Universidad del Norte

División de Ciencias Básicas
Departamento de Matemáticas

Códigos de red correctores de errores en el espacio proyectivo

Nelson Fabián Martínez Herrera

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

Director: Prof. Dr. Ismael Gutiérrez García

Barranquilla, Septiembre de 2014

Agradecimientos

A Dios, por darme la oportunidad de cumplir uno de mis deseos personales y dar un gran paso en mi formación profesional.

A mi profesor, Dr. Ismael Gutierrez García por aceptar ser la base de este trabajo, que con su experiencia y sencillez dirigió paso a paso.

Al profesor Darwin Villar por su gran aporte en el uso del software MAGMA para obtener datos importantes en el desarrollo de este trabajo.

Introducción

Este trabajo consta de tres capítulos y está basado principalmente en lo desarrollado por T. Etzion y A. Vardy [5]. En el capítulo 1, con los preliminares necesarios, se presentan definiciones, teoremas, propiedades, lemas y ejemplos relacionados con el q-ésimo coeficiente de Gauss, los grafos de Johnson y Grassmann, la partición de un espacio vectorial y los esquemas de asociación. Esto con el fin de justificar su uso en el desarrollo de los siguientes capítulos. Cabe anotar que para la obtención del ejemplo del grafo de Grassmman, se hizo necesario el uso del software MAGMA Computational Algebra System.

En el capítulo 2 se presentan los códigos en el espacio proyectivo, $\mathbb{P}_q(n)$. Los llamados (n, M, d) y $(n, M, d, k)-$códigos en el espacio proyectivo son similares, respectivamente, a los ampliamente conocidos, códigos en el espacio de Hamming, y códigos de dimensión constante en el espacio de Johnson, donde la distancia de Hamming sirve como la métrica.

Recientemente, R. Koetter y F. R. Kschischang [9], [10] demostraron que los códigos en el espacio proyectivo son precisamente los que se necesitan para la corrección de errores en la red. Además trata de unos anticódigos y conjuntos con t-intersección. Finalmente, se presentan cotas superiores para el tamaño de un código en el espacio proyectivo.

R. Koetter y F. R. Kschischang probaron en [10] las cotas equivalentes a las del empaquetamiento esférico, la de Singleton y la de Gilbert-Varshamov de la teoría clásica de códigos. Se establecen además algunas cotas superiores para el tamaño de los códigos en la k-Grassmanniana, $G_q(n, k)$. Este tipo de códigos se estudiaron esporádicamente entre los últimos veinte años.

En el capítulo 3, se presentan algunas construcciones de códigos en $\mathbb{P}_q(n)$ y $G_q(n, k)$. Estos códigos están basados en las estructuras de Steiner y programas computacionales para la consecución de códigos cíclicos en $\mathbb{P}_q(n)$. En este capítulo se presentan nuevos ejemplos de códigos cíclicos, los cuales fueron construidos con el apoyo del software libre GAP - Groups, Algorithms, Programming - a System for Computational Discrete Algebra.

Índice general

Capítulo 1

Preliminares

1.1 El q-ésimo coeficiente de Gauss

Denotemos con $\mathbb{F}_q^n$ el espacio vectorial n-dimensional sobre en cuerpo finito $\mathbb{F}_q$, con q elementos. Existen muchas analogías entre el conjunto parcialmente ordenado por inclusión de todos los subconjuntos de un conjunto finito y el conjunto parcialmente ordenado de todos los subespacios vectoriales de $\mathbb{F}_q^n$, [15].

Abordamos el siguiente problema: obtener una expresión para el número de cadenas máximas (cadenas de longitud $n+1$ que contienen un subespacio vectorial de $\mathbb{F}_q^n$ para cada posible dimensión) en el conjunto parcialmente ordenado de todos los subespacios de $\mathbb{F}_q^n$, iniciando con el espacio vectorial nulo. Es decir, el subespacio de dimensión cero. Una vez elegido un subespacio vectorial i-dimensional, U_i, con $0 \leq i < n$, podemos elegir un subespacio vectorial $(i+1)$-dimensional, U_{i+1} que contenga a U_i de

$$\frac{q^n - q^i}{q^{i+1} - q^i}$$

formas, ya que podemos tomar el espacio generado por U_i y cualquiera de los $q^n - q^i$ vectores que no están en U_i, pero cualquier subespacio de dimensión $(i+1)$ aparece exactamente $q^{i+1} - q^i$ veces de esta manera. En resumen, el número de cadenas máximas de subespacios en $\mathbb{F}_q^n$ es:

$$M(n,q) = \frac{(q^n-1)(q^{n-1}-1)(q^{n-2}-1)\cdots(q^2-1)(q-1)}{(q-1)^n}.$$

Por otro lado, si q es reemplazado por 1, tenemos que $M(n,1) = n!$, el cual corresponde al número de cadenas máxima en el conjunto parcialmente ordenado de subconjuntos de un conjunto con n elementos.

1.1.1 Definición. Sean $n, k \in \mathbb{N}$ con $k \leq n$. El q-ésimo coeficiente de Gauss, notado con $\begin{bmatrix} n \\ k \end{bmatrix}_q$, se define como el número de subespacios de dimensión k en el espacio vectorial $\mathbb{F}_q^n$.

En adelante sólo escribiremos $\begin{bmatrix} n \\ k \end{bmatrix}$ para referirnos a este número.

Para encontrar una expresión para $\begin{bmatrix} n \\ k \end{bmatrix}$, contamos el número N de parejas (U, C), donde U es un subespacio vectorial de dimensión k y C es una cadena máxima que contiene U. Por supuesto, cada cadena máxima contiene exactamente un subespacio de dimensión k, en consecuencia $N = M(n,q)$.

Por otro lado, podemos obtener cada una de tales cadenas máximas únicamente añadiendo a una cadena máxima en el conjunto parcialmente ordenado de todos los subespacios de U, de las cuales hay $M(k,q)$, una cadena máxima en el conjunto parcialmente ordenado de los subespacios de $\mathbb{F}_q^n$ que contienen U, de las cuales hay $M(n-k,q)$, ya que el conjunto parcialmente ordenado

$$\{W \mid U \subseteq W \subseteq V\}$$

es isomorfo al conjunto parcialmente ordenado de subespacios del espacio cociente V/U que tienen dimensión $(n-k)$. Por lo tanto,

$$\begin{aligned} \begin{bmatrix} n \\ k \end{bmatrix} &= \frac{M(n,q)}{M(k,q)M(n-k,q)} \\ &= \frac{(q^n-1)(q^{n-1}-1)(q^{n-2}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)(q^{k-2}-1)\cdots(q-1)}. \end{aligned}$$

A continuación mostramos otra alternativa para la deducción de este número. ¿Cuántos subespacios de $\mathbb{F}_q^n$ de dimensión k existen?. Sea $U = \langle u_1, u_2, \ldots, u_k \rangle$ un subespacio k-dimensional de $\mathbb{F}_q^n$.

¿Cuántas posibilidades hay para escoger w_1?. Dado que $u_1 \neq 0$, existen $q^n - 1$ posibilidades.

¿Cuántas posibilidades hay para escoger w_2?. Dado que w_2 debe ser linealmente independiente con w_1, este no puede ser un múltiplo escalar de w_1 y puesto que hay $q-1$ múltiplos de w_1, las posibilidades para w_2 se reducen a $q^n - q$.

Razonando de esta manera, tenemos que para elegir w_k existen $q^n - q^{k-1}$ posibilidades. Entonces el número de subconjuntos de $\mathbb{F}_q^n$ linealmente inde-

pendientes que tienen k elementos es

$$(q^n-1)(q^n-q)\cdots(q^n-q^{k-1}).$$

Por otro lado, recuerde que dos conjuntos linealmente independientes distintos, pueden generar el mismo subespacio. En consecuencia podemos preguntarnos ahora, ¿Cuántas bases tiene U?.

Dado que $|U|=q^k$, usando el mismo razonamiento para el conteo de subconjuntos de $\mathbb{F}_q^n$ linealmente independientes con k elementos, tenemos que para $u_1\in U$ hay q^k-1 posibilidades, para $u_2\in U$ hay q^k-q posibilidades y para $w_k\in U$ hay q^k-q^{k-1} posibilidades, así el número de bases para U es

$$(q^k-1)(q^k-q)\cdots(q^k-q^{k-1}).$$

Entonces, el número de subespacios de $\mathbb{F}_q^n$ con dimensión k es el cociente de el número de subconjuntos de $\mathbb{F}_q^n$ que son linealmente independientes con tamaño k entre el número de bases de un espacio vectorial de dimensión k. Es decir,

$$\begin{aligned}\frac{(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})} &= \frac{(q^n-1)q(q^{n-1}-1)\cdots q^{k-1}(q^{n-k+1}-1)}{(q^k-1)q(q^{k-1}-1)\cdots q^{k-1}(q-1)}\\ &= \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}\\ &= \begin{bmatrix} n \\ k \end{bmatrix}.\end{aligned}$$

1.1.2 Ejemplos. (a) $\begin{bmatrix} 1 \\ 1 \end{bmatrix}=1$.

(b) $\begin{bmatrix} 2 \\ 1 \end{bmatrix}=q+1$.

(c) $\begin{bmatrix} 3 \\ 1 \end{bmatrix}=q^2+q+1$.

(d) $\begin{bmatrix} 4 \\ 2 \end{bmatrix}=q^4+q^3+2q^2+q+1$.

(e) $\begin{bmatrix} 4 \\ 3 \end{bmatrix}=q^3+q^2+q+1$.

1.1.3 Observación. Notemos con $[n]$ el número

$$\frac{q^n-1}{q-1}=1+q+q^2+\cdots+q^{n-1},$$

y con $[n]!$ el tradicional factorial. Esto es,

$$[n]!=[n][n-1]\cdots[2][1].$$

Las siguientes son algunas de propiedades del q-ésimo coeficiente de Gauss.

1.1.4 Teorema. Sean $n, k \in \mathbb{N}$ con $k \leq n$. Entonces

(a) $\begin{bmatrix} n \\ k \end{bmatrix} = \dfrac{[n]!}{[k]![n-k]!}$.

(b) $\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n \\ n-k \end{bmatrix}$. En particular $\begin{bmatrix} n \\ 0 \end{bmatrix} = \begin{bmatrix} n \\ n \end{bmatrix} = 1$.

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

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

(e) $\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n-1 \\ k \end{bmatrix} + q^{n-1} \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}$.

Demostración.

(a)

$$\begin{aligned}
\begin{bmatrix} n \\ k \end{bmatrix} &= \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1\cdots(q-1)} \\
&= \frac{\left(\dfrac{q^n-1}{q-1}\right)\left(\dfrac{q^{n-1}-1}{q-1}\right)\cdots\left(\dfrac{q^{n-k+1}-1}{q-1}\right)}{\left(\dfrac{q^k-1}{q-1}\right)\left(\dfrac{q^{k-1}-1}{q-1}\right)\cdots\left(\dfrac{q-1}{q-1}\right)} \\
&= \frac{[n][n-1]\cdots[n-k+1]}{[k][k-1]\cdots[1]} \\
&= \frac{[n]!}{[k]![n-k]!}.
\end{aligned}$$

(b)

$$\begin{bmatrix} n \\ k \end{bmatrix} = \frac{[n]!}{[k]![n-k]!} = \frac{[n]!}{[n-k]![n-(n-k)]!} = \begin{bmatrix} n \\ n-k \end{bmatrix}.$$

(c) La primera igualdad se sigue de (b). Para la segunda tenemos

$$\begin{bmatrix} n \\ n-1 \end{bmatrix} = \frac{[n]!}{[n-1]!} = \frac{[n][n-1]!}{[n-1]!} = [n] = 1 + q + \cdots + q^{n-1}.$$

(d)

$$\begin{aligned}
\begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + q^k \begin{bmatrix} n-1 \\ k \end{bmatrix} &= \frac{[n-1][n-2]\cdots[1]}{[k-1][k-2]\cdots[1][n-k]!} \\
&\quad + q^k \frac{[n-1][n-2]\cdots[1]}{[k]![n-k-1][n-k-2]\cdots[1]} \\
&= \frac{[n][k]}{[n][k]} \frac{[n-1][n-2]\cdots[1]}{[k-1][k-2]\cdots[1][n-k]!} \\
&\quad + q^k \frac{[n][n-k]}{[k]![n][n-k]} \frac{[n-1][n-2]\cdots[1]}{[n-k-1][n-k-2]\cdots[1]} \\
&= \frac{[n]![k]}{[n][k]![n-k]!} + q^k \frac{[n]![n-k]}{[k]![n][n-k]!} \\
&= \frac{[n]!}{[k]![n-k]!} \underbrace{\left(\frac{[k]}{[n]} + \frac{q^k[n-k]}{[n]} \right)}_{1} \\
&= \begin{bmatrix} n \\ k \end{bmatrix}.
\end{aligned}$$

(e) Se demuestra similar como (d). □

1.1.5 Lema. Sean $0 \leq i, j \leq n$ y $V = \mathbb{F}_q^n$. Entonces

(a) Si X es un subespacio vectorial de V de dimensión j, entonces existen exactamente $q^{ij} \begin{bmatrix} n-j \\ i \end{bmatrix}$ subespacios vectoriales Y de V de dimension i tales que $X \cap Y = \{0\}$.

(b) Si X es un subespacio vectorial de V de dimensión j, entonces existen exactamente $q^{(i-m)(j-m)} \begin{bmatrix} n-j \\ i-m \end{bmatrix} \begin{bmatrix} j \\ m \end{bmatrix}$ subespacios vectoriales Y de V de dimension i tales que $X \cap Y$ tiene dimensión m.

Demostración.

(a) Dada un i-tupla de vectores linealmente independientes en V/X existen q^{ij} formas de levantar esta i-tupla a una i-tupla de vectores linealmente independientes en V.

(b) De la definición del q-ésimo coeficiente de Gauss se sigue que existen $\begin{bmatrix} j \\ m \end{bmatrix}$ subespacios Z de X de dimensión m y por (a), para cada uno de estos podemos encontrar $q^{(i-m)(j-m)} \begin{bmatrix} n-j \\ i-m \end{bmatrix} \begin{bmatrix} j \\ m \end{bmatrix}$ subespacios vectoriales Y de V de dimension i tales que $X \cap Y = Z$. Es decir, subespacios Y/Z en V/Z de dimensión $(i-m)$ tales que $(X/Z) \cap (Y/Z) = \{0\}$. □

1.2 Dos grafos importantes

Iniciamos esta sección presentando el vocabulario básico de la teoría de grafos, a fin de justificar algunas afirmaciones sobre el grafo de Grassmann.

1.2.1 Definición. Un grafo G es una pareja $G = (V, E)$, donde V es un conjunto finito, cuyos elementos se denominan vértices o nodos y E es un conjunto de parejas no ordenados de vértices, notados con $\{u, v\}$, que se denominan lados o aristas. En este caso decimos que u y v son adyacentes.

1.2.2 Definición. Sea $G = (V, E)$ un grafo.

(a) Si $u, v \in V$, entonces un `camino` de u hasta v es una $n+1$-tupla $(v_0, v_1, \ldots, v_n)$ con $v_0 = u$, $v_n = v$, cada $v_j \in V$ y cada v_j es adyacente con v_{j+1}. Este número n, que representa la cantidad de aristas en el camino, se denomina la `longitud` del camino.

(b) El número de aristas que concurren en un vértice se llama el `grado` de dicho vértice.

(c) Si para todo $u, v \in V$ existe un camino desde u hasta v, entonces el grafo se denomina `conexo`.

(d) La `distancia` $d(u, v)$ entre dos vértices distintos u y v se define como la longitud del camino más corto entre u y v, si tal camino existe. El `diámetro` de un grafo es el máximo de las distancias entre cualquier par de vértices.

(e) Un grafo `simple` G, es decir, sin lados múltiples ni lazos, se denomina `completo`, si todo par de vértices de G son adyacentes.

1.2.3 Definición. Dos grafos $G_1 = (V_1, E_1)$ y $G_2 = (V_2, E_2)$ se llaman `isomorfos`, si existe una biyeccón f de V_1 hasta V_2 tal que, para todo par de vértices $u, v \in V_1$ se verifica que $\{u, v\} \in E_1$ si y solo si $\{f(u), f(v)\} \in E_2$. En este caso, como es usual, escribimos $G_1 \cong G_2$. En otras palabras, G_1 y G_2 son isomorfos, si existe una correspondencia de un vértice a otro y se conserva la adyacencia.

Sea $G = (V, E)$ un grafo conexo. Para cada $v \in V$ definimos

$$G_j(v) := \{u \in V \mid d(u, v) = j\},$$

donde $0 \leq j \leq D$ y D es el diámetro de G. Es claro que $G_0(v) = \{v\}$ y que el conjunto de vértices queda particionado en conjuntos disyuntos $G_0(v)$, $G_1(v), \ldots, G_D(v)$, para cada $v \in V$.

1.2.4 Ejemplo. Grafos isomorfos y grafos conexos.

(a) Un isomorfismo podría estar descrito de la siguiente manera: $\{(a,1),(b,2),(c,8),(d,3),(e,7),(f,4),(g,6),(h,5)\}$.

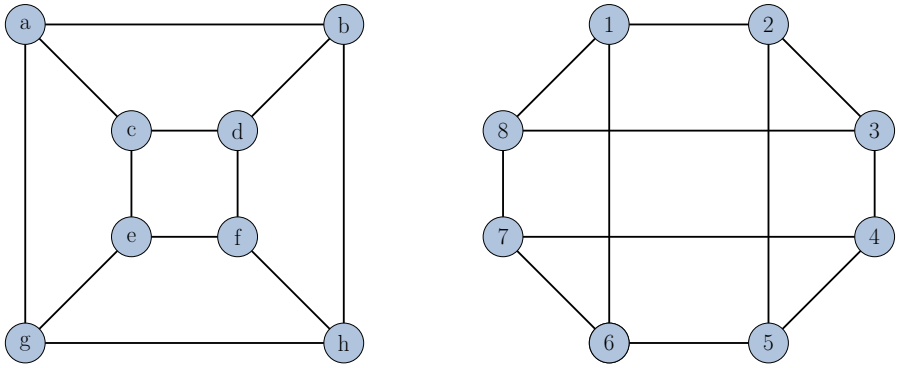

Figura 1.1: Grafos isomorfos

(b) Si $G_1 \cong G_2$, entonces $|V(G_1)| = |V(G_2)|$ y $|E(G_1)| = |E(G_2)|$. El recíproco, no es cierto. En este caso mostramos además un grafo no conexo y uno conexo.

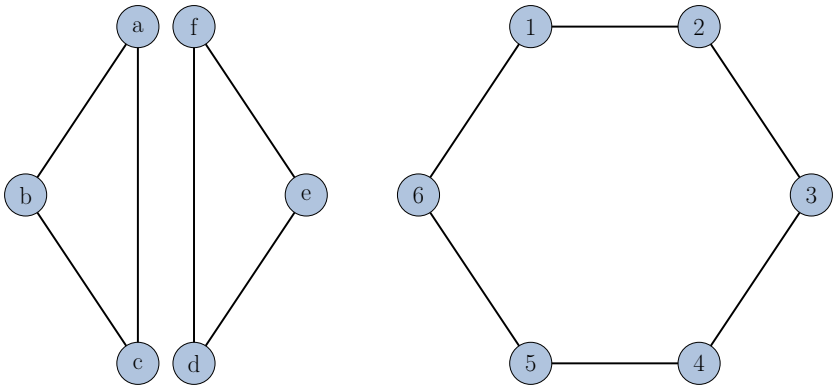

Figura 1.2: Grafo No conexo y Grafo conexo

(c) Si dos grafos son isomorfos, entonces tienen la misma sucesión de grados. El recíproco es falso. Note que ambos tienen 6 vértices, 5 aristas, y su

sucesión de grados es $(1, 1, 1, 2, 2, 3)$, sin embargo no son isimorfos ya que el vértice a es vecino de dos de vértices de grado 1 y uno de grado 2, mientras que el vértice 3 es vecino de uno de grado 1 y dos de grado 2.

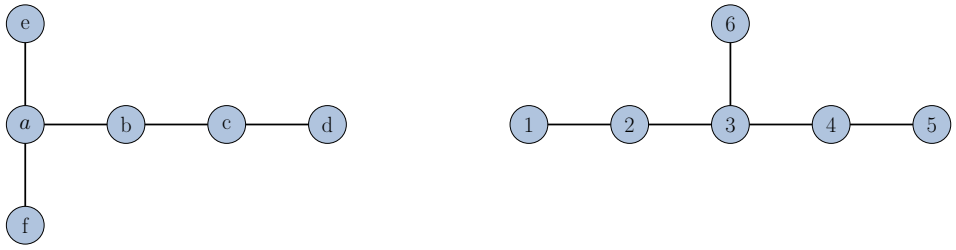

Figura 1.3: Grafos No isomorfos

1.2.5 Definición. Un grafo conexo $G = (V, E)$ con diámetro D es `distancia-regular` si, satisface la siguiente propiedad:

Existen números naturales $b_0 = k, b_1, \ldots, b_{D-1}$, $c_1 = 1, c_2, \ldots, c_d$ tales que para cada par de vértices $u, v \in V$ con $d(u, v) = j$ se tiene que

(1) El número de vértices en $G_{j-1}(v)$ adyacentes a u es c_j, con $1 \leq j \leq D$.

(2) El número de vértices en $G_{j+1}(v)$ adyacentes a u es b_j, con $0 \leq j \leq D-1$.

La definición más usual en la literatura de grafos distancia-regular se presenta de la siguiente manera:

1.2.6 Definición. Un grafo conexo $G = (V, E)$ es `distancia-regular` si, para cualquier par de vértices $u, v \in V$ con $d(u, v) = j$, los números a_j, b_j y c_j de vértices que son adyacentes a v, y están a distancia $j - 1$, j, y $j + 1$, respectivamente, de u solo dependen de j.

1.2.1 El grafo de Johnson

1.2.7 Definición. Sea X un conjunto con n elementos. El grafo de Johnson $J(n, k)$ con $k \leq n$ es el conjunto con $\binom{n}{k}$ vértices, con dos vértices adyacentes cuando tienen $k - 1$ elementos en común. Por ejemplo el grafo $J(n, 0)$ tiene un solo vértice.

1.2.8 Ejemplos. (a) El grafo $J(3,2)$. Sea $X = \{1,2,3\}$. Dado que $\binom{3}{2} = 3$, el conjunto de vértices viene dado por: $\{\{1,2\},\{1,3\},\{2,3\}\}$. Luego

$$\{1,2\} \cap \{1,3\} = \{1\}$$
$$\{1,2\} \cap \{2,3\} = \{2\}$$
$$\{1,3\} \cap \{2,3\} = \{3\}$$

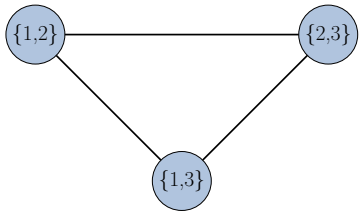

Figura 1.4: Grafo de Johnson $J(3,2)$

(b) El grafo $J(4,2)$. Sea $X = \{1,2,3,4\}$. Dado que $\binom{4}{2} = 6$ el conjunto de vértices viene dado por: $\{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\}$. Luego

$$\{1,2\} \cap \{1,3\} = \{1\}$$
$$\{1,2\} \cap \{1,4\} = \{1\}$$
$$\{1,2\} \cap \{2,3\} = \{2\}$$
$$\{1,2\} \cap \{2,4\} = \{2\}$$
$$\{1,2\} \cap \{3,4\} = \emptyset$$
$$\{1,3\} \cap \{1,4\} = \{1\}$$
$$\{1,3\} \cap \{2,3\} = \{3\}$$
$$\{1,3\} \cap \{2,4\} = \emptyset$$
$$\{1,3\} \cap \{3,4\} = \{3\}$$
$$\{1,4\} \cap \{2,3\} = \emptyset$$
$$\{1,4\} \cap \{2,4\} = \{4\}$$
$$\{1,4\} \cap \{3,4\} = \{4\}$$
$$\{2,3\} \cap \{2,4\} = \{2\}$$
$$\{2,3\} \cap \{3,4\} = \{3\}$$
$$\{2,4\} \cap \{3,4\} = \{4\}.$$

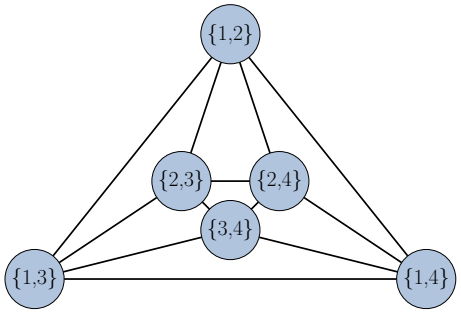

Figura 1.5: Grafo de Johnson $J(4,2)$

1.2.2 El grafo de Grassmann

1.2.9 Definición. (k-Grassmanniana) Consideremos el espacio vectorial n-dimensional W sobre $\mathbb{F}_q$. Dados dos números naturales n y k con $k \leq n$, el conjunto de todos los subespacios de W que tienen dimensión k es denominado una k-Grassmanniana. Esta es usualmente notada con $G_q(n,k)$.

1.2.10 Definición. (Grafo de Grassmann) Sean $n, k \in \mathbb{N}$. El grafo de Grassmann es el grafo con conjunto de vértices $G_q(n,k)$ y conjunto de aristas determinado de la siguiente manera: Dos vértices X, Y son adyacentes si y solo si

$$\dim_{\mathbb{F}_q}(X \cap Y) = k - 1.$$

Note que si $k = 1$, entonces se tiene que el grafo de Grassmann es un grafo completo. Por lo tanto podemos asumir que $k \geq 2$.

Por otro lado, del teorema 1.1.4 (b) se sigue que $G_q(n,k)$ y $G_q(n,n-k)$ tienen el mismo número de elementos.

Si $(\cdot \mid \cdot)$ define un producto punto sobre $\mathbb{F}_q^n$, entonces el complemento ortogonal de $U \leq \mathbb{F}_q^n$ esta definido por

$$U^{\perp} := \{v \in \mathbb{F}_q^n \mid (u \mid v) = 0, \quad \forall u \in U\}.$$

Si $U \leq \mathbb{F}_q^n$, entonces se verifica que

$$\dim_{\mathbb{F}_q} U^{\perp} = n - \dim_{\mathbb{F}_q} U.$$

Si $U, V \leq \mathbb{F}_q^n$, entonces se puede demostrar que

$$\dim_{\mathbb{F}_q} U^\perp - \dim_{\mathbb{F}_q}(U^\perp \cap V^\perp) = \dim_{\mathbb{F}_q} V - \dim_{\mathbb{F}_q}(U \cap V).$$

En consecuencia basta definir f de $G_q(n,k)$ en $G_q(n,n-k)$ que a cada k-subespacio U asigne su complemento ortogonal $U^\perp$, para demostrar que $G_q(n,k) \cong G_q(n,n-k)$. Por lo tanto es suficiente considerar el caso cuando $n \geq 2k$.

1.2.11 Ejemplo. Usando el q-esimo coeficiente de Gauss se tiene que existen 15 subespacios vectoriales de dimensión 3 en $\mathbb{F}_2^4$, los cuales listamos a continuación:

$$\begin{aligned}
W01 &:= \langle (0,1,0,0),(0,0,1,0),(0,0,0,1)\rangle \\
W02 &:= \langle (1,0,0,0),(0,0,1,0),(0,0,0,1)\rangle \\
W03 &:= \langle (1,1,0,0),(0,0,1,0),(0,0,0,1)\rangle \\
W04 &:= \langle (1,0,0,0),(0,1,0,0),(0,0,0,1)\rangle \\
W05 &:= \langle (1,0,1,0),(0,1,0,0),(0,0,0,1)\rangle \\
W06 &:= \langle (1,0,0,0),(0,1,1,0),(0,0,0,1)\rangle \\
W07 &:= \langle (1,0,1,0),(0,1,1,0),(0,0,0,1)\rangle \\
W08 &:= \langle (1,0,0,0),(0,1,0,0),(0,0,1,0)\rangle \\
W09 &:= \langle (1,0,0,1),(0,1,0,0),(0,0,1,0)\rangle \\
W10 &:= \langle (1,0,0,0),(0,1,0,1),(0,0,1,0)\rangle \\
W11 &:= \langle (1,0,0,1),(0,1,0,1),(0,0,1,0)\rangle \\
W12 &:= \langle (1,0,0,0),(0,1,0,0),(0,0,1,1)\rangle \\
W13 &:= \langle (1,0,0,1),(0,1,0,0),(0,0,1,1)\rangle \\
W14 &:= \langle (1,0,0,0),(0,1,0,1),(0,0,1,1)\rangle \\
W15 &:= \langle (1,0,0,1),(0,1,0,1),(0,0,1,1)\rangle
\end{aligned}$$

Usando MAGMA se tiene que

$$
\begin{aligned}
W_1 \cap W_2 &= \langle (0,0,1,0), (0,0,0,1) \rangle \\
W_1 \cap W_3 &= \langle (0,1,0,0), (0,0,0,1) \rangle \\
W_1 \cap W_4 &= \langle (0,1,0,0), (0,0,0,1) \rangle \\
W_1 \cap W_5 &= \langle (0,1,1,0), (0,0,0,1) \rangle \\
W_1 \cap W_6 &= \langle (0,1,1,0), (0,0,0,1) \rangle \\
W_1 \cap W_7 &= \langle (0,1,0,0), (0,0,1,0) \rangle \\
W_1 \cap W_8 &= \langle (0,1,0,0), (0,0,1,0) \rangle \\
W_1 \cap W_9 &= \langle (0,1,0,1), (0,0,1,0) \rangle \\
W_1 \cap W_{10} &= \langle (0,1,0,1), (0,0,1,0) \rangle \\
W_1 \cap W_{11} &= \langle (0,1,0,0), (0,0,1,1) \rangle \\
W_1 \cap W_{12} &= \langle (0,1,0,0), (0,0,1,1) \rangle \\
W_1 \cap W_{13} &= \langle (0,1,0,1), (0,0,1,1) \rangle \\
W_1 \cap W_{14} &= \langle (0,1,0,1), (0,0,1,1) \rangle \\
W_1 \cap W_{15} &= \langle (0,0,1,0), (0,0,0,1) \rangle
\end{aligned}
$$

$$
\begin{aligned}
W_2 \cap W_3 &= \langle (1,0,0,0), (0,0,0,1) \rangle \\
W_2 \cap W_4 &= \langle (1,0,1,0), (0,0,0,1) \rangle \\
W_2 \cap W_5 &= \langle (1,0,0,0), (0,0,0,1) \rangle \\
W_2 \cap W_6 &= \langle (1,0,1,0), (0,0,0,1) \rangle \\
W_2 \cap W_7 &= \langle (1,0,0,0), (0,0,1,0) \rangle \\
W_2 \cap W_8 &= \langle (1,0,0,1), (0,0,1,0) \rangle \\
W_2 \cap W_9 &= \langle (1,0,0,0), (0,0,1,0) \rangle \\
W_2 \cap W_{10} &= \langle (1,0,0,1), (0,0,1,0) \rangle \\
W_2 \cap W_{11} &= \langle (1,0,0,0), (0,0,1,1) \rangle \\
W_2 \cap W_{12} &= \langle (1,0,0,1), (0,0,1,1) \rangle \\
W_2 \cap W_{13} &= \langle (1,0,0,0), (0,0,1,1) \rangle \\
W_2 \cap W_{14} &= \langle (1,0,0,1), (0,0,1,1) \rangle \\
W_2 \cap W_{15} &= \langle (0,0,1,0), (0,0,0,1) \rangle
\end{aligned}
$$

$$
\begin{aligned}
W_3 \cap W_4 &= \langle (1,1,1,0),(0,0,0,1) \rangle \\
W_3 \cap W_5 &= \langle (1,1,1,0),(0,0,0,1) \rangle \\
W_3 \cap W_6 &= \langle (1,1,0,0),(0,0,0,1) \rangle \\
W_3 \cap W_7 &= \langle (1,1,0,0),(0,0,1,0) \rangle \\
W_3 \cap W_8 &= \langle (1,1,0,1),(0,0,1,0) \rangle \\
W_3 \cap W_9 &= \langle (1,1,0,1),(0,0,1,0) \rangle \\
W_3 \cap W_{10} &= \langle (1,1,0,0),(0,0,1,0) \rangle \\
W_3 \cap W_{11} &= \langle (1,1,0,0),(0,0,1,1) \rangle \\
W_3 \cap W_{12} &= \langle (1,1,0,1),(0,0,1,1) \rangle \\
W_3 \cap W_{13} &= \langle (1,1,0,1),(0,0,1,1) \rangle \\
W_3 \cap W_{14} &= \langle (1,1,0,0),(0,0,1,1) \rangle \\
W_3 \cap W_{15} &= \langle (0,0,0,1) \rangle
\end{aligned}
$$

$$
\begin{aligned}
W_4 \cap W_5 &= \langle (1,0,0,0),(0,0,0,1) \rangle \\
W_4 \cap W_6 &= \langle (1,1,0,0),(0,0,0,1) \rangle \\
W_4 \cap W_7 &= \langle (1,0,0,0),(0,1,0,0) \rangle \\
W_4 \cap W_8 &= \langle (1,0,0,1),(0,1,0,0) \rangle \\
W_4 \cap W_9 &= \langle (1,0,0,0),(0,1,0,1) \rangle \\
W_4 \cap W_{10} &= \langle (1,0,0,1),(0,1,0,1) \rangle \\
W_4 \cap W_{11} &= \langle (1,0,0,0),(0,1,0,0) \rangle \\
W_4 \cap W_{12} &= \langle (1,0,0,1),(0,1,0,0) \rangle \\
W_4 \cap W_{13} &= \langle (1,0,0,0),(0,1,0,1) \rangle \\
W_4 \cap W_{14} &= \langle (1,0,0,1),(0,1,0,1) \rangle \\
W_4 \cap W_{15} &= \langle (0,0,0,1) \rangle
\end{aligned}
$$

$$W_5 \cap W_6 = \langle (1,0,1,0),(0,0,0,1) \rangle$$
$$W_5 \cap W_7 = \langle (1,0,1,0),(0,1,0,0) \rangle$$
$$W_5 \cap W_8 = \langle (1,0,1,1),(0,1,0,0) \rangle$$
$$W_5 \cap W_9 = \langle (1,0,1,0),(0,1,0,1) \rangle$$
$$W_5 \cap W_{10} = \langle (1,0,1,1),(0,1,0,1) \rangle$$
$$W_5 \cap W_{11} = \langle (1,0,1,1),(0,1,0,0) \rangle$$
$$W_5 \cap W_{12} = \langle (1,0,1,0),(0,1,0,0) \rangle$$
$$W_5 \cap W_{13} = \langle (1,0,1,1),(0,1,0,1) \rangle$$
$$W_5 \cap W_{14} = \langle (1,0,1,0),(0,1,0,1) \rangle$$
$$W_5 \cap W_{15} = \langle (0,0,0,1) \rangle$$

$$W_6 \cap W_7 = \langle (1,0,0,0),(0,1,1,0) \rangle$$
$$W_6 \cap W_8 = \langle (1,0,0,1),(0,1,1,0) \rangle$$
$$W_6 \cap W_9 = \langle (1,0,0,0),(0,1,1,1) \rangle$$
$$W_6 \cap W_{10} = \langle (1,0,0,1),(0,1,1,1) \rangle$$
$$W_6 \cap W_{11} = \langle (1,0,0,0),(0,1,1,1) \rangle$$
$$W_6 \cap W_{12} = \langle (1,0,0,1),(0,1,1,1) \rangle$$
$$W_6 \cap W_{13} = \langle (1,0,0,0),(0,1,1,0) \rangle$$
$$W_6 \cap W_{14} = \langle (1,0,0,1),(0,1,1,0) \rangle$$
$$W_6 \cap W_{15} = \langle (0,0,0,1) \rangle$$

$$W_7 \cap W_8 = \langle (1,0,1,1),(0,1,1,0) \rangle$$
$$W_7 \cap W_9 = \langle (1,0,1,0),(0,1,1,1) \rangle$$
$$W_7 \cap W_{10} = \langle (1,0,1,1),(0,1,1,1) \rangle$$
$$W_7 \cap W_{11} = \langle (1,0,1,1),(0,1,1,1) \rangle$$
$$W_7 \cap W_{12} = \langle (1,0,1,0),(0,1,1,1) \rangle$$
$$W_7 \cap W_{13} = \langle (1,0,1,1),(0,1,1,0) \rangle$$
$$W_7 \cap W_{14} = \langle (1,0,1,0),(0,1,1,0) \rangle$$
$$W_7 \cap W_{15} = \langle (0,0,1,0) \rangle$$

$$W_8 \cap W_9 = \langle (1,0,0,0),(0,0,1,0) \rangle$$
$$W_8 \cap W_{10} = \langle (1,1,0,0),(0,0,1,0) \rangle$$
$$W_8 \cap W_{11} = \langle (1,0,0,0),(0,1,0,0) \rangle$$
$$W_8 \cap W_{12} = \langle (1,0,1,0),(0,1,0,0) \rangle$$
$$W_8 \cap W_{13} = \langle (1,0,0,0),(0,1,1,0) \rangle$$
$$W_8 \cap W_{14} = \langle (1,0,1,0),(0,1,1,0) \rangle$$
$$W_8 \cap W_{15} = \langle (0,0,1,0) \rangle$$

$$W_9 \cap W_{10} = \langle (1,0,0,1),(0,0,1,0) \rangle$$
$$W_9 \cap W_{11} = \langle (1,0,1,1),(0,1,0,0) \rangle$$
$$W_9 \cap W_{12} = \langle (1,0,0,1),(0,1,0,0) \rangle$$
$$W_9 \cap W_{13} = \langle (1,0,1,1),(0,1,1,0) \rangle$$
$$W_9 \cap W_{14} = \langle (1,0,0,1),(0,1,1,0) \rangle$$
$$W_9 \cap W_{15} = \langle (0,0,1,0) \rangle$$

$$W_{10} \cap W_{11} = \langle (1,0,0,0),(0,1,1,1) \rangle$$
$$W_{10} \cap W_{12} = \langle (1,0,1,0),(0,1,1,1) \rangle$$
$$W_{10} \cap W_{13} = \langle (1,0,0,0),(0,1,0,1) \rangle$$
$$W_{10} \cap W_{14} = \langle (1,0,1,0),(0,1,0,1) \rangle$$
$$W_{10} \cap W_{15} = \langle (0,0,1,0) \rangle$$

$$W_{11} \cap W_{12} = \langle (1,0,0,1),(0,1,1,1) \rangle$$
$$W_{11} \cap W_{13} = \langle (1,0,1,1),(0,1,0,1) \rangle$$
$$W_{11} \cap W_{14} = \langle (1,0,0,1),(0,1,0,1) \rangle$$
$$W_{11} \cap W_{15} = \langle (0,0,1,1) \rangle$$

$$W_{12} \cap W_{13} = \langle (1,0,0,0),(0,0,1,1) \rangle$$
$$W_{12} \cap W_{14} = \langle (1,1,0,0),(0,0,1,1) \rangle$$
$$W_{12} \cap W_{15} = \langle (0,0,1,1) \rangle$$

$$W_{13} \cap W_{14} = \langle (0,0,1,1) \rangle$$
$$W_{13} \cap W_{15} = \langle (0,0,1,1) \rangle$$
$$W_{14} \cap W_{15} = \langle (0,0,1,1) \rangle$$

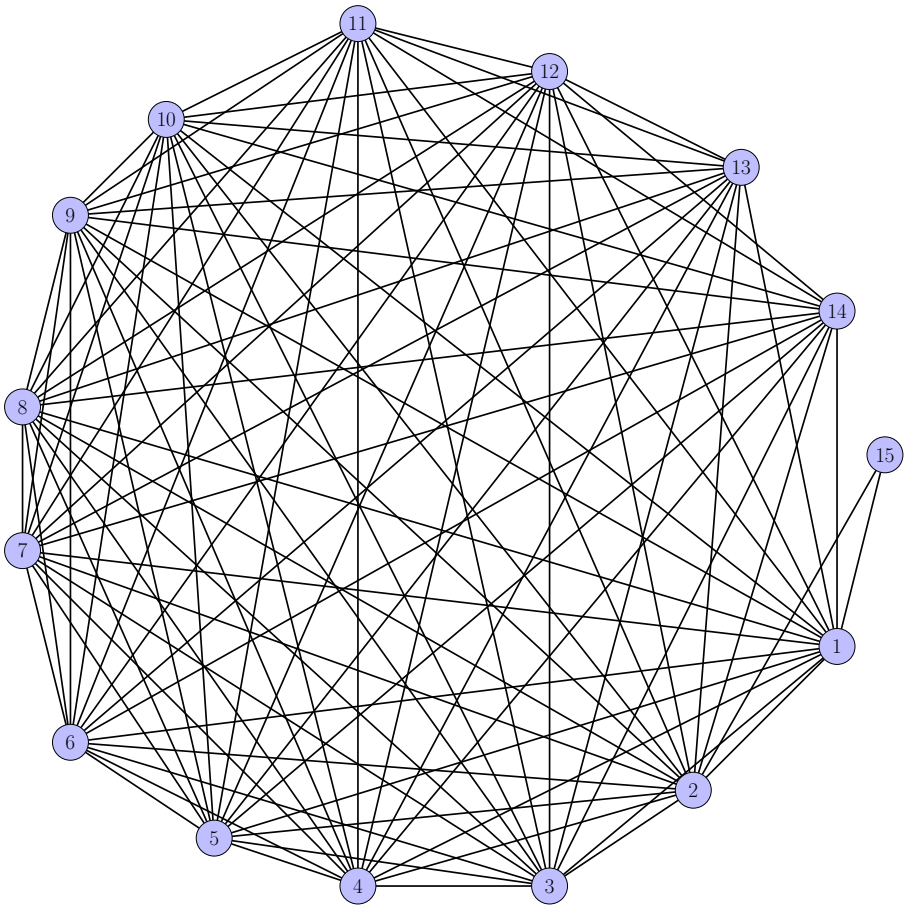

Figura 1.6: Grafo de Grassmman

1.2.12 Lema. Sean $X, Y, Z \in G_q(n,k)$ y asuma que $\dim_{\mathbb{F}_q}(Y \cap Z) = k-1$. Es decir, Y y Z son vértices incidentes en el grafo de Grassmann. Entonces

$$\dim_{\mathbb{F}_q}(X \cap Y) \geq \dim_{\mathbb{F}_q}(X \cap Z) - 1.$$

Demostración.

$$\begin{aligned}\dim_{\mathbb{F}_q}(X \cap Y) &\geq \dim_{\mathbb{F}_q}(X \cap Y \cap Z) \\ &= \dim_{\mathbb{F}_q}(X \cap Z) + \dim_{\mathbb{F}_q}(Y \cap Z) - \dim_{\mathbb{F}_q}(X \cap Z + Y \cap Z) \\ &\geq \dim_{\mathbb{F}_q}(X \cap Z) + \dim_{\mathbb{F}_q}(Y \cap Z) - \dim_{\mathbb{F}_q} Z \\ &= \dim_{\mathbb{F}_q}(X \cap Z) - 1. \qquad \square\end{aligned}$$

En consecuencia, si $\dim_{\mathbb{F}_q}(X \cap Y) = \dim_{\mathbb{F}_q}(X \cap Z) - 1$ se sigue que

$$X \cap Y \subseteq Z = (X \cap Z) + (Y \cap Z).$$

Como demostramos a continuación, el grafo de Grassmann $G_q(n,k)$ es un grafo distancia-regular de diámetro k. Para ello probamos que la distancia entre dos vértices X y Y es $d(X,Y) = k - \dim_{\mathbb{F}_q}(X \cap Y)$.

1.2.13 Teorema. Sean $X, Y \in G_q(n,k)$. Entonces la distancia entre X y Y está dada por

$$d(X,Y) = k - \dim_{\mathbb{F}_q}(X \cap Y). \tag{1.1}$$

Demostración. Si $\dim_{\mathbb{F}_q}(X \cap Y) = k - i$, para $i \in \{0, 1, \ldots, k\}$, entonces se puede construir explícitamente un camino de longitud i teniendo como puntos inicial y final a X y Y respectivamente. Por lo tanto $d(X,Y) \leq i$ y se tiene que

$$d(X,Y) \leq k - \dim_{\mathbb{F}_q}(X \cap Y).$$

La desigualdad recíproca puede ser demostrada por inducción sobre la distancia. Si $d(X,Y) = 1$, entonces los vértices son adyacentes y se verifica que

$$\dim_{\mathbb{F}_q}(X \cap Y) = k - 1$$

y se tiene la afirmación.

Supóngase entonces que X y Y están a una distancia $i \geq 2$. Entonces escojamos Z a una distancia $i-1$ de X y a una distancia 1 desde Y. Usando la hipótesis de inducción se tiene que

$$\dim_{\mathbb{F}_q}(X \cap Z) \geq k - (i-1).$$

Entonces la conclusión se sigue de la desigualdad en el lema anterior. $\square$

1.2.14 Lema. Dado $V \leq \mathbb{F}_q^n$, con $\dim V = k$, entonces V está contenido en

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

elementos de $G_q(n, n-1)$.

Demostración. Es claro que el número de subespacios de dimensión k en $\mathbb{F}_q^n$ es $\begin{bmatrix} n \\ k \end{bmatrix} =: A$. El número de subespacios de dimensión $n-1$ en $\mathbb{F}_q^n$ es $\begin{bmatrix} n \\ n-1 \end{bmatrix} =: B$. El número de subespacios de dimensión k en un subespacio de dimensión $n-1$ es $\begin{bmatrix} n-1 \\ k \end{bmatrix} =: C$. Entonces $\frac{A}{B}$ denota el número de subespacios de dimensión $n-1$ que contienen un subespacio dado de dimensión k. En efecto

$$\begin{aligned} BC &= \frac{(q^n-1)}{(q-1)} \frac{(q^{n-1}-1)\cdots(q^{n-1-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)} \\ &= \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k}-1)}{(q-1)(q^k-1)(q^{k-1}-1)\cdots(q-1)} \end{aligned}$$

luego,

$$\frac{BC}{A} = \frac{\dfrac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k}-1)}{(q-1)(q^k-1)(q^{k-1}-1)\cdots(q-1)}}{\dfrac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}} = \frac{q^{n-k}-1}{q-1}.\square$$

Para algunos fines, es mejor pensar en $\begin{bmatrix} n \\ k \end{bmatrix}$ como un polinomio en la indeterminada q en lugar de una función, potencia de un primo p. Por ejemplo:

$$\begin{aligned} \begin{bmatrix} 5 \\ 2 \end{bmatrix} = \frac{(q^5-1)(q^4-1)}{(q^2-1)(q-1)} &= \frac{(q-1)(q^4+q^3+q^2+q+1)(q^2-1)(q^2+1)}{(q^2-1)(q-1)} \\ &= (q^2+1)(q^4+q^3+q^2+q+1) \\ &= q^6+q^5+2q^4+2q^3+2q^2+q+1 \end{aligned}$$

En forma general:

$$\begin{bmatrix} n \\ k \end{bmatrix} = \sum_{i=0}^{k(n-k)} a_i q^i$$

donde el coeficiente a_i es el número de particiones distintas de k elementos que caben dentro de un rectángulo de tamaño $k \times (n-k)$.

1.3 Partición de un espacio vectorial y esquemas de asociación

1.3.1 Definición. Sea $\{V_i\}_1^k$ un conjunto de subespacios de un espacio vectorial V sobre $\mathbb{F}_q$. Decimos que tal conjunto es una partición de V si y solo si $V = \bigcup V_i$ y $V_i \cap V_j = \{0\}$ para todo $i \neq j$. El espacio vectorial V lo podemos escribir $V = \bigcup_{i=1}^{t} V_i$.

Definamos ahora $n_i = \dim V_i$. Se verifica que

$$q^n - 1 = \sum_1^k (q^{n_i} - 1)$$

y $n_i + n_j \leq n$ para $i \neq j$. En efecto, la primera condición se cumple porque cada vector no nulo en $\mathbb{F}_q^n$ pertenece a exactamente uno de los subespacios V_i y la segunda debido a que $V_i \bigoplus V_j$ es un subespacio de V con dimensión $n_i + n_j$.

Una serie de condiciones suficientes para la existencia de ciertas particiones de $\mathbb{F}_q^n$, se dan con detalles en [2]. A continuación, presentamos dos lemas muy importantes.

1.3.2 Lema. Sea W un subespacio de $\mathbb{F}_q^n$ con dimensión $n-1$. Definamos $n_i' = \dim(V_i \cap W)$ con $i = 1, 2, \ldots, k$. Entonces

$$n_i' = n_i = \dim V_i \text{ si } V_i \subseteq W$$
$$n_i' = n_i - 1 = \dim V_i - 1 \text{ si } V_i \nsubseteq W$$

En particular,

$$q^{n-1} - 1 = \sum_1^k (q^{n_i'} - 1)$$

Demostración. Del álgebra lineal, sabemos que

$$\dim(V_i + W) + \dim(V_i \cap W) = \dim W + \dim V_i.$$

Dado que $\dim(V_i + W) = n$ si $V_i \nsubseteq W$ y $\dim(V_i + W) = n - 1$ si $V_i \subseteq W$, se tiene el resultado. La particularidad se tiene del hecho de que $\{V_i \cap W\}_i^k$ es una partición de W.□

1.3.3 Lema. Si k divide a n y $t = \frac{q^n-1}{q^k-1}$, entonces existe una partición de $\mathbb{F}_q^n$ con t subespacios, todos de dimensión k.

Demostración. Identifiquemos el espacio vectorial n-dimensional $\mathbb{F}_q^n$ con el cuerpo $\mathbb{F}_{q^n}$. Si k divide a n, entonces $\mathbb{F}_{q^k}$ es un subcuerpo de $\mathbb{F}_{q^n}$. Luego, el grupo cíclico $H := \mathbb{F}_{q^k}^*$ es un subgrupo de $G := \mathbb{F}_{q^n}^*$. Por lo tanto, existe $T \subseteq G$ tal que $|T| = t$ y

$$G = \dot{\bigcup_{g \in T}} gH.$$

y además, para todo $g, h \in T$ con $g \neq h$ se verifica que $gH \cap hH = \emptyset$. A T se le denomina transversal de H en G o sistema de representantes para las clases laterales.

Definamos ahora, $V_i := g_i \mathbb{F}_{q^k}$, con $i = 1, 2, \ldots, t$. Dado que cada V_i es un subespacio vectorial de $\mathbb{F}_{q^n}$ y las clases laterales anteriores son disyuntas, se deduce que

$$\mathbb{F}_q^n = \bigcup_{i=1}^{t} V_i.$$

□

1.3.4 Ejemplo. Consideremos el cuerpo finito $\mathbb{F}_{2^4}$ como un espacio vectorial. Dado que $2|4$, se tiene que $\mathbb{F}_{2^2}^\times \leq \mathbb{F}_{2^4}^\times$. Por otro lado,

$$\begin{aligned} \mathbb{F}_{2^2} &= \mathbb{F}_2[x]/\langle x^2 + x + 1 \rangle \\ &= \{0, 1, x, x+1\}, \end{aligned}$$

donde $\mathbb{F}_{2^2}^\times = \langle \alpha \rangle$, siendo α una raíz del polinomio irreducible $x^2 + x + 1$.

De igual manera,

$$\begin{aligned} \mathbb{F}_{2^4} &= \mathbb{F}_2[x]/\langle x^4 + x + 1 \rangle \\ &= \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1, x^3, x^3+1, x^3+x, \\ &\quad x^3+x+1, x^3+x^2, x^3+x^2+1, x^3+x^2+x, x^3+x^2+x+1\}, \end{aligned}$$

donde $\mathbb{F}_{2^4}^\times = \langle \alpha^2 + 1 \rangle$. Dado que $|T| = t = \frac{q^4-1}{q^2-1} = 5$, se tiene que $\mathbb{F}_{2^4}^\times \supseteq T = \{x_1, x_2, x_3, x_4, x_5\}$. Determinemos ahora la partición de $\mathbb{F}_{2^4}^\times$. Para ello definamos $V_i = x_i \mathbb{F}_{2^2}$, con $x_i \in T$. Tomemos

$$\begin{aligned} x_1 &= 1 \\ x_2 &= \alpha^3 + \alpha^2 + \alpha + 1 \\ x_3 &= \alpha^3 + \alpha^2 + 1 \\ x_4 &= \alpha^3 + \alpha + 1 \\ x_5 &= \alpha^2 + \alpha. \end{aligned}$$

En consecuencia

$$\begin{aligned}
V_1 &= \mathbb{F}_{2^2} = \{0, 1, \alpha, \alpha+1\} \\
V_2 &= x_2\mathbb{F}_{2^2} = \{0, \alpha^3+\alpha^2+\alpha+1, \alpha^3, \alpha^2+\alpha+1\} \\
V_3 &= x_3\mathbb{F}_{2^2} = \{0, \alpha^3+\alpha^2+1, \alpha^3+1, \alpha^2\} \\
V_4 &= x_4\mathbb{F}_{2^2} = \{0, \alpha^3+\alpha+1, \alpha^2+1, \alpha^3+\alpha^2+\alpha\} \\
V_5 &= x_5\mathbb{F}_{2^2} = \{0, \alpha^2+\alpha, \alpha^3+\alpha^2, \alpha^3+\alpha\}.
\end{aligned}$$

Así, el conjunto $\{V_1, \ldots, V_5\}$ es una partición de $\mathbb{F}_2^4$.

1.3.5 Definición. Sea X un conjunto finito con al menos 2 elementos, y para cualquier número entero $n \geq 1$, sea $R = \{R_0, R_1, \ldots, R_n\}$ una familia de $(n+1)$ relaciones binarias R_i definidas sobre el conjunto X. Es decir, para cada i se verifica que $R_i \subseteq X \times X$. La pareja (X, R) es llamada un esquema de asociación con n clases si se satisfacen las siguientes propiedades:

(a) El conjunto R es una partición de $X \times X$.

(b) $R_0 = \{(x, x) \mid x \in X\}$.

(c) Las relaciones R_i son simétricas. Es decir, para todo i, $R_i^{-1} = R_i$.

(d) Para tres enteros cualesquiera $i, j, k = 0, 1, \ldots, n$, existe un número $p_{ij}^k = p_{ji}^k$, tal que para todo $(x, y) \in R_k$:

$$|\{z \in X \mid (x, z) \in R_i; (z, y) \in R_j\}| = p_{ij}^k.$$

El número p_{ij}^k es llamado el número de intersecciones del esquema (X, R). Decimos que $x, y \in X$ son i-esimos asociados cuando $(x, y) \in R_i$.

El hecho de que p_{ii}^0 exista, significa que hay un número constante de i-esimas asociaciones, usualmente se denota r_i, donde $p_{ii}^0 = r_i$ y $p_{ij}^0 = 0$ si $i \neq j$, además

$$r_0 = 1, \quad r_0 + r_1 + \cdots + r_k = N,$$

con $N := |X|$. Los números $r_0, r_1, \ldots, r_k$ son llamados lo grados del esquema.

1.3.6 Ejemplo. El grafo de Johnson $J(4, 2)$ representa un esquema de asociación 2-clase con 6 elementos. Dos k-subconjuntos A y B de $J(n, k)$ se llaman i-th asociados cuando $|A \cap B| = k - i$. En este caso, se tiene que $p_{11}^0 = r_1 = 4$, $p_{22}^0 = r_2 = 1$, así, $r_0 + r_1 + r_2 = 6$.

1.3.7 Definición. Sea $R = \{R_0, R_1, \ldots, R_n\}$ una familia de $(n+1)$ relaciones binarias R_i definidas sobre el conjunto X, la cual satisface las las condiciones (a) y (c) establecida en la definición 1.3.5. Sea además $M \subseteq \{0, 1, \ldots, n\}$ con $0 \in M$. Un subconjunto no vacío Y de X es llamado una M-cuadrilla (en ingles M-clique) con respecto a R, si y solo si se satisface

$$R_i \cap (Y \times Y) = \emptyset,$$

para todo $i \in \{0, 1, \ldots, n\} \setminus M$. Es decir, cualquier par de elementos de Y son j-asociados para algún $j \in M$.

Un problema interesante es encontrar una cota superior para el número de puntos en una M-cuadrilla. En el siguiente teorema de Delsarte se presenta una respuesta a este interrogante. Notamos con M^* al conjunto $M \setminus \{0\}$.

1.3.8 Teorema. (Delsarte) Sea $M \subseteq \{0, 1, \ldots, n\}$ con $0 \in M$ y sea $\hat{M} = \{0, 1, \ldots, n\} \setminus M^*$. Si Y es una M-cuadrilla y Z es una $\hat{M}$-cuadrilla en un esquema de asociación (X, R), entonces

$$|Y||Z| \leq |X|.$$

Demostración. Ver Teorema 3.9 en [4]. □

Capítulo 2

Códigos en el espacio proyectivo

Sea $\mathbb{F}_q$ el cuerpo finito con q elementos y sea W un espacio vectorial arbitrario, pero fijo, de dimensión n sobre $\mathbb{F}_q$. El espacio proyectivo de orden n sobre el cuerpo finito $\mathbb{F}_q$, denotado como $\mathbb{P}_q(n)$, es el conjunto de todos los subespacios del espacio vectorial W, incluyendo $\{0\}$ y W. Por lo tanto

$$\mathbb{P}_q(n) = \bigcup_{0 \leq k \leq n} G_q(n,k).$$

2.1 Una métrica sobre el espacio proyectivo

Definamos una función distancia $d : \mathbb{P}_q(n) \times \mathbb{P}_q(n) \longrightarrow \mathbb{N}_0$ de la siguiente manera

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

para todo $U, V \in \mathbb{P}_q(n)$.

Dado que

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

podemos escribir:

$$d(U,V) = \dim U + \dim V - 2\dim(U \cap V) \tag{2.1}$$

2.1.1 Lema. La función d define una métrica sobre $\mathbb{P}_q(n)$. Es decir, para todo $U, V, X \in \mathbb{P}_q(n)$ se verifican

(a) $d(U,V) \geq 0$ y $d(U,V) = 0$ si y sólo si $U = V$.

(b) $d(U,V) = d(V,U)$.

(c) $d(U,V) \leq d(U,X) + d(X,V)$. (Desigualdad triangular)

Demostración. Las dos primeras condiciones son claramente ciertas, por lo que nos centramos en la desigualdad triangular.

Tenemos que

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

entonces

$$\begin{aligned} \tfrac{1}{2}\left[d(U,V) - d(U,X) - d(X,V)\right] &= \dim(U\cap X) + \dim(X\cap V) - \dim X \\ &\quad - \dim(U\cap V) \\ &= \underbrace{\dim\left(U\cap X + X\cap V\right) - \dim X}_{\leq 0} \\ &\quad + \underbrace{\dim\left(U\cap X\cap V\right) - \dim(U\cap V)}_{\leq 0} \\ &\leq 0. \end{aligned}$$

La primera desigualdad se tiene ya que $(U\cap X + X\cup V) \subseteq X$ y la segunda desigualdad porque $(U\cap X\cap V) \subseteq (U\cap V)$. $\square$

2.1.2 Nota. Como consecuencia del lema anterior se tiene que tanto $\mathbb{P}_q(n)$ como $G_q(n,k)$, pueden considerarse como espacios métricos.

2.1.3 Definición. Sea $C \subseteq \mathbb{P}_q(n)$.

(a) La distancia mínima de C se nota y define de la siguiente manera:

$$d(C) := \min\{d(U,V) \mid U,V \in C, U \neq V\}.$$

(b) Decimos que C es un (n,M,d)-código en el espacio proyectivo, si $|C| = M$ y $d(C) = d$. Si un (n,M,d)-código C está contenido en $G_q(n,k)$ para algún k, decimos que C es un (n,M,d,k)-código, o también un código de dimensión constante.

(c) Los números (n,M,d) o (n,M,d,k) son llamados los parámetros de C.

Los (n, M, d) y (n, M, d, k)-códigos en el espacio proyectivo son similares, respectivamente, a los ampliamente conocidos códigos en el espacio de Hamming, y códigos de dimensión constante en el espacio de Johnson, donde la distancia de Hamming sirve como la métrica.

No obstante existen diferencias sustanciales. Para todo q, n y k, el espacio métrico $G_q(n, k)$ corresponde a grafos de distancia-regular, similar a los grafos de distancia-regular que aparecen en espacio de Johnson.

Por otro lado, mientras que el espacio de Hamming $\mathbb{F}_q^n$ es siempre distancia-regular (como grafo), el espacio proyectivo $\mathbb{P}_q(n)$, no lo es. Esto implica que la intuición geométrica convencional no aplica siempre, por ejemplo, dos esferas del mismo radio en $\mathbb{P}_q(n)$ pueden tener una cantidad distinta de elementos.

Códigos en $G_q(n, k)$ se estudiaron esporadicamente entre los últimos veinte años. Recientemente, R. Koetter y F. R. Kschischang [9], [10] demostraron que los códigos en $\mathbb{P}_q(n)$ son precisamente los que se necesitan para la corrección de errores en la red.

Un (n, M, d)-código puede corregir cualquier t paquete de errores y cualquier ρ paquetes de borraduras introducidos en algún lugar de la red, siempre que $2(t + \rho) < d$.

2.2 Anticódigos y conjuntos con t-intersección

Sea V un espacio vectorial sobre $\mathbb{F}_q$. Denotamos con $\begin{bmatrix} V \\ k \end{bmatrix}$ el conjunto de todos los subespacios de V que tienen dimensión k.

2.2.1 Definición. Sea ahora V de dimensión n sobre $\mathbb{F}_q$ y sean $t \leq k \leq n$. Una familia $\mathcal{F} \subseteq \begin{bmatrix} V \\ k \end{bmatrix}$ se denomina un conjunto con t-intersección, si para todo $X, Y \in \mathcal{F}$ se verifica que

$$\dim_{\mathbb{F}_q}(X \cap Y) \geq t.$$

2.2.2 Definición. Un anticódigo $\mathcal{A}(D)$, de diámetro D, en $G_q(n, k)$ es cualquier subconjunto de $G_q(n, k)$ tal que $d(U, V) \leq D$, para todo $U, V \in \mathcal{A}(D)$. Un anticódigo $\mathcal{A}(D)$ es llamado optimal, si este es el anticódigo más grande entre todos los anticódigos con los mismos parámetros (longitud y distancia máxima) que $\mathcal{A}(D)$.

Note que todo antiódigo $\mathcal{A}(D)$ en el grafo de Grassmann $G_q(n, k)$ es un conjunto con $(k - D)$-intersección. En efecto, recordemos que la distancia entre dos codewords $X, Y \in \mathcal{A}(D)$ está dada por

$$d(X, Y) = k - \dim_{\mathbb{F}_q}(X \cap Y).$$

Además se verifica que

$$d(X,Y) \leq D.$$

Por lo tanto

$$\dim_{\mathbb{F}_q}(X \cap Y) \geq k - D$$

y se tiene la afirmación.

Existen dos tipos triviales de familias con la propiedad de t-intersección.

Caso 1. Si $n \leq 2k-t$, entonces una familia con t-intersección es el conjunto de todos los subespacios k-dimensionales de V. En efecto, si $X, Y \in \begin{bmatrix} V \\ k \end{bmatrix}$, entonces

$$n \geq \dim_{\mathbb{F}_q}(X+Y) = 2k - \dim_{\mathbb{F}_q}(X \cap Y).$$

Con lo cual se tiene que

$$\dim_{\mathbb{F}_q}(X \cap Y) \geq 2k - n \geq t.$$

Este conjunto tiene $\begin{bmatrix} n \\ k \end{bmatrix}$ elementos.

Caso 2. Si $k = n$ o $t = k$, entonces una familia con t-intersección contiene un solo elemento.

Como consecuencia los casos interesantes de familia con t-intersección se tienen cuando $t < k < n$ y cuando $n > 2k - t$. El tamaño y la estructura de los conjuntos óptimos no triviales con t-intersección fueron establecidos por P. Frankl y R. M. Wilson en [7]. El resultado principal se presenta a continuación.

2.2.3 Teorema. Sea $\mathcal{F} \subseteq \begin{bmatrix} V \\ k \end{bmatrix}$ una familia con t-intersección. Entonces

$$|\mathcal{F}| \leq \max\left\{ \begin{bmatrix} n-t \\ k-t \end{bmatrix}, \begin{bmatrix} 2k-t \\ k \end{bmatrix} \right\}.$$

Demostración. Ver teorema 1 en [7]. □

2.2.4 Nota. En este mismo trabajo los autores examinaron las dos posible soluciones involucradas en el teorema anterior.

Caso 3. Si $2k - t < n < 2k$, entonces la cota superior está dada por

$$|\mathcal{F}| \leq \begin{bmatrix} 2k-t \\ k \end{bmatrix} \tag{2.2}$$

y esta es alcanzada en una única forma, tomando algún $Y \in \begin{bmatrix} V \\ 2k-t \end{bmatrix}$ y definiendo

$$\mathcal{F} := \left\{ X \in \begin{bmatrix} V \\ k \end{bmatrix} \mid \dim_{\mathbb{F}_q}(X \cap Y) \geq k \right\}$$

Esta familia es denominada anticódigos de `tipo I`.

Caso 4. Si $2k < n$, entonces la cota superior está dada por

$$|\mathcal{F}| \leq \begin{bmatrix} n-t \\ k-t \end{bmatrix} \tag{2.3}$$

y esta es alcanzada en una única forma, tomando algún $Y \in \begin{bmatrix} V \\ t \end{bmatrix}$ y definiendo

$$\mathcal{F} := \left\{ X \in \begin{bmatrix} V \\ k \end{bmatrix} \mid \dim_{\mathbb{F}_q}(X \cap Y) \geq t \right\}$$

Esta familia es denominada anticódigos de `tipo II`.

Caso 5. Si $n = 2k$, entonces la cota superior es

$$|\mathcal{F}| \leq \begin{bmatrix} n-t \\ k-t \end{bmatrix} = \begin{bmatrix} 2k-t \\ k \end{bmatrix} \tag{2.4}$$

y esta es alcanzada tanto por los anticódigos de tipo I como por los de tipo II.

2.3 Cotas superiores para el tamaño de un código en el espacio proyectivo

R. Koetter y F. R. Kschischang probaron en [10] las cotas equivalentes a las del empaquetamiento esférico, la de Singleton y la de Gilbert-Varshamov de la teoría clásica de códigos. En esta sección se establecen algunas cotas superiores para el tamaño de los códigos en la k-Grassmanniana $G_q(n,k)$.

2.3.1 Definición. Con $A_q(n,d)$ y $A_q(n,d,k)$ denotamos los siguientes números:

$$A_q(n,d) := \max\{|C| : C \subseteq \mathbb{P}_q(n),\ d(C) \geq d\}$$
$$A_q(n,d,k) := \max\{|C| : C \subseteq G_q(n,k),\ d(C) \geq d\}.$$

En general el cálculo de $A_q(n,d)$ y $A_q(n,d,k)$ es un problema notablemente difícil. Solamente en unos casos particulares de los parámetros q, n, d y k se conocen valores exactos. Entonces una primera forma de atacar el problema es encontrar cotas superiores razonables. Muchas cotas superiores para códigos en $G_q(n,k)$ se han podido determinar. Por ejemplo la cota del empaquetamiento esférico, la cota de Singleton y cotas para anticódigos.

El panorama para las cotas inferiores es aún mas pobre, se conoce por ejemplo la versión q-aria de la cota de Gilbert - Varshamov.

2.3.2 Notas. Sea $C \subseteq G_q(n,k)$.

(a) La distancia entre dos elementos de C es siempre un número par. En efecto, para todo $U, V \in C$ se verifica que

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

(b) De (a) se sigue que

- $d(C) \leq 2k$ ó
- $d(C) = 2k$ si y solo si $(U \cap V) = \{0\}$, para todo $U, V \in C$.

Como consecuencia de lo anterior, en adelante es suficiente considerar $A_q(n,d,k)$ con $d = 2\delta$.

2.3.3 Definición. La esfera $S(V,k,t)$ de radio t y centro en $V \in G_q(n,k)$ se define de la siguiente manera:

$$S(V,k,t) := \{U \in G_q(n,k) \mid d(U,V) \leq 2t\}.$$

2.3.4 Teorema. El número de subespacios en $S(V,k,t)$ es independiente del centro V y está dado por

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

para $t \leq k$.

Demostración. Dado que $G_q(n,k)$ es un grafo distancia-regular, se tiene que $|S(V,k,t)|$ es independiente de V.

Determinamos ahora el número de subespacios U cuya intersección con V es un subespacio de dimensión $k-i$. Se pueden elegir los subespacios intersección con dimensión $k-i$ en $\begin{bmatrix} k \\ i \end{bmatrix} = \begin{bmatrix} k \\ k-i \end{bmatrix}$ formas.

Seguidamente podemos completar el subespacio en

$$\begin{aligned} &\frac{(q^n - q^k)(q^n - q^{k+1}) \dots (q^n - q^{k+i-1})}{(q^k - q^{k-i})(q^k - q^{k-i+1}) \dots (q^k - q^{k-1})} = \\ &\frac{(q^{n-k} - 1)(q^{n-k-1} - 1) \dots (q^{n-k-i+1} - 1)}{(q^i - 1)(q^{i-1} - 1) \dots (q - 1)} q^{i^2} = \\ &\qquad \begin{bmatrix} n-k \\ i \end{bmatrix} q^{i^2} \end{aligned}$$

formas. En consecuencia, la cardinalidad de un nivel de espacios a una distancia $2i$ de V es igual a

$$\begin{bmatrix} n-k \\ i \end{bmatrix} \begin{bmatrix} k \\ i \end{bmatrix} q^{i^2}.$$

Sumando las cardinalidades de los distintos niveles se tiene la afirmación. □

2.3.5 Teorema. (Cota de Hamming o del empaquetamiento esférico) Sea $C \subseteq G_q(n,k)$ con $d(C) \geq 2\delta$ y sea $t = \left\lfloor \frac{\delta-1}{2} \right\rfloor$. Entonces

$$A_q(n, 2\delta, k) \leq \frac{|G_q(n,k)|}{|S(V,k,t)|} = \frac{\begin{bmatrix} n \\ k \end{bmatrix}}{\sum_{i=0}^{t} \begin{bmatrix} k \\ i \end{bmatrix} \begin{bmatrix} n-k \\ i \end{bmatrix} q^{i^2}}. \tag{2.5}$$

Demostración. Se sigue inmediatamente del teorema anterior. □

El teorema 2.5 corresponde en este contexto a la muy conocida cota de empaquetamiento esférico en el espacio de Hamming de la teoría clásica.

2.3.6 Teorema. (Cota de Singleton) Sea $C \subseteq G_q(n,k)$ con $d(C) \geq 2\delta$ y sea $t = \left\lfloor \frac{\delta-1}{2} \right\rfloor$. Entonces

$$A_q(n, 2\delta, k) \leq \begin{bmatrix} n-\delta+1 \\ k-\delta+1 \end{bmatrix}. \tag{2.6}$$

Demostración. Ver teorema 9 en [10]. □

2.3.7 Teorema. Sea $C \subseteq G_q(n,k)$. Si $d(C) = 2k$, entonces

$$|C| \leq \frac{q^n - 1}{q^k - 1}.$$

En particular, si se cumple la igualdad, entonces $k \mid n$.

Demostración. Dado que $d(C) = 2k$, para todo $U, V \in C$ con $U \neq V$, se verifica que $U \cap V = \{0\}$. Si $C = \{V_1, \ldots, V_r\}$, entonces si definimos $V_j^{\times} = V_j \setminus \{0\}$ se tiene que

$$\bigcup_{j=1}^{r} V_j^{\times} \subseteq \mathbb{F}_q^n \setminus \{0\},$$

donde la union anterior es disyunta. Por lo tanto

$$\Big|\bigcup_{j=1}^{r} V_j^{\times}\Big| = \sum_{j=1}^{r} |V_j^{\times}| = r\left(q^k - 1\right) \leq q^n - 1,$$

con lo cual se tiene la afirmación.

Finalmente, supongamos que $|C| = \frac{q^n-1}{q^k-1}$ y demostremos que $k \mid n$. Para ello consideremos los grupos multiplicativos asociados a $V \in G_q(n,k)$ y a $\mathbb{F}_q^n$ con ordenes q^k-1 y q^n-1 respectivamente. Del teorema de Lagrange se tiene que q^k-1 divide a q^n-1. Supongamos que $k \nmid n$. Entonces $n = kd + r$, con $0 \leq r < k$, y se tiene que

$$\begin{aligned} q^n - 1 &= q^{kd+r} - 1 \\ &= q^r(q^{kd} - 1) + (q^r - 1) \end{aligned}$$

Así, $q^k - 1$ divide a $q^{kd} - 1$, por lo tanto $q^k - 1$ divide a $q^r - 1$, lo cual es posible si $r = 0$, ya que $q^k - 1 > q^r - 1$. Entonces $n = kd$. □

Observamos que la esfera no es realmente la estructura adecuada para considerar en el caso $G_q(n,k)$. La cota de empaquetamiento esférico, es un caso especial de la cota de anticódigos que fue probada por P. Delsarte [4] para un esquema de asociación arbitrario.

El Teorema de Delsarte 1.3.8 implica que

$$A_q(n, 2\delta, k) \leq \frac{|G_q(n,k)|}{|A(\delta - 1)|}$$

para cualquier anticódigo de diámetro $\delta - 1$.

2.3.8 Nota. La esfera $S(V,k,t)$ es claramente un ejemplo de un anticódigo. Pero en contraste con el espacio binario de Hamming, donde las esferas son los anticódigos más grandes, $S(V,k,t)$ es sólo un pequeño anticódigo en $G_q(n,k)$. Los anticódigos óptimos en $G_q(n,k)$ se presentaron en la nota 2.2.4.

Combinando los resultados de [7] con la discusión anterior, obtenemos:

2.3.9 Teorema. Sean $n, k \in \mathbb{N}$ con $n > 2k$. Entonces

$$A_q(n, 2\delta + 2, k) \leq \frac{\begin{bmatrix} n \\ k \end{bmatrix}}{\begin{bmatrix} n-k+\delta \\ \delta \end{bmatrix}}.$$

Demostración. Sabemos que un anticódigo de diámetro δ es un conjunto con t-intersección, donde $t = k - \delta$. En este caso, el tamaño del anticódigo optimo de diámetro δ en $G_q(n,k)$ está dado por $\begin{bmatrix} n-t \\ k-t \end{bmatrix} = \begin{bmatrix} n-k+\delta \\ \delta \end{bmatrix}$, con lo cual se tiene la afirmación. □

Una forma completamente diferente de mejorar la cota superior establecida en (2.5) se basa en un argumento estandar de cobertura.

2.3.10 Teorema.

$$A_q(n, 2\delta + 2, k) \leq \frac{\begin{bmatrix} n \\ k-\delta \end{bmatrix}}{\begin{bmatrix} k \\ k-\delta \end{bmatrix}}.$$

Demostración. Sea C un $(n, M, 2\delta + 2, k)$-código en $G_q(n,k)$. Entonces todo codeword de C contiene exactamente $\begin{bmatrix} k \\ k-\delta \end{bmatrix}$ subespacios de dimensión $k - \delta$.

Por otro lado, dado un subespacio de $\mathbb{F}_q^n$ de dimension $k - \delta$, este no puede estar contenido en dos codewords distintos $U, V \in C$, ya que si este no es el caso entonces

$$\begin{aligned} d(U,V) &= 2k - 2\dim(U \cap V) \\ &\leq 2k - 2(k-\delta) \\ &= 2\delta \\ &< 2\delta + 2, \end{aligned}$$

lo cual es una contradicción.

Dado que el número total de subespacios de $\mathbb{F}_q^n$ de dimensión $k - \delta$ es $\begin{bmatrix} n \\ k-\delta \end{bmatrix}$ se tiene que M no puede exceder el cociente

$$\frac{\begin{bmatrix} n \\ k-\delta \end{bmatrix}}{\begin{bmatrix} k \\ k-\delta \end{bmatrix}},$$

con lo cual se tiene el resultado. □

Los dos siguientes teoremas corresponden a las versiones q-arias de las dos cotas clásicas de Johnson para códigos de peso constante.

2.3.11 Teorema.

$$A_q(n, 2\delta, k) \leq \tfrac{q^n-1}{q^k-1} A_q(n-1, 2\delta, k-1).$$

Demostración. Sea C un $(n, M, 2\delta, k)$-código en $G_q(n,k)$ y supongamos que $M = A_q(n, 2\delta, k)$. Entonces cada codeword de C contiene $\frac{q^k-1}{q-1}$ subespacios 1-dimensional de $\mathbb{F}_q^n$. Dado que el número total de tales subespacios es

$\frac{q^n-1}{q-1}$, existe un subespacio $X \in G_q(n,1)$ que está contenido en por lo menos

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

codeword de C. Supongamos que

$$X = \langle x \rangle = \{\lambda x \mid \lambda \in \mathbb{F}_q\}.$$

con $x \in \mathbb{F}_q^n$ y escribamos

$$\mathbb{F}_q^n = \langle x \rangle \oplus S,$$

donde $S \in G_q(n, n-1)$. Este subespacio S puede obtenerse a partir de una base de $\mathbb{F}_q^n$ que contenga a x, por ejemplo, si $B = (x, e_1, \ldots, e_{n-1})$ es una base para $\mathbb{F}_q^n$, entonces defina $S = \langle e_1, \ldots, e_{n-1} \rangle$. Sea ahora

$$C' := \{V \cap S \mid V \in C; X \subset V\}.$$

Se verifica que todos los codewords de C' están contenidos en S y que estos tienen dimensión $k-1$. En efecto, sea $(V \cap S) \in C'$. Claramente $(V \cap S)$ está contenido en S. Se verifica además que $V + S = \mathbb{F}_q^n$. Para demostrarlo, tomemos $v \in \mathbb{F}_q^n$, entonces

$$v = (x + \sum_{j=1}^{n-1} \lambda_j e_j) \in V + S.$$

Por lo tanto

$$n = \dim_{\mathbb{F}_q}(V + S) = k + n - 1 - \dim(V \cap S),$$

de donde se sigue que

$$\dim(V \cap S) = k - 1.$$

Entonces C' puede considerarse como un $(n-1, M', 2\delta', k-1)$-código, donde $M' \geq M\frac{q^k-1}{q^n-1}$, ya que en cada elemento de C' está X y este está contenido en por lo menos $M\frac{q^k-1}{q^n-1}$ elementos. Resta demostar que $\delta = \delta'$ ya que esto implicaría que

$$A_q(n-1, 2\delta, k-1) \geq M' \geq \frac{q^k-1}{q^n-1} A_q(n, 2\delta, k).$$

Para finalizar, consideremos dos codewords arbitrarios $U', V' \in C'$ tales que $U' = U \cap S$ y $V' = V \cap S$, donde $U, V \in C$ y $X \subset U$ y $X \subset V$. Note que

$$U' \cap V' = (U \cap S) \cap (V \cap S) = (U \cap V) \cap S,$$

lo cual implica que

$$\begin{aligned}\dim(U' \cap V') &= \dim(U \cap V) + \dim S - \dim((U \cap V) + S) \\ &= \dim(U \cap V) + (n-1) - n,\end{aligned}$$

donde la segunda igualdad se sigue del hecho que $U \cap V$ contiene a X. Se sigue entonces que

$$\dim(U' \cap V') = \dim(U \cap V) - 1.$$

Usando (2.1) se tiene que

$$\begin{aligned}d(U', V') &= \dim U' + \dim V' - 2\dim(U' \cap V') \\ &= (k-1) + (k-1) - 2(\dim(U \cap V) - 1) \\ &= k + k - 2\dim(U \cap V) \\ &= \dim U + \dim V - 2\dim(U \cap V) \\ &= d(U, V),\end{aligned}$$

con lo cual podemos afirmar que $\delta = \delta'$ y se tiene la afirmación. □

2.3.12 Teorema.

$$A_q(n, 2\delta, k) \leq \frac{q^n - 1}{q^{n-k} - 1} A_q(n-1, 2\delta, k)$$

Demostración. Sea C un $(n, M, 2\delta, k)$-código en $G_q(n, k)$ y supongamos que $M = A_q(n, 2\delta, k)$. Para cada $S \in G_q(n, n-1)$ definamos

$$C_S = \{V \mid V \in C; V \subset S\}.$$

Entonces se verifica que C_S es un $(n-1, M_S, 2\delta', k)$-código con $\delta' \geq \delta$, para todo $S \in G_q(n, n-1)$. Del lema 1.2.14 se tiene que dado un subespacio de $\mathbb{F}_q^n$ de dimensión k este, está contenido en $\frac{q^{n-k}-1}{q-1}$ elementos de $G_q(n, n-1)$. Entonces cada codeword de C pertenece a $\frac{q^{n-k}-1}{q-1}$ códigos distintos C_S y por lo tanto

$$\sum_S |C_S| = M \frac{q^{n-k} - 1}{q - 1},$$

donde la suma corre sobre todos los $\frac{q^n-1}{q-1}$ elementos de $G_q(n, n-1)$. Por lo tanto, existe por lo menos un $S \in G_q(n, n-1)$ tal que

$$|C_S| \geq M \frac{q^{n-k} - 1}{q^n - 1}.$$

Dado que es obvio que $A_q(n-1, 2\delta, k) \geq |C_S|$, para todo S, se tiene la afirmación. □

Los teoremas 2.3.11 y 2.3.12 pueden ser iterados para obtener una cota para $A_q(n, 2\delta, k)$ para cualquier valor específico de n, δ y k.

No resulta claro en que orden deben hacerse las iteraciones para producir la mejor cota. De hecho este problema aún sigue abierto para el espacio de Johnson clásico. No obstante, se puede iterar el teorema 2.3.11 con sí mismo. Con la observación que $A_q(n, 2\delta, k) = 1$, para todo $k < \delta$, se tiene la siguiente cota:

2.3.13 Teorema.

$$A_q(n, 2\delta, k) \leq \left\lfloor \frac{q^n - 1}{q^k - 1} \left\lfloor \frac{q^{n-1} - 1}{q^{k-1} - 1} \ldots \left\lfloor \frac{q^{n-k+\delta} - 1}{q^\delta - 1} \right\rfloor \ldots \right\rfloor \right\rfloor$$

El siguiente teorema es consecuencia inmediata de 2.3.11.

2.3.14 Teorema.

$$A_q\left(n, 2\delta, k\right) \leq \prod_{i=0}^{k-\delta} \frac{q^{n-i} - 1}{q^{k-i} - 1} \tag{2.7}$$

Demostración. Efectúe $k-\delta+1$ iteraciones del teorema 2.3.11, deteniendo el proceso con la igualdad $A_q(n-k+\delta-1, 2\delta, \delta-1) = 1$. □

2.3.15 Observación. Los teoremas 2.3.9, 2.3.10 y 2.3.14 se demostraron utilizando métodos completamente diferentes. Por lo tanto es notable que estas tres cotas coincidan. Esto es,

$$\frac{\begin{bmatrix} n \\ k \end{bmatrix}}{\begin{bmatrix} n-k+\delta \\ \delta \end{bmatrix}} = \frac{\begin{bmatrix} n \\ k-\delta \end{bmatrix}}{\begin{bmatrix} k \\ k-\delta \end{bmatrix}} = \prod_{i=0}^{k-\delta-1} \frac{q^{n-i} - 1}{q^{k-i} - 1}. \tag{2.8}$$

Estas igualdades se puede verificar directamente a partir de la definición del q-esimo coeficiente de Gauss.

Para la primera igualdad note que

$$\begin{aligned}
\begin{bmatrix} n \\ k \end{bmatrix} \begin{bmatrix} k \\ k-\delta \end{bmatrix} &= \begin{bmatrix} n \\ k \end{bmatrix} \begin{bmatrix} k \\ \delta \end{bmatrix} \\
&= \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)} \frac{(q^k-1)(q^{k-1}-1)\cdots(q^{k-\delta+1}-1)}{(q^\delta-1)(q^{\delta-1}-1)\cdots(q-1)} \\
&= \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^{k-\delta}-1)\cdots(q-1)} \frac{1}{(q^\delta-1)\cdots(q-1)}
\end{aligned}$$

Por otro lado,

$$\begin{bmatrix} n \\ k-\delta \end{bmatrix}\begin{bmatrix} n-k+\delta \\ k-\delta \end{bmatrix} = \frac{(q^n-1)\cdots(q^{n-k+\delta+1}-1)}{(q^{k-\delta}-1)\cdots(q-1)} \cdot \frac{(q^{n-k+\delta}-1)\cdots(q^{n-k+1}-1)}{(q^{\delta}-1)\cdots(q-1)}$$
$$= \frac{(q^n-1)\cdots(q^{n-k+1}-1)}{(q^{k-\delta}-1)\cdots(q-1)} \cdot \frac{1}{(q^{\delta}-1)\cdots(q-1)}$$

Para la segunda igualdad, note que:

$$\frac{\begin{bmatrix} n \\ k-\delta \end{bmatrix}}{\begin{bmatrix} k \\ k-\delta \end{bmatrix}} = \frac{\dfrac{(q^n-1)\cdots(q^{n-k+\delta+1}-1)}{(q^{k-\delta}-1)\cdots(q-1)}}{\dfrac{(q^k-1)\cdots(q^{\delta+1}-1)}{(q^{k-\delta}-1)\cdots(q-1)}}$$
$$= \frac{(q^n-1)\cdots(q^{n-k+\delta+1}-1)}{(q^k-1)\cdots(q^{\delta+1}-1)}$$
$$= \prod_{i=0}^{k-\delta-1} \frac{q^{n-i}-1}{q^{k-i}-1}.$$

Es de notar que en contraste con la cota del empaquetamiento esférico (2.5) las cotas establecidas anteriormente son siempre más fuertes que la cota de Singleton (2.6), como se demostró en [17]. R. Koetter y F. R. Kschischang demostraron en [10] que la cota de Singleton (2.6) difiere del valor de $A_q\left(n, 2\delta, k\right)$ en un factor de a lo más 4. Esto inmediatamente implica que todas las cotas en (2.8) tienen la misma propiedad. Sin embargo, estas cotas pueden mejorarse aún más, aunque ligeramente, como vimos anteriormente.

Concluimos esta sección con una cota superior e inferior para $A_q(n,d)$, la contraparte de la muy conocida cota de Gilbert-Varshamov para códigos en $G_q(n,k)$ demostrada por R. Koetter y F. R. Kschischang en [10]. La generalización de esta cota en $\mathbb{P}_q(n)$ no es trivial, ya que esferas del mismo radio en $\mathbb{P}_q(n)$ pueden tener una cantidad distinta de elementos.

2.3.16 Lema. Una esfera de radio r con centro en $X \in \mathbb{P}_q(n)$ se define en la forma usual

$$S_r(X) = \{Y \in \mathbb{P}_q(n) \mid d(X,Y) \leq r\}.$$

Sea $c(j,k,r)$ el número de subespacios de dimensión j en una esfera de radio r con centro en un subespacio vectorial de dimensión k de $\mathbb{F}_q^n$. Esto es,

$$c(j,k,r) = |S_r(X) \cap G_q(n,j)|, \text{ para todo} X \in G_q(n,k)$$

Entonces

$$c(j,k,r) = \sum_{i=\lceil \frac{k+j-r}{2} \rceil}^{\min\{j,k\}} \begin{bmatrix} k \\ i \end{bmatrix} \begin{bmatrix} n-k \\ j-i \end{bmatrix} q^{(j-i)(k-i)} \tag{2.9}$$

Demostración. Dado $X \in G_q(n,k)$, existen $\begin{bmatrix} k \\ i \end{bmatrix}$ formas de escoger un subespacio Z de X que tenga dimensión i. Para un Z fijo, asumiendo que $i \leq j$, el número de subespacios $Y \in G_q(n,j)$ tales que $X \cap Y = Z$ está dado por

$$\lambda := \frac{(q^n - q^k)(q^n - q^{k+1}) \cdots (q^n - q^{k+j-i-1})}{(q^j - q^i)(q^j - q^{i+1}) \cdots (q^j - q^{j-1})} = \begin{bmatrix} n-k \\ j-i \end{bmatrix} q^{(j-i)(k-i)}.$$

En efecto, el número de elementos en el complemento de X es $q^n - q^k$, y el número de elementos en $Y - Z$ es $q^j - q^i$.

Note que $\frac{q^n - q^k}{q^j - q^i}$ representa el número de elementos en el complemento de X que complementan a Z con dimensión $i+1$. El siguiente nivel suministra $\frac{q^n - q^{k+1}}{q^j - q^{i+1}}$ elementos. Razonando de este modo, obtenemos:

$$\begin{aligned} \lambda &= \frac{q^k(q^{n-k}-1)q^{k+1}(q^{n-k-1}-1)\cdots q^{k+j-i-1}(q^{n-k-j+i+1}-1)}{q^i(q^{j-i}-1)q^{i+1}(q^{j-i-1}-1)\cdots q^{j-1}(q-1)} \\ &= \begin{bmatrix} n-k \\ j-i \end{bmatrix} \underbrace{q^{k-i}q^{k-i}\cdots q^{k-i}}_{j-i \ veces} \\ &= \begin{bmatrix} n-k \\ j-i \end{bmatrix} q^{(j-i)(k-i)}. \end{aligned}$$

Finalmente, note que $d(X,Y) \leq r$ si y solo si se verifica que

$$\dim X + \dim Y - 2\dim(X \cap Y) \leq r$$

O equivalentemente, $k + j - 2i \leq r$. En resumen tenemos que

$$d(X,Y) \leq r \Leftrightarrow 2i \geq k + j - r,$$

con lo que se sigue inmediatamente la afirmación. □

En el siguiente lema, usando (2.9) podemos calcular el tamaño de la esfera de radio r con centro en $X \in G_q(n,k)$. Note que esta expresión es diferente a la obtenida en el teorema 2.3.4. En realidad en ese teorema se calculó $c(k,k,r) = |S_r(X) \cap G_q(n,k)|$.

En lo que sigue, asumimos por convención que $\begin{bmatrix} k \\ i \end{bmatrix} = 0$, para todo $i \notin \{0,1,\ldots,k\}$.

2.3.17 Lema. Para todo $X \in \mathbb{P}_q(n)$ con $\dim X = k$, se tiene que

$$|S_r(X)| = S_{k,r} := \sum_{j=0}^{r} \sum_{i=0}^{j} \begin{bmatrix} k \\ i \end{bmatrix} \begin{bmatrix} n-k \\ j-i \end{bmatrix} q^{i(j-i)}. \tag{2.10}$$

Demostración. Dado que $c(j,k,r) = |S_r(X) \cap G_q(n,j)|$ para todo $X \in G_q(n,k)$, donde cada uno de los $c(j,k,r)$ representa el cardinal de una "subesfera" de $S_r(X)$ de dimensión constante j, tenemos que

$$|S_r(X)| = \sum_{j=0}^{n} c(j,k,r) = \sum_{j=0}^{n} \sum_{i=\lceil \frac{k+j-r}{2} \rceil}^{\min\{j,k\}} \begin{bmatrix} k \\ i \end{bmatrix} \begin{bmatrix} n-k \\ j-i \end{bmatrix} q^{(j-i)(k-i)}.$$

Ahora, si definimos $j := j + k - 2i$ e $i := k - i$ resulta que: si $i = \frac{k+j-r}{2}$, entonces $j = r$ y si $i = j$, entonces $j = k - j$ de modo que $j = \min\{j,k\}$. Así, podemos escribir:

$$|S_r(X)| = \sum_{j=0}^{r} \sum_{i=0}^{j} \begin{bmatrix} k \\ i \end{bmatrix} \begin{bmatrix} n-k \\ j-i \end{bmatrix} q^{i(j-i)},$$

con lo que se tiene la afirmación. □

El siguiente teorema es el equivalente a la cota de Gilbert-Varshamov.

2.3.18 Teorema.

$$A_q(n,d) \geq \frac{\displaystyle\sum_{k=0}^{n} \sum_{j=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} \begin{bmatrix} n \\ j \end{bmatrix}}{\displaystyle\sum_{k=0}^{n} \sum_{j=0}^{d-1} \sum_{i=0}^{j} \begin{bmatrix} n \\ k \end{bmatrix} \begin{bmatrix} k \\ i \end{bmatrix} \begin{bmatrix} n-k \\ j-i \end{bmatrix} q^{i(j-i)}}.$$

Demostración. Para la demostración, usamos el resultado dado en [14] en el que se manifiesta que:

Si S_r^p es el tamaño promedio de una esfera de radio r en un grafo $G(V,E)$, entonces existe un código C en G con distancia mínima al menos d y

$$|C| \geq \frac{|V|}{S_{d-1}^p}.$$

En el caso de $\mathbb{P}_q(n)$, se tiene que:

$$S_{d-1}^p = \frac{\sum_{X \in \mathbb{P}_q(n)} |S_{d-1}|}{|\mathbb{P}_q(n)|} = \frac{1}{|\mathbb{P}_q(n)|} \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} S_{k,d-1}$$

es el tamaño promedio de una esfera de radio $d-1$. Finalmente, el teorema se sigue de (2.10). □

2.3.19 Definición. Dado un código C en el espacio proyectivo $\mathbb{P}_q(n)$, denotamos con $D_0, D_1, \ldots, D_n$ su `distribución de dimensión`. Esto es, para $0 \leq k \leq n$ se verifica que

$$D_k = |C \cap G_q(n,k)|.$$

Adoptamos por convención que $D_k = 0$, siempre que $k \notin \{0, 1, \ldots, n\}$.

2.3.20 Ejemplo. Sea $C \subset \mathbb{P}_2(5)$, el código dado en el ejemplo 3.2.7. Se nota que $D_0 = D_1 = D_5 = 0$ y $D_2 = D_3 = 9$

La siguiente cota para $A_q(n,d)$ se obtiene utilizando métodos de programación lineal.

2.3.21 Teorema. Sea $f^* = \max \sum_{k=0}^{n} D_k$ sujeto a las $2n+2$ restricciones lineales

$$D_k \leq A_q(n, 2e+2, k), \qquad k = 0, 1, \ldots, n, \tag{2.11}$$

y

$$\sum_{i=-e}^{e} c(k, k+i, e) D_{k+i} \leq \begin{bmatrix} n \\ k \end{bmatrix}, \qquad k = 0, 1, \ldots, n, \tag{2.12}$$

donde los coeficiente $c(k, k+i, e)$ se definen como en (2.9). Entonces f^* es una cota superior para $A_q(n, 2e+1)$.

Demostración. Las expresiones (2.11) y (2.12) son las restricciones de la distribución de dimensión de un $(n, M, 2e+1)$ código en $\mathbb{P}_q(n)$.

Para la restricción (2.11), consideremos un código $C \subseteq \mathbb{P}_q(n)$ con distancia mínima $2e+1$. Dado que $D_k = |C \cap G_q(n,k)|$ para $k = 0, \ldots, n$, se tiene entonces que $\sum_{k=0}^{n} D_k = |C|$. Así $D_k \leq A_q(n, 2e+2, k)$.

Por otra parte, para la expresión (2.12), note que las esferas de radio e centradas en los codewords de C son disyuntas dos a dos, dado que no dependen de la elección de X en C. Por lo tanto los conjuntos $S_e(X) \cap G_q(n,k)$ son pares disyuntos de $G_q(n,k)$. Así (2.12) cuenta el número de puntos de $G_q(n,k)$ contenidos en tales esferas. □

Capítulo 3

Algunas construcciones de códigos

3.1 Estructuras de Steiner

En esta seccicón V denota un espacio vectorial de dimensión n sobre $\mathbb{F}_q$. Las estructuras de Steiner pueden entenderse como una generalización de los sistemas de Steiner estudiados en la geometría finita.

3.1.1 Definición. Una familia $\mathcal{F} \subseteq \begin{bmatrix} V \\ k \end{bmatrix}$ se denomina una estructura de Steiner, notada con $S_q(t,k,n)$, si los bloques de $\mathcal{F}$ son subespacios de dimensión k de V y cada subespacio de dimensión t de V está contenido en exactamente un bloque de $\mathcal{F}$.

3.1.2 Ejemplo. Consideremos $V := \mathbb{F}_{2^4}$ como en el ejemplo 3.3.2 y tomemos $k = 2$ y $t = 1$. Dado que $\begin{bmatrix} V \\ k \end{bmatrix} = \{V_1, V_2, \ldots, V_{35}\}$, donde cada V_i con $i = \{1, \ldots, 35\}$ es un subespacios de V de dimensión 2. Definamos

$$\mathcal{F} = \{V_1, V_{20}, V_{27}, V_{29}V_{34}\} = \{\{0, \alpha^0, \alpha, \alpha^4\}, \{0, \alpha^2, \alpha^3, \alpha^6\}, \\ \{0, \alpha^7, \alpha^8, \alpha^{11}\}, \{0, \alpha^5, \alpha^{12}, \alpha^{14}\}, \{0, \alpha^9, \alpha^{10}, \alpha^{13}\}\}.$$

Observe que cada subespacio de V de dimensión 1:

$$\{\{0, \alpha^0\}, \{0, \alpha\}, \{0, \alpha^2\}, \{0, \alpha^3\}, \{0, \alpha^4\}, \{0, \alpha^5\}, \\ \{0, \alpha^6\}, \{0, \alpha^7\}, \{0, \alpha^8\}, \{0, \alpha^9\}, \{0, \alpha^{10}\}, \{0, \alpha^{11}\}, \\ \{0, \alpha^{12}\}, \{0, \alpha^{13}\}, \{0, \alpha^{14}\}\}$$

está contenido en exactamente un bloque de $\mathcal{F}$, por tanto $\mathcal{F}$ es una estructura de Steiner, $S_2(1,2,4)$.

Note que $\{V_1, V_{20}, V_{27}, V_{29}V_{34}\}$, excluyendo en todos el vector nulo, forma una partición del espacio vectorial V.

3.1.3 Lema. El número total de bloques en un $S_q(t,n,k)$ es

$$\frac{\begin{bmatrix} n \\ t \end{bmatrix}}{\begin{bmatrix} k \\ t \end{bmatrix}}.$$

Demostración. Sabemos que el número total de subespacios de dimensión t de un espacio vectorial de dimensión n está dado por $\begin{bmatrix} n \\ t \end{bmatrix}$. Cada bloque de $S_q(t,n,k)$ contiene $\begin{bmatrix} k \\ t \end{bmatrix}$ subespacios de dimensión t. Ahora, dado que cada subespacio de dimensión t está contenido en exactamente un bloque, se tiene el resultado. □

3.2 Construcción de códigos

Los códigos óptimos en el espacio de Johnson pueden ser construidos a partir de las estructuras de Steiner. Se observa que una construcción completamente análoga se puede llevar a cabo en el espacio proyectivo.

Se puede demostrar facilmente que cualquier estructura de Steiner $S_q(t,n,k)$ es un (n, M, d, k)-código C en $G_q(n,k)$ con $M = \begin{bmatrix} n \\ t \end{bmatrix} / \begin{bmatrix} k \\ t \end{bmatrix}$ y $d(C) = 2(k-t+1)$. En efecto, sin perdida de generalidad, para $t = 2$.

$$\begin{aligned} t = 2 &\Leftrightarrow d(C) = 2(k-t+1) = 2(k-2+1) = 2k-2 \\ &\leq d(U,V) = 2k - 2\dim(U \cap V) \\ &\Leftrightarrow \dim(U \cap V) \leq 1 \end{aligned}$$

para todo $U \neq V$ en C. Luego, cada subespacio 2-dimensional de $\mathbb{F}_q^n$ está contenido en exactamente $\begin{bmatrix} n \\ 2 \end{bmatrix} / \begin{bmatrix} k \\ 2 \end{bmatrix}$.

La estructura de Steiner dada en el ejemplo 3.1.2, es un $(4, 5, 4, 2)$- código en $G_2(4,2)$.

En particular, Schwartz y Etzion [13], construyen una Estructura de Steiner para todo q cuando k divide a n.

Como consecuencia del comentario anterior, se tiene que

$$A_q(n, 2k, k) = \frac{q^n - 1}{q^k - 1}; \qquad \text{cuando } k|n, \tag{3.1}$$

la particularidad del teorema 2.3.7.

En este trabajo se extienden los resultados de [2], [6] y [13] para el caso en que k no divide a n. Nuestra construcción se resume en el siguiente teorema que incluye (3.1) como un caso especial.

3.2.1 Teorema. Sea $n \equiv r \mod k$. Entonces para todo q se tiene que

$$A_q(n, 2k, k) \geq \frac{q^n - q^k(q^r - 1) - 1}{q^k - 1} \tag{3.2}$$

Demostración. Sea r el residuo que se obtiene cuando k divide a n y definamos $m = k + r$. En adelante, se representan los vectores en $\mathbb{F}_q^n$ como:

$$\mathbb{F}_q^n = \left\{(x, y) : x \in \mathbb{F}_{q^{n-m}}, y \in \mathbb{F}_{q^m}\right\}$$

Sea α un elemento primitivo de $\mathbb{F}_{q^{n-m}}$ y sea β un elemento primitivo de $\mathbb{F}_{q^m}$. Además, sea

$$W = \left\langle (0, \beta^0), (0, \beta^1), \ldots, (0, \beta^{k-1}) \right\rangle \tag{3.3}$$

Dado que $\beta^0, \beta^1, \ldots, \beta^{k-1}$ son independientes sobre $\mathbb{F}_q$ y $m \geq k$, vemos que $\dim W = k$. Ahora, definamos $t = \frac{q^{n-m}-1}{q^k-1}$ cuando k divide a $n-m$ por nuestra elección de m. Sea $\gamma = \alpha^t$. Entonces el orden multiplicativo de γ en $\mathbb{F}_{q^{n-m}}$ es $q^k - 1$ y por lo tanto γ es un elemento primitivo de $\mathbb{F}_{q^k}$, como un subcuerpo de $\mathbb{F}_{q^{n-m}}$. Esto implica que $\gamma^0, \gamma^1, \ldots, \gamma^{k-1}$ forman una base para $\mathbb{F}_{q^k}$ sobre $\mathbb{F}_q$ y por lo tanto son linealmente independiente sobre $\mathbb{F}_q$.Ahora, consideremos $t + t(q^m - 1)$ subespacios de $\mathbb{F}_q^n$ dados por

$$U_i = \left\langle (\alpha^i, 0), (\alpha^i\gamma, 0), \ldots, (\alpha^i\gamma^{k-1}, 0) \right\rangle \tag{3.4}$$

$$V_{i,j} = \left\langle (\alpha^i, \beta^j), (\alpha^i\gamma, \beta^{j+1}), \ldots, (\alpha^i\gamma^{k-1}, \beta^{j+k-1}) \right\rangle \tag{3.5}$$

donde $i = 0, 1, \ldots, t-1$ y $0 \leq i, j \leq q^m - 2$. Dado que $\gamma^0, \gamma^1, \ldots, \gamma^{k-1}$ son independientes sobre $\mathbb{F}_q$, es facil ver que $\dim U_i = \dim V_{i,j} = k$ para todo i, j.

Construimos el código C como sigue:

$$C = \left(\bigcup_i U_i\right) \cup \left(\bigcup_{i,j} V_{i,j}\right) \cup W.$$

Observe que C tiene el número requerido de codewords, pues $t + t(q^m - 1) + 1$ se evalua al lado derecho de (3.2) por nuestra elección de m y t.

Para completar la prueba, resta por demostrar que la distancia mínima de C es $2k$. Dado que $C \subset G_q(n,k)$, esto significa que debemos demostrar que para todo $X, Y \in C$, distintos, tenemos que $X \cap Y = \{0\}$.

En primer lugar, observe que para cualquier vector no nulo (x,y) en $\mathbb{F}_q^n$, se tiene que

$$\begin{aligned}(x,y) \in W &\Rightarrow x = 0, y \neq 0\\ (x,y) \in U_i &\Rightarrow x \neq 0, y = 0\\ (x,y) \in V_{i,j} &\Rightarrow x \neq 0, y \neq 0\end{aligned}$$

ya que ambos $\alpha^i, \alpha^i\gamma, \ldots, \alpha^i\gamma^{k-1}$ y $\beta^j, \beta^{j+1}, \ldots, \beta^{j+k-1}$ son linealmente independientes sobre $\mathbb{F}_q$ para todo i, j. Se sigue que

$$W \cap U_i = W \cap V_{i,j} = U_i \cap V_{i,j} = \{0\} \text{ para todo } i, j.$$

Ahora, observe que los t espacios vectoriales $U_0, U_1, \ldots, U_{t-1}$ forman una partición de $\mathbb{F}_q^{n-m}$. Por lo tanto $U_{i_1} \cap U_{i_2} = \{0\}$ para todo $i_1 \neq i_2$. Por la misma razón $V_{i_1,j_1} \cap V_{i_2,j_2} = \{0\}$ para todo j_1 y j_2 siempre que $i_1 \neq i_2$.

Resta por demostrar que $V_{i,j_1} \cap V_{i,j_2} = \{0\}$ para cada i fijo y todo $j_1 \neq j_2$.

Supongamos lo contario, que (x,y) es un vector no nulo en $V_{i,j_1} \cap V_{i,j_2}$ y consideremos las correspondientes combinaciones lineales de los vectores de la base en (3.5), a saber

$$\begin{aligned}x &= a_0\alpha^i + a_1\alpha^i\gamma + \cdots + a_{k-1}\alpha^i\gamma^{k-1}\\ &= b_0\alpha^i + b_1\alpha^i\gamma + \cdots + b_{k-1}\alpha^i\gamma^{k-1}\end{aligned} \tag{3.6}$$

$$\begin{aligned}y &= a_0\beta^{j_1} + a_1\beta^{j_1+1} + \cdots + a_{k-1}\beta^{j_1+k-1}\\ &= b_0\beta^{j_2} + b_1\beta^{j_2+1} + \cdots + b_{k-1}\beta^{j_2+k-1}\end{aligned} \tag{3.7}$$

Dado que $\gamma^0, \gamma^1, \ldots, \gamma^{k-1}$ son linealmente independientes sobre $\mathbb{F}_q$, (3.6) implica que $b_l = a_l$ para todo l. Por lo tanto, podemos reescribir (3.7) como sigue:

$$(\beta^{j_1} - \beta^{j_2})(a_0 + a_1\beta + a_2\beta^2 + \cdots + a_{k-1}\beta^{k-1}) = 0.$$

Pero como $1, \beta, \beta^2, \ldots, \beta^{k-1}$ también son independientes sobre $\mathbb{F}_q$, esto implica que $\beta^{j_1} = \beta^{j_2}$, y por lo tanto $j_1 = j_2$, lo cual es una contradicción.□

3.2.2 Definición. Sea C un código en $\mathbb{P}_q(n)$. El **código dual** de C, notado con $C^\perp$ es definido de la siguiente manera:

$$C^\perp = \{V^\perp \mid V \in C\} \subseteq \mathbb{P}_q(n).$$

El complemento ortogonal se considera por primera vez en el contexto de los códigos de dimensión constante, es decir en $G_q(n,k)$, en los trabajos de [10] y [17]. Presentamos ahora algunas extensiones al espacio proyectivo $\mathbb{P}_q(n)$, y pruebas formales que no fueron dadas en [10] y [17].

3.2.3 Lema. Sean $U, V \in \mathbb{P}_q(n)$. Entonces

$$\dim(U^\perp \cap V^\perp) = n - \dim U - \dim V + \dim(U \cap V).$$

Demostración. Note inicialmente que

$$(U+V)^\perp = U^\perp \cap V^\perp.$$

En efecto, si $x \in U^\perp \cap V^\perp$, entonces $\langle x, u\rangle = 0$, para todo $u \in U$ y $\langle x, v\rangle = 0$, para todo $v \in V$. Entonces $\langle x, au+bv\rangle = 0$, para todo $a, b \in \mathbb{F}_q$ y por lo tanto $x \in (U+V)^\perp$.

Recíprocamente, si $x \in (U+V)^\perp$, entonces dado que U y V son subespacios de $U+V$ se sigue que $x \in U^\perp \cap V^\perp$.

Finalmente, de la ampliamente conocida igualdad

$$\dim(U+V)^\perp = n - \dim(U+V)$$

se sigue que

$$\begin{aligned}\dim(U^\perp \cap V^\perp) &= \dim(U+V)^\perp \\ &= n - \dim(U+V) \\ &= n - \dim U - \dim V + \dim(U \cap V). \ \square\end{aligned}$$

3.2.4 Lema. Si C es un (n, M, d)-código en $\mathbb{P}_q(n)$, entonces su código dual $C^\perp$ también es un (n, M, d)-código.

Demostración. La igualdad de los dos primeros parámetros es evidente. Sean $U, V \in C$, con $\dim U = i$ y $\dim V = j$. Sea además, $U^\perp$ y $V^\perp$ los correspondientes elementos de $C^\perp$. Entonces, por el lema anterior, se tiene que

$$\begin{aligned}d(U^\perp, V^\perp) &= \dim U^\perp + \dim V^\perp - 2\dim(U^\perp \cap V^\perp) \\ &= (n-i) + (n-j) - 2(n-i-j+\dim(U \cap V)) \\ &= i + j - 2\dim(U \cap V) \\ &= \dim U + \dim V - 2\dim(U \cap V) \\ &= d(U, V).\end{aligned}$$

Por consiguiente, C y $C^\perp$ tienen la misma distribución de distancia, y en particular, la misma distancia mínima. $\square$

3.2.5 Nota. El lema anterior nos lleva facilmente a una demostración alternativa del teorema 2.3.12. En efecto, del lema 3.2.4 se sigue que

$$A_q(n, 2\delta, k) = A_q(n, 2\delta, n-k),$$

y del teorema 2.3.11 se tiene que

$$A_q(n, 2\delta, n-k) \leq \frac{q^n - 1}{q^{n-k} - 1} A_q(n-1, 2\delta, n-k-1).$$

Pero se verifica que

$$A_q(n-1, 2\delta, n-k-1) = A_q(n-1, 2\delta, k),$$

en consecuencia del lema anterior se sigue el teorema 2.3.12.

3.2.6 Lema.

$$A_q(n, 2k, k) \leq \left\lfloor \frac{q^n - 1}{q^k - 1} \right\rfloor - 1 \quad \text{si} \quad n \not\equiv 0 \mod k$$

Demostración. Supongamos que k divide a n y escribamos $n = mk + r$ donde $r \neq 0$ por nuestra hipótesis. Es fácil ver que

$$q^n - 1 = q^r \left(q^{(m-1)k} + \cdots + q^k + 1 \right) (q^k - 1) + (q^r - 1). \tag{3.8}$$

En efecto:

$$\begin{aligned} q^n - 1 &= q^{mk} q^r - 1 \\ &= q^r (q^{mk} - 1) + (q^r - 1) \\ &= q^r \left(\frac{q^{mk} - 1}{q^k - 1} \right) (q^k - 1) + (q^r - 1) \\ &= q^r \left(q^{(m-1)k} + \cdots + q^k + 1 \right) (q^k - 1) + (q^r - 1). \end{aligned}$$

Ahora supongamos por el contrario que existe un $(n, M, 2k, k)$-código en $G_q(n, k)$ con $M = \left\lfloor \frac{q^n - 1}{q^k - 1} \right\rfloor$. Además, sean $V_1, V_2, \ldots, V_M$ codewords de C, y observe que $V_i \cap V_j = \{0\}$ para todo $i \neq j$. Por lo tanto, se puede particionar $\mathbb{F}_q^n \setminus \{0\}$ en $M + 1$ conjuntos disyuntos como sigue:

$$\mathbb{F}_q^n \setminus \{0\} = V_1^* \cup V_2^* \cup \cdots \cup V_M^* \cup X \tag{3.9}$$

donde $V_i^* = V_i \setminus \{0\}$ para todo i, y X denota el conjunto de todos los vectores en $\mathbb{F}_q^n$ que no están contenidos en cualquier codeword de C. Así

$$|X| = (q^n - 1) - M(q^k - 1) = q^r - 1$$

por (3.8) y (3.9).

Ahora, consideremos un vector fijo no nulo $u \in \mathbb{F}_q^n$ y un subconjunto $S \subseteq \mathbb{F}_q^n$, además sea $\eta_u(S)$ el número de vectores en S que no son ortogonales a u, es decir,

$$\eta_u(S) := |\{x \in S : \langle x, u\rangle \neq 0\}|$$

donde el producto interno es sobre $\mathbb{F}_q$. Note que $\eta_u(V_i^*) = \eta_u(V_i)$ es cero o $q^k - q^{k-1} = (q-1)q^{k-1}$, para todo i, pues V_i es un espacio vectorial de dimensión k. Además $\eta_u(\mathbb{F}_q^n) = (q-1)q^{n-1}$. Por lo tanto,

$$\eta_u(X) = \eta_u(\mathbb{F}_q^n \setminus \{0\}) - \sum_{i=1}^{M} \eta_u(V_i^*) \tag{3.10}$$

es divisible por q^{k-1}. Pero, $|X| = q^r - 1 < q^{k-1}$, lo cual implica que $\eta_u(X) = 0$. Dado que esto es cierto para todo vector no nulo $u \in \mathbb{F}_q^n$, el conjunto X no puede contener cualquiera de los vectores no nulos, lo cual es una contradicción. □

Presentamos ahora algunos ejemplos específicos de los códigos en $\mathbb{P}_q(n)$.

3.2.7 Ejemplo. Consideremos en código $C \subseteq \mathbb{P}_2(5)$, $C := \{V_1, V_2, \ldots, V_{18}\}$

$$\begin{aligned}
V_1 &= \langle (0,0,0,1,1), (0,0,1,0,1)\rangle \\
V_2 &= \langle (0,1,1,0,1), (1,0,1,0,0)\rangle \\
V_3 &= \langle (0,1,1,1,1), (1,0,0,1,0)\rangle \\
V_4 &= \langle (0,0,1,1,1), (0,1,0,1,1)\rangle \\
V_5 &= \langle (0,1,1,1,1), (1,0,1,0,1)\rangle \\
V_6 &= \langle (0,0,0,1,0), (1,0,0,0,1)\rangle \\
V_7 &= \langle (0,0,1,0,0), (1,1,0,0,0)\rangle \\
V_8 &= \langle (0,1,0,1,0), (1,0,0,0,0)\rangle \\
V_9 &= \langle (0,1,0,0,0), (1,0,1,1,0)\rangle \\
V_{10} &= \langle (0,0,1,1,1), (0,1,0,0,0), (1,0,0,0,0)\rangle \\
V_{11} &= \langle (0,0,0,1,0), (0,1,0,0,1), (1,0,1,0,1)\rangle
\end{aligned}$$

$$V_{12} = \langle (0,0,1,0,1), (0,1,0,0,1), (1,0,0,1,1) \rangle$$
$$V_{13} = \langle (0,0,0,1,0), (0,0,1,0,0), (1,1,0,0,1) \rangle$$
$$V_{14} = \langle (0,0,0,1,1), (0,1,1,0,1), (1,0,1,0,0) \rangle$$
$$V_{15} = \langle (0,0,0,1,1), (0,1,0,0,1), (1,0,0,0,1) \rangle$$
$$V_{16} = \langle (0,0,0,0,1), (0,1,1,0,0), (1,0,0,0,0) \rangle$$
$$V_{17} = \langle (0,0,0,0,1), (0,0,1,1,0), (1,0,0,1,0) \rangle$$
$$V_{18} = \langle (0,0,0,0,1), (0,0,1,0,0), (0,1,0,1,0) \rangle$$

Se puede verificar por simple inspección que la distancia mínima de C es 3. En efecto, dado que

$$\dim V_i + \dim V_j = \dim(V_i + V_j) + \dim(V_i \cap V_j),$$

para los V_i de C pueden presentarse los siguientes casos:

(a) $3 + 3 = 5 + \dim(V_{10} \cap V_{16})$, entonces $\dim(V_{10} \cap V_{16}) = 1$

(b) $3 + 2 = 5 + \dim(V_3 \cap V_{18})$, entonces $\dim(V_3 \cap V_{18}) = 0$

(c) $3 + 2 = 4 + \dim(V_1 \cap V_{14})$, entonces $\dim(V_1 \cap V_{14}) = 1$

(d) $2+2 = 4+\dim(V_i \cap V_j)$, entonces $\dim(V_i \cap V_j) = 0$, para $i, j = \{1, 2, \ldots, 9\}$

por lo tanto, usando

$$d(V_i, V_j) = \dim V_i + \dim V_j - 2\dim(V_i \cap V_j),$$

en C se presentan las siguientes distancias:

(a) $d(V_{10}, V_{16}) = 3 + 3 - 2(1) = 4$

(b) $d(V_3, V_{18}) = 3 + 2 - 2(0) = 5$

(c) $d(V_1, V_{14}) = 3 + 2 - 2(1) = 3$

(d) $d(V_i, V_j) = 2 + 2 - 2(0) = 4$, para $i, j = \{1, 2, \ldots, 9\}$.

Se concluye entonces que la distancia mínima de C es 3 y por tanto un $(5, 18, 3)$-código binario en el espacio proyectivo.

El siguiente teorema muestra que C es un código óptimo.

3.2.8 Teorema. $A_2(5,3) = 18$.

Demostración. Sea C un $(5, M, 3)$-código en el espacio proyectivo sobre $\mathbb{F}_2$ con la distribución de dimensión $D_0, D_1, \ldots, D_5$. Del lema 3.2.6 se sigue que $D_2 \leq 9$ y que $D_4 \leq 1$. Por lo tanto $D_2 + D_4 \leq 10$. Demostramos a continuación que, de hecho, $D_2 + D_4 \leq 9$.

Supongamos por el contrario que $C \cap G_2(5,4) = \{X\}$ y que

$$C_2 := C \cap G_2(5,2) = \{V_1, V_2, \ldots, V_9\}.$$

Sea $U = V_1 \cup V_2 \cup V_9$. Puesto que la distancia mínima de C_2 es 4, se tiene que $V_i \cap V_j = \{0\}$ para todo $V_i, V_j \in C_2$. Por lo tanto $|U| = 2^5 - 1 = \sum_{i=1}^{9}(2^{n_i} - 1)$, es decir, $|U| = 1 + 9 \cdot 3 = 28$.

Ahora, contemos el número de vectores que hay en $U \cap X$. Dado que la distancia mínima de C es 3, se tiene que $\dim(V_i \cap X) = 1$ para todo $V_i \in C_2$. En efecto, si $V_i \subseteq X$, entonces $\dim(X + V_i) = n - 1$; además, como

$$\begin{aligned} \dim(X + V_i) + \dim(X \cap V_i) &= \dim X + \dim V_i \text{ y} \\ d(X, V_i) &= \dim X + \dim V_i - 2\dim(X \cap V_i), \end{aligned}$$

entonces $3 + 2\dim(X \cap V_i) = \dim X + \dim V_i$.

Luego,

$$\begin{aligned} 3 + 2\dim(X \cap V_i) &= \dim(X + V_i) + \dim(X \cap V_i) \\ \dim(X \cap V_i) &= 4 - 3 = 1. \end{aligned}$$

Además, como

$$U \cap X = \bigcup_{i=1}^{9}(X \cap V_i) \text{ y } n_i' := \dim(X \cap V_i) = 1,$$

se tiene que

$$|U \cap X| = 2^5 - 1 = \sum_{i=1}^{9}(2^{n_i'} - 1)$$

así, $|U \cap X| = 1 + 9 = 10$.

Por lo tanto, existen 18 vectores diferentes en U que no están en X, lo cual es una contradicción pues $|\mathbb{F}_2^5 \setminus X| = 16$.

Por otro lado, el hecho de que $D_2 + D_4 \leq 9$ en relación con el lema 3.2.4 implica que $D_3 + D_1 \leq 9$. Así por el teorema 2.3.21, la adición de estas dos restricciones resulta que $A_2(5,3) \leq 18$. □

3.3 Códigos cíclicos en el espacio proyectivo

3.3.1 Definición. Sea α un elemento primitivo de $\mathbb{F}_{2^n}$. Decimos que un código $C \subseteq \mathbb{P}_2(n)$ es cíclico, si y sólo si, si $\{0, \alpha^{i_1}, \alpha^{i_2}, \ldots, \alpha^{i_m}\} \in C$, entonces $\{0, \alpha^{i_1+1}, \alpha^{i_2+1}, \ldots, \alpha^{i_m+1}\} \in C$. En otras palabras, si enviamos cada espacio vectorial $V \in C$ a el correspondiente vector característico binario $x_V = (x_0, x_1, \ldots, x_{2^n-2})$ dado por

$$x_i = 1 \text{ si } \alpha^i \in V \quad \text{y} \quad x_i = 0 \text{ si } \alpha^i \notin V,$$

entonces el conjunto de todos los vectores característicos es cerrado bajo traslaciones cíclicas.

Note que la propiedad de ser cíclico, no depende de la elección de un elemento primitivo α en $\mathbb{F}_{2^n}$.

3.3.2 Ejemplos. Algunos códigos cíclicos.

(a) Códigos cíclicos en $\mathbb{F}_{2^4}$ de dimensión 2.

Para la construcción de nuestro código cíclico, consideramos el espacio vectorial $V := \mathbb{F}_{2^4}$, una extensión finita del cuerpo $\mathbb{F}_2$ definido por

$$\begin{aligned}\mathbb{F}_{2^4} &= \mathbb{F}_2[x]/\langle x^4 + x + 1\rangle \\ &= \{0, 1, x, x^2, x^3, x+1, x^2+1, x^2+x, x^2+x+1, x^3+1, x^3+x, \\ &\quad x^3+x+1, x^3+x^2, x^3+x^2+1, x^3+x^2+x, x^3+x^2+x+1\},\end{aligned}$$

donde α es la raíz del polinomio irreducible $x^4 + x + 1$.

En notación vectorial, tenemos:

$$\begin{aligned}\mathbb{F}_{2^4} = \{&(0,0,0,0), (0,0,0,1), (0,0,1,0), (0,0,1,1), (0,1,0,0), \\ &(0,1,0,1), (0,1,1,0), (0,1,1,1), (1,0,0,0), (1,0,0,1), (1,0,1,0), \\ &(1,0,1,1), (1,1,0,0), (1,1,0,1), (1,1,1,0), (1,1,1,1)\}.\end{aligned}$$

Dado que existen 35 subespacios de V de dimensión 2, usamos GAP para obtenerlos y los listamos a continuación:

$$\begin{aligned}V_1 &= \{0, \alpha^0, \alpha^1, \alpha^4\} \\ V_2 &= \{0, \alpha^0, \alpha^2, \alpha^8\} \\ V_3 &= \{0, \alpha^0, \alpha^5, \alpha^{10}\} \\ V_4 &= \{0, \alpha^0, \alpha^3, \alpha^{14}\} \\ V_5 &= \{0, \alpha^0, \alpha^7, \alpha^9\}\end{aligned}$$

$$
\begin{aligned}
V_6 &= \{0, \alpha^0, \alpha^6, \alpha^{13}\} \\
V_7 &= \{0, \alpha^0, \alpha^{11}, \alpha^{12}\} \\
V_8 &= \{0, \alpha^1, \alpha^2, \alpha^5\} \\
V_9 &= \{0, \alpha^1, \alpha^8, \alpha^{10}\} \\
V_{10} &= \{0, \alpha^1, \alpha^3, \alpha^9\} \\
V_{11} &= \{0, \alpha^1, \alpha^7, \alpha^{14}\} \\
V_{12} &= \{0, \alpha^1, \alpha^6, \alpha^{11}\} \\
V_{13} &= \{0, \alpha^1, \alpha^{12}, \alpha^{13}\} \\
V_{14} &= \{0, \alpha^2, \alpha^4, \alpha^{10}\} \\
V_{15} &= \{0, \alpha^4, \alpha^5, \alpha^8\} \\
V_{16} &= \{0, \alpha^3, \alpha^4, \alpha^7\} \\
V_{17} &= \{0, \alpha^4, \alpha^9, \alpha^{14}\} \\
V_{18} &= \{0, \alpha^4, \alpha^6, \alpha^{12}\} \\
V_{19} &= \{0, \alpha^4, \alpha^{11}, \alpha^{13}\} \\
V_{20} &= \{0, \alpha^2, \alpha^3, \alpha^6\} \\
V_{21} &= \{0, \alpha^2, \alpha^{13}, \alpha^{14}\} \\
V_{22} &= \{0, \alpha^2, \alpha^9, \alpha^{11}\} \\
V_{23} &= \{0, \alpha^2, \alpha^7, \alpha^{12}\} \\
V_{24} &= \{0, \alpha^3, \alpha^8, \alpha^{13}\} \\
V_{25} &= \{0, \alpha^6, \alpha^8, \alpha^{14}\} \\
V_{26} &= \{0, \alpha^8, \alpha^9, \alpha^{12}\} \\
V_{27} &= \{0, \alpha^7, \alpha^8, \alpha^{11}\} \\
V_{28} &= \{0, \alpha^3, \alpha^5, \alpha^{11}\} \\
V_{29} &= \{0, \alpha^5, \alpha^{12}, \alpha^{14}\} \\
V_{30} &= \{0, \alpha^5, \alpha^6, \alpha^9\} \\
V_{31} &= \{0, \alpha^5, \alpha^7, \alpha^{13}\} \\
V_{32} &= \{0, \alpha^3, \alpha^{10}, \alpha^{12}\} \\
V_{33} &= \{0, \alpha^{10}, \alpha^{11}, \alpha^{14}\} \\
V_{34} &= \{0, \alpha^9, \alpha^{10}, \alpha^{13}\} \\
V_{35} &= \{0, \alpha^6, \alpha^7, \alpha^{10}\}.
\end{aligned}
$$

Sea $C \subset G_2(4,2)$ definido por $C := \{V_3, V_{12}, V_{17}, V_{23}, V_{24}\}$, se verifica que C es un $(4,5,4,2)$-código cíclico. En efecto: por (3.1) se tiene que $A_2(4,4,2) = 5$, además $d(V_i, V_j) = 2 + 2 - 2(0) = 4$, para todo $i \neq j$ en el conjunto de índices $\{3, 12, 17, 23, 24\}$.

Por otra parte, si a cada $V \in C$ le asignamos su vector característico binario, obtenemos

$$\begin{aligned}
x_{V_3} &= (1,0,0,0,0,1,0,0,0,0,1,0,0,0,0)\\
x_{V_{12}} &= (0,1,0,0,0,0,1,0,0,0,0,1,0,0,0)\\
x_{V_{23}} &= (0,0,1,0,0,0,0,1,0,0,0,0,1,0,0)\\
x_{V_{24}} &= (0,0,0,1,0,0,0,0,1,0,0,0,0,1,0)\\
x_{V_{17}} &= (0,0,0,0,1,0,0,0,0,1,0,0,0,0,1).
\end{aligned}$$

El conjunto formado por los x_V es cerrado bajo traslaciones cíclicas.

En $G_2(4,2)$ encontramos otro código cíclico C' cuya distancia mínima es diferente de $2k$:

$$C' := \{V_1, V_4, V_7, V_8, V_{13}, V_{15}, V_{16}, V_{20}, V_{21}, V_{26}, V_{27}, V_{30}, V_{33}, V_{34}, V_{35}\}$$

Se verifica que C' es un $(4, 15, 2, 2)$-código, por lo tanto $A_2(4,2,2) \geq 15$. Luego por el teorema 2.3.14 se tiene que $A_2(4,2,2) \leq 35$.

(b) Códigos cíclicos en $\mathbb{F}_{2^4}$ de dimensión 3.

Sabemos que existen 15 subespacios de V de dimensión 3:

$$\begin{aligned}
V_1 &= \{0, \alpha^0, \alpha^1, \alpha^2, \alpha^4, \alpha^5, \alpha^8, \alpha^{10}\}\\
V_2 &= \{0, \alpha^0, \alpha^1, \alpha^3, \alpha^4, \alpha^7, \alpha^9, \alpha^{14}\}\\
V_3 &= \{0, \alpha^0, \alpha^1, \alpha^4, \alpha^6, \alpha^{11}, \alpha^{12}, \alpha^{13}\}\\
V_4 &= \{0, \alpha^0, \alpha^2, \alpha^3, \alpha^6, \alpha^8, \alpha^{13}, \alpha^{14}\}\\
V_5 &= \{0, \alpha^0, \alpha^2, \alpha^7, \alpha^8, \alpha^9, \alpha^{11}, \alpha^{12}\}\\
V_6 &= \{0, \alpha^0, \alpha^3, \alpha^5, \alpha^{10}, \alpha^{11}, \alpha^{12}, \alpha^{14}\}\\
V_7 &= \{0, \alpha^0, \alpha^5, \alpha^6, \alpha^7, \alpha^9, \alpha^{10}, \alpha^{13}\}\\
V_8 &= \{0, \alpha^1, \alpha^2, \alpha^3, \alpha^5, \alpha^6, \alpha^9, \alpha^{11}\}\\
V_9 &= \{0, \alpha^1, \alpha^2, \alpha^5, \alpha^7, \alpha^{12}, \alpha^{13}, \alpha^{14}\}\\
V_{10} &= \{0, \alpha^1, \alpha^3, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{12}, \alpha^{13}\}
\end{aligned}$$

$$V_{11} = \{0, \alpha^1, \alpha^6, \alpha^7, \alpha^8, \alpha^{10}, \alpha^{11}, \alpha^{14}\}$$
$$V_{12} = \{0, \alpha^2, \alpha^3, \alpha^4, \alpha^6, \alpha^7, \alpha^{10}, \alpha^{12}\}$$
$$V_{13} = \{0, \alpha^2, \alpha^4, \alpha^9, \alpha^{10}, \alpha^{11}, \alpha^{13}, \alpha^{14}\}$$
$$V_{14} = \{0, \alpha^3, \alpha^4, \alpha^5, \alpha^7, \alpha^8, \alpha^{11}, \alpha^{13}\}$$
$$V_{15} = \{0, \alpha^4, \alpha^5, \alpha^6, \alpha^8, \alpha^9, \alpha^{12}, \alpha^{14}\}.$$

Sea $C \subseteq G_2(4,3)$ definido por $C := \{V_1, \ldots, V_{15}\}$, se verifica que C es un $(4, 15, 2, 3)$-código cíclico. En efecto: por el teorema 2.3.12 se tiene que $A_2(4,2,3) \leq 15$, además $d(V_i, V_j) = 3 + 3 - 2(2) = 2$, para todo $i \neq j$ en el conjunto de índices $\{1, \ldots, 15\}$

(c) Sea α la raíz del polinomio irreducible $x^6 + x + 1$, usemos este polinomio para generar el cuerpo $\mathbb{F}_{2^6}$. Consideremos el código C en $G_2(6,3)$ que consiste en todas las traslaciones cíclicas de

$$\{\alpha^0, \alpha^1, \alpha^4, \alpha^6, \alpha^{16}, \alpha^{24}, \alpha^{33}\}.$$

Note que aquí, y en lo que sigue, omitimos el vector nulo para especificar codewords de los códigos cíclicos en el espacio proyectivo.

Se puede verificar que C es un $(6, 63, 4, 3)$-código. por lo tanto $A_2(6,4,3) \geq 63$. Por otra parte, del lema 3.2.6 y los teoremas 2.3.11 y 2.3.12 se tiene que $A_2(6,4,3) \leq 81$.

(d) Sea α la raíz del polinomio irreducible $x^8 + x^7 + x^2 + x + 1$, usemos este polinomio para generar el cuerpo $\mathbb{F}_{2^8}$. Consideremos el código C en $G_2(8,3)$ que consiste en todas las traslaciones cíclicas de

$$\{\alpha^0, \alpha^1, \alpha^{18}, \alpha^{33}, \alpha^{69}, \alpha^{99}, \alpha^{109}\}$$
$$\{\alpha^0, \alpha^2, \alpha^{58}, \alpha^{135}, \alpha^{163}, \alpha^{198}, \alpha^{246}\}$$
$$\{\alpha^0, \alpha^3, \alpha^{22}, \alpha^{82}, \alpha^{134}, \alpha^{205}, \alpha^{250}\}$$
$$\{\alpha^0, \alpha^4, \alpha^{24}, \alpha^{97}, \alpha^{104}, \alpha^{110}, \alpha^{141}\}$$
$$\{\alpha^0, \alpha^{12}, \alpha^{41}, \alpha^{55}, \alpha^{102}, \alpha^{125}, \alpha^{221}\}$$

Se puede verificar que C es un $(8, 1275, 4, 3)$-código; por lo tanto $A_2(8,4,3) \geq 1275$. Por otra parte, del lema 3.2.6 y el teorema 2.3.11 se tiene que $A_2(8,4,3) \leq 1493$.

(*e*) Sea α la raíz del polinomio irreducible $x^9 + x^4 + 1$, usemos este polinomio para generar el cuerpo $\mathbb{F}_{2^9}$. Consideremos el código C en $G_2(9, 3)$ que consiste en todas las traslaciones cíclicas de

$$\{\alpha^0, \alpha^1, \alpha^{27}, \alpha^{130}, \alpha^{142}, \alpha^{185}, \alpha^{277}\}$$
$$\{\alpha^0, \alpha^2, \alpha^{207}, \alpha^{228}, \alpha^{260}, \alpha^{300}, \alpha^{432}\}$$
$$\{\alpha^0, \alpha^3, \alpha^{99}, \alpha^{157}, \alpha^{220}, \alpha^{244}, \alpha^{420}\}$$
$$\{\alpha^0, \alpha^4, \alpha^9, \alpha^{51}, \alpha^{110}, \alpha^{305}, \alpha^{454}\}$$
$$\{\alpha^0, \alpha^6, \alpha^{60}, \alpha^{131}, \alpha^{290}, \alpha^{329}, \alpha^{504}\}$$
$$\{\alpha^0, \alpha^8, \alpha^{18}, \alpha^{170}, \alpha^{187}, \alpha^{255}, \alpha^{320}\}$$
$$\{\alpha^0, \alpha^{11}, \alpha^{139}, \alpha^{177}, \alpha^{299}, \alpha^{333}, \alpha^{470}\}$$
$$\{\alpha^0, \alpha^{14}, \alpha^{98}, \alpha^{114}, \alpha^{134}, \alpha^{216}, \alpha^{238}\}$$
$$\{\alpha^0, \alpha^{15}, \alpha^{48}, \alpha^{77}, \alpha^{126}, \alpha^{196}, \alpha^{476}\}$$
$$\{\alpha^0, \alpha^{19}, \alpha^{155}, \alpha^{192}, \alpha^{278}, \alpha^{308}, \alpha^{421}\}$$
$$\{\alpha^0, \alpha^{23}, \alpha^{69}, \alpha^{97}, \alpha^{186}, \alpha^{262}, \alpha^{337}\}$$
$$\{\alpha^0, \alpha^{73}, \alpha^{146}, \alpha^{219}, \alpha^{292}, \alpha^{365}, \alpha^{438}\}$$

Se puede verificar que C es un $(9, 5694, 4, 3)$-código; por lo tanto $A_2(9, 4, 3) \geq 5694$. Por otra parte, $A_2(8, 4, 3) \leq 6205$ por el teorema 2.3.9.

3.4 Inexistencia de códigos perfectos no triviales

El estudio de códigos perfectos es uno de los temas más fascinantes de la investigación en la teoria de códigos.

Dado un espacio métrico S, un código $C \subseteq S$, se dice que es e-perfecto si las esferas de radio e centradas en los codewords de C cubren a S; en otras palabras, cada elemento de S está contenido en una y sólo una de estas esferas. Un espacio métrico finito S siempre admite dos códigos triviales perfectos: todo el espacio es 0-perfecto y cualquier elemento $x \in S$ es n-perfecto, donde $n = \max_{y \in S} d(x, y)$.

El espacio binario de Hamming, el espacio de Johnson $J(2n, n)$, y el espacio proyectivo $\mathbb{P}_q(n)$, pero no la Grassmannian, admiten un tercer código perfecto trivial cuando $n = 2e + 1$. En el caso de $\mathbb{P}_q(n)$, este consiste en el espacio nulo $\{0\}$ y $\mathbb{F}_q^n$.

Es conocido en [3] y [12] que para todo q, n, k no hay códigos perfectos no triviales en $G_q(n, k)$. Pero esto no excluye códigos perfectos en $\mathbb{P}_q(n)$; al igual

que la no existencia de códigos perfectos no triviales en el espacio de Johnson no descarta códigos perfectos no triviales en el espacio de Hamming. Nuestro principal resultado de esta sección es una prueba propia de la no existencia existencia de códigos perfectos no triviales en $\mathbb{P}_q(n)$.

3.4.1 Teorema. Para todo q y n, no existen códigos perfectos no triviales en el espacio proyectivo $\mathbb{P}_q(n)$

Demostración. Supongamos lo contrario, que C es un código e-perfecto en $\mathbb{P}_q(n)$. Sea $d = 2e+1$ y definamos $C_k := C \cap G_q(n,k)$ para todo $k = 0, 1, \ldots, n$. Distinguimos dos casos.

Caso 1. $\{0\} \in C$

Aquí se tiene que $C_1 = C_2 = \cdots = C_{2e} = \emptyset$, y todos los puntos en $G_q(n, e+1)$ deben ser cubiertos por los codewords de C_d. En efecto, en $G_q(n,k)$ no existen códigos perfectos no triviales, por tanto $k = 1, 2, \ldots, n-1$. Además dado que $\mathbb{P}_q(n)$ admite un tercer código perfecto trivial cuando $n = 2e+1$ donde $n = \max\limits_{x,y \in \mathbb{P}_q(n)} d(x,y)$, entonces $k = 1, 2, \ldots, 2e$. Esto implica que C_d es una estructura de Steiner $S_q(e+1, d, n)$ y por lo tanto $|C_d| = \begin{bmatrix} n \\ e+1 \end{bmatrix} / \begin{bmatrix} d \\ e+1 \end{bmatrix}$.

Cada subespacio de C_d cubre $\begin{bmatrix} d \\ e+2 \end{bmatrix}$ puntos en $G_q(n, e+2)$.

Esto deja $\begin{bmatrix} n \\ e+2 \end{bmatrix} - |C| \begin{bmatrix} d \\ e+2 \end{bmatrix}$ puntos descubiertos en $G_q(n, e+2)$ y cada uno de ellos debe estar cubierto por un codeword de C_{d+1}. Además, cada codeword de C_{d+1} cubre exactamente $\begin{bmatrix} d+1 \\ e+2 \end{bmatrix}$ puntos en $G_q(n, e+2)$.

Por lo tanto:

$$|C_{d+1}| = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-e}-1)}{(q^{d+1}-1)(q^d-1)\cdots(q^{e+1}-1)}(q^{n-e-1}-q^e)$$

Ahora observe que $A_q(n, d+1, d+1) \geq |C_{d+1}|$ (Teorema 2.3.10). A partir de esto y aplicando el teorema 2.3.11 de manera iterativa $(e+1)$-veces, obtenemos que

$$A_q(m, 2k, k) \geq \frac{q^m - q^{k-1}}{q^k - 1} \tag{3.11}$$

donde $m = n-(e+1)$ y $k = e+1$. Por otra parte, el hecho de que C_d sea una estructura de Steiner $S_q(e+1, d, n)$ implica que $e+1$ divida a $n-e = m+1$. Esto implica que

$$\frac{q^m - q^{k-1}}{q^k - 1} = q^{m-k} + q^{m-2k} + \cdots + q^{k-1} = \left\lfloor \frac{q^m - 1}{q^k - 1} \right\rfloor.$$

También, puesto que $k = e+1$ divide a $m+1$, no puede dividir a m, lo cual establece una contradicción entre (3.11) y el lema 3.2.6.

Caso 2. $\{0\} \notin C$

Nuestra prueba para este caso se basa en la construcción de una partición de $\mathbb{F}_q^n$, y luego aplicamos un argumento de conteo a esta partición para llegar a una contradicción. Para el argumento de conteo, vamos a introducir una función η de subconjuntos de $\mathbb{F}_q^n$, definidos como sigue: dado un $S \subseteq \mathbb{F}_q^n$, sea $\eta(S)$ el número de vectores $(x_1, x_2, \ldots, x_n)$ en S tales que $x_1 = 1$. Note que si S es un espacio vectorial de dimensión i y $\eta(S) \neq 0$, entonces $\eta(S) = q^{i-1}$. Ahora, sea $X \in C$ un espacio vectorial cuya dimensión es la más pequeña entre todos los espacios vectoriales en C. Dado que $X \neq \{0\}$, podemos suponer sin perdida de generalidad que $\eta(X) \neq 0$.

La partición de $\mathbb{F}_q^n$ es construida como sigue.

Sea $k = \dim X$. Dado que X debe cubrir el espacio nulo, se tiene que $k \leq e$. Es facil ver que un espacio vectorial V en $\mathbb{P}_q(n)$ que cumpla con la siguiente condición, siempre existe:

$$\dim V = e - k,\ X \cap V = \{0\},\ \eta(V) = 0 \tag{3.12}$$

Definamos ahora $W = X \bigoplus V$. En vista de (3.12), se tiene que $\dim W = e$ y $\eta(X) \neq 0$ lo cual implica que $\eta(W) = q^{e-1}$.

Finalmente, definamos un subcódigo C' de C como sigue:

$$C' := \{Y \in C : V \subset Y \text{ y } \dim Y = d - k\} \tag{3.13}$$

Supongamos que C' contiene M codewords $Y_1, Y_2, \ldots, Y_M$ (donde $M = q^k \frac{q^{n-e}-1}{q^{e+1}-1}$ lo cual no se requiere para la prueba).

Para todo $i = 1, 2, \ldots, M$, sea $Y_i^* = Y_i \setminus V$. La partición de $\mathbb{F}_q^n$ que se tiene en mente es la siguiente:

$$\mathbb{F}_q^n = Y_1^* \cup Y_2^* \cup \cdots \cup Y_M^* \cup W \tag{3.14}$$

Supongamos que (3.14) es, en efecto, una partición de $\mathbb{F}_q^n$, podemos llegar facilmente a una contradicción. Dado que $\dim Y_i^* = d - k$ y $\eta(V) = 0$, encontramos que $\eta(Y_i^*) = \eta(Y_i)$ es o bien cero o bien $q^{d-k-1} = q^{2e-k}$ para todo i. Además $\eta(F_q^n) = q^{n-1}$ y por lo tanto

$$\eta(W) = \eta(\mathbb{F}_q^n) - \sum_{i=1}^{M} \eta(Y_i^*) \tag{3.15}$$

debe ser divisible por q^{2e-k}. Esto es una contradicción, ya que hemos demostrado que $\eta(W) = q^{e-1}$, pero $e - 1 < 2e - k$ para todo $k \leq e$.

Para completar la prueba, queda por establecer (3.14).

Afirmación 1.

Sea u un vector de $\mathbb{F}_q^n$ que está por fuera de W. Entonces existe $Y_i \in C'$ tal que $u \in Y_i$

Demostración. Sea $U = V \bigoplus \{0, u\}$. Entonces U es un espacio vectorial de dimensión $e-k+1$ que debe ser cubierto por algún codeword Y de C. Este codeword no es X dado que $X \cap Y = \{0\}$, y entonces

$$d(X, U) = \dim X + \dim U = k + (e - k + 1) = e + 1.$$

Dado que X y Y son codeword diferentes de C, se tiene que $d(X, Y) \geq d$ lo cual implica que $\dim Y \geq d - k$. Ahora, por el hecho de que Y cubre a U, se tiene que

$$d(U, Y) = \dim U + \dim Y - 2\dim(U \cap Y) \leq e. \tag{3.16}$$

Por otro lado, dado que $\dim Y \geq d - k$, la única forma en la que se puede cumplir (3.16) es cuando $\dim Y = d - k$ y

$$\dim(U \cap Y) = \dim U = e - k + 1. \tag{3.17}$$

Pero (3.17) implica que $V \subset U \subset Y$ y por lo tanto $Y \in C'$. Finalmente $U \subset Y$ también implica que $u \in Y$. ◄

Si u está por fuera de $W = X \bigoplus V$ y $u \in Y_i$, entonces claramente u debe pertenecer a $Y_i^* \setminus V$. Por lo tanto, la afirmación 1 muestra que la unión de los conjuntos $Y_1^* \cup Y_2^* \cup \cdots \cup Y_M^* \cup W$ contiene efectivamente todo $\mathbb{F}_q^n$.

Afirmación 2.

Los conjuntos $Y_1^*, Y_2^*, \cdots, Y_M^*$ y W son disyuntos.

Demostración. Dados dos codewords cualesquiera de Y_i y Y_j de C', se tiene que

$$d(Y_i, Y_j) = 2(d - k) - 2\dim(Y_i \cap Y_j) \geq d.$$

Esto implica que $\dim(Y_i \cap Y_j) \leq e - k = \dim V$ y por lo tanto $Y_i \cap Y_j = V$. En consecuencia los conjuntos $Y_1^*, Y_2^*, \cdots, Y_M^*$ son disyuntos.

Ahora supongamos lo contrario, que existe un vector no nulo y en la intersección $Y_i \cap W$ para algún i. Luego $y \in Y_i^*$ y $y = x + v$ para algún $0 \neq x \in X$ y algún $v \in V$. Pero Y_i es un espacio vectorial que contiene a V como subespacio. Por lo tanto Y_i también contiene al vector $y - v = x$ con $\dim(X \cap Y_i) \geq 1$. Pero esto se contradice claramente con la distancia mínima de C, dado que $d(X, Y_i) = k + (d - k) - 2\dim(X \cap Y_i) \leq d - 2$. ◄

La afirmación 2 completa la prueba que (3.14) es, en efecto, una partición de $\mathbb{F}_q^n$. Esto a su vez completa la prueba de nuestro teorema.□

Bibliografía & Referencias

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

[2] Tor Bu, *Partitions of a vector space*, Discrete Math., Vol. 31, pp 79-83, Jan. 1980.

[3] L. Chihara*On the zeros of the Askey-Wilson polynomials, whit applications to coding theory*, SIAM J. Math. Anal., vol.18, pp. 191-207, 1987.

[4] Ph. Delsarte, *An algebraic approach to association schemes of coding theory*, Philips J. Res., vol. 10, pp. 1-97, 1973.

[5] T. Etzion and A. Vardy, *Error-Correcting Codes in Projective Space*, IEEE Trans. Inf. Theory, vol. 57, No. 2, 2011.

[6] T. Etzion, *Perfect byte-correcting codes*, IEEE Trans. Inf. Theory, vol. 44, no. 7, pp. 3140-3146, Nov. 1998. in the encyclopedia of mathematics, G.-C. Rota, Ed. Reading, MA: Addison-Wesley, 1983, vol 20.

[7] P. Frankl and R. M. Wilson, *The Erdös-Ko-Rado theorem for vector space*, J. Combin. Theory, Series A, Vol. 43, pp. 228-236, 1986.

[8] I. Gutiérrez. *Códigos de red, Notas de clase*, 2012.

[9] R. Koetter, F. R. Kschischang. *Error correcting in random Network Coding*, presented at the 2nd Annual Workshop on Information Theory and Applications, La Jolla, CA, Jan. 2007

[10] R. Koetter, F. R. Kschischang. *Coding for Errors and Erasures in Random Network Coding,* IEEE Transactions on Information Theory, Vol 54, No 8 pp 3579 - 3591 2008.

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

[12] W. J. Martin and X. J. Zhu, *Anticodes for the Grassmann and bilinear forms graph*, Designs, Codes, Crypto., vol. 6, pp. 73-79, 1995. Curvas y códigos algebraicos, Universidad de Sevilla 2009.

[13] M. Schwartz and T. Etzion, *Codes and anticodes in the Grassmann graph*, J. Combin. Theory, ser. A, vol. 97, pp. 27-42, 2002.

[14] Ludo M. G. M. Tolhuizen, *The Generalized Gilbert Varshamov Bound is Implied by Turan's Theorem*, IEEE Trans. Inf. Theory, vol. 43, No. 6,pp. 1605-1606, sep. 1997.

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

[16] A. Vardy and Y. Be'ery , *Maximun-likelihood soft decision decoding of BCH codes* , IEEE Trans. Inf. Theory, vol. 40, no. 2, pp. 546-554, Mar. 1994.

[17] S. T. Xia and F. W. Fu, *Johnson type bounds on constant dimensión codes*, Designs, Codes, Crypto., vol. 50, pp. 163-172, Feb. 2009.