Finite Fields and Their Applications 49 (2018) 180–197

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Maximum distance separable codes for b-symbol read channels ☆

Baokun Ding [a], Tao Zhang [b], Gennian Ge [b,*]

[a] *School of Mathematical Sciences, Zhejiang University, Hangzhou 310027, China*
[b] *School of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China*

ARTICLE INFO

Article history:
Received 26 October 2016
Received in revised form 23 August 2017
Accepted 16 October 2017
Available online 27 October 2017
Communicated by Olga Polverino

MSC:
94B25
94B60

Keywords:
MDS b-symbol codes
Projective geometry
Constacyclic codes

ABSTRACT

Recently, Yaakobi et al. introduced codes for b-symbol read channels, where the read operation is performed as a consecutive sequence of $b > 2$ symbols. In this paper, we establish a Singleton-type bound for b-symbol codes. Codes meeting the Singleton-type bound are called maximum distance separable (MDS) codes, and they are optimal in the sense they attain the maximal minimum b-distance. We introduce a construction method using projective geometry, and then construct several infinite families of linear MDS b-symbol codes over finite fields. The lengths of these codes have a large range. And in some sense, we completely determine the existence of linear MDS b-symbol codes over finite fields for certain parameters.

☆ The research is supported by the National Natural Science Foundation of China under Grant Nos. 11431003 and 61571310, Beijing Scholars Program, Beijing Hundreds of Leading Talents Training Project of Science and Technology, and Beijing Municipal Natural Science Foundation.

* Corresponding author.
E-mail address: gnge@zju.edu.cn (G. Ge).

https://doi.org/10.1016/j.ffa.2017.10.002
1071-5797/

1. Introduction

In the traditional information theory, noisy channels are analyzed generally by dividing the message into individual information units. However, with the development of storage technologies, one finds that symbols cannot always be written and read consistently in channels that output overlapping symbols.

In 2011, Cassuto and Blaum [1] first proposed a new coding framework for symbol-pair read channels. The outputs of the read process in the channels are overlapping pairs of symbols. After that, Chee et al. [3] established a Singleton-type bound for symbol-pair codes and considered the constructions of symbol-pair codes meeting the bound. For a complete comprehension of the fruitful results on this topic, please refer to [1–7,9,10] and the references therein.

Recently, Yaakobi et al. [10] generalized the coding framework for symbol-pair read channels to that for b-symbol read channels, where the read operation is performed as a consecutive sequence of $b > 2$ symbols. They also generalized some of the known results for symbol-pair read channels to those for b-symbol read channels.

This paper continues the investigation of codes for b-symbol read channels. We establish a Singleton-type bound for b-symbol codes, and codes meeting this bound are maximum distance separable (MDS). MDS b-symbol codes are optimal in the sense they attain the maximal minimum b-distance and thus have the best possible capability against errors in b-symbol read channels. We show that there exists a linear MDS b-symbol code once one finds a suitable matrix. And then we introduce a method using projective geometry, which allows us to construct linear MDS b-symbol codes with a large range of lengths. As a result, we construct the following families of linear MDS b-symbol codes over finite fields.

(1) There exists an MDS $(n, 7)_q$ 3-symbol code for q being a prime power and $7 \le n \le q^3 + q^2 + q + 1$ (see Theorem 3.8).
(2) There exists an MDS $(n, 9)_q$ 4-symbol code for $q \ge 3$ being a prime power and $9 \le n \le q^4 + q^3 + q^2 + q + 1$ (see Theorem 3.10).
(3) There exists an MDS $(n, 2b+1)_q$ b-symbol code for q being a prime power, $q \ge b \ge 5$ and $2b + 1 \le n \le q^b - bq^{b-1} + \frac{b^2+3b}{2}$ (see Theorem 3.11).
(4) There exists an MDS $(n, 2b)_q$ b-symbol code with $n \ge 2b$ for $q \ge b - 1$ being a prime power, $b \ge 3$ or $q = 2, b = 4$ (see Theorem 3.13).
(5) There exists an MDS $(n, 10)_q$ 5-symbol code for $q \ge 3$ being a prime power and $n \ge 10$ (see Theorem 3.14).
(6) There exists an MDS $(\frac{q^{b+1}-1}{q-1}, 2b + 1)_q$ b-symbol code for q being prime power and any $b \ge 4$ (see Theorem 4.2).

We also propose the following two conjectures in Section 5.

- There exist linear MDS $(n, 2b+1)_q$ b-symbol codes for q being a prime power, $b > 2$ and $2b+1 \leq n \leq \frac{q^{b+1}-1}{q-1}$.
- There exist linear MDS $(n, 2b)_q$ b-symbol codes for q being a prime power, $b > 2$ and $n \geq 2b$.

The first four families are our main results. We claim that a linear MDS $(n, 2b+1)_q$ b-symbol code over $\mathbb{F}_q$ exists only when $2b+1 \leq n \leq \frac{q^{b+1}-1}{q-1}$ (Lemma 3.3). And the family (4) indicates that a linear MDS b-symbol code over $\mathbb{F}_q$ with $b = 3, d_3 = 6$ or $b = 4, d_4 = 8$ exists for any length n, $n \geq 2b$. Thus, in some sense, some of the families above completely determine the existence of linear MDS b-symbol codes over finite fields for certain parameters.

The families (5) and (6) are presented mainly to support the conjectures. The family (5) indicates that $q \geq b-1$ is not an essential condition in the family (4) and the family (6) shows the existence of MDS b-symbol codes with length $\frac{q^{b+1}-1}{q-1}$. We also show that a linear MDS $(n, d_b)_q$ b-symbol code with $d_b < n$ is also an MDS $(n, d_b+1)_q$ $(b+1)$-symbol code (Theorem 2.5). Therefore, we can derive new MDS b-symbol codes from each family above.

This paper is organized as follows. In Section 2, we introduce basic notations and definitions and establish a Singleton-type bound for b-symbol codes. In Section 3, we construct MDS b-symbol codes from projective geometry. And in Section 4, we give a construction of MDS b-symbol codes from constacyclic codes. Section 5 concludes the paper.

2. Preliminaries

Let Σ be the alphabet consisting of q elements, each element of which is called a symbol. Let b be an integer and $b \geq 1$. For a vector $\mathbf{x} = (x_0, x_1, \cdots, x_{n-1})$ in Σ^n, we define the b-symbol read vector of $\mathbf{x}$ as

$$\pi_b(\mathbf{x}) = ((x_0, \cdots, x_{b-1}), (x_1, \cdots, x_b), \cdots, (x_{n-1}, x_0, \cdots, x_{b-2})) \in (\Sigma^b)^n.$$

Throughout this paper, let q be a prime power and $\mathbb{F}_q$ be the finite field containing q elements. We will focus on vectors over $\mathbb{F}_q$, so $\Sigma = \mathbb{F}_q$. For two vectors $\mathbf{x}$, $\mathbf{y}$ in $\mathbb{F}_q^n$, we have

$$\pi_b(\mathbf{x} + \mathbf{y}) = \pi_b(\mathbf{x}) + \pi_b(\mathbf{y}),$$

and the b-distance between $\mathbf{x}$ and $\mathbf{y}$ is defined as

$$D_b(\mathbf{x}, \mathbf{y}) := |\{0 \leq i \leq n-1 : (x_i, \cdots, x_{i+b-1}) \neq (y_i, \cdots, y_{i+b-1})\}|,$$

where the subscripts are reduced modulo n. Accordingly, the b-weight of $\mathbf{x} \in \mathbb{F}_q^n$ is defined as

$$wt_b(\mathbf{x}) := |\{0 \le i \le n-1 : (x_i, \cdots, x_{i+b-1}) \neq \mathbf{0}\}|,$$

where the subscripts are reduced modulo n and $\mathbf{0}$ denotes the all-zeros vector. The Hamming distance between two vectors $\mathbf{x}$ and $\mathbf{y}$ is denoted by $d_H(\mathbf{x}, \mathbf{y})$. Similarly, the Hamming weight of a vector $\mathbf{x}$ is denoted by $wt_H(\mathbf{x})$. We have the following connection between the b-distance and the b-weight.

Proposition 2.1. *For all* $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$, $D_b(\mathbf{x}, \mathbf{y}) = wt_b(\mathbf{x} - \mathbf{y})$.

Proof. Note that for $\mathbf{x}$, $\mathbf{y}$ in $\mathbb{F}_q^n$, we have $D_b(\mathbf{x}, \mathbf{y}) = d_H(\pi_b(\mathbf{x}), \pi_b(\mathbf{y})) = wt_H(\pi_b(\mathbf{x}) - \pi_b(\mathbf{y})) = wt_H(\pi_b(\mathbf{x} - \mathbf{y})) = wt_b(\mathbf{x} - \mathbf{y})$. □

Meanwhile, the connection between the Hamming weight and the b-weight was proven in [10] for vectors over the alphabet $\{0, 1\}$. Since the proof also works for vectors over $\mathbb{F}_q$, we present the following proposition directly.

Proposition 2.2. *Let* $\mathbf{x} \in \mathbb{F}_q^n$ *be such that* $0 < wt_H(\mathbf{x}) \le n - (b-1)$. *Then,*

$$wt_H(\mathbf{x}) + b - 1 \le wt_b(\mathbf{x}) \le b \cdot wt_H(\mathbf{x}).$$

Considering the b-weight and $(b+1)$-weight of a nonzero vector in $\mathbb{F}_q^n$, we have the following proposition holds.

Proposition 2.3. *For any nonzero vector* $\mathbf{x} = (x_0, x_1, \cdots, x_{n-1})$ *in* $\mathbb{F}_q^n$ *and* $wt_b(\mathbf{x}) < n$, *we have* $wt_{b+1}(\mathbf{x}) \ge wt_b(\mathbf{x}) + 1$.

Proof. It is obvious that $wt_{b+1}(\mathbf{x}) \ge wt_b(\mathbf{x})$, since if $(x_i, \cdots, x_{i+b-1}) \neq \mathbf{0}$ then $(x_i, \cdots, x_{i+b-1}, x_{i+b}) \neq \mathbf{0}$, where the subscripts are reduced modulo n, for all $0 \le i \le n-1$. We also have $(x_j, \cdots, x_{j+b-1}) = \mathbf{0}$ and $x_{j+b} \neq 0$ for some $0 \le j \le n-1$ since $wt_b(\mathbf{x}) < n$. It follows that $(x_j, \cdots, x_{j+b-1}, x_{j+b}) \neq \mathbf{0}$, and thus $wt_{b+1}(\mathbf{x}) \ge wt_b(\mathbf{x}) + 1$. □

As an example, the Hamming weight of the four vectors $v_1 = 1110000, v_2 = 1100001, v_3 = 1101000$, $v_4 = 1010100$ are all 3 while their 3-weights equal $5, 5, 6, 7$ respectively and their 4-weights equal $6, 6, 7, 7$ respectively. An obvious observation is that when the nonzero elements of a vector become closer, the b-weight tends to be smaller. And for vectors with fixed Hamming weight, one has the smallest b-weight when all the nonzero elements are in cyclically consecutive positions.

A code $\mathcal{C}$ over $\mathbb{F}_q$ of length n is a nonempty subset of $\mathbb{F}_q^n$ and the elements of $\mathcal{C}$ are called codewords. The minimum b-distance of $\mathcal{C}$ is defined as

$$d_b = \min\{D_b(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in \mathcal{C}, \mathbf{x} \neq \mathbf{y}\},$$

and the size of $\mathcal{C}$ is the number of codewords it contains. In general, a code $\mathcal{C}$ over $\mathbb{F}_q$ of length n, size M and minimum b-distance d_b is called an $(n, M, d_b)_q$ b-symbol code.

Note that the case $b = 1$ is just the conventional codes that are widely studied. And the case $b = 2$ corresponds to symbol-pair codes. Besides, if $\mathcal{C}$ is a subspace of $\mathbb{F}_q^n$, then $\mathcal{C}$ is called a linear b-symbol code. In this paper, we focus on linear b-symbol codes ($b > 2$) over $\mathbb{F}_q$.

Theorem 2.4 *(Singleton bound). Let $q \geq 2$ and $b \leq d_b \leq n$. If $\mathcal{C}$ is an $(n, M, d_b)_q$ b-symbol code, then we have $M \leq q^{n-d_b+b}$.*

Proof. Suppose that $\mathcal{C}$ is an $(n, M, d_b)_q$ b-symbol code with $q \geq 2$ and $b \leq d_b \leq n$. Delete the last $d_b - b$ coordinates from all the codewords in $\mathcal{C}$. Note that any $d_b - b$ consecutive coordinates contribute at most $d_b - 1$ to the b-distance; thus the resulting vectors of length $n - d_b + b$ are still distinct since $\mathcal{C}$ has b-distance d_b. The conclusion follows from the fact that the maximum number of distinct vectors of length $n - d_b + b$ over $\mathbb{F}_q$ is q^{n-d_b+b}. □

An $(n, M, d_b)_q$ b-symbol code $\mathcal{C}$ with $M = q^{n-d_b+b}$ is called a maximum distance separable (MDS) $(n, d_b)_q$ b-symbol code.

Theorem 2.5. *A linear MDS $(n, d_b)_q$ b-symbol code $\mathcal{C}$ with $d_b < n$ is also an MDS $(n, d_b + 1)_q$ $(b + 1)$-symbol code.*

Proof. From Propositions 2.1 and 2.3, we always have $d_{b+1} \geq d_b + 1$, and thus $|\mathcal{C}| = q^{n-d_b+b} \geq q^{n-d_{b+1}+b+1}$. The proof is completed. □

This theorem is simple but useful. One can derive new families of MDS b-symbol codes from each family in this paper and in [1–7,9,10] and the references therein.

Now, we are ready to give a sufficient condition for the existence of MDS b-symbol codes.

Theorem 2.6. *There exists a linear MDS $(n, d + 2b - 2)_q$ b-symbol code $\mathcal{C}$ if there exists a matrix with $d + b - 2$ rows and $n \geq d + 2b - 2 \geq 2b$ columns over $\mathbb{F}_q$, denoted by $H = [H_0, H_1, \cdots, H_{n-1}]$, where H_i $(0 \leq i \leq n - 1)$ is the i-th column of H, satisfying:*

1. *any $d - 1$ columns of H are linearly independent;*
2. *there exist d linearly dependent columns;*
3. *any $d + b - 2$ cyclically consecutive columns are linearly independent, i.e., H_i, $H_{i+1}, \cdots, H_{i+d+b-3}$ are linearly independent for $0 \leq i \leq n - 1$, where the subscripts are reduced modulo n.*

Proof. Let $\mathcal{C}$ be the linear code with parity check matrix H. Then the first two conditions indicate that $\mathcal{C}$ is an $[n, n - d - b + 2, d]_q$ linear code with size $q^{n-d-b+2}$. For a nonzero

codeword $c = (c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}$, if there exists j such that $c_j = c_{j+1} = \cdots = c_{j+b-2} = 0$ and $c_{j+b-1} \neq 0$, where the subscripts are reduced modulo n, then one can consider the vector $v = (c_{j+b-1}, \cdots, c_{n-1}, c_0, \cdots, c_{j+b-2})$. Rewrite v as $v = (v_0, v_1, \cdots, v_t, 0, \cdots, 0)$ for some $t \leq n-b$, where $v_0, v_t \neq 0$. We also have $t \geq d+b-2$, since any $d+b-2$ cyclically consecutive columns are linearly independent. Moreover, there are at least d nonzero elements in the set $\{v_0, v_1, \cdots, v_t\}$. It is easy to see $wt_b(c) = wt_b(v) \geq d+2b-2$. If there does not exist j such that $c_j = c_{j+1} = \cdots = c_{j+b-2} = 0$ and $c_{j+b-1} \neq 0$, then it is easy to see that $wt_b(c) = n$. Hence $d_b \geq d+2b-2$. □

3. MDS b-symbol codes from projective geometry

Let $V(r+1, q)$ be a vector space of rank $r+1$ over $\mathbb{F}_q$. The projective r-space over $\mathbb{F}_q$, denoted by $PG(r, q)$, is the geometry whose points, lines, planes, $\cdots$, hyperplanes are the subspaces of $V(r+1, q)$ of rank $1, 2, 3, \cdots, r$, respectively. The dimension of a subspace of $PG(r, q)$ is one less than the rank of a subspace of $V(r+1, q)$. We refer to [8] for more information on projective geometry.

Label the point of $PG(r, q)$ as $\langle (a_0, a_1, \cdots, a_r) \rangle$, the subspace spanned by a nonzero vector $(a_0, a_1, \cdots, a_r)$, where $a_i \in \mathbb{F}_q$ for $0 \leq i \leq r$. Since these coordinates are defined only up to multiplication by a nonzero scalar $\lambda \in \mathbb{F}_q$ (here $\langle (\lambda a_0, \lambda a_1, \cdots, \lambda a_r) \rangle = \langle (a_0, a_1, \cdots, a_r) \rangle$), we refer to $a_0, a_1, \cdots, a_r$ as homogeneous coordinates. Thus, the number of points in $PG(r, q)$ is given by $\frac{q^{r+1}-1}{q-1}$.

Lemma 3.1. *There exist $q+1$ hyperplanes in $PG(r, q)$ covering all the points in $PG(r, q)$ and intersecting in a projective $(r-2)$-space.*

Proof. Fix a projective $(r-2)$-space U in $PG(r, q)$. Choose an arbitrary point P_0 in $PG(r, q) \setminus U$, then P_0 and U generate a hyperplane V_0. Next, choose a point P_1 in $PG(r, q) \setminus V_0$, then P_1 and U form another hyperplane V_1. Repeat the procedure until all the points are covered. We obtain $q+1$ hyperplanes $V_0, \cdots, V_q$, which intersect in U. □

In Theorem 2.6, if we fix $d = 3$, choose n points in $PG(b, q)$, $b \geq 2$, and regard them as column vectors of the matrix H, then we have the following lemma.

Lemma 3.2. *There exists a linear MDS $(n, 2b+1)_q$ b-symbol code $\mathcal{C}$ if there exists a set $\mathcal{S}$ of $n \geq 2b+1$ points of $PG(b, q)$ satisfying the following conditions:*

1. *there exist 3 points in $\mathcal{S}$ lying on a line;*
2. *if the n points are ordered, say $P_0, P_1, \cdots, P_{n-1}$, then any $b+1$ cyclically consecutive points, i.e., $P_i, P_{i+1}, \cdots, P_{i+b}$, where the subscripts are reduced modulo n, do not lie in a projective $(b-1)$-space for $0 \leq i \leq n-1$.*

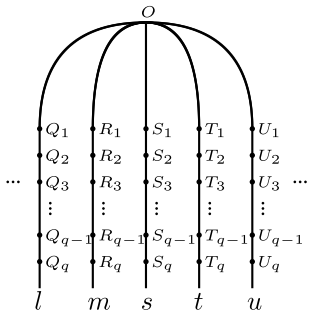

Fig. 1. The structure of $PG(2, q)$.

Note that the first condition in Lemma 3.2 can be easily satisfied; thus we focus on ordering points in $PG(b, q)$ such that any $b + 1$ cyclically consecutive points do not lie in a projective $(b - 1)$-space.

Since a nonzero element in a codeword can contribute at most b to the b-weight, a b-symbol code whose minimum b-distance equals $2b+1$ must have the minimum Hamming distance being equal to or greater than 3. In other words, the parity-check matrix of any linear MDS $(n, 2b + 1)_q$ b-symbol code should be of size $(b + 1) \times n$ and has no two linearly dependent columns. Thus linear MDS $(n, 2b + 1)_q$ b-symbol codes exist only when $n \leq \frac{q^{b+1}-1}{q-1}$.

Lemma 3.3. *A linear MDS $(n, 2b + 1)_q$ b-symbol code over $\mathbb{F}_q$ exists only when $2b + 1 \leq n \leq \frac{q^{b+1}-1}{q-1}$.*

3.1. $b = 2$

A projective plane $PG(2, q)$ is an incidence system of points and lines such that

- For any two distinct points, there is exactly one line through both.
- Any two distinct lines meet in exactly one point.
- There exist four points such that no three are collinear.

From Lemma 3.1 we know that all the points in $PG(2, q)$ lie on $q + 1$ lines, all of which intersect in a point, just as shown in Fig. 1.

Lemma 3.4. *There exist n ordered points in $PG(2, q)$ such that no three cyclically consecutive points are collinear for $q \geq 3$ being a prime power and $3 \leq n \leq q^2 + q + 1$.*

Proof. Let the notations be as in Fig. 1. There are many approaches to attain this goal and we give one of the strategies as follows.

- The case when q is odd.

In this case, through O we have an even number of lines. Choose O to be the first point, and then choose arbitrary points from lines l and m in turn. Suppose we have ordered the points as $O, Q_1, R_1, Q_2, R_2, \cdots, Q_q, R_q$. Next we choose a point S_1 not on the line Q_qR_q to be the next, and then a point T_1 not on the line R_qS_1. After that, choose points from lines s and t in turn. We can keep doing this until we have covered n $(3 \leq n \leq q^2 + q + 1)$ points.

Note that we have ordered n points in $PG(2, q)$ and it is easy to check that no three consecutive points are collinear. Denote the last three points as $P_{n-3}, P_{n-2}, P_{n-1}$. We further need to make sure that P_{n-2}, P_{n-1}, O are not collinear, neither are P_{n-1}, O, Q_1. Since P_{n-1} is always not lying on the line OP_{n-2}, we have P_{n-2}, P_{n-1}, O are not collinear. Points P_{n-1}, O, Q_1 may be collinear when P_{n-1} lies on the line l, i.e., $4 \leq n \leq 2q$ and n is even. If this happens we choose another point not lying on lines l, m and $P_{n-3}P_{n-2}$ to be the new last point, which can always succeed.

- The case when q is even.

This case is different from the case when q is odd since there are an odd number of lines through O. For $n \leq q^2 + 1$, we can choose an even number of lines and order the points on them just as we do in the case when q is odd. For $n > q^2 + 1$, we first put the points on the lines l, m, s in order and then we can just proceed as in the case when q is odd. Similarly we choose O to be the first point, and then choose points from lines l, m, s in turn, making sure that no three consecutive points are collinear. Since two lines meet in exactly one point, we can always do this until there is only one point left on each line. Suppose we have ordered the points as $O, Q_1, R_1, S_1, Q_2, \cdots, Q_{q-1}, R_{q-1}, S_{q-1}$. Choose R_q, S_q to be the next two points, after that, choose a point T_1 not on lines R_qS_q and Q_qS_q to be the next. Let the point Q_q be the next, and then choose a point U_1 not on Q_qT_1, a point T_2 not on Q_qU_1. So far, we have ordered the points as $O, Q_1, R_1, S_1, \cdots, Q_{q-1}, R_{q-1}, S_{q-1}R_q, S_q, T_1, Q_q, U_1, T_2$ and no three consecutive points are collinear. There are an even number of lines left and we can then simply proceed as in the case when q is odd. □

Note that in the lemma above, we exclude the case $q = 2$. We show this in the following example.

Example 3.5. We can order $3 \leq n \leq 7$ points in $PG(2, 2)$ such that any 3 cyclically consecutive points are not collinear as shown in Table 1, where the column vectors of H denote the points.

Remark 3.1. We have ordered n points in $PG(2, q)$ for q being a prime power and $3 \leq n \leq q^2 + q + 1$. Actually, we can obtain linear MDS $(n, 5)_q$ 2-symbol codes (symbol-pair

Table 1
Ordered points in $PG(2,2)$.

n	H
3	$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$
4	$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$
5	$\begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$
6	$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$
7	$\begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$

codes) for q being a prime power with length n ranging from 5 to q^2+q+1 according to Lemma 3.2. Codes with the same parameters were constructed in our former work [5] by a method based on linear algebra. Besides providing a new proof of the result, the discussion in Lemma 3.4 is also essential in the proof of Lemma 3.9. Compared to the results in [3] and [6], our codes have a much larger range of parameters and cover the results in [3] and [6] for $b=2$, $d_2=5$. Thus, one can also see the advantage of our method from this.

3.2. $b=3, d_3=7$

First, we collect some axioms for projective 3-space, in which the objects (points, lines and planes) and the incidence relations are given:

- Any two distinct points are incident with exactly one line.
- Any two distinct planes meet in exactly one line.
- Given any plane π and any line l not on π, there exists a unique point incident with both.
- Every plane incident with a given line l is also incident with every point on l.
- Any two distinct lines meet in a point, if and only if they lie on a common plane.
- There exists a set of five points, of which no four lie on a common plane.

From Lemma 3.1 we know that all the points in $PG(3,q)$ lie on $q+1$ planes, all of which intersect in a line, just as shown in Fig. 2. For example, lines $l, l_1, \cdots, l_q$ form a plane, lines $l, m_1, \cdots, m_q$ form another and the two planes share a common line l.

Lemma 3.6. *There exist n ordered points in $PG(3,q)$ such that no four cyclically consecutive points lie on a plane for $q \geq 3$ being a prime power and $4 \leq n \leq q^3+q^2+q+1$.*

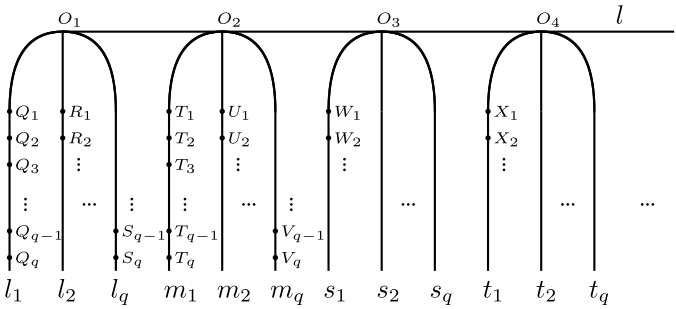

Fig. 2. The structure of $PG(3, q)$.

Proof. Fix a line l and denote the $q+1$ planes intersecting in l as $\pi_0, \cdots, \pi_q$. In Fig. 2 we present four of them, and denote the plane corresponding to lines $l, l_1, l_2, \cdots, l_q$ as π_0, and the next three planes as π_1, π_2, π_3. We give one of the strategies as follows.

- The case when q is odd.

In this case, we have an even number of planes $\pi_0, \cdots, \pi_q$ sharing the line l. Choose O_1, O_2 to be the first two points and then choose arbitrary points from lines l_1,m_1 in turn. Suppose we have ordered the points as $O_1, O_2, Q_1, T_1, Q_2, \cdots, T_{q-1}, Q_q, T_q$. It is obvious that O_1, O_2, Q_1, T_1 do not lie on a plane, neither do O_2, Q_1, T_1, Q_2. For any other four consecutive points, we must have two of the points lying on l_1 and two on m_1. If they lie on a plane then the lines l_1 and m_1 must intersect. Suppose they meet in a point O', then O' lies on both π_0 and π_1, and thus on l, a contradiction. Therefore, any four consecutive points do not lie on a plane.

Next, we choose a point R_1 not on the plane $Q_qT_{q-1}T_q$, a point U_1 not on the plane $Q_qT_qR_1$, and a point R_2 not on the plane $T_qR_1U_1$. Then choose points from l_2, m_2 in turn and we can proceed as above until all the points on lines $l_1, \cdots, l_q, m_1, \cdots, m_q$ are covered.

Suppose we have ordered the points as $O_1, O_2, Q_1, T_1, \cdots, S_{q-1}, V_{q-1}, S_q, V_q$. Then we choose the following points to be $O_3, O_4, W_1, X_1, W_2, X_2$, where W_1, W_2 are arbitrary points on s_1 and X_1, X_2 are arbitrary points on t_1. It is easy to check that any four consecutive points are not on a plane. Repeat the procedure until we have covered n $(4 \leq n \leq q^3 + q^2 + q + 1)$ points in $PG(3, q)$.

Note that we have ordered n points in $PG(3, q)$ and no four consecutive points lie on a plane. Denote the last four points as $P_{n-4}, P_{n-3}, P_{n-2}$ and P_{n-1}, we further need to make sure:

(1) P_{n-1}, O_1, O_2, Q_1 do not lie on a plane.
This fails only when P_{n-1} lies on π_0, i.e., $5 \leq n \leq 2q^2 + 1$ and n is odd. In this case, we choose a point not lying on planes π_0, π_1, $P_{n-4}P_{n-3}P_{n-2}$ and $P_{n-3}P_{n-2}O_1$ to be the new last point P_{n-1}.

(2) $P_{n-2}, P_{n-1}, O_1, O_2$ do not lie on a plane.
This is always true in our construction, since P_{n-2}, P_{n-1} are always on different π_is.
(3) $P_{n-3}, P_{n-2}, P_{n-1}, O_1$ do not lie on a plane.
If P_{n-3}, P_{n-1} lie on a line l_i, $1 \leq i \leq q$, then we can fix this as we do in case (1). Otherwise, $P_{n-3}, P_{n-2}, P_{n-1}, O_1$ may lie on a plane only if they are chosen from different lines. For example, T_q, R_1, U_1 are chosen from lines m_1, l_2, m_2 respectively. In this case, we can always find a new suitable point P_{n-1} since there are enough points remaining.

- The case when q is even.

This case is different from the case when q is odd since there are an odd number of planes. For $n \leq q^3 + q$, we can choose an even number of planes and proceed just as in the case when q is odd. For $n > q^3 + q$, we first order the points on the lines $l_1, \cdots, l_q, m_1, \cdots, m_q, s_1, \cdots, s_q$ and then proceed as in the case when q is odd. Note that there are $3q$ lines, an even number; thus we can still consider the lines from different π_is in pairs, $i = 0, 1, 2$, and order the points as in the case when q is odd. There are an even number of planes remaining. After a similar discussion, we can order n points such that no four cyclically consecutive points are on a plane for $4 \leq n \leq q^3 + q^2 + q + 1$. □

Example 3.7. We can also order $4 \leq n \leq 15$ points in $PG(3, 2)$ such that any 4 cyclically consecutive points do not lie on a plane as shown in Table 2, where the first n columns of H denote the ordered n points.

Combining Lemmas 3.2, 3.6 and Example 3.7, we have the following theorem.

Theorem 3.8. *There exists a linear MDS* $(n, 7)_q$ 3*-symbol code for* q *being a prime power with length* n *ranging from* 7 *to* $q^3 + q^2 + q + 1$.

3.3. $b = 4, d_4 = 9$

From Lemma 3.1 we know that all the points in $PG(4, q)$ lie in $(q + 1)$ projective 3-spaces, all of which intersect in a plane, just as shown in Fig. 3. Lines $l_0, l_1, \cdots, l_q$ intersect in a point O and form a plane π. Similarly, the sets of lines $\{l_0, m_{11}, m_{12}, \cdots, m_{1q}\}$, $\{l_0, m_{21}, m_{22}, \cdots, m_{2q}\}, \cdots, \{l_0, m_{q1}, m_{q2}, \cdots, m_{qq}\}$ form planes $\pi_{01}, \pi_{02}, \cdots, \pi_{0q}$ respectively. Planes $\pi, \pi_{01}, \cdots, \pi_{0q}$ intersect in the line l_0 and they together form the projective 3-space V_0. In total, we have $q+1$ such projective 3-spaces, denoted as $V_0, V_1, \cdots, V_q$, all of which form the projective space $PG(4, q)$ and intersect in the plane π.

Note that in $PG(2, q)$ we order points such that no three cyclically consecutive points are collinear. To attain this goal, we choose points from different lines by an interleaving technique. After that, in $PG(3, q)$, we order points such that no four cyclically consecutive points lie on a plane by choosing points from pairs of skew lines (lines that do not

Table 2
Ordered points in $PG(3,2)$.

n	H
5	$\begin{pmatrix} 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}$
7	$\begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$
8	$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$
10	$\begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$
13	$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$
4, 6, 9, 11, 12, 14, 15	$\begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$

intersect) alternatively and using the axiom that two lines on a projective plane must intersect.

Ordering points in $PG(4,q)$ such that no five cyclically consecutive points are in a projective 3-space is more complicated. We only show the main idea in the proof of the following lemma.

Lemma 3.9. *There exist n ordered points in $PG(4,q)$ such that no five cyclically consecutive points are in a projective 3-space for $q \geq 3$ being a prime power and $5 \leq n \leq q^4+q^3+q^2+q+1$.*

Proof. Let the structure of $PG(4,q)$ be as shown in Fig. 3 and the notations be defined as above. Note that there are $q+1$ planes (including π) sharing a common line in each projective 3-space V_i, $0 \leq i \leq q$. Set aside the plane π and denote the remaining q planes in V_i as $\pi_{i1}, \cdots, \pi_{iq}$. Let O be the first point. For two lines on the same plane π_{ij}, for example m_{11} and m_{12}, if we connect the point O to every point of m_{11} then we get $q+1$ lines, each of which intersects m_{12} in exactly one point. Thus, we can build a one-to-one correspondence between the points on every two lines on the same plane π_{ij}. Consider the points lying on the lines in $\pi_{ij} \setminus l_i$, for example, points on $m_{11}, \cdots, m_{1q}$ when $i=0, j=1$. We can easily order all the points such that no three consecutive points are collinear and no two consecutive points are collinear with O for $q \geq 3$ after a similar discussion as in Lemma 3.4.

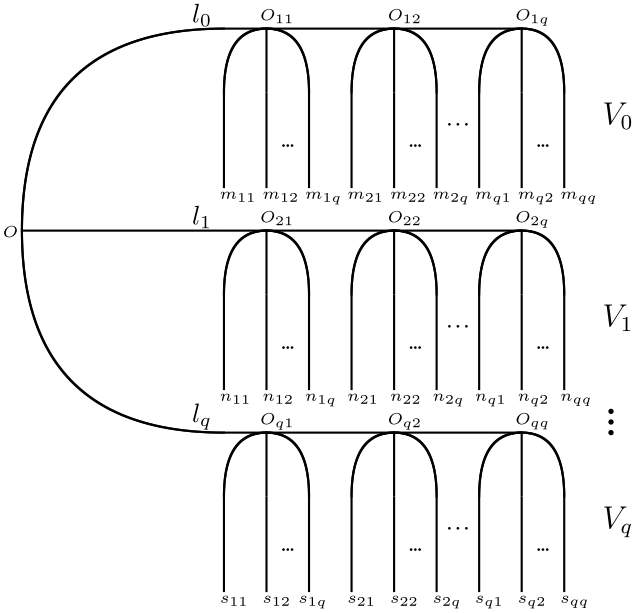

Fig. 3. The structure of $PG(4, q)$.

Choose two planes $\pi_{ij}, \pi_{st}, i \neq s$ and suppose we have ordered the points corresponding to the two planes as $P_0, \cdots, P_{q^2}$ and $Q_0, \cdots, Q_{q^2}$. We then order the points alternately as $P_0, Q_0, P_1, Q_1, \cdots, P_{q^2}, Q_{q^2}$. Note that if we choose any five consecutive points, then three of them form the plane π_{ij} or π_{st} and the other two points form a line not through O. Thus they are not in a projective 3-space, since in a projective 3-space, every plane incident with a given line is also incident with every point on the line, and a line not on a plane must meet the plane in a point.

The number of such planes π_{ij} is $q(q+1)$, an even number. Thus we can always consider planes from different V_is in pairs, $0 \leq i \leq q$. Similar to Lemma 3.4 and Lemma 3.6, we can repeat the procedure above until we have put n $(5 \leq n \leq q^4 + q^3 + q^2 + q + 1)$ points in order and make sure that no five cyclically consecutive points lie in a projective 3-space. We omit the tedious details here since the argument is analogous. □

Combining Lemma 3.2 and Lemma 3.9, we have the following theorem.

Theorem 3.10. *There exists a linear MDS* $(n, 9)_q$ *4-symbol code for* $q \geq 3$ *being a prime power with length* n *ranging from* 9 *to* $q^4 + q^3 + q^2 + q + 1$.

3.4. More constructions

We first show the existence of MDS b-symbol codes for general $b \geq 5$ in the following theorem, which works quite well when q is sufficiently larger than b.

Theorem 3.11. *There exists a linear MDS $(n, 2b+1)_q$ b-symbol code for q being a prime power, $q \geq b \geq 5$, with length n ranging from $2b+1$ to $q^b - bq^{b-1} + \frac{b^2+3b}{2}$.*

Proof. From Lemma 3.2, we mainly need to order n points in $PG(b,q)$ such that any $b+1$ cyclically consecutive points do not lie in a projective $(b-1)$-space. We prove this theorem by induction. In $PG(b,q)$, we can easily find $b+1$ points that generate the whole space. Suppose we already have k ordered points, $b+1 \leq k < q^b - bq^{b-1} + 2b$, denoted as $P_1, P_2, \cdots, P_k$, such that any $b+1$ cyclically consecutive points do not lie in a projective $(b-1)$-space.

Consider the $b+1$ projective $(b-1)$-spaces $V_0, V_1, \cdots, V_b$ generated by $\{P_{k-b+1}, P_{k-b+2}, \cdots, P_k\}$, $\{P_{k-b+2}, P_{k-b+3}, \cdots, P_k, P_1\}$, $\cdots$, $\{P_1, P_2, \cdots, P_b\}$ respectively. We can always find a new suitable point P_{k+1} if the remaining points, i.e., points in $PG(b,q) \setminus \{P_1, P_2, \cdots, P_k\}$, are not all covered by the projective spaces $V_0, V_1, \cdots, V_b$.

We determine the largest number of the remaining points covered by the $b+1$ spaces above. Two projective $(b-1)$-spaces in $PG(b,q)$ must intersect in a projective $(b-2)$-space. Thus V_0 covers $\frac{q^b-1}{q-1}$ points and any other V_i covers at most $\frac{q^b-1}{q-1} - \frac{q^{b-1}-1}{q-1}$ new points for $1 \leq i \leq q$. However, we should exclude the points $P_{k-b+1}, P_{k-b+2}, \cdots, P_k, P_1, \cdots, P_b$ when we count for each space. For example, we should exclude points $P_{k-b+1}, P_{k-b+2}, \cdots, P_k$ when counting the points for V_0. And we exclude only one point P_1 when counting for V_1 since points $P_{k-b+2}, \cdots, P_k$ are in the intersection of V_0 and V_1. Note that some of the $2b$ points $P_{k-b+1}, P_{k-b+2}, \cdots, P_k, P_1, \cdots, P_b$ may be the same when $k < 2b$. And the total number of points we should exclude takes the minimum value $2b$ when $k = b+1$. Therefore, the $b+1$ projective spaces $V_0, V_1, \cdots, V_b$ can cover in total at most $(b+1)\frac{q^b-1}{q-1} - b\frac{q^{b-1}-1}{q-1} - 2b$ points in $PG(b,q) \setminus \{P_1, P_2, \cdots, P_k\}$. Therefore we can always find a new suitable point P_{k+1} when $k < q^b - bq^{b-1} + 2b$.

Since $q \geq b$, from the conclusion above, we can always order $2b$ points such that any $b+1$ cyclically consecutive points do not lie in a projective $(b-1)$-space. Suppose we have ordered at least $2b$ points, i.e., $k \geq 2b$. In this case, no two of the $2b$ points $P_{k-b+1}, P_{k-b+2}, \cdots, P_k, P_1, \cdots, P_b$ are the same and the largest number of points in $PG(b,q) \setminus \{P_1, P_2, \cdots, P_k\}$ covered by the $b+1$ projective $(b-1)$-spaces becomes $(b+1)\frac{q^b-1}{q-1} - b\frac{q^{b-1}-1}{q-1} - \frac{b^2+3b}{2}$. The conclusion follows. □

According to Theorem 2.6, if we let $d = 2$ and regard the columns of H as vectors in $V(b,q)$, then we have the following lemma.

Lemma 3.12. *There exists a linear MDS $(n, 2b)_q$ b-symbol code $\mathcal{C}$ if there exists a set $\mathcal{S}$ of $n \geq 2b$ vectors of $V(b,q)$ satisfying:*

1. *there exist 2 linearly dependent vectors;*
2. *any b cyclically consecutive vectors are linearly independent.*

Similar to Theorem 3.11, we can derive the following theorem.

Theorem 3.13. *There exists a linear MDS* $(n, 2b)_q$ *b-symbol code with* $n \geq 2b$ *for* $q \geq b-1$ *being a prime power,* $b \geq 3$ *or* $q = 2, b = 4$.

Proof. In a b-dimensional vector space $V(b, q)$, we can easily find b vectors that generate the whole space. Suppose we already have $k \geq b$ ordered vectors, denoted as $v_1, v_2, \cdots, v_k$, such that any b cyclically consecutive vectors are linearly independent.

First, we consider the $(b-1)$-dimensional vector spaces $V_1, V_2, \cdots, V_b$ generated by $\{v_{k-b+2}, v_{k-b+3}, \cdots, v_k\}, \{v_{k-b+3}, v_{k-b+4}, \cdots, v_k, v_1\}, \cdots, \{v_1, v_2, \cdots, v_{b-1}\}$ respectively. Two $(b-1)$-dimensional vector spaces in $V(b, q)$ must intersect in a $(b-2)$-dimensional vector space. Next we determine the largest number of nonzero vectors covered by the spaces above. V_1 covers $q^{b-1} - 1$ nonzero vectors and any other V_i covers at most $q^{b-1} - q^{b-2}$ new nonzero vectors for $2 \leq i \leq b$. Besides, we should exclude the vectors $v_{k-b+2}, \cdots, v_k, \cdots, v_1, v_{b-1}$ when we count for each vector space. Thus they can totally cover at most $bq^{b-1} - (b-1)q^{b-2} - 2(b-1) - 1$ nonzero vectors. We can always find a new suitable vector v_{k+1} unless all the nonzero vectors are covered by the b vector spaces. In other words, we can always find a new suitable vector if $q^b - bq^{b-1} + (b-1)q^{b-2} + 2(b-1) \geq 1$, which turns out to be $q \geq b-1$ or $q = 2, b = 4$. □

Remark 3.2. The authors in [10] also constructed b-symbol codes with $d_b = 2b$ by the interleaving technique. The lengths are limited to be multiples of b while our codes do not have this limitation. However, for the binary case, their result gives MDS b-symbol codes that are not contained in our theorem.

In the previous subsections we have given strategies to order n vectors in the projective space $PG(b, q)$ such that any $b+1$ cyclically consecutive vectors are linearly independent for $b = 2, 3, 4$ and $2b + 1 \leq n \leq \frac{q^{b+1}-1}{q-1}$. The following result shows that $q \geq b - 1$ is not an essential condition in Theorem 3.13 if we order the vectors carefully.

Theorem 3.14. *There exists a linear MDS* $(n, 10)_q$ 5*-symbol code for* $q \geq 3$ *being a prime power and* $n \geq 10$.

Proof. For $n \geq 10$, we can find integers $n_1, n_2, \cdots, n_t$ such that $n = n_1 + n_2 + \cdots + n_t$, where $t \geq 2$ and $5 \leq n_i \leq \frac{q^5-1}{q-1}$. From the conclusion in Subsection 3.3, we can find t sequences of ordered points in $PG(4, q)$, denoted as $S_1, S_2, \cdots, S_t$, each of which has n_i points and any 5 cyclically consecutive points are linearly independent. Let the first 4 points of the t sequences be the same, which can be easily satisfied. Concatenating the t sequences, we get a sequence of length n satisfying the conditions in Lemma 3.12. □

4. MDS *b*-symbol codes from constacyclic codes

For $\eta \in \mathbb{F}_q^*$, a q-ary linear code C of length n is called η-constacyclic if it is invariant under the η-constacyclic shift of $\mathbb{F}_q^n$:

$$(c_0, c_1, \cdots, c_{n-1}) \to (\eta c_{n-1}, c_0, \cdots, c_{n-2}).$$

If we identify each codeword $c = (c_0, c_1, \cdots, c_{n-1})$ with its polynomial representation $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$, then an η-constacyclic code C of length n over $\mathbb{F}_q$ is identified with an ideal of the quotient ring $\mathbb{F}_q[x]/\langle x^n - \eta\rangle$, and $xc(x)$ corresponds to an η-constacyclic shift of $c(x)$. Moreover, $\mathbb{F}_q[x]/\langle x^n - \eta\rangle$ is a principal ideal ring, and C is generated by a monic divisor $g(x)$ of $x^n - \eta$. In this case, $g(x)$ is called the generating polynomial of C and we write $C = \langle g(x)\rangle$.

Let $\eta \in \mathbb{F}_q$ be a primitive r-th root of unity. Since $\gcd(n, q) = 1$, there exists a primitive (rn)-th root of unity ω in some extension field of $\mathbb{F}_q$ such that $\omega^n = \eta$. It can be verified that

$$x^n - \eta = \prod_{i=0}^{n-1}(x - \omega^{1+ir}).$$

Let $\Omega = \{1+ir | 0 \le i \le n-1\}$. For each $j \in \Omega$, let C_j be the q-cyclotomic coset modulo rn containing j. Let C be an η-constacyclic code of length n over $\mathbb{F}_q$ with generating polynomial $g(x)$. Then the set $Z = \{j \in \Omega | g(\omega^j) = 0\}$ is called the defining set of C. We can see that the defining set of C is a union of some q-cyclotomic cosets modulo rn and $\dim(C) = n - |Z|$.

Similar to cyclic codes, there exists the following BCH bound for constacyclic codes.

Theorem 4.1 *([6] The BCH bound for constacyclic codes). Let C be an η-constacyclic code of length n over $\mathbb{F}_q$, where η is a primitive r-th root of unity. Let ω be a primitive (rn)-th root of unity in an extension field of $\mathbb{F}_q$ such that $\omega^n = \eta$. Assume the generating polynomial of C has roots that include the set $\{\omega^{1+ri} | i_1 \le i \le i_1 + d - 2\}$. Then the minimum Hamming distance of C is at least d.*

Unlike all the other constructions described in this paper, which provide a large range of lengths, the following result only focuses on the case when $n = \frac{q^{b+1}-1}{q-1}$. And we present this result mainly to support the first conjecture we propose.

Theorem 4.2. *There exists a linear MDS $(\frac{q^{b+1}-1}{q-1}, 2b+1)_q$ b-symbol code for any $b \ge 4$ and q being a prime power.*

Proof. Let $n = \frac{q^{b+1}-1}{q-1}$, ω be a primitive element of $\mathbb{F}_q$ and δ be a primitive element of $\mathbb{F}_{q^{b+1}}$ such that $\delta^n = \omega$. Note that $g(x) = (x-\delta)(x-\delta^q)\cdots(x-\delta^{q^b}) \in \mathbb{F}_q[x]$ divides $x^n - \omega$. Let C be the ω-constacyclic code $\langle g(x)\rangle \subseteq \mathbb{F}_q[x]/(x^n - \omega)$. Then C is an $[n, n-b-1, d]_q$ linear code with $3 \le d \le b+2$.

If $d = b+2$, then it is easy to see that $d_b \ge 2b+1$.

If $3 \le d \le b+1$, let $c(x) = \sum_{i=0}^{n-1} c_i x^i$ be a nonzero codeword of C. If there exists j such that $c_j = c_{j+1} = \cdots = c_{j+b-2} = 0, c_{j+b-1} \ne 0$, where the subscripts are reduced

modulo n, then $x^{n-j-b+1}c(x) = \sum_{i=0}^{t} a_i x^i \in C$, for some $a_i \in \mathbb{F}_q$, $t \leq n-b$ and $a_0, a_t \neq 0$. Note that $3 \leq d \leq b+1$ and $t \geq b+1$ since $g(x)|c(x)$; thus we have $wt_b(x^{n-j-b+1}c(x)) = wt_b(c(x)) \geq 2b+1$. If there does not exist j such that $c_j = c_{j+1} = \cdots = c_{j+b-2} = 0, c_{j+b-1} \neq 0$, then it is easy to see that $wt_b(c(x)) = n$. Hence $d_b \geq 2b+1$. □

5. Conclusion

In this paper, we establish a Singleton-type bound for b-symbol codes and show that any linear MDS b-symbol code with $d_b < n$ is also an MDS $(b+1)$-symbol code. We give a sufficient condition for the existence of linear MDS b-symbol codes and show that there exists a linear MDS b-symbol code once one finds a suitable matrix. And then, in specific cases, the problem turns out to be ordering points in $PG(b,q)$ such that no $b+1$ cyclically consecutive points lie in a projective $(b-1)$-space. As a result, we construct new families of linear MDS b-symbol codes with a large range of parameters and completely determine the existence of linear MDS b-symbol codes over finite fields for certain parameters.

This method is quite interesting and deserves further investigation. Consider the structure established by Lemma 3.1. Our goal is to order points in $PG(b,q)$ such that no $b+1$ cyclically consecutive points lie in a projective $(b-1)$-space. The main idea is as follows. For even b, in $PG(b,q)$, any two projective $\frac{b}{2}$-spaces in different projective $(b-1)$-spaces intersect in a point. For example, when $b=2$, any two of the $q+1$ lines meet in a point, and when $b=4$, π_{ij} and π_{st} meet in point O $(i \neq s)$. For a pair of projective $\frac{b}{2}$-spaces, we first order the points in each space separately such that any $\frac{b}{2}+1$ consecutive points generate the space (more details are omitted here), and then choose points alternatively from the pair of sequences of ordered points, just as we do in Lemma 3.4 and Lemma 3.9. For odd b, in $PG(b,q)$, any two projective $\frac{b-1}{2}$-spaces in different projective $(b-1)$-spaces have no points in common. For example, when $b=3$, in the structure established by Lemma 3.1, lines on different planes have no points in common. Similarly, for a pair of projective $\frac{b-1}{2}$-spaces, we first order the points in each space separately such that any $\frac{b-1}{2}+1$ consecutive points generate the space. Then we choose points alternatively from the pair of sequences of ordered points, just as we do in Lemma 3.6.

By the discussion above, it seems that we can give a strategy or an algorithm to order points in $PG(b,q)$ for any b by induction, and thus can construct linear MDS $(n, 2b+1)_q$ b-symbol codes for any b and $2b+1 \leq n \leq \frac{q^{b+1}-1}{q-1}$. However, we believe that such a proof will be tedious, and we prefer to present this as the following conjecture which calls for a neat and brief proof. We give more constructions in Subsection 3.4 and in Section 4 to support the conjecture.

Conjecture 1. *There exist linear MDS $(n, 2b+1)_q$ b-symbol codes for q being a prime power, $b>2$ and $2b+1 \leq n \leq \frac{q^{b+1}-1}{q-1}$.*

Following the discussions and conclusions in Subsection 3.4, we also propose the following conjecture.

Conjecture 2. *There exist linear MDS* $(n, 2b)_q$ *b-symbol codes for* q *being a prime power,* $b > 2$ *and* $n \geq 2b$.

References

[1] Y. Cassuto, M. Blaum, Codes for symbol-pair read channels, IEEE Trans. Inf. Theory 57 (12) (2011) 8011–8020.
[2] Y. Cassuto, S. Litsyn, Symbol-pair codes: algebraic constructions and asymptotic bounds, in: IEEE Int. Symp. Inf. Theory, 2011, pp. 2348–2352.
[3] Y.M. Chee, L. Ji, H.M. Kiah, C. Wang, J. Yin, Maximum distance separable codes for symbol-pair read channels, IEEE Trans. Inf. Theory 59 (11) (2013) 7259–7267.
[4] B. Chen, L. Lin, H. Liu, Constacyclic symbol-pair codes: lower bounds and optimal constructions, arXiv:1605.03460.
[5] B. Ding, G. Ge, J. Zhang, T. Zhang, Y. Zhang, New constructions of MDS symbol-pair codes, Des. Codes Cryptogr. (2017), https://doi.org/10.1007/s10623-017-0365-1.
[6] X. Kai, S. Zhu, P. Li, A construction of new MDS symbol-pair codes, IEEE Trans. Inf. Theory 61 (11) (2015) 5828–5834.
[7] S. Li, G. Ge, Constructions of maximum distance separable symbol-pair codes using cyclic and constacyclic codes, Des. Codes Cryptogr. 84 (3) (2017) 359–372.
[8] S. Payne, Topics in Finite Geometry: Ovals, Ovoids and Generalized Quadrangles, UC Denver Course Notes, 2009.
[9] E. Yaakobi, J. Bruck, P.H. Siegel, Decoding of cyclic codes over symbol-pair read channels, in: IEEE Int. Symp. Inf. Theory, 2012, pp. 2891–2895.
[10] E. Yaakobi, J. Bruck, P.H. Siegel, Constructions and decoding of cyclic codes over b-symbol read channels, IEEE Trans. Inf. Theory 62 (4) (2016) 1541–1551.