Constructions of Cyclic and Quasi-Cyclic Grassmannian Codes

I. Gutierrez-Garcia, and I. Molina-Naizir

***Abstract*—Linear random network coding is a newly created powerful scheme for information transmission in a network, which allows almost optimal performance. It has opened a significant research area not only in information technology, but also in discrete mathematics with widespread applications for communication networks like the Internet, wireless communication systems, and cloud computing. The construction of good network codes in some projective space is of highly mathematical nature and requires strong computational power for the resulting searches. In this paper was construct, using GAP System for Computational Discrete Algebra and Wolfram Mathematica, some cyclic Grassmannian codes, specially an optimal code over the finite field $\mathbb{F}_{2^{10}}$. Also, it has been introduced the q-analogous of the classic quasi-cyclic block codes over finite fields, namely, the m-quasi-cyclic Grassmannian codes. Further, it was classified all the full length and degenerated orbits and quasi-orbits in the projective space $\mathbb{P}_q(n)$, for n up to 11.**

***Index Terms*—Finite fields, Grassmannian codes, orbits, quasi-orbits, cyclic and quasi-cyclic Grassmannian codes.**

I. Introducción

La entrega de datos en una red convencional de comunicación, como Internet, se realiza mediante el enrutamiento multidifusión. Es decir, la transmisión de datos se hace desde un nodo fuente emisor hacia un conjunto de nodos sumideros o receptores. Este tipo de redes en el proceso de enrutamiento pueden repetir paquetes por algunos enlaces y también crean colas de espera en las interfaces de salida hacia los nodos destinos. Es decir, los nodos que conforman la red trabajan con la política de almacenamiento y reenvío, de tal modo que los paquetes deben reenviarse, en el mejor de los casos, en el orden en que ingresan al nodo enrutador, esto sin duda origina retardo y por ende menor eficiencia en la transmisión.

Como respuesta a este deficiencia se introduce el año 2000 un esquema potente para la transmisión de información en una red multidifusión, denominado codificación aleatoria en red, (en ingles Random Network Coding), que permite un rendimiento casi óptimo, ya que los nodos intermedios de la red tienen la opción de mezclar la información entrante antes de transmitirla. Esto es, se lleva a cabo una combinación lineal de los paquetes que ingresan, produciendo un paquete de salida codificado de igual tamaño que los entrantes, aumentando el uso del ancho de banda por la no espera en los buffers de las interfaces de salida. Esto redunda, sin dudas, en una tasa de flujo de información superior, [1], [4], [13], [14].

I. Gutierrez-García is with the Department of Mathematics nas Statistics, Universidad del Norte, Barranquilla - Colombia, Km 5 via a Puerto Colombia, e-mail: isgutier@uninorte.edu.co.

I. Molina-Naizir is with the Department of Mathematics nas Statistics, Universidad del Norte, Barranquilla - Colombia, Km 5 via a Puerto Colombia, e-mail: inaizir@uninorte.edu.co.

La codificación aleatoria en red se ha convertido desde entonces en un área de investigación importante en matemáticas discretas y en tecnologías de la información, la cual tiene potenciales aplicaciones prácticas en sistemas de redes, tales como redes de distribución de contenido peer-to-peer, el tráfico bidireccional en una red inalámbrica, redes inalámbricas residenciales, redes de sensores Ad-hoc y la computación en la nube, entre otros, [4], [7], [11], [13], [14], [16], [19], [20].

Para entender la esencia y la formalidad matemática de la codificación aleatoria en red iniciamos fijando el espacio vectorial $\mathbb{F}_q^n$, de dimensión n sobre el cuerpo finito con q elementos $\mathbb{F}_q$, (donde q es potencia de un número primo), el cual llamamos espacio ambiente.

Para la comunicación entre el transmisor y los sumideros se produce en una serie de rondas o generaciones; durante cada generación, el transmisor inyecta un número de paquetes de longitud fija n en la red, cada uno de los cuales puede ser visto formalmente como un elemento de $\mathbb{F}_q^n$. Siempre que un nodo intermedio tiene la oportunidad de enviar un paquete, crea aleatoriamente una combinación lineal, sobre $\mathbb{F}_q$, de los paquetes que tiene disponible y transmite esta combinación lineal aleatoria. Finalmente, los receptores reciben tales paquetes generados aleatoriamente y trata de inferir el conjunto de paquetes inyectados en la red.

Para definir los códigos en este universo consideramos el espacio proyectivo de orden n, notado con $\mathbb{P}_q(n)$. Esto es, el conjunto de todos los subespacios vectoriales de $\mathbb{F}_q^n$, incluidos los triviales. Cualquier subconjunto $\mathscr{C}$ de $\mathbb{P}_q(n)$ es denominado un código de subespacios, o simplemente un código. Los elementos de $\mathscr{C}$ son llamados palabras de códigos (en inglés codewords). Un caso particular y de central importancia en este trabajo se tiene cuando la dimensión de cada palabra de código es constante. En esta situación $\mathscr{C}$ es denominado un código de dimensión constante o un código Grassmanniano. Para un número natural k con $0 \leq k \leq n$ se denota con $G_q(n,k)$ al conjunto de todos los subespacios de $\mathbb{F}_q^n$ que tiene dimensión k y lo llamamos la k-Grassmanniana. El número de elementos en una k-Grassmaniana está dada por el q-ésimo coeficiente de Gauus $\begin{bmatrix} n \\ k \end{bmatrix}_q$. Es conocido que

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}. \qquad \text{(I.1)}$$

Similar como en la teoría clásica de códigos, existen dos direcciones principales para la investigación en la codificación aleatoria en red:

(1) La existencia y construcción de códigos de subespacios con buenos parámetros,
(2) Esquemas eficientes de codificación y decodificación para un código de subespacios dado.

Desde el punto de vista matemático y de la ciencias de la computación se han considerado cinco grandes subtemas para investigación:

(a) Construcción de los códigos de subespacios y códigos Grassmannianos,
(b) Determinación de cotas para el tamaño de códigos en términos de n, k y q,
(c) Aspectos prácticos de la codificación aleatoria en red,
(d) Criptografía fundamentada en códigos de subespacios,
(e) Métodos algebraicos en la codificación aleatoria en red.

Algunos trabajos relevantes desarrollados en esta dirección pueden consultarse en [6], [5], [2], [21], [15], [18], [3], [10].

En este trabajo nos concentramos en un caso particular de (a). Abordaremos la construcción de una clase especial de códigos Grassmannianos, los cíclicos y los cuasi-cíclicos.

II. Los Parámetros de un Código de Subespacios

Como es natural en este tipo de procesos de propagación de información en una red, es posible que se generen errores en la transmisión de paquetes, causados por ruido o interferencia intencional en los nodos intermedios (NI). Supongamos que se tiene un código de red $\mathscr{C}$ y que una generación de paquetes es inyectada en la red y que este conjunto de vectores es modelado por un subespacio $V \in \mathscr{C}$. Supongamos además que se recibe un subespacio $U \in \mathbb{P}_q(n)$ no necesariamente igual a V. Una ilustración se presenta en la siguiente figura.

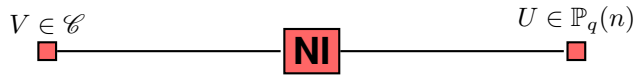

Fig. 1. Transmisión de un palabra de código V.

Esto trae como consecuencia la necesidad de introducir una medida del grado de discrepancia entre el espacio transmitido, digamos V y el recibido U. Como en la teoría clásica, se define una distancia d de la siguiente manera:

$$d(V,U) = \dim(U+V) - \dim(U \cap V). \qquad \text{(II.1)}$$

Note que

$$d(U,V) = \dim(U) + \dim(V) - 2\dim(U \cap V). \qquad \text{(II.2)}$$

R. Koetter y F. Kschischang demostraron en [16], que d define una métrica sobre $\mathbb{P}_q(n)$. Esta distancia d se denomina distancia de subespacios. La distancia mínima $d(\mathscr{C})$ del código $\mathscr{C}$ se define como es usual; es decir, como la menor distancia de subespacios entre dos elementos diferentes de $\mathscr{C}$.

Si $\mathscr{C}$ es un código de subespacios con distancia mínima d, entonces decimos que $\mathscr{C}$ es un $[n, |\mathscr{C}|, d]$-código sobre $\mathbb{F}_q$ y $[n, |\mathscr{C}|, d]$ son sus parámetros. Si comparamos con la teoría clásica de códigos, los códigos Grassmannianos corresponden a los de peso constante. Si $\mathscr{C}$ es un código Grassmanniano, digamos $\mathscr{C} \subseteq G_q(n,k)$ y tiene distancia mínima d, entonces se dice que $\mathscr{C}$ es un $[n, k, |\mathscr{C}|, d]$-código sobre $\mathbb{F}_q$ y sus parámetros están dados por $[n, k, |\mathscr{C}|, d]$. En este caso, note que si $U, V \in \mathscr{C}$, entonces

$$d(U,V) = 2k - 2\dim(U \cap V). \qquad \text{(II.3)}$$

Por lo tanto $d(\mathscr{C})$ es siempre un número par.

III. Códigos Grassmannianos Cíclicos

Los códigos Grassmannianos cíclicos fueron introducidos por A. Kohnert y S. Kurz en [17] desde un punto de vista algebraico y geométrico. Posteriormente T. Etzion y A. Vardy en [6] los han definido utilizando el concepto de traslación cíclica para un subespacio fijo en una Grassmaniana sobre un cuerpo finito.

Usando acciones de grupos, J. Rosenthal et al. [21] y H. Gluesing et al. [9] estudiaron una versión general de los códigos de subespacios cíclicos, los códigos de órbitas cíclicos. Específicamente, han utilizado una acción del grupo lineal general $\mathrm{GL}(n,q)$ sobre el conjunto de todos los subespacios k-dimensionales de $\mathbb{F}_q^n$ para definir dichos códigos. Sin embargo, en [21] no se da una construcción no trivial de dichos códigos y en [9] se presenta la construcción de un código de subespacios cíclico, con órbita de longitud no completa. En ambos artículos, resulta relevante la siguiente conjetura:

Conjetura III.1 *Para cualquier par de enteros positivos n, k con $k < n/2$ existe un código de subespacios cíclico en $G_q(n,k)$ de tamaño $\frac{q^n-1}{q-1}$ y distancia mínima $2k-2$.*

Recientemente, T. Etzion et al. han presentado en [2] un nuevo método para construir códigos de subespacios cíclicos, el cual se fundamenta en el uso de un tipo especial de polinomios linealizados, los polinomios de subespacios y también de las funciones de Frobenius.

En este artículo presentamos la construcción de códigos de subespacios cíclicos. Para ello, hemos diseñado e implementado en Java y en C++ un conjunto de algoritmos. Además, utilizamos las librerías sobre cuerpos finitos contenidos en GAP System for Computational Discrete Algebra [8]. También presentamos la definición de códigos de subespacios m-quasi cíclicos como una generalización natural de los códigos cíclicos y mostramos algunos resultados sobre el tamaño de una cuasi órbita.

Sea $\mathbb{F}_{q^n}$ la extensión de grado n del cuerpo $\mathbb{F}_q$. Es ampliamente conocido que $\mathbb{F}_{q^n}$ puede considerarse como un espacio vectorial de dimensión n sobre $\mathbb{F}_q$. Es decir, para una base fija, podemos identificar cada elemento de $\mathbb{F}_{q^n}$ con una n-tupla de elementos en $\mathbb{F}_q$. Por lo tanto, no distinguiremos entre $\mathbb{F}_{q^n}$ y $\mathbb{F}_q^n$.

Definición III.2 *Sea γ un elemento primitivo de $\mathbb{F}_{q^n}$ y $\sigma = (12\cdots q^k-1) \in \mathrm{Sym}(q^k-1)$. Un código de subespacios $\mathscr{C} \subseteq \mathbb{P}_q(n)$ se denomina `cíclico`, si satisface la siguiente propiedad:*

$$\{0, \gamma^{i_1}, \ldots, \gamma^{i_s}\} \in \mathscr{C} \Rightarrow \{0, \gamma^{\sigma(i_1)}, \ldots, \gamma^{\sigma(i_s)}\} \in \mathscr{C}. \quad \text{(III.1)}$$

Es decir, satisface la propiedad:

$$\{0, \gamma^{i_1}, \ldots, \gamma^{i_s}\} \in \mathscr{C} \Rightarrow \{0, \gamma^{i_1+1}, \ldots, \gamma^{i_s+1}\} \in \mathscr{C}. \quad \text{(III.2)}$$

(Asumiendo que $s = q^k - 1$, con k la dimensión de la palabra de código).

Una construcción trivial de un código de subespacios cíclico es la siguiente:

Ejemplo III.3 *Sea γ una raíz primitiva de $x^{10}+x^6+x^5+x^3+x^2+x+1$ y usemos este polinomio para generar el cuerpo $\mathbb{F}_{2^{10}}$. Sea $\mathscr{C} \subseteq G_2(10,5)$ definido como sigue:*

$$\mathscr{C} := \{\alpha\mathbb{F}_{2^5} \mid \alpha \in \mathbb{F}_{2^{10}}^*\}.$$

Esto es, $\mathscr{C}$ es una órbita de $\mathbb{F}_{2^5}$ en $\mathbb{F}_{2^{10}}$. Note que los elementos no nulos de $\mathbb{F}_{2^5}$ forman un grupo cíclico, generado por γ^{33}. Entonces el tamaño de $\mathscr{C}$ es $\frac{2^{10}-1}{2^5-1} = 33$. Por otro lado, note que, si $U, V \in \mathscr{C}$, con $U \neq V$, entonces $dim(U \cap V) = 0$. Por lo tanto, para $\alpha, \alpha' \in \mathbb{F}_{2^{10}}^*$ tenemos

$$d(\alpha\mathbb{F}_2^5, \alpha'\mathbb{F}_2^5) = 5+5-2\cdot 0 = 10. \tag{III.3}$$

En resumen, $\mathscr{C}$ es un $[10,5,33,10]$-código. Específicamente $\mathscr{C}$ consta de todas las traslaciones cíclicas del subespacio
$\{\gamma^0,\gamma^{33},\gamma^{66},\gamma^{99},\gamma^{132},\gamma^{165},\gamma^{198},\gamma^{231},\gamma^{264},\gamma^{297},\gamma^{330},\gamma^{363},$
$\gamma^{396},\gamma^{429},\gamma^{462},\gamma^{495},\gamma^{528},\gamma^{561},\gamma^{594},\gamma^{627},\gamma^{660},\gamma^{693},\gamma^{726},$
$\gamma^{759},\gamma^{792},\gamma^{825},\gamma^{858},\gamma^{891},\gamma^{924},\gamma^{957},\gamma^{990}\}$.

Tenga en cuenta que en este ejemplo, el vector nulo se ha omitido del conjunto. En lo sucesivo, este se eliminará explícitamente cuando especifiquemos los elementos de un código de subespacios cíclico o cuasi-cíclico.

Observación III.4 *Un subconjunto S de $G_q(n,k)$ es llamado un `código de extensión` de $\mathbb{F}_q^n$, si se satisfacen:*
(1) $V \cap W = \{0\}$, para todo $V, W \in S$, y
(2) para todo $0 \neq v \in \mathbb{F}_q^n$, existe un único $V \in S$, tal que $v \in V$.
Es conocido que los códigos de extensión existen si y solo si $k \mid n$. El código del ejemplo III.3 es un código de extensión de $\mathbb{F}_2^{10}$.

Denotemos respectivamente con $\mathcal{A}_q(n,d)$ y $\mathcal{A}_q(n,d,k)$ el número máximo de palabras de códigos en un $[n,|\mathscr{C}|,d]$-código en $\mathbb{P}_q(n)$ y en un $[n,k,|\mathscr{C}|,d]$-código en $G_q(n,k)$. En el contexto de los códigos cíclicos introducimos la notación $\mathcal{C}_q(n,d,k)$, para indicar el mayor número de subespacios en un código cíclico con longitud n, dimensión k, y distancia mínima d sobre $\mathbb{F}_q$. Es evidente que

$$\mathcal{C}_q(n,d,k) \leq \mathcal{A}_q(n,d,k). \tag{III.4}$$

Ejemplo III.5 *Sea γ una raíz primitiva de $x^8+x^4+x^3+x^2+1$ y usemos este polinomio para generar el cuerpo $\mathbb{F}_{2^8}$. Sea $\mathscr{C} \subseteq G_2(8,4)$, el cual consiste de todas las traslaciones cíclicas de*
$\{\gamma^0,\gamma^2,\gamma^{29},\gamma^{39},\gamma^{49},\gamma^{50},\gamma^{60},\gamma^{71},\gamma^{74},\gamma^{103},\gamma^{106},\gamma^{109},\gamma^{132},$
$\gamma^{181},\gamma^{197}\}$
$\{\gamma^0,\gamma^2,\gamma^{31},\gamma^{45},\gamma^{50},\gamma^{91},\gamma^{110},\gamma^{123},\gamma^{126},\gamma^{163},\gamma^{182},\gamma^{183},$
$\gamma^{205},\gamma^{207},\gamma^{209}\}$
$\{\gamma^0,\gamma^{23},\gamma^{64},\gamma^{70},\gamma^{79},\gamma^{97},\gamma^{110},\gamma^{124},\gamma^{126},\gamma^{154},\gamma^{174},\gamma^{180},$
$\gamma^{190},\gamma^{196},\gamma^{201}\}$
$\{\gamma^0,\gamma^1,\gamma^{25},\gamma^{38},\gamma^{81},\gamma^{94},\gamma^{124},\gamma^{155},\gamma^{156},\gamma^{159},\gamma^{160},\gamma^{169},$
$\gamma^{180},\gamma^{184},\gamma^{202}\}$
$\{\gamma^0,\gamma^1,\gamma^{25},\gamma^{56},\gamma^{64},\gamma^{65},\gamma^{70},\gamma^{71},\gamma^{89},\gamma^{95},\gamma^{109},\gamma^{131},\gamma^{162},$
$\gamma^{176},\gamma^{203}\}$
$\{\gamma^0,\gamma^{16},\gamma^{31},\gamma^{45},\gamma^{49},\gamma^{88},\gamma^{114},\gamma^{145},\gamma^{155},\gamma^{159},\gamma^{166},\gamma^{171},$
$\gamma^{175},\gamma^{197},\gamma^{211}\}$
$\{\gamma^0,\gamma^7,\gamma^{30},\gamma^{46},\gamma^{66},\gamma^{76},\gamma^{87},\gamma^{88},\gamma^{89},\gamma^{112},\gamma^{113},\gamma^{137},\gamma^{167},$
$\gamma^{175},\gamma^{203}\}$
$\{\gamma^0,\gamma^5,\gamma^{10},\gamma^{21},\gamma^{37},\gamma^{40},\gamma^{76},\gamma^{84},\gamma^{113},\gamma^{114},\gamma^{138},\gamma^{143},$
$\gamma^{150},\gamma^{166},\gamma^{179}\}$
$\{\gamma^0,\gamma^8,\gamma^{16},\gamma^{54},\gamma^{69},\gamma^{87},\gamma^{125},\gamma^{130},\gamma^{145},\gamma^{163},\gamma^{167},\gamma^{182},$
$\gamma^{194},\gamma^{200},\gamma^{208}\}$
$\{\gamma^0,\gamma^{40},\gamma^{41},\gamma^{53},\gamma^{65},\gamma^{80},\gamma^{84},\gamma^{98},\gamma^{124},\gamma^{139},\gamma^{147},\gamma^{157},$
$\gamma^{162},\gamma^{168},\gamma^{180}\}$
$\{\gamma^0,\gamma^{27},\gamma^{59},\gamma^{62},\gamma^{82},\gamma^{89},\gamma^{90},\gamma^{104},\gamma^{114},\gamma^{117},\gamma^{122},\gamma^{125},$
$\gamma^{166},\gamma^{194},\gamma^{203}\}$
$\{\gamma^0,\gamma^{19},\gamma^{47},\gamma^{62},\gamma^{78},\gamma^{80},\gamma^{90},\gamma^{92},\gamma^{101},\gamma^{128},\gamma^{140},\gamma^{168},$
$\gamma^{205},\gamma^{207},\gamma^{212}\}$
$\{\gamma^0,\gamma^9,\gamma^{28},\gamma^{38},\gamma^{47},\gamma^{49},\gamma^{93},\gamma^{97},\gamma^{101},\gamma^{120},\gamma^{158},\gamma^{184},$
$\gamma^{190},\gamma^{193},\gamma^{197}\}$
$\{\gamma^0,\gamma^7,\gamma^9,\gamma^{57},\gamma^{62},\gamma^{64},\gamma^{70},\gamma^{72},\gamma^{83},\gamma^{90},\gamma^{112},\gamma^{120},\gamma^{156},$
$\gamma^{169},\gamma^{195}\}$
$\{\gamma^0,\gamma^7,\gamma^{47},\gamma^{59},\gamma^{79},\gamma^{82},\gamma^{91},\gamma^{94},\gamma^{101},\gamma^{112},\gamma^{148},\gamma^{174},\gamma^{202},$
$\gamma^{206},\gamma^{209}\}$
$\{\gamma^0,\gamma^6,\gamma^{12},\gamma^{49},\gamma^{53},\gamma^{58},\gamma^{107},\gamma^{127},\gamma^{147},\gamma^{149},\gamma^{156},\gamma^{169},$
$\gamma^{188},\gamma^{191},\gamma^{197}\}$
$\{\gamma^0,\gamma^1,\gamma^8,\gamma^{20},\gamma^{25},\gamma^{42},\gamma^{76},\gamma^{93},\gamma^{113},\gamma^{135},\gamma^{144},\gamma^{151},\gamma^{158},$
$\gamma^{178},\gamma^{200}\}$
$\{\gamma^0,\gamma^{13},\gamma^{14},\gamma^{38},\gamma^{54},\gamma^{85},\gamma^{98},\gamma^{99},\gamma^{123},\gamma^{139},\gamma^{170},\gamma^{183},$
$\gamma^{184},\gamma^{208},\gamma^{224}\}$
$\{\gamma^0,\gamma^9,\gamma^{32},\gamma^{35},\gamma^{37},\gamma^{85},\gamma^{94},\gamma^{117},\gamma^{120},\gamma^{122},\gamma^{170},\gamma^{179},$
$\gamma^{202},\gamma^{205},\gamma^{207}\}$

Este código $\mathscr{C}$ es un $[8,4,4590,4]$-código y se verifica que

$$4590 \leq \mathcal{A}_2(8,4,4) \leq 6477. \tag{III.5}$$

Ejemplo III.6 *Sea γ una raíz primitiva de $x^{10}+x^6+x^5+x^3+x^2+x+1$ y usemos este polinomio para generar el cuerpo $\mathbb{F}_{2^{10}}$. Sea $\mathscr{C} \subseteq G_2(10,3)$, el cual consiste de todas las traslaciones cíclicas de*

$\{\gamma^0,\gamma^{37},\gamma^{104},\gamma^{170},\gamma^{251},\gamma^{269},\gamma^{576}\}$
$\{\gamma^0,\gamma^{37},\gamma^{104},\gamma^{170},\gamma^{251},\gamma^{269},\gamma^{576}\}$
$\{\gamma^0,\gamma^{68},\gamma^{240},\gamma^{257},\gamma^{389},\gamma^{560},\gamma^{587}\}$
$\{\gamma^0,\gamma^{126},\gamma^{169},\gamma^{243},\gamma^{452},\gamma^{487},\gamma^{707}\}$
$\{\gamma^0,\gamma^{164},\gamma^{324},\gamma^{491},\gamma^{684},\gamma^{710},\gamma^{762}\}$
$\{\gamma^0,\gamma^{59},\gamma^{295},\gamma^{418},\gamma^{537},\gamma^{631},\gamma^{718}\}$
$\{\gamma^0,\gamma^{21},\gamma^{36},\gamma^{335},\gamma^{365},\gamma^{650},\gamma^{711}\}$
$\{\gamma^0,\gamma^{70},\gamma^{173},\gamma^{380},\gamma^{457},\gamma^{654},\gamma^{811}\}$
$\{\gamma^0,\gamma^{10},\gamma^{216},\gamma^{469},\gamma^{544},\gamma^{613},\gamma^{635}\}$
$\{\gamma^0,\gamma^{105},\gamma^{161},\gamma^{289},\gamma^{424},\gamma^{517},\gamma^{565}\}$
$\{\gamma^0,\gamma^{156},\gamma^{306},\gamma^{382},\gamma^{488},\gamma^{678},\gamma^{789}\}$
$\{\gamma^0,\gamma^{31},\gamma^{42},\gamma^{131},\gamma^{143},\gamma^{241},\gamma^{399}\}$
$\{\gamma^0,\gamma^{109},\gamma^{247},\gamma^{249},\gamma^{374},\gamma^{432},\gamma^{476}\}$

$$\{\gamma^0, \gamma^{124}, \gamma^{246}, \gamma^{524}, \gamma^{527}, \gamma^{577}, \gamma^{672}\}$$
$$\{\gamma^0, \gamma^{49}, \gamma^{163}, \gamma^{235}, \gamma^{440}, \gamma^{628}, \gamma^{802}\}$$
$$\{\gamma^0, \gamma^{60}, \gamma^{176}, \gamma^{291}, \gamma^{353}, \gamma^{553}, \gamma^{786}\}$$
$$\{\gamma^0, \gamma^{107}, \gamma^{286}, \gamma^{441}, \gamma^{482}, \gamma^{578}, \gamma^{793}\}$$
$$\{\gamma^0, \gamma^{4}, \gamma^{208}, \gamma^{222}, \gamma^{254}, \gamma^{279}, \gamma^{502}\}$$
$$\{\gamma^0, \gamma^{298}, \gamma^{515}, \gamma^{523}, \gamma^{543}, \gamma^{588}, \gamma^{607}\}$$
$$\{\gamma^0, \gamma^{1}, \gamma^{154}, \gamma^{192}, \gamma^{575}, \gamma^{609}, \gamma^{622}\}$$
$$\{\gamma^0, \gamma^{7}, \gamma^{23}, \gamma^{175}, \gamma^{434}, \gamma^{497}, \gamma^{580}\}$$
$$\{\gamma^0, \gamma^{252}, \gamma^{258}, \gamma^{338}, \gamma^{518}, \gamma^{680}, \gamma^{719}\}.$$

Entonces $\mathscr{C}$ es un $[10, 3, 21483, 4]$-código y se verifica que

$$21483 \leq \mathcal{A}_2(10, 4, 3) \leq 24893. \tag{III.6}$$

Observación III.7 *Obtener límites o cotas tanto superiores como inferiores para el tamaño de un código de subespacios resulta ser una herramienta fundamental para la construcción de tales conjuntos.* `Subspaces codes`*, [12], es un proyecto liderado por Daniel Heinlein et al. en el instituto de Matemáticas de la Universidad de Bayreuth en Alemania, el cual proporciona una tabla de búsqueda para las cotas del tamaño de códigos de subespacios y en particular códigos Grassmannianos. Los códigos construidos en los ejemplos III.5 y III.6 son casi óptimos.*

Una definición alternativa para un código cíclico es la siguiente:

Definición III.8 *Sean $\alpha \in \mathbb{F}_{q^n}^*$ y $V \in G_q(n,k)$. La* `traslación cíclica` *o la* `órbita` *de V es definida como sigue:*

$$\alpha V := \{\alpha v \mid v \in V\}. \tag{III.7}$$

Es evidente que el conjunto αV es también un subespacio con la misma dimensión que V. Si para $0 \neq \alpha, \beta \in \mathbb{F}_{q^n}$ se satisface que $\alpha V \neq \beta V$, entonces se dice que estas traslaciones cíclicas son `distintas`*. Un código de subespacio $\mathscr{C} \subseteq G_q(n,k)$ es llamado* `cíclico`*, si para todo $\alpha \in \mathbb{F}_{q^n}^*$ y todo subespacio $V \in \mathscr{C}$ se tiene que $\alpha V \in \mathscr{C}$. El conjunto $\mathcal{O}rb(V) := \{\alpha V \mid \alpha \in \mathbb{F}_{q^n}^*\}$ se llama* `órbita` *de V.*

Lema III.9 *[2, Lemma 9] Si $V \in G_q(n,k)$, entonces*

$$|\mathcal{O}rb(V)| = \frac{q^n - 1}{q^t - 1}, \tag{III.8}$$

para algún número natural t, que divide a n.

Se sigue inmediatamente que

Corolario III.10

$$\mathcal{C}_q(n, d, k) = \sum_{t|n} \alpha_t \frac{q^n - 1}{q^t - 1}, \tag{III.9}$$

para algunos valores de $\alpha_t \geq 0$.

Como consecuencia directa del Lema anterior se tiene que el tamaño máximo de una órbita se alcanza cuando $t = 1$. Esto justifica la siguiente definición:

Definición III.11 *Se dice que $V \in G_q(n,k)$ tiene una* `órbita de longitud completa`*, si*

$$|\mathcal{O}rb(V)| = \tfrac{q^n - 1}{q - 1}. \tag{III.10}$$

Si V no tiene una órbita de longitud completa, entonces decimos que V tiene una `órbita degenerada`*.*

Observación III.12 *En el código del ejemplo III.5 las primeras 17 órbitas son de longitud completa y las 3 restantes son órbitas con 85 subespacios.*

IV. Clasificación de Órbitas en $\mathbb{F}_q^n$

Las siguientes tablas han sido calculadas usando el Sistema para Álgebra Computacional Discreta GAP y algunos algoritmos programados en lenguajes C++ y Java.

(1) $n = 6$

TABLA I
ÓRBITAS EN $\mathbb{P}_2(6)$

Número de órbitas				Órbitas completas			
$k \setminus d$	2	4	6	$k \setminus d$	2	4	6
1	1	0	0	1	1	0	0
2	10	1	0	2	10	0	0
3	14	8	1	3	14	8	0

Hay dos órbitas degeneradas: la primera consiste en 21 subespacios de dimensión 2 y tiene una distancia mínima de 4 y la segunda es solo el código de extensión

$$\{\alpha \mathbb{F}_{2^3} \mid \alpha \in \mathbb{F}_{2^6}^*\}.$$

Este tiene 9 subespacios.

(2) $n = 7$

TABLA II
ÓRBITAS EN $\mathbb{P}_2(7)$

Número de órbitas		
$k \setminus d$	2	4
1	1	0
2	21	0
3	21	72

(3) $n = 8$

TABLA III
ÓRBITAS EN $\mathbb{P}_2(8)$

Número de órbitas					Órbitas completas				
$k \setminus d$	2	4	6	8	$k \setminus d$	2	4	6	8
1	1	0	0	0	1	1	0	0	0
2	42	1	0	0	2	42	0	0	0
3	61	320	0	0	3	61	320	0	0
4	40	750	0	1	4	40	746	0	0

Hay seis órbitas degeneradas: las primeras cinco órbitas se componen de 85 subespacios, una de dimensión 2 y cuatro

de dimensión 4. Todas tienen una distancia mínima 4. La última es solo el código de extensión $\{\alpha\mathbb{F}_{2^4} \mid \alpha \in \mathbb{F}_{2^8}^*\}$, el cual tiene 17 subespacios.

(4) $n = 9$

TABLA IV
ÓRBITAS EN $\mathbb{P}_2(9)$

Número de órbitas				Órbitas completas			
$k \setminus d$	2	4	6	$k \setminus d$	2	4	6
1	1	0	0	1	1	0	0
2	85	0	0	2	85	0	0
3	84	1458	1	3	84	1458	0
4	93	5736	648	4	93	5736	648

Solo hay una órbita degenerada, consta de 73 subespacios de dimensión 3 y tiene distancia mínima 6.

(5) $n = 10$

TABLA V
ÓRBITAS EN $\mathbb{P}_2(10)$

Número de órbitas					
$k \setminus d$	2	4	6	8	10
1	1	0	0	0	0
2	170	1	0	0	0
3	255	5950	0	0	0
4	166	31487	20894	0	0
5	522	41772	64472	0	1

Órbitas completas					
$k \setminus d$	2	4	6	8	10
1	1	0	0	0	0
2	170	0	0	0	0
3	255	5950	0	0	0
4	166	31470	20894	0	0
5	522	41772	64472	0	0

Hay diecinueve órbitas degeneradas: las primeras dieciocho órbitas se componen de 341 subespacios, diecisiete de dimensión 4 y uno de dimensión 2. Todas tienen una distancia mínima de 4. El último es el código de extensión $\{\alpha\mathbb{F}_{2^4} \mid \alpha \in \mathbb{F}_{2^8}^*\}$, que tiene 33 subespacios.

(6) $n = 11$

TABLA VI
ÓRBITAS EN $\mathbb{P}_2(11)$

Número de órbitas				
$k \setminus d$	2	4	6	8
1	1	0	0	0
2	341	0	0	0
3	341	24552	0	0
4	341	132308	290532	0
5	341	193688	1539637	11

Observación IV.1 *La conjetura 1 puede ser refutada por el resultado en la tabla V. Tenga en cuenta que no hay una órbita completa en $\mathbb{F}_2^{10}$ con dimensión 5 y distancia mínima 8. (Un contraejemplo a la conjetura fue dado inicialmente por H. Gluesing et al. en [9]).*

V. CÓDIGOS GRASSMANNIANOS CUASI-CÍCLICOS

Presentamos ahora una generalización natural de la definición de órbitas de subespacios y de la longitud de una órbita.

Definición V.1 *Sean $\alpha \in \mathbb{F}_{q^n}^*$, $V \in G_q(n,k)$ y m un número natural con $m \mid q^n - 1$. La m-cuasi traslación cíclica de V se define así:*

$$\alpha^m V := \{\alpha^m v \mid v \in V\}. \tag{V.1}$$

Está claro que el conjunto $\alpha^m V$ es nuevamente un subespacio con la misma dimensión que V. Un código Grassmanniano $\mathscr{C} \subseteq G_q(n,k)$ se llama m-cuasi cíclico, si para todo $\alpha \in \mathbb{F}_{q^n}^*$ y todo subespacio $V \in \mathscr{C}$ se tiene que $\alpha^m V \in \mathscr{C}$. El conjunto

$$\mathcal{O}rb_m(V) := \{\alpha^m V \mid \alpha \in \mathbb{F}_{q^n}^*\} \tag{V.2}$$

se llama m-cuasi órbita de V.

El siguiente lema determina el tamaño de las cuasi-órbitas. La idea de la prueba es la misma que la presentada por T. Etzion et al. in [2, Lema 9] para el caso $m = 1$. Esta prueba se obtiene realizando solo modificaciones básicas al mencionado.

Teorema V.2 *Si m es un número natural con $m \mid q^n - 1$ y $V \in G_q(n,k)$, entonces*

$$|\mathcal{O}rb_m(V)| = \frac{1}{m}\Big(\frac{q^n-1}{q^t-1}\Big), \tag{V.3}$$

para algún número natural t, el cual divide a n.

Proof: Let γ un elemento primitivo en $\mathbb{F}_{q^n}$, esto es, $\mathbb{F}_{q^n}^* = \langle\gamma\rangle$ y sea l el número natural más pequeño con $\gamma^{lm}V = V$. Es claro que $lm \mid q^n - 1$. Sea ahora $0 \le s < l$ y $i \in \mathbb{N}$, entonces

$$\gamma^{iml+s}V = \gamma^s(\gamma^{iml}V) \tag{V.4}$$
$$= \gamma^s(\gamma^{ml}\cdots\gamma^{ml})V \tag{V.5}$$
$$= \gamma^s V. \tag{V.6}$$

Esto es, para cada número natural i y para cada $0 \le s < l$ se verifica que $\gamma^s V = \gamma^{iml+s}V$. Adicionalmente, para cada $0 \le s_1, s_2 < l$ los conjuntos

$$A_{s_j} := \{\gamma^{iml+s_j} \mid i \in \mathbb{N}\} \tag{V.7}$$

satisfacen que $|A_{s_1}| = |A_{s_2}|$. En efecto, dado que $q^n - 1 = wml$, para algún $w \in \mathbb{N}$, entonces tenemos

$$A_{s_j} = \{\gamma^{s_j}, \gamma^{ml+s_j}, \ldots, \gamma^{ml(w-1)+s_j}\}. \tag{V.8}$$

En consecuencia $|A_{s_1}| = |A_{s_2}| = w$. Sea $\gamma^{iml}, \gamma^{rml} \in A_0$, para algunos $i, r \in \mathbb{N}$. Dado que $A_0 = \{\gamma^{iml} \mid i \in \mathbb{N}\}$, se sigue que

$$(\gamma^{iml} + \gamma^{rml})V \subseteq \gamma^{iml}V + \gamma^{rml}V = V + V = V, \tag{V.9}$$

y en consecuencia $\gamma^{iml} + \gamma^{rml} \in A_0$. Es claro que A_0 es cerrado bajo la multiplicación, entonces tenemos que $\langle\gamma^{ml}\rangle$ es el grupo multiplicativo de un subcuerpo de $\mathbb{F}_{q^n}$, digamos $\mathbb{F}_{q^t}$, para algún número natural t, el cual divide a n. Entonces

$$|\mathcal{O}rb_m(V)| = l = \frac{q^n-1}{mw} = \frac{1}{m}\Big(\frac{q^n-1}{q^t-1}\Big), \tag{V.10}$$

lo cual prueba el lema. □

Una consecuencia inmediata del Teorema V.2 es que el tamaño mas largo posible de una m-cuasi órbita is $\frac{1}{m}\left(\frac{q^n-1}{q-1}\right)$. Esto justifica la siguiente definición:

Definición V.3 *Decimos que $V \in G_q(n,k)$ tiene una* `m-cuasi órbita completa`*, si*

$$|\mathcal{O}rb_m(V)| = \tfrac{1}{m}\left(\tfrac{q^n-1}{q-1}\right). \tag{V.11}$$

En otro caso decimos que V tiene una `m-cuasi órbita degenerada`*.*

Ejemplo V.4 *Let γ una raíz primitiva de $x^8+x^4+x^3+x^2+1$ y use este polinomio para generar el cuerpo $\mathbb{F}_{2^8}$. Sea $\mathscr{C}$ el código Grassmanniano en $G_2(8,4)$, el cual consiste de todas las 3-traslaciones cíclicas de*

$\{\gamma^0,\gamma^{19},\gamma^{58},\gamma^{62},\gamma^{90},\gamma^{92},\gamma^{93},\gamma^{107},\gamma^{117},\gamma^{122},\gamma^{125},\gamma^{128},\gamma^{140},\gamma^{158},\gamma^{194}\}$
$\{\gamma^0,\gamma^6,\gamma^{13},\gamma^{47},\gamma^{99},\gamma^{101},\gamma^{118},\gamma^{149},\gamma^{156},\gamma^{163},\gamma^{164},\gamma^{169},\gamma^{182},\gamma^{188},\gamma^{191}\}$
$\{\gamma^1,\gamma^{27},\gamma^{42},\gamma^{58},\gamma^{59},\gamma^{60},\gamma^{62},\gamma^{72},\gamma^{83},\gamma^{84},\gamma^{108},\gamma^{110},\gamma^{158},\gamma^{187},\gamma^{199}\}$
$\{\gamma^1,\gamma^{18},\gamma^{20},\gamma^{59},\gamma^{68},\gamma^{69},\gamma^{80},\gamma^{93},\gamma^{108},\gamma^{126},\gamma^{152},\gamma^{175},\gamma^{179},\gamma^{195},\gamma^{217}\}$
$\{\gamma^2,\gamma^{25},\gamma^{62},\gamma^{77},\gamma^{89},\gamma^{95},\gamma^{96},\gamma^{120},\gamma^{134},\gamma^{160},\gamma^{166},\gamma^{169},\gamma^{198},\gamma^{201},\gamma^{204}\}$
$\{\gamma^2,\gamma^{22},\gamma^{44},\gamma^{49},\gamma^{83},\gamma^{96},\gamma^{103},\gamma^{125},\gamma^{126},\gamma^{150},\gamma^{162},\gamma^{182},\gamma^{185},\gamma^{204},\gamma^{208}\}$
$\{\gamma^2,\gamma^{30},\gamma^{39},\gamma^{40},\gamma^{51},\gamma^{64},\gamma^{92},\gamma^{120},\gamma^{150},\gamma^{166},\gamma^{181},\gamma^{186},\gamma^{195},\gamma^{199},\gamma^{208}\}$
$\{\gamma^2,\gamma^{12},\gamma^{22},\gamma^{23},\gamma^{33},\gamma^{42},\gamma^{44},\gamma^{47},\gamma^{64},\gamma^{78},\gamma^{86},\gamma^{92},\gamma^{115},\gamma^{153},\gamma^{180}\}$
$\{\gamma^0,\gamma^7,\gamma^{38},\gamma^{52},\gamma^{72},\gamma^{79},\gamma^{94},\gamma^{112},\gamma^{141},\gamma^{156},\gamma^{169},\gamma^{174},\gamma^{184},\gamma^{195},\gamma^{202}\}$
$\{\gamma^2,\gamma^9,\gamma^{46},\gamma^{48},\gamma^{63},\gamma^{78},\gamma^{81},\gamma^{96},\gamma^{114},\gamma^{115},\gamma^{139},\gamma^{176},\gamma^{188},\gamma^{204},\gamma^{217}\}$
$\{\gamma^0,\gamma^5,\gamma^{37},\gamma^{40},\gamma^{67},\gamma^{74},\gamma^{84},\gamma^{95},\gamma^{103},\gamma^{135},\gamma^{138},\gamma^{144},\gamma^{176},\gamma^{179},\gamma^{216}\}$
$\{\gamma^1,\gamma^7,\gamma^{14},\gamma^{48},\gamma^{100},\gamma^{102},\gamma^{119},\gamma^{150},\gamma^{157},\gamma^{164},\gamma^{165},\gamma^{170},\gamma^{183},\gamma^{189},\gamma^{192}\}$
$\{\gamma^1,\gamma^{17},\gamma^{33},\gamma^{36},\gamma^{88},\gamma^{96},\gamma^{98},\gamma^{109},\gamma^{126},\gamma^{146},\gamma^{162},\gamma^{168},\gamma^{177},\gamma^{191},\gamma^{195}\}$
$\{\gamma^1,\gamma^3,\gamma^{51},\gamma^{61},\gamma^{63},\gamma^{72},\gamma^{91},\gamma^{110},\gamma^{111},\gamma^{127},\gamma^{133},\gamma^{135},\gamma^{164},\gamma^{178},\gamma^{183}\}$
$\{\gamma^1,\gamma^7,\gamma^{24},\gamma^{33},\gamma^{36},\gamma^{53},\gamma^{75},\gamma^{104},\gamma^{142},\gamma^{144},\gamma^{151},\gamma^{188},\gamma^{192},\gamma^{197},\gamma^{205}\}$
$\{\gamma^0,\gamma^{12},\gamma^{27},\gamma^{31},\gamma^{45},\gamma^{65},\gamma^{87},\gamma^{104},\gamma^{127},\gamma^{155},\gamma^{159},\gamma^{162},\gamma^{167},\gamma^{171},\gamma^{211}\}$
$\{\gamma^2,\gamma^6,\gamma^{36},\gamma^{45},\gamma^{55},\gamma^{66},\gamma^{72},\gamma^{102},\gamma^{112},\gamma^{123},\gamma^{128},\gamma^{138},\gamma^{149},\gamma^{156},\gamma^{203}\}$
$\{\gamma^0,\gamma^{26},\gamma^{41},\gamma^{57},\gamma^{58},\gamma^{59},\gamma^{61},\gamma^{71},\gamma^{82},\gamma^{83},\gamma^{107},\gamma^{109},\gamma^{157},\gamma^{186},\gamma^{198}\}$
$\{\gamma^0,\gamma^6,\gamma^{23},\gamma^{53},\gamma^{55},\gamma^{58},\gamma^{63},\gamma^{74},\gamma^{89},\gamma^{103},\gamma^{107},\gamma^{147},\gamma^{191},\gamma^{196},\gamma^{203}\}$
$\{\gamma^2,\gamma^6,\gamma^8,\gamma^{49},\gamma^{56},\gamma^{102},\gamma^{103},\gamma^{127},\gamma^{157},\gamma^{161},\gamma^{165},\gamma^{184},\gamma^{193},\gamma^{196},\gamma^{210}\}$
$\{\gamma^1,\gamma^{14},\gamma^{16},\gamma^{18},\gamma^{34},\gamma^{56},\gamma^{64},\gamma^{66},\gamma^{69},\gamma^{77},\gamma^{100},\gamma^{114},\gamma^{155},\gamma^{163},\gamma^{202}\}$
$\{\gamma^2,\gamma^4,\gamma^9,\gamma^{32},\gamma^{52},\gamma^{68},\gamma^{74},\gamma^{91},\gamma^{114},\gamma^{130},\gamma^{142},\gamma^{158},\gamma^{171},\gamma^{197},\gamma^{205}\}$
$\{\gamma^2,\gamma^{39},\gamma^{43},\gamma^{48},\gamma^{55},\gamma^{82},\gamma^{95},\gamma^{139},\gamma^{149},\gamma^{159},\gamma^{160},\gamma^{165},\gamma^{170},\gamma^{181},\gamma^{184}\}$
$\{\gamma^2,\gamma^4,\gamma^{42},\gamma^{43},\gamma^{52},\gamma^{59},\gamma^{63},\gamma^{67},\gamma^{85},\gamma^{86},\gamma^{110},\gamma^{159},\gamma^{163},\gamma^{164},\gamma^{188}\}$
$\{\gamma^1,\gamma^5,\gamma^6,\gamma^7,\gamma^{30},\gamma^{31},\gamma^{55},\gamma^{67},\gamma^{95},\gamma^{101},\gamma^{139},\gamma^{182},\gamma^{192},\gamma^{203},\gamma^{209}\}$
$\{\gamma^2,\gamma^{28},\gamma^{32},\gamma^{41},\gamma^{68},\gamma^{108},\gamma^{112},\gamma^{127},\gamma^{128},\gamma^{145},\gamma^{150},\gamma^{152},\gamma^{196},\gamma^{200},\gamma^{208}\}$
$\{\gamma^1,\gamma^5,\gamma^{11},\gamma^{20},\gamma^{22},\gamma^{38},\gamma^{70},\gamma^{73},\gamma^{93},\gamma^{101},\gamma^{115},\gamma^{131},\gamma^{167},\gamma^{180},\gamma^{196}\}$
$\{\gamma^1,\gamma^{41},\gamma^{60},\gamma^{61},\gamma^{73},\gamma^{76},\gamma^{83},\gamma^{85},\gamma^{94},\gamma^{133},\gamma^{159},\gamma^{188},\gamma^{196},\gamma^{200},\gamma^{205}\}$
$\{\gamma^2,\gamma^{21},\gamma^{60},\gamma^{64},\gamma^{92},\gamma^{94},\gamma^{95},\gamma^{109},\gamma^{119},\gamma^{124},\gamma^{127},\gamma^{130},\gamma^{142},\gamma^{160},\gamma^{196}\}$
$\{\gamma^1,\gamma^8,\gamma^{39},\gamma^{53},\gamma^{73},\gamma^{80},\gamma^{95},\gamma^{113},\gamma^{142},\gamma^{157},\gamma^{170},\gamma^{175},\gamma^{185},\gamma^{196},\gamma^{203}\}$
$\{\gamma^1,\gamma^{32},\gamma^{46},\gamma^{59},\gamma^{89},\gamma^{108},\gamma^{115},\gamma^{125},\gamma^{136},\gamma^{145},\gamma^{167},\gamma^{176},\gamma^{181},\gamma^{190},\gamma^{220}\}$
$\{\gamma^2,\gamma^8,\gamma^{12},\gamma^{23},\gamma^{41},\gamma^{87},\gamma^{93},\gamma^{97},\gamma^{108},\gamma^{126},\gamma^{172},\gamma^{178},\gamma^{182},\gamma^{193},\gamma^{211}\}$
$\{\gamma^2,\gamma^{15},\gamma^{16},\gamma^{40},\gamma^{56},\gamma^{87},\gamma^{100},\gamma^{101},\gamma^{125},\gamma^{141},\gamma^{172},\gamma^{185},\gamma^{186},\gamma^{210},\gamma^{226}\}$
$\{\gamma^0,\gamma^9,\gamma^{32},\gamma^{35},\gamma^{37},\gamma^{85},\gamma^{94},\gamma^{117},\gamma^{120},\gamma^{122},\gamma^{170},\gamma^{179},\gamma^{202},\gamma^{205},\gamma^{207}\}$
$\{\gamma^0,\gamma^7,\gamma^{19},\gamma^{27},\gamma^{49},\gamma^{85},\gamma^{92},\gamma^{104},\gamma^{112},\gamma^{134},\gamma^{170},\gamma^{177},\gamma^{189},\gamma^{197},\gamma^{219}\}$
$\{\gamma^0,\gamma^{17},\gamma^{34},\gamma^{51},\gamma^{68},\gamma^{85},\gamma^{102},\gamma^{119},\gamma^{136},\gamma^{153},\gamma^{170},\gamma^{187},\gamma^{204},\gamma^{221},\gamma^{238}\}$.

Las primeras 35 órbitas son 3-cuasi órbitas completas con 85 subespacios y la última es una órbita con 17 subespacios. Este código $\mathscr{C}$ tiene parámetros $[8,4,2992,4]$. Tenga en cuenta que, a pesar del factor 1/3 garantizado por el Teorema V.2, este código tiene una gran cantidad de palabras de códigos. No tan lejos comparado con el código cíclico de Ejemplo III.6.

VI. Clasificación de Cuasi-órbitas en $\mathbb{F}_q^n$

Las siguientes tablas han sido calculadas usando el Sistema para Álgebra Computacional Discreta GAP y algunos algoritmos programados en lenguajes C++ y Java.

(1) $n = 6$, $m = 3$.

TABLA VII
Cuasi-Órbitas en $\mathbb{P}_2(6)$ con $m = 3$

Número de cuasi órbitas				Cuasi órbitas completas			
$k \setminus d$	2	4	6	$k \setminus d$	2	4	6
1	3	0	0	1	3	0	0
2	21	12	0	2	21	9	0
3	33	33	3	3	33	33	0

Hay seis 3-cuasi órbitas degeneradas: las tres primeras cuasi órbitas se componen de 3 subespacios de dimensión 3. Todos ellos tienen una distancia mínima de 6. Las

últimas tres cuasi órbitas consisten de 7 subespacios de dimensión 2. La distancia mínima en cada caso es 2.

(2) $n = 6$, $m = 7$.

TABLA VIII
CUASI-ÓRBITAS EN $\mathbb{P}_2(6)$ CON $m = 7$

Número de cuasi órbitas				Cuasi órbitas completas			
$k \setminus d$	2	4	6	$k \setminus d$	2	4	6
1	7	0	0	1	7	0	0
2	21	56	0	2	21	49	0
3	56	84	14	3	56	84	14

Hay siete 7-cuasi órbitas degeneradas: todas tienen dimensión 2 y distancia mínima 4.

(3) $n = 6$, $m = 9$.

TABLA IX
CUASI-ÓRBITAS EN $\mathbb{P}_2(6)$ CON $m = 9$

Número de cuasi órbitas				Cuasi órbitas completas			
$k \setminus d$	2	4	6	$k \setminus d$	2	4	6
1	9	0	0	1	9	0	0
2	9	81	0	2	9	81	0
3	0	126	72	3	0	126	72

Hay nueve 9-cuasi órbitas degeneradas con un subespacio de dimensión 3.

(4) $n = 6$, $m = 21$.

TABLA X
CUASI-ÓRBITAS EN $\mathbb{P}_2(6)$ CON $m = 21$

Número de cuasi órbitas				Cuasi órbitas completas			
$k \setminus d$	2	4	6	$k \setminus d$	2	4	6
1	21	0	0	1	21	0	0
2	0	210	0	2	0	210	0
3	105	0	357	3	105	0	357

Hay veintiún 21-cuasi órbitas degeneradas con un subespacio de dimensión 2.

(5) $n = 8$, $m = 3$.

TABLA XI
CUASI-ÓRBITAS EN $\mathbb{P}_2(8)$ CON $m = 3$

Cuasi órbitas completas		
$k \setminus d$	2	4
1	3	0
2	102	24
3	99	1044
4	96	2262

No hay 3-cuasi órbitas degeneradas.

(6) $n = 8$, $m = 5$.

TABLA XII
CUASI-ÓRBITAS EN $\mathbb{P}_2(8)$ CON $m = 5$

Número de cuasi órbitas				Cuasi órbitas completas			
$k \setminus d$	2	4	6	$k \setminus d$	2	4	6
1	5	0	0	1	5	0	0
2	120	95	0	2	120	90	0
3	225	1680	0	3	225	1680	0
4	120	3590	240	4	120	3570	240

Hay veinte 5-cuasi órbitas degeneradas con 17 subespacios de dimensión 4. Cada una tiene distancia mínima 4.

(7) $n = 8$, $m = 15$.

TABLA XIII
CUASI-ÓRBITAS EN $\mathbb{P}_2(8)$ CON $m = 15$

Número de cuasi órbitas			
$k \setminus d$	2	4	6
1	15	0	0
2	120	510	0
3	120	4380	1215
4	120	6000	5670

No hay 15-cuasi órbitas degeneradas.

(8) $n = 8$, $m = 17$.

TABLA XIV
CUASI-ÓRBITAS EN $\mathbb{P}_2(8)$ CON $m = 17$

Número de cuasi órbitas				
$k \setminus d$	2	4	6	8
1	17	0	0	0
2	34	697	0	0
3	357	2040	4080	0
4	0	4930	8160	340

Cuasi órbitas completas				
$k \setminus d$	2	4	6	8
1	17	0	0	0
2	34	680	0	0
3	357	2040	4080	0
4	0	4930	8160	272

Hay ciento dos 17-cuasi órbitas degeneradas: las primeras 85 están compuestas cada una de 5 subespacios; 17 de dimensión 2 y distancia mínima 4, y los 68 restantes tienen dimensión 4 y distancia mínima 8. Las últimas 17 tienen solo un subespacio de dimensión 4.

(9) $n = 8$, $m = 51$.

TABLA XV
CUASI-ÓRBITAS EN $\mathbb{P}_2(8)$ CON $m = 51$

Número de cuasi órbitas				
$k \setminus d$	2	4	6	8
1	51	0	0	0
2	102	2040	0	0
3	51	6120	13260	0
4	0	5610	32640	1836

No hay 51-cuasi órbitas degeneradas.

(10) $n = 8$, $m = 85$.

TABLA XVI
CUASI-ÓRBITAS EN $\mathbb{P}_2(8)$ CON $m = 85$

Número de cuasi órbitas				
$k \setminus d$	2	4	6	8
1	85	0	0	0
2	0	3570	0	0
3	1785	0	30600	0
4	0	17850	0	48960

Cuasi órbitas completas				
$k \setminus d$	2	4	6	8
1	85	0	0	0
2	0	3570	0	0
3	1785	0	30600	0
4	0	17850	0	48960

Hay cuatrocientas veinticinco 85-cuasi órbitas degeneradas con un solo subespacio: Las primeras 85 tienen dimensión 2 y las 340 restantes tiene dimensión 4.

(11) $n = 9$, $m = 7$.

TABLA XVII
CUASI-ÓRBITAS EN $\mathbb{P}_2(9)$ CON $m = 7$

Número de cuasi órbitas			
$k \setminus d$	2	4	6
1	7	0	0
2	210	385	0
3	210	10458	126
4	210	22512	22617

No hay 7-cuasi órbitas degeneradas.

(12) $n = 9$, $m = 73$.

TABLA XVIII
CUASI-ÓRBITAS EN $\mathbb{P}_2(9)$ CON $m = 73$

Número de cuasi órbitas				
$k \setminus d$	2	4	6	8
1	73	0	0	0
2	73	6132	0	0
3	0	9198	103368	0
4	657	6132	171696	294336

Cuasi órbitas completas				
$k \setminus d$	2	4	6	8
1	73	0	0	0
2	73	6132	0	0
3	0	9198	103368	0
4	657	6132	171696	294336

Hay setenta y tres 73-cuasi órbitas degeneradas con un subespacio de dimensión 3.

(13) $n = 10$, $m = 3$.

TABLA XIX
CUASI-ÓRBITAS EN $\mathbb{P}_2(10)$ CON $m = 3$

Número de cuasi órbitas					
$k \setminus d$	2	4	6	8	10
1	3	0	0	0	0
2	390	120	0	0	0
3	390	18225	0	0	0
4	378	75375	81837	0	0
5	375	98511	221412	0	3

Cuasi órbitas completas			
$k \setminus d$	2	4	6
1	3	0	0
2	390	120	0
3	390	18225	0
4	378	75375	81837
5	375	98511	221412

Hay tres 3-cuasi órbitas degeneradas con 11 subespacios de dimensión 5. Cada una tiene distancia mínima 10.

(14) $n = 10$, $m = 11$

TABLA XX
CUASI-ÓRBITAS EN $\mathbb{P}_2(10)$ CON $m = 11$

Número de cuasi órbitas					
$k \setminus d$	2	4	6	8	10
1	11	0	0	0	0
2	385	1496	0	0	0
3	1320	57475	9460	0	0
4	341	135410	442134	132	0
5	4257	107327	1059058	3784	11

Cuasi órbitas completas				
$k \setminus d$	2	4	6	8
1	11	0	0	0
2	385	1485	0	0
3	1320	57475	9460	0
4	341	135355	442134	0
5	4257	107327	1059058	3784

Hay once 11-cuasi órbitas degeneradas con 3 subespacios de dimensión 5, cada una de estas tiene distancia mínima 10. Existen once 11-cuasi órbitas degeneradas con 31 subespacios de dimensión 2, cada una con distancia mínima 4. A su vez hay cincuenta y cinco 11-cuasi órbitas degeneradas con 31 subespacios de dimensión 4, cada una de ellas con distancia mínima 4 y finalmente, hay ciento treinta y dos 11-cuasi órbitas degeneradas con 31 subespacios de dimensión 4, cada una de ellas con distancia mínima 8.

(15) $n = 10$, $m = 31$

TABLA XXI
CUASI-ÓRBITAS EN $\mathbb{P}_2(10)$ CON $m = 31$

Número de cuasi órbitas					
$k \setminus d$	2	4	6	8	10
1	31	0	0	0	0
2	465	4836	0	0	0
3	3100	93310	95945	0	0
4	465	231105	1366542	30845	0
5	11532	132680	2816474	348998	62

Cuasi órbitas completas					
$k \setminus d$	2	4	6	8	10
1	31	0	0	0	0
2	465	4805	0	0	0
3	3100	93310	95945	0	0
4	465	230950	1366542	30473	0
5	11532	132680	2816474	348998	62

Existen treinta y un 31-cuasi órbitas degeneradas con 11 subespacios de dimensión 2, cada una de estas tiene distancia mínima 4. Por otro lado hay ciento cincuenta y cinco 31-cuasi órbitas degeneradas con 11 subespacios de dimensión 4, cada una con distancia mínima 4 y finalmente, hay trescientos setenta y dos 31-cuasi órbitas degeneradas con 11 subespacios de dimensión 4, cada una de ellas con distancia mínima 8.

(16) $n = 10$, $m = 33$

TABLA XXII
CUASI-ÓRBITAS EN $\mathbb{P}_2(10)$ CON $m = 33$

Número de cuasi órbitas					
$k \setminus d$	2	4	6	8	10
1	33	0	0	0	0
2	165	5445	0	0	0
3	165	40920	163680	0	0
4	33	47685	1227600	458172	0
5	0	42966	1514040	1964160	2112

Cuasi órbitas completas					
$k \setminus d$	2	4	6	8	10
1	33	0	0	0	0
2	165	5445	0	0	0
3	165	40920	163680	0	0
4	33	47685	1227600	458172	0
5	0	42966	1514040	1964160	2112

Hay treinta y tres 33-cuasi órbitas degeneradas con un subespacio de dimensión 5.

(17) $n = 10$, $m = 93$

TABLA XXIII
CUASI-ÓRBITAS EN $\mathbb{P}_2(10)$ CON $m = 93$

Número de cuasi órbitas					
$k \setminus d$	2	4	6	8	10
1	93	0	0	0	0
2	465	15345	0	0	0
3	465	110670	465930	0	0
4	465	130665	3193806	1560354	0
5	465	136245	4194207	5572095	26226

No hay 93-cuasi órbitas degeneradas.

(18) $n = 10$, $m = 341$

TABLA XXIV
CUASI-ÓRBITAS EN $\mathbb{P}_2(10)$ CON $m = 341$

Número de cuasi órbitas					
$k \setminus d$	2	4	6	8	10
1	341	0	0	0	0
2	0	57970	0	0	0
3	28985	0	2086920	0	0
4	0	1217370	0	16695360	0
5	121737	0	10434600	0	25850869

Cuasi órbitas completas					
$k \setminus d$	2	4	6	8	10
1	341	0	0	0	0
2	0	57970	0	0	0
3	28985	0	2086920	0	0
4	0	1217370	0	16695360	0
5	121737	0	10434600	0	25850869

Hay seis mil ciento treinta y ocho 341-cuasi órbitas degeneradas con un subespacio: las primeras 341 tienen dimensión 2, y las 5797 restantes tienen dimensión 4.

VII. DUALIDAD

Consideremos ahora el producto interno usual $(\cdot, \cdot)$ definido sobre $\mathbb{F}_q^n$, esto es, para $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$ en $\mathbb{F}_q^n$

$$(x, y) = \sum_{j=0}^{n} x_j y_j. \tag{VII.1}$$

Si $U \in G_q(n, k)$, entonces el `complemento ortogonal` de U es el subespacio $(n-k)$-dimensional de $\mathbb{F}_q^n$ definido como sigue:

$$U^{\perp} = \{x \in \mathbb{F}_q^n \mid (u, x) = 0, \forall u \in U\}. \tag{VII.2}$$

Definición VII.1 *Si $\mathscr{C}$ es un código de red, entonces el `código dual` de $\mathscr{C}$, notado con $\mathscr{C}^{\perp}$, es definido por*

$$\mathscr{C}^{\perp} = \{V^{\perp} \mid V \in \mathscr{C}\} \subseteq \mathbb{P}_q(n). \tag{VII.3}$$

Se sabe que la distancia entre los subespacios U y V se refleja en la distancia entre los subespacios ortogonales $U^{\perp}$ y $V^{\perp}$.

Lema VII.2 (Dualidad) *[6, Lemma 13] Si $\mathscr{C}$ es un código de red con parámetros $[n, k, |\mathscr{C}|, d]$, entonces el código dual $\mathscr{C}^{\perp}$ tiene parámetros $[n, n-k, |\mathscr{C}|, d]$.*

Observación VII.3 *En la teoría clásica de códigos se verifica que, si C es un $[n, k]$-código cíclico sobre $\mathbb{F}_q$, entonces su dual $C^{\perp}$ también lo es. Como podemos ver a continuación, esto no es cierto en el contexto de los códigos de subespacios.*

Ejemplo VII.4 *Sea γ una raíz primitiva de $x^6 + x^4 + x^3 + x + 1$ y use este polinomio para generar el cuerpo $\mathbb{F}_{2^6}$. A continuación presentamos el código de extensión*

$$\mathscr{C} = \{\alpha \mathbb{F}_{2^3} \mid \alpha \in \mathbb{F}_{2^6}^*\} \tag{VII.4}$$

y su correspondiente código dual $\mathscr{C}^{\perp}$.

$$\begin{aligned}\mathscr{C} = \{&\{\gamma^0,\gamma^9,\gamma^{18},\gamma^{27},\gamma^{36},\gamma^{45},\gamma^{54}\},\\ &\{\gamma^1,\gamma^{10},\gamma^{19},\gamma^{28},\gamma^{37},\gamma^{46},\gamma^{55}\},\\ &\{\gamma^2,\gamma^{11},\gamma^{20},\gamma^{29},\gamma^{38},\gamma^{47},\gamma^{56}\},\\ &\{\gamma^3,\gamma^{12},\gamma^{21},\gamma^{30},\gamma^{39},\gamma^{48},\gamma^{57}\},\\ &\{\gamma^4,\gamma^{13},\gamma^{22},\gamma^{31},\gamma^{40},\gamma^{49},\gamma^{58}\},\\ &\{\gamma^5,\gamma^{14},\gamma^{23},\gamma^{32},\gamma^{41},\gamma^{50},\gamma^{59}\},\\ &\{\gamma^6,\gamma^{15},\gamma^{24},\gamma^{33},\gamma^{42},\gamma^{51},\gamma^{60}\},\\ &\{\gamma^7,\gamma^{16},\gamma^{25},\gamma^{34},\gamma^{43},\gamma^{52},\gamma^{61}\},\\ &\{\gamma^8,\gamma^{17},\gamma^{26},\gamma^{35},\gamma^{44},\gamma^{53},\gamma^{62}\}\}.\end{aligned}$$

$$\begin{aligned}\mathscr{C}^{\perp} = \{&\{\gamma^3,\gamma^{17},\gamma^{19},\gamma^{22},\gamma^{32},\gamma^{47},\gamma^{51}\},\\ &\{\gamma^{12},\gamma^{23},\gamma^{27},\gamma^{34},\gamma^{35},\gamma^{46},\gamma^{58}\},\\ &\{\gamma^{16},\gamma^{45},\gamma^{52},\gamma^{53},\gamma^{59},\gamma^{60},\gamma^{61}\},\\ &\{\gamma^4,\gamma^8,\gamma^{10},\gamma^{30},\gamma^{39},\gamma^{54},\gamma^{57}\},\\ &\{\gamma^1,\gamma^5,\gamma^{25},\gamma^{36},\gamma^{42},\gamma^{48},\gamma^{62}\},\\ &\{\gamma^0,\gamma^2,\gamma^6,\gamma^{26},\gamma^{37},\gamma^{43},\gamma^{49}\},\\ &\{\gamma^7,\gamma^9,\gamma^{13},\gamma^{33},\gamma^{44},\gamma^{50},\gamma^{56}\},\\ &\{\gamma^{11},\gamma^{14},\gamma^{20},\gamma^{24},\gamma^{38},\gamma^{40},\gamma^{55}\},\\ &\{\gamma^{15},\gamma^{18},\gamma^{21},\gamma^{28},\gamma^{29},\gamma^{31},\gamma^{41}\}\}.\end{aligned}$$

Se puede ver que el código dual $\mathscr{C}^{\perp}$ no es cíclico.

Los siguientes ejemplos muestran que en general la búsqueda de códigos auto-duales puede ser poco interesante, los códigos encontrados poseen parámetros muy pequeños.

Ejemplo VII.5 *Sea γ una raíz primitiva de x^4+x+1 y use este polinomio para generar el cuerpo $\mathbb{F}_{2^4}$.*

(1) El código $\mathscr{C}$ dado por

$$\begin{aligned}\mathscr{C} = \{&\{\gamma^2,\gamma^3,\gamma^6\},\{\gamma^5,\gamma^6,\gamma^9\},\{\gamma^8,\gamma^9,\gamma^{12}\},\\ &\{\gamma^0,\gamma^{11},\gamma^{12}\},\{\gamma^0,\gamma^3,\gamma^{14}\}\}\end{aligned}$$

es un código 3-cuasi cíclico con parámetros $[4,2,5,2]$.

(2) El código $\mathscr{C}$ dado por

$$\mathscr{C} = \{\{\gamma^2,\gamma^7,\gamma^{12}\},\{\gamma^4,\gamma^9,\gamma^{14}\}\}. \quad \text{(VII.5)}$$

es un código 5-cuasi cíclico con parámetros $[4,2,2,4]$. Este es el único código 5-cuasi cíclico auto-dual en el espacio proyectivo $\mathbb{P}_2(4)$.

Ejemplo VII.6 *Sea γ una raíz primitiva de $x^8+x^4+x^3+x^2+1$ y use este polinomio para generar el cuerpo $\mathbb{F}_{2^8}$. Sea*

$$\begin{aligned}\mathscr{C} = \{&\{\gamma^{27},\gamma^{34},\gamma^{46},\gamma^{54},\gamma^{76},\gamma^{112},\gamma^{119},\gamma^{131},\gamma^{139},\gamma^{161},\\ &\gamma^{197},\gamma^{204},\gamma^{216},\gamma^{224},\gamma^{246}\},\{\gamma^5,\gamma^{27},\gamma^{63},\gamma^{70},\gamma^{82},\\ &\gamma^{90},\gamma^{112},\gamma^{148},\gamma^{155},\gamma^{167},\gamma^{175},\gamma^{197},\gamma^{233},\gamma^{240},\gamma^{252}\}\}.\end{aligned}$$

Entonces $\mathscr{C}$ es el único código 85-cuasi cíclico auto-dual en el espacio proyectivo $\mathbb{P}_2(8)$, con parámetros $[8,4,2,4]$.

VIII. Métodos para Construir Códigos Grassmannianos Cíclicos

Para realizar los cálculos que originaron todos los códigos anteriores se realizó el siguiente procedimiento:

(1) Hallar todas las órbitas de la Grassmanniana $G_q(n,k)$, llamemos ese conjunto $\mathfrak{O}$. Esto es,

$$\mathcal{O} := \{\mathcal{O}rb(V) \mid V \in G_q(n,k)\}. \quad \text{(VIII.1)}$$

(2) Se calcula de manera independiente la distancia mínima de cada órbita. Es decir, se calcula

$$d_{\mathcal{O}rb(\cdot)} := \min\{d(v,w) \mid v \neq w \in \mathcal{O}rb(\cdot)\}, \quad \text{(VIII.2)}$$

para toda $\mathcal{O}rb(V) \in \mathcal{O}$, con d la distancia de subespacios y construimos las parejas $(\mathcal{O}rb(\cdot), d_{\mathcal{O}rb(\cdot)})$.

(3) Se fija una distancia mínima d, para la cual se quiere obtener el código cíclico.

(4) Se construye el grafo $\mathcal{G} = (\mathcal{O}, \mathcal{E})$, donde $\mathcal{E}$ es el conjunto de aristas. Dos órbitas son adyacentes, si la unión de estas tiene distancia mínima mayor o igual a d. Es decir,

$$\begin{aligned}\mathcal{E} = \{&\{\mathcal{O}rb(\cdot),\mathcal{O}rb(*)\} \mid d_{\mathcal{O}rb(\cdot)}, d_{\mathcal{O}rb(*)} \geq d,\\ &d(v,w) \geq d,\ \forall v \in \mathcal{O}rb(\cdot), w \in \mathcal{O}rb(*)\}.\end{aligned}$$

En los pasos siguientes de la construcción juegan un papel importante los conceptos de `clique` y `número de clique` en un grafo. Precisamos estas definiciones:

Definición VIII.1 *Sea $G=(V,E)$ un grafo.*

(1) Un `clique` en G es un subconjunto de V en el cual cada par de vértices es adyacente.

(2) La cantidad de vértices del clique más grande en G se denomina `número de clique` de G.

Como consecuencia inmediata de la construcción anterior tenemos el siguiente resultado:

Teorema VIII.2 *Sea $\mathscr{C}$ un clique en el grafo G construido en el item (4). Entonces $\mathscr{C}$ es un código cíclico con distancia mínima d y dimensión constante k.*

(5) Se obtienen cliques del grafo para obtener códigos cíclicos.

(6) Para determinar los valores máximos de cada α_t de la igualdad (III.9), se separa el grafo en subgrafos independientes por el numero de espacios en sus órbitas (Cada vértice en cada subgrafo con la misma cantidad de espacios asociados) y se calcula el numero de clique en cada uno, Este número de clique representa el valor máximo del α_i asociado.

IX. Software Utilizados

1) Los espacios vectoriales son calculados con GAP.
2) La construcción de las órbitas y del grafo son calculados con Java y algoritmos diseñados e implementados en C++.
3) Los cliques son calculados con Wolfram Mathematica.

X. Conclusión

En este artículo se han presentado algunas clasificaciones de órbitas y cuasi-órbitas completas y degeneradas de un subespacio en el espacio proyectivo $\mathbb{P}_q(n)$, hasta $n=11$. Además, se definen los códigos de subespacio m-cuasi cíclicos, como una generalización natural de los códigos de subespacios cíclicos y se muestra una clasificación de algunas m-cuasi órbitas. Es conocido en la literatura algunos métodos teóricos para construir códigos de subespacios y en particular

códigos Grassmannianos [2], [18], [17], [21], algunos de ellos usan polinomios linealizados, o acciones de grupos sobre Grassmannianas, no ibstante esta clasificación presentada de órbitas para facilitar la costrucción de códigos Grassmannianos cíclicos es novedosa.

Para futuras investigaciones, consideramos la acción definida de $\mathrm{Sym}(q^k-1)$ sobre la Grassmanniana $G_q(n,k)$, como una generalización de los códigos cíclicos y códigos Grassmannianos cuasi-cíclicos para construir nuevos códigos. Concretamente, si γ es un elemento primitivo del cuerpo finito $\mathbb{F}_{q^n}$ y $\sigma \in \mathrm{Sym}(q^k-1)$. Un código $\mathscr{C} \subseteq G_q(n,k)$ es denominado σ-código, si se verifica la siguiente propiedad:

$$\{0,\gamma^{i_1},\ldots,\gamma^{i_s}\} \in \mathscr{C} \Rightarrow \{0,\gamma^{\sigma(i_1)},\ldots,\gamma^{\sigma(i_s)}\} \in \mathscr{C}, \quad \text{(X.1)}$$

asumiendo que $s = q^k - 1$, con k la dimensión de una palabra de código.

REFERENCIAS

[1] R. Ahlswede, N. Cai, Shuo-Yen, R. Li, and R. W. Yeung. Network information flow. *IEEE Transactions on Information Theory*, 46(4), July 2000.

[2] E. Ben-Sasson, T. Etzion, A. Gabizon, and N. Raviv. Subspace polynomials and cyclic subspace codes. *IEEE Transactions on Information Theory*, 62(3):1157 – 1165, March 2016.

[3] B. Chen and H. Liu. Constructions of cyclic constant dimension codes. *Designs, Codes and Cryptography*, 86(6):1267 – 1279, 2018.

[4] P. A. Chou, Y. Wu, and K. Jain. Practical network coding. *Proc. 2003 Allerton Conf. Communications, Control and Computing, Monticello*, 25(IL), Octuber 2003.

[5] T. Etzion and S. R. Blackburn. The asymptotic behavior of grassmannian codes. *IEEE Transactions on Information Theory*, 58(10):6605–6609, October 2012.

[6] T. Etzion and A. Vardy. Error-correcting codes in projective space. *IEEE Transactions on Information Theory*, 57(2):1165 – 1173, 2011.

[7] C. Fragouli, J.-Y. L. Boudec, and J. Widmer. Network coding: An instant primer. *ACM SIGCOMM Computer Communication Review*, 36:63–68, 2006.

[8] GAP. Groups, algorithms, programming - a system for computational discrete algebra. http://www.gapsystem.org/.

[9] H. Gluesing-Luerssen, K. Morrison, and C. Troha. Cyclic orbit codes and stabilizer subfields. *Advances in Mathematics of Communications*, 9(2):177–197, May 2015.

[10] I. Gutierrez, M. Falco, J. Marquez, and S. Valle. Packet output and input configuration in a multicasting session using network coding. *KSII Transactions on Internet and Information Systems*, 13(2):686–710, 2019.

[11] I. Gutierrez and J. Marquez. Coding and decoding packet ia a multicast network: Programming test. *IEEE Lantin America Transactions*, 16(2):598–603, 2018.

[12] D. Heinlein, M. Kiermaier, S. Kurz, and A. Wassermann. Tables of subspace codes. *arXiv preprint arXiv:1601.02864*, 2016.

[13] T. Ho, R. Koetter, M. Médard, D. Karger, and M. Effros. The benefits of coding over routing in a randomized setting. *Proc. 2003 IEEE Int. Symp. on Inform. Theory (Yokohama)*, page 442, June 29 - July 4 2003.

[14] T. Ho, M. Médard, R. Koetter, D. Karger, M. Effros, J. Shi, and B. Leong. A random linear network coding approach to multicast. *IEEE Trans. on Inform. Theory*, 52:4413 – 4430, Oct 2006.

[15] A.-L. Horlemann-Trautmann, K. Marshall, and J. Rosenthal. Considerations for rank-based cryptosystems. *(ISIT), 2016 IEEE International Symposium on Information Theory*, 2016.

[16] R. Koetter and F. R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Transactions on Information Theory*, 54:3579 – 3591, 2008.

[17] A. Kohnert and S. Kurz. Construction of large constant dimension codes with a prescribed minimum distance. *Mathematical Methods in Computer Science. Lecture Notes in Computer Science*, 5393:31–42, 2008.

[18] K. Otal and F. Özbudak. Cyclic subspace codes via subspace polynomials. *Designs, Codes and Cryptography*, 85(2):191 – 204, 2017.

[19] J. Pääkkönen, C. Hollanti, D. Prathapasinghe, and O. Tirkkonen. Distributed storage for proximity based services. *In IEEE Communication Technologies Workshop (SweCTW)*, 35:30–35, 2012.

[20] J. Pääkkönen, C. Hollanti, and O. Tirkkonen. Device-to-device data storage for mobile cellular systems. *IEEE In Globecom Workshops (GC Wkshps)*, 35:671–676, 2013.

[21] A.-L. Trautmann, F. Manganiello, M. Braun, and J. Rosenthal. Cyclic orbit codes. *IEEE Transactions on Information Theory*, 59:7386–7404, 2013.

Ismael Gutierrez Garcia, Licenciado en Matemáticas y Física de la Universidad del Atlántico, recibió su título de Magister en Matemáticas en Universidad del Norte – Universidad del Valle, el grado de Dr. rer. nat. En la Universidad Johannes Gutenberg de Mainz - Alemania. Sus áreas de interés son los Grupos finitos soluble, las aplicaciones de cuerpos finitos en codificación lineal aleatoria en redes.

Ivan Molina Naizir, recibió el título de Matemático en 2014 en la Universidad del Norte y Magister en Ingeniería de Sistemas de la misma Universidad en 2015. Sus áreas de interés son las matemáticas discretas y las ciencias de la computación.