LETTER

New Constructions of Sidon Spaces and Cyclic Subspace Codes*

Xue-Mei LIU[†a)], **Tong SHI**[†b)], **Min-Yao NIU**[††c)], ***Nonmembers***, **Lin-Zhi SHEN**[†d)], ***Member***, ***and*** **You GAO**[†††e)], ***Nonmember***

SUMMARY Sidon space is an important tool for constructing cyclic subspace codes. In this letter, we construct some Sidon spaces by using primitive elements and the roots of some irreducible polynomials over finite fields. Let q be a prime power, k, m, n be three positive integers and $\rho = \lceil \frac{m}{2k} \rceil - 1$, $\theta = \lceil \frac{n}{2m} \rceil - 1$. Based on these Sidon spaces and the union of some Sidon spaces, new cyclic subspace codes with size $\frac{3(q^n-1)}{q-1}$ and $\frac{\theta\rho q^k(q^n-1)}{q-1}$ are obtained. The size of these codes is lager compared to the known constructions from [14] and [10].

key words: *random network coding, cyclic subspace codes, Sidon spaces*

1. Introduction

Let $\mathbb{F}_q$ be the finite field of size q and q be a prime power. Let $\mathbb{F}_{q^n}$ be an extension field of degree n over $\mathbb{F}_q$, which can be viewed as a vector space of dimension n over $\mathbb{F}_q$. For any nonnegative integers $k \leq n$, $\mathcal{G}_q(n, k)$ is the set of all k-dimensional subspaces of $\mathbb{F}_{q^n}$ (see [1]). We can equip $\mathcal{G}_q(n, k)$ with a metric: $d(U, V) = 2k - 2\dim(U \cap V)$, where $U, V \in \mathcal{G}_q(n, k)$. If C is a nonempty subset of $\mathcal{G}_q(n, k)$, then C is called a constant dimension subspace code. A subspace code C is cyclic if $\alpha V \in C$ for any $\alpha \in \mathbb{F}_{q^n}^*$ and $V \in C$. Define the *orbit* of V as $orb(V) = \{\alpha V \mid \alpha \in \mathbb{F}_{q^n}^*\}$, then consider the action of the multiplicative group $\mathbb{F}_{q^n}^*$ to the set $orb(V)$, it is evident that $orb(V)$ is a cyclic constant dimension subspace code. The size of $orb(V)$ is $\frac{q^n-1}{q^t-1}$ for some $t \mid n$ and the distance of $orb(V)$ is $2k-2s$ with $0 \leq s \leq k$ (see [12]). If the size of $orb(V)$ is $\frac{q^n-1}{q-1}$, it is called a *full-length orbit code*. The largest minimum distance of such code is $2k - 2$, if it reaches this bound then the code is optimal (see [13]).

Subspace codes, particularly cyclic subspace codes have attracted extensive attention due to their applications in random network coding (see [4]) for correction of errors and erasures (see [2], [16], [18], [21]). One of the research directions is the construction of cyclic subspace codes with large minimum distance and as many codewords as possible for fixed q, n and k (see [19]). There are two main systematic methods to construct cyclic subspace codes. One is to use subspace polynomials (see [3], [5]–[7], [20]), the other is to use Sidon spaces. In [8], Roth et al. found the connection between Sidon spaces and cyclic subspace codes. They proved that the cyclic subspace code $orb(V)$ has size $\frac{q^n-1}{q-1}$ and minimum distance $2k-2$ if and only if V is a Sidon space. In [9], Niu, Yue and Wu used the union of Sidon spaces to construct cyclic subspace codes with more codewords and the minimum distance is still $2k-2$. In [14], Li and Liu gave a sufficient condition that the sum of several Sidon spaces is still a Sidon space, and provided a new idea for constructing Sidon spaces. For more methods of constructing cyclic subspace codes by Sidon spaces, see articles [14], [17].

In this letter, some new Sidon spaces can be constructed with primitive elements and the roots of some irreducible polynomials over finite fields. Moreover, several new kinds of cyclic subspace codes are presented, whose size is the multiple of $\frac{q^n-1}{q-1}$ and the minimum distance is still $2k-2$.

The structure of this letter is as follows. In Sect. 2, we state some relevant preliminaries which will be needed in our constructions. In Sect. 3, some new Sidon spaces are presented. In Sect. 4, based on these Sidon spaces, some cyclic subspace codes with new parameters are obtained. Finally, conclusions are presented in Sect. 5.

2. Preliminaries

Let $\mathbb{F}_q$ be a finite field with q elements and $\mathbb{F}_{q^n}$ be an extension field of degree n over $\mathbb{F}_q$, which can be viewed as a vector space of dimension n over $\mathbb{F}_q$.

Definition 2.1 ([11]) A subspace $\mathcal{U} \in \mathcal{G}_q(n, k)$ is called a Sidon space if for any nonzero elements $a, b, c, d \in \mathcal{U}$, if $ab = cd$, then $\{a\mathbb{F}_q, b\mathbb{F}_q\} = \{c\mathbb{F}_q, d\mathbb{F}_q\}$.

Proposition 2.2 shows that we can construct cyclic subspace codes by Sidon spaces.

Proposition 2.2 ([8]) For a subspace $\mathcal{U} \in \mathcal{G}_q(n, k)$, the

Manuscript received August 31, 2022.
Manuscript revised December 9, 2022.
Manuscript publicized January 30, 2023.

[†]The authors are with College of Sciences, Civil Aviation University of China, Tianjin, 300300, China.
[††]The author is with School of Sciences, Beijing University of Posts and Telecommunications, Beijing, 100876, China.
[†††]The author is with College of Science, Tianjin Key Lab for Advanced Signal Processing, Civil Aviation University of China, Tianjin, 300300, China.

*This research is supported by the National Natural Science Foundation of China (No. 11701558), the Scientific Research Project of Tianjin Education Commission (No. 2022KJ075), the Fundamental Research Funds for the Central Universities of China (No. 3122023QD25) and Foundation of Tianjin Key Lab for Advanced Signal Processing (No. 2022ASP-TJ02).

a) E-mail: xm-liu771216@163.com
b) E-mail: shitong1214@163.com
c) E-mail: myniu06080923@163.com (Corresponding author)
d) E-mail: linzhishen@mail.nankai.edu.cn
e) E-mail: gao_you@263.net

DOI: 10.1587/transfun.2022EAL2074

cyclic subspace code $orb(\mathcal{U})$ has size $\frac{q^n-1}{q-1}$ and minimum distance $2k-2$ if and only if $\mathcal{U}$ is a Sidon space.

Proposition 2.3 shows that we can construct cyclic subspace codes from the union of some Sidon spaces.

Proposition 2.3 ([8]) For any distinct subspaces $\mathcal{U}, \mathcal{V} \in \mathcal{G}_q(n,k)$, the following two conditions are equivalent.

(1) For any $\alpha \in \mathbb{F}_{q^n}^*$, $\dim(U \cap \alpha V) \leq 1$.

(2) For any nonzero elements $a, c \in \mathcal{U}$ and nonzero elements $b, d \in \mathcal{V}$, if $ab = cd$, then $\{a\mathbb{F}_q\} = \{c\mathbb{F}_q\}$ and $\{b\mathbb{F}_q\} = \{d\mathbb{F}_q\}$.

Conjecture 2.4 ([12], [15]) For any positive integers n, k and $n > 2k$, there exists a cyclic subspace code $C \subseteq \mathcal{G}_q(n,k)$ with size $\frac{q^n-1}{q-1}$ and minimum distance $2k-2$.

Lemma 2.5 ([10]) Suppose that l, k are two positive integers with $gcd(l,k) = 1$ and u, v, s, t are nonzero elements of $\mathbb{F}_{q^k}$ such that $uv = st$ and $u^{q^l}v = s^{q^l}t$. Then $\frac{u}{s} = \frac{t}{v} \in \mathbb{F}_q^*$.

Remark 2.6 From *Definition* 2.1, $\mathcal{U}$ is a Sidon space if for nonzero elements $a, b, c, d \in \mathcal{U}$, $ab = cd$, then $\{a\mathbb{F}_q, b\mathbb{F}_q\} = \{c\mathbb{F}_q, d\mathbb{F}_q\}$. There are two cases. When $\{a\mathbb{F}_q\} = \{c\mathbb{F}_q\}$ and $\{b\mathbb{F}_q\} = \{d\mathbb{F}_q\}$, there exist $\lambda_1, \lambda_2, \lambda_3, \lambda_4 \in \mathbb{F}_q$ such that $a\lambda_1 = c\lambda_2$ and $b\lambda_3 = d\lambda_4$. Then $\frac{a}{c} = \frac{\lambda_2}{\lambda_1} \in \mathbb{F}_q$ and $\frac{d}{b} = \frac{\lambda_3}{\lambda_4} \in \mathbb{F}_q$. By $ab = cd$, we have $\frac{a}{c} = \frac{d}{b} \in \mathbb{F}_q$. The other case could be similar to getting $\frac{a}{d} = \frac{c}{b} \in \mathbb{F}_q$. Therefore, $\{a\mathbb{F}_q, b\mathbb{F}_q\} = \{c\mathbb{F}_q, d\mathbb{F}_q\}$ is equivalent to $\frac{a}{c} = \frac{d}{b} \in \mathbb{F}_q$ or $\frac{a}{d} = \frac{c}{b} \in \mathbb{F}_q$.

3. Constructions of Sidon Space

In order to make the following proof more concise, we give some results.

Theorem 3.1 Suppose that t is a positive integer such that $\gcd(t,k) = 1$ and $u, u', v, v' \in \mathbb{F}_{q^k}^*$ are nonzero elements such that $uv = u'v'$, $uv^{q^t} + u^{q^t}v = u'v'^{q^t} + u'^{q^t}v'$. Then $\frac{u}{v'} = \frac{u'}{v} \in \mathbb{F}_q^*$.

Proof From $uv = u'v'$, suppose $\frac{u}{u'} = \frac{v'}{v} = \tau \in \mathbb{F}_{q^k}^*$. Replace the equation $uv^{q^t} + u^{q^t}v = u'v'^{q^t} + u'^{q^t}v'$ by $u = \tau u'$, $v' = \tau v$. We have

$$\tau u' v^{q^t} + \tau^{q^t} u'^{q^t} v = \tau^{q^t} u' v^{q^t} + \tau u'^{q^t} v.$$

Thus, $(\frac{u'}{v})^{q^t-1} = 1$, hence $\frac{u'}{v} \in \mathbb{F}_{q^t}$. Since $gcd(t,k) = 1$, we have $\frac{u'}{v} \in \mathbb{F}_q^*$. □

Now we construct Sidon spaces with the roots of some irreducible polynomials over finite fields.

Theorem 3.2 Let n, k, m, t be positive integers and $k \mid m \mid n$. Let $\gamma \in \mathbb{F}_{q^m}^*$ be a root of an irreducible polynomial of degree $\frac{m}{k} \geq 3$ over $\mathbb{F}_{q^k}$, $\xi \in \mathbb{F}_{q^n}^*$ be a root of an irreducible polynomial of degree $\frac{n}{m} \geq 3$ over $\mathbb{F}_{q^m}$. Then

$$\mathcal{U} = \{u + u^q\gamma + u^{q^t}\xi \mid u \in \mathbb{F}_{q^k}\}$$

is a Sidon space with dimension k.

Proof Now we check whether $\mathcal{U}$ is a Sidon space by *Definition* 2.1. Let $\alpha = u + u^q\gamma + u^{q^t}\xi$, $\alpha' = u' + u'^q\gamma + u'^{q^t}\xi$, $\beta = v + v^q\gamma + v^{q^t}\xi$ and $\beta' = v' + v'^q\gamma + v'^{q^t}\xi$ be four nonzero elements in $\mathcal{U}$ such that $\alpha\beta = \alpha'\beta'$, where $u, u', v, v' \in \mathbb{F}_{q^k}^*$.

Since $\frac{m}{k} \geq 3$ and $\frac{n}{m} \geq 3$, we know that $\{1, \gamma, \xi, \gamma\xi, \gamma^2, \xi^2\}$ is a linear independent set over $\mathbb{F}_{q^k}$. By comparing and simplifying their coefficients in $\alpha\beta = \alpha'\beta'$ after expansion, we deduce that

$$\begin{cases} uv = u'v' \\ uv^q + u^q v = u'v'^q + u'^q v' \\ uv^{q^t} + u^{q^t}v = u'v'^{q^t} + u'^{q^t}v' \\ u^q v^{q^t} + u^{q^t}v^q = u'^q v'^{q^t} + u'^{q^t}v'^q. \end{cases} \tag{1}$$

From $uv = u'v'$, suppose $\frac{u}{u'} = \frac{v'}{v} = \tau \in \mathbb{F}_{q^k}^*$. Replace the equation $uv^q + u^q v = u'v'^q + u'^q v'$ by $u = \tau u'$, $v' = \tau v$. Hence

$$\tau u' v^q + \tau^q u'^q v = \tau^q u' v^q + \tau u'^q v.$$

We have $(\frac{u'}{v})^{q-1} = 1$, so $\frac{u'}{v} \in \mathbb{F}_q^*$. Suppose $\frac{u'}{v} = \frac{u}{v'} = \tau' \in \mathbb{F}_q^*$. Replace the equation $\frac{\alpha}{\beta'} = \frac{u + u^q\gamma + u^{q^t}\xi}{v' + v'^q\gamma + v'^{q^t}\xi}$ by $u' = \tau' v$, $u = \tau' v'$. We have $\frac{\alpha}{\beta'} = \tau' \in \mathbb{F}_q^*$, hence $\frac{\alpha}{\beta'} = \frac{\alpha'}{\beta} = \tau' \in \mathbb{F}_q^*$. By *Remark* 2.6, $\mathcal{U}$ is a Sidon space.

It is evident that for any $u \in \mathbb{F}_{q^k}$, there is a unique $\alpha \in \mathcal{U}$ corresponding to it. Therefore, $\mathcal{U}$ has q^k distinct elements. Since $\mathbb{F}_{q^k}$ can be viewed as a vector space of dimension k over $\mathbb{F}_q$, we know that $\mathcal{U}$ is a $\mathbb{F}_q$−subspace of dimension k.

Therefore, $\mathcal{U}$ is a Sidon space with dimension k. □

Remark 3.3 The conditions are the same as *Theorem* 3.2. Similarly, $\mathcal{V} = \{u^{q^t} + u^q\gamma + u\xi \mid u \in \mathbb{F}_{q^k}\}$ is a Sidon space with dimension k.

We introduce some notations that will be used.

Definition 3.4 For three positive integers k, m, n and $k|m|n$. Let q be a prime power and ω be a primitive element in $\mathbb{F}_{q^k}$. Let $\gamma \in \mathbb{F}_{q^m}^*$ be a root of an irreducible polynomial of degree $\frac{m}{k} \geq 3$ over $\mathbb{F}_{q^k}$ and $\xi \in \mathbb{F}_{q^n}^*$ be a root of an irreducible polynomial of degree $\frac{n}{m} \geq 3$ over $\mathbb{F}_{q^m}$. Set $\rho := \lceil \frac{m}{2k} \rceil - 1$, set $\theta := \lceil \frac{n}{2m} \rceil - 1$. We define: $\gamma_{ij} = \omega^i\gamma^j$, $\xi_{ir} = \omega^i\xi^r$, where $0 \leq i \leq q^k - 2, 1 \leq j \leq \rho, 1 \leq r \leq \theta$.

Then we construct Sidon spaces consisting of primitive elements and the roots of irreducible polynomials over finite fields.

Theorem 3.5 Let i, j, r be fixed integers such that $0 \leq i \leq q^k - 2, 1 \leq j \leq \rho, 1 \leq r \leq \theta$ and let γ_{ij}, ξ_{ir} be as in *Definition* 3.4. Let t be a positive integer such that $\gcd(t,k) = 1$. Then

$$\mathcal{U}_{i,j,r} = \{u + u\gamma_{ij} + u^{q^t}\xi_{ir} \mid u \in \mathbb{F}_{q^k}\}$$

is a Sidon space with dimension k.

Proof Now we check whether $\mathcal{U}_{i,j,r}$ is a Sidon space by *Definition* 2.7. Let $\alpha = u + u\gamma_{ij} + u^{q^t}\xi_{ir}$, $\alpha' = u' + u'\gamma_{ij} + u'^{q^t}\xi_{ir}$, $\beta = v + v\gamma_{ij} + v^{q^t}\xi_{ir}$, $\beta' = v' + v'\gamma_{ij} + v'^{q^t}\xi_{ir}$ be four nonzero elements in $\mathcal{U}_{i,j,r}$ such that $\alpha\beta = \alpha'\beta'$, where $u, u', v, v' \in \mathbb{F}_{q^k}^*$.

Since $1 \leq j \leq \rho, 1 \leq r \leq \theta$, we know that $\{1, \gamma^j, \gamma^{2j}, \xi^r, \xi^{2r}, \gamma^j\xi^r\}$ is a linear independent set over $\mathbb{F}_{q^k}$. Comparing their coefficients in $\alpha\beta = \alpha'\beta'$ after expansion, we deduce that

$$\begin{cases} uv = u'v' \\ w^i(uv + uv) = w^i(u'v' + u'v') \\ w^{2i}uv = w^{2i}u'v' \\ w^i(uv^{q^t} + u^{q^t}v) = w^i(u'v'^{q^t} + u'^{q^t}v') \\ w^{2i}(uv)^{q^t} = w^{2i}(u'v')^{q^t} \\ w^{2i}(uv^{q^t} + u^{q^t}v) = w^{2i}(u'v'^{q^t} + u'^{q^t}v'). \end{cases}$$

Since ω be a primitive element in $\mathbb{F}_{q^k}$, $0 \le i \le q^k - 2$, we know that $w^i, w^{2i} \neq 0$. Upon simplification we have

$$\begin{cases} uv = u'v' \\ uv^{q^t} + u^{q^t}v = u'v'^{q^t} + u'^{q^t}v'. \end{cases} \tag{2}$$

By *Theorem* 3.1, we have $\frac{u}{v'} = \frac{u'}{v} \in \mathbb{F}_q^*$. Hence $\frac{\alpha}{\beta'} = \frac{\alpha'}{\beta} \in \mathbb{F}_q^*$.

Therefore, $\mathcal{U}_{i,j,r} \in \mathcal{G}_q(n,k)$ is a Sidon space. □

Theorem 3.6 Let j, r be fixed integers such that $1 \le j \le \rho$, $1 \le r \le \theta$ and let γ, ξ be as in *Definition* 3.4. Let t be a positive integer such that $\gcd(t,k) = 1$. Then

$$\mathcal{U}_{q^k-1,j,r} = \{u^{q^t} + u\gamma^j + u\xi^r \mid u \in \mathbb{F}_{q^k}\}$$

is a Sidon space with dimension k.

Proof The proof is similar to that of *Theorem* 3.5, and we omit the details. □

4. Subspace Codes via Sidon Spaces

Recall that the cyclic subspace code $orb(\mathcal{U})$ has size $\frac{q^n-1}{q-1}$ and minimum distance $2k-2$ if and only if $\mathcal{U}$ is a Sidon space. Now we construct some new cyclic subspace codes with size larger than $\frac{q^n-1}{q-1}$ and minimum distance still remain $2k-2$.

Theorem 4.1 The conditions are the same as *Theorem* 3.2 and *Remark* 3.3. Let $\mathcal{U} = \{u + u^q\gamma + u^{q^t}\xi \mid u \in \mathbb{F}_{q^k}\}$, $\mathcal{V} = \{v^{q^t} + v^q\gamma + v\xi \mid v \in \mathbb{F}_{q^k}\}$ and $\mathcal{X} = \{w\gamma + w^q\xi \mid w \in \mathbb{F}_{q^k}\}$. Define $C_1 = \{\lambda\mathcal{U} \mid \lambda \in \mathbb{F}_{q^n}^*\}$, $C_2 = \{\delta\mathcal{V} \mid \delta \in \mathbb{F}_{q^n}^*\}$ and $C_3 = \{\eta\mathcal{X} \mid \eta \in \mathbb{F}_{q^n}^*\}$. If $gcd(k,t) = 1$, then

$$C = C_1 \cup C_2 \cup C_3$$

is a cyclic subspace code with size $\frac{3(q^n-1)}{q-1}$ and minimum distance $2k-2$.

Proof It is easy to verify that $\mathcal{U}$, $\mathcal{V}$ and $\mathcal{X}$ are distinct Sidon spaces and C_1, C_2, C_3 are cyclic subspace codes of size $\frac{q^n-1}{q-1}$ and minimum distance $2k-2$ by Proposition 2.2. Therefore, $|C| = \frac{3(q^n-1)}{q-1}$.

To show that C has minimum distance $2k-2$, it remains to show that dim $(\mathcal{U} \cap \delta\mathcal{V}) \le 1$, dim $(\mathcal{V} \cap \eta\mathcal{X}) \le 1$ and dim $(\mathcal{X} \cap \lambda\mathcal{U}) \le 1$, where $\lambda, \delta, \eta \in \mathbb{F}_{q^n}^*$. By Proposition 2.3, it is equivalent to proof for nonzero elements $\alpha, \alpha' \in \mathcal{U}$, $\beta, \beta' \in \mathcal{V}$ and $\chi, \chi' \in \mathcal{X}$, if $\alpha\beta = \alpha'\beta'$, $\beta\chi = \beta'\chi'$, $\alpha\chi = \alpha'\chi'$, then

$$\{\alpha\mathbb{F}_q\} = \{\alpha'\mathbb{F}_q\} \text{ and } \{\beta\mathbb{F}_q\} = \{\beta'\mathbb{F}_q\},$$
$$\{\beta\mathbb{F}_q\} = \{\beta'\mathbb{F}_q\} \text{ and } \{\chi\mathbb{F}_q\} = \{\chi'\mathbb{F}_q\},$$
$$\{\alpha\mathbb{F}_q\} = \{\alpha'\mathbb{F}_q\} \text{ and } \{\chi\mathbb{F}_q\} = \{\chi'\mathbb{F}_q\}.$$

From *Remark* 2.6, we only need to prove

$$\frac{\alpha}{\alpha'} = \frac{\beta'}{\beta} \in \mathbb{F}_q^*. \tag{3}$$

$$\frac{\beta}{\beta'} = \frac{\chi'}{\chi} \in \mathbb{F}_q^*. \tag{4}$$

$$\frac{\alpha}{\alpha'} = \frac{\chi'}{\chi} \in \mathbb{F}_q^*. \tag{5}$$

Let $\alpha = u + u^q\gamma + u^{q^t}\xi$, $\alpha' = u' + u'^q\gamma + u'^{q^t}\xi$ be nonzero elements of $\mathcal{U}$, $\beta = v^{q^t} + v^q\gamma + v\xi$, $\beta' = v'^{q^t} + v'^q\gamma + v'\xi$ be nonzero elements of $\mathcal{V}$ such that $\alpha\beta = \alpha'\beta'$ where $u, u', v, v' \in \mathbb{F}_{q^k}^*$. Since $\frac{m}{k} \ge 3$ and $\frac{n}{m} \ge 3$, we know that $\{1, \gamma, \xi, \gamma\xi, \gamma^2, \xi^2\}$ is a linear independent set over $\mathbb{F}_{q^k}$. By comparing and simplifying their coefficients in $\alpha\beta = \alpha'\beta'$ after expansion, we deduce that

$$\begin{cases} uv^{q^t} = u'v'^{q^t} \\ uv^q + u^q v^{q^t} = u'v'^q + u'^q v'^{q^t} \\ uv = u'v' \\ u^q v + u^{q^t} v^q = u'^q v' + u'^{q^t} v'^q \\ u^{q^t} v = u'^{q^t} v'. \end{cases} \tag{6}$$

By Lemma 2.5 and the equation group (6), we have $\frac{u}{u'} = \frac{v'}{v} \in \mathbb{F}_q^*$. Suppose $\frac{u}{u'} = \frac{v'}{v} = \tau' \in \mathbb{F}_q^*$. Replace the equation $\frac{\alpha}{\alpha'} = \frac{u+u^q\gamma+u^{q^t}\xi}{u'+u'^q\gamma+u'^{q^t}\xi}$ by $u = \tau'u'$, $v' = \tau'v$, we have $\frac{\alpha}{\alpha'} = \tau' \in \mathbb{F}_q^*$. Since $\alpha\beta = \alpha'\beta'$, we have $\frac{\alpha}{\alpha'} = \frac{\beta'}{\beta} = \tau' \in \mathbb{F}_q^*$. Hence Eq. (3) holds.

Similar to the proof of Eq. (3), the Eqs. (4) and (5) hold.

To summarize, C is a cyclic subspace code with size $\frac{3(q^n-1)}{q-1}$ and minimum distance $2k-2$. □

Theorem 4.2 The conditions are the same as *Theorem* 3.5. For $0 \le i \le q^k-2, 1 \le j \le \rho, 1 \le r \le \theta$, set $\mathcal{U}_{i,j,r} = \{u + u\gamma_{ij} + u^{q^t}\xi_{ir} \mid u \in \mathbb{F}_{q^k}\}$. Define $C_{i,j,r} = \{\lambda\mathcal{U}_{i,j,r} | \lambda \in \mathbb{F}_{q^n}^*\}$ for each pair (i,j,r) correspondingly. Then the set

$$C_1 = \cup_{r=1}^{\theta} \cup_{j=1}^{\rho} \cup_{i=0}^{q^k-2} C_{i,j,r} \subseteq \mathcal{G}_q(n,k)$$

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

Proof Each of the $\mathcal{U}_{i,j,r}$ are Sidon spaces by *Theorem* 3.5 and each $C_{i,j,r}$ is a cyclic subspace code of size $\frac{q^n-1}{q-1}$ and minimum distance $2k-2$ by *Proposition* 2.2. To show that C_1 has minimum distance $2k-2$, it remains to show that dim $(\mathcal{U}_{i_1,j_1,r_1} \cap \lambda\mathcal{U}_{i_2,j_2,r_2}) \le 1$, where $\lambda \in \mathbb{F}_{q^n}^*$ and $(i_1, j_1, r_1) \neq (i_2, j_2, r_2)$.

We consider two separate cases, and establish the claim by utilizing *Proposition* 2.3.

Case 1: $i_1 \neq i_2$.

Let $\alpha = u + u\gamma_{i_1j_1} + u^{q^t}\xi_{i_1r_1}$, $\alpha' = u' + u'\gamma_{i_1j_1} + u'^{q^t}\xi_{i_1r_1}$ be nonzero elements of $\mathcal{U}_{i_1,j_1,r_1}$ and $\beta = v + v\gamma_{i_2j_2} + v^{q^t}\xi_{i_2r_2}$, $\beta' = v' + v'\gamma_{i_2j_2} + v'^{q^t}\xi_{i_2r_2}$ be nonzero elements of $\mathcal{U}_{i_2,j_2,r_2}$ such that $\alpha\beta = \alpha'\beta'$, where $u, u', v, v' \in \mathbb{F}_{q^k}^*$.

(a) If $j_1 \neq j_2, r_1 \neq r_2$. Since $1 \le j \le \rho$ and $1 \le r \le \theta$, we know that $\{1, \gamma^{j_1}, \gamma^{j_2}, \gamma^{j_1+j_2}, \xi^{r_1}, \xi^{r_2}, \xi^{r_1+r_2}, \gamma^{j_2}\xi^{r_1}, \gamma^{j_1}\xi^{r_2}\}$ is a linear independent set over $\mathbb{F}_{q^k}$. By comparing and simplifying their coefficients in $\alpha\beta = \alpha'\beta'$ after expansion, we deduce that

$$\begin{cases} uv = u'v' \\ uv^{q^t} = u'v'^{q^t} \\ u^{q^t}v = u'^{q^t}v'. \end{cases} \tag{7}$$

By *Lemma* 2.5 and the equation group (7), we have $\frac{u}{u'} = \frac{v'}{v} \in \mathbb{F}_q^*$. Hence $\frac{\alpha}{\alpha'} = \frac{\beta'}{\beta} \in \mathbb{F}_q^*$.

(b) If $j_1 = j_2 = j, r_1 \neq r_2$. Since $1 \leq j \leq \rho$ and $1 \leq r \leq \theta$, we know that $\{1, \gamma^j, \gamma^{2j}, \xi^{r_1}, \xi^{r_2}, \xi^{r_1+r_2}, \gamma^j\xi^{r_1}, \gamma^j\xi^{r_2}\}$ is a linear independent set over $\mathbb{F}_{q^k}$. This case is similar to the proof of *case a* and we omit it.

(c) If $j_1 \neq j_2, r_1 = r_2 = r$. Since $1 \leq j \leq \rho$ and $1 \leq r \leq \theta$, we know that $\{1, \gamma^{j_1}, \gamma^{j_2}, \gamma^{j_1+j_2}, \xi^r, \xi^{2r}, \gamma^{j_1}\xi^r, \gamma^{j_2}\xi^r\}$ is a linear independent set over $\mathbb{F}_{q^k}$. This case is similar to the proof of *case a* and we omit it.

(d) If $j_1 = j_2 = j$, $r_1 = r_2 = r$. Since $1 \leq j \leq \rho$ and $1 \leq r \leq \theta$, we know that $\{1, \gamma^j, \gamma^{2j}, \xi^r, \xi^{2r}, \gamma^j\xi^r\}$ is a linear independent set over $\mathbb{F}_{q^k}$. By comparing and simplifying their coefficients in $\alpha\beta = \alpha'\beta'$ after expansion, we deduce that

$$\begin{cases} uv = u'v' \\ uv^{q^t} + u^{q^t}v = u'v'^{q^t} + u'^{q^t}v'. \end{cases} \tag{8}$$

By *Theorem* 3.1 and the equation group (8), we have $\frac{u}{v'} = \frac{u'}{v} \in \mathbb{F}_q^*$. Hence $\frac{\alpha}{\beta'} = \frac{\alpha'}{\beta} \in \mathbb{F}_q^*$.

Case 2: $i_1 = i_2 = i$.

Let $\alpha = u + u\gamma_{ij_1} + u^{q^t}\xi_{ir_1}$, $\alpha' = u' + u'\gamma_{ij_1} + u'^{q^t}\xi_{ir_1}$ be nonzero elements of $\mathcal{U}_{i,j_1,r_1}$ and $\beta = v + v\gamma_{ij_2} + v^{q^t}\xi_{ir_2}$, $\beta' = v' + v'\gamma_{ij_2} + v'^{q^t}\xi_{ir_2}$ be nonzero elements of $\mathcal{U}_{i,j_2,r_2}$ such that $\alpha\beta = \alpha'\beta'$, where $u, u', v, v' \in \mathbb{F}_{q^k}^*$.

(e) If $j_1 \neq j_2, r_1 \neq r_2$, this case is similar to the proof of *case a* and we omit it.

(f) If $j_1 = j_2 = j, r_1 \neq r_2$, this case is similar to the proof of *case b* and we omit it.

(g) If $j_1 \neq j_2, r_1 = r_2 = r$, this case is similar to the proof of *case c* and we omit it.

To summarize, we have shown that C_1 has minimum distance $2k-2$. In particular, we have shown that the $\frac{\theta\rho(q^k-1)(q^n-1)}{q-1}$ elements of C_1 are distinct, so $|C_1| = \frac{\theta\rho(q^k-1)(q^n-1)}{q-1}$. □

Theorem 4.3 The conditions are the same as *Theorem* 3.6. For $1 \leq j \leq \rho, 1 \leq r \leq \theta$, set $\mathcal{U}_{q^k-1,j,r} = \{u^{q^t} + u^q\gamma^j + u\xi^r \mid u \in \mathbb{F}_q\}$. Define $C_{q^k-1,j,r} = \{\lambda\mathcal{U}_{q^k-1,j,r} | \lambda \in \mathbb{F}_{q^n}^*\}$ for each pair (j, r) correspondingly. Then the set

$$C_2 = \cup_{r=1}^{\theta} \cup_{j=1}^{\rho} C_{q^k-1,j,r} \subseteq \mathcal{G}_q(n, k)$$

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

Proof Each of the $\mathcal{U}_{q^k-1,j,r}$ are Sidon spaces by *Theorem* 3.6 and each $C_{q^k-1,j,r}$ is a cyclic subspace code of size $\frac{q^n-1}{q-1}$ and minimum distance $2k-2$ by *Proposition* 2.2. To show that C_2 has minimum distance $2k-2$, it remains to show that $\dim(\mathcal{U}_{q^k-1,j_1,r_1} \cap \lambda\mathcal{U}_{q^k-1,j_2,r_2}) \leq 1$, where $\lambda \in \mathbb{F}_{q^n}^*$ and $(j_1, r_1) \neq (j_2, r_2)$. Let $\alpha = u^{q^t} + u\gamma^{j_1} + u\xi^{r_1}$, $\alpha' = u'^{q^t} + u'\gamma^{j_1} + u'\xi^{r_1}$ be nonzero elements of $\mathcal{U}_{q^k-1,j_1,r_1}$ and $\beta = v^{q^t} + v\gamma^{j_2} + v\xi^{r_2}, \beta' = v'^{q^t} + v'\gamma^{j_2} + v'\xi^{r_2}$ be nonzero elements of $\mathcal{U}_{q^k-1,j_2,r_2}$ such that $\alpha\beta = \alpha'\beta'$, where $u, u', v, v' \in \mathbb{F}_{q^k}^*$.

We consider three separate cases, and establish the claim by utilizing *Proposition* 2.3.

Case 1: $j_1 \neq j_2, r_1 \neq r_2$.

Since $1 \leq j \leq \rho$ and $1 \leq r \leq \theta$, we know that $\{1, \gamma^{j_1}, \gamma^{j_2}, \gamma^{j_1+j_2}, \xi^{r_1}, \xi^{r_2}, \xi^{r_1+r_2}, \gamma^{j_2}\xi^{r_1}, \gamma^{j_1}\xi^{r_2}\}$ is a linear independent set over $\mathbb{F}_{q^k}$. By comparing and simplifying their coefficients in $\alpha\beta = \alpha'\beta'$ after expansion, we deduce that

$$\begin{cases} uv = u'v' \\ uv^{q^t} = u'v'^{q^t} \\ u^{q^t}v = u'^{q^t}v'. \end{cases} \tag{9}$$

By *Lemma* 2.5 and the equation group (9), we have $\frac{u}{u'} = \frac{v'}{v} \in \mathbb{F}_q^*$. Hence $\frac{\alpha}{\alpha'} = \frac{\beta'}{\beta} \in \mathbb{F}_q^*$.

Case 2: $j_1 = j_2 = j, r_1 \neq r_2$. This case is similar to the proof of *case b* form *Theorem* 4.2 and we omit it.

Case 3: $j_1 \neq j_2, r_1 = r_2 = r$. This case is similar to the proof of *case c* form *Theorem* 4.2 and we omit it.

To summarize, we have shown that C_2 has minimum distance $2k-2$. In particular, we have shown that the $\frac{\theta\rho(q^n-1)}{q-1}$ elements of C_2 are distinct, so $|C_2| = \frac{\theta\rho(q^n-1)}{q-1}$. □

Theorem 4.4 The conditions are the same as *Theorem* 4.2 and *Theorem* 4.3. Then the set

$$C = C_1 \cup C_2$$

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

Proof It is evident that $|C| = \frac{\theta\rho q^k(q^n-1)}{q-1}$. To show that C has minimum distance $2k-2$, it remains to show that $\dim(\mathcal{U}_{i_1,j_1,r_1} \cap \lambda\mathcal{U}_{q^k-1,j_2,r_2}) \leq 1$, where $\lambda \in \mathbb{F}_{q^n}^*$ and $0 \leq i_1 \leq q^k-2, 1 \leq j_1, j_2 \leq \rho, 1 \leq r_1, r_2 \leq \theta$. The proof is similar to *Theorem* 4.3, and we omit the details. □

Example 4.5 Take $q = k = 3$. Let ω be a primitive element in $\mathbb{F}_{3^3}$. Let $\gamma \in \mathbb{F}_{3^9}^*$ be a root of an irreducible polynomial over $\mathbb{F}_{3^3}$ and $\xi \in \mathbb{F}_{3^{45}}^*$ be a root of an irreducible polynomial over $\mathbb{F}_{3^9}$. Then $\rho = \lceil\frac{9}{2\times3}\rceil - 1 = 1, \theta = \lceil\frac{45}{2\times9}\rceil - 1 = 2$. *Theorem* 4.4 thus permits us to produce a cyclic subspace code with size $\frac{\theta\rho q^k(q^n-1)}{q-1} = 3^3(3^{45}-1)$. The cardinality is lager than 3^9-1 in *Theorem* 4.3 of [14] and $\frac{3^3(3^9-1)}{2}$ in *Theorem* 3.1 of [10], and the minimum distance is still $2k-2 = 4$.

5. Conclusion

In this letter, we present several new Sidon spaces through primitive elements and distinct roots of irreducible polynomials over finite fields. Moreover, through the union of Sidon spaces, cyclic subspace codes of size $\frac{3(q^n-1)}{q-1}$ and $\frac{\theta\rho q^k(q^n-1)}{q-1}$ are obtained, and the minimum distance is still $2k-2$. This yields cyclic subspace codes with new cardinalities by comparing with the known constructions in [14] and [10].

References

[1] T. Etzion and A. Vardy, "Error-correcting codes in projective space," IEEE Trans. Inf. Theory, vol.57, no.2, pp.1165–1173, Feb. 2011.

[2] R. Koetter 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.

[3] 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, March 2016.

[4] R. Ahlswede, Ning Cai, S.-Y.R. Li, and R.W. Yeung, "Network information flow," IEEE Trans. Inf. Theory, vol.46, no.4, pp.1204–1216, July 2000.

[5] B. Chen and H. Liu, "Constructions of cyclic constant dimension codes," Des. Codes Cryptogr., vol.86, no.6, pp.1267–1279, July 2017.

[6] 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.

[7] K. Otal and F. Özbudak, "Cyclic subspace codes via subspace polynomials," Des. Codes Cryptogr., vol.85, no.2, pp.191–204, Nov. 2016.

[8] R.M. Roth, N. Raviv, and I. Tamo, "Construction of Sidon spaces with applications to coding," IEEE Trans. Inf. Theory, vol.64, no.6, pp.4412–4422, June 2018.

[9] Y. Niu, Q. Yue, and Y. Wu, "Several kinds of large cyclic subspace codes via Sidon spaces," Discrete Math., vol.343, no.5, 111788, May 2020.

[10] T. Feng and Y. Wang, "New constructions of large cyclic subspace codes and Sidon spaces," Discrete Math, vol.344, no.4, 112273, April 2021.

[11] C. Bachoc, O. Serra, and G. Zemor, "An analogue of Vosper's theorem for extension fields," Math. Proc. Cambridge Philos. Soc., vol.163, no.3, pp.423–452, Nov. 2017.

[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, May 2015.

[13] H. Gluesing-Luerssen and H. Lehmann, "Distance distributions of cyclic orbit codes," Des. Codes Cryptogr., vol.89, no.3, pp.447–470, Jan.2021.

[14] Y. Li and H. Liu, "Cyclic subspace codes via the sum of Sidon spaces," arXiv: 2105.12520v1 [cs.IT], 2021.

[15] A. Trautmann, F. Manganiello, M. Braun, and J. Rosenthal, "Cyclic orbit codes," IEEE Trans. Inf. Theory, vol.59, no.11, pp.7386–7404, Nov. 2013.

[16] E. Gabidulin, N. Pilipchuk, and M. Bossert, "Decoding of random network codes," Probl. Inf. Transm., vol.46, no.4, pp.300–320, Jan. 2010.

[17] H. Zhang and X. Cao, "Constructions of Sidon spaces and cyclic subspace codes," Front. Math. China, vol.17, pp.275–288, May 2022.

[18] Y. Gao and G. Wang, "Error-correcting codes in attenuated space over finite fields," Finite Fields Appl., vol.33, pp.103–117, May 2015.

[19] M. Braun, "Construction of linear codes with large minimum distance," IEEE Trans. Inf. Theory, vol.50, no.8, pp.1687–1691, Aug. 2004.

[20] W. Zhao and X. Tang, "A characterization of cyclic subspace codes via subspace polynomials," Finite Fields Appl., vol.57, pp.1–12, May 2019.

[21] G. Wang, M. Niu, and F. Fu, "Deterministic construction of compressed sensing matrices from constant dimension codes," Discrete Appl. Math., vol.285, pp.9–17, Oct. 2020.