Construction of Constant Dimension Codes in Some Cases

You Gao*, Liyun Zhao

College of Science, Civil Aviation University of China, Tianjin 300300, P.R. China

Abstract: In this paper, we study some bounds of constant dimension codes further in Grassmannian space $\mathcal{G}_q(n,k)$. There is an increasing interest in subspace codes since they are precisely what is needed for errors-correction in networks. There is also a connection to the theory over finite fields. By revising the specific construction method of the constant dimension codes in [1], [2], we can improve some bounds on q-ary constant dimension codes in some given cases.

Keywords: Constant dimension codes; Subspaces; Dimension distance; Upper bound; Finite fields.

§1 Introduction

Let $\mathbb{F}_q$ be the finite field with q elements, where q is a power of a prime. Let $\mathbb{F}_q^n$ be the n-dimensional row vector space over $\mathbb{F}_q$, where n is a positive integer. The projective space of order n over $\mathbb{F}_q$ is the set of all the subspaces of $\mathbb{F}_q^n$, denoted herein by $\mathcal{P}_q(n)$, including $\{\mathbf{0}\}$ and $\mathbb{F}_q^n$ itself. Given a nonnegative integer $k \leq n$, the set of all subspaces of $\mathbb{F}_q^n$ that have dimension k is known as a Grassmannian space, and usually denoted by $\mathcal{G}_q(n,k)$. Thus $\mathcal{P}_q(n) = \cup_{0\leq k\leq n}\mathcal{G}_q(n,k)$. Now we introduce some formulas (see [3]), which will be needed in the following sections. For brevity we use the Gaussian coefficient

$$|\mathcal{G}_q(n,k)| = \begin{bmatrix} n \\ k \end{bmatrix}_q \stackrel{\text{def}}{=} \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}.$$

*Corresponding author.
E-mail addresses: gao_you@263.net.

By convenience $\begin{bmatrix} n \\ 0 \end{bmatrix}_q = 1$ for all integer n and $\begin{bmatrix} n \\ k \end{bmatrix}_q = 0$ for all $k < 0$ and $n < k$. For any $U, V \in \mathcal{P}_q(n)$, denote

$$U + V = \{u + v \mid u \in U, v \in V\}.$$

That is the smallest subspace containing both U and V. If $U \cap V = \{\mathbf{0}\}$, i.e., if U and V have trivial intersection, then the sum $U + V$ is a direct sum, denoted as $U \oplus V$. Clearly,

$$\dim U \oplus V = \dim U + \dim V.$$

A subspace code $\mathcal{C}$ is a nonempty collection of some subspaces of $\mathbb{F}_q^n$, namely, a nonempty subset of $\mathcal{P}_q(n)$. Thus the subspace code $\mathcal{C}$ is not different from classical codes in which each of codewords is a vector. However, here each codeword of $\mathcal{C}$ is an entire space of vectors. A code in which each codeword has the same dimension is called a constant dimension code. In other words, a code is contained within a single Grassmannian space. The projective space can be endowed with the distance function

$$d(U, V) = \dim(U + V) - \dim(U \cap V),$$

which is equal to

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

Then the distance function turns $\mathcal{P}_q(n)$ and $\mathcal{G}_q(n, k)$ into metric spaces. Given a metric space, then we can define codes. We say that $\mathcal{C} \subseteq \mathcal{P}_q(n)$ is an (n, M, d) code in projective space if $|\mathcal{C}| = M$ and $d(U, V) \geq d$ for all U,V in $\mathcal{C}$. We say that $\mathcal{C}$ is an (n, M, d, k) code if an (n, M, d) code $\mathcal{C}$ in which each codeword has the same dimension for some k. Let $\mathcal{A}_q(n, d)$ denote the maximum number of codewords in an (n, M, d) code in $\mathcal{P}_q(n)$. Let $\mathcal{A}_q(n, d, k)$ denote the maximum number of codewords in an (n, M, d, k) code in $\mathcal{G}_q(n, k)$. There is no doubt that the distance between any two different codewords must be even in an (n, M, d, k) code. We always put d as 2δ, namely, $d = 2\delta$.

Very recently, Liao et al. [1] improved some bounds on q-ary constant dimension codes in some cases, and showed that there exists no optimal constant dimension code $\mathcal{A}_q(n, 2\delta, k)$ meeting both Wang-Xing-Safavi-Naini-Bound and the maximal distance separate bound simultaneously. Etzion et al. [2] presented several specific constructions of an $(n, M, 2k, k)$ code. And presented several new bounds on the size of codes in $\mathcal{P}_q(n)$, which may be thought of as counterparts of the classical bounds in coding theory due to Johnson, Delsarte, and Gilbert-Varshamoy. An operator channel was defined by Koetter and Kschischang [4] when they studied random network coding theory. They also introduced constant dimension codes and

demonstrated that these codes can be employed to correct errors and/or erasures over the operator channel. And stated that sphere-packing and sphere-covering bounds as well as a generalization of the Singleton bound are proved for constant dimension codes. Xia et al. [5] proved that constant dimension codes achieve the Wang-Xing-Safavi-Naini bound if and only if they are certain Steiner structures in $\mathbb{F}_q$. And, they also derived two Johnson type upper bounds, say I and II, on constant dimension codes. Compared with Wang-Xing-Safavi-Naini bound Johnson type bound II is slightly improved. And pointed out that optimal constant dimension codes which achieve both the Johnson type bounds I and II are actually a family of so-called Steiner stuctures. Khaleghi et al. [6] constructed lifted rank-metric codes along with improved constructions leading to codes with strictly more codewords. Kohnert et al. [7] gave a table of the best found constant dimension space codes. However, most of the results in above are still needed further research in constructing more codes which close to the upper bound, especially.

For any code $\mathcal{C}$ in $\mathcal{P}_q(n)$, the orthogonal complement of $\mathcal{C}$ can be defined as following: $\mathcal{C}^{\perp} = \{V^{\perp} \mid V \in \mathcal{C}\}$. Such orthogonal complements were first considered in the paper [4] by Kotter and Kschischang. Then the relation of $\mathcal{C}$ and $\mathcal{C}^{\perp}$ is as follows.

Lemma 1 Let U, V be two arbitrary elements of $\mathcal{P}_q(n)$. Then

$$d(U^{\perp}, V^{\perp}) = n - \dim U - \dim V + \dim(U \cap V).$$

Lemma 2 If $\mathcal{C}$ is an (n, M, d) code in $\mathcal{P}_q(n)$, then its orthogonal complement $\mathcal{C}^{\perp}$ is also an (n, M, d) code.

From Lemma 1 and Lemma 2 we immediately have

Corollary 3 For any positive integers n, k and $k < n$, if $\mathcal{C}$ is an (n, M, d, k) code, then $\mathcal{C}^{\perp}$ is an $(n, M, d, n-k)$ code.

Recently, Koetter-Kschischang [4] proved a bound which may be regarded as a counterpart of the classical Singleton bound, and they also found that the upper bound is stronger than the sphere-packing bound. The upper bound is shown below.

Proposition 4 [[4], Theorem 3] (Singleton type bound)

$$\mathcal{A}_q(n, 2\delta, k) \leq \begin{bmatrix} n-\delta+1 \\ k-\delta+1 \end{bmatrix}_q.$$

In 2003, Wang, Xing and Safavi-Naini [8] stated that constant dimension codes are equivalent to the so-called linear authentication codes, and then yielded an upper bound on linear authentication codes. Namely, the upper bound is equivalent to the following bound on constant dimension codes.

Proposition 5 [[8], Theorem 5.2] (Wang-Xing-Safavi-Naini Bound)

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

Proposition 6 [[2], Theorem 11] Let $n \equiv r \pmod{k}$. Then, for all q, we have

$$\mathcal{A}_q(n, 2k, k) \geq \frac{q^n - q^k(q^r - 1) - 1}{q^k - 1}.$$

In this paper, we study some bounds for optimal constant dimension codes further. Revising the construction for constant dimension codes in [2], [1] improved some bounds on q-ary constant dimension codes. Thus, we will have the following proposition.

Proposition 7 [[1], Theorem 1.4] Let $n \equiv r \pmod{k}$, $0 \leq r \leq k$. Then, for all q, we have

$$\mathcal{A}_q(n, 2, k) \geq \frac{q^n - q^k(q^r - 1) - 1}{q^k - 1},$$

and

$$\mathcal{A}_q(n, 2(k-1), k) \geq \frac{q^n - q^k(q^r - 1) - 1}{q^k - 1}.$$

§2. Constructions of codes

It is well known that how to construct optimal codes is the most important problem while the parameters n, k and d been fixed. By making use of the knowledge of finite fields and revising the construction of constant dimension codes in [1], [2], we can construct many constant dimension codes with a larger number of codewords than previously known codes. Then we have the following theorems.

Theorem 8 Let $n \equiv r \pmod{k}$. Then, for all q, we have

$$\mathcal{A}_q(n, 2, k) \geq \frac{q^n - q^r}{q^k - 1}.$$

Proof: Let r be the remainder obtained when k is divided into n. Henceforth, we will represent the vectors in $\mathbb{F}_q^n$ as follows:

$$\mathbb{F}_q^n = \{(x, y, z) : x \in \mathrm{GF}(q^{n-k-r}), y \in \mathrm{GF}(q^k), z \in \mathrm{GF}(q^r)\}.$$

Let α be a primitive element of GF(q^{n-k-r}), β be a primitive element of GF(q^k) and γ be a primitive element of GF(q^r). Further, let

$$M = \langle (0, \beta^0, 0), (0, \beta^1, 0), \cdots, (0, \beta^{k-1}, 0) \rangle.$$

Since $\beta^0, \beta^1, \cdots, \beta^{k-1}$ are independent over $\mathbb{F}_q$, it is easy to note that $\dim M = k$. We define $t = \frac{q^{n-k-r}-1}{q^k-1}$. Then t is an integer since k divides $n-k-r$. Then the multiplicative order of α^t in GF(q^k) is $q^k - 1$, and therefore α^t is a primitive element of GF(q^k), namely, $\beta = \alpha^t$. Then GF(q^k) is a subfield of GF(q^{n-k-r}). Now we consider the following subspaces of $\mathbb{F}_q^n$ that are given by

$$\begin{aligned}
W_l &= \langle (0, \beta^0, \gamma^l), (0, \beta^1, \gamma^l), \cdots, (0, \beta^{k-1}, \gamma^l) \rangle, \\
U_i &= \langle (\alpha^i, 0, 0), (\alpha^i\beta, 0, 0), \cdots, (\alpha^i\beta^{k-1}, 0, 0) \rangle, \\
V_{i,l} &= \langle (\alpha^i, 0, \gamma^l), (\alpha^i\beta, 0, \gamma^l), \cdots, (\alpha^i\beta^{k-1}, 0, \gamma^l) \rangle, \\
V_{i,j} &= \langle (\alpha^i, \beta^j, 0), (\alpha^i\beta, \beta^j, 0), \cdots, (\alpha^i\beta^{k-1}, \beta^j, 0) \rangle, \\
V_{i,j,l} &= \langle (\alpha^i, \beta^j, \gamma^l), (\alpha^i\beta, \beta^j, \gamma^l), \cdots, (\alpha^i\beta^{k-1}, \beta^j, \gamma^l) \rangle.
\end{aligned}$$

where i ranges over $\{0, 1, \cdots, t-1\}$, $j \in \{0, 1, \cdots, q^k-2\}$ and $l \in \{0, 1, \cdots, q^r - 2\}$. It is easy to see that

$\dim W_l = \dim U_i = \dim V_{i,l} = \dim V_{i,j} = \dim V_{i,j,l} = k$ for all i, j and l.

We construct the code $\mathcal{C}$ as follows:

$$\mathcal{C} = M \cup (\bigcup_l W_l) \cup (\bigcup_i U_i) \cup (\bigcup_{i,l} V_{i,l}) \cup (\bigcup_{i,j} V_{i,j}) \cup (\bigcup_{i,j,l} V_{i,j,l}).$$

Now we consider the minimum dimension distant d of the constant dimension code $\mathcal{C}$.

(I) Since both $\alpha^i\beta^0, \alpha^i\beta, \cdots, \alpha^i\beta^{k-1}$ and $\beta^0, \beta^1, \cdots, \beta^{k-1}$ are linearly independent over $\mathbb{F}_q$, for all i. It follows that

$$M \cap U_i = M \cap V_{i,l} = M \cap V_{i,j} = M \cap V_{i,j,l} = \{\mathbf{0}\},$$

and

$$W_l \cap U_i = W_l \cap V_{i,l} = W_l \cap V_{i,j} = W_l \cap V_{i,j,l} = \{\mathbf{0}\}.$$

Observe that the t vector spaces $U_0, U_1, \cdots, U_{t-1}$ form a spread in $\mathbb{F}_q^{n-k-r}$. The fact is well-known, see [9], [10] for a detailed proof, therefore,

$$U_{i_1} \cap U_{i_2} = \{\mathbf{0}\} \text{ for all } i_1 \neq i_2.$$

With the same reason,

$$V_{i_1,l_1} \cap V_{i_2,l_2} = V_{i_1,j_1} \cap V_{i_2,j_2} = V_{i_1,j_1,l_1} \cap V_{i_2,j_2,l_2} = \{\mathbf{0}\}$$
for all j_1, j_2, l_1, l_2, whenever $i_1 \neq i_2$.

And any two of $U_i, V_{i,j}, V_{i,l}, V_{i,j,l}$ have trivial intersection when $i_1 \neq i_2$.

(II) Now, we consider the subspace $W_{l_1} \cap W_{l_2}$, $0 \leq l_1 \neq l_2 \leq q^r - 2$. For any $A \in W_{l_1} \cap W_{l_2}$, Then there exists some $a_0, a_1, \cdots, a_{k-1} \in \mathbb{F}_q$ and $b_0, b_1, \cdots, b_{k-1} \in \mathbb{F}_q$, such that

$$A = (0, \sum_{m=0}^{k-1} a_m \beta^m, \sum_{m=0}^{k-1} a_m \gamma^{l_1}) = (0, \sum_{m=0}^{k-1} b_m \beta^m, \sum_{m=0}^{k-1} b_m \gamma^{l_2}).$$

Namely,

$$\sum_{m=0}^{k-1} a_m \beta^m = \sum_{m=0}^{k-1} b_m \beta^m \quad \text{and} \quad \sum_{m=0}^{k-1} a_m \gamma^{l_1} = \sum_{m=0}^{k-1} b_m \gamma^{l_2}.$$

Since $\beta^0, \beta^1, \cdots, \beta^{k-1}$ are independent over $\mathbb{F}_q$ and $\gamma^{l_1} \neq \gamma^{l_2}$ $(0 \leq l_1 \neq l_2 \leq q^r - 2)$, the above equations imply that

$$a_m = b_m (0 \leq m \leq k-1) \quad \text{and} \quad \sum_{m=0}^{k-1} a_m = 0.$$

Namely,

$$W_{l_1} \cap W_{l_2} = \{(0, \sum_{m=0}^{k-1} a_m \beta^m, 0) \mid a_m \in \mathbb{F}_q, \sum_{m=0}^{k-1} a_m = 0,\ 0 \leq l_1 \neq l_2 \leq q^r - 2\}.$$

Thus, we can get

$$\dim(W_{l_1} \cap W_{l_2}) = k - 1.$$

With the same reason, for all $0 \leq l_1 \neq l_2 \leq q^r - 2$ and $0 \leq j_1 \neq j_2 \leq q^k - 2$, then we will have
$\dim(V_{i,l_1} \cap V_{i,l_2}) = \dim(V_{i,j,l_1} \cap V_{i,j,l_2}) = \dim(V_{i,j_1} \cap V_{i,j_2}) = \dim(V_{i,j_1,l} \cap V_{i,j_2,l}) = \dim(V_{i,j_1,l_1} \cap V_{i,j_2,l_2}) = \dim(V_{i,j_1} \cap V_{i,j_2,l}) = \dim(V_{i,l_1} \cap V_{i,j,l_2}) = k - 1$.

(III) Now, we consider $M \cap W_l$, $0 \leq l \leq q^r - 2$, set $A \in M \cap W_l$. Then there exists some $a_0, a_1, \cdots, a_{k-1} \in \mathbb{F}_q$ and $b_0, b_1, \cdots, b_{k-1} \in \mathbb{F}_q$, such that

$$A = (0, \sum_{m=0}^{k-1} a_m \beta^m, 0) = (0, \sum_{m=0}^{k-1} b_m \beta^m, \sum_{m=0}^{k-1} b_m \gamma^l).$$

Namely,

$$\sum_{m=0}^{k-1} a_m \beta^m = \sum_{m=0}^{k-1} b_m \beta^m \quad \text{and} \quad \sum_{m=0}^{k-1} b_m \gamma^l = 0.$$

Since $\beta^0, \beta^1, \cdots, \beta^{k-1}$ are independent over $\mathbb{F}_q$, the above equations imply that

$$a_m = b_m \ (0 \le m \le k-1) \ \text{ and } \ b_0 + b_1 + \cdots + b_{k-1} = 0.$$

Namely,

$$M \cap W_l = \{(0, \sum_{m=0}^{k-1} a_m \beta^m, 0) \mid a_m \in \mathbb{F}_q, \sum_{m=0}^{k-1} a_m = 0\}.$$

Therefore

$$\dim(M \cap W_l) = k-1, \quad l = 0, 1, \cdots, q^r - 2.$$

(IV) For any $A \in U_i \cap V_{i,j,l}$, then there exists some $a_0, a_1, \cdots, a_{k-1} \in \mathbb{F}_q$ and $b_0, b_1, \cdots, b_{k-1} \in \mathbb{F}_q$, such that

$$A = (\sum_{m=0}^{k-1} a_m \alpha^i \beta^m, 0, 0) = (\sum_{m=0}^{k-1} b_m \alpha^i \beta^m, \sum_{m=0}^{k-1} b_m \beta^j, \sum_{m=0}^{k-1} b_m \gamma^l).$$

Namely,

$$\sum_{m=0}^{k-1} a_m \alpha^i \beta^m = \sum_{m=0}^{k-1} b_m \alpha^i \beta^m, \ \sum_{m=0}^{k-1} b_m \beta^j = 0 \ \text{ and } \ \sum_{m=0}^{k-1} b_m \gamma^l = 0.$$

Since both $\alpha^i \beta^0, \alpha^i \beta, \cdots, \alpha^i \beta^{k-1}$ and $\beta^0, \beta^1, \cdots, \beta^{k-1}$ are linearly independent over $\mathbb{F}_q$, for all i. It follows that

$$\sum_{m=0}^{k-1} b_m = 0 \ \text{ and } \ a_m = b_m \ (0 \le m \le k-1).$$

Namely,

$$U_i \cap V_{i,j,l} = \{(\sum_{m=0}^{k-1} a_m \alpha^i \beta^m, 0, 0) \mid a_m \in \mathbb{F}_q, \sum_{m=0}^{k-1} a_m = 0\}.$$

Thus , we can get

$$\dim(U_i \cap V_{i,j,l}) = k-1.$$

With the same reason,

$$\dim(U_i \cap V_{i,l}) = \dim(U_i \cap V_{i,j}) = k-1.$$

(V) Let any $A \in V_{i,j,l} \cap V_{i,l}$. Then

$$A = (\sum_{m=0}^{k-1} a_m \alpha^i \beta^m, \sum_{m=0}^{k-1} a_m \beta^j, \sum_{m=0}^{k-1} a_m \gamma^l) = (\sum_{m=0}^{k-1} b_m \alpha^i \beta^m, 0, \sum_{m=0}^{k-1} b_m \gamma^l).$$

Namely,

$$\sum_{m=0}^{k-1} a_m\alpha^i\beta^m = \sum_{m=0}^{k-1} b_m\alpha^i\beta^m\ ,\ \sum_{m=0}^{k-1} a_m\beta^j = 0 \ \text{ and } \ \sum_{m=0}^{k-1} a_m\gamma^l = \sum_{m=0}^{k-1} b_m\gamma^l.$$

Then

$$\sum_{m=0}^{k-1} b_m = 0 \ \text{ and } \ a_m = b_m \ (0 \le m \le k-1).$$

Namely,

$$V_{i,j,l} \cap V_{i,l} = \{(\sum_{m=0}^{k-1} a_m\alpha^i\beta^m, 0, 0) \mid a_m \in \mathbb{F}_q, \sum_{m=0}^{k-1} a_m = 0\}.$$

Thus, we can get

$$\dim(V_{i,j,l} \cap V_{i,l}) = k-1.$$

For the same reason,

$$\dim(V_{i,j,l} \cap V_{i,j}) = k-1.$$

(VI) Let any $A \in V_{i,l} \cap V_{i,j}$. Then

$$A = (\sum_{m=0}^{k-1} a_m\alpha^i\beta^m, 0, \sum_{m=0}^{k-1} a_m\gamma^l) = (\sum_{m=0}^{k-1} b_m\alpha^i\beta^m, \sum_{m=0}^{k-1} b_m\beta^j, 0).$$

Namely,

$$\sum_{m=0}^{k-1} a_m\alpha^i\beta^m = \sum_{m=0}^{k-1} b_m\alpha^i\beta^m\ ,\ \sum_{m=0}^{k-1} b_m\beta^j = 0 \ \text{ and } \ \sum_{m=0}^{k-1} a_m\gamma^l = 0.$$

Then

$$\sum_{m=0}^{k-1} b_m = 0 \ \text{ and } \ a_m = b_m \ (0 \le m \le k-1).$$

Namely,

$$V_{i,l} \cap V_{i,j} = \{(\sum_{m=0}^{k-1} a_m\alpha^i\beta^m, 0, 0) \mid a_m \in \mathbb{F}_q, \sum_{m=0}^{k-1} a_m = 0\}.$$

Hance,

$$\dim(V_{i,l} \cap V_{i,j}) = k-1.$$

Now from (I-VI) and the dimension distance formula (1) of constant dimension codes, we have $\delta = 1$ and

$$\begin{aligned}|\mathcal{C}| &= 1 + (q^r - 1) + t + t(q^k - 1) + t(q^r - 1) + t(q^k - 1)(q^r - 1) \\ &= \frac{q^n - q^r}{q^k - 1}.\end{aligned}$$

Therefore

$$\mathcal{A}_q(n, 2, k) \geq \frac{q^n - q^r}{q^k - 1}.$$

Theorem 9 Let $n \equiv r \pmod{k}$ and $r = k - 1$. Then, for all q, we have

$$\mathcal{A}_q(n, 2(k-1), k) \geq \frac{q^n - q^r}{q^k - 1}.$$

Proof: Let M be the same as defined in Theorem 8. Now we consider the following subspaces of $\mathbb{F}_q^n$ that are given by

$$\begin{aligned}
W_l^* &= \langle (0, \beta^0, \gamma^l), (0, \beta^1, \gamma^{l+1}), \cdots, (0, \beta^{k-2}, \gamma^{l+k-2}), (0, \beta^{k-1}, 0) \rangle, \\
U_i^* &= \langle (\alpha^i, \beta^i, 0), (\alpha^i\beta, \beta^i, 0), \cdots, (\alpha^i\beta^{k-1}, \beta^i, 0) \rangle, \\
V_{i,j}^* &= \langle (\alpha^i, \beta^j, 0), (\alpha^i\beta, \beta^{j+1}, 0), \cdots, (\alpha^i\beta^{k-1}, \beta^{j+k-1}, 0) \rangle, \\
V_{i,l}^* &= \langle (\alpha^i, \beta^i, \gamma^l), (\alpha^i\beta, \beta^i, \gamma^{l+1}), \cdots, (\alpha^i\beta^{k-2}, \beta^i, \gamma^{l+k-2}), (\alpha^i\beta^{k-1}, \beta^i, 0) \rangle, \\
V_{i,j,l}^* &= \langle (\alpha^i, \beta^j, \gamma^l), (\alpha^i\beta, \beta^{j+1}, \gamma^{l+1}), \cdots, (\alpha^i\beta^{k-1}, \beta^{j+k-2}, \gamma^{l+k-2}), \\
&\qquad (\alpha^i\beta^{k-1}, \beta^{j+k-1}, 0) \rangle.
\end{aligned}$$

where i ranges over $\{0, 1, \cdots, t-1\}$, $j \in \{0, 1, \cdots, q^k - 2\}$ and $l \in \{0, 1, \cdots, q^r - 2\}$. It is easy to see that $\dim W_l^* = \dim U_i^* = \dim V_{i,j}^* = \dim V_{i,l}^* = \dim V_{i,j,l}^* = k$ for all i, j and l. We construct the code $\mathcal{C}^*$ as follows:

$$\mathcal{C}^* = M \cup (\bigcup_l W_l^*) \cup (\bigcup_i U_i^*) \cup (\bigcup_{i,j} V_{i,j}^*) \cup (\bigcup_{i,l} V_{i,l}^*) \cup (\bigcup_{i,j,l} V_{i,j,l}^*).$$

Now we consider the minimum dimension distant d of the constant dimension code $\mathcal{C}^*$.

(I)In the same proof as that in Theorem 8, one can show that

$$M \cap U_i^* = M \cap V_{i,j}^* = M \cap V_{i,l}^* = M \cap V_{i,j,l}^* = \{\mathbf{0}\},$$

and

$$W_l^* \cap U_i^* = W_l^* \cap V_{i,j}^* = W_l^* \cap V_{i,l}^* = W_l^* \cap V_{i,j,l}^* = \{\mathbf{0}\}.$$

From Theorem 8 we can see that $U_{i_1} \cap U_{i_2} = \{\mathbf{0}\}$ for all $0 \leq i_1 \neq i_2 \leq t-1$. With the same reason,

$$U_{i_1}^* \cap U_{i_2}^* = V_{i_1,l}^* \cap V_{i_2,l}^* = V_{i_1,j_1}^* \cap V_{i_2,j_2}^* = V_{i_1,j_1,l}^* \cap V_{i_2,j_2,l}^* = \{\mathbf{0}\}$$

for all j_1, j_2 and l. And any two of $U_i^*, V_{i,j}^*, V_{i,l}^*, V_{i,j,l}^*$ have trivial intersection. From the proof of [2] Theorem 11 we can know that

$$V_{i,j_1}^* \cap V_{i,j_2}^* = V_{i,j_1,l}^* \cap V_{i,j_2,l}^* = V_{i,j_1}^* \cap V_{i,j_2,l}^* = \{\mathbf{0}\}$$

for every fixed i and all $0 \le j_1 \ne j_2 \le q^k - 2$.

(II) Let $A \in W_{l_1}^* \cap W_{l_2}^*$. Then there exists some $a_0, a_1, \cdots, a_{k-1} \in \mathbb{F}_q$ and $b_0, b_1, \cdots, b_{k-1} \in \mathbb{F}_q$, such that

$$A = (0, \sum_{m=0}^{k-1} a_m \beta^m, \sum_{m=0}^{k-2} a_m \gamma^{l_1+m}) = (0, \sum_{m=0}^{k-1} b_m \beta^m, \sum_{m=0}^{k-2} b_m \gamma^{l_2+m}).$$

Namely,

$$\sum_{m=0}^{k-1} a_m \beta^m = \sum_{m=0}^{k-1} b_m \beta^m \quad \text{and} \quad \sum_{m=0}^{k-2} a_m \gamma^{l_1+m} = \sum_{m=0}^{k-2} b_m \gamma^{l_2+m}.$$

Since $\beta^0, \beta^1, \cdots, \beta^{k-1}$ are independent over $\mathbb{F}_q$ and $\gamma^{l_1} \ne \gamma^{l_2}$ $(0 \le l_1 \ne l_2 \le q^r - 2)$ the above equations imply that

$$a_m = b_m \ (0 \le m \le k-1) \quad \text{and} \quad a_0\gamma^0 + a_1\gamma^1 + \cdots + a_{k-2}\gamma^{k-2} = 0.$$

Note that $r = k - 1$, then $\gamma^{k-2} = \gamma^{r-1}$. Therefore we can know that

$$a_0\gamma^0 + a_1\gamma^1 + \cdots + a_{k-2}\gamma^{r-1} = 0.$$

Since $\gamma^0, \gamma^1, \cdots, \gamma^{r-1}$ are independent over $\mathbb{F}_q$,

$$a_0 = a_1 = \cdots = a_{k-2} = 0 \text{ and } a_{k-1} \ne 0.$$

Thus, we have

$$\dim(W_{l_1}^* \cap W_{l_2}^*) = 1.$$

With the same reason,

$$\dim(V_{i,l_1}^* \cap V_{i,l_2}^*) = \dim(V_{i,j,l_1}^* \cap V_{i,j,l_2}^*) = \dim(M \cap W_l^*) = 1.$$

(III) Let $A \in U_i^* \cap V_{i,j}^*$. Then there exists some $a_0, a_1, \cdots, a_{k-1} \in \mathbb{F}_q$ and $b_0, b_1, \cdots, b_{k-1} \in \mathbb{F}_q$, such that

$$\sum_{m=0}^{k-1} a_m \alpha^i \beta^m = \sum_{m=0}^{k-1} b_m \alpha^i \beta^m \quad \text{and} \quad \sum_{m=0}^{k-1} a_m \beta^i = \sum_{m=0}^{k-1} b_m \beta^{j+m}.$$

Therefore

$$a_m = b_m (0 \le m \le k-1) \quad \text{and} \quad \sum_{m=0}^{k-1} a_m \beta^i = \sum_{m=0}^{k-1} b_m \beta^{j+m}.$$

Note that β is a primitive element in GF(q^k), hence

$$a_0 = \cdots = a_{e-1} = a_{e+1} = \cdots = a_{k-1} = 0$$
$$\text{for } i \equiv j + e \pmod{q^k - 1}, 0 \leq e \leq k-1.$$

It means that there exists some $i = 0, \cdots, t-1$ and $j = 0, \cdots, q^k - 2$, such that

$$\dim(U_i^* \cap V_{i,j}^*) = 1.$$

With the same reason,

$$\dim(V_{i,l}^* \cap V_{i,j,l}^*) = 1.$$

(IV) Let $A \in U_i^* \cap V_{i,l}^*$. Then we will have

$$\sum_{m=0}^{k-1} a_m \alpha^i \beta^m = \sum_{m=0}^{k-1} b_m \alpha^i \beta^m, \sum_{m=0}^{k-1} a_m \beta^i = \sum_{m=0}^{k-1} b_m \beta^i \text{ and } \sum_{m=0}^{k-2} b_m \gamma^{l+m} = 0.$$

Therefore,

$$a_m = b_m \ (0 \leq m \leq k-1),$$

and

$$\gamma^l (b_0 \gamma^0 + b_1 \gamma^1 + \cdots + b_{k-2} \gamma^{k-2}) = 0.$$

Namely,

$$\gamma^l (a_0 \gamma^0 + a_1 \gamma^1 + \cdots + a_{k-2} \gamma^{r-1}) = 0.$$

Note that γ is a primitive element in $GF(q^r)$, and $\gamma^0, \gamma^1, \cdots, \gamma^{r-1}$ is independent in $GF(q^r)$, hence

$$a_0 = a_1 = \cdots = a_{k-2} = 0 \text{ and } a_{k-1} \neq 0.$$

Therefore,

$$\dim(U_i^* \cap V_{i,l}^*) = 1.$$

With the same reason,

$$\dim(V_{i,j}^* \cap V_{i,j,l}^*) = 1.$$

(V) Let $A \in V_{i,j}^* \cap V_{i,l}^*$. Then we will have

$$\sum_{m=0}^{k-1} a_m \alpha^i \beta^{m_i} = \sum_{m=0}^{k-1} b_m \alpha^i \beta^{m_i}, \sum_{m=0}^{k-1} a_m \beta^{j+m} = \sum_{m=0}^{k-1} b_m \beta^i, \sum_{m=0}^{k-2} b_m \gamma^{l+m} = 0.$$

Therefore

$$a_m = b_m \ (0 \leq m \leq k-1), \ \sum_{m=0}^{k-1} a_m \beta^{j+m} = \sum_{m=0}^{k-1} b_m \beta^i$$

and

$$\gamma^l(b_0\gamma^0 + b_1\gamma^1 + \cdots + b_{k-2}\gamma^{k-2}) = 0.$$

Note that β is a primitive element in $GF(q^k)$, hence

$$a_0 = \cdots = a_{e-1} = a_{e+1} = \cdots = a_{k-1} = 0$$
$$\text{for } i \equiv j + e \pmod{q^k - 1}, 0 \leq e \leq k-1,$$

and

$$a_0 = a_1 = \cdots = a_{k-2} = 0.$$

This means that

$$\dim(V^*_{i,j} \cap V^*_{i,l}) = 1 \text{ if } e = k-1,$$

and

$$\dim(V^*_{i,j} \cap V^*_{i,l}) = 0 \text{ if } e \neq k-1.$$

Namely,

$$\dim(V^*_{i,j} \cap V^*_{i,l}) \leq 1.$$

With the same reason,

$$\dim(U^*_i \cap V^*_{i,j,l}) = \dim(V^*_{i,l_1} \cap V^*_{i,j,l_2}) \leq 1.$$

Now from (I-V) and the dimension distance formula (1) of constant dimension codes, we have $\delta = k-1$ and

$$\begin{aligned} |\mathcal{C}^*| &= 1 + (q^r - 1) + t + t(q^k - 1) + t(q^r - 1) + t(q^k - 1)(q^r - 1) \\ &= \frac{q^n - q^r}{q^k - 1}. \end{aligned}$$

Therefore

$$\mathcal{A}_q(n, 2(k-1), k) \geq \frac{q^n - q^r}{q^k - 1}.$$

From the proof of Theorem 8 and Theorem 9, we can imply that $\mathcal{C}$, respectively $\mathcal{C}^*$, in Theorem 8, respectively in Theorem 9 are more perfect than that in Proposition 7 ([1], Theorem 1.4). While we herein add a condition $r = k-1$ to the case of $\mathcal{C}^*$, we can imply that the code $\mathcal{C}^*$ which constructed in [1] is not perfect. Of course, from Proposition 4 and Proposition 5 we can know that the codes $\mathcal{C}$ and $\mathcal{C}^*$ in above do not achieve the upper bound. From Corollary 3 we can also compute the codewords of $\mathcal{C}^\perp$ and $\mathcal{C}^{*\perp}$.

Acknowledgements

This work is supported by the National Natural Science Foundation of China under Grant No.61179026 and the Fundamental Research Funds for the Central Universities under Grant No.Y15-26.

References

[1] Q. Liao and J. Zhu, A note on optimal constant dimension codes, *International Journal of Foundations of Computer Science*, 26(1), 143-152(2015).

[2] T. Etzion and A. Vardy, Error-correcting codes in projective spaces, *IEEE Trans. Inf. Theory*, 57(2), 1165-1173(2011).

[3] Z. Wan, Geometry of classical groups over finite fields, 2nd edition, Science Press, Beijing/New York, 2002.

[4] E. R. Koetter and F. R. Kschischang, Coding for errors and erasures in random network coding, *IEEE Trans. Inf.Theory*, 54(8), 3579-3591(2008).

[5] S. Xia and F. Fu, Johnson type bounds on constant dimension codes, *Designs, Codes Cryptogr*, 50, 163-172, (2009).

[6] A. Khaleghi, D. Silva and F. R. Kschischang, Subspace codes, *Pro. 12th IMA lnt. Conf. Cryptography Coding*, 49(4), 1-21(2009).

[7] A. Kohnert and S. Kurz, Construction of dimension codes with a prescribed minimum distance, *Mathematical Methods in Computer Science: Essays in Memory of Thomas Beth*, 5393, 31-42(2008).

[8] H. Wang, C.Xing, and R. Safavi-Naini, Linear authentication codes: Bounds and constructions, *IEEE Trans. Inf. Theory*, 49(4), 866-872(2003).

[9] T. Bu, Partitions of a vector space, *Discrete Math*, 31, 79-83(1980).

[10] M. Schwartz and T. Etzion, Codes and anticodes in the Grassmann graph, *J. Combin. Theory, ser. A*, 97, 27-42(2002).