J. Algebra Comb. Discrete Appl.
8(1) • 31–39

Received: 16 February 2020
Accepted: 13 September 2020

Journal of Algebra Combinatorics Discrete Structures and Applications

A new construction of anticode-optimal Grassmannian codes

Research Article

Ben Paul Dela Cruz, John Mark Lampos, Herbert Palines, Virgilio Sison

Abstract: In this paper, we consider the well-known unital embedding from $\mathbb{F}_{q^k}$ into $M_k(\mathbb{F}_q)$ seen as a map of vector spaces over $\mathbb{F}_q$ and apply this map in a linear block code of rate ρ/ℓ over $\mathbb{F}_{q^k}$. This natural extension gives rise to a rank-metric code with k rows, $k\ell$ columns, dimension ρ and minimum distance k that satisfies the Singleton bound. Given a specific skeleton code, this rank-metric code can be seen as a Ferrers diagram rank-metric code by appending zeros on the left side so that it has length $n-k$. The generalized lift of this Ferrers diagram rank-metric code is a Grassmannian code. By taking the union of a family of the generalized lift of Ferrers diagram rank-metric codes, a Grassmannian code with length n, cardinality $\frac{q^n-1}{q^k-1}$, minimum injection distance k and dimension k that satisfies the anticode upper bound can be constructed.

2010 MSC: 94B05, 94B60, 94B65

Keywords: Ferrers diagram, Rank-metric code, Grassmannian, Constant dimension, Anticode bound

1. Introduction

Let $\mathbb{F}_q$ be the finite field of order q. The projective space of order n over $\mathbb{F}_q$, denoted by $\mathcal{P}_q(n)$, is the set of all subspaces of $\mathbb{F}_q^n$. Given an integer k such that $0 \leq k \leq n$, the set of all k-dimensional subspaces of $\mathbb{F}_q^n$ is known as a Grassmannian, denoted by $\mathcal{G}_q(n,k)$. A subspace code is a nonempty subset of $\mathcal{P}_q(n)$, while a Grassmannian code is a nonempty subset of $\mathcal{G}_q(n,k)$. Subspace codes are used in network coding, a method that is far more efficient than classical coding. This paper aims to generalize the results of [4], i.e. to construct maximum rank distance (MRD) codes whose generalized lifts form an anticode-optimal Grassmannian code.

The paper is organized as follows. The next section gives some preliminaries and the construction of subspace codes in [2]. Section 3 shows how to construct MRD codes from linear block codes. Given

Ben Paul Dela Cruz (Corresponding Author), John Mark Lampos, Herbert Palines, Virgilio Sison; Institute of Mathematical Sciences and Physics, University of the Philippines, Los Baños, College, Laguna 4031, Philippines (email: bbdelacruz2@up.edu.ph, jtlampos@up.edu.ph, hspalines@up.edu.ph, vpsison@up.edu.ph).

https://doi.org/10.13069/jacodesmath.858732

ISSN 2148-838X

a specific skeleton code, these MRD codes turn out to be Ferrers diagram maximum rank distance (FDMRD) codes. In Section 4, anticode-optimal Grassmannian code will be constructed using these FDMRD codes and the multi-level construction in [2]. Instead of using pending dots, we will use the multi-level construction as presented in [6]. Lastly, we give our conclusion in Section 5.

2. Preliminaries

A $[k \times \ell]$ *matrix code* over $\mathbb{F}_q$ is a nonempty subset 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 $d_R(A, B) = \operatorname{rank}(A - B)$.

The *minimum rank distance* of a matrix code $\mathbb{C}$, denoted by δ, is defined by $\delta = \min\{\mathbf{d}_R(A, B)|A, B \in \mathbb{C}, A \neq B\}$. A $[k \times \ell, \delta]$ *rank-metric code* is a $[k \times \ell]$ matrix code with minimum rank distance δ. It is worth noting that a linear code in $M_{k\times\ell}(\mathbb{F}_q)$ is a subspace of the vector space $M_{k\times\ell}(\mathbb{F}_q)$. A $[k \times \ell, \rho, \delta]$ *rank-metric code* $\mathbb{C}$ is a linear code in $M_{k\times\ell}(\mathbb{F}_q)$ with dimension ρ and minimum distance δ.

The following theorem gives the relationship of the minimum distance of a rank-metric code with its minimum nonzero rank.

Theorem 2.1. *[4] Let $\mathbb{C}$ be a $[k \times \ell, \rho, \delta]$ rank-metric code with minimum nonzero rank Ω. Then $\delta = \Omega$.*

Theorem 2.2. *[1] For a $[k \times \ell, \rho, \delta]$ rank−metric code $\mathbb{C}$,*

$$\rho \leq \min\{k(\ell - \delta + 1), \ell(k - \delta + 1)\}.$$

A code that attains the bound in Theorem 2.2 is called a *maximum rank distance code* or an *MRD code*.

Before we go to Grassmannian codes, we first give two definitions which are vital to our construction. Let $A \in M_{k\times\ell}(\mathbb{F}_q)$. The *lift* of A, denoted by $L(A)$, is the standard matrix $(I_k\ A)$. We adapted this definition from [4]. For a given matrix A, we denote the row space of A by $\langle A\rangle$.

Example 2.3. *Let $A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \in M_{2\times3}(\mathbb{F}_2)$. Then*

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

Moreover, the rowspace generated by $L(A)$ is the linear block code of length 5, rate $2/5$ over $\mathbb{F}_2$. $\langle L(A)\rangle = \{(0, 0, 0, 0, 0), (1, 0, 1, 0, 1), (0, 1, 0, 1, 1), (1, 1, 1, 1, 0)\}$.

Definition 2.4. *[4] Let $\mathbb{C}$ be a $[k \times \ell]$ rank-metric code. The set*

$$\Lambda(\mathbb{C}) = \{\langle L(A)\rangle|A \in \mathbb{C}\}$$

is called the lift of $\mathbb{C}$.

It is well known that the cardinality of $\mathcal{G}_q(n, k)$ is given by the q-ary Gaussian coefficient

$$|\mathcal{G}_q(n, k)| = \begin{bmatrix} n \\ k \end{bmatrix}_q = \prod_{i=0}^{k-1} \frac{q^{n-i} - 1}{q^{k-i} - 1}. \tag{1}$$

Consequently, $|\mathcal{P}_q(n)| = | \cup_{k=0}^{n} \mathcal{G}_q(n, k)|$.

Furthermore, the subspace distance and the injection distance, defined as

$$\mathbf{d}_S(A, B) = \dim(A + B) - \dim(A \cap B)$$

and

$$\mathbf{d}_I(A,B) = \max\{\dim A, \dim B\} - \dim(A \cap B)$$

respectively, for any A, B in $\mathcal{P}_q(n)$ are metrics on $\mathcal{P}_q(n)$, and so in $\mathcal{G}_q(n,k)$. It is clear that if A and B have the same dimension, then

$$\mathbf{d}_I(A,B) = \frac{1}{2}\mathbf{d}_S(A,B).$$

We say that $\mathcal{C} \subseteq \mathcal{G}_q(n,k)$ is an $(n, M, d, k)_q$ code in the Grassmannian, or a constant-dimension code, if $|\mathcal{C}| = M$ and the minimum injection distance of $\mathcal{C}$ is $d = \min\{\mathbf{d}_I(A,B) | A, B \in \mathcal{C}, A \neq B\}$. Since $\mathbf{d}_I(A,B) = \frac{1}{2}\mathbf{d}_S(A,B)$, then the minimum subspace distance of a Grassmannian code is twice of its minimum injection distance. Equivalently, one may opt to use the subspace distance instead of injection distance.

The next theorem gives the parameters of the resulting Grassmannian code from a lifted rank-metric code.

Theorem 2.5. *[6] Let $\mathbb{C}$ be a $[k \times \ell, \rho, \delta]$ rank-metric code. Then $\Lambda(\mathbb{C})$ is a $(k+\ell, q^\rho, \delta, k)_q$ Grassmannian code.*

The maximum number of codewords in an $(n, M, d, k)_q$ code is denoted by $\mathcal{A}_q(n,d,k)$. Bounds for $\mathcal{A}_q(n,d,k)$ were given in [7], [3] and [11]. The lift of maximum rank distance (MRD) codes in [10] asymptotically attains the bounds given in [3] and [7]. The next theorem gives the bound that were used to check the optimality of our constructed code.

Theorem 2.6. *[11] Anticode Bound.*

$$\mathcal{A}_q(n,d,k) \leq \frac{\begin{bmatrix} n \\ k \end{bmatrix}_q}{\begin{bmatrix} n-k+d-1 \\ d-1 \end{bmatrix}_q} = \frac{\begin{bmatrix} n \\ k-d+1 \end{bmatrix}_q}{\begin{bmatrix} k \\ k-d+1 \end{bmatrix}_q} \tag{2}$$

Etzion and Silberstein provided a multi-level construction of Grassmannian codes in [2]. The codes constructed using multi-level construction are called lifted Ferrers Diagram (FD) codes in [6]. Furthermore, an alternative form of the construction of lifted FD codes which uses matrices instead of the usual pending dots were presented in [6]. In this paper, we opt to use the alternative form of the said construction. As defined in [6], for a nonzero $X \in M_{k\times\ell}(\mathbb{F}_q)$, there corresponds a vector $\mathrm{prof}(X) \in \{0,1\}^n$, called the *profile vector* of X, in which $\mathrm{supp}(\mathrm{prof}(X))$ is the set of column positions of the leading ones in the rows of the row reduced echelon form of X. If $X = 0$, then we set $\mathrm{prof}(X)$ to be the zero vector. Associated with a vector space $U \in \mathcal{G}_q(n,k), k > 0$, is a unique $k \times n$ matrix X_U in row reduced echelon form such that $U = \langle X_U \rangle$. Now define the profile vector of U, denoted by $\mathrm{prof}(U)$, given by

$$\mathrm{prof}(U) = \mathrm{prof}(X_U).$$

In addition, $\mathrm{prof}(U) = 0 \in \mathbb{F}_2^n$ if $\dim(U) = 0$. Let $b \in \mathbb{F}_2^n$, the *Schubert cell* in $\mathcal{P}_q(n)$ corresponding to b is the set

$$\mathcal{S}_q(b) = \{U \in \mathcal{P}_q(n) | \mathrm{prof}(U) = b\}.$$

Some papers denote this set as $\mathrm{prof}^{-1}(b)$.

Given any binary vector b of length n and Hamming weight k, the permutation matrix with respect to b, denoted by $P(b)$, is the $n \times n$ permutation matrix whose rows indexed by $\mathrm{supp}(b)$ form $P(b)_{supp(b)} = \left(I_k \,\middle|\, 0_{k\times(n-k)} \right)$ and the remaining rows of $P(b)$ form $P(b)_{supp(\bar{b})} = \left(0_{(n-k)\times k} \,\middle|\, I_{(n-k)} \right)$, where $b + \bar{b}$ is the all one vector of length n.

Example 2.7. *Let $b = (1, 0, 0, 1, 0)$. So $\bar{b} = (0, 1, 1, 0, 1)$.*

$$P(b) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

We changed some notations in the next definition to be consistent with our earlier notations but the essence is exactly the same.

Definition 2.8. *[6] Let b be a binary vector of length n and Hamming weight k. For $X \in M_{k\times(n-k)}(\mathbb{F}_q)$, define the generalized lifting of X with respect to b, denoted by $\Lambda_b(X)$, as*

$$\Lambda_b(X) = \langle L(X)\rangle P(b)^{-1} = \langle L(X)P(b)^{-1}\rangle.$$

Definition 2.9. *[6] Let b be a binary vector of length n, Hamming weight k and let $\mathcal{C}_b$ be a $[k \times (n-k)]$ rank-metric code. The set*

$$\Lambda_b(\mathcal{C}_b) = \{\Lambda_b(C) | C \in \mathcal{C}_b\}$$

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

We now present some necessary conditions for the definition of lifted FD codes which were established in [6]. Let $Q = [a_{ij}]$ be the $n \times n$ upper triangular matrix with $a_{ij} = 1$ if $j \geq i$ and $a_{ij} = 0$ otherwise. Given a binary profile vector b of length n and Hamming weight k, regarded as an element of $\mathbb{Z}^{1\times n}$, define the vector $c(b) \in \mathbb{Z}^{1\times n}$ via

$$c(b) = bQP(b).$$

Let $X = [x_{ij}] \in M_{k\times(n-k)}(\mathbb{F}_q)$. According to [6], $\Lambda_b(X)$ is guaranteed to be in the Schubert cell corresponding to b provided that for $1 \leq i \leq k$ and $1 \leq j \leq n-k$,

$$i > c(b)_{j+k} \text{ implies that } x_{ij} = 0. \tag{3}$$

An *FD(b) code* is a rank-metric code $\mathcal{C}_b \subseteq M_{k\times(n-k)}(\mathbb{F}_q)$ in which each codeword satisfies (3) while the code $\Lambda_b(\mathcal{C}_b)$ is referred to as *lifted FD(b) code.*

We now consider the minimum distance between elements in distinct Schubert cells. Let $u, v \in \mathbb{F}_2^n$ and $u \neq v$. Now define the logical AND of u and v, denoted by $u \wedge v$, as $(u \wedge v)_i = u_i v_i$. Also the asymmetric distance between u and v, denoted by $d_a(u, v)$, is given by $d_a(u, v) = \max\{wt_H(u), wt_H(v)\} - wt_H(u \wedge v)$.

Theorem 2.10. *[5] Let $u, v \in \mathbb{F}_2^n$, $u \neq v$, $U \in S_q(u)$ and $V \in S_q(v)$ and $d(U, V)$ be the injection distance of U and V. Then $d(U, V) \geq d_a(u, v)$.*

The following steps to construct an $(n, M, d, k)_q$ code $\mathcal{C}$ are from [5].

1. Choose a binary constant weight code $\mathcal{B}$ of length n, Hamming weight k, and minimum asymmetric distance d.
2. For each $b \in \mathcal{B}$, consider an FD(b) code with minimum rank distance d.
3. Construct the lifted FD(b) code $\Lambda_b(\mathcal{C}_b)$ for each $b \in \mathcal{B}$.
4. Set $\mathcal{C} = \displaystyle\bigcup_{b\in\mathcal{B}} \Lambda_b(\mathcal{C}_b)$

The cardinality M of $\mathcal{C}$ greatly depends on the choice of $\mathcal{B}$.

Theorem 2.11. *[2] $\mathcal{C}$ is an $(n, M, d, k)_q$ constant-dimension code, where $M = \sum_{b\in\mathcal{B}} |\Lambda_b(\mathcal{C}_b)|$.*

3. Rank-metric codes and Grassmannian codes

The following well-known theorem will be the cornerstone of our construction.

Theorem 3.1. *[9] Let $f(x) = \sum_{i=0}^{k} a_i x^i \in \mathbb{F}_q[x]$ be a monic irreducible polynomial and X be its companion matrix. Then the mapping*

$$\pi : \mathbb{F}_q[x] \to M_k(\mathbb{F}_q), g(x) \mapsto g(X) \tag{4}$$

induces a unital embedding

$$\tau : \mathbb{F}_q[x]/(f) = \mathbb{F}_{q^k} \to M_k(\mathbb{F}_q). \tag{5}$$

Let n be a positive integer. Note that τ can be extended to the following monomorphism ϕ defined by $\phi : \mathbb{F}_{q^k}^n \to M_{k\times kn}(\mathbb{F}_q)$ where

$$\phi(\alpha_1, \alpha_2, ..., \alpha_n) = \begin{pmatrix} \tau(\alpha_1) & \tau(\alpha_2) & \dots & \tau(\alpha_n) \end{pmatrix}.$$

Lemma 3.2. *If C is a linear block code of length n over $\mathbb{F}_{q^k}$ then $C \cong \phi(C)$ as $\mathbb{F}_q-$vector spaces.*

The following theorem is a generalization of Theorem 3.7 of [4].

Theorem 3.3. *Let C be a linear block code of length n over $\mathbb{F}_{q^k}$ and ρ its dimension as an $\mathbb{F}_q$-vector space. Then*

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

ii. $\Lambda(\phi(C))$ is a $(k + kn, q^\rho, k, k)_q$ code,

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

Proof. Let C be a linear block code of length n over $\mathbb{F}_{q^k}$ and ρ its dimension as an $\mathbb{F}_q$-vector space. By Lemma 3.2, C and $\phi(C)$ are isomorphic as $\mathbb{F}_q-$vector spaces. Hence, the dimension of $\phi(C)$ is ρ. Consider the case $n = 1$. Since $\mathbb{F}_{q^k}$ is a field, then $\forall \alpha \in \mathbb{F}_{q^k} - \{0\}, \phi(\alpha) = \tau(\alpha) \in M_k(\mathbb{F}_q)$ is a unit and thus has rank k, where τ is as defined in (5). Thus, $\begin{pmatrix} \tau(\alpha_1) & \tau(\alpha_2) & \dots & \tau(\alpha_n) \end{pmatrix}$ has rank k for any positive integer n where $\alpha_i \in \mathbb{F}_{q^k} - \{0\}$ for some i, $1 \le i \le n$. Therefore, by Theorem 2.1, the minimum distance of $\phi(C)$ is k.

Clearly, ii. follows directly from Theorem 2.5

If $\Lambda(\phi(C))$ is a $(k + kn, q^\rho, k, k)_q$ code, the minimum injection distance of $\Lambda(\phi(C))$ is k. Let $A, B \in \Lambda(\phi(C))$. We have $k \le d(A, B) = \max\{\dim A, \dim B\} - \dim(A \cap B)$. Hence, $k \le k - \dim(A \cap B)$ which makes $\dim(A \cap B)$ to be equal to 0. Therefore, the pairwise intersection of codewords of $\Lambda(\phi(C))$ is trivial. □

Note that for any positive integer n, the rank-metric code $\phi(\mathbb{F}_{q^k}^n)$ meets the Singleton bound as given in Theorem 9 of [7].

Example 3.4. *Consider the irreducible polynomial $x^2 + x + 1$ over $\mathbb{F}_2$ and its companion matrix $X = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, and the linear block code $\mathbb{F}_4^2$. Then $\phi(\mathbb{F}_4^2)$ is a $[2 \times 4, 4, 2]$ rank-metric code which satisfies the Singleton bound. Moreover, $\Lambda(\phi(\mathbb{F}_4^2))$ is a $(6, 16, 2, 2)_2-$code.*

4. Anticode-optimal Grassmannian code

Now we construct Grassmannian codes using the multi-level construction in [2] and the result in Theorem 3.3. Let n be a multiple of k and $n > k$. For the skeleton code $\mathcal{B}$, choose

$$\mathcal{B} = \{b_\ell = (\underbrace{0,\cdots,0}_{n-k-k\ell},\underbrace{1,\cdots,1}_{k},\underbrace{0,\cdots,0}_{k\ell}) | 0 \leq \ell \leq \frac{n-k}{k}\}.$$

Clearly, $\mathcal{B}$ is a binary constant weight code of length n, weight k, and minimum asymmetric distance k.

Then for $0 \leq \ell \leq \frac{n-k}{k}$

$$P(b_\ell) = \begin{pmatrix} & I_{n-k-k\ell} & \\ I_k & & \\ & & I_{k\ell} \end{pmatrix}.$$

Let $Q = [a_{ij}]$ be the $n \times n$ upper triangular matrix with $a_{ij} = 1$ if $j \geq i$ and $a_{ij} = 0$ otherwise. Then,

$$\begin{aligned} c(b_\ell) &= b_\ell Q P(b_\ell) \\ &= (\underbrace{0,\cdots,0}_{n-k-k\ell},\underbrace{1,\cdots,1}_{k},\underbrace{0,\cdots,0}_{k\ell}) Q P(b_\ell) \\ &= (\underbrace{0,\cdots,0}_{n-k-k\ell},1,2,\cdots,k,\underbrace{k,\cdots,k}_{k\ell}) P(b_\ell). \\ &= (1,2,\cdots,k,\underbrace{0,\cdots,0}_{n-k-k\ell},\underbrace{k,\cdots,k}_{k\ell}) \end{aligned}$$

Lemma 4.1. *Let n be a multiple of k, $n > k$ and*

$$\mathcal{C}_{b_\ell} = \left\{ \begin{pmatrix} 0_{k\times(n-k-k\ell)} & \phi(v) \end{pmatrix} \middle| v \in \mathbb{F}_{q^k}^{\ell} \right\}$$

where $1 \leq \ell \leq \frac{n-k}{k}$. Then, for $1 \leq \ell \leq \frac{n-k}{k}$, $\mathcal{C}_{b_\ell}$ is an FD(b_ℓ) code and has minimum rank distance k.

Proof. Recall that for a rank-metric code $\mathcal{C}$ to be an FD(b) code, $\mathcal{C}$ must be a subset of $M_{k\times(n-k)}(\mathbb{F}_q)$ and all of its codewords must satisfy (3). Let $1 \leq \ell \leq \frac{n-k}{k}$. Clearly, $\mathcal{C}_{b_\ell} \subseteq M_{k\times(n-k)}(\mathbb{F}_q)$. Now let $X = [x_{ij}] \in \mathcal{C}_{b_\ell}$. By (3), for $1 \leq i \leq k$, $1 \leq j \leq n-k$, $i > c(b_\ell)_{j+k}$ implies that $x_{ij} = 0$. Notice that in (3), we only check the last $n-k$ components of $c(b_\ell)$. Now

$$c(b_\ell)_{j+k} = \begin{cases} 0 & \text{if } 1 \leq j \leq n-k-k\ell \\ k & \text{if } n-k-k\ell < j \leq n-k. \end{cases}$$

Hence the entries in the first $n-k-k\ell$ columns of the elements of $\mathcal{C}_{b_\ell}$ must be all zero. Clearly, $\mathcal{C}_{b_\ell}$ satisfies this. Lastly, by Theorem 3.3, $\phi(v)$ has minimum rank distance k. Clearly, $\mathcal{C}_{b_\ell}$ has minimum rank distance k. □

Theorem 4.2. *The rank-metric code $\mathcal{C}_{b_0} = \{(0_{k\times(n-k)})\}$ is an FD(b_0) code.*

Although $\mathcal{C}_{b_0}$ does not have a minimum distance k as required in [2] and [6], it will not pose any problem since the resulting Grassmannian will still have a minimum distance k. Ironically, b_0 is included in Example 10 of [2]. Note also that $\mathcal{C}_{b_0}$ is the only rank-metric code that will satisfy b_0.

Now we are ready to construct the lifted FD(b) code $\Lambda_b(\mathcal{C}_b)$. By Definition 2.8 and Definition 2.9,

$$\Lambda_{b_\ell}(\mathcal{C}_{b_\ell}) = \begin{cases} \left\{ \left\langle \begin{array}{ccc} 0_{k\times(n-k-k\ell)} & I_k & \phi(v) \end{array} \right\rangle \middle| v \in \mathbb{F}_{q^k}^{\ell} \right\}, & 1 \le \ell \le \frac{n-k}{k} \\ \left\{ \left\langle \begin{array}{cc} 0_{k\times(n-k)} & I_k \end{array} \right\rangle \right\}, & \ell = 0. \end{cases}$$

The lifted FD code, denoted by $\Omega(\mathcal{B})$, is given by

$$\Omega(\mathcal{B}) = \bigcup_{b\in\mathcal{B}} \Lambda_b(\mathcal{C}_b).$$

As an immediate consequence of Lemma 4.1 and Theorem 4.2, we have the following theorem.

Theorem 4.3. *$\Omega(\mathcal{B})$ is an $\left(n, \frac{q^n-1}{q^k-1}, k, k\right)_q$ code.*

Since $\mathcal{C}_{b_0}$ does not have a minimum distance k and b_0 appeared only as an example in [2], we will separate the case of b_0 in our proof.

Proof. For $1 \le \ell \le \frac{n-k}{k}$, $\mathcal{C}_{b_\ell}$ is an FD(b_ℓ) code with minimum rank distance k by Lemma 4.1. Now,

$$\Omega(\mathcal{B}) = \bigcup_{b\in\mathcal{B}} \Lambda_b(\mathcal{C}_b) = \left(\bigcup_{b\in\mathcal{B}, b\neq b_0} \Lambda_b(\mathcal{C}_b) \right) \cup \Lambda_b(\mathcal{C}_{b_0}).$$

By Theorem 2.11, $\bigcup_{b\in\mathcal{B},b\neq b_0} \Lambda_b(\mathcal{C}_b)$ is an $(n, M, k, k)_q$ code where $M = \sum_{b\in\mathcal{B},b\neq b_0} |\Lambda_b(\mathcal{C}_b)|$. Clearly, $\Lambda_{b_0}(\mathcal{C}_{b_0}) \subseteq \mathcal{G}_q(n,k)$. Now we compute for the distance of codewords $U \in \bigcup_{b\in\mathcal{B},b\neq b_0} \Lambda_b(\mathcal{C}_b)$ and $V \in \Lambda_{b_0}(\mathcal{C}_{b_0})$. Since $U \in \bigcup_{b\in\mathcal{B},b\neq b_0} \Lambda_b(\mathcal{C}_b)$, then $U \in \Lambda_{b_\ell}(\mathcal{C}_{b_\ell})$ for some $b_\ell \in \mathcal{B} - \{b_0\}$. By Theorem 2.10, $d(U,V) \ge d_a(b_\ell, b_0) \ge k - 0 = k$. Note that $\Lambda_{b_0}(\mathcal{C}_{b_0})$ has only one codeword. Therefore, $\Omega(\mathcal{B})$ has minimum distance k.

Observe that $\Lambda_{b_\ell}(\mathcal{C}_{b_\ell}) \cap \Lambda_{b_j}(\mathcal{C}_{b_j}) = \emptyset$, where $\ell \neq j$. Hence,

$$|\Omega(\mathcal{B})| = \sum_{b\in\mathcal{B}} |\Lambda_b(\mathcal{C}_b)| = \sum_{i=0}^{\frac{n-k}{k}} q^{ki} = \frac{q^n-1}{q^k-1}.$$

□

Note that $\Omega(\mathcal{B})$ attains the Anticode bound. The following illustrates the construction of an Anticode-optimal Grassmannian code.

Example 4.4. *Consider the irreducible polynomial x^3+x+1 over $\mathbb{F}_2$, its companion matrix $X = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$,*

$$\phi_1 : \mathbb{F}_{2^3} \to M_{3\times3}(\mathbb{F}_2), \alpha_1 \mapsto \tau(\alpha_1),$$

$$\phi_2 : \mathbb{F}_{2^3}^2 \to M_{3\times6}(\mathbb{F}_2), (\alpha_1,\alpha_2) \mapsto \left(\tau(\alpha_1) \,|\, \tau(\alpha_2) \right),$$

and the skeleton code

$$\mathcal{B} = \{b_\ell = (\underbrace{0,\cdots,0}_{6-3\ell}, \underbrace{1,\cdots,1}_{3}, \underbrace{0,\cdots,0}_{3\ell}) | 0 \le \ell \le 2\}.$$

Now,

$$\mathcal{C}_{b_0} = \{0_{3\times 6}\}$$

$$\mathcal{C}_{b_1} = \{(0_{3\times 3}|\phi_1(v)) : v \in \mathbb{F}_{2^3}\}$$

$$\mathcal{C}_{b_2} = \{\phi_2(v) : v \in \mathbb{F}_{2^3}^2\}.$$

So

$$\Lambda_{b_0}(\mathcal{C}_{b_0}) = \{\langle 0_{3\times 6}|I_3\rangle\}$$

$$\Lambda_{b_1}(\mathcal{C}_{b_1}) = \{\langle 0_{3\times 3}|I_3|\phi_1(v)\rangle : v \in \mathbb{F}_{2^3}\}$$

$$\Lambda_{b_2}(\mathcal{C}_{b_2}) = \{\langle I_3|\phi_2(v)\rangle : v \in \mathbb{F}_{2^3}^2\}.$$

Finally, $\Omega(\mathcal{B}) = \Lambda_{b_0}(\mathcal{C}_{b_0}) \cup \Lambda_{b_1}(\mathcal{C}_{b_1}) \cup \Lambda_{b_2}(\mathcal{C}_{b_2})$ *with cardinality* $1 + 8 + 64 = 73 = \mathcal{A}_2(9, 3, 3)$.

Theorem 4.3 is a generalization of Theorem 3.16 in [4] and is similar with the construction of spread codes in [8]. Note that by choosing v to be in a different linear block code C of length ℓ over $\mathbb{F}_{q^k}$ instead of $\mathbb{F}_{q^k}^{\ell}$ in Lemma 4.1, one may construct a Grassmannian code that is not a spread code.

5. Summary and conclusion

We presented two constructions of Grassmannian codes for any length, over any finite field and whose dimension is equal to its minimum injection distance. These two constructions are generalizations of some constructions in [4]. The first construction uses a linear block code to construct a rank-metric code. The resulting rank-metric code was then used to create a Grassmannian code that meets the Singleton bound. The second construction uses the results in the first construction together with the concept of Ferrers diagram to get an anticode-optimal Grassmannian code. The resulting code from the second construction is similar to the construction of spread codes found in [8].

Acknowledgment: The authors would like to thank the reviewer for his/her valuable comments.

References

[1] T. Etzion, Subspace codes − bounds and constructions, 1st European Training School on Network Coding, Barcelona, Spain, (2013).
[2] T. Etzion, N. Silberstein, Error-Correcting codes in projective spaces via rank-metric codes and Ferrers diagrams, IEEE Trans. Inform. Theory 55(7) (2009) 2909–2919.
[3] T. Etzion, A. Vardy, Error-correcting codes in projective space, IEEE Trans. Inform. Theory 57(2) (2011) 1165–1173,
[4] B. Hernandez, V. Sison, Grassmannian codes as lifts of matrix codes derived as images of linear block codes over finite fields, Global Journal of Pure and Applied Mathematics 12(2) (2016) 1801–1820.
[5] A. Khaleghi, F. R. Kschischang, Projective space codes for the injection metric, In: Proc. 11th Canadian Workshop on Information Theory, Ottawa, 54(8) (2009) 9–12.
[6] A. Khaleghi, D. Silva, F. R. Kschischang, Subspace codes, IMA Int. Conf. 49(4) (2009) 1–21.

[7] R. Koetter, F. R. Kschischang, Coding for errors and erasures in random network coding, IEEE Trans. Inform. Theory 54(8) (2008) 3579–3591.

[8] F. Manganiello, E. Gorla, J. Rosenthal, Spread codes and spread decoding in network coding, In: Proc. 2008 IEEE ISIT, Toronto, Canada, (2008) 851–855.

[9] A. J. Menezes, I. F. Blake, X. Gao, R. C. Mullen, S. A. Vanstine, T. Yaghoobian, Applications of finite fields, Boston, MA: Kluwer Academic Publishers 1993.

[10] D. Silva, F. R. Kschischang, R. Koetter, A rank-metric approach to error control in random network coding, IEEE Trans. Inform. Theory 54(9) (2008) 3951–3967.

[11] H. Wang, C. Xing, R. Safavi-Naini, Linear authentication codes: bounds and constructions, IEEE Trans. Inform. Theory 49(4) (2003) 866–872.