Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2014, Article ID 497958, 9 pages
http://dx.doi.org/10.1155/2014/497958

Research Article

Bounds on Subspace Codes Based on Subspaces of Type $(m, 1)$ in Singular Linear Space

You Gao and Gang Wang

College of Science, Civil Aviation University of China, Tianjin 300300, China

Correspondence should be addressed to You Gao; gao_you@263.net

Received 7 March 2014; Revised 7 July 2014; Accepted 15 July 2014; Published 5 August 2014

Academic Editor: Qi Cheng

The Sphere-packing bound, Singleton bound, Wang-Xing-Safavi-Naini bound, Johnson bound, and Gilbert-Varshamov bound on the subspace codes $(n+l, M, d, (m, 1))_q$ based on subspaces of type $(m, 1)$ in singular linear space $\mathbb{F}_q^{(n+l)}$ over finite fields $\mathbb{F}_q$ are presented. Then, we prove that codes based on subspaces of type $(m, 1)$ in singular linear space attain the Wang-Xing-Safavi-Naini bound if and only if they are certain Steiner structures in $\mathbb{F}_q^{(n+l)}$.

1. Introduction

Let $\mathbb{F}_q$ be a finite field with q elements, where q is a power of a prime and $\mathbb{F}_q^{(n)}$ is the n-dimensional row vector space over $\mathbb{F}_q$, where n is a positive integer. The set of all the subspaces with dimension k of $\mathbb{F}_q^{(n)}$ is called Grassmannian space over $\mathbb{F}_q$, denoted by $\mathcal{G}_q(n, k)$. The set of all the subspaces of $\mathbb{F}_q^{(n)}$, including $\{0\}$ and $\mathbb{F}_q^{(n)}$, is called projective space of order n over $\mathbb{F}_q$, denoted by $\mathcal{P}_q(n)$. For any subspaces U and V in $\mathcal{P}_q(n)$, define the distance function between U and V as

$$d(U, V) = \dim U + \dim V - 2\dim(U \cap V). \qquad (1)$$

The function above is proved a metric (see [1]); thus, $\mathcal{P}_q(n)$ can be regarded as a metric space.

A nonempty collection $\mathbb{C}$ of projective space $\mathcal{P}_q(n)$ is called a subspace code and the subspaces in $\mathbb{C}$ are codewords of code $\mathbb{C}$. The minimum distance of a subspace code $\mathbb{C}$ is

$$d(\mathbb{C}) = \min\{d(U, V) : U \neq V, U, V \in \mathbb{C}\}. \qquad (2)$$

A subspace code $\mathbb{C}$ is denoted by $(n, M, d)_q$, if the size of codewords is M and the minimum distance of $\mathbb{C}$ is d. Furthermore, if $\mathbb{C} \subseteq \mathcal{G}_q(n, k)$, $\mathbb{C}$ is denoted by $(n, M, d, k)_q$.

Subspace code plays an important role in random network coding (see [2, 3]). Koetter et al. [4, 5] defined an operator channel when they studied random network coding. Meanwhile, they showed that the errors and erasures could be corrected by a subspace code $(n, M, d, k)_q$ over the operator channel if the sum of errors and erasures is less than $d/2$. These research results motivate many domestic and overseas scholars' great interest in subspace codes (see [3–8]).

Bounds on subspace codes and optimal subspace codes in projective space are considered in recent years. Koetter and Kschischang [1] provided Sphere-packing bound and Singleton bound on subspace codes in projective space, which are regarded as a counterpart of the classical Sphere-packing bound and Singleton bound [9]. Wang et al. [10] provided the Wang-Xing-Safavi-Naini bound on subspace codes in projective space. Etzion and Vardy [11] provided Johnson bound and Gilbert-Varshamov bound on subspace codes in projective space. Meanwhile, Xia and Fu [12] proved that codes in projective space achieved the Wang-Xing-Safavi-Naini bound if and only if they are certain Steiner structures [13, 14] in $\mathbb{F}_q^{(n)}$.

In this paper, denote by $\mathcal{M}(m, 1; n+l, n)$ the collection of all the subspaces of type $(m, 1)$ in $(n+l)$-dimensional singular linear space $\mathbb{F}_q^{(n+l)}$, where $1 \leq m \leq n+1$. For any two subspaces U and V of type $(m, 1)$ in $\mathcal{M}(m, 1; n+l, n)$, the natural distance function between U and V in $\mathcal{M}(m, 1; n+l, n)$ is defined as

$$d(U, V) = 2m - 2\dim(U \cap V). \qquad (3)$$

A nonempty collection $\mathbb{C}$ of $\mathcal{M}(m,1;n+l,n)$ is called an $(n+l,M,d,(m,1))_q$ code if it has the size of codewords M and the minimum distance d. Denote by $\mathcal{A}_q(n+l,d,(m,1))$ the maximum number of codewords in an $(n+l,M,d,(m,1))_q$ code. The goal of this paper is to determine bounds of $\mathcal{A}_q(n+l,d,(m,1))$ and construct the corresponding optimal subspace codes.

The Sphere-packing bound, Singleton bound, Wang-Xing-Safavi-Naini bound, Johnson bound, and Gilbert-Varshamov bound on the subspace codes $(n+l,M,d,(m,1))_q$ based on subspaces of type $(m,1)$ in singular linear space $\mathbb{F}_q^{(n+l)}$ over $\mathbb{F}_q$ are given for the first time in this paper. We prove that the Steiner structure $\mathbb{S}_q((m-\delta+1,0),(m,1),n+l)$ is an $(n+l,M,2\delta,(m,1))_q$ code, which attains the Wang-Xing-Safavi-Naini bound. The study of optimal subspace codes is one of the main research problems in coding theory. The obtained bounds are of vital importance to construct the optimal subspace codes.

The rest of the paper is organized as follows. In Section 2, the relevant concepts of $(n+l)$-dimensional singular linear space $\mathbb{F}_q^{(n+l)}$ over $\mathbb{F}_q$ are introduced and the anzahl formulas in singular linear space $\mathbb{F}_q^{(n+l)}$ are given. In Section 3, the Sphere-packing bound, Singleton bound, Wang-Xing-Safavi-Naini bound, Johnson bound, and Gilbert-Varshamov bound on the subspace codes $(n+l,M,d,(m,1))_q$ based on subspaces of type $(m,1)$ in singular linear space $\mathbb{F}_q^{(n+l)}$ over $\mathbb{F}_q$ are presented. In Section 4, we prove that the Steiner structure $\mathbb{S}_q((m-\delta+1,0),(m,1),n+l)$ is an $(n+l,M,2\delta,(m,1))_q$ code, which attains the Wang-Xing-Safavi-Naini bound. That is, the Steiner structure $\mathbb{S}_q((m-\delta+1,0),(m,1),n+l)$ is an optimal subspace code. In Section 5, a conclusion is made for this paper.

2. Preliminaries

Let $\mathbb{F}_q$ be a finite field with q elements, where q is a prime power. $\mathbb{F}_q^{(n+l)}$ is the $(n+l)$-dimensional row vector space over $\mathbb{F}_q$, where n and l are two nonnegative integers. The set of all $(n+l)\times(n+l)$ nonsingular matrices over $\mathbb{F}_q$ of the form

$$\begin{pmatrix} T_{11} & T_{12} \\ 0 & T_{22} \end{pmatrix}, \tag{4}$$

where T_{11} and T_{22} are nonsingular $n\times n$ and $l\times l$ matrices, respectively, forms a group under matrix multiplication, called the singular general linear group of degree $n+l$ over $\mathbb{F}_q$ and denoted by $\mathrm{GL}_{n+l,n}(\mathbb{F}_q)$.

We have an action of $\mathrm{GL}_{n+l,n}(\mathbb{F}_q)$ on $\mathbb{F}_q^{(n+l)}$ defined as follows:

$$\begin{gathered} \mathbb{F}_q^{(n+l)} \times \mathrm{GL}_{n+l,n}(\mathbb{F}_q) \longrightarrow \mathbb{F}_q^{(n+l)}, \\ ((x_1,\ldots,x_n,x_{n+1},\ldots,x_{n+l}),T) \longmapsto (x_1,\ldots,x_n,\ldots,x_{n+l})\,T. \end{gathered} \tag{5}$$

The vector space $\mathbb{F}_q^{(n+l)}$, together with the above group action, is called the $(n+l)$-dimensional singular linear space over $\mathbb{F}_q$ (see [15]).

Let e_i $(1\le i\le n+l)$ be the row vector in $\mathbb{F}_q^{(n+l)}$ whose ith coordinate is 1 and all other coordinates are 0. Denote by E the l-dimensional subspace of $\mathbb{F}_q^{(n+l)}$ generated by $e_{n+1},e_{n+2},\ldots,e_{n+l}$. An m-dimensional subspace P of $\mathbb{F}_q^{(n+l)}$ is called a subspace of type (m,k) if $\dim(P\cap E)=k$.

Introduce the anzahl formulas (see [15]) and use the Gaussian coefficient [16] for brevity:

$$\begin{bmatrix} m_2 \\ m_1 \end{bmatrix}_q = \frac{\prod_{t=m_2-m_1+1}^{m_2}(q^t-1)}{\prod_{t=1}^{m_1}(q^t-1)}. \tag{6}$$

By convenience, $\left[\begin{smallmatrix} m_2 \\ 0 \end{smallmatrix}\right]_q=1$ and $\left[\begin{smallmatrix} m_2 \\ m_1 \end{smallmatrix}\right]_q=0$ whenever $m_1<0$ and $m_2<m_1$.

Denote the set of all the subspaces of type (m,k) in $\mathbb{F}_q^{(n+l)}$ by $\mathcal{M}(m,k;n+l,n)$ and let

$$N(m,k;n+l,n)=|\mathcal{M}(m,k;n+l,n)|. \tag{7}$$

It is verified that $\mathcal{M}(m,k;n+l,n)$ is nonempty if and only if

$$0\le k\le l,\qquad 0\le m-k\le n. \tag{8}$$

Moreover, if $\mathcal{M}(m,k;n+l,n)$ is nonempty, then

$$N(m,k;n+l,n)=q^{(m-k)(l-k)}\begin{bmatrix} n \\ m-k \end{bmatrix}_q\begin{bmatrix} l \\ k \end{bmatrix}_q. \tag{9}$$

Let P be a fixed subspace of type (m,k) in $\mathbb{F}_q^{(n+l)}$. Denote by $\mathcal{M}(m_1,k_1;m,k;n+l,n)$ the set of all the subspaces of type (m_1,k_1) contained in P. Let

$$N(m_1,k_1;m,k;n+l,n)=\left|\mathcal{M}(m_1,k_1;m,k;n+l,n)\right|. \tag{10}$$

It is verified that $\mathcal{M}(m_1,k_1;m,k;n+l,n)$ is nonempty if and only if

$$0\le k_1\le k\le l,\qquad 0\le m_1-k_1\le m-k\le n. \tag{11}$$

Moreover, if $\mathcal{M}(m_1,k_1;m,k;n+l,n)$ is nonempty, then

$$N(m_1,k_1;m,k;n+l,n)=q^{(m_1-k_1)(k-k_1)}\begin{bmatrix} m-k \\ m_1-k_1 \end{bmatrix}_q\begin{bmatrix} k \\ k_1 \end{bmatrix}_q. \tag{12}$$

Let P be a fixed subspace of type (m_1,k_1) in $\mathbb{F}_q^{(n+l)}$. Denote by $\mathcal{M}'(m_1,k_1;m,k;n+l,n)$ the set of all the subspaces of type (m,k) containing P. Let

$$N'(m_1,k_1;m,k;n+l,n)=\left|\mathcal{M}'(m_1,k_1;m,k;n+l,n)\right|. \tag{13}$$

It is verified that $\mathcal{M}'(m_1,k_1;m,k;n+l,n)$ is nonempty if and only if

$$0\le k_1\le k\le l,\qquad 0\le m_1-k_1\le m-k\le n. \tag{14}$$

Moreover, if $\mathcal{M}'(m_1,k_1;m,k;n+l,n)$ is nonempty, then

$$\begin{aligned} N'&(m_1,k_1;m,k;n+l,n) \\ &= q^{(l-k)(m-k-m_1+k_1)}\begin{bmatrix} n-(m_1-k_1) \\ (m-k)-(m_1-k_1) \end{bmatrix}_q\begin{bmatrix} (l-k_1) \\ (k-k_1) \end{bmatrix}_q. \end{aligned} \tag{15}$$

3. Bounds on Subspace Codes Based on Subspaces of Type $(m,1)$ in Singular Linear Space

Denote by $\mathscr{A}_q(n+l,d,(m,1))$ the maximum number of codewords in an $(n+l,M,d,(m,1))_q$ code based on subspaces of type $(m,1)$ in singular linear space $\mathbb{F}_q^{(n+l)}$. By (3), the distance of any two elements in $\mathscr{M}(m,1;n+l,n)$ must be an even number; thus, we only need to consider $\mathscr{A}_q(n+l,d,(m,1))$ for even $d=2\delta$.

Definition 1. The sphere $S(V,(m,1),t)$ of radius t centered at a subspace V of type $(m,1)$ in $\mathscr{M}(m,1;n+l,n)$ is defined as the set of all subspaces U of type $(m,1)$ in $\mathscr{M}(m,1;n+l,n)$ that satisfy $d(U,V)\le 2t$. That is,

$$S(V,(m,1),t)=\{U\in\mathscr{M}(m,1;n+l,n):d(U,V)\le 2t\}. \tag{16}$$

Theorem 2. *The number of subspaces of type $(m,1)$ in $S(V,(m,1),t)$ is independent of the choice of V and*

$$\begin{aligned}|S(V,(m,1),t)| &= \sum_{i=0}^{t}\big(N_q(n+l,(m,1),(m,1),(m-i,1)) \\ &\quad +N_q(n+l,(m,1),(m,1),(m-i,0))\big),\end{aligned} \tag{17}$$

where $V\in\mathscr{M}(m,1;n+l,n)$ is a fixed subspace of type $(m,1)$ in $\mathbb{F}_q^{(n+l)}$. $N_q(n+l,(m,1),(m,1),(m-i,1))$ is the number of elements $W\in\mathscr{M}(m,1;n+l,n)$ satisfying

$$V\cap W\in\mathscr{M}(m-i,1;n+l,n). \tag{18}$$

$N_q(n+l,(m,1),(m,1),(m-i,0))$ is the number of elements $W\in\mathscr{M}(m,1;n+l,n)$ satisfying

$$V\cap W\in\mathscr{M}(m-i,0;n+l,n). \tag{19}$$

Proof. Let $V\in\mathscr{M}(m,1;n+l,n)$ be a fixed subspace of type $(m,1)$ in $\mathbb{F}_q^{(n+l)}$. Let $N_q(n+l,(m,1),(j,1),(s,1))$ denote the number of elements $W\in\mathscr{M}(j,1;n+l,n)$ satisfying $W\cap V\in\mathscr{M}(s,1;n+l,n)$. Choose the subspace of type $(s,1)$ of intersection in

$$N(s,1;m,1;n+l,n)=\begin{bmatrix}m-1\\ s-1\end{bmatrix}_q \tag{20}$$

ways. Once this is done, the subspace can be extended to a subspace of type $(j,1)$ in

$$\begin{aligned}&\big((q^{n+l}-q^m-q^l)(q^{n+l}-q^{m+1}-q^l)\\ &\quad\cdots(q^{n+l}-q^{m+j-s-1}-q^l)\big)\\ &\times\big((q^j-q^s)(q^j-q^{s+1})\cdots(q^j-q^{j-1})\big)^{-1}\end{aligned} \tag{21}$$

ways. Thus,

$$\begin{aligned}&N_q(n+l,(m,1),(j,1),(s,1))\\ &\quad=\begin{bmatrix}m-1\\ s-1\end{bmatrix}_q\\ &\qquad\times\big((q^{n+l}-q^m-q^l)(q^{n+l}-q^{m+1}-q^l)\\ &\qquad\quad\cdots(q^{n+l}-q^{m+j-s-1}-q^l)\big)\\ &\qquad\times\big((q^j-q^s)(q^j-q^{s+1})\cdots(q^j-q^{j-1})\big)^{-1}.\end{aligned} \tag{22}$$

From this,

$$\begin{aligned}&N_q(n+l,(m,1),(m,1),(m-i,1))\\ &\quad=\begin{bmatrix}m\\ i\end{bmatrix}_q\times\big((q^{n+l}-q^m-q^l)(q^{n+l}-q^{m+1}-q^l)\\ &\qquad\cdots(q^{n+l}-q^{m+i-1}-q^l)\big)\\ &\qquad\times\big((q^m-q^{m-i})(q^m-q^{m-i+1})\cdots(q^m-q^{m-1})\big)^{-1}.\end{aligned} \tag{23}$$

Let $N_q(n+l,(m,1),(j,1),(s,0))$ denote the number of elements $W\in\mathscr{M}(j,1;n+l,n)$ satisfying $W\cap V\in\mathscr{M}(s,0;n+l,n)$. Choose the subspace of type $(s,0)$ of intersection in

$$N(s,0;m,1;n+l,n)=q^s\begin{bmatrix}m-1\\ s\end{bmatrix}_q \tag{24}$$

ways. Once this is done, the subspace can be extended to a subspace of type $(j,1)$ in

$$\begin{aligned}&\left(\frac{q^l-1}{q-1}-1\right)\\ &\quad\times\big((q^{n+l}-q^m-q^l)(q^{n+l}-q^{m+1}-q^l)\\ &\qquad\cdots(q^{n+l}-q^{m+j-s-2}-q^l)\big)\\ &\quad\times\big((q^j-q^{s+1})(q^j-q^{s+2})\cdots(q^j-q^{j-1})\big)^{-1}\end{aligned} \tag{25}$$

ways. Thus,

$$\begin{aligned}&N_q(n+l,(m,1),(j,1),(s,0))\\ &\quad=q^s\begin{bmatrix}m-1\\ s\end{bmatrix}_q\left(\frac{q^l-1}{q-1}-1\right)\\ &\qquad\times\big((q^{n+l}-q^m-q^l)(q^{n+l}-q^{m+1}-q^l)\\ &\qquad\quad\cdots(q^{n+l}-q^{m+j-s-2}-q^l)\big)\\ &\qquad\times\big((q^j-q^{s+1})(q^j-q^{s+2})\cdots(q^j-q^{j-1})\big)^{-1}.\end{aligned} \tag{26}$$

From this,

$$
\begin{aligned}
& N_q(n+l,(m,1),(m,1),(m-i,0)) \\
& = q^{m-i} \begin{bmatrix} m-1 \\ i-1 \end{bmatrix}_q \left(\frac{q^l - 1}{q-1} - 1 \right) \\
& \times \left(\left(q^{n+l} - q^m - q^l \right) \left(q^{n+l} - q^{m+1} - q^l \right) \right. \\
& \qquad \left. \cdots \left(q^{n+l} - q^{m+j-s-2} - q^l \right) \right) \\
& \times \left(\left(q^j - q^{s+1} \right) \left(q^j - q^{s+2} \right) \cdots \left(q^j - q^{j-1} \right) \right)^{-1}.
\end{aligned}
\tag{27}
$$

$N_q(n+l,(m,1),(m,1),(m-i,1))$ and $N_q(n+l,(m,1),(m,1),(m-i,0))$ denote the number of subspaces of type $(m,1)$ at distance $2i$ from the fixed subspace V of type $(m,1)$. Therefore,

$$
\begin{aligned}
& |S(V,(m,1),t)| \\
& = \sum_{i=0}^{t} \left(N_q(n+l,(m,1),(m,1),(m-i,1)) \right. \\
& \qquad \left. + N_q(n+l,(m,1),(m,1),(m-i,0)) \right),
\end{aligned}
\tag{28}
$$

which is clearly independent of the choice of V. □

Theorem 3 (Sphere-packing bound). *Let $t = \lfloor (\delta - 1)/2 \rfloor$, and then*

$$
\begin{aligned}
& \mathscr{A}_q(n+l,2\delta,(m,1)) \\
& \leq \left(q^{(m-1)(l-1)} \begin{bmatrix} n \\ m-1 \end{bmatrix}_q \begin{bmatrix} l \\ 1 \end{bmatrix}_q \right) \\
& \quad \times \left(\sum_{i=0}^{t} \left(N_q(n+l,(m,1),(m,1),(m-i,1)) \right. \right. \\
& \qquad \left. \left. + N_q(n+l,(m,1),(m,1),(m-i,0)) \right) \right)^{-1}.
\end{aligned}
\tag{29}
$$

Proof. Let $\mathbb{C} \subseteq \mathscr{M}(m,1;n+l,n)$ be an $(n+l,M,2\delta,(m,1))_q$ code and let $t = \lfloor (\delta - 1)/2 \rfloor$. Then the spheres of radius t centered at every codeword of $\mathbb{C}$ disjoint with each other and each of these spheres contains

$$
\begin{aligned}
& \sum_{i=0}^{t} \left(N_q(n+l,(m,1),(m,1),(m-i,1)) \right. \\
& \qquad \left. + N_q(n+l,(m,1)(m,1),(m-i,0)) \right)
\end{aligned}
\tag{30}
$$

subspaces of type $(m,1)$ in $\mathscr{M}(m,1;n+l,n)$. Since the total number of subspaces of type $(m,1)$ in $\mathbb{F}_q^{(n+l)}$ is

$$
\begin{aligned}
& |\mathscr{M}(m,1;n+l,n)| = N(m,1;n+l,n) \\
& \qquad = q^{(m-1)(l-1)} \begin{bmatrix} n \\ m-1 \end{bmatrix}_q \begin{bmatrix} l \\ 1 \end{bmatrix}_q , \\
& M \leq \left(q^{(m-1)(l-1)} \begin{bmatrix} n \\ m-1 \end{bmatrix}_q \begin{bmatrix} l \\ 1 \end{bmatrix}_q \right) \\
& \quad \times \left(\sum_{i=0}^{t} \left(N_q\left(n+l,(m,1),(m,1), \right. \right. \right. \\
& \qquad \left. (m-i,1) \right) \\
& \qquad + N_q(n+l,(m,1),(m,1), \\
& \qquad \left. \left. (m-i,0)) \right) \right)^{-1}.
\end{aligned}
\tag{31}
$$

Then the theorem follows immediately. □

Suppose $\mathbb{C}$ is a collection of subspaces of type $(m,1)$ in $\mathscr{M}(m,1;n+l,n)$ and let W' be any $(n+l-1)$-dimensional subspace of $\mathbb{F}_q^{(n+l)}$. Define

$$
\mathbb{C}' = \left\{ V' : V' = \mathscr{H}_{m-1}\left(V \cap W'\right), V \in \mathbb{C} \right\}
\tag{32}
$$

by replacing each subspace $V \in \mathbb{C}$ by $V' = \mathscr{H}_{m-1}(V \cap W')$, where $\mathscr{H}_{m-1}(V \cap W')$ is defined as follows: V is replaced by $V \cap W'$ if $V \cap W'$ is a subspace of type $(m-1,1)$ in $\mathbb{F}_q^{(n+l)}$; otherwise, V is replaced by some subspace of type $(m-1,1)$ of V.

Lemma 4. *If $\mathbb{C} \subseteq \mathscr{M}(m,1;n+l,n)$ is an $(n+l,M,d,(m,1))_q$ code with $d > 2$, then $\mathbb{C}' = \{V' : V' = \mathscr{H}_{m-1}(V \cap W'), V \in \mathbb{C}\}$ is an $(n+l-1,M,d',(m-1,1))_q$ code with $d' \geq d-2$.*

Proof. It is sufficient to consider the cardinality and the minimum distance of code $\mathbb{C}'$. Let U and V be any two distinct codewords of code $\mathbb{C}$ and the corresponding codewords $U' = \mathscr{H}_{m-1}(U \cap W')$ and $V' = \mathscr{H}_{m-1}(V \cap W')$ of code $\mathbb{C}'$ are obtained. Obviously $U' \subseteq U$ and $V' \subseteq V$, and then $U' \cap V' \subseteq U \cap V$ and

$$
2\dim\left(U' \cap V'\right) \leq 2\dim(U \cap V) \leq 2m - d,
\tag{33}
$$

where the latter inequality follows from the fact that

$$
d(U,V) = 2m - 2\dim(U \cap V) \geq d.
\tag{34}
$$

Considering $d(U',V')$ with (33),

$$
\begin{aligned}
d\left(U',V'\right) &= 2(m-1) - 2\dim\left(U' \cap V'\right) \\
&\geq 2(m-1) - (2m-d) = d-2,
\end{aligned}
\tag{35}
$$

which implies that $d' \geq d-2$.

By $d > 2$, $d(U', V') \geq d - 2 > 0$, so U' and V' are distinct, which shows that code $\mathbb{C}'$ has the same number of codewords as code $\mathbb{C}$. □

Theorem 5 (Singleton bound). *Consider*

$$\mathscr{A}_q(n+l, 2\delta, (m,1)) \leq q^{(m-\delta)(l-1)} \begin{bmatrix} n-\delta+1 \\ m-\delta \end{bmatrix}_q \begin{bmatrix} l \\ 1 \end{bmatrix}_q. \quad (36)$$

Proof. Let $\mathbb{C} \subseteq \mathscr{M}(m, 1; n+l, n)$ be an $(n+l, M, 2\delta, (m,1))_q$ code. When Lemma 4 is applied $(\delta - 1)$ times, an $(n+l-\delta+1, M, 2\delta', (m-\delta+1, 1))_q$ code is obtained, where every codeword is of subspace of type $(m-\delta+1, 1)$ in $\mathbb{F}_q^{(n+l-\delta+1)}$. It is well known that

$$\begin{aligned} &|\mathscr{M}(m-\delta+1, 1; n+l-\delta+1, n-\delta+1)| \\ &\quad = N(m-\delta+1, 1; n+l-\delta+1, n-\delta+1) \\ &\quad = q^{(m-\delta)(l-1)} \begin{bmatrix} n-\delta+1 \\ m-\delta \end{bmatrix}_q \begin{bmatrix} l \\ 1 \end{bmatrix}_q. \end{aligned} \quad (37)$$

Hence

$$M \leq q^{(m-\delta)(l-1)} \begin{bmatrix} n-\delta+1 \\ m-\delta \end{bmatrix}_q \begin{bmatrix} l \\ 1 \end{bmatrix}_q, \quad (38)$$

where the inequality follows from the fact that the obtained $(n+l-\delta+1, M, 2\delta', (m-\delta+1,1))_q$ code cannot have more codewords than the total subspaces of type $(m-\delta+1, 1)$ in $\mathbb{F}_q^{(n+l-\delta+1)}$. Then the theorem follows. □

Theorem 6 (Wang-Xing-Safavi-Naini bound). *Consider*

$$\mathscr{A}_q(n+l, 2\delta+2, (m,1)) \leq q^{(m-\delta)(l-1)} \frac{\begin{bmatrix} n \\ m-\delta \end{bmatrix}_q}{\begin{bmatrix} m-1 \\ m-\delta \end{bmatrix}_q}. \quad (39)$$

Proof. Let $\mathbb{C} \subseteq \mathscr{M}(m, 1; n+l, n)$ be an $(n+l, M, 2\delta+2, (m,1))_q$ code. On the one hand, each codeword of $\mathbb{C}$ contains exactly

$$N(m-\delta, 0; m, 1; n+l, n) = q^{(m-\delta)} \begin{bmatrix} m-1 \\ m-\delta \end{bmatrix}_q \quad (40)$$

subspaces of type $(m-\delta, 0)$.

On the other hand, if $\dim(U \cap V) \geq m-\delta$ for any two distinct codewords U and V of $\mathbb{C}$, by (3),

$$d(U, V) = 2m - 2\dim(U \cap V) \leq 2\delta, \quad (41)$$

a contradiction to the minimum distance $2\delta+2$ of $\mathbb{C}$, which implies that a given subspace of type $(m-\delta, 0)$ in $\mathbb{F}_q^{(n+l)}$ cannot be contained in two distance codewords of $\mathbb{C}$. The total number of subspaces of type $(m-\delta, 0)$ in $\mathbb{F}_q^{(n+l)}$ is

$$N(m-\delta, 0; n+l, n) = q^{(m-\delta)l} \begin{bmatrix} n \\ m-\delta \end{bmatrix}_q, \quad (42)$$

so $M \leq q^{(m-\delta)(l-1)}(\begin{bmatrix} n \\ m-\delta \end{bmatrix}_q / \begin{bmatrix} m-1 \\ m-\delta \end{bmatrix}_q)$. □

Theorem 7 (Johnson bound). *Consider*

$$\begin{aligned} &\mathscr{A}_q(n+l, 2\delta, (m,1)) \\ &\quad \leq \frac{q^l(q^n-1)}{q^m-q} \mathscr{A}_q(n+l-1, 2\delta, (m-1, 1)). \end{aligned} \quad (43)$$

Proof. Let $\mathbb{C} \subseteq \mathscr{M}(m, 1; n+l, n)$ be an $(n+l, M, 2\delta, (m,1))_q$ code, which attains the value of $\mathscr{A}_q(n+l, 2\delta, (m,1))$; that is, $M = \mathscr{A}_q(n+l, 2\delta, (m,1))$. Each codeword (subspace of type $(m,1)$) of $\mathbb{C}$ contains

$$\frac{q^m - q}{q-1} \quad (44)$$

subspaces of type $(1,0)$ in $\mathbb{F}_q^{(n+l)}$. There are totally

$$\frac{q^l(q^n-1)}{q-1} \quad (45)$$

subspaces of type $(1,0)$ in $\mathbb{F}_q^{(n+l)}$. Hence, there exists a subspace P of type $(1,0)$ satifying the fact that the subspace P is contained in at least

$$\frac{M(q^m-q)}{q^l(q^n-1)} \quad (46)$$

codewords of $\mathbb{C}$.

Let $\mathbb{F}_q^{(n+l)} = P \oplus W$, where W is a subspace of type $(n+l-1, l)$ in $\mathbb{F}_q^{(n+l)}$. Define the following set:

$$\mathbb{C}' = \{V \cap W : V \in \mathbb{C}, P \subset V\}. \quad (47)$$

Clearly $\mathbb{C}'$ consists of the subspaces of type $(m-1, 1)$ of W; thus, $\mathbb{C}'$ can be regarded as an $(n+l-1, M', 2\delta', (m-1,1))_q$ code with the size M' and the minimum distance $2\delta'$, where $M' \geq M(q^m - q)/q^l(q^n-1)$.

Let U' and V' be any two codewords of $\mathbb{C}'$ and there exist two corresponding codewords U and V of $\mathbb{C}$ such that $U' = U \cap W$ and $V' = V \cap W$ with $P \subset U$ and $P \subset V$. Noting that

$$\begin{aligned} U' \cap V' &= (U \cap W) \cap (V \cap W) = (U \cap V) \cap W, \\ \dim(U' \cap V') &= \dim((U \cap V) \cap W) \\ &= \dim(U \cap V) + \dim W \\ &\quad - \dim((U \cap V) + W) \\ &= \dim(U \cap V) + (n+l-1) - (n+l) \\ &= \dim(U \cap V) - 1, \end{aligned} \quad (48)$$

where the third equality follows from the fact that $U \cap V$ contains P, hence,

$$\dim(U' \cap V') = \dim(U \cap V) - 1. \quad (49)$$

By (3) and (49), $d(U',V') = d(U,V)$ from which $\delta = \delta'$ follows. With all the above discussions,

$$\mathscr{A}_q(n+l-1, 2\delta, (m-1,1)) \geq M' \geq \frac{q^m - q}{q^l(q^n-1)} \mathscr{A}_q(n+l, 2\delta, (m,1)). \tag{50}$$

The theorem is completed. □

Corollary 8. *Consider*

$$\mathscr{A}_q(n+l, 2\delta, (m,1)) \leq q^{l(m-\delta+1)} \prod_{i=0}^{m-\delta} \frac{q^{n-i}-1}{q^{m-i}-q}. \tag{51}$$

Proof. When Theorem 7 is applied iteratively $(m-\delta+1)$ times, note the trivial equality

$$\begin{aligned} &\mathscr{A}_q(n+l-m+\delta-1, 2\delta, (\delta-1,1)) = 1, \\ &\mathscr{A}_q(n+l, 2\delta, (m,1)) \\ &\leq q^l \frac{q^n-1}{q^m-q} q^l \frac{q^{n-1}-1}{q^{m-1}-q} \cdots q^l \frac{q^{n-m+\delta}-1}{q^\delta - q} \\ &\times \mathscr{A}_q(n+l-m+\delta-1, 2\delta, (\delta-1,1)) \\ &= q^{l(m-\delta+1)} \prod_{i=0}^{m-\delta} \frac{q^{n-i}-1}{q^{m-i}-q}. \end{aligned} \tag{52}$$

□

Corollary 9. *Consider*

$$\begin{aligned} &\mathscr{A}_q(n+l, 2\delta, (m,1)) \\ &\leq q^{l(m-\delta+1)} \left\lfloor \frac{q^n-1}{q^m-q} \left\lfloor \frac{q^{n-1}-1}{q^{m-1}-q} \cdots \left\lfloor \frac{q^{n-m+\delta}-1}{q^\delta-q} \right\rfloor \cdots \right\rfloor \right\rfloor. \end{aligned} \tag{53}$$

Theorem 10 (Johnson bound). *Consider*

$$\begin{aligned} &\mathscr{A}_q(n+l, 2\delta, (m,1)) \\ &\leq \frac{q^{(m-1)(l-1)}\left(q^{n-1}-1\right)\left(q^n-1\right)\left(q^l-1\right)}{\left(q^{n-m}-1\right)\left(q^{n-m+1}-1\right)(q-1)} \\ &\times \mathscr{A}_q(n+l-1, 2\delta, (m,1)). \end{aligned} \tag{54}$$

Proof. Let $\mathbb{C} \subseteq \mathscr{M}(m,1;n+l,n)$ be an $(n+l, M, 2\delta, (m,1))_q$ code, which attains the value of $\mathscr{A}_q(n+l,2\delta,(m,1))$; that is, $M = \mathscr{A}_q(n+l,2\delta,(m,1))$. For each

$$W \in \mathscr{M}(n-1,1;n+l,n), \tag{55}$$

define the following set:

$$\mathbb{C}_W = \{V : V \in \mathbb{C}, V \subset W\}. \tag{56}$$

Clearly, for each $W \in \mathscr{M}(n-1,1;n+l,n)$, $\mathbb{C}_W$ is an $(n+l-1, M_W, 2\delta', (m,1))_q$ code with the size M_W and the minimum distance $2\delta'$ and $\delta' \geq \delta$. There are precisely

$$q^{(n-m-1)(l-1)} \frac{\left(q^{n-m}-1\right)\left(q^{n-m+1}-1\right)}{(q-1)(q^2-1)} \tag{57}$$

elements containing any given subspace of type $(m,1)$ in $\mathscr{M}(n-1,1;n+l,n)$; hence each codeword (subspace of type $(m,1)$) of $\mathbb{C}$ is contained in

$$q^{(n-m-1)(l-1)} \frac{\left(q^{n-m}-1\right)\left(q^{n-m+1}-1\right)}{(q-1)(q^2-1)} \tag{58}$$

different codes $\mathbb{C}_W$. Consider

$$\sum_W |\mathbb{C}_W| = M \cdot q^{(n-m-1)(l-1)} \frac{\left(q^{n-m}-1\right)\left(q^{n-m+1}-1\right)}{(q-1)(q^2-1)}, \tag{59}$$

from which

$$\begin{aligned} &\frac{\sum_W |\mathbb{C}_W|}{|\mathscr{M}(n-1,1;n+l,n)|} \\ &= M \cdot \frac{\left(q^{n-m}-1\right)\left(q^{n-m+1}-1\right)(q-1)}{q^{(l-1)(m-1)}\left(q^n-1\right)\left(q^l-1\right)}, \end{aligned} \tag{60}$$

where

$$\begin{aligned} &|\mathscr{M}(n-1,1;n+l,n)| \\ &= N(n-1,1;n+l,n) \\ &= q^{(n-2)(l-1)} \frac{\left(q^{n-1}-1\right)\left(q^n-1\right)\left(q^l-1\right)}{(q-1)^2(q^2-1)}. \end{aligned} \tag{61}$$

Thus, there exists at least one $W \in \mathscr{M}(n-1,1;n+l,n)$ such that

$$|\mathbb{C}_W| \geq M \cdot \frac{\left(q^{n-m}-1\right)\left(q^{n-m+1}-1\right)(q-1)}{q^{(l-1)(m-1)}\left(q^n-1\right)\left(q^l-1\right)}. \tag{62}$$

Obviously, for any $W \in \mathscr{M}(n-1,1;n+l,n)$,

$$\mathscr{A}_q(n+l-1, 2\delta, (m,1)) \geq |\mathbb{C}_W|, \tag{63}$$

and then the theorem follows immediately. □

Theorem 11 (Gilbert-Varshamov bound). *If* $V \in (n+l, M, 2\delta, (m,1))_q$, $M = \mathscr{A}_q(n+l,2\delta,(m,1))$, *then*

$$\mathscr{A}_q(n+l, 2\delta, (m,1)) \geq \frac{q^{(m-1)(l-1)} \begin{bmatrix} n \\ m-1 \end{bmatrix}_q \begin{bmatrix} l \\ 1 \end{bmatrix}_q}{|S(V,(m,1),(\delta-1))|}, \tag{64}$$

where

$$\begin{aligned} &|S(V,(m,1),(\delta-1))| \\ &= \sum_{i=0}^{\delta-1} \Big(N_q(n+l,(m,1),(m,1),(m-i,1)) \\ &\quad + N_q(n+l,(m,1),(m,1),(m-i,0)) \Big). \end{aligned} \tag{65}$$

Proof. Let $\mathbb{C} \subseteq \mathcal{M}(m,1;n+l,n)$ be an $(n+l, M, 2\delta, (m,1))_q$ code, which attains the value of $\mathcal{A}_q(n+l, 2\delta, (m,1))$; that is, $M = \mathcal{A}_q(n+l, 2\delta, (m,1))$. There is no subspace U of type $(m,1)$ in $\mathcal{M}(m,1;n+l,n)$ satisfying

$$d(U,V) \geq 2\delta, \tag{66}$$

for any $V \in \mathbb{C}$. Otherwise, by adding the subspace U of type $(m,1)$ to $\mathbb{C}$, a new $(n+l, M+1, 2\delta, (m,1))_q$ code is obtained, which is a contradiction to $M = \mathcal{A}_q(n+l, 2\delta, (m,1))$. Therefore, for any $V \in \mathbb{C}$,

$$M \cdot |S(V,(m,1),(\delta-1))| \geq N(m,1;n+l,n) = q^{(m-1)(l-1)} \begin{bmatrix} n \\ m-1 \end{bmatrix}_q \begin{bmatrix} l \\ 1 \end{bmatrix}_q. \tag{67}$$

That is,

$$\mathcal{A}_q(n+l, 2\delta, (m,1)) \geq \frac{q^{(m-1)(l-1)} \begin{bmatrix} n \\ m-1 \end{bmatrix}_q \begin{bmatrix} l \\ 1 \end{bmatrix}_q}{|S(V,(m,1),(\delta-1))|}, \tag{68}$$

where

$$|S(V,(m,1),(\delta-1))| = \sum_{i=0}^{\delta-1} \left(N_q(n+l,(m,1),(m,1),(m-i,1)) + N_q(n+l,(m,1),(m,1),(m-i,0)) \right). \tag{69}$$

□

4. Steiner Structure

Definition 12. A Steiner structure $\mathbb{S}_q((m_1,0),(m,1),n+l)$ is a collection $\mathbb{S}$ of elements from $\mathcal{M}(m,1;n+l,n)$ satisfying the fact that each element from $\mathcal{M}(m_1,0;n+l,n)$ is contained in exactly one element of $\mathbb{S}$. The subspaces of type $(m,1)$ in $\mathbb{S}$ are called blocks of the Steiner structure $\mathbb{S}_q((m_1,0),(m,1),n+l)$.

Theorem 13. *The total number of blocks in the* $\mathbb{S}_q((m_1,0),(m,1),n+l)$ *is*

$$q^{m_1(l-1)} \frac{\begin{bmatrix} n \\ m_1 \end{bmatrix}_q}{\begin{bmatrix} m-1 \\ m_1 \end{bmatrix}_q}. \tag{70}$$

Proof. Each block (subspace of type $(m,1)$) of the Steiner structure $\mathbb{S}_q((m_1,0),(m,1),n+l)$ contains

$$N(m_1,0;m,1;n+l,n) = q^{m_1} \begin{bmatrix} m-1 \\ m_1 \end{bmatrix}_q \tag{71}$$

subspaces of type $(m_1,0)$. By the definition of the Steiner structure $\mathbb{S}_q((m_1,0),(m,1),n+l)$, each subspace of type $(m_1,0)$ is contained in exactly one block. The total number of subspaces of type $(m_1,0)$ in $\mathbb{F}_q^{(n+l)}$ is

$$N(m_1,0;n+l,n) = q^{m_1 l} \begin{bmatrix} n \\ m_1 \end{bmatrix}_q; \tag{72}$$

thus, the total number of blocks of the $\mathbb{S}_q((m_1,0),(m,1),n+l)$ is

$$q^{m_1(l-1)} \frac{\begin{bmatrix} n \\ m_1 \end{bmatrix}_q}{\begin{bmatrix} m-1 \\ m_1 \end{bmatrix}_q}. \tag{73}$$

□

Theorem 14. *The Steiner structure* $\mathbb{S}_q((m_1,0),(m,1),n+l)$ *is an* $(n+l, M, 2\delta, (m,1))_q$ *code with the size* $M = q^{m_1(l-1)}(\begin{bmatrix} n \\ m_1 \end{bmatrix}_q / \begin{bmatrix} m-1 \\ m_1 \end{bmatrix}_q)$ *and* $\delta = m - m_1 + 1$.

Proof. By Definition 12 and Theorem 13, it is sufficient to prove $\delta = m - m_1 + 1$. Firstly, for any two distinct blocks $X, Y \in \mathbb{S}_q((m_1,0),(m,1),n+l)$,

$$\dim(X \cap Y) \leq m_1 - 1, \tag{74}$$

where the inequality follows from the definition of the Steiner structure $\mathbb{S}_q((m_1,0),(m,0),n+l)$ in which each subspace of type $(m_1,0)$ is contained in exactly one block of the $\mathbb{S}_q((m_1,0),(m,1),n+l)$. By (3) and (74),

$$d(X,Y) = 2m - 2\dim(X \cap Y) \geq 2(m - m_1 + 1). \tag{75}$$

Furthermore, 2δ is the minimum distance of the code; then $\delta \geq m - m_1 + 1$.

Conversely, let V be a fixed subspace of type $(m_1 - 1, 0)$ in $\mathbb{F}_q^{(n+l)}$, and then choose two subspaces U_1 and U_2 of type $(m_1, 0)$ in $\mathbb{F}_q^{(n+l)}$ such that

$$V = U_1 \cap U_2. \tag{76}$$

By the definition of the Steiner structure $\mathbb{S}_q((m_1,0),(m,1),n+l)$, there exist the uniquely corresponding subspaces X_1 and X_2 of type $(m,1)$ in the Steiner structure $\mathbb{S}_q((m_1,0),(m,1),n+l)$ satisfying

$$U_1 \subseteq X_1, \qquad U_2 \subseteq X_2, \tag{77}$$

respectively. Then,

$$V = U_1 \cap U_2 \subseteq X_1 \cap X_2, \tag{78}$$

from which

$$\dim(X_1 \cap X_2) \geq \dim V = m_1 - 1. \tag{79}$$

By (3) and (79),

$$d(X_1, X_2) = 2m - 2\dim(X_1 \cap X_2) \leq 2(m - m_1 + 1). \tag{80}$$

Furthermore, 2δ is the minimum distance of the code, and then $\delta \leq m - m_1 + 1$.

From the above two aspects, $\delta = m - m_1 + 1$. □

The sufficient and necessary conditions for an $(n+l, M, 2\delta, (m,1))_q$ code to attain the Wang-Xing-Safavi-Naini bound in Theorem 6 are presented below.

Theorem 15. *An* $(n+l, M, 2\delta, (m,1))_q$ *code* $\mathbb{C}$ *attains the Wang-Xing-Safavi-Naini bound; that is,* $M = q^{(m-\delta+1)(l-1)}\left(\begin{bmatrix} n \\ m-\delta+1 \end{bmatrix}_q / \begin{bmatrix} m-1 \\ m-\delta+1 \end{bmatrix}_q\right)$ *if and only if* $\mathbb{C}$ *is the Steiner structure* $\mathbb{S}_q((m-\delta+1,0),(m,1),n+l)$.

Proof. From Theorems 6 and 14, if $\mathbb{C}$ is the Steiner structure $\mathbb{S}_q((m-\delta+1,0),(m,1),n+l)$, $\mathbb{C}$ is an $(n+l, M, 2\delta, (m,1))_q$ code with

$$M = q^{(m-\delta+1)(l-1)} \frac{\begin{bmatrix} n \\ m-\delta+1 \end{bmatrix}_q}{\begin{bmatrix} m-1 \\ m-\delta+1 \end{bmatrix}_q}. \quad (81)$$

Obviously such a code attains the Wang-Xing-Safavi-Naini bound.

Conversely, let $\mathbb{C}$ be an $(n+l, M, 2\delta, (m,1))_q$ code attaining the Wang-Xing-Safavi-Naini bound; that is,

$$M = q^{(m-\delta+1)(l-1)} \frac{\begin{bmatrix} n \\ m-\delta+1 \end{bmatrix}_q}{\begin{bmatrix} m-1 \\ m-\delta+1 \end{bmatrix}_q}. \quad (82)$$

Firstly, any subspace of type $(m-\delta+1, 0)$ cannot be contained in two distinct codewords U and V of $\mathbb{C}$. Otherwise, by (3),

$$d(U,V) = 2m - 2\dim(U \cap V) \le 2\delta - 2, \quad (83)$$

a contradiction to the minimum distance 2δ of $\mathbb{C}$. Each codeword of $\mathbb{C}$ contains

$$N(m-\delta+1, 0; m, 1; n+l, n) = q^{(m-\delta+1)} \begin{bmatrix} m-1 \\ m-\delta+1 \end{bmatrix}_q \quad (84)$$

distinct subspaces of type $(m-\delta+1, 0)$; thus, all the codewords of $\mathbb{C}$ contain totally

$$M \cdot q^{(m-\delta+1)} \begin{bmatrix} m-1 \\ m-\delta+1 \end{bmatrix}_q = q^{(m-\delta+1)l} \begin{bmatrix} n \\ m-\delta+1 \end{bmatrix}_q \quad (85)$$

distinct subspaces of type $(m-\delta+1, 0)$. There are totally

$$q^{(m-\delta+1)l} \begin{bmatrix} n \\ m-\delta+1 \end{bmatrix}_q \quad (86)$$

distinct subspaces of type $(m-\delta+1, 0)$ in $\mathbb{F}_q^{(n+l)}$, which implies that each subspace of type $(m-\delta+1, 0)$ is contained in exactly one codeword of $\mathbb{C}$.

When regarding all the codewords of $\mathbb{C}$ as blocks, code $\mathbb{C}$ is the Steiner structure $\mathbb{S}_q((m-\delta+1,0),(m,1),n+l)$. □

Theorem 15 shows that certain Steiner structure is an optimal code.

Corollary 16. *Consider*

$\mathscr{A}_q(n+l, 2\delta, (m,1)) = q^{(m-\delta+1)(l-1)}\left(\begin{bmatrix} n \\ m-\delta+1 \end{bmatrix}_q / \begin{bmatrix} m-1 \\ m-\delta+1 \end{bmatrix}_q\right)$ *if and only if the Steiner structure* $\mathbb{S}_q((m-\delta+1,0),(m,1),n+l)$ *exists.*

5. Conclusion

In this paper, a subspace code $(n+l, M, d, (m,1))_q$ based on subspaces of type $(m,1)$ in singular linear space $\mathbb{F}_q^{(n+l)}$ over $\mathbb{F}_q$ is constructed and the Sphere-packing bound, Singleton bound, Wang-Xing-Safavi-Naini bound, Johnson bound, and Gilbert-Varshamov bound on $(n+l, M, d, (m,1))_q$ code are presented. Meanwhile, we prove that codes based on subspaces of type $(m,1)$ in singular linear space attain the Wang-Xing-Safavi-Naini bound if and only if they are certain Steiner structures $\mathbb{F}_q^{(n+l)}$. We could consider whether there exist nontrivial perfect subspace codes in $\mathscr{M}(m,1; n+l, n)$ in the following steps.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work is supported by the National Natural Science Foundation of China under Grant no. 61179026 and the (Boeing) Technical Challenge Foundation of Civil Aviation University of China under Grant no. 20140159201. The authors would like to thank the referee for his suggestions on simplifying the earlier version of the paper.

References

[1] R. Koetter and F. R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Transactions on Information Theory*, vol. 54, no. 8, pp. 3579–3591, 2008.

[2] R. Ahlswede, N. Cai, and S. R. a. Li, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, 2000.

[3] M. Gadouleau and Z. Yan, "Packing and covering properties of subspace codes for error control in random linear network coding," *IEEE Transactions on Information Theory*, vol. 56, no. 5, pp. 2097–2108, 2010.

[4] R. Koetter and F. R. Kschischang, "Error correction in random network," in *Proceedings of the 2nd Annual Workshop on Information Theory and Applications*, La Jolla, Calif, USA, 2007.

[5] T. Ho, M. Médard, R. Koetter et al., "A random linear network coding approach to multicast," *IEEE Transactions on Information Theory*, vol. 52, no. 10, pp. 4413–4430, 2006.

[6] D. Silva, F. R. Kschischang, and R. Koetter, "A rank-metric approach to error control in random network coding," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 3951–3967, 2008.

[7] E. M. Gabidulin and M. Bossert, "Codes for network coding," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT '08)*, pp. 867–870, Toronto, Canada, July 2008.

[8] M. Gadouleau and Z. Yan, "Constant-rank codes," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT '08)*, pp. 876–880, Toronto, Canada, July 2008.

[9] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, The Netherlands, 1977.

[10] H. Wang, C. Xing, and R. Safavi-Naini, "Linear authentication codes: bounds and constructions," *IEEE Transactions on Information Theory*, vol. 49, no. 4, pp. 866–872, 2003.

[11] T. Etzion and A. Vardy, "Error-correcting codes in projective space," *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 1165–1173, 2011.

[12] S. T. Xia and F. W. Fu, "Johnson type bounds on constant dimension codes," *Designs, Codes and Cryptography*, vol. 50, no. 2, pp. 163–172, 2009.

[13] M. Schwartz and T. Etzion, "Codes and anticodes in the Grassman graph," *Journal of Combinatorial Theory A*, vol. 97, no. 1, pp. 27–42, 2002.

[14] T. Etzion, "Perfect byte-correcting codes," *IEEE Transactions on Information Theory*, vol. 44, no. 7, pp. 3140–3146, 1998.

[15] K. Wang, J. Guo, and F. Li, "Singular linear space and its applications," *Finite Fields and Their Applications*, vol. 17, no. 5, pp. 395–406, 2011.

[16] Z. Wan, *Geometry of Classical Groups Over Finite Fields*, Science Press, Beijing, China, 2nd edition, 2002.