\mid T_{[n,k]_q} \mid$, y para esto utilizaremos algunas definiciones y teoremas que nos daran una función generadora para este número.

Definición 2.3.16. Sean X un conjunto finito y G un grupo finito que actúa sobre X.Denotamos por $a_i(g)$ con $i \in \{1, 2, ..., \mid X \mid\}$ y $g \in G$ al número de órbitas en X bajo la acción del grupo $\langle g \rangle$, de largo i, es decir

$$a_i(g) = \mid \{w \in (X/\langle g \rangle) \mid \mid w \mid = i\} \mid$$

Y a la secuencia

$$(a_1(g), ..., a_{|X|}(g))$$

la llamaremos tipo de ciclos de g (cycle type of g)

Definición 2.3.17. Sean X un conjunto finito y G un grupo finito que actúa sobre X. Se define el índice de ciclos de la acción del grupo G en el conjunto X, denotado por $C(G, X)$, como el polinomio

$$C(G, X) := \frac{1}{\mid G \mid} \sum_{g \in G} \prod_{i=1}^{|X|} z_i^{a_i(g)}$$

Teorema 2.3.18. *Sea H un grupo finito actuando en el conjunto finito Y. La función generadora para el número de órbitas generadas por la acción del grupo $(H \times S_n)$ en el conjunto Y^n es*

$$\sum_{i \in \mathbb{N}} \mid Y^n/(H \times S_n) \mid x^i = C(H, Y)$$

donde el lado derecho lo evaluamos en $z_i = \sum_{j=0}^{\infty} x^{ij}$

Corolario 2.3.19. *La función generadora para el valor $\mid T_{[n,k]_q} \mid$ es obtenida como sigue*

$$\sum_{i \in \mathbb{N}} \mid T_{[i,k]_q} \mid x^i = C(GL_k(q), \mathbb{F}_q\mathbb{P}^{k-1}) \mid_{z_i = \sum_{j=0}^{\infty}} x^{ij}$$

Ejemplo 2.3.20. *(i) Sea $q = k = 2$, entonces como $GL_2(2)$ consta de estas seis matrices*

$$g_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, g_2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, g_3 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, g_4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$g_5 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, g_6 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

y estas actúan de la siguiente manera en el conjunto

$$\mathbb{F}_2\mathbb{P}^1 = \mathbb{F}_2^2 \setminus \{0\} = \{1 = (0,1), 2 = (1,0), 3 = (1,1)\}$$

$1 \cdot g_1 = 2, \quad 2 \cdot g_1 = 1, \quad 3 \cdot g_1 = 3$ *luego* $\overline{g_1} = (12)(3)$
$1 \cdot g_2 = 2, \quad 2 \cdot g_2 = 3, \quad 3 \cdot g_2 = 1$ *luego* $\overline{g_2} = (123)$
$1 \cdot g_3 = 3, \quad 3 \cdot g_3 = 2, \quad 2 \cdot g_3 = 1$ *luego* $\overline{g_3} = (132)$
$1 \cdot g_4 = 1, \quad 2 \cdot g_4 = 2, \quad 3 \cdot g_4 = 3$ *luego* $\overline{g_4} = (1)(2)(3)$
$1 \cdot g_5 = 3, \quad 3 \cdot g_5 = 1, \quad 2 \cdot g_5 = 2$ *luego* $\overline{g_5} = (13)(2)$
$1 \cdot g_6 = 1, \quad 2 \cdot g_6 = 3, \quad 3 \cdot g_6 = 2$ *luego* $\overline{g_6} = (32)(1)$

Tenemos que

$$\overline{GL_2(2)} = \{(12)(3), (123), (132), (1)(2)(3), (13)(2), (32)(1)\} = S_3$$

Luego el tipo de ciclos de g_1 es (1, 1, 0), de g_2 es (0, 0, 1), de g_3 es (0, 0, 1), de g_4 es (3, 0, 0), de g_5 es (1, 1, 0), de g_6 es (1, 1, 0). Por lo que

$$C(GL_2(2), \mathbb{F}_2\mathbb{P}^1)) = \frac{1}{6} \sum_{g \in GL_2(2)} \prod_{i=1}^{3} z_i^{a_i(g)} = \frac{1}{|\,6\,|}(z_1z_2 + z_3 + z_3 + z_1^3 + z_1z_2 + z_1z_2)$$

$$= \frac{1}{|\,6\,|}(z_1^3 + 3z_1z_2 + 2z_3)$$

luego

$$\sum_{n \in \mathbb{N}} |\, T_{[n,2]_2} \,| \, x^n = C(GL_2(2), \mathbb{F}_2\mathbb{P}^1) \,|_{z_i = \sum_{j=0}^{\infty} x^{ij}}$$

Y ahora reemplazando $\quad z_1 = 1 + x + x^2 + x^3 .... = \dfrac{1}{1-x}$

$$z_2 = 1 + x^2 + x^4 + x^6 .... = \frac{1}{1-x^2}$$

$$z_3 = 1 + x^3 + x^6 + x^9 .... = \frac{1}{1-x^3}$$

Obtenemos que

$$\sum_{n \in \mathbb{N}} |\, T_{[n,2]_2} \,| \, x^n = 1 + x + 2x^2 + 3x^3 + 4x^4 + 5x^5 + 7x^6 + 8x^7 + 10x^8 .....$$

que notamos corresponde a la expansión de Taylor centrada en 0 de la función racional; luego

$$\frac{1}{6}\left(\left(\frac{1}{1-x}\right)^3+3\left(\left(\frac{1}{1-x}\right)\left(\frac{1}{1-x^2}\right)\right)+2\left(\frac{1}{x^3-1}\right)\right)$$

Y así
$\mid T_{[1,1]_2} \mid = 1,\ \mid T_{[2,1]_2} \mid = 2,\ \mid T_{[3,1]_2} \mid = 3,\ \mid T_{[4,1]_2} \mid = 4,\ \mid T_{[5,1]_2} \mid = 5,$
$\mid T_{[6,1]_2} \mid = 7,\ \mid T_{[7,1]_2} \mid = 8, \mid T_{[8,1]_2} \mid = 10$

Ahora para saber el valor de $\mid V_{[n,2]_2} \mid$ *necesitamos el valor de* $\mid T_{[n,1]_2} \mid$. *Este se puede calcular fácilmente ya que* $\mid T_{[n,1]_2} \mid = 1\ \forall\ n \in \mathbb{N}$. *Luego*

$\mid V_{[1,2]_2} \mid = 0,\ \mid V_{[2,2]_2} \mid = 1,\ \mid V_{[3,2]_2} \mid = 2,\ \mid V_{[4,2]_2} \mid = 3,\ \mid V_{[5,2]_2} \mid = 4,$
$\mid V_{[6,2]_2} \mid = 6,\ \mid V_{[7,2]_2} \mid = 7, \mid V_{[8,2]_2} \mid = 9$

Y así que
$\mid U_{[1,2]_2} \mid = 0,\ \mid U_{[2,2]_2} \mid = 1,\ \mid U_{[3,2]_2} \mid = 3,\ \mid U_{[4,2]_2} \mid = 6,\ \mid U_{[5,2]_2} \mid = 10,$
$\mid U_{[6,2]_2} \mid = 16,\ \mid U_{[7,2]_2} \mid = 23, \mid U_{[8,2]_2} \mid = 32$

(ii) Sea $q = 2$ *y* $k = 3$, *al hacer actuar el grupo* $GL_3(2)$ *sobre el conjunto* $\mathbb{F}_2\mathbb{P}^2 = \mathbb{F}_2^3 \setminus \{0\}$, *obtenemos que*

$$\overline{GL_3(2)} = \langle (45)(67), (46)(57), (23)(67), (24)(35), (12)(56) \rangle$$

Lo que necesitamos encontrar es el tipo de ciclo de cada elemento de $GL_3(2)$, *es decir necesitamos saber la estructura cíclica de cada elemento de* $\overline{GL_3(2)}$. *Para esto utilizaremos el hecho, de que los elementos de las clases de conjungación de un subgrupo de permutaciones tienen la misma estructura cíclica.*
Por lo tanto, si conocemos las clases de conjugación de $\overline{GL_3(2)} \leq S_7$ *y la cantidad de elementos que posee cada una de estas, podremos obtener* $C(GL_3(2), \mathbb{F}_2\mathbb{P}^2)$.

Así las clases de conjugación de $\overline{GL_3(2)}$ *son*
$\{(1)(2)(3)(4)(5)(6)(7), (1)(2)(3)(45)(67), (1)(23)(4657), (1)(246)(357), (1243675), (1245736)\}$
y las cantitades de elementos por cada clase de conjugación son 1, 21, 42, 56, 24, 24 respectivamente.Así

$$C(GL_3(2), \mathbb{F}_2\mathbb{P}^2) = \frac{1}{\mid 6 \mid}(z_1^7 + 21z_1^3z_2^2 + 42z_1z_2z_4 + 56z_1z_3^2 + 48z_7)$$

por lo cual

$$\sum_{n\in\mathbb{N}} \mid T_{[n,3]_2} \mid x^n = 1+x+2x^2+4x^3+7x^4+11x^5+19x^6+29x^7+44x^8.....$$

Y así
$\mid T_{[1,3]_2} \mid = 1, \mid T_{[2,3]_2} \mid = 2, \mid T_{[3,3]_2} \mid = 4, \mid T_{[4,3]_2} \mid = 7, \mid T_{[5,3]_2} \mid = 11,$
$\mid T_{[6,3]_2} \mid = 19, \mid T_{[7,3]_2} \mid = 29, \mid T_{[8,3]_2} \mid = 44$

Ahora para saber el valor de $\mid V_{[n,2]_2} \mid$ *necesitamos el valor de* $\mid T_{[n,2]_2} \mid$ *el cual ya tenemos. Luego*

$\mid V_{[1,3]_2} \mid = 0, \mid V_{[2,3]_2} \mid = 0, \mid V_{[3,3]_2} \mid = 1, \mid V_{[4,3]_2} \mid = 3, \mid V_{[5,3]_2} \mid = 6,$
$\mid V_{[6,3]_2} \mid = 12, \mid V_{[7,3]_2} \mid = 21, \mid V_{[8,3]_2} \mid = 34$

Y así que
$\mid U_{[1,3]_2} \mid = 0, \mid U_{[2,3]_2} \mid = 0, \mid U_{[3,3]_2} \mid = 1, \mid U_{[4,3]_2} \mid = 4, \mid U_{[5,3]_2} \mid = 10,$
$\mid U_{[6,3]_2} \mid = 22, \mid U_{[7,3]_2} \mid = 43, \mid U_{[8,3]_2} \mid = 77$

Capítulo 3

Construcción de Códigos lineales con distancia mínima prescrita.

3.1. Caracterización de matrices generadoras de Códigos lineales con distancia mínima prescrita.

El propósito en este capítulo es mostrar un método para construir un $[n, k, d]_q$- código fijando una distancia mínima d. Teniendo en cuenta que queremos de alguna manera encontrar códigos que alcanzen la Cota de Griesmer 1.2.12.

Como lo que queremos en particular es costruir códigos lineales, y sabemos que estos parten de una matriz generadora, comenzaremos con un examen más detallado de ésta, para poder relacionarla con la distancia mínima del código lineal generado por ella.

Sea C un $[n, k, d]_q$- código, generado por la matriz $\Gamma = (\gamma_i^t)$, nuestro primer objetivo es encontrar relaciones entre el conjunto de las columnas de esta matriz $\gamma = \{\gamma_1, \gamma_2, ..., \gamma_n\}$ y la distancia mínima d de C. Para encontrar estas relaciones, como estamos restringiendo nuestro estudio a códigos lineales, donde la distancia mínima coincide con el peso mínimo, comenzaremos buscando relaciones entre el peso de una palabra $c \in C$ y las columnas de Γ.

Observación 3.1.1. Recordemos que $w(c)$, denota las coordenadas de la palabra c distintas de cero, por lo tanto $n - w(c)$ corresponde a la cantidad

de coordenadas iguales a cero de c.
Así también si c la escribimos en términos de la forma bilineal estandar ($< v, w >= \sum_{i=1}^{k} v_i w_i$ para todo $v, w \in \mathbb{F}_q^k$)

$$c = v\Gamma = (< v, \gamma_1 >, < v, \gamma_2 >, \cdots, < v, \gamma_{n-1} >, < v, \gamma_n >) \quad v \in \mathbb{F}_q^k$$

podemos observar, que si $c_i = 0$, implica que γ_i es ortogonal al vector mensaje v.
Uniendo nuestros dos resultados podemos concluir que hay $n - w(c)$ columnas de la matriz generadora que son ortogonales con el vector mensaje v. Es decir que el hiperplano

$$H(v) = \{w \in \mathbb{F}_q^k \mid < v, w >= 0\}$$

contiene exactamente $n - w(c)$ columnas de la matriz generadora Γ.

De estas observaciones se desprende el siguiente teorema que relaciona a la matriz generadora de un código lineal con la distancia mínima de este.

Teorema 3.1.2. *Una matriz Γ de $(k \times n)$ es una matriz generadora de un $[n, k, d]_q$- código si y sólo si satisface las siguientes condiciones*

i) Todo hiperplano $H(v)$ con $v \in \mathbb{F}_q^k \backslash \{0\}$ contiene a lo más $n-d$ columnas de Γ.

ii) Existe al menos un hiperplano $H(v)$ que contiene exactamente $n - d$ columnas de Γ.

DEMOSTRACIÓN: Supongamos que Γ es una matriz generadora de un $[n, k, d]_q$-código C, tal que Γ no cumple la condición i). Entonces existe un vector $v \in \mathbb{F}_q^k \backslash \{0\}$ tal que $H(v)$ contiene más de $n - d$ columnas de Γ, lo que implica que la palabra $c = v\Gamma \in C$ posee más de $n - d$ ceros, por lo cual $w(c)$ es menor que d, lo que produce una contradición.
Así también como C posee distancia mínima d, tenemos que existe una palabra $c = v\Gamma \in C$ con $w(c) = d$ y $n - d$ coordenadas igual a cero, lo que equivale a decir que el hiperplano $H(v)$ contiene exactamente $n - d$ columnas de Γ, lo que demuestra ii)
Ahora supongamos que Γ cumple con las condiciones i) y ii).Por la condición i) tenemos que el código lineal C generado por Γ posee solo palabras con peso menor o igual a d y por los condición ii) tenemos que existe una palabra en C con peso d, lo que implica que C posee distancia mínima d.
Lo que nos falta demostrar, es que C como subespacio de $\mathbb{F}_q^k$ sobre $\mathbb{F}_q$ tenga

dimensión k, para esto procederemos por contradicción.
Supongamos que el rango de Γ es menor que k, así las filas de Γ son linealmente dependientes, luego existe un vector $v \in \mathbb{F}_q^k \backslash \{0\}$ tal que

$$c = v\Gamma = 0$$

Esto implica que $H(v)$ contiene todas las columnas de Γ, lo que contradice la condición i).

□

Este teorema, nos da una idea de como generar códigos lineales con una distancia mínima prescrita, ya que teniendo un multiconjunto de vectores, es decir un conjunto en el cual se pueden repetir los elementos (denotado por $\{\{\}\}$), que cumpla con las condiciones dadas en el teorema anterior, podemos crear una matriz Γ en que todos los vectores de este conjunto sean columnas de esta matriz, de este modo Γ es una matriz generadora de un $[n,k,d]_q$-código.
En el cápitulo anterior estudiamos cuando dos códigos son isométricos, ahora queremos ver qué condiciones cumplen las columnas de la matrices generadoras de estos códigos para así en el proceso de construcción poder descartar la mayor cantidad de códigos isométricos.

Si recordamos la observación 2.2.7, donde se define la acción del grupo de isometrías lineales $M_n(q)$ en el conjunto $\mathbb{F}_q^{k\times n,k}$, de la siguiente manera

$$\begin{aligned} M_n(q) \times \mathbb{F}_q^{k\times n,k} &\longrightarrow \mathbb{F}_q^{k\times n,k} \\ (M_{(\varphi,\sigma)} \ , \ \Gamma) &\longmapsto \Gamma \ M_{(\varphi,\sigma)}^t \end{aligned}$$

donde la (n,n)-matriz $M_{\varphi,\sigma} = (a_{i,j})$ es de la forma,

$$a_{i,j} = \begin{cases} \varphi_{\sigma(i)} & \text{si } j = \sigma(i) \\ 0 & \text{en otro caso} \end{cases}$$

Tenemos que

$$\Gamma \ M_{(\varphi,\sigma)}^t = (\ \varphi_1\gamma_{\sigma^{-1}(1)}^t \mid \varphi_2\gamma_{\sigma^{-1}(2)}^t \mid \cdots \mid \varphi_n\gamma_{\sigma^{-1}(n)}^t\ ) \quad \text{con } \gamma_i \in \mathbb{F}_q^k,\ i \in \{1,2,...,n\}$$

De aquí podemos deducir que una sucesión de las siguientes operaciones en las columnas de una matriz Γ, producen una matriz Γ' la cual genera un código lineal isométrico al código generado por Γ:

1. La ponderación de columnas por elementos de $\mathbb{F}_q^* = (\mathbb{F}_q \backslash \{0\})$

2. La permutación de columnas.

Es importante recordar que $\mathbb{F}_q^{k\times n,k}/M_n(q)$ es una partición en el conjunto de matrices generadoras, pero no representa una partición en el conjunto $U[n,k]_q$ de todos los $[n,k]_q$-códigos.

También si $\Gamma = (\gamma_i^t)$ con $i \in \{1,2,...,n\}$ es una matriz generadora de un código lineal no redundante, esta se puede representar por la función

$$\gamma : \{1,2,...,n\} \longrightarrow \mathbb{F}_q^k \backslash \{0\}$$

$$i \longmapsto \gamma_i$$

Y luego por la condición 1., la función $\widetilde{\gamma}$ representa a una matriz generadora de un código isométrico al generado por Γ.

$$\widetilde{\gamma} : \{1,2,...,n\} \longrightarrow \mathbb{F}_q\mathbb{P}^{k-1}$$

$$i \longmapsto [\gamma_i]$$

De la siguiente manera; colocando como columna i-ésima de la matriz $\widetilde{\Gamma}$ un representante cualquiera de la órbita $[\gamma_i]$. Más aún, debido a la condición 2.la función $\widetilde{\gamma}_\sigma$ representa a una matriz generadora de un código isométrico al generado por Γ.

$$\widetilde{\gamma}_\sigma : \{1,2,...,n\} \longrightarrow \mathbb{F}_q\mathbb{P}^{k-1}$$

$$i \longmapsto [\gamma_{\sigma^{-1}(i)}]$$

utilizando el mismo método anteriormente descrito.

Definición 3.1.3. Sea $[v] \in \mathbb{F}_q\mathbb{P}^{k-1}$ denotamos por $H[v]$ al subconjunto de $\mathbb{F}_q\mathbb{P}^{k-1}$ que se define, en analogía con $H(v)$, por

$$H[v] = \{[w] \in \mathbb{F}_q\mathbb{P}^{k-1} \mid < v, w >= 0\}$$

Observación 3.1.4. $w \in H(v) \Leftrightarrow [w] \in H[v] \Leftrightarrow [v] \in H[w]$

Ahora estamos en condiciones de reescribir el teorema 3.1.2 en términos de multiconjuntos.

Teorema 3.1.5. *Existe un $[n,k,d]_q$-código no redundante si y sólo si existe un multiconjunto χ de $\mathbb{F}_q\mathbb{P}^{k-1}$ de orden n tal que*

$$\text{máx}\{|\chi \cap H[v]| \mid [v] \in \mathbb{F}_q\mathbb{P}^{k-1}\} = n - d$$

DEMOSTRACIÓN: Sea C un $[n,k,d]_q$-código no redundante, y sea $\Gamma = (\gamma_i^t)$ la matriz generadora de C, luego el multiconjunto $\gamma = \{\{[\gamma_1], ..., [\gamma_n]\}\}$ es un multiconjunto de $\mathbb{F}_q\mathbb{P}^{k-1}$ de orden n. Ahora como C posee distancia mínima d, tenemos por teorema 3.1.2, que todo hiperplano $H(v)$ con $v \in \mathbb{F}_q^k$ contiene a lo más $n-d$ columnas de Γ, lo que implica que el

$$\text{máx}\{|\chi \cap H[v]| \mid v \in \mathbb{F}_q^k\} \leq n-d$$

y que existe a lo menos un hiperplano $H(v)$ que contiene exactamente $n-d$ columnas de Γ, es decir que este máximo se alcanza.
Sea $\chi = \{\{[\chi_1], ..., [\chi_n]\}\}$ un multiconjunto de $\mathbb{F}_q\mathbb{P}^{k-1}$ de orden n tal que $\text{máx}\{|\chi \cap H[v]| \mid v \in \mathbb{F}_q^k\} = n-d$, esto implica que si $\chi = \{\{\chi_1, ..., \chi_n\}\}$ entonces $\text{máx}\{|\chi \cap H(v)| \mid v \in \mathbb{F}_q^k\} = n-d$, luego por el teorema 3.1.2 tenemos que la matriz $\Gamma = (\chi_i^t)$ genera un $[n,k,d]_q$- código no redundante.

□

Definición 3.1.6. Un $[n,k]_q$-código es llamado proyectivo si las columnas de cualquier matriz generadora de éste son a pares linealmente independientes.

Ahora nos vamos a restringir a conjuntos, y así generar códigos lineales proyectivos

Corolario 3.1.7. *Existe un $[n,k,d]_q$-código proyectivo si y sólo si existe un conjunto X de $\mathbb{F}_q\mathbb{P}^{k-1}$ de orden n tal que*

$$\text{máx}\{|X \cap H[v]| \mid v \in \mathbb{F}_q^k\} = n-d$$

Así nuestro estudio se restringe a la busqueda de conjuntos $X \subseteq \mathbb{F}_q\mathbb{P}^{k-1}$ que cumplan ciertas condiciones.

3.1.1. Minihypers, T-Bloques y Grafos

Con el propósito de facilitar nuestro trabajo, buscaremos los complementos de estos conjuntos, que ya han sido estudiados en el aréa de la Geometría Proyectiva Finita, donde hay resultados que nos serán de mucha utilidad . A tales conjuntos se les llama minihyper.

Definición 3.1.8. Un (b,t)-minihyper en $\mathbb{F}_q\mathbb{P}^{k-1}$, es un conjunto B de $\mathbb{F}_q\mathbb{P}^{k-1}$ tal que

$$|B| = b \quad \text{y} \quad \text{mín}\{|B \cap H[v]| \mid [v] \in \mathbb{F}_q\mathbb{P}^{k-1}\} = t$$

Corolario 3.1.9. *(Hamada)[7] Existe un $[n,k,d]_q$-código proyectivo si y sólo si existe un (b,t)-minihyper en $\mathbb{F}_q\mathbb{P}^{k-1}$ con*

$$(b,t) = (\theta_{k-1}(q) - n, \theta_{k-2}(q) - (n-d))$$

recordando que $\theta_{k-1}(q) = |\ \mathbb{F}_q\mathbb{P}^{k-1}\ | = \dfrac{q^k-1}{q-1}$

DEMOSTRACIÓN: Sea C un $[n,k,d]_q$-código lineal proyectivo, y sea Γ una matriz generadora de C, llamemos γ al subconjunto de $\mathbb{F}_q\mathbb{P}^{k-1}$ definido por $\gamma = \{[\gamma_i] \mid \gamma_i^t$ es una columna de $\Gamma\}$ este conjunto cumple con

I. $\gamma \subseteq \mathbb{F}_q\mathbb{P}^{k-1}$, $|\gamma| = n$, ya que C es un código proyectivo de largo n.

II. $\max\{|\gamma \cap H[v]| \mid [v] \in \mathbb{F}_q\mathbb{P}^{k-1}\} = n-d$, ya que C posee distancia mínima d.

Luego el conjunto γ^c cumple con

$\gamma^c \subseteq \mathbb{F}_q\mathbb{P}^{k-1}$, $|\gamma^c| = \theta_{k-1}(q) - n$, por I.

$\min\{|\gamma^c \cap H[v]| \mid [v] \in \mathbb{F}_q\mathbb{P}^{k-1}\} = \theta_{k-2}(q) - (n-d)$, por II., donde $\theta_{k-2}(q)$ es la cardinalidad de $H[v]$ para cualquier $[v] \in \mathbb{F}_q\mathbb{P}^{k-1}$

y así γ^c es un $(\theta_{k-1}(q) - n, \theta_{k-2}(q) - (n-d))$-minihyper.

Ahora demostremos el recíproco. Sea B un $(\theta_{k-1}(q) - n, \theta_{k-2}(q) - (n-d))$-minihyper, luego el conjunto B^c cumple con

1. $B^c \subseteq \mathbb{F}_q\mathbb{P}^{k-1}$, $|B^c| = n$

2. $\max\{|B^c \cap H[v]| \mid [v] \in \mathbb{F}_q\mathbb{P}^{k-1}\} = n-d$

Luego si formamos la matriz Γ, tal que b es una columna de γ para cada $[b] \in B$, tenemos que Γ por la condición 1 es la matriz generadora de un código proyectivo de largo n, y por la condición 2, este posee distancia mínima d.

□

Tambien dentro del area de la Geometría proyectiva finita, se definen otros conjuntos llamados t-bloque que poseen menos características que los minihypers, pero que han sido muy estudiados y hay resultados sobre la existencia de estos conjuntos, que también nos serán de mucha utilidad.

Definición 3.1.10. Un t-bloque en $\mathbb{F}_q\mathbb{P}^{k-1}$ es un conjunto $B \subseteq \mathbb{F}_q\mathbb{P}^{k-1}$ tal que

$$\text{mín}\{|B \cap H[v]| \mid [v] \in \mathbb{F}_q\mathbb{P}^{k-1}\} \geq t$$

Ahora introduciremos el concepto de grafo y luego matriz de adyacencia, para poder facilitar la forma de encontrar estos conjuntos de $\mathbb{F}_q\mathbb{P}^{k-1}$

Definición 3.1.11. Un grafo G es un par $G = (V, E)$, donde V es un conjunto finito y E es un multiconjunto de pares no ordenados de V. Llamamos a cada elemento $v \in V$ vértice y cada par no ordenado $\{v, w\} \in E$ arista. Denotamos por $V(G)$ al conjunto de vértices y $E(G)$ al conjunto de aristas de G.

Definición 3.1.12. Dos vértices v y w de un grafo G se dicen adyacentes si $\{v, w\} \in E(G)$.

Definición 3.1.13. Sea G un grafo con $V(G) = \{v_1, ..., v_\nu\}$ y $E(G) = \{e_1, ..., e_\epsilon\}$, definimos la matriz de adyacencia de G como la $\nu \times \nu$-matriz $A(G) = (a_{ij})$ donde $a_{ij} = 1$ es el número de aristas $\{v_i, v_j\} \in E(G)$.

Ahora reescribiremos lo estudiado en términos de estas definiciones.

Observación 3.1.14. Formemos el grafo G, donde

$$V(G) = \mathbb{F}_q\mathbb{P}^{k-1} = \{P_1, ..., P_{\theta_{k-1}(q)}\} \quad \text{donde} \quad \theta_{k-1}(q) = \frac{q^k - 1}{q - 1}$$

$$E(G) = \{\{P_i, P_j\} \mid P_i \in H(P_j)\}$$

Luego la matriz de adyacencia de G, puede ser descrita de la siguiente forma:

$A(G) = (a_{ij})$ donde $a_{ij} = 1$ si el par no ordenado $\{P_i, P_j\} \in E(G)$, lo que implica que si $P_i \in H(P_j)$ y $a_{ij} = 0$ en otro caso, es decir;

$$a_{ij} = \begin{cases} 1 & si \quad P_i \in H(P_j) \\ 0 & \text{en otro caso} \end{cases}$$

Luego como un t-bloque es una selección conveniente de puntos de $\mathbb{F}_q\mathbb{P}^{k-1}$, éste puede ser descrito por la matriz de adyacencia del grafo G, de la siguiente manera:

Observación 3.1.15. Si B es un t-bloque de $\mathbb{F}_q\mathbb{P}^{k-1}$, le asociamos el vector $x = (x_1, ..., x_{\theta_{k-1}(q)})$

$$\text{talque } x_i = \begin{cases} 1 & P_i \in B \\ \\ 0 & \text{en otro caso} \end{cases}$$

así obtenemos la propiedad:

$$A(G)x = \begin{pmatrix} y_1 \\ . \\ . \\ . \\ y_{\theta_{k-1}(q)} \end{pmatrix} \quad \text{donde} \quad y_i \in \{t, ..., \theta_{k-2}(q)\} \tag{3.1}$$

Luego el recíproco también se cumple, es decir, si tenemos un vector $x = (x_1, ..., x_{\theta_{k-1}(q)})$ con $x_i \in \{0, 1\}$ tal que cumpla con (3.1), podemos asociarle un t-bloque B tal que

$$B = \{P_j \mid x_j = 1\}$$

De aquí se desprende el siguiente corolario

Corolario 3.1.16. *Existe una biyección entre el conjunto de todos los t-bloque de $\mathbb{F}_q\mathbb{P}^{k-1}$ y el conjunto de vectores $\begin{pmatrix} x \\ y \end{pmatrix}$ con $x = (x_1, ..., x_{\theta_{k-1}(q)})$ donde $x_i \in \{0, 1\}$ e $y = (y_1, ..., y_{\theta_{k-1}(q)})$ donde $y_i \in \{t, ..., \theta_{k-2}(q)\}$ que resuelve el sistema*

$$(A(G)| - I)\begin{pmatrix} x \\ y \end{pmatrix} = 0 \tag{3.2}$$

Si $\begin{pmatrix} x \\ y \end{pmatrix}$ cumple con (3.2) entonces el correspondiente t-bloque de $\mathbb{F}_q\mathbb{P}^{k-1}$ es

$$B = \{P_j \mid x_j = 1\}$$

Luego reuniendo todos los resultados expuestos, tenemos que

Lema 3.1.17. *Existe una biyección entre el conjunto de todos los* $[n,k,d]_q$*-códigos proyectivos, con* $n < \theta_{k-1}(q)$ *y* $d \geqslant t$, *y el conjunto de vectores* $\begin{pmatrix} x \\ y \end{pmatrix}$ *con* $x = (x_1, ..., x_{\theta_{k-1}(q)})$ *donde* $x_i \in \{0,1\}$ *e* $y = (y_1, ..., y_{\theta_{k-1}(q)})$ *donde* $y_i \in \{t, ..., \theta_{k-2}(q)\}$ *que resuelve el sistema 3.2*

Si $\begin{pmatrix} x \\ y \end{pmatrix}$ *cumple con (3.2) entonces el correspondiente*$[n,k,d]_q$*-códigos lineales proyectivos sobre* $\mathbb{F}_q$ *es el generado por la matriz* $\Gamma = (\gamma_i^t)$ *tal que*

$$[\gamma_i] \in \{P_j \mid x_j = 1\}^C \quad \forall i \in \{1, 2...n\}$$

con $[\gamma_i] \neq [\gamma_j] \quad \forall i \neq j$.

Ahora veamos un ejemplo.

Ejemplo 3.1.18. *Sea* $k = 3$ *y* $q = 3$, *nuestro propósito es encontrar un vector* x *tal que cumpla con (3.1). El grafo con el que trabajaremos es* $G = (\mathbb{F}_3\mathbb{P}^2, E(G))$ *donde tenemos que la cardinalidad del conjunto* $\mathbb{F}_3\mathbb{P}^2$ *es* $\theta_2(3) = \frac{3^3-1}{3-1} = 13$ *y este conjunto es*

$\mathbb{F}_3\mathbb{P}^2 = \{P_1 = [(0,0,1)], P_2 = [(0,1,0)], P_3 = [(0,1,0)], P_4 = [(0,1,2)], P_5 = [(1,0,0)],$
$P_6 = [\,(1,0,1)], P_7 = [(1,0,2)], P_8 = [(1,1,0)], P_9 = [(1,1,1)], P_{10} = [(1,1,2)],$
$P_{11} = [(1,2,0)], P_{12} = [(1,2,1)], P_{13} = [(1,2,2)]\}$

$H = \{H(P_1) = \{P_2, P_5, P_8, P_{11}\}, H(P_2) = \{P_1, P_5, P_6, P_7\}, H(P_3) = \{P_4, P_5, P_{10}, P_{12}\},$
$H(P_4) = \{P_3, P_5, P_{11}, P_{13}\}, H(P_5) = \{P_1, P_2, P_3, P_4\}, H(P_6) = \{P_2, P_7, P_{10}, P_{13}\},$
$H(P_7) = \{P_2, P_6, P_9, P_{12}\}, H(P_8) = \{P_1, P_{11}, P_{12}, P_{13}\}, H(P_9) = \{P_4, P_7, P_9, P_{11}\},$
$H(P_{10}) = \{P_3, P_6, P_{10}, P_{11}\}, H(P_{11}) = \{P_1, P_8, P_9, P_{10}\}, H(P_{12}) = \{P_3, P_7, P_8, P_{12}\},$
$H(P_{13}) = \{P_4, P_6, P_8, P_{13}\}\}$

$E(G) = \{\{P_1, P_2\}, \{P_1, P_5\}, \{P_1, P_8\}, \{P_1, P_{11}\}, \{P_2, P_5\}, \{P_2, P_6\}, \{P_2, P_7\}, \{P_3, P_4\}, \{P_3, P_5\}, \{P_3, P_{10}\}, \{P_3, P_{12}\}$
$\{P_4, P_5\}, \{P_4, P_{11}, \}, \{P_4, P_{13}\}, \{P_6, P_7\}, \{P_6, P_{10}\}, \{P_6, P_{13}\}, \{P_7, P_9\}, \{P_7, P_{12}\}, \{P_8, P_{11}\}, \{P_8, P_{12}\},$
$\{P_8, P_{13}\}, \{P_9, P_9\}, \{P_9, P_{11}, \}, \{P_{10}, P_{10}\}, \{P_{10}, P_{11}\}, \{P_{12}, P_{12}\}, \{P_{13}, P_{13}\},$

Y así la matriz de adyacencia de G *es:*

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

Luego el vector $x = (1,1,1,1,0,0,0,0,0,0,0,0,0]$ *al multiplicarlo por la matriz de adyacencia*

$$A(G)x = (1,1,1,1,4,1,1,1,1,1,1,1,1) \in \{1,2,...,13\}^{13}$$

con lo cual x *cumple la condición 3.1 con* $t = 21$.

De aquí sigue que este vector x *esta en correspondencia con un 1-bloque el cual es*

$$B = \{P_1, P_2, P_3, P_4\}$$

Notemos que este 1-bloque B *es un* $(4,1)$*-minihyper el que esta en correspondencia con un* $[n,3,d]_3$*-código proyectivo donde*

$$(4,1) = (13-n, 4-n+d)$$

de donde se desprende que $n = 9$ *y* $d = 6$*, el cual es un código que alcanza la cota de Griesmer ya que,*

$$\sum_{j=0}^{2} \left\lceil \frac{6}{3^j} \right\rceil = 6+2+1 = 9.$$

Este código lineal tiene como matriz generadora Γ*, a la matriz cuyas columnas son los representantes de cada clase perteneciente a*
$B^c = \{P_5, P_6, P_7, P_8, P_9, P_{10}, P_{11}, P_{12}, P_{13}\}$*, como por ejemplo;*

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

3.1.2. Con Grupo de Automorfismos fijo

El método aquí mostrado nos sirve para construir códigos lineales proyectivos con una distancia mínima mayor o igual a un t fijo,el problema con el cual nos encontramos es que el tamaño de la matriz de adyacencia puede llegar a ser muy grande, que ni siquiera computacionalmente se puede resolver el problema expuesto en la observación 3.1.15, es por esto que buscaremos otro método que reduzca el tamaño de esta matriz .

Para el procedimiento utilizaremos la acción del grupo $GL_k(q)$ en $\mathbb{F}_q\mathbb{P}^{k-1}$, definida por

$$\begin{aligned}(\cdot) := \quad GL_k(q) \times \mathbb{F}_q\mathbb{P}^{k-1} &\longrightarrow \mathbb{F}_q\mathbb{P}^{k-1} \\ (\ M,\ \ [v]\ ) &\longmapsto [vM^t]\end{aligned}$$

así también se define la acción de $GL_k(q)$ en el conjunto
$H = \{H[v] \mid [v] \in \mathbb{F}_q\mathbb{P}^k\}$

$$\begin{aligned}(*) := \quad GL_k(q) \times H &\longrightarrow H \\ (\ M,\ \ H[v]\ ) &\longmapsto H[vM^{-1}]\end{aligned}$$

Observación 3.1.19. Si $[v]$, $[w] \in \mathbb{F}_q\mathbb{P}^{k-1}$ y $K \leq GL_k(q)$ tenemos que

$$|[[v]] \cap [H[w]]| = |[[v]] \cap H[w]| \quad \forall\, M \in K$$

es decir no depende del representante de la clase $[H[w]]$ escogido.

DEMOSTRACIÓN: Sea $H[w_1] \in [H[w]]$, tenemos que $H[w_1] = H[wM^{-1}]$ para algún $M \in K$. Luego tenemos que: $[v_1] \in ([[v]] \cap H[w_1])$

$\Leftrightarrow [v_1] \in H[w_1]$ y $[v_1] \in [[v]]$

$\Leftrightarrow [v_1] \in H[wM^{-1}]$ y $[v_1] \in [[v]]$

$\Leftrightarrow < v_1, wM^{-1} >= 0$ y $[v_1] \in [[v]]$

$\Leftrightarrow < v_1(M^{-1})^t, w >= 0$ y $[v_1(M^{-1})^t] \in [[v]]$

$\Leftrightarrow [v_1(M^{-1})^t] \in H[w]$ y $[v_1(M^{-1})^t] \in [[v]]$

$\Leftrightarrow [v_1(M^{-1})^t] \in (H[w] \cap [[v]])$

□

Definición 3.1.20. Sean $M \in GL_k(q)$ y B un t-bloque de $\mathbb{F}_q\mathbb{P}^{k-1}$, decimos que M es un automorfismo de B, si M permuta los puntos de B, es decir;

$$MB := \{M \cdot P \mid P \in B\} = B$$

Observación 3.1.21. Sean B un t-bloque de $\mathbb{F}_q\mathbb{P}^{k-1}$y $K \leq GL_k(q)$,entonces K es un grupo de automorfismos de B, si y sólo si, B es una unión de K-órbitas de $\mathbb{F}_q\mathbb{P}^{k-1}$.

Enunciadas estas acciones y propiedades vamos a crear un nuevo grafo que posee una matriz de adyacencia, de menor tamaño que la ya mencionada, la cual utilizaremos para encontrar t-bloques de $\mathbb{F}_q\mathbb{P}^{k-1}$, con la característica de tener un grupo de automorfismos definido.

Observación 3.1.22. Sea $K \leq GL_k(q)$, formamos el grafo G^K donde

$$V(G^K) = \mathbb{F}_q\mathbb{P}^{k-1}/K = \{t_1, ..., t_r\}$$

donde $r = |\mathbb{F}_q\mathbb{P}^{k-1}/K|$ y

$$E(G^K) = \{\{\{t_i, t_j\} \mid t_i \cap H[\bar{t_j}] \neq \varnothing\}\}$$

luego la $r \times r$-matriz de adyacencia definida por este grafo es $A(G^K) = (a_{ij})$ donde $a_{ij} = |t_j \cap H[\bar{t_i}]|$.

Observación 3.1.23. Si B es un t-bloque de $\mathbb{F}_q\mathbb{P}^{k-1}$, y $K \leq GL_k(q)$ donde K es un grupo de automorfismos de B , a este t-bloque le podemos asociar el vector $x = (x_1, ..., x_r)$ con $r = |\mathbb{F}_q\mathbb{P}^{k-1}/K|$

$$\text{talque } x_i = \begin{cases} 1 & [P_i] \subseteq B \\ 0 & \text{en otro caso} \end{cases}$$

así obtenemos la propiedad:

$$A(G^k)x = \begin{pmatrix} y_1 \\ . \\ . \\ . \\ y_r \end{pmatrix} \quad \text{con} \quad y_i \in \{t, ..., \theta_{k-2}(q)\} \tag{3.3}$$

Luego el recíproco también se cumple, es decir, si tenemos un vector $x = (x_1, ..., x_r)$ con $x_i \in \{0, 1\}$ tal que cumpla con (3.3), podemos asociarle un t-bloque B de $\mathbb{F}_q\mathbb{P}^{k-1}$ con grupo de automorfismo K tal que

$$B = \bigcup_j \{[P_j] \mid x_j = 1\}$$

De aquí se desprende el siguiente teorema

Teorema 3.1.24. *Existe una biyección entre el conjunto de todos los t-bloque de $\mathbb{F}_q\mathbb{P}^{k-1}$ con el subgrupo $K \leq GL_{k-1}(q)$ como grupo de automorfismos y el conjunto de soluciones $\begin{pmatrix} x \\ y \end{pmatrix}$, con $x_i \in \{0,1\}$ y $y_i \in \{t, ..., \theta_{k-2}(q)\}$, que cumplan el siguiente sistema de ecuaciones lineales*

$$\begin{pmatrix} A(G^K) & -I \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 0 \tag{3.4}$$

donde $x = (x_1, ..., x_r)$, $y = (y_1, ..., y_r)$ con $r = |\mathbb{F}_q\mathbb{P}^{k-1}/K|$. Si $\begin{pmatrix} x \\ y \end{pmatrix}$ es una solución, entonces el correspondiente t-bloque B es:

$$B = \bigcup_j \{[P_j] \mid x_j = 1\}$$

Lema 3.1.25. *Existe una biyección entre el conjunto de todos los $[n, k, d]_q$-códigos proyectivos, con $n < \theta_{k-1}(q)$ y $d \geqslant t$ que posee al subgrupo $K \leq GL_{k-1}(q)$ como grupo de automorfismos, y el conjunto de vectores $\begin{pmatrix} x \\ y \end{pmatrix}$ con $x = (x_1, ..., x_r)$ donde $x_i \in \{0, 1\}$ e $y = (y_1, ..., y_r)$ con $r = |\mathbb{F}_q\mathbb{P}^{k-1}/K|$, donde $y_i \in \{t, ..., \theta_{k-2}(q)\}$ que resuelve el sistema (3.4).*

Si $\begin{pmatrix} x \\ y \end{pmatrix}$ cumple con (3.4) entonces el correspondiente $[n, k, d]_q$-código proyectivo es el generado por la $(n \times k)$-matriz $\Gamma = (\gamma_i^t)$ tal que

$$[\gamma_i] \in \left(\bigcup_j \{[P_j] \mid x_j = 1\} \right)^C \quad \forall i \in \{1, 2...n\}$$

con $[\gamma_i] \neq [\gamma_j] \quad \forall i \neq j$.

Ejemplo 3.1.26. *Sea $k = 3$ y $q = 3$, y sea*

$$K = \left\langle \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \right\rangle$$

Nuestro objetivo es encontrar t-bloques de $\mathbb{F}_3\mathbb{P}^2$ con grupo de automorfismos a K.
El grafo con el que trabajaremos es $G^K = (\mathbb{F}_3\mathbb{P}^2/K, E(G^K))$ donde los conjuntos

$\mathbb{F}_3\mathbb{P}^2 = \{P_1 = [(0,0,1)], P_2 = [(0,1,0)], P_3 = [(0,1,1)], P_4 = [(0,1,2)], P_5 = [(1,0,0)],$
$P_6 = [\,(1,0,1)], P_7 = [(1,0,2)], P_8 = [(1,1,0)], P_9 = [(1,1,1)], P_{10} = [(1,1,2)],$
$P_{11} = [(1,2,0)], P_{12} = [(1,2,1)], P_{13} = [(1,2,2)]\}$

$H = \{H(P_1) = \{P_2, P_5, P_8, P_{11}\}, H(P_2) = \{P_1, P_5, P_6, P_7\}, H(P_3) = \{P_4, P_5, P_{10}, P_{12}\},$
$H(P_4) = \{P_3, P_5, P_{11}, P_{13}\}, H(P_5) = \{P_1, P_2, P_3, P_4\}, H(P_6) = \{P_2, P_7, P_{10}, P_{13}\},$
$H(P_7) = \{P_2, P_6, P_9, P_{12}\}, H(P_8) = \{P_1, P_{11}, P_{12}, P_{13}\}, H(P_9) = \{P_4, P_7, P_9, P_{11}\},$
$H(P_{10}) = \{P_3, P_6, P_{10}, P_{11}\}, H(P_{11}) = \{P_1, P_8, P_9, P_{10}\}, H(P_{12}) = \{P_3, P_7, P_8, P_{12}\},$
$H(P_{13}) = \{P_4, P_6, P_8, P_{13}\}\}$

Luego el conjunto de K-órbitas en $\mathbb{F}_3\mathbb{P}^2$ es

$\mathbb{F}_3\mathbb{P}^2/K = \{t_1 = \{P_1, P_2, P_5\}, t_2 = \{P_3, P_6, P_8\}, t_3 = \{P_4, P_7, P_{11}\}, t_4 = \{P_9\},$
$t_5 = \{P_{10}, P_{12}, P_{13}\}\}$

y el conjunto de K-órbitas en H es

$H/K = \{[H[P_1]] = \{H[P_1], H[P_2], H[P_5]\}, [H[P_3]] = \{H[P_3], H[P_6], H[P_8]\}.$
$[H[P_4]] = \{H[P_4], H[P_7], H[P_{11}]\}, [H[P_9]] = \{H[P_9]\},$
$[H[P_{10}]] = \{H[P_{10}], H[P_{12}], H[P_{13}]\}\}$

Por lo cual, el conjunto de aristas del grafo G^k es

$E(G^K) = \{\{\{t_1, t_1\}, \{t_1, t_1\}, \{t_1, t_2\}, \{t_1, t_3\}, \{t_2, t_1\}, \{t_2, t_3\}, \{t_2, t_5\}, \{t_2, t_5\}, \{t_3, t_1\},$
$\{t_3, t_2\}, \{t_3, t_4\}, \{t_3, t_4\}, \{t_3, t_4\}, \{t_3, t_5\}, \{t_4, t_3\}, \{t_4, t_4\}, \{t_5, t_2\},$
$\{t_5, t_2\}, \{t_5, t_3\}, \{t_5, t_5\}\}\}$

Y así la matriz de adyacencia de G es:

$$A(G^K) = \begin{pmatrix} 2 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 2 \\ 1 & 1 & 0 & 3 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 2 & 1 & 0 & 1 \end{pmatrix}$$

Y así por ejemplo el vector $x = (0,0,1,1,0)$ *al multiplicarlo por la matriz de adyacencia*
$A(G^k)x = (1,1,3,2,1) \in \{1,2,3...,13\}^{13}$ *con lo cual* x *cumple la condición (3.4) con* $t = 1$. *Luego este vector* x *esta en correspondencia de un 1-bloque el cual es*

$$B = \{t_3, t_4\} = \{P_4, P_7, P_{11}, P_9\}$$

este 1-bloque B *es un* $(4,1)$*-minihyper el que está en correspondencia con un* $[n,3,d]_3$*-código proyectivo con grupo de automorfismo* K *donde*
$(4,1) = (13-n, 4-n+d)$ *de donde se desprende que* $n = 9$ *y* $d = 6$. *Este código lineal alcanza la cota de Griesmer ya que*

$$\sum_{j=0}^{2} \left\lceil \frac{6}{3^j} \right\rceil = 6+2+1 = 9$$

y tiene como matriz generadora Γ, *a la matriz cuyas columnas son los representantes de cada clase perteneciente a* $B^c = \{P_1, P_2, P_5, P_3, P_6, P_8, P_{10}, P_{12}, P_{13}\}$, *como por ejemplo;*

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

Mientras si escojemos $x = (1,0,1,1,0)$ *al multiplicarlo por la matriz de adyacencia*
$A(G^k)x = (2,3,5,1,1) \in \{1,2,3...,13\}^{13}$ *con lo cual* x *cumple la condición (3.4) con* $t = 1$. *Luego este vector* x *esta en correspondencia de un 1-bloque el cual es*

$$B = \{t_1, t_3, t_4\} = \{P_1, P_2, P_5, P_4, P_7, P_{11}, P_9\}$$

este 1-bloque B *es un* $(7,1)$*-minihyper el que esta en correspondencia con un* $[n,3,d]_3$*-código proyectivo con grupo de automorfismo a* K *donde*
$(7,1) = (13-n, 4-n+d)$ *de donde se desprende que* $n = 6$ *y* $d = 3$. *Este código lineal tiene como matriz generadora* β, *a la matriz cuyas columnas son los representantes de cada clase perteneciente a* $B^c = \{P_3, P_6, P_8, P_{10}, P_{12}, P_{13}\}$, *como por ejemplo;*

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

Capítulo 4

Construcción de códigos lineales proyectivos que alcanzan la Cota de Griesmer

Con la ayuda de la Geometría proyectiva finita en este capítulo, estudiaremos algunos teoremas que nos servirán para construir códigos lineales optimales, y demostrar la no existencia en algunos casos de códigos que alcanzen la cota de Griesmer. Cabe destacar que para que un código lineal sea optimal no es necesario que alcanze la cota de Griesmer.

Ejemplo 4.0.27. *Para $k = 4$, $q = 3$ y $d = 3$ la cota de Griesmer es*

$$\sum_{i=0}^{3} \left\lceil \frac{3}{3^i} \right\rceil = 3 + 1 + 1 + 1 = 6$$

y si existiera un $[6, 4, 3]_3$-código, debería satisfacer la cota de Hamming,

$$3^4 \sum_{i=0}^{1} \binom{7}{i} (3-1)^i = 3^4(1 + 14) = 1297 \geqslant 3^6 = 729$$

la cual no satisface.

Teorema 4.0.28. *(Innamorati y Maturo)[6] En $\mathbb{F}_q\mathbb{P}^2$, $q \geqslant 4$, existe un $(b, 1)$-minihyper para todo b tal que $2q - 1 \leqslant b \leqslant 3q - 3$.*

Corolario 4.0.29. *Si $q \geqslant 4$ existe un $[n, 3, d]_q$-código proyectivo que alcanza la cota de Griesmer para $n = q^2 - q + 2$ y $n = q^2 - q + 1$.*

DEMOSTRACIÓN: Del teorema anterior sabemos que existe un $(b,1)$-minihyper en $\mathbb{F}_q\mathbb{P}^2$ para todo b tal que $2q-1 \leqslant b \leqslant 3q-3$, y por corolario 3.1.9 tenemos que este minihyper está en correspondencia con un $[n,3,d]_q$-código proyectivo, donde

$$(b,1) = (\theta_2(q) - n, \theta_1(q) - n + d)$$

y de aquí se desprende que $n = q^2+q+1-b$ y $d = q^2+1-b$.

Luego si calculamos la cota de Griesmer para un $[q^2+q+1-b\,,3,\ q^2+1-b]_q$-código con $2q-1 \leqslant b \leqslant 3q-3$, tenemos que

$$\sum_{i=0}^{2} \left\lceil \frac{q^2+1-b}{q^i} \right\rceil = q^2+1-b+\left\lceil \frac{q^2+1-b}{q} \right\rceil + \left\lceil \frac{q^2+1-b}{q^2} \right\rceil$$

y así caemos en dos casos

1. Si $b = 2q-1$ ó $b = 2q$ tenemos que:

$$\sum_{i=0}^{2} \left\lceil \frac{q^2+1-b}{q^i} \right\rceil = q^2+1-b+q-1+1 = q^2+q+1-b = n$$

2. Si $2q+1 \leqslant b \leqslant 3q-3$ tenemos que:

$$\sum_{i=0}^{2} \left\lceil \frac{q^2+1-b}{q^i} \right\rceil = q^2+1-b+q-2+1 = q^2+q-b < n$$

□

Teorema 4.0.30. *(Hamada and Helleseth)[8] Sean k, q, y ϵ_0, ϵ_1 enteros tales que $k \geqslant 3$, $q > (\epsilon_0+\epsilon_1-1)^2$. Entonces F es un $(\epsilon_0+\epsilon_1(q+1),\epsilon_1)$-minihyper en $\mathbb{F}_q\mathbb{P}^{k-1}$ si y sólo si F es la unión disjunta de un conjunto de ϵ_0 puntos y ϵ_1 lineas.*

Corolario 4.0.31. *Sean k, q, y ϵ_0, ϵ_1 enteros positivos tales que $k \geqslant 3$, $q > (\epsilon_0+\epsilon_1-1)^2$. Entonces existe un $(\epsilon_0+\epsilon_1(q+1),\epsilon_1)$-minihyper en $\mathbb{F}_q\mathbb{P}^{k-1}$, si y sólos si existe un $[\theta_{k-1}(q) - (\epsilon_0+\epsilon_1(q+1)), k]_q$-código proyectivo que alcanza la cota de Griesmer .Además si $\Gamma = (\gamma_i^t)$ es la matriz generadora de un $[\theta_{k-1}(q) - (\epsilon_0+\epsilon_1(q+1)), k]_q$-código proyectivo que alcanza la cota de Griesmer el conjunto $\{[\gamma_1],...,[\gamma_n]\}^c$ es la unión disjunta de un conjunto de ϵ_0 puntos y ϵ_1 lineas en $\mathbb{F}_q\mathbb{P}^{k-1}$.*

DEMOSTRACIÓN: Supongamos que existe un $(\epsilon_0+\epsilon_1(q+1),\epsilon_1)$-minihyper, por el corolario 3.1.9, tenemos que existe un $[n,k,d]_q$-código, tal que

$$(\epsilon_0+\epsilon_1(q+1),\epsilon_1)=(\theta_{k-1}(q)-n,\theta_{k-2}(q)-n+d)$$

luego,

$$n=\theta_{k-1}(q)-\epsilon_0-\epsilon_1(q+1)$$

y

$$\begin{aligned} d &= \theta_{k-1}(q)-\theta_{k-2}(q)-\epsilon_0-q\epsilon_1 \\ &= q^{k-1}-\epsilon_0-q\epsilon_1 \end{aligned}$$

Luego la cota de Griesmer esta dada por:

$$\begin{aligned} \sum_{j=0}^{k-1}\left\lceil\frac{q^{k-1}-\epsilon_0-q\epsilon_1}{q^j}\right\rceil &= q^{k-1}-\epsilon_0-q\epsilon_1+\left\lceil q^{k-2}-\epsilon_1-\frac{\epsilon_0}{q}\right\rceil+\left\lceil q^{k-3}-\frac{q\epsilon_1+\epsilon_0}{q^2}\right\rceil \\ &\quad+\left\lceil q^{k-4}-\frac{q\epsilon_1+\epsilon_0}{q^3}\right\rceil+\ldots+\left\lceil 1-\frac{q\epsilon_1+\epsilon_0}{q^{k-1}}\right\rceil \end{aligned}$$

Ahora utilizando el hecho que $\lceil a-b\rceil=a-\lfloor b\rfloor$ para todo $a,b\in\mathbb{Q}$ donde $\lfloor x\rfloor$ corresponde al menor número entero más cercano a x (parte entera), obtenemos que

$$\begin{aligned} \sum_{j=0}^{k-1}\left\lceil\frac{q^{k-1}-\epsilon_0-q\epsilon_1}{q^j}\right\rceil &= q^{k-1}-\epsilon_0-q\epsilon_1+q^{k-2}-\epsilon_1-\left\lfloor\frac{\epsilon_0}{q}\right\rfloor+q^{k-3}-\left\lfloor\frac{q\epsilon_1+\epsilon_0}{q^2}\right\rfloor \\ &\quad+q^{k-4}-\left\lfloor\frac{q\epsilon_1+\epsilon_0}{q^3}\right\rfloor+\ldots+1-\left\lfloor\frac{q\epsilon_1+\epsilon_0}{q^{k-1}}\right\rfloor \end{aligned}$$

Luego por la condición $q>(\epsilon_0+\epsilon_1-1)^2$, tenemos que

$$\left\lfloor\frac{\epsilon_0}{q}\right\rfloor=\left\lfloor\frac{q\epsilon_1+\epsilon_0}{q^i}\right\rfloor=0\quad\forall\, i\in\{2,3\ldots k-1\}$$

Así

$$\begin{aligned} \sum_{j=0}^{k-1}\left\lceil\frac{q^{k-1}-\epsilon_0-q\epsilon_1}{q^j}\right\rceil &= q^{k-1}-\epsilon_0-q\epsilon_1+q^{k-2}-\epsilon_1+q^{k-3}+q^{k-4}+\ldots+1 \\ &= \theta_{k-1}(q)-\epsilon_0-\epsilon_1(q+1) \\ &= n \end{aligned}$$

Ahora supongamos existe un $[\theta_{k-1}(q) - (\epsilon_0 + \epsilon_1(q+1)), k]_q$-código proyectivo que alcanza la cota de Griesmer, luego la distancia mínima de este código es $d = q^{k-1} - \epsilon_0 - q\epsilon_1$. Luego por el corolario 3.1.9 tenemos que existe un $(b,t)-$ *minihyper* donde

$$(b,t) = (\theta_{k-1}(q) - \theta_{k-1}(q) + \epsilon_0 + \epsilon_1(q+1), \theta_{k-2}(q) - \theta_{k-1}(q) + \epsilon_0 + \epsilon_1(q+1) + q^{k-1} - \epsilon_0 - q\epsilon_1)$$

$$= (\epsilon_0 + \epsilon_1(q+1), \epsilon_1).$$

Además de la demostración del corolario 3.1.9 tenemos que si $\Gamma = (\gamma_i^t)$ es la matriz generadora de esté código el conjunto $B = \{[\gamma_1], [\gamma_2] \cdots [\gamma_n]\}^c$ corresponde a un $(\epsilon_0 + \epsilon_1(q+1), \epsilon_1)$-minihyper, y por el teorema anterior tenemos que B es la unión disjunta de un conjunto de ϵ_0 puntos y ϵ_1 lineas.

□

Ejemplo 4.0.32. *Sean $q = 5$, $k = 3$, $\epsilon_0 = 2$ y $\epsilon_1 = 1$, luego como $5 > (2+1-1)^2 = 4$, tenemos que para construir un $[n, 3, d]_5$-código proyectivo con $n = 5^2 + 5 + 1 - (2 + 1(5+1)) = 23$ y $d = 5^2 - 2 - 5 \cdot 1 = 18$ tenemos que formar la unión disjunta de 2 puntos y 1 linea en $\mathbb{F}_5\mathbb{P}^2$. Tomemos los puntos $P_0 = [1,0,0]$, $P_1 = [1,1,1]$ y la linea $H[[1,0,0]] = \{[0,1,0], [0,0,1], [0,1,1], [0,1,2], [0,1,3], [0,1,4]\}$ así por el teorema 4.0.30 formamos el $(b,1)$-minihyper con $b = 2 + 1(5+1) = 8$ dado por:*

$$\gamma = \{[1,0,0], [1,1,1], [0,1,0], [0,0,1], [0,1,1], [0,1,2], [0,1,3], [0,1,4]\}$$

que por el corolario 3.1.9 está en correspondencia con el $[23, 3, 18]_5$-código proyectivo que alcanza la cota de Griesmer ya que

$$\sum_{j=0}^{2} \left\lceil \frac{18}{5^j} \right\rceil = 18 + 4 + 1 = 23$$

donde la matriz generadora de este código como ya sabemos se construye con los representantes de cada elemento del conjunto γ^c como columnas de está matriz. Así una matriz generadora para esté código es

$$\Gamma = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 & 3 & 4 & 4 & 4 & 4 & 4 \\ 1 & 2 & 3 & 4 & 0 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 \end{pmatrix}$$

Lema 4.0.33. *Sea k, q, h, y λ_i con $i = \{1, 2...h\}$, números naturales tales que, $1 \leqslant k$, $0 \leqslant \lambda_1 \leqslant \lambda_2 ... \leqslant \lambda_h < k-1$ y a lo más hay $q-1$ valores repetidos de λ_i. Luego existe un $\left(\sum_{i=1}^{h} \theta_{\lambda_i}(q), \sum_{i=1}^{h} \theta_{\lambda_i - 1}(q)\right)$-minihyper en $\mathbb{F}_q\mathbb{P}^{k-1}$ si y sólo si existe un $[\theta_{k-1}(q) - \sum_{i=1}^{h} \theta_{\lambda_i}(q), k]_q$-código proyectivo que alcanza la cota de Griesmer .*

DEMOSTRACIÓN: Supongamos existe un $\left(\sum_{i=1}^{h} \theta_{\lambda_i}(q), \sum_{i=1}^{h} \theta_{\lambda_i - 1}(q)\right)$-minihyper, por el corolario 3.1.9, tenemos que existe un $[n, k, d]_q$-código, tal que

$$\left(\sum_{i=1}^{h} \theta_{\lambda_i}(q), \sum_{i=1}^{h} \theta_{\lambda_i - 1}(q)\right) = (\theta_{k-1}(q) - n, \theta_{k-2}(q) - n + d)$$

luego,

$$n = \theta_{k-1}(q) - \sum_{i=1}^{h} \theta_{\lambda_i}(q)$$

y

$$\begin{aligned} d &= \sum_{i=1}^{h} \theta_{\lambda_i - 1}(q) + \theta_{k-1}(q) - \sum_{i=1}^{h} \theta_{\lambda_i}(q) - \theta_{k-2}(q) \\ &= \theta_{k-1}(q) - \theta_{k-2}(q) + \sum_{i=1}^{h} \theta_{\lambda_i - 1}(q) - \theta_{\lambda_i}(q) \\ &= \frac{q^k - 1}{q-1} - \frac{q^{k-1} - 1}{q-1} + \sum_{i=1}^{h} \frac{q^{\lambda_i} - 1}{q-1} - \frac{q^{\lambda_i + 1} - 1}{q-1} \\ &= q^{k-1} - \sum_{i=1}^{h} q^{\lambda_i} \end{aligned}$$

Luego utilizando el hecho que que, $\lceil a - b \rceil = a - \lfloor b \rfloor$ para todo $a, b \in \mathbb{Q}$ donde $\lfloor x \rfloor$ corresponde al menor número entero más cercano a x (parte entera),la cota de Griesmer corresponde a:

$$\sum_{j=0}^{k-1} \left\lceil \frac{q^{k-1} - \sum_{i=1}^{h} q^{\lambda_i}}{q^j} \right\rceil = \sum_{j=0}^{k-1} \left(q^{k-j} - \left\lfloor \sum_{i=1}^{h} \frac{q^{\lambda_i}}{q^j} \right\rfloor \right)$$

Observemos que si tomamos un j fijo, sin perdida de generalidad podemos suponer que $\lambda_t \geqslant j > \lambda_{t-1}$. Ahora como a los más hay $q-1$ valores repetidos de λ_i y $\lambda_i - j \leqslant 0$ para todo $i < t$, tenemos que

$$\begin{aligned} \sum_{i=1}^{t-1} q^{\lambda_i - j} &\leqslant \sum_{i=1}^{r} (q-1)\frac{1}{q^i} \qquad \text{para algún } r \leqslant h \\ &\leqslant (q-1)\frac{q^{n+1} - q}{q^{n+2} - q^{n+1}} = 1 - \frac{1}{q^n} \\ &< 1 \end{aligned}$$

Además como $\lambda_i - j \geqslant 0$ para todo $i \geqslant t$ tenemos que $q^{\lambda_i - j} \in \mathbb{Z}$ para todo $i \geqslant t$, y así

$$\left\lfloor \sum_{i=1}^{h} \frac{q^{\lambda_i}}{q^j} \right\rfloor = \sum_{i=t}^{h} q^{\lambda_i - j} = \sum_{i=1}^{h} \left\lfloor \frac{q^{\lambda_i}}{q^j} \right\rfloor$$

Por lo cual

$$\begin{aligned}
\sum_{j=0}^{k-1} \left\lceil \frac{q^{k-1} - \sum_{i=1}^{h} q^{\lambda_i}}{q^j} \right\rceil &= \sum_{j=0}^{k-1} \left(q^{k-1-j} - \sum_{i=1}^{h} \left\lfloor \frac{q^{\lambda_i}}{q^j} \right\rfloor \right) \\
&= \sum_{j=0}^{k-1} q^{k-1-j} - \sum_{j=0}^{k-1} \sum_{i=1}^{h} \left\lfloor \frac{q^{\lambda_i}}{q^j} \right\rfloor \\
&= \sum_{j=0}^{k-1} q^{k-1-j} - \sum_{i=1}^{h} \sum_{j=0}^{k-1} \left\lfloor \frac{q^{\lambda_i}}{q^j} \right\rfloor \\
&= \theta_{k-1}(q) - \sum_{i=1}^{h} \theta_{\lambda_i}(q) = n.
\end{aligned}$$

Supongamos existe un $[\theta_{k-1}(q) - \sum_{i=1}^{h} \theta_{\lambda_i}(q), k, d]_q$-código proyectivo que alcanza la cota de Griesmer, entonces tenemos que:

$$\theta_{k-1}(q) - \textstyle\sum_{i=1}^{t+1} \theta_{\lambda_i}(q) = \displaystyle\sum_{j=0}^{k-1} \left\lceil \frac{d}{q^j} \right\rceil$$

luego como ya demostramos que $d = q^{k-1} - \sum_{i=1}^{h} q^{\lambda_i}$ cumple con esta condición, esta es la distancia mínima para este código, y así por corolario 3.1.9 tenemos que existe un (b,t)-minihyper tal que

$$\begin{aligned}
(b,t) &= \left(\textstyle\sum_{i=1}^{h} \theta_{\lambda_i}(q), \theta_{k-2}(q) - \theta_{k-1}(q) + \sum_{i=1}^{h} \theta_{\lambda_i}(q) + q^{k-1} - \sum_{i=1}^{h} q^{\lambda_i} \right) \\
(b,t) &= \left(\textstyle\sum_{i=1}^{h} \theta_{\lambda_i}(q), \sum_{i=1}^{h} \theta_{\lambda_i}(q) - q^{\lambda_i} \right) \\
(b,t) &= \left(\textstyle\sum_{i=1}^{h} \theta_{\lambda_i}(q), \sum_{i=1}^{h} \theta_{\lambda_{i-1}}(q) \right)
\end{aligned}$$

□

Observación 4.0.34. Si $1 \leqslant d < q^{k-1}$ este se puede escribir de manera única como $d = q^{k-1} - \sum_{i=1}^{h} q^{\lambda_i}$ tal que:

(a) $0 \leqslant \lambda_1 \leqslant \lambda_2 ... \leqslant \lambda_h < k-1$

(b) a lo más hay $q-1$ valores repetidos de λ_i.

(c) $1 \leqslant h \leqslant (k-1)(q-1)$

Corolario 4.0.35. *Si $1 \leqslant d < q^{k-1}$ existe una correspondencia uno a uno entre el conjunto de todos los $[n,k,d]_q$-códigos proyectivos, donde $d = q^{k-1} - \sum_{i=1}^{h} q^{\lambda_i}$, que alcanzan la cota de Griesmer y el conjunto de todos los $\left(\sum_{i=1}^{h} \theta_{\lambda_i}(q), \sum_{i=1}^{h} \theta_{\lambda_i - 1}(q)\right)$-minihyper en $\mathbb{F}_q\mathbb{P}^{k-1}$.*

Teorema 4.0.36. *(Hamada and Helleseth [8], Hamada and Maekawa [9]) Sea k, q, h, y λ_i con $i = \{1, 2...h\}$, números naturales tales que, $k \geqslant 1$, $h \geqslant 1$ y $q > (h-1)^2$ y $0 \leqslant \lambda_1 \leqslant \lambda_2 ... \leqslant \lambda_h < k-1$*

(i) Si $k-1 < \lambda_{h-1} + \lambda_h + 1$, entonces no existe un $\left(\sum_{i=1}^{h} \theta_{\lambda_i}, \sum_{i=1}^{h} \theta_{\lambda_i - 1}\right)$-minihyper en $\mathbb{F}_q\mathbb{P}^{k-1}$.

(ii) Si $k-1 \geqslant \lambda_{h-1} + \lambda_h + 1$, entonces F es un $\left(\sum_{i=1}^{h} \theta_{\lambda_i}, \sum_{i=1}^{h} \theta_{\lambda_i - 1}\right)$-minihyper en $\mathbb{F}_q\mathbb{P}^{k-1}$ si y sólo si F es la unión a pares disjunta de un subespacio isomorfo a $\mathbb{F}_q\mathbb{P}^{\lambda_1 - 1}$,un subespacio isomorfo a $\mathbb{F}_q\mathbb{P}^{\lambda_2 - 1}$,...,un subespacio isomorfo a $\mathbb{F}_q\mathbb{P}^{\lambda_h - 1}$.

Corolario 4.0.37. *Sea k, $q \neq 2$, h, y λ_i con $i = \{1, 2...h\}$, números naturales tales que, $k \geqslant 1$, $h \geqslant 1$, $q > (h-1)^2$ y $0 \leqslant \lambda_1 \leqslant \lambda_2 ... \leqslant \lambda_h < k-1$*

(i) Si $k-1 < \lambda_{h-1} + \lambda_h + 1$, entonces no existe un $\left[\theta_{k-1}(q) - \sum_{i=1}^{h} \theta_{\lambda_i}, k\right]_q$-código proyectivo que alcanze la cota de Griesmer.

(ii) Si $k-1 \geqslant \lambda_{h-1} + \lambda_h + 1$, entonces C es un $\left[\theta_{k-1}(q) - \sum_{i=1}^{h} \theta_{\lambda_i}, k\right]$-código proyectivo que alcanza la cota de Griesmer con matriz generadora $\Gamma = (\gamma_i^t)$ si y sólo si $\{[\gamma_1], ..., [\gamma_n]\}^C \subseteq \mathbb{F}_q\mathbb{P}^{k-1}$ es la unión a pares disjunta de un subespacio isomorfo a $\mathbb{F}_q\mathbb{P}^{\lambda_1}$,un subespacio isomorfo a $\mathbb{F}_q\mathbb{P}^{\lambda_2}$,...,un subespacio isomorfo a $\mathbb{F}_q\mathbb{P}^{\lambda_h}$.

Ejemplo 4.0.38. *1. Sea* $k = 4$, $q = 7$, $0 \leqslant 1 \leqslant 1 \leqslant 2 < 3$, *luego tomamos* $h = 3$, $\lambda_1 = \lambda_2 = 1$, $\lambda_3 = 2$, $7 > (3-1)^2 = 4$ *y como* $4 - 1 = 3 < 1 + 2 + 1 = 4$, *entonces como*

$$\theta_{4-1}(7) - \sum_{i=1}^{3} \theta_{\lambda_i}(7) = \frac{7^4 - 1}{7 - 1} - \left(2\left(\frac{7^2 - 1}{7 - 1}\right) + \frac{7^3 - 1}{7 - 1}\right) = 327$$

no existe un $[327, 4]_7$*-código proyectivo que alcanze la cota de Griesmer, es decir como ya conocemos esta cota*

$$d = 7^{4-1} - \sum_{i=1}^{3} 7^{\lambda_i} = 343 - (14 + 49) = 280$$

no existe un $[327, 4, 280]_7$*-código proyectivo .*

2. Sea $k = 4$, $q = 3$, $0 \leqslant 1 \leqslant 1 < 3$, *luego tomamos* $h = 2$, $\lambda_1 = 1$,$\lambda_2 = 1$, $3 > (2-1)^2 = 1$ *y como* $4 - 1 = 3 \geqslant 1 + 1 + 1 = 3$, *entonces como*

$$\theta_{4-1}(3) - \sum_{i=1}^{2} \theta_{\lambda_i}(3) = \frac{3^4 - 1}{3 - 1} - 2\left(\frac{3^2 - 1}{3 - 1}\right) = 40 - 8 = 32$$

existe un $[32, 4]_3$*-código proyectivo que alcanza la cota de Griesmer es decir:*

$$d = 3^{4-1} - \sum_{i=1}^{2} 3^{\lambda_i} = 21$$

existe un $[32, 4, 21]_3$*-código proyectivo .*
Luego el $(8, 2)$*-minihyper sobre* $\mathbb{F}_3\mathbb{P}^3$ *que corresponde al complemento del conjunto formado por las clases de las filas de una matriz generadora de este código es la unión a pares disjunta de un subespacio isomorfo a* $\mathbb{F}_3\mathbb{P}^1$ *,un subespacio isomorfo a* $\mathbb{F}_3\mathbb{P}^1$.

$B = \{[0,0,0,1], [0,0,1,0], [0,0,1,1], [0,0,1,2], [0,1,0,0], [1,0,0,0], [1,1,0,0], [1,2,0,0]\}$

Y una matriz generadora que representa a este código es

$$\begin{pmatrix}
0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&2&2&2&2&2&2&2&2\\
0&0&1&1&1&2&2&2&0&0&1&1&1&2&2&2&0&0&1&1&1&2&2&2&0&0&1&1&1&2&2&2\\
1&2&0&1&2&0&1&2&1&2&0&1&2&0&1&2&1&2&0&1&2&0&1&2&1&2&0&1&2&0&1&2
\end{pmatrix}$$

3. *Sea* $k = 7$, $q = 5$, $0 \leqslant 1 \leqslant 2 < 6$, *luego tomamos* $h = 2$, $\lambda_1 = 1, \lambda_2 = 2$, $5 > (2-1)^2 = 1$ *y como* $7 - 1 = 6 > 1 + 2 + 1 = 4$, *entonces como*

$$\theta_{7-1}(5) - \sum_{i=1}^{2} \theta_{\lambda_i} = \frac{5^7 - 1}{5 - 1} - \left(\frac{5^2 - 1}{5 - 1} + \frac{5^3 - 1}{5 - 1} \right) = 19494$$

existe un $[19494, 7]_5$*-código proyectivo que alcanza la cota de Griesmer, es decir*

$$d = 5^{7-1} - \sum_{i=1}^{2} 5^{\lambda_i} = 15595$$

existe un $[19494, 7, 15595]_5$*-código proyectivo .*
Es claro que la matriz generadora de este código es muy grande.por lo cual no la podemos mostrar, pero lo que si podemos mostrar es el $(37, 7)$*- minihyper sobre* $\mathbb{F}_5\mathbb{P}^6$ *que corresponde al complemento del conjunto formado por las filas de esta matriz generadora. Y que como dice el corolario anterior esta es la de un subespacio isomorfo a* $\mathbb{F}_5\mathbb{P}^1$ *,un subespacio isomorfo a* $\mathbb{F}_5\mathbb{P}^2$.

$B = \{[0,0,0,0,0,0,1],[0,0,0,0,0,1,0],[0,0,0,0,0,1,1],[0,0,0,0,0,1,1],[0,0,0,0,0,1,3],$
$[0,0,0,0,0,1,4],[0,0,1,0,0,0,0],[0,1,0,0,0,0,0],[0,1,1,0,0,0,0],[0,1,1,0,0,0,0],$
$[0,1,3,0,0,0,0],[0,1,4,0,0,0,0],[1,0,0,0,0,0,0],[1,0,1,0,0,0,0],[1,0,1,0,0,0,0],$
$[1,0,3,0,0,0,0],[1,0,4,0,0,0,0],[1,1,0,0,0,0,0],[1,1,1,0,0,0,0],[1,1,1,0,0,0,0],$
$[1,1,3,0,0,0,0],[1,1,4,0,0,0,0],[1,1,0,0,0,0,0],[1,1,1,0,0,0,0],[1,1,1,0,0,0,0],$
$[1,1,3,0,0,0,0],[1,1,4,0,0,0,0],[1,3,0,0,0,0,0],[1,3,1,0,0,0,0],[1,3,1,0,0,0,0],$
$[1,3,3,0,0,0,0],[1,3,4,0,0,0,0],[1,4,0,0,0,0,0],[1,4,1,0,0,0,0],[1,4,1,0,0,0,0],$
$[1,4,3,0,0,0,0],[1,4,4,0,0,0,0]\}$

Capítulo 5

Anexo

En este anexo, mostraremos como fueron generados a través del programa gap algunos ejemplos vistos en los distintitos cápitulos de la tesis.

Ejemplo 2.3.20(ii)

Primero construiremos el conjunto $\mathbb{F}_2P^2$

```
gap> K:=Elements(GF(2)^3);
gap> i:=1;j1:=1;f23:=[];for j1 in [1..Length(K)] do if
    Dimension(VectorSpace(GF(2),[K[j1]]))<>0 then
    f23[i]:=BasisVectors(Basis(VectorSpace(GF(2),[K[j1]])))[1];
    i:=i+1;j1:=j1+1;fi;od;f2p3:=Set(f23);
```

también construieremos el grupo de matrices $GL_3(2)$

```
gap> G:=Elements(GL(3,2));
```

y así construir el grupo de permutaciones $\overline{GL_3(2)}$

```
gap> i:=1;j1:=1;p:=[];for j1 in [1..Length(G)] do p[i]:= Permutation(G[j1],f2p3);
    j1:=j1+1;i:=i+1;od;P:=Set(p);
```

para luego encontar sus generadores

```
gap> AsGroup(P);
Group([ (4,5)(6,7), (4,6)(5,7), (2,3)(6,7), (2,4)(3,5), (1,2)(5,6) ])
```

sus clases de conjugación

```
gap> Pe:= Group((4,5)(6,7), (4,6)(5,7), (2,3)(6,7), (2,4)(3,5), (1,2)(5,6));
gap> c:=ConjugacyClasses(Pe);
```

y el largo de éstas.

```
gap> i:=1;j1:=1;l:=[];for j1 in [1..Length(Elements(c))] do
    l[i]:= Length(Elements(c[i]));j1:=j1+1;i:=i+1;od;
```

Ejemplo 2.2.10

Primero construiremos el espacio de matrices $\mathbb{F}_2^{2\times 3,2}$

```
gap> K:=Elements(GF(2)^3);
```

```
gap> f232:=[];i:=1;j1:=1;j2:=1; for j1 in [1..Length(K)] do for j2 in [1..Length(K)]
    do if Dimension(VectorSpace(GF(2),[K[j1],K[j2]]))=2 then f232[i]:=[K[j1],K[j2]];
    i:=i+1;fi;j2:=j2+1;od;j1:=j1+1;od;
```

también construieremos el grupo de matrices $GL_2(2)$

```
gap> gl22:= Elements(GL(2,2));
```

luego el conjunto $(\mathbb{F}_2^*)^3$

```
gap> f23:=[];i:=1;j1:=1;for j1 in [1..Length(K)] do if 0*Z(2) in K[j1] then j1:=j1+1;
    else f23[i]:=K[j1];i:=i+1;j1:=j1+1;fi;od;
```

y el grupo S_3

```
gap> s3:=Elements(Group((1,2),(1,2,3)));
```

y así formar el grupo $M_3(2)$

```
gap> M23:=[];m23:=[];m:=[];i:=1;w:=1;j1:=1;j2:=1;j3:=1;for j1 in [1..Length(f23)] do
    for j2 in [1..Length(s3)]do for i in [1..Length(f23[1])]dofor j3 in [1..Length(f23[1])]
    do if j3=i^s3[j2] then m[j3]:=f23[j1][j3]; else m[j3]:=0*Z(2);fi;j3:=j3+1;od;m23[i]:=m;
    m:=[];j3:=1;i:=i+1;od;M23[w]:=m23;w:=w+1;m23:=[];j2:=j2+1;od;j1:=j1+1;od;
```

Ahora teniendo estos conjuntos y grupos, podemos definir la acción de $GL_2(2)$ *en* $\mathbb{F}_2^{2\times 3,2}$*, para luego mostrar las órbitas formada por está.*

```
gap> orbitasgl22:=[];orbitagl22:=[];i:=1;w:=1;j1:=1;j2:=1;for j1 in [1..Length(f232)]do for
    j2 in [1..Length(gl22)] do orbitagl22[i]:=gl22[j2]*f232[j1];i:=i+1;j2:=j2+1;od;
    orbitasgl22[w]:=Set(orbitagl22);w:=w+1;i:=1;j1:=j1+1;od;Orbitasgl22:=Set(orbitasgl22);
```

Y luego definimos la acción que muestra las clases de isometría

```
gap> M23t:=List(M23, x->TransposedMat(x));
```

```
gap> orbitasiso:=[];orbitaiso:=[];i:=1;w:=1;j1:=1;j2:=1;j3:=1;for j1 in [1..Length(f232)]
     do for j2 in [1..Length(gl22)] do for j3 in [1..Length(M23)] do
     orbitaiso[i]:=gl22[j2]*f232[j1]*M23t[j3];i:=i+1;j3:=j3+1;od;j2:=j2+1;od;
     orbitasiso[w]:=Set(orbitaiso);w:=w+1;i:=1;j1:=j1+1;od;Orbitasiso:=Set(orbitasiso);
```

Ejemplo 2.3.10 (2)

Primero construiremos el conjunto $\mathbb{F}_3P^1$

```
gap> K:=Elements(GF(3)^2);
```

```
gap> i:=1;j1:=1;f32:=[];for j1 in [1..Length(K)] do if
    Dimension(VectorSpace(GF(3),[K[j1]]))<>0 then
    f31[i]:=BasisVectors(Basis(VectorSpace(GF(3),[K[j1]])))[1];i:=i+1;j1:=j1+1;fi;od;
    f3p1:=Set(f31);
```

luego el conjunto $(\mathbb{F}_3\mathbb{P}^1)^3$.

```
gap> i:=1;j1:=1;j2:=1;j3:=1;f3:=[];for j1 in [1..Length(f3p1)] do for
    j2 in [1..Length(f3p1)] do for j3 in [1..Length(f3p1)] do
    f3p13[i]:=[f3p1[j1],f3p1[j2],f3p1[j3]];i:=i+1;j3:=j3+1;od;j2:=j2+1;od;j1:=j1+1;od;
```

Ahora definiremos la función contenido

```
gap> contenido:=function(z) local f; f:= function(z,x) local v ; v:=function(z, x, y)
    if f3p1[x]=f3p13[z][y] then return 1;else return 0;fi;end;return
    Sum(List(f3p13[z],t-> v(z,x,Position(f3p13[z],t))));end; return
    List(f3p1,x-> f(z,Position(f3p1,x)));end;
```

y así encontramos los representantes de las órbitas de la acción del grupo S_3
en el conjunto $(\mathbb{F}_3\mathbb{P}^1)^3$

```
gap> j:=1;i:=1;valores:=[];representantes:=[];for j in [1..Length(f3)] do if contenido(j)
    in valores then j:=j+1; else  valores[i]:=contenido(j); representantes[i]:=f3[j];
    i:=i+1;fi;j:=j+1;od;
```

Ejemplo 3.1.18

Primero construiremos el conjunto $\mathbb{F}_3P^2$

```
gap> K:=Elements(GF(3)^3);
```

```
gap> i:=1;j1:=1;f32:=[];for j1 in [1..Length(K)] do if
    Dimension(VectorSpace(GF(3),[K[j1]]))<>0 then
    f32[i]:=BasisVectors(Basis(VectorSpace(GF(3),[K[j1]])))[1];i:=i+1;j1:=j1+1;fi;od;
    f3p2:=Set(f32);
```

luego los hiperplanos $H[v]$ *para todo* $v \in \mathbb{F}_3\mathbb{P}^2$

```
gap> H:=[];h:=[];i:=1;w:=1;j1:=1;j2:=1;for j1 in [1..Length(f3p2)] do for
    j2 in [1..Length(f3p2)] do  if f3p2[j1]*f3p2[j2]=0*Z(3) then h[i]:=f3p2[j2];i:=i+1;fi;
    j2:=j2+1;od;H[w]:=Set(h);w:=w+1;h:=[];i:=1;j1:=j1+1;od;
```

y así podemos construir la matriz de adyacencia del grafo $(\mathbb{F}_3\mathbb{P}^2, E(G))$

```
gap> Ag:=[];ag:=[];i:=1;w:=1;j1:=1;j2:=1;for j1 in [1..Length(f3p2)] do for
    j2 in [1..Length(f3p2)] do  if f3p2[j1] in H[j2] then ag[i]:=1; else ag[i]:=0;
    fi;i:=i+1;j2:=j2+1;od;Ag[w]:=ag;w:=w+1;ag:=[];i:=1;j1:=j1+1;od;
```

Ahora nos damos un vector que represente un t-bloque

```
gap> x:=[1,1,1,1,0,0,0,0,0,0,0,0];
```

para luego multiplicarlo por la matriz de adyacencia del grafo y saber quien es t.

```
gap> Ag*x;
```

Y por último escribir la matriz generadora del código encontrado

```
gap> Gamma:=TransposedMat([f3p2[5],f3p2[6],f3p2[7],f3p2[8],f3p2[9],f3p2[10],
    f3p2[11],f3p2[12],f3p2[13]]);
```

Ejemplo 3.1.18

Primero construiremos el conjunto $\mathbb{F}_3P^2$

```
gap> K:=Elements(GF(3)^3);
```

```
gap> i:=1;j1:=1;f32:=[];for j1 in [1..Length(K)] do if
    Dimension(VectorSpace(GF(3),[K[j1]]))<>0 then
    f32[i]:=BasisVectors(Basis(VectorSpace(GF(3),[K[j1]])))[1];i:=i+1;j1:=j1+1;fi;od;
    f3p2:=Set(f32);
```

luego los hiperplanos $H[v]$ *para todo* $v \in \mathbb{F}_3\mathbb{P}^2$.

```
gap> H:=[];h:=[];i:=1;w:=1;j1:=1;j2:=1;for j1 in [1..Length(f3p2)] do for
    j2 in [1..Length(f3p2)] do  if f3p2[j1]*f3p2[j2]=0*Z(3) then h[i]:=f3p2[j2];i:=i+1;fi;
    j2:=j2+1;od;H[w]:=Set(h);w:=w+1;h:=[];i:=1;j1:=j1+1;od;
```

Ahora escribimos el grupo de automorfismos que queremos que posea nuestro t-bloque

```
gap> G:=Elements(Group([[0*Z(3), Z(3)^0,0*Z(3)],[Z(3)^0,0*Z(3),0*Z(3)],
    [0*Z(3),0*Z(3),Z(3)^0]],[[0*Z(3), 0*Z(3),Z(3)^0],[0*Z(3),Z(3)^0,0*Z(3)],
    [Z(3)^0,0*Z(3),0*Z(3)]],[[0*Z(3), 0*Z(3),Z(3)^0],[Z(3)^0,0*Z(3),0*Z(3)],
    [0*Z(3),Z(3)^0,0*Z(3)]]));
```

y definimos la acción de este grupo en los puntos de $\mathbb{F}_3\mathbb{P}^2$

```
gap> GT:=List(G, x->TransposedMat(x));
```

```
gap> i:=1;j1:=1;j2:=1;w:=1;orbitapunto:=[];Orbitaspuntos:=[];for j1 in [1..Length(f3p2)]
    do for j2 in [1..Length(GT)]do
    orbitapunto[i]:=BasisVectors(Basis(VectorSpace(GF(3),[fpk[j1]*GT[j2]])))[1];i:=i+1;
    j2:=j2+1;od;Orbitaspuntos[w]:=Set(orbitapunto);orbitapunto:=[];i:=1;w:=w+1;j1:=j1+1;
    od;orbitaspuntos:=Set(Orbitaspuntos);
```

y definimos la acción de este grupo en los hiperplanos $H[v]$ para todo $v \in \mathbb{F}_3\mathbb{P}^2$

```
gap> GI:=List(G, x->Inverse(x));
```

```
gap> i:=1;j1:=1;j2:=1;w:=1;orbitaplano:=[];Orbitasplanos:=[];for j1 in [1..Length(fpk)]
    do for j2 in [1..Length(GI)]do
    orbitaplano[i]:=BasisVectors(Basis(VectorSpace(GF(3),[fpk[j1]*GI[j2]])))[1];i:=i+1;
    j2:=j2+1;od;Orbitasplanos[w]:=Set(orbitaplano);orbitaplano:=[];i:=1;w:=w+1;j1:=j1+1;
    od;orbitasplanos:=Set(Orbitasplanos);
```

y así podemos construir la matriz de adyacencia del grafo $(\mathbb{F}_3\mathbb{P}^2, E(G))$.

```
gap> AgK:=[];agK:=[];i:=1;w:=1;j1:=1;j2:=1;for j1 in [1..Length(orbitaspuntos)] do for
    j2 in [1..Length(orbitasplanos)] do
    agK[i]:=Length(Intersection(orbitaspuntos[j1],H[Position(fpk,orbitasplanos[j2][1])]));
    i:=i+1;j2:=j2+1;od;AgK[w]:=agK;w:=w+1;agK:=[];i:=1;j1:=j1+1;od;
```

Ahora nos damos un vector que represente un t-bloque

```
gap> x:=[0,0,1,1,0];
```

para luego multiplicarlo por la matriz de adyacencia del grafo y saber quien es t.

```
gap> Ag*x;
```

Y por último escribir la matriz generadora del código encontrado

```
gap> B:=Union(orbitaspuntos[3],orbitaspuntos[4]);
```

```
gap> GammaT:=Difference(fpk,B);
```

```
gap> Gamma:=TransposedMat(GammaT);
```

Bibliografía

[1] R. Podesta, *Introducción a la teoría de códigos autocorrectores*, *www.emis.famaf.unc.edu.ar/series/pdf/pdfCMat/CMat35 – 3.pdf.*

[2] A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert, A. Wassermann, *Error-Correcting Linear Codes, Classification by Isometry and Applications*, Springer-Verlag; Berlin Heidelberg, 2006.

[3] *http : //linearcodes.uni – bayreuth.de/CD/index.html.*

[4] Cary Huffman, W., Vera Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press; New York 2003.

[5] T. Maruta, *The nonexistence of [116; 5; 85]4 codes and [187; 5; 139]4 codes, in: Proceedings of the Second International Workshop on Optimal Codes and Related Topics*, Sozopol, 1998, pp. 168 - 174.

[6] S. Innamorati, A. Maturo, *On irreducible blocking set in proyective planes*, Ratio Maht.(2), 1991, pp. 151 - 155.

[7] N. Hamada. *A characterization of some* $[n, k, d; q]$*-codes meeting the Griesmer bound using a minihyper in a finite projective geometry.* Discrete Math.116(1-3), 1993, pp. 229-268,

[8] N. Hamada,T. Helleseth. *A characterization of some q-ary codes* $(q > (h-1)^2, h \geqslant 3)$ *meeting the Griesmer bound*, Math. Japonica 38 , 1993, pp. 925 - 940.

[9] N. Hamada,T. Maekawa. *A characterization of some q-ary codes* $(q > (h-1)^2, h \geqslant 3)$ *meeting the Griesmer bound: Part 2*, Math. Japonica 46 , 1997, pp. 241 - 252.

[10] J.W.P Hirschfeld, L.Storme. *The packing problem in statistics.*