Bull. Korean Math. Soc. **53** (2016), No. 1, pp. 263–272
http://dx.doi.org/10.4134/BKMS.2016.53.1.263

ON THE SEPARATION OF LINEAR CONSTANT-WEIGHT CODES

Zihui Liu

Abstract. By using the finite projective geometry method, the separating properties of linear constant-weight codes are presented. An algorithm is given for computing the cardinality of separating coordinate positions of certain disjoint codeword sets of linear constant-weight codes.

1. Introduction

The separating properties of linear q-ary codes (codes over the finite field $GF(q)$) and their applications were first addressed in [2] and [4], where *separating codes* were introduced as a type of codes used to realize digital watermarking, and each codeword of a separating code is regarded as a content assigned to a user (each codeword represent the same content) with an embedded watermark. If a separating code was used in a digital watermarking system, the security performance of the system was determined by the separating property of certain codeword sets of the code, and a code is called separating if the minimum cardinality of separating coordinate positions with respect to the codeword sets is nonzero. To construct codes with separating properties and to give judging criterions for the separation are meaningful and interesting research work [2], [3], [4], and [5].

The *value function* (also called *value assignment*) was introduced in [1]. Wood [8] also called it *multiplicity function*. The value function is an effective tool to study codes, and we will use it in this paper to address our results.

Definition 1. A value function is a correspondence $m(\cdot) : PG(k-1,q) \to \mathbb{Z}$, where $\mathbb{Z}$ represents the set of integers and $PG(k-1,q)$ represents a $(k-1)$-dimensional projective space over the finite field $GF(q)$. For any point $p \in PG(k-1,q)$, call $m(p)$ the *value* of p.

Received February 4, 2015; Revised May 10, 2015.
2010 *Mathematics Subject Classification.* 94B05.
Key words and phrases. feasible set, separating property, intersection number, value assignment, disjoint codeword sets.
This work was supported by The National Science Foundation of China (No. 11171366 and No. 61170257).

©2016 Korean Mathematical Society

Define *value* of $S \subset PG(k-1,q)$ by $m(S) = \sum_{p\in S} m(p)$. The value function can determine a linear code up to equivalence in a way as follows: take a point $p \in PG(k-1,q)$ as a column in a matrix and repeat it $m(p)$ times in the columns of the matrix, then the code generated by the matrix is determined (up to equivalence). Conversely, consider the columns of G (with no zero-column), a generator matrix of a k-dimensional q-ary linear code $\mathcal{C}$, as projective points in $PG(k-1,q)$. For a point $p \in PG(k-1,q)$, let $m(p)$ be the number of the times the point p occurs in the columns of G. We thus obtain a value function $m(\cdot) : PG(k-1,q) \to \mathbb{Z}$ such that $m(\cdot) \geq 0$. Note that a linear code may have many value functions, however, the value function is unique once one fixes a generator matrix of the code.

Definition 2. A code $\mathcal{C}$ determined by a value function $m(\cdot)$ is called projective if $m(p) \leq 1$, for all $p \in PG(k-1,q)$.

Assume a generator matrix with the value function $m(\cdot)$ has n columns (thus, the code $\mathcal{C}$ generated by this matrix has length n). Then, $m(PG(k-1,q)) = \sum_{p\in PG(k-1,q)} m(p) = n$.

2. The value function and the separation

A code is called t-intersecting if any t nonzero codewords contain some common nonzero coordinate positions which are called *intersection* of these t codewords. The minimum size of intersections among all the possible t nonzero codewords is called t-intersection number of the code. Obviously, a code is t-intersecting if and only if its t-intersection number is greater than zero. When the code is 2-intersecting, the code is briefly called intersecting.

Assume T is a codeword set of a q-ary code $\mathcal{C}$ with length n. For any position i, $1 \leq i \leq n$, define

$$T_i = \{x_i : \text{ there exists } x = (x_1, \ldots, x_i, \ldots, x_n) \text{ such that } x \in T\}.$$

The *feasible set* of T is defined by

$$F(T) = \{x = (x_1, \ldots, x_i, \ldots, x_n) \in GF(q)^n \ : \ x_i \in T_i, \ \text{ for } i = 1, \ldots, n\}.$$

Definition 3 ([2])**.** A code $\mathcal{C}$ is (t,t')-separating if, for any pair (T,T') of disjoint codeword sets of $\mathcal{C}$ where $|T| = t$ and $|T'| = t'$, the feasible sets are disjoint, that is, $F(T) \cap F(T') = \emptyset$.

Obviously, if a linear code is (t,t')-separating, then it is also (t',t)-separating.

For any disjoint codeword sets T and T' of $\mathcal{C}$, define $\theta(T,T') = \{i \mid T_i \cap T'_i = \emptyset\}$. We call an element of $\theta(T,T')$ a *separating coordinate position* of T and T'. Denote

$$\theta_{t,t'} = \min\{|\theta(T,T')|, \text{ for all disjoint codeword sets } T, T' \subset \mathcal{C} \text{ , with } |T| = t \text{ and } |T'| = t'\}. \tag{1}$$

Then, $\mathcal{C}$ is (t,t')-separating if and only if $\theta_{t,t'} > 0$. Since the operation of minus a same vector from the vectors in T and T' does not change $|\theta(T,T')|$, one

may additionally assume that one of vectors in T or in T' is zero vector. Then, it can be observed that the $(t,1)$-separation is equivalent to the t-intersection.

Remark 4. It can be checked that equivalent codes have the same parameter $\theta_{t,t'}$, and thus have the same separation properties. We may use the value function to study the separation of codes.

Throughout the paper, if A is a set, then $\overline{A} := \{x : x \notin A\}$. If G is the generator matrix (generating a k-dimensional q-ary code $\mathcal{C}$) determined by a value function $m(\cdot)$ and $c \in \mathcal{C}$ is a codeword, then one may write

$$c = vG$$

for some $v \in GF(q)^k$. Define

$$v^{\perp} := \{p : p \in GF(q)^k, \text{ and } (v,p) = 0\}, \tag{2}$$

where (v,p) represents the usual inner product of v and p. Note that $v^{\perp}$ is a $(k-2)$-dimensional subspace when considered as a subset of $PG(k-1,q)$.

Definition 5. Call the $(k-2)$-dimensional (projective) subspace $v^{\perp}$ in (2) the subspace corresponding to the codeword c.

Obviously, if P corresponds to the codeword c, then $m(P)$ is exactly the number of the coordinate positions of c being equal to zero.

We may state the separation of codes in our viewpoint as follows: If

$$c_1 = v_1 G$$
$$c_2 = v_2 G$$

are two codewords, then the equal coordinate positions of c_1 and c_2 are those points p appeared in the columns of G such that

$$(v_1, p) = (v_2, p),$$

or equivalently,

$$(v_1 - v_2, p) = 0. \tag{3}$$

Likewise, the nonequal coordinate positions of c_1 and c_2 are those points p appeared in the columns of G such that

$$(v_1, p) \neq (v_2, p),$$

or equivalently,

$$(v_1 - v_2, p) \neq 0. \tag{4}$$

Thus, if we denote S_1 the set of points p satisfying (3), and denote S_2 the set of points p satisfying (4), then, according to the viewpoint of value function $m(\cdot)$, the number of equal coordinate positions of c_1 and c_2 and the number of nonequal coordinate positions are $m(S_1)$ and $m(S_2)$, respectively. Note also that S_1 is exactly the subspace corresponding to the codeword $c_1 - c_2$ by Definition 5.

In addition, if P_1 and P_2 correspond to the codewords c_1 and c_2, respectively, then $m(S)$ is exactly the size of the intersection of c_1 and c_2, where $S = \{p : p \notin (P_1 \cup P_2)\} = \overline{P_1 \cup P_2}$. Thus, $m(S) = m(PG(k-1,q) - m(P_1 \cup P_2) = n - m(P_1 \cup P_2)$. Similarly, if the subspaces P_i correspond to the codewords c_i, $1 \le i \le t$, then the size of the intersection of these t codewords is equal to $m(PG(k-1,q)) - m(\cup_{i=1}^{i=t} P_i) = n - m(\cup_{i=1}^{i=t} P_i)$.

Summing up the text, we get:

Lemma 6. *Assume $\mathcal{C}$ is a q-ary $[n,k]$ code determined by a value function $m(\cdot)$. Then, $\mathcal{C}$ is $(\tau,1)$-separating if and only if $n - m(\cup_{i=1}^{i=\tau} P_i) = m(PG(k-1,q)) - m(\cup_{i=1}^{i=\tau} P_i) > 0$ for any τ projective subspaces P_i with dimension $k-2$, $1 \le i \le \tau$.*

It is well known that the equation $PG(k-1,q) = \cup_{i=1}^{i=q+1} P_i$ can be achieved when one chooses the $(k-2)$-dimensional subspaces P_i, $1 \le i \le q+1$, properly, and then $m(PG(k-1,q)) - m(\cup_{i=1}^{i=q+1} P_i) = 0$. Thus, if a q-ary code is $(\tau,1)$-separating, then $\tau \le q$ by Lemma 6. In addition, if a code is (t,t')-separating, then it is also (u,u')-separating for any $u \le t$ and $u' \le t'$. These facts yield:

Corollary 7 ([3])**.** *If a q-ary code is (t,t')-separating, then* $\max\{t,t'\} \le q$.

Linear constant-weight codes play an important role in coding theory, and they have been extensively studied. It was shown in [6] and [7] that the value function of a constant-weight code takes the same value at each projective point, namely, $m(\cdot) \equiv \iota$, for some constant $\iota > 0$. Equivalently, a constant-weight code can be viewed as copies of a *simplex* code which has value function $m(\cdot) \equiv 1$. Obviously, a simplex code is projective. If a simplex code has parameter $\theta_{t,t'}$ (see (1)), then the minimum cardinality of separating coordinate positions of a constant-weight code with $m(\cdot) \equiv \iota$ is equal to $(\theta_{t,t'})\iota$. Thus, we get:

Lemma 8. *A linear constant-weight code has the same (t,t')-separating property as a simplex code for any parameters t and t'.*

3. General separation

Cohen [3] has shown that a constant-weight code is $(2,2)$-separating. Such a result can be substantially improved by using our viewpoint in Section 2.

The following lemma is useful.

Lemma 9. *Let $\mathcal{C}$ be an $[n,k]$ code. If $\mathcal{C}$ is $(\tau,1)$-separating, then it is (t,t')-separating for any $tt' \le \tau$.*

Proof. Assume G is a generator matrix of $\mathcal{C}$. Let $T = \{c_i : i = 1,\dots,t\}$ and $T' = \{c'_j : j = 1,\dots,t'\}$ be any two disjoint codeword sets, and let

$$c_i = v_i G,\ i = 1,\dots,t$$
$$c'_j = v'_j G,\ j = 1,\dots,t'.$$

Assume P_{ij} is the $(k-2)$-dimensional subspace corresponding to $c_i - c'_j$, $1 \le i \le t$, $1 \le j \le t'$. Then, according to Definition 5, the statement below holds.

(5) $(v_i - v'_j, p) = 0$ if and only if $p \in P_{ij}, 1 \le i \le t, 1 \le j \le t'$.

From (5), we get

$$\begin{aligned} |\theta(T,T')| &= m(\overline{\cup_{i=1}^{i=t}(\cup_{j=1}^{j=t'} P_{ij})}) \\ &= m(PG(k-1,q)) - m(\cup_{i=1}^{i=t}(\cup_{j=1}^{j=t'} P_{ij})). \\ &= n - m(\cup_{i=1}^{i=t}(\cup_{j=1}^{j=t'} P_{ij})). \end{aligned}$$

Since $\mathcal{C}$ is $(\tau,1)$-intersecting and $tt' \le \tau$, it follows that $|\theta(T,T')| > 0$ by Lemma 6. Thus, $\mathcal{C}$ is (t,t')-separating. □

Remark 10. The converse of Lemma 9 is not right, for example, a binary or a ternary constant-weight code is $(2,2)$-separating [3], but it is not $(4,1)$-separating by Corollary 7.

If a q-ary code is $(t,1)$-separating, then $t \le q$ by Corollary 7. The following lemma shows that a simplex code is perfect in this respect.

Lemma 11. *Assume $\mathcal{C}$ is a k-dimensional q-ary simplex code. Then, $\mathcal{C}$ is $(q,1)$-separating.*

Proof. It is suffice to show by Lemma 6 that

$$m(PG(k-1,q)) - m(\cup_{i=1}^{i=q} P_i) > 0$$

for any q (projective) subspaces P_i, $1 \le i \le q$, of dimension $(k-2)$.

Since $m(p) \equiv 1$ for a simplex code, it follows that

$$\begin{aligned} & m(PG(k-1,q)) - m(\cup_{i=1}^{i=q} P_i) \\ = & \frac{q^k-1}{q-1} - |\cup_{i=1}^{i=q} P_i| \\ \ge & \frac{q^k-1}{q-1} - \left(q\frac{q^{k-1}-1}{q-1} - (q-1)\frac{q^{k-2}-1}{q-1}\right) \\ = & q^{k-2} > 0. \end{aligned}$$

□

Lemma 8, Lemma 9 and Lemma 11 yield.

Theorem 12. *Assume $\mathcal{C}$ is a q-ary $[n,k]$ constant-weight code. If $q \ge tt'$, then $\mathcal{C}$ is (t,t')-separating.*

If we fix $t = 2$ or $t' = 2$ and consider $(2,t)$-separating property of a linear constant-weight code, then the result of Theorem 12 can be further improved.

Lemma 13. *Assume $\mathcal{C}$ is a q-ary $[n,k]$ projective code with value function $m(\cdot)$, and let D represent the maximum codeword weight of $\mathcal{C}$. If $D < n - \frac{q^{k-1}-1}{q-1} + q^{k-3}$, then $\mathcal{C}$ is $(2,t)$-separating for any $t \le q$. Particularly, any q-ary $[n,k]$ projective code with $n > \frac{q^k-1}{q-1} - q^{k-3}$ is $(2,t)$-separating for any $t \le q$.*

Proof. Let $c_0 \in \mathcal{C}$ be a codeword with the maximum weight D, and P_0 is the $(k-2)$-dimensional subspace corresponding to c_0. Then, it can be checked that $D = n - m(P_0)$, furthermore,

$$n - D = m(P_0) = \min\{m(P) : P \text{ ia a } (k-2)\text{-dimensional subspace}\}. \tag{6}$$

Since $n - D > \frac{q^{k-1}-1}{q-1} - q^{k-3}$ according to the condition of the theorem, it follows by (6) that

$$m(P) > \frac{q^{k-1}-1}{q-1} - q^{k-3} \tag{7}$$

for any $(k-2)$-dimensional subspace P. Now let $T = \{0, c_1\}$ and $T' = \{c_1', c_2', \ldots, c_t'\}$ be any two disjoint codeword sets, and assume that the $(k-2)$-dimensional subspaces P_1 and P_i' correspond to c_1 and c_i', $1 \le i \le t$, respectively.

Let G be a generator matrix of $\mathcal{C}$, and write

$$\begin{aligned} c_1 &= v_1 G, \\ c_i' &= v_i' G,\ i = 1, \ldots, t. \end{aligned}$$

Consider the set S of the projective points p such that

$$\begin{aligned} (v_1, p) &= 0, \\ (v_i', p) &\neq 0,\ i = 1, \ldots, t. \end{aligned}$$

Then, it can be checked that $S \subset \theta(T, T')$ and so $|\theta(T,T')| \ge m(S)$. Thus, to prove $|\theta(T,T')| > 0$, it suffices to show $m(S) > 0$.

Note that the set S of the points p may be written as

$$P_1 \cap (\cap_{i=1}^{i=t} \overline{P_i'}).$$

Then,

$$\begin{aligned} m(S) &= m(P_1 \cap (\cap_{i=1}^{i=t} \overline{P_i'})) \\ &= m(P_1 \cap (\overline{\cup_{i=1}^{i=t} P_i'})) \\ &= m(P_1 \cap (\overline{\cup_{i=1}^{i=t} (P_1 \cap P_i')})) \\ &= m(P_1) - m(\cup_{i=1}^{i=t} (P_1 \cap P_i')) \\ &> \left(\frac{q^{k-1}-1}{q-1} - q^{k-3}\right) - |\cup_{i=1}^{i=t} (P_1 \cap P_i')| \qquad \text{(by (7) and } m(\cdot) \le 1) \\ &\ge \left(\frac{q^{k-1}-1}{q-1} - q^{k-3}\right) - \left(t\frac{q^{k-2}-1}{q-1} - (t-1)\frac{q^{k-3}-1}{q-1}\right) \end{aligned}$$

$$\begin{aligned}&(\text{by } \dim(P_1 \cap P_i') = k-2)\\ &= q^{k-3}(q-t) \geq 0.\end{aligned}$$

Thus, $\mathcal{C}$ is $(2,t)$-separating for any $t \leq q$. □

Since a q-ary $[n,k]$ simplex code has $n = \frac{q^k-1}{q-1} > \frac{q^k-1}{q-1} - q^{k-3}$, by using Lemma 13, we have:

Corollary 14. *A q-ary simplex code is $(2,t)$-separating for any $t \leq q$.*

Lemma 8 and Corollary 14 yield.

Theorem 15. *Assume $\mathcal{C}$ is a q-ary $[n,k]$ constant-weight code. Then, $\mathcal{C}$ is $(2,t)$-separating for any $t \leq q$.*

4. The parameter $\theta_{t,t'}$ of a linear constant-weight code and its applications

In the previous section, we present the separating properties of constant-weight codes by estimating $\theta_{t,t'}$. In general, it is enough to give the estimation of $\theta_{t,t'}$ in order to judge the (t,t') separating property. In this section, we will, however, aim at computing the parameter $\theta_{t,t'}$ explicitly. The reason is that the parameter $\theta_{t,t'}$ can not only be used to judge the (t,t')-separation of codes, but also can be used to construct new (t,t')-separating codes from linear constant-weight codes as follows.

Let $\mathcal{C}$ be a q-ary $[n,k]$ constant-weight code with value function $m(\cdot) \equiv \iota$. If $\theta_{t,t'} > 1$ for $\mathcal{C}$, then, since $m(p) \equiv \iota > 0$, $\forall\ p \in PG(k-1,q)$, we may obtain another (t,t')-separating $[n-1,k]$ code $\mathcal{C}'$ by penetrating a separating coordinate position of $\mathcal{C}$. $\mathcal{C}'$ has parameter $\theta_{t,t'} - 1$, and if $\theta_{t,t'} - 1 > 1$, we may proceed to consider similar operations applied to $\mathcal{C}'$ to get additional k-dimensional (t,t')-separating codes.

In general, in such a way above, we may obtain many (t,t')-separating k-dimensional q-ary codes by penetrating some separating coordinate positions of $\mathcal{C}$.

It is lucky that computing $\theta_{t,t'}$ for a constant-weight code is possible particular for smaller t and t', though the task is difficult for general linear codes.

Taking the computation of $\theta_{2,3}$ of a constant-weight code as an example, we describe the algorithm.

Let $T = \{0, c_1\}$ and $T' = \{c_2, c_3, c_4\}$ be any two disjoint codeword sets of a q-ary $[n,k]$ constant-weight code. Assume

$$\begin{aligned}c_1 &= v_1 G\\ c_i &= v_i G,\ \ i = 2,3,4.\end{aligned}$$

Then, since $m(\cdot) \equiv \iota$, $|\theta(T, T')|$ is equal to $|W|\iota$, where W is the set of the projective points p satisfying

$$\begin{cases} (v_2, p) \neq 0 \\ (v_3, p) \neq 0 \\ (v_4, p) \neq 0 \\ (v_2 - v_1, p) \neq 0 \\ (v_3 - v_1, p) \neq 0 \\ (v_4 - v_1, p) \neq 0. \end{cases}$$

Assume the subspaces W_i, $1 \leq i \leq 6$, correspond to the codeword c_2, c_3, c_4, $c_2 - c_1$, $c_3 - c_1$ and $c_4 - c_1$, respectively (see Definition 5). Then,

$$W = \cap_{i=1}^{i=6} \overline{W_i}.$$

To compute $|W| = |\cap_{i=1}^{i=6} \overline{W_i}| = |\overline{\cup_{i=1}^{i=6} W_i}| = |PG(k-1, q)| - |\cup_{i=1}^{i=6} W_i|$, we may use the formula

$$\begin{aligned} |\cup_{i=1}^{i=6} W_i| = & \sum_{1 \leq i_1 \leq t} |W_{i_1}| - \sum_{1 \leq i_1 < i_2 \leq 6} |W_{i_1} \cap W_{i_2}| \\ & + \sum_{1 \leq i_1 < i_2 < i_3 \leq 6} |W_{i_1} \cap W_{i_2} \cap W_{i_3}| - \cdots - |\cap_{i=1}^{i=6} W_i|. \end{aligned} \tag{8}$$

Each term in (8) can be considered as the number of the nonzero solutions (viewed as projective points) of an equations system. For example, $W_1 \cap W_2 \cap W_4$ is the set of the nonzero solutions (viewed as projective points) of the equations system below

$$\begin{cases} (v_2, p) = 0 \\ (v_3, p) = 0 \\ (v_2 - v_1, p) = 0. \end{cases} \tag{9}$$

Thus, to get $|W_1 \cap W_2 \cap W_4|$, it is suffice to obtain $\text{rank}\{v_2, v_3, v_2 - v_1\}$, namely, the rank of the coefficient matrix of the equations system. To get each term in (8), we may divide the analysis into several cases:

(case i) $\text{rank}\{v_1, v_2, v_3, v_4\} = 4$. Then, the rank of the coefficient matrix of each equations system such as (9) can be determined.

(case ii) $\text{rank}\{v_1, v_2, v_3, v_4\} = 3$ and $\text{rank}\{v_1, v_2, v_3\} = 3$ (without loss of generality), and assume $v_4 = x_1 v_1 + x_2 v_2 + x_3 v_3$. Then, the rank of the coefficient matrix of each equations system such as (9) can be determined according to x_1, x_2 and x_3.

(case iii) $\text{rank}\{v_1, v_2, v_3, v_4\} = 2$ and $\text{rank}\{v_1, v_2\} = 2$ (without loss of generality), and assume $v_3 = x_1 v_1 + x_2 v_2$ and $v_4 = y_1 v_1 + y_2 v_2$. Then, the rank of the coefficient matrix of each equations system such as (9) can be determined according to x_1, x_2, y_1 and y_2.

(case iv) $\text{rank}\{v_1, v_2, v_3, v_4\} = 1$ and assume $v_i = x_i v_1$, $2 \leq i \leq 4$. Then, the rank of the coefficient matrix of each equations system such as (9) can be determined.

By comparing (case i)-(case iv), both $\theta_{2,3} = \min_{T,T'} \theta(T,T')$ and a group of vectors $\{v_1, v_2, v_3, v_4\}$ attaining $\theta_{2,3}$ can be determined. Using this group of vectors $\{v_1, v_2, v_3, v_4\}$ attaining $\theta_{2,3}$, one gets the set W, and then as stated above, some other $(2,3)$-separating codes can be obtained by using the set W.

We sum up the algorithm as follows.

Proposition 16. *For modest small parameters t and t', $\theta_{t,t'}$ can be exactly determined for a linear constant-weight code $\mathcal{C}$, and some other (t,t')-separating codes can be obtained from $\mathcal{C}$.*

If $q \geq 7$, we may determine $\theta_{2,3}$ for a q-ary constant-weight code in an alternative way which is simpler than that above. Preserve the same notations as before. Then, since

$$\begin{aligned}\theta(T,T') = |W|\iota &= (|PG(k-1,q)| - |\cup_{i=1}^{i=6} W_i|)\iota \\ &\geq \left(\frac{q^k-1}{q-1} - \left(6\cdot\frac{q^{k-1}-1}{q-1} - 5\cdot\frac{q^{k-2}-1}{q-1}\right)\right)\iota \\ &= q^{k-2}(q-5)\iota,\end{aligned}$$

$\theta_{2,3}$ satisfies $\theta_{2,3} \geq q^{k-2}(q-5)\iota$. Furthermore, $\theta_{2,3} = q^{k-2}(q-5)\iota$ if and only if $|\cup_{i=1}^{i=6} W_i| = 6\cdot\frac{q^{k-1}-1}{q-1} - 5\cdot\frac{q^{k-2}-1}{q-1}$, which is equivalent to $W_i \neq W_j$ and $W_i \cap W_j = \cap_{l=1}^{l=6} W_l$ for any $1 \leq i < j \leq 6$. This equivalently demands that

$$\begin{aligned}&\text{rank}\{v_2, v_3, v_4, v_2 - v_1, v_3 - v_1, v_4 - v_1\} = 2, \text{ and no two vectors} \\ &\text{differ only by a nonzero multiple.}\end{aligned} \tag{10}$$

Since $\text{rank}\{v_2, v_3, v_4, v_2 - v_1, v_3 - v_1, v_4 - v_1\} = \text{rank}\{v_1, v_2, v_3, v_4\}$, we may without loss of generality assume $\text{rank}\{v_1, v_2\} = 2$ and $v_3 = x_{31}v_1 + x_{32}v_2$, and $v_4 = x_{41}v_1 + x_{42}v_2$. Then,

$$\begin{aligned}&\{v_2, v_3, v_4, v_2 - v_1, v_3 - v_1, v_4 - v_1\} = \{v_2, x_{31}v_1 + x_{32}v_2, x_{41}v_1 + x_{42}v_2, \\ &-v_1 + v_2, (x_{31}-1)v_1 + x_{32}v_2, (x_{41}-1)v_1 + x_{42}v_2\},\end{aligned}$$

and condition (10) is satisfied only if the following conditions hold:

$$\begin{aligned}&x_{32} \neq 0, x_{42} \neq 0, \text{ and the elements} \\ &\text{of the set } \left\{0, -1, \frac{x_{31}}{x_{32}}, \frac{x_{41}}{x_{42}}, \frac{x_{31}-1}{x_{32}}, \frac{x_{41}-1}{x_{42}}\right\} \text{ are} \\ &\text{different ones of the finite field } GF(q).\end{aligned} \tag{11}$$

If $q \geq 7$, we may denote $GF(q) = \{0, -1, a_1, a_2, a_3, a_4, \ldots, a_{q-2}\}$ and let

$$\begin{cases} \frac{x_{31}}{x_{32}} = a_1 \\ \frac{x_{41}}{x_{42}} = a_2 \\ \frac{x_{31}-1}{x_{32}} = a_3 \\ \frac{x_{41}-1}{x_{42}} = a_4, \end{cases}$$

or equivalently,

$$\begin{cases} x_{31} = \dfrac{a_1}{a_1 - a_3} \\ x_{32} = \dfrac{1}{a_1 - a_3} \\ x_{41} = \dfrac{a_2}{a_2 - a_4} \\ x_{42} = \dfrac{1}{a_2 - a_4}, \end{cases} \tag{12}$$

then the condition (11) can be satisfied. Thus, we have:

Theorem 17. *Let $q \geq 7$ and $GF(q) = \{0, -1, a_1, a_2, a_3, a_4, \ldots, a_{q-2}\}$. Then, a q-ary $[n, k]$ constant-weight code with $m(\cdot) \equiv \iota$ satisfies $\theta_{2,3} = q^{k-2}(q-5)\iota$, and a group of vectors $\{v_1, v_2, v_3, v_4\}$ can achieve $\theta_{2,3}$, where rank$\{v_1, v_2, v_3, v_4\}$ = rank$\{v_1, v_2\} = 2$, and $v_3 = x_{31}v_1 + x_{32}v_2$, and $v_4 = x_{41}v_1 + x_{42}v_2$, and x_{31}, x_{32}, x_{41} and x_{42} satisfy* (12).

5. Conclusion

In this paper, we present separating properties of linear constant-weight codes, and state an effective computing method to determine the size of the separating coordinate positions of a linear constant-weight code by using the value function.

References

[1] W. D. Chen and T. Kløve, *The weight hierarchies of q-ary codes of dimension 4*, IEEE Trans. Inform. Theory **42** (1996), no. 6, 2265–2272.
[2] G. Cohen, S. Encheva, S. Litsyn, and H. G. Schaathun, *Intersecting codes and separating codes*, Discrete Appl. Math. **128** (2003), no. 1, 75–83.
[3] G. Cohen, S. Encheva, and H. G. Schaathun, *More on* $(2, 2)$*-separating systems*, IEEE Trans. Inform. Theory **48** (2002), no. 9, 2606–2609.
[4] G. Cohen and G. Zémor, *Intersecting codes and independent families*, IEEE Trans. Inform. Theory **40** (1994), 1872–1881.
[5] S. Encheva and G. Cohen, *Constructions of intersecting codes*, IEEE Trans. Inform. Theory **45** (1999), no. 4, 1234–1237.
[6] Z. H. Liu and W. D. Chen, *Notes on the value function*, Des. Codes Cryptogr. **54** (2010), no. 1, 11–19.
[7] J. A. Wood, *The structure of linear codes of constant weight*, Trans. Amer. Math. Soc. **354** (2002), no. 3, 1007–1026.
[8] ———, *Relative one-weight linear codes*, Des. Codes Cryptogr. **72** (2014), no. 2, 331–344.

Department of Mathematics
Beijing Institute of Technology
Beijing 100081, P. R. China
E-mail address: lzhui@bit.edu.cn