

Constructions of cyclic constant dimension codes

Bocong Chen¹, Hongwei Liu²

¹ School of Mathematics, South China University of Technology, Guangzhou, Guangdong, 510641, China

² School of Mathematics and Statistics, Central China Normal University, Wuhan, Hubei, 430079, China

Abstract

Subspace codes and particularly constant dimension codes have attracted much attention in recent years due to their applications in random network coding. As a particular subclass of subspace codes, cyclic subspace codes have additional properties that can be applied efficiently in encoding and decoding algorithms. It is desirable to find cyclic constant dimension codes such that both the code sizes and the minimum distances are as large as possible. In this paper, we explore the ideas of constructing cyclic constant dimension codes proposed in ([2], IEEE Trans. Inf. Theory, 2016) and ([17], Des. Codes Cryptogr., 2016) to obtain further results. Consequently, new code constructions are provided and several previously known results in [2] and [17] are extended.

Keywords: Cyclic subspace codes, random network coding, constant dimension codes, linearized polynomials, subspace polynomials.

2010 Mathematics Subject Classification: 11T71, 11T06.

1 Introduction

Let \mathbb{F}_q be the finite field of size q and let \mathbb{F}_{q^N} be the field extension of degree N over \mathbb{F}_q ; \mathbb{F}_{q^N} can be viewed as an N -dimensional vector space over \mathbb{F}_q . The set of all subspaces of \mathbb{F}_{q^N} , denoted by $\mathcal{P}_q(N)$, is called the *projective space* of order N over \mathbb{F}_q (see [9]). For any $U, V \in \mathcal{P}_q(N)$, the *subspace distance* between U and V is defined to be

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

It turns out that the set $\mathcal{P}_q(N)$ equipped with the subspace distance is indeed a *metric space* (see [13]). A *subspace code* \mathcal{C} is simply a nonempty subset of $\mathcal{P}_q(N)$; if, in addition, all the elements of \mathcal{C} have the same dimension k , then \mathcal{C} is called a *k -dimensional subspace code* (or *constant dimension code* for short). The *minimum (subspace) distance* of any subspace code \mathcal{C} is defined to be

$$d(\mathcal{C}) = \min_{U \neq V \in \mathcal{C}} d(U, V).$$

Subspace codes and particularly constant dimension codes have attracted much attention in recent years due to their applications in random network coding for correction of errors and erasures [13]. Subspace codes are also of interest from mathematical viewpoints (see, for example, [1], [7], [16], [18] and [22]). One of the main research problems on constant dimension codes is to find systematic methods to produce good k -dimensional subspace codes with a large code size and a large minimum distance when q, N , and k are fixed. The seminal works [13, 19] presented novel constructions of large constant dimension codes through linearized polynomials.

As a particular subclass of subspace codes, cyclic subspace codes have additional properties that can be applied efficiently in encoding and decoding algorithms (e.g., see [20]). For a given subspace $U \in \mathcal{P}_q(N)$ and $\alpha \in \mathbb{F}_{q^N}^*$ (where $\mathbb{F}_{q^N}^* = \mathbb{F}_{q^N} \setminus \{0\}$), the *cyclic shift* of U is defined by $\alpha U = \{\alpha u \mid u \in U\}$, where the product αu is taken in \mathbb{F}_{q^N} . It is clear that αU is a vector space over \mathbb{F}_q having the same

Email addresses: bocong_chen@yahoo.com (B. Chen), hwliu@mail.ccnu.edu.cn (H. Liu).

dimension as U . Two cyclic shifts are called *distinct* if they form two different subspaces. A subspace code \mathcal{C} is said to be *cyclic* if $\alpha U \in \mathcal{C}$ for any $\alpha \in \mathbb{F}_{q^N}^*$ and any $U \in \mathcal{C}$. Several optimal cyclic subspace codes with small dimensions were found in [9] and [14]. A thorough analysis of the algebraic structure of cyclic subspace codes was given in [20]. In [5], an optimal code which also forms a q -analog of Steiner system was presented.

We tacitly assume $k > 1$, as the case $k = 1$ is uninteresting. The biggest possible value for the minimum distance of any k -dimensional cyclic subspace code is $2k$. However, it is not hard to see that if the size of a k -dimensional cyclic subspace code is greater than or equal to $(q^N - 1)/(q - 1)$ then its minimum distance cannot achieve $2k$. In other words, the best minimum distance of a k -dimensional cyclic subspace code whose size is greater than or equal to $(q^N - 1)/(q - 1)$ can attain is thus $2k - 2$. By virtue of this fact and using computer searches, [20] and [12] raised the following conjecture: For any positive integers N and k with $k < N/2$, there exists a k -dimensional cyclic subspace code of size $(q^N - 1)/(q - 1)$ and of minimum distance $2k - 2$. As mentioned at the end of [12], it would also be interesting to find systematic methods to produce k -dimensional cyclic subspace codes whose sizes exceed $(q^N - 1)/(q - 1)$ and whose minimum distances remain exactly $2k - 2$.

Recently, Ben-Sasson *et al.* [2] used subspace polynomials to generate k -dimensional cyclic subspace codes with size $(q^N - 1)/(q - 1)$ and minimum distance $2k - 2$: Let V denote the set of roots of the trinomial $X^{q^k} + X^q + X \in \mathbb{F}_q[X]$ (suppose V is contained in \mathbb{F}_{q^N}). Then $\{\alpha V \mid \alpha \in \mathbb{F}_{q^N}^*\}$ is a cyclic subspace code of which the size is $(q^N - 1)/(q - 1)$ and the minimum distance is $2k - 2$. The conclusion of this result reveals that the aforementioned conjecture holds true for any given k and infinitely many values of N . Furthermore, in the same paper the authors provided a construction of k -dimensional cyclic subspace codes of size $r \frac{q^N - 1}{q - 1}$ and minimum distance $2k - 2$, which is the first systematic construction of cyclic constant dimension codes of size greater than $(q^N - 1)/(q - 1)$. Otal and Özbudak [17] generalized and improved the construction in [2] by studying the roots of the trinomials $X^{q^k} + \theta_i X^q + \gamma_i X \in \mathbb{F}_{q^n}[X]$, where θ_i and γ_i are nonzero elements of \mathbb{F}_{q^n} for $1 \leq i \leq r$. As a consequence, some constraint conditions in [2] are relaxed, the density of the length parameter N is increased, and the size of k -dimensional cyclic subspace codes can be increased up to $(q^n - 1) \frac{q^N - 1}{q - 1}$ without decreasing the minimum distance $2k - 2$.

The present paper is to extend the previous works [2] and [17] by proposing a different approach. We explore the ideas of constructing cyclic constant dimension codes proposed in [2] and [17] to obtain further results; consequently, new code constructions are provided and several previously known results in [2] and [17] are extended. More explicitly, we show that if the set of roots of the trinomial $X^{q^k} + a_\ell X^{q^\ell} + a_0 X \in \mathbb{F}_{q^n}[X]$ is denoted by V (suppose V is contained in \mathbb{F}_{q^N}), where $1 \leq \ell < k$ is a positive integer relatively prime to k , n is an arbitrary positive integer and a_0, a_ℓ are nonzero elements of \mathbb{F}_{q^n} , then $\{\alpha V \mid \alpha \in \mathbb{F}_{q^N}^*\}$ is a cyclic subspace code of which the size is $(q^N - 1)/(q - 1)$ and the minimum distance is $2k - 2$ (see Lemma 3.1). Moreover, unions of such cyclic constant dimension codes from the roots of trinomials and binomials are also discussed (see Theorem 3.10 and its corollaries). Several examples are provided to illustrate our results. We mention that we can produce an infinite family of k -dimensional cyclic subspace codes with size $(q^n - 1) \frac{(q^N - 1)}{q - 1} + \frac{q^N - 1}{q^k - 1}$ and minimum distance $2k - 2$ (see Corollary 3.11).

The remainder of this paper is organized as follows. Section 2 establishes some notations that will be used throughout, and reviews some basic results that will be needed in subsequent sections, including the notions of linearized polynomials and subspace polynomials. Section 3 contains our main results. Section 4 summarizes this paper.

2 Preliminaries

A class of polynomials that plays an important role in the study of subspace codes is the so-called linearized polynomials (e.g., see [15, P. 107]). In this section we will briefly review the definitions and some basic properties about linearized polynomials.

Throughout this paper, \mathbb{F}_q denotes the finite field of size q . Let $n \geq 1$ be a positive integer and let \mathbb{F}_{q^n} be the field extension of degree n over \mathbb{F}_q . Recall that $\mathcal{P}_q(N)$ denotes the set of all subspaces of \mathbb{F}_{q^N} ,

where $N \geq 1$ is an integer. A *linearized polynomial* over \mathbb{F}_{q^n} is a polynomial of the form

$$f(X) = \alpha_k X^{q^k} + \alpha_{k-1} X^{q^{k-1}} + \cdots + \alpha_1 X^q + \alpha_0 X \in \mathbb{F}_{q^n}[X],$$

where α_i are elements of \mathbb{F}_{q^n} for $0 \leq i \leq k$. If $\alpha_k \neq 0$ then k is called the q -degree of f . Linearized polynomials have the following properties (see [15]):

Proposition 2.1. *The roots of any linearized polynomial form a subspace in some extension field over \mathbb{F}_{q^n} . Conversely, for any subspace $V \in \mathcal{P}_q(N)$, the polynomial*

$$\prod_{v \in V} (X - v)$$

is a linearized polynomial.

It is well known that a linearized polynomial has no multiple roots if and only if the coefficient of X is nonzero (see [15, Theorem 3.50]). We will be particularly interested in such linearized polynomials, which merit a special name: A monic linearized polynomial is called a *subspace polynomial* if it has no multiple roots (see [3], [4], [6] or [21]). We remark that a subspace polynomial with respect to \mathbb{F}_{q^n} can be defined alternatively as the annihilator polynomial of a subspace of \mathbb{F}_{q^n} , in order to make sense into using the term “subspace”. There is an obvious one-to-one correspondence between the k -dimensional subspaces of $\mathcal{P}_q(N)$ and the subspace polynomials with q -degree k whose splitting fields are \mathbb{F}_{q^N} . In particular, two subspaces are identical if and only if their corresponding subspace polynomials are identical. This suggests that the resolution of vector space problems can be converted into the resolution of polynomial problems.

Given a k -dimensional subspace $V \in \mathcal{P}_q(N)$ and a nonzero element $\alpha \in \mathbb{F}_{q^N}$, the subspace polynomial corresponding to the subspace $\alpha V = \{\alpha v \mid v \in V\}$ has been characterized in [2, Lemma 5]:

Lemma 2.2. *Let V be a k -dimensional subspace of \mathbb{F}_{q^N} and let α be a nonzero element of \mathbb{F}_{q^N} . If*

$$T(X) = \prod_{v \in V} (X - v) = X^{q^k} + \sum_{i=0}^{k-1} a_i X^{q^i}$$

is the subspace polynomial corresponding to V , then the subspace polynomial corresponding to αV is given by

$$T_\alpha(X) = \prod_{v \in V} (X - \alpha v) = X^{q^k} + \sum_{i=0}^{k-1} \alpha^{q^k - q^i} a_i X^{q^i}.$$

3 Constructions of cyclic constant dimension codes

We first propose a new approach to generalize [2, Theorem 3], which can be seen as the $\ell = 1$ case of the following lemma.

Lemma 3.1. *Let k and ℓ be positive integers with $1 \leq \ell < k$ and $\gcd(\ell, k) = 1$. Let a_0 and a_ℓ be nonzero elements of \mathbb{F}_{q^n} , where n is a positive integer. Suppose that the set V of roots of the subspace polynomial*

$$T(X) = X^{q^k} + a_\ell X^{q^\ell} + a_0 X \in \mathbb{F}_{q^n}[X]$$

is contained in \mathbb{F}_{q^N} . Then

$$\mathcal{C} = \left\{ \alpha V \mid \alpha \in \mathbb{F}_{q^N}^* \right\}$$

is a k -dimensional cyclic subspace code with size $\frac{q^N - 1}{q - 1}$ and minimum distance $2k - 2$.

Proof. It is a known fact that if \mathcal{C} has size $(q^N - 1)/(q - 1)$ then \mathcal{C} cannot have minimum distance $2k$; this is simply because if it were $2k$ then $\mathbb{F}_{q^N}^* \setminus \{0\}$ would contain $\frac{(q^N - 1)(q^k - 1)}{(q - 1)}$ elements, which is impossible. Therefore, to obtain the desired result, it suffices to prove that

$$\dim(V \cap \alpha V) \leq 1 \quad \text{for any } \alpha \in \mathbb{F}_{q^N}^* \setminus \mathbb{F}_q^*. \quad (3.1)$$

Fix an element $\alpha \in \mathbb{F}_{q^N}^* \setminus \mathbb{F}_q^*$. By Lemma 2.2, the subspace polynomial corresponding to αV is

$$T_\alpha(X) = X^{q^k} + a_\ell \alpha^{q^k - q^\ell} X^{q^\ell} + a_0 \alpha^{q^k - 1} X.$$

Suppose now a and b are any nonzero elements of $V \cap \alpha V$. We aim to show that an element $\lambda \in \mathbb{F}_q^*$ can be found such that $a = \lambda b$; we then conclude that (3.1) is achieved, and thus the proof is complete. To this end, we first claim that if exactly one of $\alpha^{q^k - q^\ell} - 1$ and $\alpha^{q^k - 1} - 1$ is equal to 0, then we arrive at (3.1) at once. Indeed, observe that

$$T_\alpha(X) - T(X) = a_\ell (\alpha^{q^k - q^\ell} - 1) X^{q^\ell} + a_0 (\alpha^{q^k - 1} - 1) X.$$

If $\alpha^{q^k - q^\ell} - 1 \neq 0$ and $\alpha^{q^k - 1} - 1 = 0$ (or, $\alpha^{q^k - q^\ell} - 1 = 0$ and $\alpha^{q^k - 1} - 1 \neq 0$), then the subspace polynomials $T_\alpha(X)$ and $T(X)$ have a unique common root 0, proving the claim. If both

$$\alpha^{q^k - q^\ell} - 1 = 0 \quad \text{and} \quad \alpha^{q^k - 1} - 1 = 0,$$

then $\alpha = \alpha^{q^k} = \alpha^{q^\ell}$, which implies that $\alpha \in \mathbb{F}_{q^k}$ and $\alpha \in \mathbb{F}_{q^\ell}$. However, our assumption $\gcd(\ell, k) = 1$ forces $\alpha \in \mathbb{F}_q^*$. This is a contradiction. Thus, it cannot occur simultaneously that $\alpha^{q^k - q^\ell} - 1 = 0$ and $\alpha^{q^k - 1} - 1 = 0$. We can assume, therefore, that $\alpha^{q^k - q^\ell} - 1 \neq 0$ and $\alpha^{q^k - 1} - 1 \neq 0$. Since a and b are contained in $V \cap \alpha V$, we have

$$T(a) = T(b) = T_\alpha(a) = T_\alpha(b) = 0.$$

This leads to

$$T_\alpha(a) - T(a) = a_\ell (\alpha^{q^k - q^\ell} - 1) a^{q^\ell} + a_0 (\alpha^{q^k - 1} - 1) a = 0$$

and

$$T_\alpha(b) - T(b) = a_\ell (\alpha^{q^k - q^\ell} - 1) b^{q^\ell} + a_0 (\alpha^{q^k - 1} - 1) b = 0.$$

It follows that

$$a^{q^\ell - 1} = \frac{-a_0 (\alpha^{q^k - 1} - 1)}{a_\ell (\alpha^{q^k - q^\ell} - 1)} = b^{q^\ell - 1},$$

or, equivalently,

$$\frac{a}{b} = \left(\frac{a}{b}\right)^{q^\ell}$$

which gives $a/b \in \mathbb{F}_{q^\ell}$. Let $a/b = \lambda \in \mathbb{F}_{q^\ell}$, namely $a = b\lambda$. By $T(a) = 0$ and $a = \lambda b$, we have

$$0 = T(a) = a^{q^k} + a_\ell a^{q^\ell} + a_0 a = \lambda^{q^k} b^{q^k} + a_\ell \lambda^{q^\ell} b^{q^\ell} + a_0 b \lambda = \lambda^{q^k} b^{q^k} + a_\ell \lambda b^{q^\ell} + a_0 b \lambda,$$

where the last equality holds because λ is an element of \mathbb{F}_{q^ℓ} . Combining with

$$\lambda T(b) = \lambda b^{q^k} + \lambda a_\ell b^{q^\ell} + \lambda a_0 b = 0,$$

we have $\lambda = \lambda^{q^k}$. By $\gcd(\ell, k) = 1$ again, we finally conclude that $\lambda \in \mathbb{F}_q$, as wanted. The proof is complete. \square

As pointed out by [17, Section 2.2], the value of N in Lemma 3.1 cannot be chosen freely; it is depending on the values of k, ℓ, n and the nonzero elements a_ℓ, a_0 . We include the following example to illustrate Lemma 3.1.

Example 3.2. We adopt the notation in Lemma 3.1. Take $q = 3$, $n = 1$, and $k = 5$. Consider the degree N' of the splitting field of the polynomial $X^{3^5} + a_\ell X^{3^\ell} + a_0 X \in \mathbb{F}_3[X]$, where $1 \leq \ell \leq 4$ and $a_\ell, a_0 \in \{1, -1\}$; the values of N' can be determined easily by using the computer algebra system GAP [11], as exhibited in Table 3.1. Lemma 3.1 ensures that there exists a 5-dimensional cyclic subspace code of size $\frac{3^N-1}{2}$ and minimum distance 8 in \mathbb{F}_{3^N} when N is a multiple of N' . For instance, the first row of Table 3.1 implies that the set of roots of the subspace polynomial $X^{3^5} + X^3 + X$ forms a 5-dimensional cyclic subspace code of size $\frac{3^N-1}{2}$ and minimum distance 8 in \mathbb{F}_{3^N} when N is a multiple of 78. We then compare among the last column of Table 3.1 to pick out the minimal elements with respect to the partially ordered by divisibility (for positive integers a, b , $a \leq b$ precisely when a divides b). After a bit of simple calculations, the minimal elements are 78, 121, 80 and 104. From the first four rows of Table 3.1, one sees that [2, Theorem 3] and [17, Theorem 3] only produce the first two values 78 and 121. This example suggests that Lemma 3.1 indeed could provide subspace codes for more various values of N .

Table 3.1: The degrees of the splitting fields of the polynomials $X^{3^5} + a_\ell X^{3^\ell} + a_0 X$

Values of ℓ	(a_ℓ, a_0)	Polynomials	The degrees N' of the splitting fields over \mathbb{F}_3
1	(1, 1)	$X^{3^5} + X^3 + X$	78
1	(1, -1)	$X^{3^5} + X^3 - X$	78
1	(-1, 1)	$X^{3^5} - X^3 + X$	242
1	(-1, -1)	$X^{3^5} - X^3 - X$	121
2	(1, 1)	$X^{3^5} + X^{3^2} + X$	80
2	(1, -1)	$X^{3^5} + X^{3^2} - X$	104
2	(-1, 1)	$X^{3^5} - X^{3^2} + X$	312
2	(-1, -1)	$X^{3^5} - X^{3^2} - X$	80
3	(1, 1)	$X^{3^5} + X^{3^3} + X$	80
3	(1, -1)	$X^{3^5} + X^{3^3} - X$	80
3	(-1, 1)	$X^{3^5} - X^{3^3} + X$	312
3	(-1, -1)	$X^{3^5} - X^{3^3} - X$	104
4	(1, 1)	$X^{3^5} + X^{3^4} + X$	78
4	(1, -1)	$X^{3^5} + X^{3^4} - X$	121
4	(-1, 1)	$X^{3^5} - X^{3^4} + X$	242
4	(-1, -1)	$X^{3^5} - X^{3^4} - X$	78

Some cyclic constant dimension codes produced by Lemma 3.1 can be put together to form a larger code, but without reducing the minimum distance. The following lemma is a generalization of [17, Theorem 3], which considers the case $\ell = 1$.

Lemma 3.3. *Let k and ℓ be positive integers with $1 \leq \ell < k$ and $\gcd(\ell, k) = 1$, and let*

$$T^{(i)}(X) = X^{q^k} + \theta_i X^{q^\ell} + \gamma_i X \in \mathbb{F}_{q^n}[X]$$

be r subspace polynomials over \mathbb{F}_{q^n} with θ_i and γ_i being nonzero elements of \mathbb{F}_{q^n} for $1 \leq i \leq r$. Suppose that V_i is the set of roots of the subspace polynomial $T^{(i)}(X)$ and that V_i ($1 \leq i \leq r$) are contained in \mathbb{F}_{q^N} . If

$$\left(\frac{\gamma_i}{\gamma_j}\right)^{\frac{q^\ell-1}{q-1}} \neq \left(\frac{\gamma_i}{\gamma_j}\left(\frac{\theta_i}{\theta_j}\right)^{-1}\right)^{\frac{q^k-1}{q-1}} \text{ for any } 1 \leq i \neq j \leq r, \quad (3.2)$$

then

$$\mathcal{C} = \bigcup_{i=1}^r \left\{ \alpha V_i \mid \alpha \in \mathbb{F}_{q^N}^* \right\}$$

is a k -dimensional cyclic subspace code of size $r \frac{q^N-1}{q-1}$ and minimum distance $2k-2$.

Proof. Using Lemma 3.1, it is enough to prove that

$$\dim(V_i \cap \alpha V_j) \leq 1 \quad \text{for any } \alpha \in \mathbb{F}_{q^N}^* \text{ and } 1 \leq i \neq j \leq r. \quad (3.3)$$

The proof is similar to that of Lemma 3.1, with a few modifications. Let $\alpha \in \mathbb{F}_{q^N}^*$ and let $1 \leq i \neq j \leq r$ be two distinct integers. The subspace polynomial corresponding to αV_j is

$$T_\alpha^{(j)}(X) = X^{q^k} + \theta_j \alpha^{q^k - q^\ell} X^{q^\ell} + \gamma_j \alpha^{q^k - 1} X,$$

and thus

$$T_\alpha^{(j)}(X) - T^{(i)}(X) = (\theta_j \alpha^{q^k - q^\ell} - \theta_i) X^{q^\ell} + (\gamma_j \alpha^{q^k - 1} - \gamma_i) X.$$

As we did in the proof of Lemma 3.1, we are done if exactly one of $\theta_j \alpha^{q^k - q^\ell} - \theta_i$ and $\gamma_j \alpha^{q^k - 1} - \gamma_i$ is equal to 0. If

$$\theta_j \alpha^{q^k - q^\ell} - \theta_i = 0 \quad \text{and} \quad \gamma_j \alpha^{q^k - 1} - \gamma_i = 0$$

then

$$\alpha^{q^\ell - 1} = \frac{\gamma_i}{\gamma_j} \left(\frac{\theta_i}{\theta_j} \right)^{-1} \quad \text{and} \quad \alpha^{q^k - 1} = \frac{\gamma_i}{\gamma_j}.$$

This leads to

$$\alpha^{\frac{(q^\ell - 1)(q^k - 1)}{q - 1}} = \left(\frac{\gamma_i}{\gamma_j} \left(\frac{\theta_i}{\theta_j} \right)^{-1} \right)^{\frac{q^k - 1}{q - 1}}$$

and

$$\alpha^{\frac{(q^\ell - 1)(q^k - 1)}{q - 1}} = \left(\frac{\gamma_i}{\gamma_j} \right)^{\frac{q^\ell - 1}{q - 1}}.$$

Therefore, one has

$$\left(\frac{\gamma_i}{\gamma_j} \left(\frac{\theta_i}{\theta_j} \right)^{-1} \right)^{\frac{q^k - 1}{q - 1}} = \alpha^{\frac{(q^\ell - 1)(q^k - 1)}{q - 1}} = \left(\frac{\gamma_i}{\gamma_j} \right)^{\frac{q^\ell - 1}{q - 1}},$$

which contradicts our assumption (3.2). We can assume, therefore, that

$$\theta_j \alpha^{q^k - q^\ell} - \theta_i \neq 0 \quad \text{and} \quad \gamma_j \alpha^{q^k - 1} - \gamma_i \neq 0.$$

At this point, taking arguments similar to those used in the proof of Lemma 3.1, we obtained the desired result. \square

The following corollaries are direct consequence of Lemma 3.3. We first specialize Lemma 3.3 to the case of $\ell = 1$ and $\theta_i = \gamma_i$.

Corollary 3.4. *Let r be an integer with $1 \leq r \leq q^n - 1$ and let*

$$T^{(i)}(X) = X^{q^k} + \theta_i X^q + \theta_i X \in \mathbb{F}_{q^n}[X]$$

be r subspace polynomials over \mathbb{F}_{q^n} , where θ_i are distinct nonzero elements of \mathbb{F}_{q^n} for $1 \leq i \leq r$. Suppose that V_i is the set of roots of the subspace polynomial $T^{(i)}(X)$ and that V_i ($1 \leq i \leq r$) are contained in \mathbb{F}_{q^N} . Then

$$\mathcal{C} = \bigcup_{i=1}^r \left\{ \alpha V_i \mid \alpha \in \mathbb{F}_{q^N}^* \right\}$$

is a k -dimensional cyclic subspace code of size $r \frac{(q^N - 1)}{q - 1}$ and minimum distance $2k - 2$.

Proof. Take $\ell = 1$ and $\theta_i = \gamma_i$ for each $1 \leq i \leq r$ in Lemma 3.3. The right-hand side of inequality (3.2) is equal to 1; however, the left-hand side of (3.2) is certainly not equal to 1. It follows that inequality (3.2) holds true, and we get the desired result by applying Lemma 3.3. \square

The following corollary aims to provide an example of large codes for the $\ell \neq 1$ case; however, in order to state the conditions compactly, we restrict ourself to the case where $q = 2$ and $n = k$.

Corollary 3.5. *Let k, ℓ , and r be positive integers with $1 \leq \ell < k$, $\gcd(\ell, k) = 1$ and $1 \leq r \leq 2^k - 1$. Let*

$$T^{(i)}(X) = X^{2^k} + \theta_i X^{2^\ell} + \theta_i X \in \mathbb{F}_{2^k}[X]$$

be r subspace polynomials over \mathbb{F}_{2^k} with θ_i being distinct nonzero elements of \mathbb{F}_{2^k} for $1 \leq i \leq r$. Suppose that V_i is the set of roots of the subspace polynomial $T^{(i)}(X)$ and that V_i ($1 \leq i \leq r$) are contained in \mathbb{F}_{2^N} . Then

$$\mathcal{C} = \bigcup_{i=1}^r \left\{ \alpha V_i \mid \alpha \in \mathbb{F}_{2^N}^* \right\}$$

is a k -dimensional cyclic subspace code of size $r(2^N - 1)$ and minimum distance $2k - 2$.

Proof. Taking $q = 2$, $n = k$ and $\theta_i = \gamma_i$ for each $1 \leq i \leq r$ in Lemma 3.3, we are left to show that

$$\left(\frac{\theta_i}{\theta_j} \right)^{2^\ell - 1} \neq 1 \quad \text{for any } 1 \leq i \neq j \leq r.$$

Since θ_i are distinct nonzero elements of \mathbb{F}_{2^k} for $1 \leq i \leq r$, we have

$$\frac{\theta_i}{\theta_j} \neq 1 \quad \text{and} \quad \left(\frac{\theta_i}{\theta_j} \right)^{2^k - 1} = 1$$

for any $1 \leq i \neq j \leq r$. If $(\theta_i/\theta_j)^{2^\ell - 1}$ were equal to 1, we would have $\theta_i/\theta_j = 1$ since $\gcd(2^k - 1, 2^\ell - 1) = 1$. This is a contradiction. We are done. \square

Here is an example to illustrate Corollary 3.5.

Example 3.6. Take $k = 5$ and $r = 5$ in Corollary 3.5. Let θ be a generator of the cyclic group $\mathbb{F}_{2^5}^*$ given by the computer algebra system GAP [11]. Set $\theta_1 = \theta^3$, $\theta_2 = \theta^6$, $\theta_3 = \theta^{12}$, $\theta_4 = \theta^{17}$, and $\theta_5 = \theta^{24}$. Fix a value ℓ , $1 \leq \ell \leq 4$. Let N'_ℓ denote the degree of the splitting field of the polynomials $T^{(i)}(X) = X^{2^5} + \theta_i X^{2^\ell} + \theta_i X \in \mathbb{F}_{2^5}[X]$, $1 \leq i \leq 5$. With ℓ ranging from 1 to 4, Corollary 3.5 then permits us to produce 4 constant cyclic subspace codes in \mathbb{F}_{2^N} having size $5(2^N - 1)$ and minimum distance $2k - 2 = 8$, where N is a multiple of N'_ℓ . Using GAP [11], the values of N'_ℓ are listed in Table 3.2.

Table 3.2: The values of N'_ℓ	
Values of ℓ	Values of N'_ℓ
1	30
2	70
3	75
4	60

Gluesing-Luerssen *et al.* studied constant cyclic subspace codes having full minimum distances in [12]; it is well known that the set of all cyclic shifts of \mathbb{F}_{q^k} (as a subfield of \mathbb{F}_{q^n}) forms a cyclic subspace code of full minimum distance $2k$. To insert such codes into those produced in Lemma 3.3 (where codes are characterized through subspace polynomials), the codes having full minimum distance are also described by subspace polynomials for consistency, as we show below.

Proposition 3.7. *Let $k > 1$ be a positive integer and let a_0 be a nonzero element of \mathbb{F}_{q^n} . Suppose that the set U of roots of the subspace polynomial*

$$T(X) = X^{q^k} - a_0 X \in \mathbb{F}_{q^n}[X]$$

is contained in \mathbb{F}_{q^N} . Then

$$\mathcal{C} = \left\{ \alpha U \mid \alpha \in \mathbb{F}_{q^N}^* \right\}$$

is a k -dimensional cyclic subspace code of size $\frac{q^N-1}{q^k-1}$ and minimum distance $2k$.

Proof. Let $\alpha \in \mathbb{F}_{q^N}^*$. The subspace polynomial corresponding to αU is

$$T_\alpha(X) = X^{q^k} - a_0 \alpha^{q^k-1} X.$$

It is readily seen that

$$T_\alpha(X) - T(X) = a_0(1 - \alpha^{q^k-1})X.$$

Hence, $\alpha U = U$ if and only if $\alpha^{q^k-1} = 1$, which implies that the size of \mathcal{C} is equal to $(q^N - 1)/(q^k - 1)$. Finally, it is trivial to see that the minimum distance of \mathcal{C} is $2k$. We are done. \square

Remark 3.8. Theoretically, the splitting field of any binomial over a finite field can be determined easily. Indeed, suppose a_0 has order s in the cyclic group $\mathbb{F}_{q^n}^*$. Then the degree of the splitting field N' of $T(X) = X^{q^k} - a_0 X \in \mathbb{F}_{q^n}[X]$ is equal to the multiplicative order of q modulo $s(q^k - 1)$, i.e., N' is the smallest positive integer such that $s(q^k - 1)$ divides $q^{N'} - 1$. In fact, a primitive $s(q^k - 1)$ -th root of unity ω in the finite field $\mathbb{F}_{q^{N'}}$ can be found such that $\omega^{q^k-1} = a_0$. It is clear that k is a divisor of N' .

We present the following example to illustrate Proposition 3.7.

Example 3.9. Let $k = 5$, $q = 3$, and $n = 5$ in Proposition 3.7. Let a_0 be an element of $\mathbb{F}_{3^5}^*$ having order $s = 11$. GAP [11] computations show that the multiplicative order of $q = 3$ modulo $s(q^k - 1) = 11(3^5 - 1) = 11 \times 242$ is equal to $N' = 55$. It follows that the splitting field of the subspace polynomial

$$T(X) = X^{3^5} - a_0 X \in \mathbb{F}_{3^5}[X]$$

is $\mathbb{F}_{3^{55}}$. Let U be the set of roots of $T(X)$, and it follows from Proposition 3.7 that

$$\mathcal{C} = \left\{ \alpha U \mid \alpha \in \mathbb{F}_{3^{55}}^* \right\}$$

is a cyclic subspace code of size $\frac{q^{55}-1}{q^5-1} = \frac{3^{55}-1}{3^5-1}$ and minimum distance $2k = 10$.

At the moment, we derive the following theorem which puts certain cyclic constant dimension codes generated by Lemma 3.3 and Proposition 3.7 together to form a new code.

Theorem 3.10. Let k and ℓ be positive integers with $1 \leq \ell < k$ and $\gcd(\ell, k) = 1$. Let

$$T(X) = X^{q^k} - a_0 X \in \mathbb{F}_{q^n}[X]$$

and

$$T^{(i)}(X) = X^{q^k} + \theta_i X^{q^\ell} + \gamma_i X \in \mathbb{F}_{q^n}[X]$$

be $r+1$ subspace polynomials over \mathbb{F}_{q^n} with a_0 , θ_i , and γ_i being nonzero elements of \mathbb{F}_{q^n} for $1 \leq i \leq r$. Suppose that U and V_i are the sets of roots of the subspace polynomials $T(X)$ and $T^{(i)}(X)$, respectively, and that U and V_i are contained in \mathbb{F}_{q^N} for all $1 \leq i \leq r$. If

$$\left(\frac{\gamma_i}{\gamma_j} \right)^{\frac{q^\ell-1}{q-1}} \neq \left(\frac{\gamma_i}{\gamma_j} \left(\frac{\theta_i}{\theta_j} \right)^{-1} \right)^{\frac{q^k-1}{q-1}} \quad \text{for any } 1 \leq i \neq j \leq r$$

then

$$\mathcal{C} = \left(\bigcup_{i=1}^r \left\{ \alpha V_i \mid \alpha \in \mathbb{F}_{q^N}^* \right\} \right) \cup \left\{ \alpha U \mid \alpha \in \mathbb{F}_{q^N}^* \right\}$$

is a k -dimensional cyclic subspace code of size $r \frac{q^N-1}{q-1} + \frac{q^N-1}{q^k-1}$ and minimum distance $2k-2$.

Proof. By Lemma 3.3 and Proposition 3.7, it is enough to show that

$$\dim(\alpha U \cap V_i) \leq 1 \quad \text{for any } \alpha \in \mathbb{F}_{q^N}^* \text{ and } 1 \leq i \leq r.$$

Fix a nonzero element $\alpha \in \mathbb{F}_{q^N}$. The subspace polynomial corresponding to αU is

$$T_\alpha(X) = X^{q^k} - a_0 \alpha^{q^k-1} X.$$

Clearly,

$$T^{(i)}(X) - T_\alpha(X) = \theta_i X^{q^\ell} + (\gamma_i + a_0 \alpha^{q^k-1}) X \in \mathbb{F}_{q^n}[X].$$

If $\gamma_i + a_0 \alpha^{q^k-1} = 0$ then the desired result holds trivially. Suppose $\gamma_i + a_0 \alpha^{q^k-1} \neq 0$. Let a and b be any nonzero elements of $\alpha U \cap V_i$. We then have

$$T^{(i)}(a) = T^{(i)}(b) = T_\alpha(a) = T_\alpha(b) = 0.$$

Hence,

$$T^{(i)}(a) - T_\alpha(a) = \theta_i a^{q^\ell} + (\gamma_i + a_0 \alpha^{q^k-1}) a = 0$$

and

$$T^{(i)}(b) - T_\alpha(b) = \theta_i b^{q^\ell} + (\gamma_i + a_0 \alpha^{q^k-1}) b = 0.$$

It follows that

$$a^{q^\ell-1} = \frac{\gamma_i + a_0 \alpha^{q^k-1}}{-\theta_i} = b^{q^\ell-1}.$$

Therefore,

$$\frac{a}{b} = \left(\frac{a}{b}\right)^{q^\ell},$$

which gives $a/b \in \mathbb{F}_{q^\ell}$. Let $a/b = \lambda \in \mathbb{F}_{q^\ell}$, or alternatively, $a = b\lambda$. As we have done in the proof of Lemma 3.1, we conclude that λ is, in fact, contained in \mathbb{F}_q^* . The proof is complete. \square

We end this section with the following two immediate corollaries of Theorem 3.10 and Corollaries 3.4 and 3.5.

Corollary 3.11. *Let $k > 1$ be a positive integer. Let n and r be positive integers with $1 \leq r \leq q^n - 1$. Let*

$$T(X) = X^{q^k} - a_0 X \in \mathbb{F}_{q^n}[X]$$

and

$$T^{(i)}(X) = X^{q^k} + \theta_i X^q + \theta_i X \in \mathbb{F}_{q^n}[X]$$

be $r+1$ subspace polynomials over \mathbb{F}_{q^n} with a_0 and θ_i being nonzero elements of \mathbb{F}_{q^n} for $1 \leq i \leq r$. Suppose that U and V_i are the sets of roots of $T(X)$ and $T^{(i)}(X)$, respectively, and that U and V_i , $1 \leq i \leq r$, are contained in \mathbb{F}_{q^N} . Then

$$\mathcal{C} = \left(\bigcup_{i=1}^r \left\{ \alpha V_i \mid \alpha \in \mathbb{F}_{q^N}^* \right\} \right) \cup \left\{ \alpha U \mid \alpha \in \mathbb{F}_{q^N}^* \right\}$$

is a k -dimensional cyclic subspace code of size $r \frac{q^N-1}{q-1} + \frac{q^N-1}{q^k-1}$ and minimum distance $2k-2$.

Here is an example to demonstrate Corollary 3.11.

Example 3.12. Take $q = 3$, $k = 5$, $n = 1$, and $r = 2$ in Corollary 3.11. Let $\theta_1 = 1$ and $\theta_2 = -1$. GAP [11] computations show that the degrees of the splitting fields of $T^{(1)}(X)$ and $T^{(2)}(X)$ are equal to 78 and 121, respectively. We simply take $a_0 = 1$, thus the degree of the splitting field of $T(X)$ is equal to 5. Setting $N = 78 \times 121 \times 5$, one knows that the vector spaces U , V_1 and V_2 are contained in \mathbb{F}_{3^N} . It follows from Corollary 3.11 that

$$\mathcal{C} = \left(\bigcup_{i=1}^2 \left\{ \alpha V_i \mid \alpha \in \mathbb{F}_{3^N}^* \right\} \right) \cup \left\{ \alpha U \mid \alpha \in \mathbb{F}_{3^N}^* \right\}$$

is a 5-dimensional cyclic subspace code of size $3^N - 1 + \frac{3^N-1}{3^5-1}$ and minimum distance 8.

Corollary 3.13. *Let k , ℓ , and r be positive integers with $1 \leq \ell < k$, $\gcd(\ell, k) = 1$ and $1 \leq r \leq 2^k - 1$. Let*

$$T(X) = X^{2^k} + a_0 X \in \mathbb{F}_{2^k}[X]$$

and

$$T^{(i)}(X) = X^{2^k} + \theta_i X^{2^\ell} + \theta_i X \in \mathbb{F}_{2^k}[X]$$

be $r+1$ subspace polynomials over \mathbb{F}_{2^k} with a_0 and θ_i being nonzero elements of \mathbb{F}_{2^k} for $1 \leq i \leq r$. Suppose that U and V_i are the sets of roots of $T(X)$ and $T^{(i)}(X)$, respectively, and that U and V_i , $1 \leq i \leq r$, are contained in \mathbb{F}_{2^N} . Then

$$\mathcal{C} = \left(\bigcup_{i=1}^r \left\{ \alpha V_i \mid \alpha \in \mathbb{F}_{2^N}^* \right\} \right) \cup \left\{ \alpha U \mid \alpha \in \mathbb{F}_{2^N}^* \right\}$$

is a k -dimensional cyclic subspace code of size $r(2^N - 1) + \frac{2^N - 1}{2^k - 1}$ and minimum distance $2k - 2$.

We present an illustrative example of Corollary 3.13.

Example 3.14. The codes generated by Example 3.6 are enlarged here to produce bigger codes without compromising the minimum distances. Take $k = 5$ and $r = 5$ in Corollary 3.13. Recall from Example 3.6 that we have already obtained four 5-dimensional cyclic subspace codes in \mathbb{F}_{2^N} , each of which has size $5(2^N - 1)$ and minimum distance 8. Take $a_0 = 1$, then \mathbb{F}_{2^5} is the splitting field for $X^{2^5} + X$. Corollary 3.13 thus gives us four 5-dimensional cyclic subspace code in \mathbb{F}_{2^N} , each of which has size $5(2^N - 1) + (2^N - 1)/31$ and minimum distance 8.

4 Concluding remarks

In this paper, we study the construction of k -dimensional cyclic subspace codes with minimum distance $2k - 2$ by exploring further the ideas proposed in [2] and [17]. Lemma 3.1 is the key ingredient in computing the minimum distance of cyclic subspace codes described by a special class of subspace polynomials. Our main result, Theorem 3.10, improves [17, Theorem 3] in two directions: First we introduce a parameter ℓ which is a positive integer small than and coprime to k , thus [2, Theorem 3] and [17, Theorem 3] can be seen as the special case $\ell = 1$ of our result; second we enlarge the code size by adjoining with a spread code, without compromising the minimum distance. However, the conjecture raised in [20] and [12] (see Section 1) is still open. It is interesting to find new tools or combine several tools in the literature in order to solve this problem. It would also be a happy outcome of this paper if one can generalize the method to get further results.

Acknowledgments We sincerely thank the Associate Editor and the anonymous referees for their carefully reading and helpful suggestions which led to significant improvements of the paper. The research of Bocong Chen is supported by NSFC (Grant No. 11601158) and the Fundamental Research Funds for the Central Universities (Grant No. 2017MS111). The research of Hongwei Liu is supported by NSFC (Grant No. 11171370) and self-determined research funds of CCNU from the colleges' basic research and operation of MOE (Grant No. CCNU14F01004).

References

- [1] R. Ahlswede, H. K. Aydinian and L. H. Khachatrian, "On perfect codes and related concepts," Des. Codes Cryptogr., vol. 22, no. 3, pp. 221-237, 2001.
- [2] E. Ben-Sasson, T. Etzion, A. Gabizon and N. Raviv, "Subspace polynomials and cyclic subspace codes," IEEE Trans. Inf. Theory, vol. 62, no. 3, pp. 1157-1165, Mar. 2016.
- [3] E. Ben-Sasson and S. Kopparty, "Affine dispersers from subspace polynomials," SIAM J. Comput., vol. 41, no. 4, pp. 880-914, 2012.
- [4] E. Ben-Sasson, S. Kopparty and J. Radhakrishnan, "Subspace polynomials and limits to list decoding of Reed-Solomon codes," IEEE Trans. Inf. Theory, vol. 56, no. 1, pp. 113-120, Jan. 2010.

- [5] M. Braun, T. Etzion, P. Ostergard, A. Vardy and A. Wasserman, "Existence of q -analogues of Steiner systems," *Forum Math Pi.*, vol. 4, no. e7, pp. 1-14, Aug. 2016.
- [6] Q. Cheng, S. Gao and D. Wan, "Constructing high order elements through subspace polynomials," in *Proc. 23rd Annu. ACM-SIAM Symp., Discrete Algorithms (SODA)*, pp. 1463-1547, 2012.
- [7] L. Chihara, "On the zeros of the Askey-Wilson polynomials, with applications to coding theory," *SIAM J. Math. Anal.*, vol. 18, no. 1, pp. 191-207, 1987.
- [8] T. Etzion and L. Storme, "Galois geometries and coding theory," *Des. Codes Cryptogr.*, vol. 78, no. 1, pp. 311-350, 2016.
- [9] T. Etzion and A. Vardy, "Error-correcting codes in projective space," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 1165-1173, Feb. 2011.
- [10] T. Etzion and A. Wachter-Zeh, "Vector network coding based on subspace codes outperforms scalar linear network coding," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Barcelona, Spain, pp. 1949-1953, Aug. 2016.
- [11] GAP, The GAP Groups, Algorithms and Programming, Version 4.7.7, <http://www.gapsystem.org>, 2015.
- [12] H. Gluesing-Luerssen, K. Morrison and C. Troha, "Cyclic orbit codes and stabilizer subfields," *Adv. Math. Commun.*, vol. 9, no. 2, pp. 177-197, 2015.
- [13] R. Köetter and F. R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3579-3591, Aug. 2008.
- [14] A. Kohnert and S. Kurz, "Construction of large constant dimension codes with a prescribed minimum distance," in *Mathematical Methods in Computer Science (Lecture Notes in Computer Science)*, vol. 5393, Berlin, Germany: Springer, pp. 31-42, 2008.
- [15] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, 2008.
- [16] W. J. Martin and X. J. Zhu, "Anticodes for the Grassman and bilinear forms graphs," *Des. Codes Cryptogr.*, vol. 6, no. 1, pp. 73-79, 1995.
- [17] K. Otal and F. Özbudak, "Cyclic subspace codes via subspace polynomials," *Des. Codes Cryptogr.*, DOI 10.1007/s10623-016-0297-1, 2016.
- [18] M. Schwartz and T. Etzion, "Codes and anticodes in the Grassman graph," *J. Combinat. Theory A*, vol. 97, no. 1, pp. 27-42, 2002.
- [19] D. Silva, F. R. Kschischang and R. Koetter, "A rank-metric approach to error control in random network coding," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 3951-3967, Sep. 2008.
- [20] A.-L. Trautmann, F. Manganiello, M. Braun and J. Rosenthal, "Cyclic orbit codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 11, pp. 7386-7404, Nov. 2013.
- [21] A. Wachter-Zeh, "Bounds on list decoding of rank-metric codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 11, pp. 7268-7277, Nov. 2013.
- [22] S. Xia and F. Fu, "Johnson type bounds on constant dimension codes," *Des. Codes Cryptogr.*, vol. 50, no. 2, pp. 163-172, 2009.