IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 3, 2020, accepted March 10, 2020, date of publication March 13, 2020, date of current version March 24, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2980670

Finding Cliques in Projective Space: A Method for Construction of Cyclic Grassmannian Codes

ISMAEL GUTIÉRREZ-GARCÍA AND IVAN MOLINA NAIZIR
Department of Mathematics and Statistics, Universidad del Norte, Barranquilla 080001, Colombia

Corresponding author: Ismael Gutiérrez-García (isgutier@uninorte.edu.co)

This work was supported by the Universidad del Norte.

ABSTRACT In general, the construction of subspace codes or, in particular, cyclic Grassmannian codes in some projective space $\mathbb{P}_q(n)$ is highly mathematical and requires substantial computational power for the resulting searches. In this paper, we present a new method for the construction of cyclic Grassmannian codes. To do that was designed and implemented a series of algorithms using the GAP System for Computational Discrete Algebra and Wolfram Mathematica software. We also present a classification of such codes in the space $\mathbb{P}_q(n)$, with n at most 9. The fundamental idea to construct and classify the cyclic Grassmannian codes is to endow the projective space $\mathbb{P}_q(n)$ with a graph structure and then find cliques.

INDEX TERMS Cliques, cyclic codes, finite fields, Grassmannian codes, orbits, projective space, subspace codes.

I. INTRODUCTION

Similar to classical coding theory, there are two main directions for research in network coding: The existence and construction of subspace codes, in particular, Grassmannian codes and the design of efficient coding and decoding schemes for a given subspace code.

From a mathematical and computer science point of view, four major sub-themes have been considered for research

- Construction of subspace codes, Grassmannian codes and cyclic Grassmannian codes.
- Determination of bounds for code size in terms of the code parameters and the size of the ground field.
- Practical aspects of network coding.
- Subspace codes based Cryptography.

Cyclic Grassmannian codes were first presented by Kohnert and Kurz in [6] from the perspective of design theory over finite fields. Later Etzion and Vardy in [3] defined them as a q-analog of cyclic code from the classical coding theory. Trautmann *et al.* [8] and Gluesing-Luerssen *et al.* [4] studied cyclic codes from the point of view of groups actions. Specifically, they have used an action of the general linear group over a Grassmannian to define them: these codes were called cyclic orbits codes. Cyclic Grassmannian codes are a special case of orbits codes.

The associate editor coordinating the review of this manuscript and approving it for publication was Guangjie Han.

Recently Ben-Sasson *et al.* [1], Otal and Özbudak [7], Niu *et al.* [9], and Chen and Liu [2] presented new methods for constructing such codes, what includes linearized polynomials, namely subspace polynomials and Frobenius mappings. A computational method for construction of cyclic Grassmannian codes was presented in [5].

Let $\mathbb{F}_{q^n}$ be the extension field, of degree n, of the finite field with q elements, $\mathbb{F}_q$ (where q is a prime power). It is well known that we may regard $\mathbb{F}_{q^n}$ as a vector space of dimension n over $\mathbb{F}_q$. That is, for a fixed basis, we can identify every element of $\mathbb{F}_{q^n}$ with a n-tuple of elements in $\mathbb{F}_q$. Therefore, we will not distinguish between $\mathbb{F}_{q^n}$ and $\mathbb{F}_q^n$. We denote with $\mathbb{P}_q(n)$ the projective space of order n, that is, the set of all subspaces of $\mathbb{F}_q^n$, including the null space and $\mathbb{F}_q^n$ itself.

For a fixed natural number k, with $0 \leq k \leq n$ we denote with $G_q(n, k)$ the set of all subspaces of $\mathbb{F}_q^n$ of dimension k and we call it the k-Grassmannian over $\mathbb{F}_q$ or Grassmannian in short. We say that $\mathscr{C} \subseteq G_q(n, k)$ is an $(n, M, d, k)_q$ Grassmannian code if $|\mathscr{C}| = M$ and $d(X, Y) \geq d$ for all distinct $X, Y \in \mathscr{C}$. Such a code is also called a constant dimension code.

Let $\mathcal{A}_q(n, d, k)$ and $\mathcal{C}_q(n, d, k)$ be the maximum number of codewords in an $(n, M, d, k)_q$ Grassmannian code over the filed $\mathbb{F}_q$ and the maximum number of codewords in an $(n, M, d, k)_q$ cyclic code over $\mathbb{F}_q$, respectively. It is clear that $\mathcal{C}_q(n, d, k) \leq \mathcal{A}_q(n, d, k)$.

Let $\alpha \in \mathbb{F}^*_{q^n}$ and $V \in G_q(n,k)$. The `cyclic shift` of V is defined as follows:

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

Clearly αV is a subspace belonging to $G_q(n,k)$. That is, it has the same dimension as V. A Grassmannian code $\mathscr{C} \subseteq G_q(n,k)$ is called `cyclic`, if for all $\alpha \in \mathbb{F}^*_{q^n}$ and all subspace $V \in \mathscr{C}$ we have that $\alpha V \in \mathscr{C}$. The set

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

is called the `orbit` of V. Observe that in this definition the zero vector was omitted from the set of an orbit. Starting now, this will be explicitly deleted when we specify the elements of a codeword of a cyclic Grassmannian code.

If $V \in G_q(n,k)$, then $|\mathcal{O}rb(V)| = \frac{q^n-1}{q^t-1}$, for some natural number t, which divides n, see [1, Lemma 9]. An immediate consequence of this result is presented in the following theorem.

Theorem 1: The maximum number of codewords in an $(n, M, d, k)_q$ cyclic Grassmannian code is given by

$$\mathcal{C}_q(n,d,k) = \sum_{t|n} \alpha_t \frac{q^n-1}{q^t-1} \tag{I.3}$$

for some integer $0 \le \alpha_t$.

II. CLIQUES CONSTRUCTION

A clique in an undirected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ is a subset of $\mathcal{V}$, such that every two distinct vertices are adjacent. The clique of the largest possible size is referred to as a maximum clique; that is, it cannot be extended by including one more adjacent vertex. The clique number $\omega(\mathcal{G})$ of $\mathcal{G}$ is the number of vertices in a maximum clique in $\mathcal{G}$. A clique of size k is called a k-clique.

To calculate the coefficients α_t in the previous theorem we proceed as follows:

(1) Find all the orbits of $G_q(n,k)$ and denote this set by $\mathcal{V}$. That is,

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

(2) Calculate the minimum subspace distance $d_{\mathcal{O}rb(\cdot)}$ of each orbit independently; then we form the pair $(\mathcal{O}rb(\cdot), d_{\mathcal{O}rb(\cdot)})$.

(3) A minimum distance d is fixed, for which we want to obtain a cyclic code.

(4) The graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ is constructed so that the set $\mathcal{E}$ of edges is obtained in the following way: two orbits are adjacent if their union has a minimum distance greater or equal than d.

(5) A clique in the graph $\mathcal{G}$ constructed in (4) is a Grassmannian cyclic code with minimum distance d and dimension k.

(6) To determine the maximum values of each α_t, the graph $\mathcal{G}$ is separated into independent subgraphs by the number of spaces in their orbits (every vertex in each subgraph with the same number of associated spaces), and the number of cliques in each one is calculated.

Algorithm 1 The Algorithm That Calculates All the Cyclic Codes of a Grassmannian

Data: d: the minimum distance required for the code
Result: Grassmannian cyclic codes with minimum distance d.
Let $V := \{O \subseteq G_q(n,k) \mid O \text{ is an orbit}\}$;
$E \leftarrow \{\}$;
forall the $O_1 \in V$ **do**
    forall the $O_2 \in V \setminus \{O_1\}$ **do**
        if $d_{O_1} \ge d$ ***and*** $d_{O_2} \ge d$ ***and*** $D(O_1, O_2) \ge d$ **then**
            $E \leftarrow E \cup \{(O_1, O_2)\}$;
We define G as the graph of orbits;
$G \leftarrow (V, E)$;
forall the C *in Cliques(G)* **do**
    print(C);

Algorithm 2 Algorithm That Calculates the Upper Bounds of the Values of α_t

Data: n, d, k, q, t
Result: A bound for α_t
Let $V := \{O \subseteq G_q(n,k) \mid O \text{ is an orbit}$ **and** $|O| = \frac{q^n-1}{q^t-1}\}$;
$E \leftarrow \{\}$;
forall the $O_1 \in V$ **do**
    forall the $O_2 \in V \setminus \{O_1\}$ **do**
        if $d_{O_1} \ge d$ ***and*** $d_{O_2} \ge d$ ***and*** $D(O_1, O_2) \ge d$ **then**
            $E \leftarrow E \cup \{(O_1, O_2)\}$;
We define G as the graph of orbits;
$G \leftarrow (V, E)$;
print("$\alpha_t \le$",NumeroDeClique(G));

Remark 2: To perform the previous algorithm we use:

(1) GAP to calculate all the vector spaces over the field $\mathbb{F}_q$;
(2) Java to construct the orbits and graph $\mathcal{G}$;
(3) Wolfram Mathematica to calculate the cliques.

III. CLASSIFICATION OF BINARY GRASSMANNIAN CODES OF LENGTH SMALLER THAN 6

Theorem 3: $\mathcal{C}_2(4,4,2) = 5$.

Proof: Let α be a primitive root of $x^4 + x + 1$ and use this polynomial to generate the field $\mathbb{F}_{2^4}$. Let $\mathscr{C} \subseteq G_2(4,2)$ which consists of all cyclic shifts of

$$\{\alpha^0, \alpha^5, \alpha^{10}\}.$$

This code $\mathscr{C}$ is an $[4,5,4,2]$-cyclic code. It consists of a unique orbit with 5 subspaces. □

Theorem 4: If $n < 6$ then $\mathcal{C}_2(n,4,k) = 0$.

Proof: The unique orbit with minimum distance 4 and $n < 6$ was presented in the previous theorem. □

IV. CLASSIFICATION OF BINARY GRASSMANNIAN CODES OF LENGTH 6

A. CALCULATING THE NUMBER $\mathcal{C}_2(6, 6, 3)$

It follows from Theorem 1 that

$$\mathcal{C}_2(6, 6, 3) = 63\alpha_1 + 21\alpha_2 + 9\alpha_3.$$

Lemma 5: Let $\mathscr{C} \subseteq G_2(6, 3)$ a cyclic code with minimum distance 6. Then

(1) $\alpha_1 \leq 0$
(2) $\alpha_2 \leq 0$
(3) $\alpha_3 \leq 1$

Proof: There are not orbits with minimum distance 6 having 63 or 21 subspaces. There is a single orbit with minimum distance 6 and nine subspaces. □

Theorem 6: $\mathcal{C}_2(6, 6, 3) = 9$.

Proof: Let α be a primitive root of $x^6 + x^4 + x^3 + x + 1$ and use this polynomial to generate the field $\mathbb{F}_{2^6}$. Let $\mathscr{C} \subseteq G_2(6, 3)$ which consists of all cyclic shifts of

$$\{\alpha^0, \alpha^9, \alpha^{18}, \alpha^{27}, \alpha^{36}, \alpha^{45}, \alpha^{54}\}.$$

This code $\mathscr{C}$ is an [6, 9, 6, 3]-cyclic code. It consists of a unique orbit with nine subspaces. □

B. CALCULATING THE NUMBER $\mathcal{C}_2(6, 4, 3)$

It follows from Theorem 1 that

$$\mathcal{C}_2(6, 4, 3) = 63\alpha_1 + 21\alpha_2 + 9\alpha_3.$$

Lemma 7: Let $\mathscr{C} \subseteq G_2(6, 3)$ a cyclic code with minimum distance 4. Then

(1) $\alpha_1 \leq 1$
(2) $\alpha_2 \leq 0$
(3) $\alpha_3 \leq 1$

Proof: The constructed graph with these parameters is the null graph. That is an edge-less graph. Therefore the clique number is one. There are no orbits with 21 subspaces and minimum distance 4. □

Lemma 8: $\alpha_1 + \alpha_3 = 1$

Proof: The combined constructed graph with the orbits with 63 and 21 subspaces is the null graph. Then the cyclic Grassmannian code has an orbit of 63 subspaces or an orbit of 9 subspaces but not both. □

Theorem 9: $\mathcal{C}_2(6, 4, 3) = 63$.

Proof: Let α be a primitive root of $x^6 + x^4 + x^3 + x + 1$ and use this polynomial to generate the field $\mathbb{F}_{2^6}$. Let $\mathscr{C} \subseteq G_2(6, 3)$ which consists of all cyclic shifts of

$$\{\alpha^0, \alpha^6, \alpha^{15}, \alpha^{26}, \alpha^{33}, \alpha^{34}, \alpha^{38}\}.$$

This code $\mathscr{C}$ is an [6, 63, 6, 3]-cyclic code. It consists of a unique orbit with 63 subspaces. □

TABLE 1. Values for $\mathcal{C}_2(6, d, k)$.

$d \setminus k$	2	3
4	21	63
6	0	9

TABLE 2. Values for $\mathcal{C}_2(7, d, k)$.

$d \setminus k$	2	3
4	0	254
6	0	0

C. CALCULATING THE NUMBER $\mathcal{C}_2(6, 4, 2)$

It follows from Theorem 1 that

$$\mathcal{C}_2(6, 4, 2) = 63\alpha_1 + 21\alpha_2 + 9\alpha_3.$$

Lemma 10: Let $\mathscr{C} \subseteq G_2(6, 2)$ a cyclic code with minimum distance 4. Then

(1) $\alpha_1 \leq 0$
(2) $\alpha_2 \leq 1$
(3) $\alpha_3 \leq 0$

Proof: There are not orbits with minimum distance 4 having 63 or 9 subspaces. The associate graph with the orbits of 21 subspaces is the null graph. □

Theorem 11: $\mathcal{C}_2(6, 4, 2) = 21$.

Proof: Let α be a primitive root of $x^6 + x^4 + x^3 + x + 1$ and use this polynomial to generate the field $\mathbb{F}_{2^6}$. Let $\mathscr{C} \subseteq G_2(6, 2)$ which consists of all cyclic shifts of

$$\{\alpha^0, \alpha^{21}, \alpha^{42}\}.$$

This code $\mathscr{C}$ is an [6, 21, 4, 2]-cyclic code. It consists of a unique orbit with 21 subspaces. □

V. CLASSIFICATION OF BINARY GRASSMANNIAN CODES OF LENGTH 7

A. CALCULATING THE NUMBER $\mathcal{C}_2(7, 4, 3)$

It follows from Theorem 1 that

$$\mathcal{C}_2(7, 4, 3) = 127\alpha_1.$$

Lemma 12: For a cyclic code $\mathscr{C} \subseteq G_2(7, 3)$ with minimum distance 4 holds that $\alpha_1 \leq 2$.

Proof: The figure above illustrates this result. We can see that there are various cliques and the big one has two vertices, that is two orbits of 127 subspaces. □

Theorem 13: $\mathcal{C}_2(7, 4, 3) = 254$.

Proof: Let α be a primitive root of $x^7 + x + 1$ and use this polynomial to generate the field $\mathbb{F}_{2^7}$. Let $\mathscr{C} \subseteq G_2(7, 3)$ which consists of all cyclic shifts of

$$\{\alpha^0, \alpha^4, \alpha^9, \alpha^{28}, \alpha^{38}, \alpha^{58}, \alpha^{90}\}$$
$$\{\alpha^0, \alpha^8, \alpha^{23}, \alpha^{39}, \alpha^{56}, \alpha^{82}, \alpha^{100}\}.$$

This code $\mathscr{C}$ is an [8, 254, 4, 3]-cyclic code. It consists of two orbits with 127 subspaces. □

VI. CLASSIFICATION OF BINARY GRASSMANNIAN CODES OF LENGTH 8

A. CALCULATING THE NUMBER $\mathcal{C}_2(8, 4, 4)$

It follows from Theorem 1 that

$$\mathcal{C}_2(8, 4, 4) = 255\alpha_1 + 85\alpha_2 + 17\alpha_4.$$

Lemma 14: Let $\mathscr{C} \subseteq G_2(8, 4)$ a cyclic code with minimum distance 4. Then
(1) $\alpha_1 \leq 17$;
(2) $\alpha_2 \leq 4$;
(3) $\alpha_4 \leq 1$.

Proof: The graph formed only by the orbits of 255 subspaces has a clique of 17 vertices, and there is no clique of greater size. In the same way, the graph formed by the orbits of 85 subspaces and the orbits of 17 subspaces is the null graph. □

Lemma 15: If $\alpha_4 = 1$ then $\alpha_1 + \alpha_2 \leq 3$

Proof: Fixing the orbit of 17 subspaces in all cliques, then the combined graph formed by the orbits of 255 subspaces and 85 subspaces do not contain a clique with more than four vertices. □

Theorem 16: $\mathcal{C}_2(8, 4, 4) \leq 4675$.

Proof: It follows directly from the two previous lemmas. □

Lemma 17: If $\alpha_2 = 4$ then $\alpha_1 \leq 16$.

Proof: Similar to the previous theorem, but now we fix the clique of four orbits with 85 subspaces. This procedure is made for every combination of four orbits of 85 subspaces that form a clique. □

Theorem 18: There is a cyclic code with 4420 codewords. That is, $\alpha_2 = 4$ and $\alpha_1 = 16$.

Proof: Let α be a primitive root of $x^8+x^4+x^3+x^2+1$ and use this polynomial to generate the field $\mathbb{F}_{2^8}$. Let $\mathscr{C} \subseteq G_2(8, 4)$ which consists of all cyclic shifts of

$\{\alpha^0, \alpha^7, \alpha^{30}, \alpha^{46}, \alpha^{66}, \alpha^{76}, \alpha^{87}, \alpha^{88}, \alpha^{89}, \alpha^{112}, \alpha^{113}, \alpha^{137}, \alpha^{167}, \alpha^{175}, \alpha^{203}\}$
$\{\alpha^0, \alpha^{40}, \alpha^{41}, \alpha^{53}, \alpha^{65}, \alpha^{80}, \alpha^{84}, \alpha^{98}, \alpha^{124}, \alpha^{139}, \alpha^{147}, \alpha^{157}, \alpha^{162}, \alpha^{168}, \alpha^{180}\}$
$\{\alpha^0, \alpha^2, \alpha^{31}, \alpha^{45}, \alpha^{50}, \alpha^{91}, \alpha^{110}, \alpha^{123}, \alpha^{126}, \alpha^{163}, \alpha^{182}, \alpha^{183}, \alpha^{205}, \alpha^{207}, \alpha^{209}\}$
$\{\alpha^0, \alpha^{27}, \alpha^{59}, \alpha^{62}, \alpha^{82}, \alpha^{89}, \alpha^{90}, \alpha^{104}, \alpha^{114}, \alpha^{117}, \alpha^{122}, \alpha^{125}, \alpha^{166}, \alpha^{194}, \alpha^{203}\}$
$\{\alpha^0, \alpha^1, \alpha^{25}, \alpha^{56}, \alpha^{64}, \alpha^{65}, \alpha^{70}, \alpha^{71}, \alpha^{89}, \alpha^{95}, \alpha^{109}, \alpha^{131}, \alpha^{162}, \alpha^{176}, \alpha^{203}\}$
$\{\alpha^0, \alpha^1, \alpha^{25}, \alpha^{38}, \alpha^{81}, \alpha^{94}, \alpha^{124}, \alpha^{155}, \alpha^{156}, \alpha^{159}, \alpha^{160}, \alpha^{169}, \alpha^{180}, \alpha^{184}, \alpha^{202}\}$
$\{\alpha^0, \alpha^7, \alpha^9, \alpha^{57}, \alpha^{62}, \alpha^{64}, \alpha^{70}, \alpha^{72}, \alpha^{83}, \alpha^{90}, \alpha^{112}, \alpha^{120}, \alpha^{156}, \alpha^{169}, \alpha^{195}\}$
$\{\alpha^0, \alpha^8, \alpha^{16}, \alpha^{54}, \alpha^{69}, \alpha^{87}, \alpha^{125}, \alpha^{130}, \alpha^{145}, \alpha^{163}, \alpha^{167}, \alpha^{182}, \alpha^{194}, \alpha^{200}, \alpha^{208}\}$
$\{\alpha^0, \alpha^5, \alpha^{10}, \alpha^{21}, \alpha^{37}, \alpha^{40}, \alpha^{76}, \alpha^{84}, \alpha^{113}, \alpha^{114}, \alpha^{138}, \alpha^{143}, \alpha^{150}, \alpha^{166}, \alpha^{179}\}$
$\{\alpha^0, \alpha^{23}, \alpha^{64}, \alpha^{70}, \alpha^{79}, \alpha^{97}, \alpha^{110}, \alpha^{124}, \alpha^{126}, \alpha^{154}, \alpha^{174}, \alpha^{180}, \alpha^{190}, \alpha^{196}, \alpha^{201}\}$
$\{\alpha^0, \alpha^{16}, \alpha^{31}, \alpha^{45}, \alpha^{49}, \alpha^{88}, \alpha^{114}, \alpha^{145}, \alpha^{155}, \alpha^{159}, \alpha^{166}, \alpha^{171}, \alpha^{175}, \alpha^{197}, \alpha^{211}\}$
$\{\alpha^0, \alpha^{19}, \alpha^{47}, \alpha^{62}, \alpha^{78}, \alpha^{80}, \alpha^{90}, \alpha^{92}, \alpha^{101}, \alpha^{128}, \alpha^{140}, \alpha^{168}, \alpha^{205}, \alpha^{207}, \alpha^{212}\}$
$\{\alpha^0, \alpha^2, \alpha^{29}, \alpha^{39}, \alpha^{49}, \alpha^{50}, \alpha^{60}, \alpha^{71}, \alpha^{74}, \alpha^{103}, \alpha^{106}, \alpha^{109}, \alpha^{132}, \alpha^{181}, \alpha^{197}\}$
$\{\alpha^0, \alpha^9, \alpha^{28}, \alpha^{38}, \alpha^{47}, \alpha^{49}, \alpha^{93}, \alpha^{97}, \alpha^{101}, \alpha^{120}, \alpha^{158}, \alpha^{184}, \alpha^{190}, \alpha^{193}, \alpha^{197}\}$
$\{\alpha^0, \alpha^7, \alpha^{47}, \alpha^{59}, \alpha^{79}, \alpha^{82}, \alpha^{91}, \alpha^{94}, \alpha^{101}, \alpha^{112}, \alpha^{148}, \alpha^{174}, \alpha^{202}, \alpha^{206}, \alpha^{209}\}$
$\{\alpha^0, \alpha^6, \alpha^{12}, \alpha^{49}, \alpha^{53}, \alpha^{58}, \alpha^{107}, \alpha^{127}, \alpha^{147}, \alpha^{149}, \alpha^{156}, \alpha^{169}, \alpha^{188}, \alpha^{191}, \alpha^{197}\}$
$\{\alpha^0, \alpha^7, \alpha^{19}, \alpha^{27}, \alpha^{49}, \alpha^{85}, \alpha^{92}, \alpha^{104}, \alpha^{112}, \alpha^{134}, \alpha^{170}, \alpha^{177}, \alpha^{189}, \alpha^{197}, \alpha^{219}\}$
$\{\alpha^0, \alpha^6, \alpha^{10}, \alpha^{21}, \alpha^{39}, \alpha^{85}, \alpha^{91}, \alpha^{95}, \alpha^{106}, \alpha^{124}, \alpha^{170}, \alpha^{176}, \alpha^{180}, \alpha^{191}, \alpha^{209}\}$
$\{\alpha^0, \alpha^{13}, \alpha^{14}, \alpha^{38}, \alpha^{54}, \alpha^{85}, \alpha^{98}, \alpha^{99}, \alpha^{123}, \alpha^{139}, \alpha^{170}, \alpha^{183}, \alpha^{184}, \alpha^{208}, \alpha^{224}\}$
$\{\alpha^0, \alpha^9, \alpha^{32}, \alpha^{35}, \alpha^{37}, \alpha^{85}, \alpha^{94}, \alpha^{117}, \alpha^{120}, \alpha^{122}, \alpha^{170}, \alpha^{179}, \alpha^{202}, \alpha^{205}, \alpha^{207}\}$

This code $\mathscr{C}$ is an $[8, 4420, 4, 4]$-cyclic code. The first sixteen orbits are sets with 255 subspaces and the remaining four with 85 subspaces. □

Theorem 19: $\mathcal{C}_2(8, 4, 4) \geq 4420$.

Proof: The previous theorem show a cyclic Grassmannian code with 4420 subspaces. □

Theorem 20: There is a cyclic code with 4590 codewords. That is, $\alpha_2 = 3$ and $\alpha_1 = 17$.

Proof: Let α be a primitive root of $x^8 + x^4 + x^3 + x^2 + 1$ and use this polynomial to generate the field $\mathbb{F}_{2^8}$. Let $\mathscr{C} \subseteq G_2(8, 4)$ which consists of all cyclic shifts of

$\{\alpha^0, \alpha^7, \alpha^{30}, \alpha^{46}, \alpha^{66}, \alpha^{76}, \alpha^{87}, \alpha^{88}, \alpha^{89}, \alpha^{112}, \alpha^{113}, \alpha^{137}, \alpha^{167}, \alpha^{175}, \alpha^{203}\}$
$\{\alpha^0, \alpha^{40}, \alpha^{41}, \alpha^{53}, \alpha^{65}, \alpha^{80}, \alpha^{84}, \alpha^{98}, \alpha^{124}, \alpha^{139}, \alpha^{147}, \alpha^{157}, \alpha^{162}, \alpha^{168}, \alpha^{180}\}$
$\{\alpha^0, \alpha^2, \alpha^{31}, \alpha^{45}, \alpha^{50}, \alpha^{91}, \alpha^{110}, \alpha^{123}, \alpha^{126}, \alpha^{163}, \alpha^{182}, \alpha^{183}, \alpha^{205}, \alpha^{207}, \alpha^{209}\}$
$\{\alpha^0, \alpha^{27}, \alpha^{59}, \alpha^{62}, \alpha^{82}, \alpha^{89}, \alpha^{90}, \alpha^{104}, \alpha^{114}, \alpha^{117}, \alpha^{122}, \alpha^{125}, \alpha^{166}, \alpha^{194}, \alpha^{203}\}$
$\{\alpha^0, \alpha^1, \alpha^{25}, \alpha^{56}, \alpha^{64}, \alpha^{65}, \alpha^{70}, \alpha^{71}, \alpha^{89}, \alpha^{95}, \alpha^{109}, \alpha^{131}, \alpha^{162}, \alpha^{176}, \alpha^{203}\}$
$\{\alpha^0, \alpha^1, \alpha^{25}, \alpha^{38}, \alpha^{81}, \alpha^{94}, \alpha^{124}, \alpha^{155}, \alpha^{156}, \alpha^{159}, \alpha^{160}, \alpha^{169}, \alpha^{180}, \alpha^{184}, \alpha^{202}\}$

$\{\alpha^0, \alpha^7, \alpha^9, \alpha^{57}, \alpha^{62}, \alpha^{64}, \alpha^{70}, \alpha^{72}, \alpha^{83}, \alpha^{90}, \alpha^{112}, \alpha^{120}, \alpha^{156}, \alpha^{169}, \alpha^{195}\}$
$\{\alpha^0, \alpha^8, \alpha^{16}, \alpha^{54}, \alpha^{69}, \alpha^{87}, \alpha^{125}, \alpha^{130}, \alpha^{145}, \alpha^{163}, \alpha^{167}, \alpha^{182}, \alpha^{194}, \alpha^{200}, \alpha^{208}\}$
$\{\alpha^0, \alpha^5, \alpha^{10}, \alpha^{21}, \alpha^{37}, \alpha^{40}, \alpha^{76}, \alpha^{84}, \alpha^{113}, \alpha^{114}, \alpha^{138}, \alpha^{143}, \alpha^{150}, \alpha^{166}, \alpha^{179}\}$
$\{\alpha^0, \alpha^{23}, \alpha^{64}, \alpha^{70}, \alpha^{79}, \alpha^{97}, \alpha^{110}, \alpha^{124}, \alpha^{126}, \alpha^{154}, \alpha^{174}, \alpha^{180}, \alpha^{190}, \alpha^{196}, \alpha^{201}\}$
$\{\alpha^0, \alpha^{16}, \alpha^{31}, \alpha^{45}, \alpha^{49}, \alpha^{88}, \alpha^{114}, \alpha^{145}, \alpha^{155}, \alpha^{159}, \alpha^{166}, \alpha^{171}, \alpha^{175}, \alpha^{197}, \alpha^{211}\}$
$\{\alpha^0, \alpha^{19}, \alpha^{47}, \alpha^{62}, \alpha^{78}, \alpha^{80}, \alpha^{90}, \alpha^{92}, \alpha^{101}, \alpha^{128}, \alpha^{140}, \alpha^{168}, \alpha^{205}, \alpha^{207}, \alpha^{212}\}$
$\{\alpha^0, \alpha^2, \alpha^{29}, \alpha^{39}, \alpha^{49}, \alpha^{50}, \alpha^{60}, \alpha^{71}, \alpha^{74}, \alpha^{103}, \alpha^{106}, \alpha^{109}, \alpha^{132}, \alpha^{181}, \alpha^{197}\}$
$\{\alpha^0, \alpha^9, \alpha^{28}, \alpha^{38}, \alpha^{47}, \alpha^{49}, \alpha^{93}, \alpha^{97}, \alpha^{101}, \alpha^{120}, \alpha^{158}, \alpha^{184}, \alpha^{190}, \alpha^{193}, \alpha^{197}\}$
$\{\alpha^0, \alpha^7, \alpha^{47}, \alpha^{59}, \alpha^{79}, \alpha^{82}, \alpha^{91}, \alpha^{94}, \alpha^{101}, \alpha^{112}, \alpha^{148}, \alpha^{174}, \alpha^{202}, \alpha^{206}, \alpha^{209}\}$
$\{\alpha^0, \alpha^6, \alpha^{12}, \alpha^{49}, \alpha^{53}, \alpha^{58}, \alpha^{107}, \alpha^{127}, \alpha^{147}, \alpha^{149}, \alpha^{156}, \alpha^{169}, \alpha^{188}, \alpha^{191}, \alpha^{197}\}$
$\{\alpha^0, \alpha^4, \alpha^{30}, \alpha^{32}, \alpha^{35}, \alpha^{49}, \alpha^{66}, \alpha^{80}, \alpha^{94}, \alpha^{100}, \alpha^{117}, \alpha^{122}, \alpha^{168}, \alpha^{197}, \alpha^{202}\}$
$\{\alpha^0, \alpha^7, \alpha^{19}, \alpha^{27}, \alpha^{49}, \alpha^{85}, \alpha^{92}, \alpha^{104}, \alpha^{112}, \alpha^{134}, \alpha^{170}, \alpha^{177}, \alpha^{189}, \alpha^{197}, \alpha^{219}\}$
$\{\alpha^0, \alpha^6, \alpha^{10}, \alpha^{21}, \alpha^{39}, \alpha^{85}, \alpha^{91}, \alpha^{95}, \alpha^{106}, \alpha^{124}, \alpha^{170}, \alpha^{176}, \alpha^{180}, \alpha^{191}, \alpha^{209}\}$
$\{\alpha^0, \alpha^{13}, \alpha^{14}, \alpha^{38}, \alpha^{54}, \alpha^{85}, \alpha^{98}, \alpha^{99}, \alpha^{123}, \alpha^{139}, \alpha^{170}, \alpha^{183}, \alpha^{184}, \alpha^{208}, \alpha^{224}\}$

This code $\mathscr{C}$ is an [8, 4590, 4, 4]-cyclic code. The first seventeen orbits are sets with 255 subspaces and the remaining three with 85 subspaces. □

Theorem 21: $\mathcal{C}_2(8, 4, 4) = 4590$.

Proof: It follows directly from previous theorem and lemmas 14, 15 and 17. □

B. CALCULATING THE NUMBER $\mathcal{C}_2(8, 4, 3)$

It follows from Theorem 1 that

$$\mathcal{C}_2(8, 4, 3) = 255\alpha_1 + 85\alpha_2 + 17\alpha_4.$$

Lemma 22: Let $\mathscr{C} \subseteq G_2(8, 3)$ *a cyclic code with minimum distance 4. Then*

(1) $\alpha_1 \leq 5$;
(2) $\alpha_2 \leq 0$;
(3) $\alpha_4 \leq 0$.

Proof: There are not orbits with 85 and 17 subspaces. There is a clique with five orbits, and there is not one with six orbits. □

Theorem 23: There is a cyclic code with 1275 codewords. That is, $\alpha_1 = 5$.

Proof: Let α be a primitive root of $x^8+x^4+x^3+x^2+1$ and use this polynomial to generate the field $\mathbb{F}_{2^8}$. Let $\mathscr{C} \subseteq G_2(8, 3)$ which consists of all cyclic shifts of

$$\{\alpha^0, \alpha^{27}, \alpha^{34}, \alpha^{98}, \alpha^{104}, \alpha^{136}, \alpha^{139}\}$$
$$\{\alpha^0, \alpha^{58}, \alpha^{60}, \alpha^{107}, \alpha^{108}, \alpha^{132}, \alpha^{161}\}$$
$$\{\alpha^0, \alpha^{76}, \alpha^{80}, \alpha^{95}, \alpha^{113}, \alpha^{168}, \alpha^{176}\}$$
$$\{\alpha^0, \alpha^{20}, \alpha^{42}, \alpha^{59}, \alpha^{82}, \alpha^{110}, \alpha^{126}\}$$
$$\{\alpha^0, \alpha^{13}, \alpha^{69}, \alpha^{99}, \alpha^{130}, \alpha^{135}, \alpha^{144}\}$$

This code $\mathscr{C}$ is an [8, 1275, 4, 3]-cyclic code. Every orbit has 255 subspaces. □

Theorem 24: $\mathcal{C}_2(8, 4, 3) = 1275$.

Proof: See the previous theorem. □

C. CALCULATING THE NUMBER $\mathcal{C}_2(8, 6, 4)$

Theorem 25: $\mathcal{C}_2(8, 6, 4) = 0$

Proof: There is no orbit with minimum distance 6. □

D. CALCULATING THE NUMBER $\mathcal{C}_2(8, 8, 4)$

It follows from Theorem 1 that

$$\mathcal{C}_2(8, 8, 4) = 255\alpha_1 + 85\alpha_2 + 17\alpha_4.$$

Lemma 26: Let $\mathscr{C} \subseteq G_2(8, 4)$ *a cyclic code with minimum distance 8. Then*

(1) $\alpha_1 \leq 0$;
(2) $\alpha_2 \leq 0$;
(3) $\alpha_4 \leq 1$.

Proof: There is a unique orbit with a minimum distance of 8 and 17 subspaces. □

Theorem 27: There is a cyclic code with 17 codewords. That is, $\alpha_4 = 1$.

Proof: Let α be a primitive root of $x^8+x^4+x^3+x^2+1$ and use this polynomial to generate the field $\mathbb{F}_{2^8}$. Let $\mathscr{C} \subseteq G_2(8, 4)$ which consists of all cyclic shifts of

$$\{\alpha^0, \alpha^{17}, \alpha^{34}, \alpha^{51}, \alpha^{68}, \alpha^{85}, \alpha^{102}, \alpha^{119}, \alpha^{136}, \alpha^{153}, \alpha^{170}, \alpha^{187}, \alpha^{204}, \alpha^{221}, \alpha^{238}\}.$$

This code $\mathscr{C}$ is an [8, 17, 8, 4]-cyclic code. It consists of a unique orbit. □

Theorem 28: $\mathcal{C}_2(8, 8, 4) = 17$.

E. CALCULATING THE NUMBER $\mathcal{C}_2(8, 6, 3)$

Theorem 29: $\mathcal{C}_2(8, 6, 3) = 0$.

Proof: There is no orbit with minimum distance of 6. □

F. CALCULATING THE NUMBER $\mathcal{C}_2(8, 8, 3)$

Theorem 30: $\mathcal{C}_2(8, 8, 3) = 0$.

Proof: There is no orbit with minimum distance 8. □

G. CALCULATING THE NUMBER $\mathcal{C}_2(8, 4, 2)$

It follows from Theorem 1 that

$$\mathcal{C}_2(8, 4, 2) = 255\alpha_1 + 85\alpha_2 + 17\alpha_4.$$

TABLE 3. Values for $\mathcal{C}_2(8, d, k)$.

$d \setminus k$	2	3	4
4	85	1275	4590
6	0	0	0
8	0	0	17

Theorem 31: Let $\mathscr{C} \subseteq G_2(8, 2)$ a cyclic code with minimum distance of 4. Then
(1) $\alpha_1 \leq 0$;
(2) $\alpha_2 \leq 1$;
(3) $\alpha_4 \leq 0$.

Proof: There is only one orbit with 85 subspaces, and it has a minimum distance of 4. There are no orbits of other sizes with minimum distance 4. □

Theorem 32: There is a cyclic code with 85 codewords. That is, $\alpha_2 = 1$.

Proof: Let α be a primitive root of $x^8 + x^4 + x^3 + x^2 + 1$ and use this polynomial to generate the field $\mathbb{F}_{2^8}$. Let $\mathscr{C} \subseteq G_2(8, 2)$ which consists of all cyclic shifts of

$$\{\alpha^0, \alpha^{85}, \alpha^{170}\}.$$

This code $\mathscr{C}$ is an $[8, 85, 4, 2]$-cyclic code. It consists of a unique orbit. □

Theorem 33: $\mathcal{C}_2(8, 4, 2) = 85$.

VII. CLASSIFICATION OF BINARY GRASSMANNIAN CODES OF LENGTH 9

A. CALCULATING THE NUMBER $\mathcal{C}_2(9, 4, 3)$

It follows from Theorem 1 that

$$\mathcal{C}_2(9, 4, 3) = 511\alpha_1 + 73\alpha_3.$$

Theorem 34: Let $\mathscr{C} \subseteq G_2(9, 3)$ a cyclic code with minimum distance 4. Then
(1) $\alpha_1 \leq 11$;
(2) $\alpha_3 \leq 1$.

Proof: There is only one orbit with 73 subspaces, and it has a minimum distance of 6. There is a clique of 11 orbits with 511 subspaces. □

Theorem 35: $\mathcal{C}_2(9, 4, 3) \leq 5621$

Proof: It follows directly from previous theorem. □

Theorem 36: There is a cyclic code with 5621 codewords. That is, $\alpha_1 = 11$.

Proof: Let α be a primitive root of $x^9 + x^4 + 1$ and use this polynomial to generate the field $\mathbb{F}_{2^9}$. Let $\mathscr{C} \subseteq G_2(9, 3)$ which consists of all cyclic shifts of

$$\{\alpha^0, \alpha^{26}, \alpha^{27}, \alpha^{142}, \alpha^{156}, \alpha^{276}, \alpha^{345}\}$$
$$\{\alpha^0, \alpha^{86}, \alpha^{162}, \alpha^{169}, \alpha^{229}, \alpha^{237}, \alpha^{247}\}$$
$$\{\alpha^0, \alpha^{33}, \alpha^{81}, \alpha^{110}, \alpha^{181}, \alpha^{305}, \alpha^{379}\}$$
$$\{\alpha^0, \alpha^{2}, \alpha^{93}, \alpha^{96}, \alpha^{154}, \alpha^{260}, \alpha^{304}\}$$
$$\{\alpha^0, \alpha^{28}, \alpha^{127}, \alpha^{232}, \alpha^{248}, \alpha^{268}, \alpha^{311}\}$$
$$\{\alpha^0, \alpha^{25}, \alpha^{56}, \alpha^{90}, \alpha^{109}, \alpha^{227}, \alpha^{281}\}$$
$$\{\alpha^0, \alpha^{133}, \alpha^{174}, \alpha^{185}, \alpha^{197}, \alpha^{277}, \alpha^{332}\}$$

TABLE 4. Value for $\mathcal{C}_2(9, d, k)$.

$d \setminus k$	2	3	4
4	0	5694	25500-50589
6	0	73	511
8	0	0	0

$$\{\alpha^0, \alpha^{21}, \alpha^{157}, \alpha^{194}, \alpha^{244}, \alpha^{306}, \alpha^{372}\}$$
$$\{\alpha^0, \alpha^{73}, \alpha^{170}, \alpha^{187}, \alpha^{219}, \alpha^{259}, \alpha^{289}\}$$
$$\{\alpha^0, \alpha^{35}, \alpha^{123}, \alpha^{180}, \alpha^{218}, \alpha^{231}, \alpha^{356}\}$$
$$\{\alpha^0, \alpha^{24}, \alpha^{131}, \alpha^{177}, \alpha^{290}, \alpha^{294}, \alpha^{299}\}$$

This code $\mathscr{C}$ is an $[8, 5621, 4, 3]$-cyclic code. It consists of eleven orbits with 511 subspaces. □

Theorem 37: There is a cyclic code with 5694 codewords. That is, $\alpha_1 = 11, \alpha_3 = 1$.

Proof: Let α be a primitive root of $x^9 + x^4 + 1$ and use this polynomial to generate the field $\mathbb{F}_{2^9}$. Let $\mathscr{C} \subseteq G_2(9, 3)$ which consists of all cyclic shifts of

$$\{\alpha^0, \alpha^{64}, \alpha^{144}, \alpha^{242}, \alpha^{313}, \alpha^{381}, \alpha^{382}\}$$
$$\{\alpha^0, \alpha^{23}, \alpha^{84}, \alpha^{190}, \alpha^{202}, \alpha^{335}, \alpha^{337}\}$$
$$\{\alpha^0, \alpha^{27}, \alpha^{41}, \alpha^{52}, \alpha^{83}, \alpha^{142}, \alpha^{161}\}$$
$$\{\alpha^0, \alpha^{15}, \alpha^{91}, \alpha^{94}, \alpha^{126}, \alpha^{166}, \alpha^{322}\}$$
$$\{\alpha^0, \alpha^{45}, \alpha^{53}, \alpha^{63}, \alpha^{225}, \alpha^{263}, \alpha^{310}\}$$
$$\{\alpha^0, \alpha^{26}, \alpha^{33}, \alpha^{93}, \alpha^{181}, \alpha^{276}, \alpha^{304}\}$$
$$\{\alpha^0, \alpha^{102}, \alpha^{141}, \alpha^{184}, \alpha^{206}, \alpha^{316}, \alpha^{397}\}$$
$$\{\alpha^0, \alpha^{57}, \alpha^{108}, \alpha^{157}, \alpha^{227}, \alpha^{244}, \alpha^{281}\}$$
$$\{\alpha^0, \alpha^{74}, \alpha^{223}, \alpha^{239}, \alpha^{259}, \alpha^{289}, \alpha^{351}\}$$
$$\{\alpha^0, \alpha^{6}, \alpha^{103}, \alpha^{158}, \alpha^{192}, \alpha^{308}, \alpha^{329}\}$$
$$\{\alpha^0, \alpha^{24}, \alpha^{131}, \alpha^{177}, \alpha^{290}, \alpha^{294}, \alpha^{299}\}$$
$$\{\alpha^0, \alpha^{73}, \alpha^{146}, \alpha^{219}, \alpha^{292}, \alpha^{365}, \alpha^{438}\}$$

This code $\mathscr{C}$ is an $[8, 5694, 4, 3]$-cyclic code. It consists of eleven orbits with 511 subspaces and the remaining orbit with 73 subspaces. □

B. CALCULATING THE NUMBER $\mathcal{C}_2(9, 4, 2)$

Theorem 38: $\mathcal{C}_2(9, 4, 2) = 0$.

Proof: There is no orbit with minimum distance 4. □

VIII. CONCLUSION

In this paper, we present an alternative to constructing cyclic Grassmannian codes, having as a basis the design and implementation of algorithms to perform exhaustive searches of cliques in the projective space. We also present a classification of such codes in the space $\mathbb{P}_q^n$, with n at most 9.

ACKNOWLEDGMENT

Ismael Gutiérrez-García would like to thank the hospitality of the Institut für Diskrete und Algorithmische Mathematik, Technische Universität at Berlin, where part of this work was carried out.

REFERENCES

[1] E. Ben-Sasson, T. Etzion, A. Gabizon, and N. Raviv, "Subspace polynomials and cyclic subspace codes," *IEEE Trans. Inf. Theory*, vol. 62, no. 3, pp. 1157–1165, Mar. 2016, doi: 10.1109/TIT.2016.2520479.

[2] B. Chen and H. Liu, "Constructions of cyclic constant dimension codes," *Des., Codes Cryptogr.*, vol. 86, no. 6, pp. 1267–1279, Jun. 2018.

[3] T. Etzion and A. Vardy, "Error-correcting codes in projective space," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 1165–1173, Feb. 2011.

[4] H. Gluesing-Luerssen, K. Morrison, and C. Troha, "Cyclic orbit codes and stabilizer subfields," *Adv. Math. Commun.*, vol. 9, no. 2, pp. 177–197, 2015.

[5] I. Gutierrez-Gracia and I. M. Naizir, "Constructions of cyclic and quasi-cyclic Grassmannian codes," *IEEE Latin Amer. Trans.*, vol. 17, no. 7, pp. 1180–1190, Jul. 2019, doi: 10.1109/TLA.2019.8931207.

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

[7] K. Otal and F. Özbudak, "Cyclic subspace codes via subspace polynomials," *Des., Codes Cryptogr.*, vol. 85, no. 2, pp. 191–204, Nov. 2017, doi: 10.1007/s10623-016-0297-1.

[8] A.-L. Trautmann, F. Manganiello, M. Braun, and J. Rosenthal, "Cyclic orbit codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 11, pp. 7386–7404, Nov. 2013.

[9] Y. Niu, Q. Yue, and Y. Wu, "Several kinds of large cyclic subspace codes via Sidon spaces," *Discrete Math.*, vol. 343, no. 5, May 2020, Art. no. 111788, doi: 10.1016/j.disc.2019.111788.

ISMAEL GUTIÉRREZ-GARCÍA received the Dr. rer. nat. degree in mathematics from Johannes Gutenberg University Mainz, Germany. His current research interests are finite soluble groups, and discrete mathematics and their applications.

IVAN MOLINA NAIZIR received the Mathematics degree and the master's degree in computer science from the Universidad del Norte, in 2014. His current research interest is discrete mathematics and their applications.