Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 12, Number 2 (2016), pp. 1801–1820

http://www.ripublication.com/gjpam.htm

Grassmannian Codes as Lifts of Matrix Codes Derived as Images of Linear Block Codes over Finite Fields

Bryan S. Hernandez
College of Arts and Science,
Malayan Colleges Laguna,
Pulo-Diezmo Road, Cabuyao,
Laguna 4025, Philippines.

Virgilio P. Sison
Institute of Mathematical Sciences and Physics,
University of the Philippines Los Baños,
College 4031, Laguna, Philippines.

Abstract

Let p be a prime such that $p \equiv 2$ or 3 (mod 5). Linear block codes over the non-commutative matrix ring $M_2(\mathbb{F}_p)$ endowed with the Bachoc weight are derived as isometric images of linear block codes over the Galois field $\mathbb{F}_{p^2}$ endowed with the Hamming metric. When seen as rank metric codes, this family of matrix codes satisfies the Singleton bound and thus are maximum rank distance codes, which are then lifted to form a special class of subspace codes, the Grassmannian codes, that meet the anticode bound. These so-called anticode-optimal Grassmannian codes are associated in some way with complete graphs. Examples of these maximum rank distance codes and anticode-optimal Grassmannian codes are given. Finally, examples of subspace codes which are not Grassmannian are given which are obtained from the anticode-optimal Grassmannian codes.

AMS subject classification:
Keywords: Network coding, subspace codes, grassmannian codes, maximum rank distance codes.

1. Introduction

This paper deals with certain concepts of "coding theory in projective space" and highlights the practical significance of subspace codes, specifically of Grassmannian codes, in error correction in networks. Let $q = p^r$, p a prime, r a positive integer, and $\mathbb{F}_q$ the Galois field with cardinality q and characteristic p. Consider the n-dimensional full vector space $\mathbb{F}_q^n$ over $\mathbb{F}_q$. The set of all subspaces of $\mathbb{F}_q^n$, denoted by $\mathcal{P}_q(n)$, is called the projective space of order n over $\mathbb{F}_q$. For an integer k, where $0 \leq k \leq n$, the set of all k-dimensional subspaces of $\mathbb{F}_q^n$, denoted by $\mathcal{G}_q(n,k)$, is called the Grassmannian. A subspace code is a nonempty subset of $\mathcal{P}_q(n)$, while a Grassmannian code is a nonempty subset of $\mathcal{G}_q(n,k)$ which is also called a constant dimension code. Subspace codes have practical importance in network coding. The seminal paper [1] refers to *network coding* as "coding at a node in a network", that is, a node receives information from all input links, then encodes and sends information to all output links. This paper focuses on how isometric images of linear block codes over $\mathbb{F}_{p^2}$ can obtain codes that are equivalent to the Gabidulin codes and spread codes.

Section 2 gives important theoretical preliminaries, while Section 3 shows how to construct Grassmannian codes endowed with the subspace distance as union of lifts of certain linear codes $\mathcal{M}$ over the non-commutative matrix ring $M_2(\mathbb{F}_p)$ endowed with the Bachoc weight together with one additional space. The matrix codes $\mathcal{M}$ are isometric images of linear block codes over $\mathbb{F}_{p^2}$ endowed with the Hamming distance. Examples of obtained codes are equivalent to the Gabidulin codes which are maximum rank distance codes, or MRD codes, that is, they satisfy the Singleton bound for matrix codes with respect to the rank metric. The constructed Grassmannian codes are spread codes that satisfy the anticode bound. Examples of MRD codes and anticode-optimal Grassmannian codes are given from this construction. In Section 4, it is shown that this family of anticode-optimal Grassmannian codes can be associated with a peculiar family of complete graphs. Finally, examples of subspace codes were given from the optimal Grassmannian codes.

2. Preliminaries

The set of all $k \times \ell$ matrices over $\mathbb{F}_q$, denoted by $M_{k\times\ell}(\mathbb{F}_q)$, is considered as a vector space over $\mathbb{F}_q$. A nonempty subset of $M_{k\times\ell}(\mathbb{F}_q)$ is called a $[k \times \ell]$ *matrix code* over $\mathbb{F}_q$. This $[k \times \ell]$ matrix code is called linear if it is a subspace of $M_{k\times\ell}(\mathbb{F}_q)$.

The *rank distance* between two $k \times \ell$ matrices over $\mathbb{F}_q$, say A and B, is given by $d_R(A,B) = \text{rank}(A - B)$. A $[k \times \ell, \delta]$ *rank-metric code* $\mathbb{C}$ is a $[k \times \ell]$ matrix code whose minimum rank distance is δ. That is, $\delta = \min\{d_R(A,B) | A, B \in \mathbb{C}, A \neq B\}$.

Definition 2.1. A $[k \times \ell, \rho, \delta]$ *rank-metric code* is a linear code in $M_{k\times\ell}(\mathbb{F}_q)$ with dimension ρ and minimum rank distance δ.

We now give a notion of equivalence of rank-metric codes.

Definition 2.2. A $[k_1 \times \ell_1, \rho_1, \delta_1]$ rank-metric code is equivalent to a $[k_2 \times \ell_2, \rho_2, \delta_2]$ rank-metric code if $k_1 = k_2$, $\ell_1 = \ell_2$, $\rho_1 = \rho_2$, and $\delta_1 = \delta_2$.

In other words, two rank-metric codes are equivalent if they have entirely the same parameters.

Theorem 2.3 is known a version of the Singleton bound for rank-metric codes.

Theorem 2.3. (P. Delsarte, [5]) For a $[k \times \ell, \rho, \delta]$ rank-metric code, $\rho \leq \min\{k(\ell - \delta + 1), \ell(k - \delta + 1)\}$.

A code that attains this bound is called a *maximum rank distance code* or an *MRD code*. Examples of MRD codes are the so-called *Gabidulin codes*.

Let $n \leq m$ and $g = (g_0, g_1, g_2, \ldots, g_{n-1})$ be linearly independent elements of $GF(q^m)$. Then the code defined by the following generator matrix

$$G = \begin{pmatrix} g_0^{[0]} & g_1^{[0]} & \cdots & g_{n-1}^{[0]} \\ g_0^{[1]} & g_1^{[1]} & \cdots & g_{n-1}^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ g_0^{[k-1]} & g_1^{[k-1]} & \cdots & g_{n-1}^{[k-1]} \end{pmatrix}$$

where $[i] = q^i$, is called a *Gabidulin code*, generated by $g = (g_0, g_1, g_2, \ldots, g_{n-1})$, with dimension k and minimum rank distance $n - k + 1$.

Example 2.4. Let ω be a root of the irreducible polynomial $x^2 + x + 1 \in \mathbb{F}_2[x]$. Consider a generator matrix $G = (1, \omega)$. We have the following Gabidulin code $C = \{(0, 0), (1, \omega), (\omega, \omega^2), (\omega^2, 1)\}$ generated by G. From the given generator matrix, $n = 2$ and $k = 1$, hence the maximum rank distance is $2 - 1 + 1 = 2$.

Definition 2.5. Let $A \in M_{k\times\ell}(\mathbb{F}_q)$. The *lift* of A, denoted by $L(A)$, is the $k \times (k + \ell)$ standard matrix $(I_k\ A)$.

Note that the space generated by the rows of the lifted matrix $L(A)$ is denoted by $\langle L(A)\rangle$.

We now give two metrics on the projective space $\mathcal{P}_q(n)$. The *subspace distance* on $\mathcal{P}_q(n)$ is given by

$$d_S(A, B) = \dim A + \dim B - 2\dim(A \cap B)$$

for all $A, B \in \mathcal{P}_q(n)$. On the other hand, the *injection distance* on $\mathcal{P}_q(n)$ is given by

$$d_I(A, B) = \max\{\dim A, \dim B\} - \dim(A \cap B)$$

for all $A, B \in \mathcal{P}_q(n)$.

In this paper we only apply the subspace distance on the constructed Grassmannian codes.

A classic formula for the cardinality of the Grassmannian $\mathcal{G}_q(n,k)$ is given by the q-ary Gaussian coefficient

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \prod_{i=0}^{k-1} \frac{q^n - q^i}{q^k - q^i}.$$

Definition 2.6. A Grassmannian code $\mathcal{C}$ in $\mathcal{G}_q(n,k)$ is called an $(n, M, d, k)_q$ code if $|\mathcal{C}| = M$ and its minimum subspace distance is d, where

$$d = \{\min d_S(U, V) | U, V \in \mathcal{C}, U \neq V\}.$$

Definition 2.7. Let $\mathcal{C}$ be a $[k \times \ell]$ rank-metric code. The set

$$\begin{aligned} \Lambda(\mathcal{C}) &= \{\langle L(A) \rangle | A \in \mathcal{C}\} \\ &= \{\langle (I_k \; A) \rangle | A \in \mathcal{C}\} \end{aligned}$$

is called the *lift* of $\mathcal{C}$.

Theorem 2.8. (D. Silva, F. R. Kschischang, and R. Kötter [12]) Let $\mathcal{C}$ be a $[k \times \ell, \rho, \delta]$ rank-metric code. The lift of $\mathcal{C}$ is a $(k + \ell, q^\rho, 2\delta, k)_q$ Grassmannian code.

Theorem 2.9. (P. Frankl and R. M. Wilson, [9]) Let $\mathcal{A}_q(n, d, k)$ be the maximum number of codewords of a code in $\mathcal{G}_q(n,k)$ with subspace distance $d = 2\delta + 2$. Then

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

Spread codes are Grassmannian codes that satisfy the Anticode bound. A subset $\mathcal{S}$ of $\mathcal{G}_q(n,k)$ is a k-spread in $\mathbb{F}_q^n$ if the following are satisfied:

i. $U \cap V = \{(0, 0, \ldots, 0)\}$ for distinct U and V in $\mathcal{S}$, and

ii. $\cup_{V \in \mathcal{S}} V = \mathbb{F}_q^n$

Consider $\mathbb{F}_q^n$ which is an n-dimensional vector space over $\mathbb{F}_q$. If A is a subspace of V then the *orthogonal subspace* of A is given by $A^\perp = \{v \in V | a \cdot v = 0 \text{ for all } a \in A\}$ where $a \cdot v$ is the inner product between vectors a and v.

Definition 2.10. (R. Kötter and F. R. Kschichang, [11]) If $\mathcal{C} \subseteq \mathcal{G}_q(n,k)$ then its dual or complementary code is given by

$$\mathcal{C}^\perp = \{C^\perp \in \mathcal{G}_q(n, n-k) | C \in \mathcal{C}\}.$$

Theorem 2.11. (R. Kötter and F. R. Kschichang, [11]) If $\mathcal{C}$ is an $(n, M, d, k)_q$ code then $\mathcal{C}^\perp$ is an $(n, M, d, n-k)_q$ code.

3. Rank-Metric Codes and Grassmannian Codes from Linear Block Codes

We now define the Bachoc weight $w_{\mathtt{B}}$ on $M_2(\mathbb{F}_p)$.

$$w_{\mathtt{B}}(A) = \begin{cases} 0 & \text{if } A = 0 \\ 1 & \text{if } A \in GL(2, p) \\ p & \text{otherwise} \end{cases}$$

In [2], an isometric map ϕ from $\mathbb{F}_4^2$ onto $M_2(\mathbb{F}_2)$ where

$$\phi((a + b\omega, c + d\omega)) = \begin{pmatrix} a+d & b+c \\ b+c+d & a+b+d \end{pmatrix}$$

was given using the Hamming weight $w_{\mathtt{Ham}}$ and the Bachoc weight $w_{\mathtt{B}}$ for $\mathbb{F}_4^2$ and $M_2(\mathbb{F}_2)$ respectively, such that $w_{\mathtt{Ham}}(\alpha) = w_{\mathtt{B}}(\phi(\alpha))$ for all $\alpha \in \mathbb{F}_4^2$. Note that ω is a root of the irreducible polynomial $x^2 + x + 1 \in \mathbb{F}_2[x]$ and $\mathbb{F}_4$ is seen as an extension of $\mathbb{F}_2$ by ω.

Table 1 shows the elements of $\mathbb{F}_4^2$ with their corresponding Hamming weights and the elements of $M_2(\mathbb{F}_2)$ with their corresponding Bachoc and rank weights.

The following lemma is trivial yet very useful.

Lemma 3.1. Let $\mathcal{C}$ be a $[k \times \ell, \rho, \delta]$ rank-metric code with minimum nonzero rank Ω. Then $\delta = \Omega$.

Lemma 3.2. Let q be a power of a prime p. The additive group $\mathbb{F}_q^n$ is an $\mathbb{F}_p$-vector space.

Lemma 3.3. Let $\phi : \left(\mathbb{F}_{p^2}\right)^2 \longrightarrow M_2(\mathbb{F}_p)$ where

$$\phi((a + b\omega, c + d\omega)) = \begin{pmatrix} a+d & b+c \\ b+c+d & a+b+d \end{pmatrix}.$$

Then ϕ is an isomorphism of $\mathbb{F}_p$-vector spaces.

Remark 3.4. From Lemma 3.3, if C is a linear block code of length 2 over $\mathbb{F}_{p^2}$ then $C \cong \phi(C)$ as $\mathbb{F}_p$-vector spaces.

For the following remark, let $\alpha_i = (a_i + b_i\omega, c_i + d_i\omega) \in \left(\mathbb{F}_{p^2}\right)^2$ and

$$A_i = \begin{pmatrix} a_i + d_i & b_i + c_i \\ b_i + c_i + d_i & a_i + b_i + d_i \end{pmatrix} \in M_2(\mathbb{F}_p)$$

where $1 \leq i \leq r$ for positive integer r.

α	$w_{\mathtt{Ham}}(\alpha)$	$\phi(\alpha)$	$w_{\mathrm{B}}(\phi(\alpha))$	$w_R(\phi(\alpha))$
$(0,0)$	0	$\begin{pmatrix}0&0\\0&0\end{pmatrix}$	0	0
$(0,1)$	1	$\begin{pmatrix}0&1\\1&0\end{pmatrix}$	1	2
$(1,0)$	1	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	1	2
$(1,1)$	2	$\begin{pmatrix}1&1\\1&1\end{pmatrix}$	2	1
$(0,\omega)$	1	$\begin{pmatrix}1&0\\1&1\end{pmatrix}$	1	2
$(\omega,0)$	1	$\begin{pmatrix}0&1\\1&1\end{pmatrix}$	1	2
(ω,ω)	2	$\begin{pmatrix}1&1\\0&0\end{pmatrix}$	2	1
$(1,\omega)$	2	$\begin{pmatrix}0&0\\1&0\end{pmatrix}$	2	1
$(\omega,1)$	2	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$	2	1
$(0,1+\omega)$	1	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	1	2
$(1+\omega,0)$	1	$\begin{pmatrix}1&1\\1&0\end{pmatrix}$	1	2
$(1,1+\omega)$	2	$\begin{pmatrix}0&1\\0&0\end{pmatrix}$	2	1
$(1+\omega,1)$	2	$\begin{pmatrix}1&0\\0&0\end{pmatrix}$	2	1
$(\omega,1+\omega)$	2	$\begin{pmatrix}1&0\\1&0\end{pmatrix}$	2	1
$(1+\omega,\omega)$	2	$\begin{pmatrix}0&1\\0&1\end{pmatrix}$	2	1
$(1+\omega,1+\omega)$	2	$\begin{pmatrix}0&0\\1&1\end{pmatrix}$	2	1

Table 1: Hamming Weights on $\mathbb{F}_4^2$ and Bachoc and Rank Weights on $M_2(\mathbb{F}_2)$.

Remark 3.5. Let r be a positive integer. Note that ϕ can be extended naturally in the following manner. We have
$\phi : \left(\mathbb{F}_{p^2}\right)^{2r} \longrightarrow M_{2\times 2r}(\mathbb{F}_p)$ where

$$\phi(\alpha_1, \alpha_2, \ldots, \alpha_{2r}) = \begin{pmatrix} A_1 & A_2 & \ldots & A_r \end{pmatrix}.$$

It is easy to see that $\left(\mathbb{F}_{p^2}\right)^{2r} \cong M_{2\times 2r}(\mathbb{F}_p)$ as $\mathbb{F}_p$-vector spaces. If C is a linear block code of length $2r$ over $\mathbb{F}_{p^2}$ then $C \cong \phi(C)$ as $\mathbb{F}_p$-vector spaces.

Lemma 3.6. (D. Falcunit, Jr. and V. Sison, [8]) If $p \equiv 2$ or $3 \pmod 5$ then the polynomial $f(x) = x^2 + x + (p-1)$ is irreducible over $\mathbb{F}_p$.

Theorem 3.7. Let C be a linear block code of length $2r$ over $\mathbb{F}_{p^2}$ and ρ its dimension as an $\mathbb{F}_p$-vector space. If $p \equiv 2$ or $3 \pmod 5$ and for all $(\alpha_1, \alpha_2, \ldots, \alpha_{2r}) \in C$, $\alpha_j = 0$ for each odd (resp. even) index j, then

i. $\phi(C)$ is a $[2 \times 2r, \rho, 2]$ rank-metric code,

ii. $\Lambda(\phi(C))$ is a $(2r+2, p^{\rho}, 4, 2)_p$ code, and;

iii. the pairwise intersection of codewords of $\Lambda(\phi(C))$ is trivial.

Proof. Let C be a linear block code of length n over $\mathbb{F}_{p^2}$. Note that by Remark 3.5, C and $\phi(C)$ are isomorphic as $\mathbb{F}_p$-vector spaces. Hence, the dimension of $\phi(C)$ is ρ. Moreover, let $(\alpha_1, \alpha_2, \ldots, \alpha_{2r}) \in C \backslash \{(0, 0, \ldots, 0)\}$, $\alpha_j = 0$ for each odd (resp. even) integer j. To simplify the proof, we consider when $r = 1$ and hence we have $(0, \alpha_2) \in C \backslash \{(0, 0)\}$. Note that $\alpha_2 = c + d\omega$ for some $c, d \in \mathbb{F}_p$. Then

$$\phi(0, c + d\omega) = \begin{pmatrix} d & c \\ c + d & d \end{pmatrix}.$$

Since c and d are not both zero, we have the following cases:

1. If $c = 0$ and $d \neq 0$ then the matrix becomes

$$\begin{pmatrix} d & 0 \\ d & d \end{pmatrix}$$

with rank 2.

2. If $c \neq 0$ and $d = 0$ then the matrix becomes

$$\begin{pmatrix} 0 & c \\ c & 0 \end{pmatrix}$$

with rank 2.

3. Let $c, d \neq 0$. Suppose rank of the matrix is not 2 then one row is a multiple of the other, that is, $(d, c) = x(c+d, d)$ for some $x \in \mathbb{F}_p$. This implies that $d = xc+xd$ and $c = xd$. Further, $d = x^2d + xd$ and $x^2 + x - 1 = 0$. Since $p \equiv 2$ or 3 (mod 5), by Lemma 3.6, $f(x) = x^2 + x - 1 = x^2 + x + (p - 1)$ is irreducible over $\mathbb{F}_p$. Thus there is no $x \in \mathbb{F}_p$ such that $(d, c) = x(c + d, d)$ and hence the rank of the matrix is 2.

Thus, the minimum rank weight of $\phi(C)$ is 2. By Lemma 3.1, the minimum rank distance of $\phi(C)$ is also 2. It follows that $\phi(C)$ is a $[2 \times 2r, \rho, 2]$ rank-metric code.

It easy to see that (ii) follows directly from Theorem 2.8.

If $\Lambda(\phi(C))$ is a $(2r+2, p^\rho, 4, 2)_2$ code, the minimum subspace distance of $\Lambda(\phi(C))$ is 4. Let $A, B \in \Lambda(\phi(C))$. Note that $\dim A = \dim B = 2$ and we have $4 \leq d_S(A, B) = \dim A+\dim B-2\dim(A\cap B)$. Thus, $4 \leq 2+2-2\dim(A\cap B)$ and hence $\dim(A\cap B) \leq 0$. Therefore, $\dim(A \cap B) = 0$. This means that the pairwise intersection of codewords of $\Lambda(\phi(C))$ is trivial. ■

Note that the Grassmannian codes constructed in Theorem 3.7ii are spread codes. Due to Theorem 3.7, if the codewords of a linear block code of length n over $\mathbb{F}_{p^2}$ are composed of zeros in the odd positions or in the even positions, such zeros in the odd or even positions can be removed. In this manner, we can simplify how to obtain matrix codes from the isometric map ϕ. This is the essence of the following remark.

Remark 3.8. Let r be a positive integer and consider

$$S = \{(0, c_1 + d_1\omega, 0, c_2 + d_2\omega, 0, \ldots, 0, c_r + d_r\omega)|c_i, d_i \in \mathbb{F}_p\},$$

a subspace of $\left(\mathbb{F}_{p^2}\right)^{2r}$ as an $\mathbb{F}_p$-vector space. By Theorem 3.7 iv, we can look at $\phi : S \longrightarrow M_{2\times 2r}(\mathbb{F}_p)$ where

$$\phi((0, c_1 + d_1\omega, 0, c_2 + d_2\omega, \ldots, 0, c_r + d_r\omega)) =$$

$$\begin{pmatrix} d_1 & c_1 & d_2 & c_2 & \ldots & d_r & c_r \\ c_1 + d_1 & d_1 & c_2 + d_2 & d_2 & \ldots & c_r + d_r & d_r \end{pmatrix}$$

as $\phi_O : \left(\mathbb{F}_{p^2}\right)^r \longrightarrow M_{2\times 2r}(\mathbb{F}_p)$ where

$$\phi_O((c_1 + d_1\omega, c_2 + d_2\omega, \ldots, c_r + d_r\omega))$$

$$= \begin{pmatrix} d_1 & c_1 & d_2 & c_2 & \cdots & d_r & c_r \\ c_1 + d_1 & d_1 & c_2 + d_2 & d_2 & \cdots & c_r + d_r & d_r \end{pmatrix}.$$

Note that $\phi(S) = \phi_O\left(\left(\mathbb{F}_{p^2}\right)^r\right)$ and hence the rank of each nonzero element of $\phi_O\left(\left(\mathbb{F}_{p^2}\right)^r\right)$ is 2. Since the odd positions of S are all zeros, we can collapse its elements in such a way that we delete these odd positions and hence we can look at the elements of S as elements of $\left(\mathbb{F}_{p^2}\right)^r$.

Correspondingly, consider

$$\overline{S} = \{(a_1 + b_1\omega, 0, a_2 + b_2\omega, 0, \ldots, a_r + b_r\omega, 0) | a_i, b_i \in \mathbb{F}_p\},$$

which is also a subspace of $\left(\mathbb{F}_{p^2}\right)^{2r}$ as an $\mathbb{F}_p$-vector space. By Theorem 3.7 iv, we can look at $\phi : \overline{S} \longrightarrow M_{2\times 2r}(\mathbb{F}_p)$ where

$$\phi((a_1 + b_1\omega, 0, a_2 + b_2\omega, 0, \ldots, a_r + b_r\omega, 0))$$
$$= \begin{pmatrix} a_1 & b_1 & a_2 & b_2 & \cdots & a_r & b_r \\ b_1 & a_1 + b_1 & b_2 & a_2 + b_2 & \cdots & b_r & a_r + b_r \end{pmatrix}$$

as $\phi_E : \left(\mathbb{F}_{p^2}\right)^r \longrightarrow M_{2\times 2r}(\mathbb{F}_p)$ where

$$\phi_E((a_1 + b_1\omega, a_2 + b_2\omega, \ldots, a_r + b_r\omega))$$
$$= \begin{pmatrix} a_1 & b_1 & a_2 & b_2 & \cdots & a_r & b_r \\ b_1 & a_1 + b_1 & b_2 & a_2 + b_2 & \cdots & b_r & a_r + b_r \end{pmatrix}.$$

Similarly, $\phi(\overline{S}) = \phi_E(\left(\mathbb{F}_{p^2}\right)^r)$ and the rank of each nonzero element of $\phi_E(\left(\mathbb{F}_{p^2}\right)^r)$ is 2. Since the even positions of S are all zeros, we can collapse its elements in such a way that we delete these even positions and hence we can look at the elements of $\overline{S}$ as elements of $\left(\mathbb{F}_{p^2}\right)^r$.

Theorem 3.9. For prime p where $p \equiv 2$ or 3 (mod 5) and for any positive integer r, the rank-metric code $\phi_O\left(\left(\mathbb{F}_{p^2}\right)^r\right)$ satisfies the Singleton bound.

Proof. Let p be prime such that $p \equiv 2$ or 3 (mod 5), r be a positive integer, and ρ be the dimension of $\left(\mathbb{F}_{p^2}\right)^r$ as an $\mathbb{F}_p$-vector space. From Remark 3.8 and Theorem 3.7, $\phi_O(\left(\mathbb{F}_{p^2}\right)^r)$ is a $[2 \times 2r, \rho, 2]$ rank-metric code. Note that

$$\left|\phi_O\left(\left(\mathbb{F}_{p^2}\right)^r\right)\right| = p^\rho$$

and

$$\left|\left(\mathbb{F}_{p^2}\right)^r\right| = p^{2r}$$

but

$$\left|\left(\mathbb{F}_{p^2}\right)^r\right| = \left|\phi_O\left(\left(\mathbb{F}_{p^2}\right)^r\right)\right|.$$

Hence it follows that $\rho = 2r$. Now, a $[k \times \ell, \rho, \delta]$ rank-metric code satisfies the Singleton bound if $\rho = \min\{k(\ell - \delta + 1), \ell(k - \delta + 1)\}$. Substituting the values in the inequality given in the Singleton bound, $2r \leq \min\{2(2r - 2 + 1), 2r(2 - 2 + 1)\}$. We have $2r = \min\{4r - 2, 2r\}$ since $4r - 2 \geq 2r$ for $r \geq 1$. Thus, for prime p where $p \equiv 2$ or 3 (mod 5) and for any positive integer r, $\phi_O\left(\left(\mathbb{F}_{p^2}\right)^r\right)$ satisfies the Singleton bound for rank-metric codes and hence a maximum rank distance code. ■

MAGMA program was created to obtain the maximum rank distance code $\phi_O\left(\left(\mathbb{F}_{p^2}\right)^r\right)$ for $p = 2$ and for any positive integer r. Just input a positive integer for the value of r, and $\phi_O\left((\mathbb{F}_4)^r\right)$ will be obtained.

α	$\phi(\alpha)$	$w_R(\phi(\alpha))$
$(0, 0)$	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$	0
$(0, 1)$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	2
$(0, \omega)$	$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	2
$(0, 1+\omega)$	$\begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$	2
$(0, 2)$	$\begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}$	2
$(0, 2\omega)$	$\begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix}$	2
$(0, 1+2\omega)$	$\begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$	2
$(0, 2+2\omega)$	$\begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}$	2
$(0, 2+\omega)$	$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$	2

Table 2: Elements of $T = \{(0, c + d\omega) | c, d \in \mathbb{F}_3\}$ and their Images under ϕ with their Rank Weights.

Similarly, we can prove that $\phi_E\left(\left(\mathbb{F}_{p^2}\right)^r\right)$ also satisfies the Singleton bound for any positive integer r.

Example 3.10. Consider $\mathbb{F}_4 = \{0, 1, \omega, 1 + \omega\}$. We have

$$\phi_O(\mathbb{F}_4) = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}.$$

Note that by Theorem 3.7 and Remark 3.8, $\phi_O(\mathbb{F}_4)$ is a $[2 \times 2, 2, 2]$ rank-metric code. By Theorem 3.9, $\phi_O(\mathbb{F}_4)$ is a maximum rank distance code.

Example 3.11. Again, consider $\mathbb{F}_4 = \{0, 1, \omega, 1 + \omega\}$. We have

$$\phi_E(\mathbb{F}_4) = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}.$$

Note that by Theorem 3.7 and Remark 3.8, $\phi_E(\mathbb{F}_4)$ is a $[2 \times 2, 2, 2]$ rank-metric code, and a maximum rank distance code.

The rank-metric codes in Example 3.10 and Example 3.11 are equivalent to the Gabidulin code in Example 2.4 as $\mathbb{F}_2$-vector spaces.

Now, let $T = \{(0, c + d\omega)|c, d \in \mathbb{F}_3\}$. Table 2 shows the elements of T and their corresponding images in $M_2(\mathbb{F}_3)$ under ϕ with their rank weights. From the given table, each nonzero element of $\phi(T)$ has rank 2.

Example 3.12. Refer to Table 2, $\phi(T) = \phi_O(\mathbb{F}_9)$ is a $[2 \times 2, 2, 2]$ rank-metric code. By Theorem 3.9, $\phi_O(\mathbb{F}_9)$ is a maximum rank distance code.

Note that the first prime that does not satisfy Theorem 3.9 is $p = 5$. We have $5 \equiv 0 \pmod 5$. Now, $2 + \omega \in \mathbb{F}_{5^2} = \mathbb{F}_{25}$ and

$$\phi_O(2 + \omega) = \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}$$

whose rank is 1. Therefore, $\phi_O(\mathbb{F}_{25})$ cannot be a rank-metric code with minimum distance 2.

Definition 3.13. Let r and m be positive integers. We define the H_m-matrix as

$$H_m = \begin{pmatrix} I_m & 0_{m\times mr} \end{pmatrix}$$

and the $\widehat{H}_m$-matrix as

$$\widehat{H}_m = \begin{pmatrix} 0_{m\times mr} & I_m \end{pmatrix}.$$

Remark 3.14. [Anticode Bound]

$$\mathcal{A}_p(2r + 2, 4, 2) \leq \frac{p^{2r+2} - 1}{p^2 - 1}$$

Remark 3.15. For any natural number r, we have

$$1 + p^2 + p^4 + p^6 + \ldots + p^{2r} = \frac{p^{2r+2} - 1}{p^2 - 1}.$$

Theorem 3.16. Let p be prime where $p \equiv 2$ or $3 \pmod 5$, r be a positive integer, and consider a class of $\mathbb{F}_p$-vector spaces $\left\{\left(\mathbb{F}_{p^2}\right)^i \,|i = 1, 2, \ldots, r\right\}$. Let D_i be the set of vectors that contain $\Lambda\left(\phi_O\left(\mathbb{F}_{p^2}\right)^i\right)$ such that the vectors are appended with zeros in the left so that they have common length $2r + 2$. Then

$$G_p(r, 2) = \langle\widehat{H}_2\rangle \bigcup \left(\bigcup_{i=1}^{r} D_i\right)$$

is a $\left(2r + 2, \frac{p^{2r+2} - 1}{p^2 - 1}, 4, 2\right)_p$ code.

Proof. For $1 \leq i \leq r$, let D_i be the set of vectors that contain $\Lambda(\phi_O(\mathbb{F}_4^i))$ such that the vectors are appended with zeros in the left so that they have common length $2r+2$. Note that

$$\left|\Lambda\left(\phi_O\left((\mathbb{F}_{p^2})^i\right)\right)\right| = \left|\phi_O\left((\mathbb{F}_{p^2})^i\right)\right| = \left|(\mathbb{F}_{p^2})^i\right| = p^{2i}.$$

Now,

$$\left|\bigcup_{i=1}^{r} D_i\right| = p^2 + p^4 + p^6 + \cdots + p^{2r}.$$

Let $G_p(r, 2) = \langle \widehat{H_2} \rangle \bigcup \left(\bigcup_{i=1}^{r} D_i\right)$ so that by Remark 3.15,

$$|C| = 1 + p^2 + p^4 + p^6 + \cdots + p^{2r} = \frac{p^{2r+2} - 1}{p^2 - 1}.$$

Note that the only intersection of the D_i's is just the zero space. Moreover, the only intersection of $\langle \widehat{H_2} \rangle$ with the D_i's is also trivial. Thus, the obtained code is a $\left(2r + 2, \frac{p^{2r+2} - 1}{p^2 - 1}, 4, 2\right)_p$ code. ■

Remark 3.17. The code obtained $G_p(r, 2)$ in Theorem 3.16 attains the Anticode bound given in Remark 3.14.

Similarly, we can also obtain a $\left(2r + 2, \frac{p^{2r+2} - 1}{p^2 - 1}, 4, 2\right)_p$ code using the mapping ϕ_E.

Example 3.18. Let $p = 2$ and $r = 1$. We have $\mathbb{F}_4 = \{0, 1, \omega, 1 + \omega\}$. Now the lifted matrices of $\phi_O(\mathbb{F}_4)$ are $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$, and $\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$. Then the elements of $G_2(1, 2)$ are

$$\begin{aligned}
C_1 &= \{(1, 0, 0, 0), (0, 1, 0, 0), (1, 1, 0, 0), (0, 0, 0, 0)\},\\
C_2 &= \{(1, 0, 0, 1), (0, 1, 1, 0), (1, 1, 1, 1), (0, 0, 0, 0)\},\\
C_3 &= \{(1, 0, 1, 0), (0, 1, 1, 1), (1, 1, 0, 1), (0, 0, 0, 0)\},\\
C_4 &= \{(1, 0, 1, 1), (0, 1, 0, 1), (1, 1, 1, 0), (0, 0, 0, 0)\}, \text{ and;}\\
C_5 &= \{(0, 0, 1, 0), (0, 0, 0, 1), (0, 0, 1, 1), (0, 0, 0, 0)\}.
\end{aligned}$$

Note that $G_2(1, 2)$ is a $(4, 5, 4, 2)_2$ code. Now, when $p = 2$ and $r = 1$, the Anticode bound becomes $\frac{2^{2+2} - 1}{3} = 5$. Thus, $G_2(1, 2)$ attains this bound.

Example 3.19. Again, consider $\mathbb{F}_4 = \{0, 1, \omega, 1+\omega\}$. Now the lifted matrices of $\phi_E(\mathbb{F}_4)$ are $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$, and $\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$. Then the elements of the Grassmannian code $\mathcal{C}$ generated by the lifted matrices, with $C_5 = \langle \widehat{H_2} \rangle$ are given by

$$\begin{aligned} C_1 &= \{(1,0,0,0), (0,1,0,0), (1,1,0,0), (0,0,0,0)\}, \\ C_2 &= \{(1,0,1,0), (0,1,0,1), (1,1,1,1), (0,0,0,0)\}, \\ C_3 &= \{(1,0,0,1), (0,1,1,1), (1,1,1,0), (0,0,0,0)\}, \\ C_4 &= \{(1,0,1,1), (0,1,1,0), (1,1,0,1), (0,0,0,0)\}, \text{ and;} \\ C_5 &= \{(0,0,1,0), (0,0,0,1), (0,0,1,1), (0,0,0,0)\}. \end{aligned}$$

Note that $\mathcal{C}$ is also a $(4, 5, 4, 2)_2$ code that attains the Anticode bound.

Corollary 3.20. The dual of $G_p(r, 2)$ is a $\left(2r+2, \dfrac{p^{2r+2}-1}{p^2-1}, 4, 2r\right)_p$ code.

Proof. This directly follows from Theorem 2.11. ■

MAGMA programs were created to obtain the anticode-optimal code $G_p(r, 2)$ and its dual in Theorem 3.16 and Corollary 3.27, respectively for $p = 2$ and for any positive integer r. For $p = 2$, just input a positive integer for the value of r and $G_2(r, 2)$ will be obtained.

Lemma 3.21. Let $\phi : \mathbb{F}_9^2 \longrightarrow M_2(\mathbb{F}_3)$ where

$$\phi((a + b\omega, c + d\omega)) = \begin{pmatrix} a+d & b+c \\ b+c+d & a+b+d \end{pmatrix}.$$

Then ϕ is an isomorphism of $\mathbb{F}_3$-vector spaces.

Remark 3.22. In a similar manner in Remark 3.8, for any positive integer r,

$$T = \{(0, c_1 + d_1\omega, 0, c_2 + d_2\omega, \ldots, 0, c_r + d_r\omega) | c_i, d_i \in \mathbb{F}_3\},$$

a subspace of $\mathbb{F}_9^{2r}$ as an $\mathbb{F}_3$-vector space. We now have $\phi : T \longrightarrow M_{2\times 2r}(\mathbb{F}_3)$ where

$$\begin{aligned} &\phi((0, c_1 + d_1\omega, 0, c_2 + d_2\omega, \ldots, 0, c_r + d_r\omega)) \\ &= \begin{pmatrix} d_1 & c_1 & d_2 & c_2 & \ldots & d_r & c_r \\ c_1+d_1 & d_1 & c_2+d_2 & d_2 & \ldots & c_r+d_r & d_r \end{pmatrix} \end{aligned}$$

and $\phi_O : \mathbb{F}_9^r \longrightarrow M_{2\times 2r}(\mathbb{F}_3)$ where

$$\phi_O((c_1 + d_1\omega, c_2 + d_2\omega, \ldots, c_r + d_r\omega))$$

$$= \begin{pmatrix} d_1 & c_1 & d_2 & c_2 & \cdots & d_r & c_r \\ c_1 + d_1 & d_1 & c_2 + d_2 & d_2 & \cdots & c_r + d_r & d_r \end{pmatrix}.$$

Note that $\phi(T) = \phi_O(\mathbb{F}_9^r)$ and hence $\phi_O(\mathbb{F}_9^r)$ is a subspace of $M_{2\times 2r}(\mathbb{F}_3)$ as an $\mathbb{F}_3$-vector space. Moreover, we can verify using Table 2 that the minimum rank of T is 2.

Theorem 3.23. For any positive integer r, the rank-metric code $\phi_O(\mathbb{F}_9^r)$ satisfies the Singleton bound.

Example 3.24. Refer to Table 2, $\phi(T) = \phi_O(\mathbb{F}_9)$ is a $[2 \times 2, 2, 2]$ rank metric code. By Theorem 3.23, $\phi_O(\mathbb{F}_9)$ is a maximum rank distance code.

Remark 3.25. [Anticode Bound]

$$\mathcal{A}_3(2r + 2, 4, 2) \leq \frac{9^{r+1} - 1}{8}$$

Remark 3.26. For any natural number r, we have

$$1 + 9 + 9^2 + 9^3 + \cdots + 9^{r-1} + 9^r = \frac{9^{r+1} - 1}{8}.$$

Theorem 3.27. Let r be a positive integer and consider a class of $\mathbb{F}_3$-vector spaces $\left\{\mathbb{F}_9^i | i = 1, 2, \ldots, r\right\}$. Let D_i be the set of vectors that contain $\Lambda(\phi_O(\mathbb{F}_9^i))$ such that the vectors are appended with zeros in the left so that they have common length $2r+2$. Then

$$G_3(r, 2) = \langle \widehat{H_2} \rangle \bigcup \left(\bigcup_{i=1}^{r} D_i \right)$$

is a $\left(2r + 2, \frac{9^{r+1} - 1}{8}, 4, 2\right)_3$ code.

Theorem 3.28. Let $\tau : \mathbb{F}_8 \longrightarrow M_3(\mathbb{F}_2)$ where

$$\tau(a + b\omega + c\omega^2) = \begin{pmatrix} b + c & a & c \\ a + b + c & b & a \\ c & a + c & a + b + c \end{pmatrix}.$$

Then τ is a monomorphism of $\mathbb{F}_2$-vector spaces.

Table 3 shows the elements of $\mathbb{F}_8$ and their corresponding matrix under τ. Note that each nonzero element of $\tau(\mathbb{F}_8)$ has rank 3.

Remark 3.29. It can be easily seen from Theorem 3.28 and Table 3 that $\mathbb{F}_8 \cong \tau(\mathbb{F}_8)$ as $\mathbb{F}_2$-vector spaces. Moreover, the minimum rank of $\tau(\mathbb{F}_8)$ is 3.

α	$\tau(\alpha)$	$w_R(\tau(\alpha))$
0	$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$	0
1	$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$	3
ω	$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	3
ω^2	$\begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$	3
$1+\omega$	$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$	3
$1+\omega^2$	$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$	3
$\omega+\omega^2$	$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}$	3
$1+\omega+\omega^2$	$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$	3

Table 3: Elements of $\mathbb{F}_8$ and their Images under τ with their Rank Weights.

For the following remark, let $\alpha_i = a_i + b_i\omega + c_i\omega^2 \in \mathbb{F}_8$ and

$$A_i = \begin{pmatrix} b_i + c_i & a_i & c_i \\ a_i + b_i + c_i & b_i & a_i \\ c_i & a_i + c_i & a_i + b_i + c_i \end{pmatrix} \in M_3(\mathbb{F}_2)$$

where $1 \leq i \leq r$ for positive integer r.

Remark 3.30. The monomorphism τ given in Theorem 3.28 can be extended naturally to $\tau : \mathbb{F}_8^r \longrightarrow M_{3\times 3r}(\mathbb{F}_2)$ where

$$\tau(\alpha_1, \alpha_2, \ldots, \alpha_r) = \begin{pmatrix} A_1 & A_2 & \cdots & A_r \end{pmatrix}$$

It is easy to see that the rank of each nonzero element of $\tau(\mathbb{F}_8^r)$ is 3.

Theorem 3.31. For any positive integer r, the rank-metric code $\tau(\mathbb{F}_8^r)$ satisfies the Singleton bound.

Example 3.32. Refer to Table 3 for the elements of $\tau(\mathbb{F}_8)$. Note that $\tau(\mathbb{F}_8)$ is a $[3 \times 3, 3, 3]$ rank metric code. By Theorem 3.31, $\tau(\mathbb{F}_8)$ is a maximum rank distance code.

Remark 3.33. [Anticode Bound]

$$\mathcal{A}_2(3r+3, 6, 3) \leq \frac{8^{r+1}-1}{7}$$

Remark 3.34. For any natural number r, we have

$$1 + 8 + 8^2 + 8^3 + \cdots + 8^{r-1} + 8^r = \frac{8^{r+1}-1}{7}.$$

Theorem 3.35. Let r be a positive integer and consider a class of $\mathbb{F}_2$-vector spaces $\{\mathbb{F}_8^i | i = 1, 2, \ldots, r\}$. Let D_i be the set of vectors that contain $\Lambda(\tau(\mathbb{F}_8^i))$ such that the vectors are appended with zeros in the left so that they have common length $3r+3$. Then

$$G_2(r, 3) = \langle \widehat{H}_3 \rangle \bigcup \left(\bigcup_{i=1}^{r} D_i \right)$$

is a $\left(3r+3, \frac{8^{r+1}-1}{7}, 6, 3\right)_2$ code.

Example 3.36. Let $r = 1$ and consider $\mathbb{F}_8$. The elements of $\tau(\mathbb{F}_8)$ can be seen on Table 3. Note that $G_2(1, 3) = \langle \widehat{H}_3 \rangle \bigcup D_1$ is a $(6, 9, 6, 3)_2$ code and hence satisfies the anticode bound.

4. Graphs of Anticode-Optimal Grassmannian Codes $G_p(r, 2)$

In this section, Grassmannian codes $G_p(r, 2)$ are associated with complete graphs. The number of vertices are determined by the number of subspaces of the code while an edge is formed when two subspaces intersect at the zero space. Example of such graph is also given.

A *graph* G is a pair (V, E) where V is a finite set whose members are called *vertices*, and E is a subset of the set $V \times V$ of unordered pairs of vertices. The members of E are called *edges* [3]. If $\{v, w\}$ is an edge of G, the vertices v and w are said to be *adjacent*. An edge with identical ends is called a *loop* and an edge with distinct ends is called a *link*. A graph is *simple* if it has no loops and no two of its links join the same pair of vertices. In a simple graph, the *degree* of a vertex $v \in G$ is the number of edges of G incident with v [4].

A simple graph in which each pair of distinct vertices is joined by an edge is called a *complete graph*. A complete graph with N vertices is denoted by K_N. The complete graph of N vertices has $\frac{N(N-1)}{2}$ edges. The degree of any vertex in K_N is $N-1$.

Note that for distinct $A, B \in G_p(r, 2)$ in Theorem 3.16, we have $A \cap B = \{0\}$.

Definition 4.1. Let the subspaces of $G_p(r, 2)$ be the vertices of the graph $\Gamma_p(r, 2)$. Two vertices A and B are adjacent if and only if $\dim(A \cap B) = 0$.

It follows that the edge set of $\Gamma_p(r, 2)$ is the set of all unordered distinct pair of vertices.

Theorem 4.2. The graph $\Gamma_p(r, 2)$ is a complete graph with $\dfrac{p^{2r+2}-1}{p^2-1}$ vertices.

Proof. Note that $|G_p(r, 2)| = \dfrac{p^{2r+2}-1}{p^2-1}$ so $\Gamma_p(r, 2)$ has $\dfrac{p^{2r+2}-1}{p^2-1}$ vertices. Since the intersection of any two subspaces in $G_p(r, 2)$ is trivial, its dimension is zero. Thus, each pair of vertices is joined by an edge. By definition, $\Gamma_p(r, 2)$ is a complete graph with $\dfrac{p^{2r+2}-1}{p^2-1}$ vertices. ■

Remark 4.3. We can easily compute the number of edges of $\Gamma_p(r, 2)$ and the degree of each vertex.

Example 4.4. When $p = 2$ and $r = 2$, we have a $(4, 21, 4, 2)_2$ code. The associated graph $\Gamma_2(2, 2)$ of the $(4, 21, 4, 2)_2$ code is a complete graph with 21 vertices. The number of edges is 210 and the degree of each vertex is 20.

5. Subspace Codes from Grassmannian Codes

The following example is a subspace code obtained from the Grassmannian codes constructed in the earlier part of this paper.

Example 5.1. Consider the subspace code $\mathcal{C}$ which consists of the row spaces generated by the following matrices:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

We can verify by inspection that $\mathcal{C}$ is a $(6, 28, 3)_2$ subspace code. MAGMA was also used to check that the minimum subspace distance of $\mathcal{C}$ is indeed 3.

Note that the set of 2-dimensional subspaces $\mathcal{C}_2$ in $\mathcal{C}$ are the elements of $\bigcup_{i=1}^{2} D_i$ where D_i is the set of vectors that contain $\Lambda(\phi_E(\mathbb{F}_2^i))$ such that the vectors are appended with zeros in the left so that they have common length 6 as given in Theorem 3.16. Moreover, the set of 3-dimensional subspaces $\mathcal{C}_3$ in $\mathcal{C}$ are the elements of $\langle \widehat{H}_3 \rangle \bigcup E_1 \setminus \langle H_3 \rangle$ where E_1 is the set of vectors that contain $\Lambda(\tau(\mathbb{F}_8))$ such that the vectors are appended by zeros in the left so that they are of length 6 as given in Theorem 3.35. Both $\mathcal{C}_2$ and $\mathcal{C}_3$ are close to optimal Grassmannian codes.

Remark 5.2. The following are $(6, 28, 3)_2$ subspace codes.

1. $\left(\bigcup_{i=1}^{2} D_i\right) \bigcup \left(\langle \widehat{H_3} \rangle \bigcup E_1 \setminus \langle H_3 \rangle\right)$ consisting of 20 2-dimensional subspaces and 8 3-dimensional subspaces (Example 5.1)

2. $\left(\langle \widehat{H_2} \rangle \bigcup \left(\bigcup_{i=1}^{2} D_i\right) \setminus \langle H_2 \rangle\right) \bigcup E_1$ consisting of 20 2-dimensional subspaces and 8 3-dimensional subspaces

3. $\left(\langle \widehat{H_2} \rangle \bigcup \left(\bigcup_{i=1}^{2} D_i\right)\right) \bigcup (E_1 \setminus \langle H_2 \rangle)$ consisting of 21 2-dimensional subspaces and 7 3-dimensional subspaces

4. $\left(\left(\bigcup_{i=1}^{2} D_i\right) \setminus \langle H_2 \rangle\right) \bigcup \left(\langle \widehat{H_3} \rangle \bigcup E_1\right)$ consisting of 19 2-dimensional subspaces and 9 3-dimensional subspaces.

References

[1] R. Ahlswede and N. Cai and S.-Y. Li and R. Yeung, "Network information flow", *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204–1216, 2000.

[2] C. Bachoc, "Application of coding theory to the construction of modular lattices," *J. Combinatorial Theory*, vol. 78, pp. 92–119, 1997.

[3] N. L. Biggs and A. T. White, Permutation Groups and Combinatorial Structures, Cambridge University Press, New York, 1979.

[4] J. A. Bondy and U. S. R. Murty, Graph Theory With Applications, *Elsevier Science Publishing Co., Inc.*, New York, 1976.

[5] P. Delsarte, Bilinear Forms over a finite field, with applications to coding theory, *J. of Comb. Theory*, Series A 25, 226–241, 1978.

[6] T. Etzion, "Subspace codes − bounds and constructions", *1st European Training School on Network Coding, Bacelona, Spain*, February 2013.

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

[8] D. Falcunit, Jr. and V. Sison, "Cyclic Codes over the Matrix Ring $M_2(\mathbb{F}_p)$ and their Isometric Images over $\mathbb{F}_{p^2} + u\mathbb{F}_{p^2}$"ž, *Proceedings of the 2014 International Zürich Seminar on Communications, Sorell Hotel Zürichberg, Zürich, Switzerland*, pp. 91–96, 26–28 February 2014.

[9] P. Frankl and R. M. Wilson, The Erdos-Ko-Rado theorem for vector spaces, *J. Combin. Theory, Series A*, vol. 23, pp. 228–236, 1986.

[10] A. Khaleghi and D. Silva and F. R. Kschischang, Subspace Codes, *IMA Int. Conf.*, vol. 49, no. 4, pp. 1–21, 2009.

[11] R. Kötter and F. R. Kschichang, Coding for errors and erasures in random network coding, *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3579–3591, 2008.

[12] Silva, D., F. R. Kschischang, and R. Kötter, A rank-metric approach to error control in random network coding, *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 3951–3967, 2008.