Journal of Algebraic Combinatorics
https://doi.org/10.1007/s10801-021-01069-z

New constructions of Sidon spaces

Tao Zhang[1] · **Gennian Ge**[2]

Received: 19 November 2019 / Accepted: 12 August 2021

Abstract
Sidon spaces can be used to characterize certain multiplicative properties of subspaces. They also have important applications in cyclic subspace codes and Sidon sets. In this paper, we give three new constructions of Sidon spaces. Our results can be applied to cyclic subspace codes. As a result, we obtain some new optimal cyclic subspace codes.

Keywords Sidon space · Cyclic subspace code · Sidon set

Mathematics Subject Classification 94B60 · 11T71

1 Introduction

According to Erdős [6], in 1932 Simon Sidon asked him about the growing of infinite sets $a_1 < a_2 < \dots$ with the property that the sums $a_i + a_j$ $(i \leq j)$ are distinct. Later Erdős named them Sidon sets. Sidon sets have attracted considerable attention over the years and many constructions are known. For a survey on Sidon sets, the reader is referred to [14].

In the past few years, interest has been growing in q-analogs of combinatorial structures, in which vectors and subsets are replaced by vector spaces over a finite field. Examples of such q-analog structures are constant dimension codes [11], q-

T. Zhang: Research supported by the National Natural Science Foundation of China under Grant No. 11801109.
G. Ge: Research supported by the National Natural Science Foundation of China under Grant No. 11971325, National Key Research and Development Program of China under Grant Nos. 2020YFA0712100 and 2018YFA0704703, and Beijing Scholars Program.

✉ Tao Zhang
taozhang@gzhu.edu.cn

[1] School of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China

[2] School of Mathematics Sciences, Capital Normal University, Beijing 100048, China

Steiner systems [4], t-designs over finite fields [10], large sets of subspace designs [5]. But what has begun as a purely theoretical area of research has recently found an important application to random network coding, starting with the work of Kötter and Kschischang [12]. After their work, the theory of subspace codes and designs has developed rapidly, see [1,7–9,11,16–20] and the references therein.

In this paper, we study Sidon spaces, which can be seen as the q-analogs of Sidon sets. Sidon spaces were first introduced in [2] for studying certain multiplicative properties of subspaces. Let $\mathbb{F}_q$ be the finite field of size q. Let $\mathbb{F}_{q^n}$ be the field extension of degree n over $\mathbb{F}_q$, which can be seen as a vector space of dimension n over $\mathbb{F}_q$. For nonnegative integers $k \leq n$, the set of all k-dimensional subspaces of $\mathbb{F}_{q^n}$ forms a Grassmannian space over $\mathbb{F}_q$, which is denoted by $\mathcal{G}_q(n,k)$. For $a \in \mathbb{F}_{q^n}$, let $a\mathbb{F}_q := \{a\lambda : \lambda \in \mathbb{F}_q\}$. Now we give the definition of Sidon space.

Definition 1.1 A subspace $V \in \mathcal{G}_q(n,k)$ is called a Sidon space if for all nonzero elements $a, b, c, d \in V$, if $ab = cd$ then $\{a\mathbb{F}_q, b\mathbb{F}_q\} = \{c\mathbb{F}_q, d\mathbb{F}_q\}$.

From the definition, it is easy to see that a Sidon space is a subspace $V \in \mathcal{G}_q(n,k)$ such that the product of any two nonzero elements of V has a unique factorization over V up to a constant multiplier from $\mathbb{F}_q$. In [15], the authors gave several constructions of Sidon spaces. In particular, they presented a construction of minimum-span Sidon spaces for prime power q and positive integers $k|n$. They also gave three explicit constructions of maximum-span Sidon spaces for certain parameters and provided an existence result of max-span Sidon spaces for $n \geq \binom{k+1}{2}$ by probabilistic method.

Besides being interesting combinatorial objects, Sidon spaces also have applications in cyclic subspace codes. A constant dimension code is a subset of $\mathcal{G}_q(n,k)$ under the subspace metric $d(U,V) = 2k - 2\dim(U \cap V)$. Cyclic subspace codes were introduced in [9] for the purpose of finding good constant dimension codes, and they may be applied efficiently for coding since cyclic subspace codes have efficient encoding and decoding algorithms [21]. For a subspace $V \in \mathcal{G}_q(n,k)$ and $a \in \mathbb{F}_{q^n}^*$, the cyclic shift of V by a is $aV = \{av : v \in V\}$. The set aV is clearly a subspace with the same dimension as V. A subspace code C is called cyclic if for every $a \in \mathbb{F}_{q^n}^*$ and every $V \in C$, we have $aV \in C$.

The orbit of a subspace $V \in \mathcal{G}_q(n,k)$ is $\mathrm{orb}(V) = \{aV : a \in \mathbb{F}_{q^n}^*\}$, and its cardinality is $(q^n-1)/(q^t-1)$ for some integer t dividing n. Then a cyclic subspace code is the union of some orbits of subspaces. In the following, we will only consider the cyclic subspace code with one orbit, and then the cardinality of such cyclic subspace code must have the form $(q^n-1)/(q^t-1)$ for some integer t dividing n.

For a cyclic subspace code $C \subseteq \mathcal{G}_q(n,k)$, we must have $d(C) \leq 2k$. For $d(C) = 2k$ and $k|n$, since $\mathbb{F}_{q^k}^*$ is a multiplicative subgroup of $\mathbb{F}_{q^n}^*$ and its cosets are $\{a\mathbb{F}_{q^k}^* : a \in \mathbb{F}_{q^n}^*\}$, hence $\{a\mathbb{F}_{q^k} : a \in \mathbb{F}_{q^n}^*\}$ is a cyclic subspace code with size $(q^n-1)/(q^k-1)$ and minimum distance $2k$. The next case is $d(C) = 2k-2$, and we have the following conjecture.

Conjecture 1 [21] For any prime power q and positive integers k and $n \geq 2k$, there exists a cyclic subspace code $C \subseteq \mathcal{G}_q(n,k)$ of minimum distance $2k-2$ and cardinality $(q^n-1)/(q-1)$.

In [3], the authors gave some constructions of cyclic subspace codes $C \subseteq \mathcal{G}_q(n,k)$ with minimum distance $2k-2$ and cardinality $(q^n-1)/(q-1)$ from certain linearized polynomials. However, the relation between n and k in the constructions of [3] is in general not known. From the connection between Sidon spaces $V \in \mathcal{G}_q(n,k)$ and cyclic subspace codes $C \subseteq \mathcal{G}_q(n,k)$ with minimum distance $2k-2$ and cardinality $(q^n-1)/(q-1)$ (see Theorem 2.4), Roth et al. [15] resolved the following cases of Conjecture 1:

- ([15, Theorem 12]) $q \geq 3$, n is even and $n \geq 2k$;
- ([15, Theorem 16]) $k \leq t$, where $t|n$ and $t < n/2$;
- ([15, Theorem 19]) $n \geq 6$ and $k \leq \lfloor \frac{n-2}{4} \rfloor$.

In this paper, we give three new constructions of Sidon spaces. In particular, these constructions can be applied to cyclic subspace codes and we can resolve some cases of Conjecture 1. This paper is organized as follows. In Sect. 2, we state some basics of Sidon spaces and the applications of Sidon spaces in cyclic subspace codes and Sidon sets. In Sect. 3, we give three new constructions of Sidon spaces. Section 4 concludes our paper.

2 Preliminaries

The following theorem gives the connection between Sidon spaces and cyclic subspace codes.

Theorem 2.1 *[15] For a subspace $V \in \mathcal{G}_q(n,k)$, the set $orb(V)$ is of size $(q^n-1)/(q-1)$ and minimum distance $2k-2$, if and only if V is a Sidon space.*

Then we have the following remark.

Remark 2.2 1. If $V \in \mathcal{G}_q(n,k)$ is a Sidon space then $2k \leq n$ whenever $k \geq 3$.
2. The existence of a Sidon space in $\mathcal{G}_q(n,k)$ implies that of Sidon spaces in $G_q(n,t)$, for any $1 \leq t \leq k$. Hence, for Conjecture 1, given a positive integer n, we only need to find the largest integer k such that there exists a cyclic subspace code $C \subseteq \mathcal{G}_q(n,k)$ of minimum distance $2k-2$ and cardinality $(q^n-1)/(q-1)$.

Sidon spaces are closely related to Sidon sets. We first give the formal definition of Sidon set.

Definition 2.3 A subset $\{n_1, n_2, \ldots, n_k\}$ of an Abelian group G is called a Sidon set if all sums $n_i + n_j$ $(1 \leq i \leq j \leq k)$ are unique.

The following two theorems show that Sidon sets can be used to construct Sidon spaces, and vice versa. Here we denote $[m] := \{1, 2, \ldots, m\}$.

Theorem 2.4 *[15] Let $S = \{n_1, n_2, \ldots, n_k\} \subseteq [m]$ be a Sidon set in $\mathbb{Z}$ such that $m = k^2(1 + o_k(1))$. Then, for an integer $n > 2m$ and a proper element γ of $\mathbb{F}_{q^n}$ (that does not belong to any proper subfield of $\mathbb{F}_{q^n}$), $V := \langle \{\gamma^{n_i} : i \in [k]\} \rangle$ is a max-span Sidon space.*

Theorem 2.5 *[15] If $V \in \mathcal{G}_q(n,k)$ is a Sidon space, γ is a primitive element in $\mathbb{F}_{q^n}$, and $A = \{\gamma^{n_i} : i \in [(q^k-1)/(q-1)]\}$ is a set of nonzero representatives of all one-dimensional subspaces of V, then $S = \{n_i : \gamma^{n_i} \in A\}$ is a Sidon set in $\mathbb{Z}_{(q^n-1)/(q-1)}$.*

Hence, the constructions in this paper can be used to construct cyclic subspace codes and Sidon sets.

3 Constructions of sidon spaces

In this section, we provide three new constructions of Sidon spaces. The first two constructions are based on subfields of finite fields. The third construction of Sidon spaces is in $\mathbb{F}_{q^n}$, where $\mathbb{F}_{q^n}$ does not need to contain large subfields.

3.1 Construction I

The following lemma can be found in [13].

Lemma 3.1 *[13, Theorem 2.5] For every prime p and every positive integer n, there exists a finite field with p^n elements. Any finite field with $q = p^n$ elements is isomorphic to the splitting field of $x^q - x$ over $\mathbb{F}_p$.*

Now we give our first construction, which is based on the subfields of finite fields.

Theorem 3.2 *Let k, n be integers such that $k|n$ and $\frac{n}{k} \geq 9$, q be a prime power, and $\gamma \in \mathbb{F}_{q^n}$ be a root of an irreducible polynomial of degree $\frac{n}{k}$ over $\mathbb{F}_{q^k}$. Set $V = \{u_1 + u_1^q\gamma + u_2\gamma^2 + u_2^q\gamma^4 : u_1, u_2 \in \mathbb{F}_{q^k}\}$, then $V \in \mathcal{G}_q(n, 2k)$ is a Sidon space.*

Proof Suppose $(u_1+u_1^q\gamma+u_2\gamma^2+u_2^q\gamma^4)(v_1+v_1^q\gamma+v_2\gamma^2+v_2^q\gamma^4) = (s_1+s_1^q\gamma+s_2\gamma^2+s_2^q\gamma^4)(t_1+t_1^q\gamma+t_2\gamma^2+t_2^q\gamma^4)$, where $u_1, u_2, v_1, v_2, s_1, s_2, t_1, t_2 \in \mathbb{F}_{q^k}$ and $u_1+u_1^q\gamma+u_2\gamma^2+u_2^q\gamma^4$, $v_1+v_1^q\gamma+v_2\gamma^2+v_2^q\gamma^4$, $s_1+s_1^q\gamma+s_2\gamma^2+s_2^q\gamma^4$, $t_1+t_1^q\gamma+t_2\gamma^2+t_2^q\gamma^4$ are all nonzero. Denote

$$\bar{u} := u_1 + u_1^q\gamma + u_2\gamma^2 + u_2^q\gamma^4, \qquad \bar{v} := v_1 + v_1^q\gamma + v_2\gamma^2 + v_2^q\gamma^4,$$
$$\bar{s} := s_1 + s_1^q\gamma + s_2\gamma^2 + s_2^q\gamma^4, \qquad \bar{t} := t_1 + t_1^q\gamma + t_2\gamma^2 + t_2^q\gamma^4.$$

Since $\gamma \in \mathbb{F}_{q^n}$ is a root of an irreducible polynomial of degree $\frac{n}{k}$ over $\mathbb{F}_{q^k}$, where $\frac{n}{k} \geq 9$, then we have

$$u_1v_1 = s_1t_1, \tag{1}$$
$$u_1v_1^q + u_1^qv_1 = s_1t_1^q + s_1^qt_1, \tag{2}$$
$$u_1v_2 + u_1^qv_1^q + u_2v_1 = s_1t_2 + s_1^qt_1^q + s_2t_1, \tag{3}$$
$$u_1^qv_2 + u_2v_1^q = s_1^qt_2 + s_2t_1^q, \tag{4}$$
$$u_1v_2^q + u_2v_2 + u_2^qv_1 = s_1t_2^q + s_2t_2 + s_2^qt_1, \tag{5}$$
$$u_1^qv_2^q + u_2^qv_1^q = s_1^qt_2^q + s_2^qt_1^q, \tag{6}$$

$$u_2v_2^q + u_2^q v_2 = s_2t_2^q + s_2^q t_2, \tag{7}$$
$$u_2^q v_2^q = s_2^q t_2^q. \tag{8}$$

We divide our discussion into two cases.

Case 1: At least one of $u_1, u_2, v_1, v_2, s_1, s_2, t_1, t_2$ is 0.

Suppose $u_1 = 0$. By Eq. (1), without loss of generality, we assume $s_1 = 0$. Since $\bar{u}, \bar{s}$ are both nonzero, we have u_2, s_2 to be nonzero. Then we can get that

$$u_2v_1 = s_2t_1 \text{ (from (3))}, \tag{9}$$
$$u_2v_1^q = s_2t_1^q \text{ (from (4))}, \tag{10}$$
$$u_2^q v_1 = s_2^q t_1 \text{ (from (5) and (8))}, \tag{11}$$
$$u_2v_2^q + u_2^q v_2 = s_2t_2^q + s_2^q t_2 \text{ (from (7))}, \tag{12}$$
$$u_2^q v_2^q = s_2^q t_2^q \text{ (from (8))}. \tag{13}$$

Subcase 1.1: v_1, t_1 **are both nonzero.**

By Eqs. (9) and (11), we have $\frac{u_2}{s_2} = \frac{t_1}{v_1} = \frac{u_2^q}{s_2^q}$. By Lemma 3.1, we have $\frac{u_2}{s_2} \in \mathbb{F}_q$. Then $u_2\gamma^2 + u_2^q\gamma^4 = \frac{u_2}{s_2}s_2\gamma^2 + \frac{u_2^q}{s_2^q}s_2^q\gamma^4 = \frac{u_2}{s_2}(s_2\gamma^2 + s_2^q\gamma^4)$. Note that $u_1 = s_1 = 0$ and since $\bar{u}\bar{v} = \bar{s}\bar{t}$, we have that $\{\bar{u}\mathbb{F}_q, \bar{v}\mathbb{F}_q\} = \{\bar{s}\mathbb{F}_q, \bar{t}\mathbb{F}_q\}$.

Subcase 1.2: $v_1 = 0$.

By Eq. (9), we have $t_1 = 0$, and then v_2, t_2 are both nonzero. Note that raising to the q-th power is an injective function, then from Eq. (13), we have $u_2v_2 = s_2t_2$. Let $a := \frac{u_2}{s_2}$, then $t_2 = av_2$. Substituting them into Eq. (12), we have

$$as_2v_2^q + a^q s_2^q v_2 = a^q s_2 v_2^q + as_2^q v_2.$$

It follows that $(a - a^q)(s_2v_2^q - s_2^q v_2) = 0$. Then $a = a^q$ or $\frac{s_2}{v_2} = \frac{s_2^q}{v_2^q}$. By Lemma 3.1, we have $a \in \mathbb{F}_q$ or $\frac{s_2}{v_2} \in \mathbb{F}_q$, which implies that $u_2\gamma^2 + u_2^q\gamma^4 = a(s_2\gamma^2 + s_2^q\gamma^4)$ or $s_2\gamma^2 + s_2^q\gamma^4 = \frac{s_2}{v_2}(v_2\gamma^2 + v_2^q\gamma^4)$. Note that $u_1 = s_1 = v_1 = t_1 = 0$ and since $\bar{u}\bar{v} = \bar{s}\bar{t}$, we have that $\{\bar{u}\mathbb{F}_q, \bar{v}\mathbb{F}_q\} = \{\bar{s}\mathbb{F}_q, \bar{t}\mathbb{F}_q\}$.

Case 2: None of $u_1, u_2, v_1, v_2, s_1, s_2, t_1, t_2$ is 0.

Let $a := \frac{u_1}{s_1}$, then from Eq. (1), we have $t_1 = av_1$. Substituting them into Eq. (2), we have

It follows that $$as_1v_1^q + a^q s_1^q v_1 = a^q s_1 v_1^q + as_1^q v_1.$$

$$(a - a^q)(s_1v_1^q - s_1^q v_1) = 0.$$

Then $a = a^q$ or $\frac{s_1}{v_1} = \frac{s_1^q}{v_1^q}$. By Lemma 3.1, we have $\frac{u_1}{s_1} = \frac{t_1}{v_1} \in \mathbb{F}_q$ or $\frac{u_1}{t_1} = \frac{s_1}{v_1} \in \mathbb{F}_q$. Similarly, from Eqs. (7) and (8), we can get that $\frac{u_2}{s_2} = \frac{t_2}{v_2} \in \mathbb{F}_q$ or $\frac{u_2}{t_2} = \frac{s_2}{v_2} \in \mathbb{F}_q$.

Subcase 2.1: $\frac{u_1}{s_1} = \frac{t_1}{v_1} \in \mathbb{F}_q$ **and** $\frac{u_2}{s_2} = \frac{t_2}{v_2} \in \mathbb{F}_q$.

Let $b := \frac{u_2}{s_2} = \frac{t_2}{v_2} \in \mathbb{F}_q$. Note that $a = \frac{u_1}{s_1} = \frac{t_1}{v_1} \in \mathbb{F}_q$. Substituting them into Eqs. (3) and (4), we have

$$\begin{aligned} as_1v_2 + as_1^q v_1^q + bs_2v_1 &= bs_1v_2 + as_1^q v_1^q + as_2v_1, \\ as_1^q v_2 + bs_2v_1^q &= bs_1^q v_2 + as_2v_1^q. \end{aligned}$$

It follows that

$$\begin{aligned} (a-b)(s_1v_2 - s_2v_1) &= 0, \\ (a-b)(s_1^q v_2 - s_2v_1^q) &= 0. \end{aligned}$$

If $a = b$, then $\bar{u} = a\bar{s}$. Therefore, $\{\bar{u}\mathbb{F}_q, \bar{v}\mathbb{F}_q\} = \{\bar{s}\mathbb{F}_q, \bar{t}\mathbb{F}_q\}$.
If $a \neq b$, then

$$\begin{aligned} s_1v_2 - s_2v_1 &= 0, \\ s_1^q v_2 - s_2v_1^q &= 0. \end{aligned}$$

We can compute to get that $\frac{s_1}{v_1} = \frac{s_2}{v_2} = \frac{s_1^q}{v_1^q}$. By Lemma 3.1, we have $\frac{s_1}{v_1} = \frac{s_2}{v_2} \in \mathbb{F}_q$. Then $\bar{s} = \frac{s_1}{v_1}\bar{v}$. Therefore, $\{\bar{u}\mathbb{F}_q, \bar{v}\mathbb{F}_q\} = \{\bar{s}\mathbb{F}_q, \bar{t}\mathbb{F}_q\}$.

Subcase 2.2: $\frac{u_1}{s_1} = \frac{t_1}{v_1} \in \mathbb{F}_q$ **and** $\frac{u_2}{t_2} = \frac{s_2}{v_2} \in \mathbb{F}_q$.

Let $b := \frac{u_2}{t_2} = \frac{s_2}{v_2} \in \mathbb{F}_q$. Note that $a = \frac{u_1}{s_1} = \frac{t_1}{v_1} \in \mathbb{F}_q$. Substituting them into Eq. (3), we have

$$as_1v_2 + as_1^q v_1^q + bt_2v_1 = s_1t_2 + as_1^q v_1^q + abv_2v_1.$$

It follows that

$$(av_2 - t_2)(s_1 - bv_1) = 0.$$

Then we have $\frac{t_2}{v_2} = a = \frac{t_1}{v_1}$ or $\frac{s_1}{v_1} = b = \frac{s_2}{v_2}$. So $\bar{t} = a\bar{v}$ or $\bar{s} = b\bar{v}$. Therefore, we have $\{\bar{u}\mathbb{F}_q, \bar{v}\mathbb{F}_q\} = \{\bar{s}\mathbb{F}_q, \bar{t}\mathbb{F}_q\}$.

Subcase 2.3: $\frac{u_1}{t_1} = \frac{s_1}{v_1} \in \mathbb{F}_q$ **and** $\frac{u_2}{s_2} = \frac{t_2}{v_2} \in \mathbb{F}_q$.

Let $b := \frac{u_1}{t_1} = \frac{s_1}{v_1} \in \mathbb{F}_q$ and $c := \frac{u_2}{s_2} = \frac{t_2}{v_2} \in \mathbb{F}_q$. Substituting them into Eq. (6), we have

$$(bt_1v_2 + cs_2v_1)^q = (bcv_1v_2 + s_2t_1)^q.$$

It follows that

$$(bv_2 - s_2)(t_1 - cv_1) = 0.$$

Then we have $\frac{s_2}{v_2} = b = \frac{s_1}{v_1}$ or $\frac{t_1}{v_1} = c = \frac{t_2}{v_2}$. So $\bar{s} = b\bar{v}$ or $\bar{t} = c\bar{v}$. Therefore, we have $\{\bar{u}\mathbb{F}_q, \bar{v}\mathbb{F}_q\} = \{\bar{s}\mathbb{F}_q, \bar{t}\mathbb{F}_q\}$.

Subcase 2.4: $\frac{u_1}{t_1} = \frac{s_1}{v_1} \in \mathbb{F}_q$ **and** $\frac{u_2}{t_2} = \frac{s_2}{v_2} \in \mathbb{F}_q$.

Let $b := \frac{u_1}{t_1} = \frac{s_1}{v_1} \in \mathbb{F}_q$ and $c := \frac{u_2}{t_2} = \frac{s_2}{v_2} \in \mathbb{F}_q$. Substituting them into Eqs. (4) and (6), we have

$$\begin{aligned} bt_1^q v_2 + ct_2 v_1^q &= bv_1^q t_2 + cv_2 t_1^q, \\ (bt_1 v_2 + ct_2 v_1)^q &= (bv_1 t_2 + cv_2 t_1)^q. \end{aligned}$$

It follows that

$$\begin{aligned} (b-c)(t_1 v_2 - t_2 v_1) &= 0, \\ (b-c)(t_1^q v_2 - t_2 v_1^q) &= 0. \end{aligned}$$

If $b = c$, then $\bar{u} = b\bar{t}$. Therefore, $\{\bar{u}\mathbb{F}_q, \bar{v}\mathbb{F}_q\} = \{\bar{s}\mathbb{F}_q, \bar{t}\mathbb{F}_q\}$.

If $b \neq c$, then

$$\begin{aligned} t_1 v_2 - t_2 v_1 &= 0, \\ t_1^q v_2 - t_2 v_1^q &= 0. \end{aligned}$$

We can compute to get that $\frac{t_1}{v_1} = \frac{t_2}{v_2} = \frac{t_1^q}{v_1^q}$. By Lemma 3.1, we have $\frac{t_1}{v_1} = \frac{t_2}{v_2} \in \mathbb{F}_q$. Then $\bar{t} = \frac{t_1}{v_1}\bar{v}$. Therefore, $\{\bar{u}\mathbb{F}_q, \bar{v}\mathbb{F}_q\} = \{\bar{s}\mathbb{F}_q, \bar{t}\mathbb{F}_q\}$.

Hence, $V \in \mathcal{G}_q(n, 2k)$ is a Sidon space. □

Remark 3.3 In ([15, Theorem 19]), the authors can give the same parameters of Sidon spaces as Theorem 3.2. But their construction is by induction, while ours is an explicit construction. Hence, Theorem 3.2 is a new construction of Sidon spaces and easy to be computed.

3.2 Construction II

If the parameters in Theorem 3.2 have more restrictions, then we can get better results. The following lemma is useful.

Lemma 3.4 *[13, Theorem 3.75] Let $t \geq 2$ be an integer and $a \in \mathbb{F}_q^*$. Then the binomial $x^t - a$ is irreducible in $\mathbb{F}_q[x]$ if and only if the following two conditions are satisfied:*

1. *each prime factor of t divides the order e of a in $\mathbb{F}_q^*$, but not $(q-1)/e$;*
2. *$q \equiv 1 \pmod 4$ if $t \equiv 0 \pmod 4$.*

The next lemma will be useful in the following theorems.

Lemma 3.5 *Let k, n be integers, q be a prime power, t be an odd integer such that $n = tk$ and $t|(q^k - 1)$. Let ω be a primitive element of $\mathbb{F}_{q^k}$. Then there exists an element $\gamma \in \mathbb{F}_{q^n}$ such that $\gamma^t = \omega$.*

Proof Since t is an odd integer and $t|(q^k - 1)$, by Lemma 3.4, $x^t - \omega$ is irreducible in $\mathbb{F}_{q^k}[x]$. Hence, $\mathbb{F}_{q^n} \cong \mathbb{F}_{q^k}[x]/(x^t - \omega)$. Therefore, there exists an element $\gamma \in \mathbb{F}_{q^n}$ such that $\gamma^t = \omega$. □

Now we state our construction.

Theorem 3.6 *Let k, n be integers, q be a prime power such that $n = 7k$ and $7|(q^k-1)$. Let ω be a primitive element of $\mathbb{F}_{q^k}$ and $\gamma \in \mathbb{F}_{q^n}$ such that $\gamma^7 = \omega$. Set $V = \{u_1 + u_1^q\gamma^3 + u_2\gamma^5 + u_2^q\gamma^6 : u_1, u_2 \in \mathbb{F}_{q^k}\}$, then $V \in \mathcal{G}_q(n, 2k)$ is a Sidon space.*

Proof The existence of γ follows from Lemma 3.5. Suppose $(u_1 + u_1^q\gamma^3 + u_2\gamma^5 + u_2^q\gamma^6)(v_1+v_1^q\gamma^3+v_2\gamma^5+v_2^q\gamma^6) = (s_1+s_1^q\gamma^3+s_2\gamma^5+s_2^q\gamma^6)(t_1+t_1^q\gamma^3+t_2\gamma^5+t_2^q\gamma^6)$, where $u_1, u_2, v_1, v_2, s_1, s_2, t_1, t_2 \in \mathbb{F}_{q^k}$ and $u_1 + u_1^q\gamma^3 + u_2\gamma^5 + u_2^q\gamma^6$, $v_1 + v_1^q\gamma^3 + v_2\gamma^5 + v_2^q\gamma^6$, $s_1 + s_1^q\gamma^3 + s_2\gamma^5 + s_2^q\gamma^6$, $t_1 + t_1^q\gamma^3 + t_2\gamma^5 + t_2^q\gamma^6$ are all nonzero. Denote

$$\tilde{u} := u_1 + u_1^q\gamma^3 + u_2\gamma^5 + u_2^q\gamma^6, \qquad \tilde{v} := v_1 + v_1^q\gamma^3 + v_2\gamma^5 + v_2^q\gamma^6,$$
$$\tilde{s} := s_1 + s_1^q\gamma^3 + s_2\gamma^5 + s_2^q\gamma^6, \qquad \tilde{t} := t_1 + t_1^q\gamma^3 + t_2\gamma^5 + t_2^q\gamma^6.$$

Since $\gamma^7 = \omega$, then we have

$$u_1v_1 = s_1t_1, \tag{14}$$
$$\omega(u_1^qv_2 + u_2v_1^q) = \omega(s_1^qt_2 + s_2t_1^q), \tag{15}$$
$$\omega(u_1^qv_2^q + u_2^qv_1^q) = \omega(s_1^qt_2^q + s_2^qt_1^q), \tag{16}$$
$$u_1v_1^q + u_1^qv_1 + \omega u_2v_2 = s_1t_1^q + s_1^qt_1 + \omega s_2t_2, \tag{17}$$
$$\omega(u_2v_2^q + u_2^qv_2) = \omega(s_2t_2^q + s_2^qt_2), \tag{18}$$
$$u_1v_2 + u_2v_1 + \omega u_2^qv_2^q = s_1t_2 + s_2t_1 + \omega s_2^qt_2^q, \tag{19}$$
$$u_1v_2^q + u_2^qv_1 + u_1^qv_1^q = s_1t_2^q + s_2^qt_1 + s_1^qt_1^q. \tag{20}$$

Noting that $\omega \neq 0$, we can get that

$$u_1v_1 = s_1t_1 \text{ (from (14))}, \tag{21}$$
$$u_1^qv_2 + u_2v_1^q = s_1^qt_2 + s_2t_1^q \text{ (from (15))}, \tag{22}$$
$$u_1v_2 + u_2v_1 = s_1t_2 + s_2t_1 \text{ (from (16))}, \tag{23}$$
$$u_2v_2^q + u_2^qv_2 = s_2t_2^q + s_2^qt_2 \text{ (from (18))}, \tag{24}$$
$$u_2v_2 = s_2t_2 \text{ (from (19) and (23))}, \tag{25}$$
$$u_1v_2^q + u_2^qv_1 = s_1t_2^q + s_2^qt_1 \text{ (from (20) and (14))}, \tag{26}$$
$$u_1v_1^q + u_1^qv_1 = s_1t_1^q + s_1^qt_1 \text{ (from (17) and (25))}. \tag{27}$$

Case 1: At least one of $u_1, u_2, v_1, v_2, s_1, s_2, t_1, t_2$ is 0.

Suppose $u_1 = 0$. By Eq. (21), we may assume $s_1 = 0$. Since $\tilde{u}, \tilde{s}$ are both nonzero, we have u_2, s_2 to be nonzero. Then we can get that

$$u_2v_1 = s_2t_1, \tag{28}$$
$$u_2v_1^q = s_2t_1^q, \tag{29}$$

$$u_2^q v_1 = s_2^q t_1, \tag{30}$$
$$u_2 v_2^q + u_2^q v_2 = s_2 t_2^q + s_2^q t_2, \tag{31}$$
$$u_2 v_2 = s_2 t_2. \tag{32}$$

Subcase 1.1: v_1, t_1 **are both nonzero.**

By Eqs. (28) and (29), we have $\frac{u_2}{s_2} = \frac{t_1}{v_1} = \frac{t_1^q}{v_1^q}$. By Lemma 3.1, we have $\frac{u_2}{s_2} = \frac{t_1}{v_1} \in \mathbb{F}_q$. Then $u_2\gamma^2 + u_2^q\gamma^4 = \frac{u_2}{s_2}(s_2\gamma^2 + s_2^q\gamma^4)$. Note that $u_1 = s_1 = 0$ and since $\tilde{u}\tilde{v} = \tilde{s}\tilde{t}$, we have that $\{\tilde{u}\mathbb{F}_q, \tilde{v}\mathbb{F}_q\} = \{\tilde{s}\mathbb{F}_q, \tilde{t}\mathbb{F}_q\}$.

Subcase 1.2: $v_1 = 0$.

By Eq. (28), we have $t_1 = 0$, and then v_2, t_2 are both nonzero. Let $a := \frac{u_2}{s_2}$, then from Eq. (32), we have $t_2 = av_2$. Substituting them into Eq. (31), we have

$$as_2v_2^q + a^q s_2^q v_2 = a^q s_2 v_2^q + as_2^q v_2.$$

It follows that $(a - a^q)(s_2v_2^q - s_2^q v_2) = 0$. Then $a = a^q$ or $\frac{s_2}{v_2} = \frac{s_2^q}{v_2^q}$. By Lemma 3.1, we have $a \in \mathbb{F}_q$ or $\frac{s_2}{v_2} \in \mathbb{F}_q$, which implies that $u_2\gamma^2 + u_2^q\gamma^4 = a(s_2\gamma^2 + s_2^q\gamma^4)$ or $s_2\gamma^2 + s_2^q\gamma^4 = \frac{s_2}{v_2}(v_2\gamma^2 + v_2^q\gamma^4)$. Note that $u_1 = s_1 = v_1 = t_1 = 0$ and since $\tilde{u}\tilde{v} = \tilde{s}\tilde{t}$, we have that $\{\tilde{u}\mathbb{F}_q, \tilde{v}\mathbb{F}_q\} = \{\tilde{s}\mathbb{F}_q, \tilde{t}\mathbb{F}_q\}$.

Case 2: None of $u_1, u_2, v_1, v_2, s_1, s_2, t_1, t_2$ **is 0.**

Let $a := \frac{u_1}{s_1}$, then from Eq. (21), we have $t_1 = av_1$. Substituting them into Eq. (27), we have

$$as_1v_1^q + a^q s_1^q v_1 = a^q s_1 v_1^q + as_1^q v_1.$$

It follows that

$$(a - a^q)(s_1v_1^q - s_1^q v_1) = 0.$$

Then $a = a^q$ or $\frac{s_1}{v_1} = \frac{s_1^q}{v_1^q}$. Hence, $\frac{u_1}{s_1} = \frac{t_1}{v_1} \in \mathbb{F}_q$ or $\frac{u_1}{t_1} = \frac{s_1}{v_1} \in \mathbb{F}_q$.

Similarly, from Eqs. (24) and (25), we can get that $\frac{u_2}{s_2} = \frac{t_2}{v_2} \in \mathbb{F}_q$ or $\frac{u_2}{t_2} = \frac{s_2}{v_2} \in \mathbb{F}_q$.

Subcase 2.1: $\frac{u_1}{s_1} = \frac{t_1}{v_1} \in \mathbb{F}_q$ **and** $\frac{u_2}{s_2} = \frac{t_2}{v_2} \in \mathbb{F}_q$.

Let $b := \frac{u_2}{s_2} = \frac{t_2}{v_2} \in \mathbb{F}_q$. Note that $a = \frac{u_1}{s_1} = \frac{t_1}{v_1} \in \mathbb{F}_q$. Substituting them into Eqs. (23) and (22), we have

$$as_1v_2 + bs_2v_1 = bs_1v_2 + as_2v_1,$$
$$as_1^q v_2 + bs_2v_1^q = bs_1^q v_2 + as_2v_1^q.$$

It follows that

$$(a - b)(s_1v_2 - s_2v_1) = 0,$$
$$(a - b)(s_1^q v_2 - s_2v_1^q) = 0.$$

If $a = b$, then we have $\{\tilde{u}\mathbb{F}_q, \tilde{v}\mathbb{F}_q\} = \{\tilde{s}\mathbb{F}_q, \tilde{t}\mathbb{F}_q\}$.
If $a \neq b$, then

$$s_1v_2 - s_2v_1 = 0,$$
$$s_1^q v_2 - s_2 v_1^q = 0.$$

Then $\frac{s_1}{v_1} = \frac{s_2}{v_2} = \frac{s_1^q}{v_1^q} \in \mathbb{F}_q$. Therefore, $\{\tilde{u}\mathbb{F}_q, \tilde{v}\mathbb{F}_q\} = \{\tilde{s}\mathbb{F}_q, \tilde{t}\mathbb{F}_q\}$.
Subcase 2.2: $\frac{u_1}{s_1} = \frac{t_1}{v_1} \in \mathbb{F}_q$ **and** $\frac{u_2}{t_2} = \frac{s_2}{v_2} \in \mathbb{F}_q$.
Let $b := \frac{u_2}{t_2} = \frac{s_2}{v_2} \in \mathbb{F}_q$. Note that $a = \frac{u_1}{s_1} = \frac{t_1}{v_1} \in \mathbb{F}_q$. Substituting them into Eq. (23), we have

$$as_1v_2 + bt_2v_1 = s_1t_2 + abv_2v_1.$$

It follows that

$$(av_2 - t_2)(s_1 - bv_1) = 0.$$

Then we have $\frac{t_2}{v_2} = a = \frac{t_1}{v_1}$ or $\frac{s_1}{v_1} = b = \frac{s_2}{v_2}$. Therefore, we have $\{\tilde{u}\mathbb{F}_q, \tilde{v}\mathbb{F}_q\} = \{\tilde{s}\mathbb{F}_q, \tilde{t}\mathbb{F}_q\}$.
Subcase 2.3: $\frac{u_1}{t_1} = \frac{s_1}{v_1} \in \mathbb{F}_q$ **and** $\frac{u_2}{s_2} = \frac{t_2}{v_2} \in \mathbb{F}_q$.
Let $b := \frac{u_1}{t_1} = \frac{s_1}{v_1} \in \mathbb{F}_q$ and $c := \frac{u_2}{s_2} = \frac{t_2}{v_2} \in \mathbb{F}_q$. Substituting them into Eq. (23), we have

$$bt_1v_2 + cs_2v_1 = bcv_1v_2 + s_2t_1.$$

It follows that

$$(bv_2 - s_2)(t_1 - cv_1) = 0.$$

Then we have $\frac{s_2}{v_2} = b = \frac{s_1}{v_1}$ or $\frac{t_1}{v_1} = c = \frac{t_2}{v_2}$. So $\bar{s} = b\bar{v}$ or $\bar{t} = c\bar{v}$. Therefore, we have $\{\bar{u}\mathbb{F}_q, \bar{v}\mathbb{F}_q\} = \{\bar{s}\mathbb{F}_q, \bar{t}\mathbb{F}_q\}$.
Subcase 2.4: $\frac{u_1}{t_1} = \frac{s_1}{v_1} \in \mathbb{F}_q$ **and** $\frac{u_2}{t_2} = \frac{s_2}{v_2} \in \mathbb{F}_q$.
Let $b := \frac{u_1}{t_1} = \frac{s_1}{v_1} \in \mathbb{F}_q$ and $c := \frac{u_2}{t_2} = \frac{s_2}{v_2} \in \mathbb{F}_q$. Substituting them into Eqs. (22) and (23), we have

$$bt_1^q v_2 + ct_2v_1^q = bv_1^q t_2 + cv_2t_1^q,$$
$$bt_1v_2 + ct_2v_1 = bv_1t_2 + cv_2t_1.$$

It follows that

$$(b - c)(t_1v_2 - t_2v_1) = 0,$$
$$(b - c)(t_1^q v_2 - t_2v_1^q) = 0.$$

If $b = c$, then $\bar{u} = b\bar{t}$. Therefore, $\{\bar{u}\mathbb{F}_q, \bar{v}\mathbb{F}_q\} = \{\bar{s}\mathbb{F}_q, \bar{t}\mathbb{F}_q\}$.
If $b \neq c$, then

$$t_1 v_2 - t_2 v_1 = 0,$$
$$t_1^q v_2 - t_2 v_1^q = 0.$$

We can compute to get that $\frac{t_1}{v_1} = \frac{t_2}{v_2} = \frac{t_1^q}{v_1^q}$. By Lemma 3.1, we have $\frac{t_1}{v_1} = \frac{t_2}{v_2} \in \mathbb{F}_q$. Then $\bar{t} = \frac{t_1}{v_1}\bar{v}$. Therefore $\{\bar{u}\mathbb{F}_q, \bar{v}\mathbb{F}_q\} = \{\bar{s}\mathbb{F}_q, \bar{t}\mathbb{F}_q\}$.
Hence, $V \in \mathcal{G}_q(n, 2k)$ is a Sidon space. □

Remark 3.7 1. By Theorem 2.4 and Remark 2.2, Theorem 3.6 resolves Conjecture 1 partially for the case $7|(q^t - 1)$, $n = 7t$ and $k \leq 2t$. In particular, when $7|(q-1)$ and $7|n$, our result works for $k \leq \frac{2}{7}n$.
2. Let q be a prime power, $n = 7l$, where $l \geq 5$ is an odd integer satisfying $3 \nmid l$ and $7|(q^l - 1)$. Theorem 3.6 shows that there exist Sidon spaces in $\mathcal{G}_q(n, k)$ with $\lfloor \frac{n-2}{4} \rfloor + 1 \leq k \leq \frac{2n}{7} (= 2l)$, which cannot be obtained by the constructions in [15].

3.3 Construction III

In the previous two constructions, we have $k|n$ and then there is a large subfield. In this subsection, we give a construction of Sidon spaces in $\mathbb{F}_{q^n}$, where $\mathbb{F}_{q^n}$ does not need to contain large subfields.

Theorem 3.8 *Let n be an odd integer, k be an integer and q be a prime power such that $n \geq 4k - 1$ and $n|(q-1)$. Let ω be a primitive element of $\mathbb{F}_q$ and $\gamma \in \mathbb{F}_{q^n}$ such that $\gamma^n = \omega$. Set $V_0 = \{v_0 + v_1\gamma^2 + \cdots + v_{k-1}\gamma^{2k-2} : v_i \in \mathbb{F}_q$ for $i = 0, \cdots, k-1\}$ and $V = \{v + v^q\gamma : v \in V_0\}$, then $V \in \mathcal{G}_q(n, k)$ is a Sidon space.*

Proof Let $d := \frac{q-1}{n}$. The existence of γ follows from Lemma 3.5. Suppose $(u + u^q\gamma)(v + v^q\gamma) = (s + s^q\gamma)(t + t^q\gamma)$, where $u, v, s, t \in V_0$ and $u, v, s, t \neq 0$. Then we have

$$uv + u^q v^q \gamma^2 + (uv^q + u^q v)\gamma = st + s^q t^q \gamma^2 + (st^q + s^q t)\gamma. \tag{33}$$

Note that $\gamma^q = \omega^d\gamma$. By the definition of V_0, we can get that $uv + u^q v^q \gamma^2$, $st + s^q t^q \gamma^2$ are linear combinations of $1, \gamma^2, \gamma^4, \ldots, \gamma^{4k-2}$, and $(uv^q + u^q v)\gamma$, $(st^q + s^q t)\gamma$ are linear combinations of $\gamma, \gamma^3, \gamma^5, \ldots, \gamma^{4k-3}$. Note that $1, \gamma, \gamma^2, \ldots, \gamma^{n-1}$ form a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and $n \geq 4k - 1$. Hence,

$$uv + u^q v^q \gamma^2 = st + s^q t^q \gamma^2, \tag{34}$$
$$uv^q + u^q v = st^q + s^q t. \tag{35}$$

Let

$$u=\sum_{i=0}^{k-1}u_i\gamma^{2i},\ v=\sum_{i=0}^{k-1}v_i\gamma^{2i},\ s=\sum_{i=0}^{k-1}s_i\gamma^{2i},\ t=\sum_{i=0}^{k-1}t_i\gamma^{2i}.$$

Then we have

$$u^q=\sum_{i=0}^{k-1}u_i\omega^{2id}\gamma^{2i},\ v^q=\sum_{i=0}^{k-1}v_i\omega^{2id}\gamma^{2i},\ s^q=\sum_{i=0}^{k-1}s_i\omega^{2id}\gamma^{2i},\ t^q=\sum_{i=0}^{k-1}t_i\omega^{2id}\gamma^{2i}.$$

From Eq. (34), we have

$$\begin{aligned}&\sum_{l=0}^{2k-2}\left(\sum_{0\le i,j\le k-1,i+j=l}u_iv_j\gamma^{2l}+\sum_{0\le i,j\le k-1,i+j=l}u_iv_j\omega^{2ld}\gamma^{2l+2}\right)\\&\quad=\sum_{l=0}^{2k-2}\left(\sum_{0\le i,j\le k-1,i+j=l}s_it_j\gamma^{2l}+\sum_{0\le i,j\le k-1,i+j=l}s_it_j\omega^{2ld}\gamma^{2l+2}\right).\end{aligned}$$

That is

$$\begin{aligned}&u_0v_0+\sum_{l=1}^{2k-2}\left(\sum_{0\le i,j\le k-1,i+j=l}u_iv_j+\sum_{0\le i,j\le k-1,i+j=l-1}u_iv_j\omega^{(2l-2)d}\right)\gamma^{2l}\\&\quad+u_{k-1}v_{k-1}\omega^{4(k-1)d}\gamma^{4k-2}\\&\quad=s_0t_0+\sum_{l=1}^{2k-2}\left(\sum_{0\le i,j\le k-1,i+j=l}s_it_j+\sum_{0\le i,j\le k-1,i+j=l-1}s_it_j\omega^{(2l-2)d}\right)\gamma^{2l}\\&\quad+s_{k-1}t_{k-1}\omega^{4(k-1)d}\gamma^{4k-2}.\end{aligned}$$

Then we can compute to get that

$$\sum_{0\le i,j\le k-1,i+j=l}u_iv_j=\sum_{0\le i,j\le k-1,i+j=l}s_it_j,\ \text{for } l=0,1,\ldots,2k-2.$$

Hence,

$$uv=st. \tag{36}$$

Let $u=as$, then from Eq. (36), we have $t=av$. Substituting them into Eq. (35), we have

$$asv^q+a^qs^qv=a^qsv^q+as^qv.$$

It follows that

$$(a - a^q)(sv^q - s^q v) = 0.$$

Then $a = a^q$ or $\frac{s}{v} = \frac{s^q}{v^q}$. Hence, $\frac{u}{s} = \frac{t}{v} \in \mathbb{F}_q$ or $\frac{s}{v} = \frac{u}{t} \in \mathbb{F}_q$. For both cases, we can get that $\{(u + u^q\gamma)\mathbb{F}_q, (v + v^q\gamma)\mathbb{F}_q\} = \{(s + s^q\gamma)\mathbb{F}_q, (t + t^q\gamma)\mathbb{F}_q\}$. Hence, $V \in \mathcal{G}_q(n, k)$ is a Sidon space. □

Remark 3.9 1. By Theorem 2.4, Theorem 3.8 resolves Conjecture 1 partially for the case $n \geq 4k - 1$, where $n|(q - 1)$.
2. Let q be a prime power, $n \geq 7$ be an odd integer satisfying $3 \nmid n$ and $n|(q-1)$. Then, Theorem 3.8 shows that there exists a Sidon space in $\mathcal{G}_q(n, k)$ with $k = \lfloor \frac{n+1}{4} \rfloor$, which cannot be obtained by the constructions in [15].

4 Conclusion

In this paper, we study the Sidon space. We give three new constructions of Sidon spaces. Although Construction I does not give Sidon spaces with new parameters, it is a new construction of Sidon spaces. Constructions II and III give some new parameters of Sidon spaces.

Let $n|(q - 1)$, then $x^n - \omega$ is an irreducible polynomial in $\mathbb{F}_q[x]$, where ω is a primitive element of $\mathbb{F}_q$. Then we can find $\gamma \in \mathbb{F}_{q^n}$ such that $\gamma^n = \omega$. Hence, it is easy to compute γ^m for any integer m. Actually, $\gamma^m = \omega^t \gamma^\ell$, where $m = tn + \ell$ and $0 \leq \ell < n$. This is one of the main tricks in Constructions II and III. Then one way to generalize these constructions may be to use three terms irreducible polynomials or other easy-to-compute irreducible polynomials in $\mathbb{F}_q[x]$.

Our results can also be applied to generate cyclic subspace codes by employing Theorem 2.4. As a result, we can resolve the following cases of Conjecture 1:

- $t|n, n/t \geq 9$ and $k \leq 2t$;
- $n = 7t, 7|(q^t - 1)$ and $k \leq 2t$;
- $n|(q - 1)$ and $k \leq \frac{n+1}{4}$.

Combining these and the results in [15], we have the following theorem.

Theorem 4.1 *There exists a cyclic subspace code $C \in \mathcal{G}_q(n, k)$ of minimum distance $2k-2$ and cardinality $(q^n-1)/(q-1)$ if n, k, q satisfy one of the following conditions:*

1. *$q \geq 3$, n is even and $n \geq 2k$;*
2. *$n = 3t$ or $5t$, and $k \leq t$;*
3. *$n = 7t$, $7|(q^t - 1)$ and $k \leq 2t$;*
4. *$n|(q - 1)$ and $k \leq \lfloor \frac{n+1}{4} \rfloor$;*
5. *$n \geq 6$ and $k \leq \lfloor \frac{n-2}{4} \rfloor$.*

Acknowledgements The authors express their gratitude to the anonymous reviewers for their detailed and constructive comments which are very helpful to the improvement of the presentation of this paper.

References

1. Bachoc, C., Passuello, A., Vallentin, F.: Bounds for projective codes from semidefinite programming. Adv. Math. Commun. **7**(2), 127–145 (2013)
2. Bachoc, C., Serra, O., Zémor, G.: An analogue of Vosper's theorem for extension fields. Math. Proc. Cambridge. Philos. Soc. **163**(3), 423–452 (2017)
3. Ben-Sasson, E., Etzion, T., Gabizon, A., Raviv, N.: Subspace polynomials and cyclic subspace codes. IEEE Trans. Inform. Theory **62**(3), 1157–1165 (2016)
4. Braun, M., Etzion, T., Östergård, P.R.J., Vardy, A., Wassermann, A.: Existence of q-analogs of Steiner systems. Forum Math. Pi **4**(e7), 1–14 (2016)
5. Braun, M., Kiermaier, M., Kohnert, A., Laue, R.: Large sets of subspace designs. J. Combin. Theory Ser. A **147**, 155–185 (2017)
6. Erdős, P.: Solved and unsolved problems in combinatorics and combinatorial number theory. Congr. Numer. **32**, 49–62 (1981)
7. Etzion, T., Silberstein, N.: Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams. IEEE Trans. Inform. Theory **55**(7), 2909–2919 (2009)
8. Etzion, T., Storme, L.: Galois geometries and coding theory. Des. Codes Cryptogr. **78**(1), 311–350 (2016)
9. Etzion, T., Vardy, A.: Error-correcting codes in projective space. IEEE Trans. Inform. Theory **57**(2), 1165–1173 (2011)
10. Fazeli, A., Lovett, S., Vardy, A.: Nontrivial t-designs over finite fields exist for all t. J. Combin. Theory Ser. A **127**, 149–160 (2014)
11. Gadouleau, M., Yan, Z.: Constant-rank codes and their connection to constant-dimension codes. IEEE Trans. Inform. Theory **56**(7), 3207–3216 (2010)
12. Kötter, R., Kschischang, F.R.: Coding for errors and erasures in random network coding. IEEE Trans. Inform. Theory **54**(8), 3579–3591 (2008)
13. R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn
14. O'Bryant, K.: A complete annotated bibliography of work related to sidon sequences. Electron. J. Combin. **575**(1), 1–39 (2004)
15. Roth, R.M., Raviv, N., Tamo, I.: Construction of sidon spaces with applications to coding. IEEE Trans. Inform. Theory **64**(6), 4412–4422 (2018)
16. Silberstein, N., Etzion, T.: Enumerative coding for Grassmannian space. IEEE Trans. Inform. Theory **57**(1), 365–374 (2011)
17. Silberstein, N., Etzion, T.: Large constant dimension codes and lexicodes. Adv. Math. Commun. **5**(2), 177–189 (2011)
18. Silva, D., Kschischang, F.R.: On metrics for error correction in network coding. IEEE Trans. Inform. Theory **55**(12), 5479–5490 (2009)
19. Silva, D., Kschischang, F.R., Kötter, R.: A rank-metric approach to error control in random network coding. IEEE Trans. Inform. Theory **54**(9), 3951–3967 (2008)
20. Skachek, V.: Recursive code construction for random networks. IEEE Trans. Inform. Theory **56**(3), 1378–1382 (2010)
21. Trautmann, A.-L., Manganiello, F., Braun, M., Rosenthal, J.: Cyclic orbit codes. IEEE Trans. Inform. Theory **59**(11), 7386–7404 (2013)