Construction of Sidon Spaces with Applications to Coding

Ron M. Roth[⋆], **Netanel Raviv**[⋆,†], and **Itzhak Tamo**[†]
[⋆]Computer Science Department, Technion – Israel Institute of Technology, Haifa 3200003, Israel
[†]Department of Electrical Engineering–Systems, Tel-Aviv University, Tel-Aviv, Israel
ronny@cs.technion.ac.il, netanel.raviv@gmail.com, zactamo@gmail.com

***Abstract*—A subspace of a finite extension field is called a Sidon space if the product of any two of its elements is unique up to a scalar multiplier from the base field. Sidon spaces were recently introduced by Bachoc *et al.* as a means to characterize multiplicative properties of subspaces, and yet no explicit constructions were given. In this paper, several constructions of Sidon spaces are provided. In particular, in some of the constructions the relation between k, the dimension of the Sidon space, and n, the dimension of the ambient extension field, is optimal.**

These constructions are shown to provide cyclic subspace codes, which are useful tools in network coding schemes. To the best of the authors' knowledge, this constitutes the first set of constructions of non-trivial cyclic subspace codes in which the relation between k and n is polynomial, and in particular, linear. As a result, a conjecture by Trautmann *et al.* regarding the existence of non-trivial cyclic subspace codes is resolved for most parameters, and multi-orbit cyclic subspace codes are attained, whose cardinality is within a constant factor (close to $1/2$) from the sphere-packing bound for subspace codes.

***Index Terms*—Sidon spaces, Network coding, Cyclic subspace Codes, Sidon sets.**

I. Introduction

Let $\mathcal{G}_q(n,k)$ be the set of all k-dimensional subspaces of $\mathbb{F}_{q^n}$, the degree-n extension field of the finite field $\mathbb{F}_q = \mathrm{GF}(q)$. *Sidon spaces* were recently defined in [1] as a tool for studying certain multiplicative properties of subspaces. In particular, this term was used to characterize subspaces S and T of $\mathbb{F}_{q^n}$ such that the subspace $S\cdot T \triangleq \langle\{s\cdot t \,:\, s\in S, t\in T\}\rangle$ is of small dimension, where $\langle\cdot\rangle$ denotes linear span over $\mathbb{F}_q$. Simply put, 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 $\mathbb{F}_q$. As noted in [1], the term "Sidon space" draws its inspiration from a *Sidon set*. A set of integers is called a Sidon set if the sums of any two (possibly identical) elements in it are distinct; thus, Sidon spaces may be seen as a multiplicative and linear variant of Sidon sets. A formal definition follows; hereafter, for $a\in\mathbb{F}_{q^n}$, the notation $a\mathbb{F}_q$ stands for $\{\lambda a \,:\, \lambda\in\mathbb{F}_q\}$.

The work of R. M. Roth was supported in part by Grant 1396/16 from the Israel Science Foundation (ISF), and the work of I. Tamo and N. Raviv was supported by ISF Grant 1030/15 and NSF-BSF Grant 2015814. Parts of this paper were presented at the International Symposium on Information Theory (ISIT), Aachen, Germany, June 2017.

Definition 1 ([1, Sec. 1])**.** A subspace $V\in\mathcal{G}_q(n,k)$ is called a Sidon space if for all nonzero $a,b,c,d\in V$, if $ab=cd$ then $\{a\mathbb{F}_q, b\mathbb{F}_q\} = \{c\mathbb{F}_q, d\mathbb{F}_q\}$.

In this paper, we present several constructions of Sidon spaces using a variety of tools. The constructions exhibit either a linear or a quadratic relation between n and k. When n is quadratic in k, some of the resulting Sidon spaces satisfy an additional property of linear independence between products of basis elements.

One of our motivations for studying Sidon spaces is the construction of cyclic subspace codes, which are defined as follows. A (constant dimension) subspace code is a subset of $\mathcal{G}_q(n,k)$ under the subspace metric $\mathsf{d_S}(U,V)\triangleq\dim U+\dim V-2\dim(U\cap V)$. The interest in subspace codes has increased recently due to their application to error correction in random network coding [8]. In order to find good subspace codes and to study their structure, *cyclic subspace codes* were introduced [5]. For a subspace $U\in\mathcal{G}_q(n,k)$ and a nonzero element $\alpha\in\mathbb{F}_{q^n}^*\triangleq\mathbb{F}_{q^n}\setminus\{0\}$, the *cyclic shift* of U by α is $\alpha U\triangleq\{\alpha\cdot u \,:\, u\in U\}$, which is clearly a subspace of the same dimension as U. The *orbit* of U is $\mathrm{orb}(U)\triangleq\{\beta U \,:\, \beta\in\mathbb{F}_{q^n}^*\}$, and its cardinality is $(q^n-1)/(q^t-1)$ for some integer t which divides n. A subspace code is called *cyclic* if it is closed under cyclic shifts. For example, if k divides n then since $\mathbb{F}_{q^k}^*$ is a multiplicative subgroup of $\mathbb{F}_{q^n}^*$ whose cosets are $\{\alpha\mathbb{F}_{q^k}^* \,:\, \alpha\in\mathbb{F}_{q^n}^*\}$, it follows that $\mathrm{orb}(\mathbb{F}_{q^k})$ is a cyclic subspace code of size $(q^n-1)/(q^k-1)$ and minimum distance[1] $2k$ (when $k\,|\,n$, this size is, in fact, the largest possible for any subspace code $\mathcal{C}\subseteq\mathcal{G}_q(n,k)$ of that minimum distance [5, Sec. 3]).

Besides the aforementioned example, no general construction of cyclic subspace codes was known until [2] provided a few constructions from orbits of root spaces of properly chosen linearized polynomials[2]. These constructions have minimum distance of $2k-2$ (i.e., intersection dimension at most 1), and orbits of full size $(q^n-1)/(q-1)$. However, the relation between n and k in the constructions of [2] is in general not known. The results of [2] were recently improved by [12], which developed a technique to increase the number of distinct orbits without compromising the minimum distance, and hence

[1]Unless otherwise stated, the term "minimum distance" refers to the minimum subspace distance according to the metric $\mathsf{d_S}(\cdot,\cdot)$.

[2]A polynomial of the form $L(x)=\sum_i a_i x^{q^i}$, where $a_i\in\mathbb{F}_{q^n}$ for all i, is called *a linearized polynomial* with respect to the base field $\mathbb{F}_q$.

to increase the size of the cyclic subspace code. Yet, [12] did not address the problem of minimizing n for a given k. The following conjecture was posed[3] in [14] regarding the relation between n and k,

Conjecture 2 ([14, Sec. IV.D]). *For any prime power q and positive integers k and $n \geq 2k$, there exists a cyclic subspace code $\mathcal{C} \subseteq \mathcal{G}_q(n,k)$ of minimum distance $2k-2$ and cardinality $(q^n-1)/(q-1)$.*

As implied by Lemma 5 below, the requirement $2k \leq n$ in Conjecture 2 is necessary. In this paper, we show that constructing a single orbit cyclic subspace code of maximum size $(q^n-1)/(q-1)$ and minimum distance $2k-2$ in $\mathcal{G}_q(n,k)$ is equivalent to constructing a Sidon space in $\mathcal{G}_q(n,k)$, a fact which is also shown in [1]. For $q \geq 3$, our constructions of Sidon spaces resolve Conjecture 2 for any k and even $n \geq 2k$; for $q = 2$, they resolve the conjecture for any k up to the largest divisor of n that is smaller than $n/2$. In some cases, a simple generalization allows to include in the code multiple orbits of distinct Sidon spaces without compromising the minimum distance; in these cases, the cardinality of the resulting code is within a constant factor (close to $1/2$) from the sphere-packing bound for subspace codes [5].

The Sidon space constructions in this paper also resolve an open question regarding the *square span* (in short, the *square*) of a Sidon space. For a subspace $V \in \mathcal{G}_q(n,k)$, the square of V is defined as the span of all products of pairs of elements from V, i.e., $V^2 \triangleq \langle \{uv : v,u \in V\} \rangle$. In [1, Thm. 18] it is proved that $\dim(V^2) \geq 2\dim V$ for any Sidon space of dimension 3 or more in $\mathbb{F}_{q^n}$. Since V^2 is spanned by $\binom{k+1}{2}$ elements of $\mathbb{F}_{q^n}$, we get the following lower and upper bounds on $\dim(V^2)$.

Proposition 3. *If $V \in \mathcal{G}_q(n,k)$ is a Sidon space then, whenever $k \geq 3$,*

$$2k \leq \dim(V^2) \leq \binom{k+1}{2}.$$

In light of Proposition 3, we study Sidon spaces in both possible endpoints and, hence, we introduce the following terms.

Definition 4. A subspace $V \in \mathcal{G}_q(n,k)$ is called a *minimum-span* (in short, *min-span*) Sidon space if it is a Sidon space and, in addition, $\dim(V^2) = 2k$; i.e., V attains the lower bound in Proposition 3. Similarly, a subspace $V \in \mathcal{G}_q(n,k)$ is called a *maximum-span* (in short, *max-span*) Sidon space if it is a Sidon space and, in addition, $\dim(V^2) = \binom{k+1}{2}$; i.e., V attains the upper bound in Proposition 3.

Finding the smallest possible value of $\dim(V^2)$ for a given k (in particular, deciding if min-span Sidon spaces exist), is listed as an open problem in [1, Sec. 8]. In Section III, we show that the answer is affirmative whenever k is a proper divisor of n (smaller than $n/2$ when $q = 2$). Then, in Section IV, we present constructions of max-span Sidon spaces. In Section V, we exhibit the connection between Sidon spaces in $\mathcal{G}_q(n,k)$ and cyclic subspace codes of minimum distance $2k-2$, thereby proving Conjecture 2 for any k and even $n \geq 2k$ when $q \geq 3$ (for $q = 2$, we prove the conjecture for any k up to the largest divisor of n that is smaller than $n/2$). In addition, we show that Sidon spaces imply Sidon sets, and hence, multiple novel constructions of Sidon sets are obtained. Finally, in Section VI, we introduce and construct r-Sidon spaces, which are natural generalizations of Sidon spaces in which the product of any r elements is unique up to a scalar multiplier from the base field.

[3]Notice that [14] uses the more general term *cyclic orbit codes*, of which cyclic subspace codes are a special case.

II. PRELIMINARIES

We start with a lemma that provides a necessary condition on n and k so that $\mathcal{G}_q(n,k)$ contains a Sidon space.

Lemma 5. *If $V \in \mathcal{G}_q(n,k)$ is a Sidon space then $2k \leq n$ whenever $k \geq 3$.*

Proof. On the one hand, by Proposition 3 we have $2k = 2\dim(V) \leq \dim(V^2)$. On the other hand, $\dim(V^2) \leq n$. $\square$

The case of Sidon spaces of dimension $k \in \{1,2\}$ is straightforward and is treated in Appendix A. In the remainder of this paper, it is assumed that $k \geq 3$.

Remark 6. It is readily verified that any subspace of a Sidon space is a Sidon space. Hence, a construction of a Sidon space in $\mathcal{G}_q(n,k)$ implies the existence of Sidon spaces in $\mathcal{G}_q(n,t)$, for any $1 \leq t \leq k$. $\square$

Sidon spaces are closely related to their namesakes Sidon sets: the latter are shown in the sequel to both imply and to be implied by Sidon spaces (Sections IV and V-B). Hereafter, $[m]$ stands for the integer set $\{1,2,\ldots,m\}$.

Definition 7. A subset $\{n_1,n_2,\ldots,n_k\}$ of an Abelian group G is called a Sidon set if all pairwise sums are unique, i.e., if the set $\{n_i+n_j : i,j \in [k], i \geq j\}$ contains $\binom{k+1}{2}$ distinct elements.

In the sequel, the group G in Definition 7 is either the set $\mathbb{Z}$ of integers or the set $\mathbb{Z}_m$ of integers modulo some natural number $m > 1$. Clearly, a Sidon set in $\mathbb{Z}_m$ is a Sidon set in $\mathbb{Z}$, but not necessarily vice versa. The main challenge in constructing Sidon sets is obtaining high *density*, i.e., having m as small as possible given the size k for Sidon sets in $\mathbb{Z}_m$, or alternatively, for Sidon sets in $\mathbb{Z}$ that are subsets of $[m]$.

Sidon sets have attracted considerable attention over the years, and many constructions are known [11]. In particular, there exist several constructions in which $m = k^2(1+o_k(1))$ (where $o_k(1)$ stands for a term that goes to 0 as k goes to infinity); moreover, as noted in [11, Sec. 4.1], such a relation between m and k is optimal (up to a factor of $1+o_k(1)$). A known example of Sidon sets is quoted next.

Example 8 ([3]). For a prime power q, a primitive element γ in $\mathbb{F}_{q^2}$, and an arbitrary element $\delta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, the set $\{\log_\gamma(\alpha+\delta) : \alpha \in \mathbb{F}_q\}$ is a Sidon set of size q in $\mathbb{Z}_{q^2-1}$. $\square$

One of our motivations for studying Sidon spaces is the construction of cyclic subspace codes, which were defined in [5] as follows.

Definition 9. A subspace code $\mathcal{C} \subseteq \mathcal{G}_q(n,k)$ is cyclic[4] if $V \in \mathcal{C}$ implies that $\alpha V \in \mathcal{C}$, for every $\alpha \in \mathbb{F}_{q^n}^*$.

Nearly optimal *non*-cyclic subspace codes are known to exist for a wide set of parameters. Specifically, the cardinality of the so-called Koetter–Kschischang codes [8, Sec. V] is within a factor of $1 + o_q(1)$ from the known upper bounds on the size of subspace codes; one of these bounds is quoted next, where we use the notation $\begin{bmatrix} t \\ s \end{bmatrix}_q$ for the q-*binomial coefficient* (also known as the Gaussian coefficient) $|\mathcal{G}_q(t,s)| = \prod_{i=0}^{s-1}((q^{t-i}-1)/(q^{i+1}-1))$.

Theorem 10 (Sphere-packing bound for subspace codes [5, Thm. 2]). *A subspace code $\mathcal{C} \subseteq \mathcal{G}_q(n,k)$ with minimum distance d satisfies*

$$|\mathcal{C}| \leq \frac{\begin{bmatrix} n \\ k-d/2+1 \end{bmatrix}_q}{\begin{bmatrix} k \\ k-d/2+1 \end{bmatrix}_q}.$$

For the parameters $n = 2k$ and $d = 2k-2$, Koetter–Kschischang codes are of size q^n, whereas the upper bound of Theorem 10 is $q^n(1+o_n(1))$. For these parameters, the largest codes presented in this paper are within a factor of $1/2+o_q(1)$ from this bound.

III. Construction of Minimum-Span Sidon Spaces

This section begins with two similar constructions of Sidon spaces in which n grows linearly with k. The first construction applies to any prime power q and $n = rk$, for an integer $r \geq 3$. The second construction applies to $q \geq 3$ and $n = 2k$, and is therefore (fully) optimal by Lemma 5.

Construction 11. For a composite integer n, let k be the largest divisor of n which is smaller than $n/2$, let $\gamma \in \mathbb{F}_{q^n}^*$ be a root of an irreducible polynomial of degree n/k over $\mathbb{F}_{q^k}$, and let $V \triangleq \{u + u^q\gamma : u \in \mathbb{F}_{q^k}\}$.

While Construction 11 requires the dimension k of V to be a divisor of n (and $2k < n$), once we establish that V is a Sidon space, we will get, by Remark 6, Sidon spaces for all dimensions that are smaller than k. The fact that V in Construction 11 is indeed a Sidon space is shown in the next theorem.

Theorem 12. *The subspace $V \in \mathcal{G}_q(n,k)$ from Construction 11 is a Sidon space.*

Proof. Given a product $(u+u^q\gamma)(v+v^q\gamma)$, for some nonzero u and v in $\mathbb{F}_{q^k}$, we notice that

$$(u+u^q\gamma)(v+v^q\gamma) = uv + (uv^q + u^qv)\gamma + (uv)^q\gamma^2. \quad (1)$$

Since $n > 2k$, it follows that $\{1, \gamma, \gamma^2\}$ is a linearly independent set over $\mathbb{F}_{q^k}$, thus the coefficients of the polynomial $P(x) = (u + u^q x)(v + v^q x) = uv + (uv^q + u^q v)x + (uv)^q x^2$ can be extracted from the right-hand side of (1). The roots of $P(x)$ are $-1/u^{q-1}$ and $-1/v^{q-1}$, from which the set $\{u\mathbb{F}_q, v\mathbb{F}_q\}$ is determined uniquely[5], and therefore so is the set $\{(u+u^q\gamma)\mathbb{F}_q, (v+v^q\gamma)\mathbb{F}_q\}$. ☐

By choosing the parameter γ in Construction 11 judiciously, we can also cover the case $n = 2k$, as long as $q \geq 3$. To this end, let W_{q-1} be the set of $(q-1)$st powers of elements in $\mathbb{F}_{q^k}$, i.e, $W_{q-1} \triangleq \{y^{q-1} : y \in \mathbb{F}_{q^k}\}$, and let $\overline{W}_{q-1} \triangleq \mathbb{F}_{q^k} \setminus W_{q-1}$.

Our next construction will require a monic irreducible quadratic polynomial over $\mathbb{F}_{q^k}$ whose free coefficient is in $\overline{W}_{q-1}$. The existence of such polynomials follows from well known properties of quadratic polynomials over finite fields (e.g., [13, Problem 3.42] and [9, Problem 3.52]), and there is a simple recipe for constructing such polynomials explicitly. Recall that for odd q, the elements of $\mathrm{QR}(q^k) \triangleq \{y^2 : y \in \mathbb{F}_{q^k}^*\}$ are called *quadratic residues* of $\mathbb{F}_{q^k}$, and the elements of $\mathrm{QNR}(q^k) = \mathbb{F}_{q^k}^* \setminus \mathrm{QR}(q^k)$ are called *quadratic non-residues* of $\mathbb{F}_{q^k}$. In addition, for an even q and an element $y \in \mathbb{F}_{q^k}$ let $\mathrm{tr}(y) \triangleq y + y^2 + y^4 + \ldots + y^{q^k/2}$ be the absolute trace polynomial over $\mathbb{F}_{q^k}$. It is known that $y \mapsto \mathrm{tr}(y)$ is a linear mapping from $\mathbb{F}_{q^k}$ to $\mathbb{F}_2$, and, in particular, half of the elements of $\mathbb{F}_{q^k}$ have trace 1.

Lemma 13 ([13, Problem 3.42]). *For any $c \in \mathbb{F}_{q^k}^*$ and any $b \in \mathbb{F}_{q^k}$, the polynomial $x^2 + bx + c$ is irreducible if and only if*

$$\begin{cases} b^2 - 4c \in \mathrm{QNR}(q^k), & \text{if } q \text{ is odd,} \\ b \neq 0 \text{ and } \mathrm{tr}\left(c/b^2\right) = 1, & \text{if } q \text{ is even.} \end{cases}$$

Corollary 14. *For any prime power $q \geq 2$, positive integer k, and any $c \in \mathbb{F}_{q^k}^*$ (in particular, any $c \in \overline{W}_{q-1}$), there exists $b \in \mathbb{F}_{q^k}$ such that $x^2 + bx + c$ is irreducible.*

Proof. By [13, Problem 3.23], for odd q and any given $c \in \mathbb{F}_{q^k}^*$, the set $\{b^2 - 4c : b \in \mathbb{F}_{q^k}\} \cap \mathrm{QNR}(q^k)$ is nonempty. For an even q we have $\{c/b^2 : b \in \mathbb{F}_{q^k}^*\} = \mathbb{F}_{q^k}^*$ for any $c \in \mathbb{F}_{q^k}^*$, and the claim follows by the properties of the mapping $y \mapsto \mathrm{tr}(y)$. ☐

Construction 15. For a prime power $q \geq 3$ and a positive integer k, let $n = 2k$, let $\gamma \in \mathbb{F}_{q^n}^*$ be a root of an irreducible polynomial $x^2 + bx + c$ over $\mathbb{F}_{q^k}$ with $c \in \overline{W}_{q-1}$, and let $V \triangleq \{u + u^q\gamma : u \in \mathbb{F}_{q^k}\}$.

Theorem 16. *The subspace $V \in \mathcal{G}_q(n,k)$ from Construction 15 is a Sidon space.*

Proof. As in the proof of Theorem 12, it suffices to show that given $(u + u^q\gamma)(v + v^q\gamma)$ for some nonzero u and v in $\mathbb{F}_{q^k}$, the set $\{u\mathbb{F}_q, v\mathbb{F}_q\}$ can be determined uniquely. Since

$$(u+u^q\gamma)(v+v^q\gamma) = \underbrace{(uv - (uv)^q c)}_{\triangleq Q_0} + \underbrace{(uv^q + u^q v - b(uv)^q)}_{\triangleq Q_1}\gamma, \quad (2)$$

[4]Definition 9 is not to be confused with the more general term "(cyclic) orbit codes" [14], in which an extension-field structure of the ambient space is not assumed. Instead, the ambient space of $\mathcal{G}_q(n,k)$ in [14] is $\mathbb{F}_q^n$, the vector space of dimension n over $\mathbb{F}_q$; and a (cyclic) orbit code is any subspace code which is closed under the action of a (cyclic) subgroup of $\mathrm{GL}_n(q)$, the group of invertible $n \times n$ matrices over $\mathbb{F}_q$. To be precise, a cyclic code may be seen as a cyclic orbit code which is closed under the action of a cyclic subgroup of $\mathrm{GL}_n(q)$ that is isomorphic to $\mathbb{F}_{q^n}^*$.

[5]A simple way to compute $u\mathbb{F}_q$ (say) is representing the equation $x^q - u^{q-1}x = 0$ (over $\mathbb{F}_{q^k}$) as a set of k linear homogeneous equations over $\mathbb{F}_q$, according to some basis of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$.

and since $\{1, \gamma\}$ is a linearly independent set over $\mathbb{F}_{q^k}$, it follows that given the product $(u + u^q\gamma)(v + v^q\gamma)$, one may easily extract Q_0 and Q_1 (both in $\mathbb{F}_{q^k}$) from the right-hand side of (2). Now, notice that Q_0 is the value of the linearized polynomial $T(x) = x - cx^q$ at the point uv. We next show that the mapping $x \mapsto T(x)$ (which is linear over $\mathbb{F}_q$) is invertible on $\mathbb{F}_{q^k}$, i.e., $T(x) = 0$ only if $x = 0$.

Indeed, if there were a nonzero $\beta \in \mathbb{F}_{q^k}$ such that $T(\beta) = 0$, then $\beta - c\beta^q = 0 \Rightarrow c = \beta^{-(q-1)} \Rightarrow c \in W_{q-1}$, a contradiction. Thus, given Q_0, it is possible to uniquely determine uv by solving a set of k linear equations over $\mathbb{F}_q$ (the equations that represent $T(x) = Q_0$ according to some basis of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$). From uv and Q_1 it is possible to compute the coefficients of the polynomial $P(x)$ defined in the proof of Theorem 12, and, as in that proof, the roots of $P(x)$ determine $\{u\mathbb{F}_q, v\mathbb{F}_q\}$ uniquely. □

Theorems 12 and 16 resolve an open question from [1] regarding the existence of min-span Sidon spaces. Since $\dim V = k = n/2$ in Construction 15, and since $\dim(V^2) \leq n$, it follows that Construction 15 attains the lower bound in Proposition 3, namely, it is a min-span Sidon space. Moreover, Construction 11 yields a min-span Sidon space too, now with $\dim(V^2)$ strictly smaller than n; we show this in the following lemma.

Lemma 17. *The subspace V in Construction 11 is a min-span Sidon space.*

Proof. First, observe that (1) implies that $V^2 = \langle\{uv + (uv^q + u^qv)\gamma + (uv)^q\gamma^2 : u, v \in V\}\rangle$. Secondly, since the mapping $A \mapsto A^q$ on $\mathbb{F}_{q^k}$ is linear over $\mathbb{F}_q$, the set $U \triangleq \{A + B\gamma + A^q\gamma^2 : A, B \in \mathbb{F}_{q^k}\}$ is a linear subspace over $\mathbb{F}_q$ and its dimension equals $2k = 2\dim V$. The result follows from the containment $V^2 \subseteq U$. □

Remark 18. Constructions 11 and 15 can be generalized to $V \triangleq \{u + u^{q^s}\gamma : u \in \mathbb{F}_{q^k}\}$, where $\gcd(s, k) = 1$. To see this, note that in the proofs of Theorems 12 and 16, the set $\{u\mathbb{F}_q\}$ can be uniquely determined from u^{q^s-1}, for every $u \in \mathbb{F}_{q^k}$; this is indeed so, since $u^{q^s-1} = (u^{(q^s-1)/(q-1)})^{q-1}$ and the mapping $u \mapsto u^{(q^s-1)/(q-1)}$ is bijective on $\mathbb{F}_{q^k}$ and on $\mathbb{F}_q$. By the same reasoning, the mapping $x \mapsto x - cx^{q^s}$ is bijective on $\mathbb{F}_{q^k}$. □

While Constructions 11 and 15 provide a Sidon space whose dimension scales linearly with n, they do not apply to all possible values of n. The following theorem, whose proof is deferred to Appendix B, shows that such Sidon spaces exist for any n.

Theorem 19. *For any prime power q and integer $n \geq 6$, there exists a Sidon space in $\mathcal{G}_q(n, \lfloor(n-2)/4\rfloor)$.*

IV. Construction of Maximum-Span Sidon Spaces

The constructions we presented in Section III attain the lower bound in Proposition 3. In this section, we consider the other extreme case—namely, constructions of max-span Sidon spaces, which attain the upper bound in that proposition. The next lemma states that if a subspace attains the upper bound in Proposition 3, then the subspace is in effect, a Sidon space.

Lemma 20. *For a subspace V in $\mathcal{G}_q(n, k)$, if $\dim(V^2) = \binom{k+1}{2}$, then V is a (max-span) Sidon space.*

Proof. In light of Definition 1, it suffices to prove that if $a, b, c, d \in V$ satisfy $ab = cd \neq 0$, then $\{a\mathbb{F}_q, b\mathbb{F}_q\} = \{c\mathbb{F}_q, d\mathbb{F}_q\}$. To this end, let $\boldsymbol{v} = (v_i)_{i\in[k]}$ be a vector over $\mathbb{F}_{q^n}$ whose entries form a basis of V over $\mathbb{F}_q$, let $a, b, c, d \in V\backslash\{0\}$, and denote

$$a = \sum_{i\in[k]} a_i \cdot v_i = p_a(\boldsymbol{v}), \qquad b = \sum_{i\in[k]} b_i \cdot v_i = p_b(\boldsymbol{v}),$$
$$c = \sum_{i\in[k]} c_i \cdot v_i = p_c(\boldsymbol{v}), \qquad d = \sum_{i\in[k]} d_i \cdot v_i = p_d(\boldsymbol{v}),$$

where a_i, b_i, c_i, and d_i are elements of $\mathbb{F}_q$ for all $i \in [k]$, and p_a, p_b, p_c, and p_d are the following multivariate polynomials over $\mathbb{F}_q$ in the indeterminates $\boldsymbol{x} = (x_i)_{i\in[k]}$:

$$p_a(\boldsymbol{x}) \triangleq \sum_{i\in[k]} a_i x_i, \qquad p_b(\boldsymbol{x}) \triangleq \sum_{i\in[k]} b_i x_i,$$
$$p_c(\boldsymbol{x}) \triangleq \sum_{i\in[k]} c_i x_i, \qquad p_d(\boldsymbol{x}) \triangleq \sum_{i\in[k]} d_i x_i.$$

Notice that $ab = cd$ implies that

$$\begin{aligned} p_a(\boldsymbol{v}) \cdot p_b(\boldsymbol{v}) &= \sum_{i\in[k]} a_i b_i v_i^2 + \sum_{i\neq j} a_i b_j v_i v_j \\ &= \sum_{i\in[k]} c_i d_i v_i^2 + \sum_{i\neq j} c_i d_j v_i v_j \\ &= p_c(\boldsymbol{v}) \cdot p_d(\boldsymbol{v}). \end{aligned} \tag{3}$$

Since $\dim(V^2) = \binom{k+1}{2}$, and since V^2 is spanned by the set $\{v_i \cdot v_j : i, j \in [k], i \geq j\}$, it follows that the latter set is linearly independent over $\mathbb{F}_q$. Hence, we may compare coefficients in (3) and obtain that

$$\begin{aligned} &a_i b_i = c_i d_i && \text{for all } i \in [k], \text{ and} \\ &a_i b_j + a_j b_i = c_i d_j + c_j d_i && \text{for all distinct } i, j \in [k]. \end{aligned} \tag{4}$$

According to (4), it is readily verified that $p_a(\boldsymbol{x})p_b(\boldsymbol{x}) = p_c(\boldsymbol{x})p_d(\boldsymbol{x})$. Since the ring of multivariate polynomials over a field is a unique factorization domain, and since p_a, p_b, p_c, and p_d are irreducible over $\mathbb{F}_q$, it follows that the sets $\{p_a, p_b\}$ and $\{p_c, p_d\}$ are equal, up to a multiplication by a nonzero element of $\mathbb{F}_q$. Hence, $\{a\mathbb{F}_q, b\mathbb{F}_b\} = \{c\mathbb{F}_q, d\mathbb{F}_b\}$. □

Clearly, max-span Sidon spaces exist in $\mathcal{G}_q(n, k)$ only if $n \geq \binom{k+1}{2}$. In the remainder of this section, three constructions of Sidon spaces are given. The first two are easily seen as being of the max-span type, whereas the third has been verified numerically to be so only for the few parameters that were tested. Note that Remark 6 holds also when the Sidon spaces referred to therein are all of the max-span type. We start with our first construction.

Construction 21. Let $\mathcal{S} \triangleq \{n_1, n_2, \ldots, n_k\} \subseteq [m]$ be a Sidon set in $\mathbb{Z}$ (see Definition 7) such that $m = k^2(1 + o_k(1))$ [11], and for an integer $n > 2m$ and a proper element γ of $\mathbb{F}_{q^n}$ (that does not belong to any proper subfield of $\mathbb{F}_{q^n}$), let $V \triangleq \langle\{\gamma^{n_i}\}_{i\in[k]}\rangle$.

Lemma 22. *The subspace $V \in \mathcal{G}_q(n,k)$ from Construction 21 is a max-span Sidon space.*

Proof. According to Lemma 20, it suffices to show that the set $\Gamma \triangleq \{\gamma^{n_i+n_j} : i,j \in [k], i \geq j\}$, which spans V^2, is linearly independent over $\mathbb{F}_q$. Since $\mathcal{S}$ is a Sidon set, it follows that the exponents of γ in Γ are distinct. Furthermore, since γ is proper in $\mathbb{F}_{q^n}$ and $n > 2m$, it follows that Γ contains $\binom{k+1}{2}$ distinct elements which are linearly independent over $\mathbb{F}_q$. Hence, V is a max-span Sidon space. $\square$

Next, we turn to our second construction of max-span Sidon spaces.

Construction 23. Let $\mathcal{I} \triangleq \{p_{s,t}(x) : s,t \in [k], s \geq t\}$ be a set of $\binom{k+1}{2}$ distinct monic irreducible polynomials over $\mathbb{F}_q$ and let Δ be the largest degree of any polynomial in $\mathcal{I}$. For any $i \in [k]$, let

$$f_i(x) \triangleq \prod_{\substack{(s,t)\in[k]\times[k]:\\ s\geq t,\, s\neq i,\, t\neq i}} p_{s,t}(x), \tag{5}$$

and, for $n > 2\Delta \cdot \binom{k}{2}$ and γ proper in $\mathbb{F}_{q^n}$, let $V \triangleq \left\langle \{f_i(\gamma)\}_{i\in[k]} \right\rangle$.

Lemma 24. *The subspace $V \in \mathcal{G}_q(n,k)$ from Construction 23 is a max-span Sidon space.*

The proof of Lemma 24 is given in Appendix C, where it is also shown that Construction 23 provides a max-span Sidon space in $\mathcal{G}_q(n,k)$ when n is (as small as) $(2+o_k(1))\, k^2 \log_q k$; in particular, when $q \geq \binom{k+1}{2}$, one can take $n = k(k-1)+1$.

The third construction we present in this section is based on the following result from [2].

Lemma 25 ([2])**.** *For any prime power q and positive integer k, the root space of the linearized polynomial $\Lambda(x) \triangleq x^{q^k} + x^q + x$ over $\mathbb{F}_q$ is a Sidon space in the splitting field $\mathbb{F}_{q^n}$ of $\Lambda(x)$.*

Clearly, Lemma 25 implies the existence of Sidon spaces for any q and k. However, no meaningful (e.g., polynomial) upper bound was given in [2] for the extension degree n of the splitting field of $\Lambda(x)$. The upcoming sequence of lemmas lead to a proof that the set V defined next is a Sidon space in $\mathcal{G}_q\left(k^2-1, k\right)$.

Construction 26. For any prime power q and for any integer $k > 1$ which is a power of q, let V be the root space of $x^{q^k} + x^q + x$ in $\mathbb{F}_{q^{k^2-1}}$.

Lemma 27 ([9, p. 116, Thm. 3.62])**.** *Let $A(x) = \sum_i a_i x^{q^i}$ and $B(x) = \sum_i b_i x^{q^i}$ be linearized polynomials over an extension field of $\mathbb{F}_q$, where $A(x) \neq 0$. Then $A(x)$ divides $B(x)$, if and only if the respective (ordinary) polynomial $a(x) = \sum_i a_i x^i$ divides $b(x) = \sum_i b_i x^i$.*

The following lemma is proved in [7, p. 92] only for $q = 2$, yet the proof extends almost verbatim to any prime power q.

Lemma 28 ([7])**.** *For $k = q^m$, the polynomial $x^k + x + 1$ over $\mathbb{F}_q$ divides $x^{k^2-1} - 1$.*

Lemma 29. *For $k = q^m$, the polynomial $x^{q^k} + x^q + x$ splits in $\mathbb{F}_{q^{k^2-1}}$.*

Proof. By Lemmas 27 and 28, that polynomial divides $x^{q^{k^2-1}} - x$ and hence it splits in $\mathbb{F}_{q^{k^2-1}}$. $\square$

Lemmas 25 and 29 imply the following result.

Lemma 30. *The subspace V from Construction 26 is a Sidon space in $\mathcal{G}_q\left(k^2-1, k\right)$.*

By using an exhaustive computer search, we have verified for $(q,k,n) \in \{(2,4,15),(2,8,63),(3,3,8),(4,4,15)\}$ that the root space of $x^{q^k} + x^q + x$ in $\mathbb{F}_{q^{k^2-1}}$ is a max-span Sidon space. It remains open whether this property holds for every q and every $k = q^m$.

We end this section with an existence result of max-span Sidon spaces, whenever $n \geq \binom{k+1}{2}$.

Theorem 31. *For any prime power q and positive integers k and $n \geq \binom{k+1}{2}$, all but a fraction of less than*

$$\frac{1}{q-1} \cdot q^{k(k+1)/2-n}$$

of the spaces in $\mathcal{G}_q(n,k)$ are max-span Sidon spaces.

The proof of this theorem is given in Appendix D. It follows from the theorem that for $q > 2$ and any $n \geq \binom{k+1}{2}$ (and also for $q = 2$ and any $n > \binom{k+1}{2}$), a max-span Sidon space in $\mathcal{G}_q(n,k)$ can be found in polynomial expected running time by a probabilistic algorithm which picks at random a space in $\mathcal{G}_q(n,k)$ and checks whether the pairwise products of its basis elements are linearly independent over $\mathbb{F}_q$.

Remark 32. While this work focuses on Sidon spaces in extension fields, this notion can be defined more generally in commutative algebras. Specifically, let $(\mathbb{F}_q^n, *)$ be the algebra given by the n-dimensional vector space over $\mathbb{F}_q$ when endowed with a commutative bilinear operation $*$. Then a k-dimensional subspace $V \subseteq \mathbb{F}_q^n$ is a Sidon space in the algebra if $a * b = c * d$ for nonzero $a,b,c,d \in V$ implies $\{a\mathbb{F}_q, b\mathbb{F}_q\} = \{c\mathbb{F}_q, d\mathbb{F}_q\}$. Lemma 20 still holds under this generalization (in the proof of the lemma, replace all $\mathbb{F}_q^n$-products by $*$). In [4], a result akin to Theorem 31 was obtained, with $*$ taken as the coordinatewise product of vectors in $\mathbb{F}_q^n$. We mention that when $q \geq \binom{k+1}{2}$, the k polynomials in (5), when constructed with a set $\mathcal{I}$ consisting of $\binom{k+1}{2}$ degree-1 polynomials, generate a max-span Sidon space in the $\binom{k+1}{2}$-dimensional algebra formed by the polynomial ring modulo $\prod_{p(x)\in\mathcal{I}} p(x)$. $\square$

V. Applications of Sidon spaces

A. Cyclic subspace codes

In this subsection, we show that the orbit of a Sidon space is a cyclic subspace code of minimum distance $2k-2$ and cardinality $(q^n-1)/(q-1)$. This topic is discussed briefly in [1, Sec. 5], and yet full proofs are provided below for completeness.

This connection between Sidon spaces and cyclic subspace codes, in conjunction with some of the constructions from Section III, proves Conjecture 2 for most parameters. Further, we show that in some cases, orbits of distinct Sidon spaces can be joined into one subspace code without compromising the minimum distance. This fact enables the construction of a cyclic subspace code whose cardinality is within a factor of $1/2 + o_q(1)$ from the upper bound of Theorem 10.

Lemma 33. *For $V \in \mathcal{G}_q(n,k)$, the following two conditions are equivalent.*

(i) $|\mathrm{orb}(V)| = (q^n-1)/(q-1)$.

(ii) An element $\alpha \in \mathbb{F}_{q^n}^*$ satisfies $\alpha V = V$, if and only if $\alpha \in \mathbb{F}_q^*$.

Proof. Since $\alpha V = (\lambda\alpha)\cdot V$ for any $\alpha \in \mathbb{F}_{q^n}$ and $\lambda \in \mathbb{F}_q^*$, we can view the elements α in (ii) as if they are elements of the quotient group $G \triangleq \mathbb{F}_{q^n}^*/\mathbb{F}_q^*$. Let H be a subgroup of G which contains all elements β such that $\beta V = V$. Then $|\mathrm{orb}(V)| = |G/H|$ and, so, (i) holds if and only if H is trivial (i.e., if and only if H contains only the unit element). On the other hand, H being trivial is equivalent to (ii). □

Lemma 34. *For a subspace $V \in \mathcal{G}_q(n,k)$, the set* $\mathrm{orb}(V)$ *is of size $(q^n-1)/(q-1)$ and minimum distance $2k-2$, if and only if V is a Sidon space.*

Proof. Suppose that $\mathrm{orb}(V)$ is of size $(q^n-1)/(q-1)$ and minimum distance $2k-2$, and let $a,b,c,d \in V$ be such that $ab = cd \neq 0$. Write $\alpha \triangleq a/d = c/b$, and notice that $a,c \in V \cap \alpha V$. If $\alpha \notin \mathbb{F}_q$, it follows from Lemma 33 and from the minimum distance of $\mathrm{orb}(V)$ that $\dim(V\cap\alpha V) \le 1$, which implies that $a\mathbb{F}_q = c\mathbb{F}_q$. Combining with $ab = cd$ thus yields $\{a\mathbb{F}_q, b\mathbb{F}_q\} = \{c\mathbb{F}_q, d\mathbb{F}_q\}$. On the other hand, if $\alpha \in \mathbb{F}_q$ then clearly $a\mathbb{F}_q = d\mathbb{F}_q$ and, so, $\{a\mathbb{F}_q, b\mathbb{F}_q\} = \{c\mathbb{F}_q, d\mathbb{F}_q\}$.

Conversely, suppose that either $|\mathrm{orb}(V)| < (q^n-1)/(q-1)$ or the minimum distance of $\mathrm{orb}(V)$ is less than $2k-2$. Then there exists $\alpha \in \mathbb{F}_{q^n}^* \setminus \mathbb{F}_q^*$ such that $\dim(V \cap \alpha V) \ge 2$, which means that there exist linearly independent elements a and c in $V \cap \alpha V$ and respective b and d in V such that $a = \alpha d$ and $c = \alpha b$. This, in turn, implies that $ab = cd$ while $a\mathbb{F}_q \neq c\mathbb{F}_q$. Yet, since $\alpha \notin \mathbb{F}_q$, we also have $a\mathbb{F}_q \neq d\mathbb{F}_q$; hence, V is not a Sidon space. □

Lemma 34 and Remark 6 yield the following corollary.

Corollary 35. *Construction 11 proves Conjecture 2 for any q, n, and any k up to the largest divisor of n that is smaller than $n/2$. In addition, Construction 15 proves Conjecture 2 for any $q \ge 3$ and any even $n \ge 2k$.*

To attain a cyclic subspace code with multiple orbits, the following lemma is given. This lemma may be seen as a variant of Lemma 34 for distinct orbits.

Lemma 36. *The following two conditions are equivalent for any distinct subspaces U and V in $\mathcal{G}_q(n,k)$.*

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

(ii) For any nonzero $a,c \in U$ and nonzero $b,d \in V$, the equality $ab = cd$ implies that $a\mathbb{F}_q = c\mathbb{F}_q$ and $b\mathbb{F}_q = d\mathbb{F}_q$.

Proof. Assume that $\dim(U \cap \alpha V) \le 1$ for all $\alpha \in \mathbb{F}_{q^n}^*$, and let $a,c \in U$ and $b,d \in V$ such that $ab = cd \neq 0$. Define $\beta \triangleq a/d = c/b$, and notice that $a,c \in U \cap \beta V$. Since $\dim(U \cap \beta V) \le 1$, it follows that $a\mathbb{F}_q = c\mathbb{F}_q$ and, so, $b\mathbb{F}_q = d\mathbb{F}_q$.

Conversely, assume that $\dim(U \cap \alpha V) \ge 2$ for some $\alpha \in \mathbb{F}_{q^n}^*$, and let a and c be two linearly independent elements in $U \cap \alpha V$. Then, there exist b and d in V such that $a = \alpha d$ and $c = \alpha b$. On the one hand $ab = cd$, yet on the other hand $a\mathbb{F}_q \neq c\mathbb{F}_q$. □

Lemma 36 yields a kind of multi-orbit counterpart of the Sidon space property: the product of any two nonzero elements from *distinct orbits* may be uniquely factorized, up to a scalar multiplier from $\mathbb{F}_q$. Using this lemma, Construction 15 can be extended to multiple orbits as follows.

Construction 37. For a prime power $q \ge 3$ and a positive integer k, let w be a primitive element in $\mathbb{F}_{q^k}$. For $c_0 \triangleq w$, let $b_0 \in \mathbb{F}_{q^k}$ be such that $M_0(x) \triangleq x^2 + b_0x + c_0$ is irreducible over $\mathbb{F}_{q^k}$ (such b_0 exists by Corollary 14). For $n = 2k$, let $\gamma_0 \in \mathbb{F}_{q^n}$ be a root of M_0. For $i \in \{0,1,\ldots,\tau-1\}$, where $\tau \triangleq \lfloor (q-1)/2 \rfloor$, let $\gamma_i \triangleq w^i\gamma_0$ and let

$$V_i \triangleq \{u + u^q\gamma_i \,:\, u \in \mathbb{F}_{q^k}\}.$$

Finally, let $\mathcal{C} \triangleq \{\alpha V_i \,:\, i \in \{0,1,\ldots,\tau-1\}, \alpha \in \mathbb{F}_{q^n}^*\}$.

Lemma 38. *The set $\mathcal{C}$ from Construction 37 is a cyclic subspace code of cardinality $\tau \cdot (q^n-1)/(q-1)$ and minimum distance $2k-2$.*

Proof. The fact that $\mathcal{C}$ is cyclic follows immediately from its definition. To prove that the minimum distance is $2k-2$, we first show that each V_i is a Sidon space. To this end, for $i \in \{0,1,\ldots,\tau-1\}$, let $M_i(x) \triangleq x^2 + b_ix + c_i$, where $b_i \triangleq w^ib_0$ and $c_i \triangleq w^{2i}c_0 = w^{2i+1}$, and notice that $M_i(\gamma_i) = 0$. Moreover, since $2i+1$ is not divisible by $q-1$, it follows that $c_i \in \overline{W}_{q-1}$. Hence, V_i is an instance of Construction 15 and is therefore a Sidon space. It is left to show that subspaces of *distinct* orbits intersect on a space of dimension at most 1; namely, we prove that for any distinct $i,j \in \{0,1,\ldots,\tau-1\}$ and any $\alpha \in \mathbb{F}_{q^n}^*$ we have that $\dim(V_i \cap \alpha V_j) \le 1$. According to Lemma 36, this amounts to showing that any product of a nonzero element of V_i with a nonzero element of V_j can be factored uniquely up to a scalar multiplier from $\mathbb{F}_q$. For any nonzero u and v in $\mathbb{F}_{q^k}$, we have

$$\begin{aligned}
&(u+u^q\gamma_i)(v+v^q\gamma_j) = \\
&\quad= (u+u^qw^i\gamma_0)(v+v^qw^j\gamma_0) \\
&\quad= uv + (uv^qw^j + vu^qw^i)\gamma_0 + (uv)^qw^{i+j}\gamma_0^2 \\
&\quad= \left(uv - c_0(uv)^qw^{i+j}\right) \\
&\qquad + \left(uv^qw^j + vu^qw^i - b_0(uv)^qw^{i+j}\right)\gamma_0 \\
&\quad= \underbrace{\left(uv - (uv)^qw^{i+j+1}\right)}_{\triangleq Q_0} \\
&\qquad + \underbrace{\left(uvw^j(v^{q-1} + u^{q-1}w^{i-j}) - b_0(uv)^qw^{i+j}\right)}_{\triangleq Q_1}\gamma_0.
\end{aligned}$$

Since $0 < i+j+1 < q-1$, it follows that $w^{i+j+1} \in \overline{W}_{q-1}$. Hence, the mapping $x \mapsto x - w^{i+j+1}x^q$ is invertible on $\mathbb{F}_{q^k}$, and uv may be uniquely extracted from Q_0. Given uv and Q_1, in turn, one can extract the values of $P_0 \triangleq (u^{q-1}w^{i-j})\cdot v^{q-1}$ and $P_1 \triangleq u^{q-1}w^{i-j} + v^{q-1}$, and compute the roots of the polynomial $x^2 + P_1x + P_0$, which are $u^{q-1}w^{i-j}$ and v^{q-1}.

Since $0 < |i-j| < q-1$, it follows that v^{q-1} is a $(q-1)$st power in $\mathbb{F}_{q^k}$, while $u^{q-1}w^{i-j}$ is not. Hence, by identifying the root which is not a $(q-1)$st power[6] and dividing it by w^{i-j}, we find u^{q-1} and v^{q-1} and, consequently, $u\mathbb{F}_q$ and $v\mathbb{F}_q$. $\square$

For odd (respectively, even) q, the set $\mathcal{C}$ from Construction 37 is a cyclic subspace code that has cardinality $(q^n-1)/2$ (respectively, $((q-2)/(2q-2)) \cdot (q^n-1)$), which is within a factor of $1/2 + o_n(1)$ (respectively, $(q-2)/(2q-2) + o_n(1)$) from the sphere-packing bound (Theorem 10). To the best of our knowledge, this constitutes the first example of a nontrivial cyclic subspace code of that size.

B. Sidon sets

By taking discrete logarithms from properly chosen elements in a Sidon space $V \in \mathcal{G}_q(n,k)$, a Sidon set in $\mathbb{Z}_{(q^n-1)/(q-1)}$ is obtained.

Theorem 39. *If $V \in \mathcal{G}_q(n,k)$ is a Sidon space, γ is a primitive element in $\mathbb{F}_{q^n}$, and $\{\gamma^{n_i} : i \in [(q^k-1)/(q-1)]\}$ is a set of nonzero representatives of all one-dimensional subspaces of V, then $\mathcal{S} \triangleq \{n_i : i \in [(q^k-1)/(q-1)]\}$ is a Sidon set in $\mathbb{Z}_{(q^n-1)/(q-1)}$.*

Proof. Assume that $a,b,c,d \in \mathcal{S}$ satisfy $a+b \equiv c+d \pmod{(q^n-1)/(q-1)}$, i.e., $a+b = c+d+t\cdot(q^n-1)/(q-1)$ for some integer t. Then,

$$\gamma^a\gamma^b = \gamma^c\gamma^d \cdot \lambda,$$

where $\lambda = \gamma^{t(q^n-1)/(q-1)} \in \mathbb{F}_q$. Since V is a Sidon space, it follows that $\{\gamma^a\mathbb{F}_q, \gamma^b\mathbb{F}_q\} = \{\gamma^c\mathbb{F}_q, \lambda\gamma^d\mathbb{F}_q\}$, i.e., $\{\gamma^a\mathbb{F}_q, \gamma^b\mathbb{F}_q\} = \{\gamma^c\mathbb{F}_q, \gamma^d\mathbb{F}_q\}$. Assume without loss of generality that $\gamma^a\mathbb{F}_q = \gamma^c\mathbb{F}_q$. This means that γ^a and γ^c are representatives of the same one-dimensional subspace of V, so we must have $a = c$ (and therefore $b = d$), thereby concluding the proof. $\square$

The Sidon set which results from applying Theorem 39 to Construction 15 is of particular interest. Since $k = n/2$ in this construction, the resulting Sidon set, $\mathcal{S} = \mathcal{S}_q(n)$ ($\subseteq \mathbb{Z}_{(q^n-1)/(q-1)}$), is of size $(q^{n/2}-1)/(q-1)$. For any fixed q, this size is within a constant factor from the square root of the size of the domain $\mathbb{Z}_{(q^n-1)/(q-1)}$; specifically,

$$\lim_{n\to\infty} \frac{|\mathcal{S}_q(n)|}{|\mathbb{Z}_{(q^n-1)/(q-1)}|^{1/2}} = \frac{1}{\sqrt{q-1}}.$$

As such, the construction $\mathcal{S}_q(n)$ is optimal, up to a constant factor (see [11, Thm. 5]).

VI. r-Sidon spaces and B_r-sets

A natural generalization of a Sidon space is an r-Sidon space, in which every product of r elements can be factored uniquely up to a scalar multiplier from the base field.

Definition 40. For positive integers $k < n$ and $r \geq 2$, a subspace $V \in \mathcal{G}_q(n,k)$ is called an r-Sidon space if for all nonzero $a_1, a_2, \ldots, a_r, b_1, b_2, \ldots, b_r \in V$, if $\prod_{i\in[r]} a_i = \prod_{i\in[r]} b_i$ then the multi-sets $\{a_i\mathbb{F}_q\}_{i\in[r]}$ and $\{b_i\mathbb{F}_q\}_{i\in[r]}$ are equal.

The following lemma provides a sphere-packing upper bound on the largest possible dimension of an r-Sidon space.

Lemma 41. *If $V \in \mathcal{G}_q(n,k)$ is an r-Sidon space, then*

$$k < \frac{n}{r} + 1 + \log_q r.$$

Proof. Since the elements in the multi-sets at hand can be seen as one-dimensional subspaces of V, it follows that the number of distinct multi-sets is $\binom{K+r-1}{r}$, where $K \triangleq (q^k-1)/(q-1)$. By the definition of an r-Sidon space, each such multi-set $\{a_i\mathbb{F}_q\}_{i\in[r]}$ induces a distinct product $\prod_{i\in[r]} a_i$ (modulo $\mathbb{F}_q^*$) and, thus,

$$\binom{K+r-1}{r} \leq \frac{q^n-1}{q-1}.$$

By using the simple bound $\binom{s}{t} \geq \left(\frac{s}{t}\right)^s$ it follows that

$$\left(\frac{K+r-1}{r}\right)^r < q^n$$

and, so,

$$(\log_q K) - (\log_q r) < \log_q(K+r-1) - (\log_q r) < \frac{n}{r}.$$

Observing that $\log_q K = \log_q((q^k-1)/(q-1)) > k-1$, the result follows. $\square$

By generalizing Constructions 11 and 15, in what follows two r-Sidon spaces are provided. The first attains $k = n/(r+1)$ for any q, whereas the second attains $k = n/r$ for $q \geq 3$.

Construction 42. For any field size q and integers $k > 0$ and $r \geq 2$, let $n = k(r+1)$, let $\gamma \in \mathbb{F}_{q^n}$ be a root of an irreducible polynomial of degree $r+1$ over $\mathbb{F}_{q^k}$, and let $V \triangleq \{u + u^q\gamma : u \in \mathbb{F}_{q^k}\}$.

Lemma 43. *The subspace V from Construction 42 is an r-Sidon space.*

Proof. We show that given a product $\prod_{i\in[r]} a_i$ of r nonzero elements $a_1, a_2, \ldots, a_r$ in V, the multi-set $\{a_i\mathbb{F}_q\}_{i\in[r]}$ can be identified uniquely. To this end, let $a_i = u_i + u_i^q\gamma$ for $i \in [r]$, and write

$$\prod_{i\in[r]} a_i = \prod_{i\in[r]} (u_i + u_i^q\gamma) = P(\gamma),$$

where $P(x) \triangleq \prod_{i\in[r]}(u_i + u_i^q x)$ is a polynomial of degree r over $\mathbb{F}_{q^k}$. Since $\{\gamma^i\}_{i=0}^r$ is a linearly independent set over $\mathbb{F}_{q^k}$, from the product $P(\gamma) = \prod_{i\in[r]}(u_i + u_i^q\gamma)$ one can obtain the coefficients of $P(x)$. The multi-set of roots of $P(x)$ is given by $\{-1/u_i^{q-1}\}_{i\in[r]}$, from which one can determine uniquely the multi-set $\{u_i\mathbb{F}_q\}_{i\in[r]}$ and, therefore, $\{a_i\mathbb{F}_q\}_{i\in[r]}$. $\square$

The next construction, which may be seen as a generalization of Construction 15, provides an r-Sidon space with $k = n/r$ for any $q \geq 3$. This construction requires an element γ which is a root of an irreducible polynomial of degree r over $\mathbb{F}_{q^k}$ whose free coefficient is in the set $\overline{W}_{q-1}$, i.e., it is

[6] Deciding whether a given element μ is a $(q-1)$st power can be done by checking if the $k \times k$ matrix representation (over $\mathbb{F}_q$) of the linear mapping $x \mapsto x^q - \mu x$ is invertible.

not a $(q-1)$st power of any element in $\mathbb{F}_{q^k}$. Such an element γ can be obtained as follows. Let β be a primitive element in $\mathbb{F}_{q^n}$, let i be an integer in $[q^n-1]$ that is divisible neither by $(q^n-1)/(q^{kt}-1)$ for any proper divisor t of $r=n/k$, nor by $q-1$, and let $\gamma=-\beta^i$.

Lemma 44. *The minimal polynomial $M(x)$ of γ over $\mathbb{F}_{q^k}$ is of degree r and satisfies $M(0)\in\overline{W}_{q-1}$.*

Proof. By the choice of i, the element β^i belongs neither to $\mathbb{F}_{q^k}$ not to any field extension of it that is a proper subfield of $\mathbb{F}_{q^n}$. Hence, $\deg M(x)=r$ and

$$\begin{aligned} M(0) &= \prod_{j=0}^{r-1}(-\gamma)^{q^{jk}} \\ &= (-\gamma)^{(q^n-1)/(q^k-1)} = \beta^{i(q^n-1)/(q^k-1)} = w^i, \end{aligned}$$

where $w \triangleq \beta^{(q^n-1)/(q^k-1)}$ is a primitive element in $\mathbb{F}_{q^k}$. Since i is not divisible by $q-1$, we get that $M(0)=w^i\in\overline{W}_{q-1}$. □

Construction 45. For any prime power $q\geq 3$ and integers $k>0$ and $r\geq 2$, let $n=kr$, let $\gamma\in\mathbb{F}_{q^n}$ be a root of an irreducible polynomial $M(x)$ of degree r over $\mathbb{F}_{q^k}$ with $M(0)\in\overline{W}_{q-1}$, and let $V\triangleq\{u+u^q\gamma\,:\,u\in\mathbb{F}_{q^k}\}$.

Lemma 46. *The subspace V from Construction 45 is an r-Sidon space.*

Proof. Following the same methodology and the same notation from the proof of Lemma 43, notice that for $a_1,a_2,\ldots,a_r\in V$, where $a_i=u_i+u_i^q\gamma$ for $i\in[r]$ and $u_1,u_2,\ldots,u_k\in\mathbb{F}_{q^k}^*$,

$$\prod_{i\in[r]}a_i=\prod_{i\in[r]}(u_i+u_i^q\gamma)=P(\gamma)=\underbrace{(P(x)-p_r\cdot M(x))}_{\triangleq Q(x)}\big|_{x=\gamma},$$

where $p_r=\prod_{i\in[r]}u_i^q=(P(0))^q$ is the leading coefficient of $P(x)$.

Since $\{\gamma^i\}_{i=0}^{r-1}$ is a linearly independent set over $\mathbb{F}_{q^k}$, from the product $\prod_{i\in[r]}(u_i+u_i^q\gamma)$ one can determine the coefficients of $Q(x)=P(x)-p_rM(x)$, which is a polynomial of degree less than r over $\mathbb{F}_{q^k}$. Similarly to the proof of Theorem 16, the free coefficient of $Q(x)$, which is given by

$$Q(0)=P(0)-p_rM(0)=P(0)-M(0)(P(0))^q,$$

is the evaluation of the linearized polynomial $T(x)\triangleq x-M(0)x^q$ at the point $x=P(0)$. Since $M(0)\in\overline{W}_{q-1}$, it follows that $x\mapsto T(x)$ is invertible, and $P(0)$ can be determined uniquely. Knowing $P(0)$, $p_r=(P(0))^q$, and $Q(x)$, we can compute $P(x)=Q(x)+p_rM(x)$, whose multi-set of roots, $\{-1/u_j^{q-1}\}_{i\in[r]}$, determines uniquely the multi-set $\{a_i\mathbb{F}_q\}_{i\in[r]}$. □

Similarly to Theorem 39, the r-Sidon space constructions in this section provide constructions of the following generalization of Sidon sets.

Definition 47 ([11])**.** A subset $\mathcal{S}$ of an Abelian group G is called a B_r-set if the sums of all multi-sets of size r of elements from $\mathcal{S}$ are distinct.

It is known that the size $R_r(m)$ of the largest B_r-set in $[m]$ satisfies (see [11, Sec. 4.2])

$$1\leq\lim_{m\to\infty}\frac{R_r(m)}{\sqrt[r]{m}}\leq\frac{1}{2e}\left(r+\frac{3}{2}\log r+o_r(\log r)\right). \quad (6)$$

Theorem 48. *For an r-Sidon space $V\in\mathcal{G}_q(n,k)$, and for a set $\{\gamma^{n_i}\,:\,i\in[(q^k-1)/(q-1)]\}$ of nonzero representatives of all one-dimensional subspaces of V for some primitive $\gamma\in\mathbb{F}_{q^n}$, the set $\mathcal{S}\triangleq\{n_i\,:\,i\in[(q^k-1)/(q-1)]\}$ is a B_r-set in $\mathbb{Z}_{(q^n-1)/(q-1)}$.*

The proof of Theorem 48 is a straightforward generalization of the proof of Theorem 39 (and is therefore omitted). Applying Theorem 48 to Construction 45 results in a B_r-set $\mathcal{S}_q(n,r)$ of size $(q^{n/r}-1)/(q-1)$ in $\mathbb{Z}_{(q^n-1)/(q-1)}$ (and therefore in $[(q^n-1)/(q-1)]$). It is readily verified that

$$\lim_{n\to\infty}\frac{|\mathcal{S}_q(n,r)|}{|\mathbb{Z}_{(q^n-1)/(q-1)}|^{1/r}}=(q-1)^{(1/r)-1}$$

(compare with (6)).

Acknowledgments

The authors would like to express their sincere gratitude to Amir Shpilka for valuable discussions.

References

[1] C. Bachoc, O. Serra, and G. Zémor, "An analogue of Vosper's theorem for extension fields," *arXiv:1501.00602 [math.NT]*, 2015.

[2] E. Ben-Sasson, T. Etzion, A. Gabizon, and N. Raviv, "Subspace polynomials and cyclic subspace codes," *IEEE Transactions on Information Theory*, vol. 62, no. 3, pp. 1157–1165, 2016.

[3] R. C. Bose and S. Chowla, "Theorems in the additive theory of numbers," *Commentarii Mathematici Helvetici*, vol. 37, no. 1, pp. 141–147, 1962.

[4] I. Cascudo, R. Cramer, D. Mirandola, and G. Zémor, "Squares of random linear codes," *IEEE Transactions on Information Theory*, vol. 61, no. 3, pp. 1159–1173, 2015.

[5] T. Etzion and A. Vardy, "Error-correcting codes in projective space," *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 1165–1173, 2011.

[6] H. Gluesing-Luerssen, K. Morrison, and C. Troha, "Cyclic orbit codes and stabilizer subfields," *Advances in Mathematics of Communications*, vol. 9, pp. 177–197, 2015.

[7] S. W. Golomb. *Shift Register Sequences*. Aegean Park Press, 1982.

[8] R. Koetter and F. R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Transactions on Information Theory*, vol. 54, no. 8, pp. 3579–3591, 2008.

[9] R. Lidl and H. Niederreiter, *Finite fields*. Cambridge University Press, 1997.

[10] H. Niederreiter, "An enumeration formula for certain irreducible polynomials with an application to the construction of irreducible polynomials over the binary fields," *Applicable Algebra in Engineering, Communication and Computing*, vol. 1, pp. 119–124, 1990.

[11] K. O'Bryant, "A complete annotated bibliography of work related to Sidon sequences," *Electronic Journal of Combinatorics*, vol. 575, 2004.

[12] K. Otal and F. Özbudak, "Cyclic subspace codes via subspace polynomials," *Designs, Codes and Cryptography*, doi:10.1007/s10623-016-0297-1, 2016.

[13] R. M. Roth, *Introduction to Coding Theory*. Cambridge University Press, 2006.

[14] A. L. Trautmann, F. Manganiello, M. Braun, and J. Rosenthal, "Cyclic orbit codes," *IEEE Transactions on Information Theory* vol. 59, no. 11, pp. 7386–7404, 2013.

APPENDIX A
SIDON SPACES OF DIMENSIONS 1 AND 2

Definition 1 readily implies that any subspace in $\mathcal{G}_q(n,1)$ is a Sidon space. The same holds for $\mathcal{G}_q(n,2)$, as stated next.

Lemma 49. *Any subspace $V \in \mathcal{G}_q(n,2)$ is either a max-span Sidon space or—if n is even—a cyclic shift of $\mathbb{F}_{q^2}$.*

Proof. Since the Sidon space property is invariant under cyclic shifts, it can be assumed without loss of generality that $V = \langle 1, v\rangle$ for some $v \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$. This implies that $V^2 = \langle 1, v, v^2\rangle$ and, hence, $\dim(V^2) \in \{2,3\}$. If $\dim(V^2) = 3$ then V is a max-span Sidon space (see Definition 4). On the other hand, if $\dim(V^2) = 2$, then $v^2 = \lambda v + \mu$ for some λ and μ in $\mathbb{F}_q$, which means that $v \in \mathbb{F}_{q^2}$ (and, so, n must be even); hence, $V = \mathbb{F}_{q^2}$ in this case. ☐

APPENDIX B
PROOF OF THEOREM 19

Constructions 11 and 15 provide Sidon spaces in which n is linear in k. However, these constructions are restricted to integers n that have a large proper divisor, and do not apply in many other cases (e.g., when n is a prime). We show here that Sidon spaces exist for *any* n and $k \le (n-2)/4$. This claim is proved in an inductive manner: given a Sidon space V, we first show that as long as $\mathbb{F}_{q^n} \setminus V$ is large enough, a new element v can be added to V without compromising the Sidon space property.

Lemma 50. *If $V \in \mathcal{G}_q(n,k)$ is a Sidon space and $q^n - q^k > 2 \cdot (q^{4k+4}-1)/(q-1)$, then there exists $v \in \mathbb{F}_{q^n} \setminus V$ such that $V + \langle v\rangle$ is a Sidon space as well.*

Proof. For $v \in \mathbb{F}_{q^n} \setminus V$, the elements of $V + \langle v\rangle$ are of the form $\alpha v + a$, where $\alpha \in \mathbb{F}_q$ and $a \in V$. Hence, in order for $V + \langle v\rangle$ to be a Sidon space, it suffices to prove that for every $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{F}_q$ and every $a, b, c, d \in V$ such that none of $\alpha_1 v + a$, $\alpha_2 v + b$, $\alpha_3 v + c$, and $\alpha_4 v + d$ is zero, we have that

$$\text{if } (\alpha_1 v + a)(\alpha_2 v + b) = (\alpha_3 v + c)(\alpha_4 v + d), \text{ then} \tag{7}$$

$$\alpha_1 v + a \in \langle \alpha_3 v + c\rangle \cup \langle \alpha_4 v + d\rangle. \tag{8}$$

Equation (7) is equivalent to v being a solution to the quadratic equation

$$\begin{aligned}(\alpha_1\alpha_2 - \alpha_3\alpha_4)\, x^2 +&\\ (\alpha_1 b + \alpha_2 a - \alpha_3 d - \alpha_4 c)\, x +&\\ ab - cd = 0,&\end{aligned} \tag{9}$$

which is trivial (i.e., the left-hand side is the zero polynomial) only if $(\alpha_1 x + a)(\alpha_2 x + b)$ and $(\alpha_3 x + c)(\alpha_4 x + d)$ are (irreducible) decompositions of the same quadratic polynomial (i.e., only if (8) holds). Therefore, the total number of solutions for x to all nontrivial equations of the form (9) serves as an upper bound on the number of elements in $\mathbb{F}_{q^n} \setminus V$ that *cannot* be added to the Sidon space V while maintaining the Sidon space property. Since each such equation is determined by four elements in $\mathbb{F}_q$ and four elements in V, it follows that there exists at most $(q^{4k+4}-1)/(q-1)$ such equations that are pairwise linearly independent over $\mathbb{F}_q$. As we assume that $q^n - |V| = q^n - q^k > 2 \cdot (q^{4k+4}-1)/(q-1)$, there exists $v \in \mathbb{F}_{q^n} \setminus V$ that satisfies *all* constraints of the form (7)–(8) and, hence, $V + \langle v\rangle$ is a Sidon space. ☐

Proof of Theorem 19. We prove by induction on $k = 1, 2, \ldots, \lfloor (n-2)/4 \rfloor$ that $\mathcal{G}_q(n,k)$ contains a Sidon space, with the induction base ($k = 1$) being straightforward.

Turning to the induction step, suppose that $\mathcal{G}_q(n,k)$ contains a Sidon space, for some $k \le \lfloor (n-6)/4 \rfloor$. By Lemma 50, any Sidon space in $\mathcal{G}_q(n,k)$ can be expanded to a Sidon space in $\mathcal{G}_q(n,k+1)$, as long as

$$q^n > \frac{2}{q-1} \cdot (q^{4k+4} - 1) + q^k$$

which, in turn, holds if

$$q^{n-k} \ge \frac{2}{q-1} \cdot q^{3k+4} + 1.$$

It is easy to see that the latter inequality is implied by $n - k \ge 3k + 6$, or, equivalently, by our induction assumption $k \le (n-6)/4$. Hence, for such k, any Sidon space in $\mathcal{G}_q(n,k)$ can be expanded to a Sidon space in $\mathcal{G}_q(n,k+1)$. ☐

APPENDIX C
ANALYSIS OF CONSTRUCTION 23

Proof of Lemma 24. First, note that since the largest degree of a polynomial in $\mathcal{I}$ is Δ, it follows that $\deg f_i \le \Delta \cdot \binom{k}{2} < n/2$, for all $i \in [k]$. Now, by Lemma 20, it suffices to prove that the set $F_\gamma \triangleq \{f_i(\gamma) \cdot f_j(\gamma) \,:\, i, j \in [k], i \ge j\}$ is linearly independent over $\mathbb{F}_q$. From $n/2 > \max\{\deg f_i \,:\, i \in [k]\}$ it follows that the set of *field elements* F_γ is linearly independent over $\mathbb{F}_q$, if and only if the set of *polynomials* $F_x \triangleq \{f_i(x) \cdot f_j(x) \,:\, i, j \in [k], i \ge j\}$ is linearly independent over $\mathbb{F}_q$.

Assume that

$$\sum_{i,j \in [k] \,:\, i \ge j} \alpha_{i,j} f_i(x) f_j(x) = 0, \tag{10}$$

for coefficients $\alpha_{i,j} \in \mathbb{F}_q$. According to (5), taking (10) modulo $p_{s,s}(x)$ for any $s \in [k]$ results in

$$\alpha_{s,s}(f_s(x))^2 \equiv 0 \pmod{p_{s,s}(x)}.$$

Since $\gcd(f_s(x), p_{s,s}(x)) = 1$, it follows that $\alpha_{s,s} = 0$ for all $s \in [k]$, and (10) becomes

$$\sum_{i,j \in [k] \,:\, i > j} \alpha_{i,j} f_i(x) f_j(x) = 0. \tag{11}$$

Taking now (11) modulo $p_{s,t}(x)$ for any $s > t$ in $[k]$ yields

$$\alpha_{s,t} f_s(x) f_t(x) \equiv 0 \pmod{p_{s,t}(x)}.$$

Again, $\gcd(f_s(x), p_{s,t}(x)) = \gcd(f_t(x), p_{s,t}(x)) = 1$ and, so, $\alpha_{s,t} = 0$ for all $s > t$ in $[k]$. ☐

To evaluate the contribution of Construction 23, we provide an upper bound on the smallest possible largest degree, Δ, of the elements of $\mathcal{I}$, under the constraint that $|\mathcal{I}| = \binom{k+1}{2}$.

Lemma 51. *For any positive integer ℓ, the number $J(\ell)$ of monic irreducible polynomials of degree at most ℓ over $\mathbb{F}_q$ satisfies $J(\ell) \ge q^\ell/\ell$.*

Proof. Let $N(\ell)$ denote the number of monic irreducible polynomials of degree (exactly) ℓ over $\mathbb{F}_q$. It is known that

$$\sum_{t|\ell} t\,N(t) = q^{\ell}$$

(see [9, Ch. 3, Cor. 3.21]). Therefore,

$$J(\ell) = \sum_{t\in[\ell]} N(t) \geq \frac{1}{\ell}\sum_{t|\ell} t\,N(t) = \frac{q^{\ell}}{\ell}.$$

□

Given q and k, we can select Δ in Construction 23 to be the smallest for which $J(\Delta) \geq |\mathcal{I}| = \binom{k+1}{2}$. By Lemma 51 we see that $\Delta = (2+o_k(1))\log_q k$ will do, in which case we can take $n = (2+o_k(1))k^2\log_q k$. In particular, when $q \geq |\mathcal{I}| = \binom{k+1}{2}$ we can take $\Delta = 1$, which yields a construction for any $n \geq k(k-1)+1$.

Appendix D
Proof of Theorem 31

In our proof of Theorem 31, we will borrow tools from [4]; specifically, we will use properties of quadratic forms over finite fields, as found in [9, Ch. 6, Sec. 2] and [4, Sec. IV and Appendix A].

A *quadratic form* (in k indeterminates) over a field F is a homogeneous polynomial of the form

$$Q(\boldsymbol{x}) = \sum_{i,j\in[k]\,:\,i\geq j} a_{i,j}x_i x_j,$$

where $a_{i,j} \in F$ and $\boldsymbol{x} = (x_1\ x_2\ \ldots\ x_k)$ is a vector of indeterminates. The *rank* of $Q(\boldsymbol{x})$ equals the smallest number of indeterminates that will actually appear in $Q(\boldsymbol{x}P)$, when P ranges over all nonsingular $k\times k$ matrices over F.

Through the canonical representation of $Q(\boldsymbol{x})$ (as in [9, Thms 6.21 and 6.30]), it readily follows that the rank of $Q(\boldsymbol{x})$ is the same in any extension field of F. The set of all quadratic forms in k indeterminates with rank r over $\mathbb{F}_q$ will be denoted by $\mathcal{Q}_q(k,r)$, and we will use the shorthand notation $\mathcal{Q}_q(k)$ for $\mathcal{Q}_q(k,k)$.

The next two lemmas are taken from [4, Thms. 4.5 and 4.6] (see also [9, Ch. 6]).

Lemma 52. *Given a prime power q and positive integers n, k, and $r\in[k]$, for any $Q\in\mathcal{Q}_q(k,r)$, the number of vectors $\boldsymbol{v}\in\mathbb{F}_{q^n}^k$ that satisfy $Q(\boldsymbol{v})=0$ is given by*

$$\begin{cases} q^{n(k-1)} & \text{if } r \text{ is odd} \\ q^{n(k-1)}\cdot\left(1\pm(q^n-1)\cdot q^{-rn/2}\right) & \text{if } r \text{ is even}\end{cases}.$$

Lemma 53. *Given a prime power q and a positive integer k,*

$$|\mathcal{Q}_q(k)| = q^{k(k+1)/2}\cdot\prod_{j\in[\lceil k/2\rceil]}\left(1-q^{1-2j}\right)$$

and, for any $r\in[k-1]$,

$$|\mathcal{Q}_q(k,r)| = \begin{bmatrix} k \\ r\end{bmatrix}_q\cdot|\mathcal{Q}_q(r)|\,.$$

We will also use the following bound on the q-binomial coefficients.

Lemma 54 ([8, Lemma 4])**.** *For any prime power q and integers $t\geq s\geq 0$,*

$$\begin{bmatrix} t \\ s\end{bmatrix}_q < 4\cdot q^{s(t-s)}.$$

Proof of Theorem 31. For $k=1$, every subspace in $\mathcal{G}_q(n,k)$ is a max-span Sidon space; hence we assume from now on in the proof that $k\geq 2$. Let $\xi_1,\xi_2,\ldots,\xi_k$ be elements that are uniformly and independently selected from $\mathbb{F}_{q^n}$. We bound from above the probability that the set $\{\xi_i\}_{i\in[k]}$ does not span a k-dimensional max-span Sidon space. That probability bounds from above the fraction of the spaces in $\mathcal{G}_q(n,k)$ that are not max-span Sidon spaces.

Write $\boldsymbol{\xi} = (\xi_1\ \xi_2\ \ldots\ \xi_k)$ and, for $r\in[k]$, let $\mathcal{E}_r$ denote the event that $Q(\boldsymbol{\xi})=0$ for some $Q\in\mathcal{Q}_q(k,r)$. Then $\cup_{r\in[k]}\mathcal{E}_r$ stands for the event that $\boldsymbol{\xi}$ is not a max-span Sidon space. By a union bound, we have

$$\mathsf{Prob}\left\{\cup_{r\in[k]}\mathcal{E}_r\right\} \leq \mathsf{Prob}\left\{\mathcal{E}_1\cup\mathcal{E}_2\right\} + \sum_{r=3}^{k}\mathsf{Prob}\left\{\mathcal{E}_r\right\}. \quad (12)$$

Next, we bound from above the terms in the right-hand side of (12).

Starting with $\mathcal{E}_1$, this event is equivalent to having $\boldsymbol{\xi}\cdot\boldsymbol{a}^{\mathsf{T}}=0$, for some nonzero $\boldsymbol{a}\in\mathbb{F}_q^k$; namely, it is equivalent to $\{\xi_i\}_{i\in[k]}$ being a linearly dependent set over $\mathbb{F}_q$. Turning to $\mathcal{E}_2$, shifting to canonical quadratic forms, as in [9, Thms. 6.21 and 6.30], it follows that this event is equivalent to $\boldsymbol{\xi}$ satisfying

$$p_0\cdot(\boldsymbol{\xi}\cdot\boldsymbol{a}^{\mathsf{T}})^2 + p_1\cdot(\boldsymbol{\xi}\cdot\boldsymbol{a}^{\mathsf{T}})(\boldsymbol{\xi}\cdot\boldsymbol{b}^{\mathsf{T}}) + p_2\cdot(\boldsymbol{\xi}\cdot\boldsymbol{b}^{\mathsf{T}})^2 = 0, \quad (13)$$

for some linearly independent vectors $\boldsymbol{a},\boldsymbol{b}\in\mathbb{F}_q^k$ over $\mathbb{F}_q$ and a nonzero $(p_0\ p_1\ p_2)\in\mathbb{F}_q^3$. Since (13) is equivalent to having $(\boldsymbol{\xi}\cdot\boldsymbol{a}^{\mathsf{T}})/(\boldsymbol{\xi}\cdot\boldsymbol{b}^{\mathsf{T}})\in\mathbb{F}_{q^2}$, it follows that $\mathcal{E}_2$ implies that $\{\xi_i\}_{i\in[k]}$ is a linearly dependent set over[7] $\mathbb{F}_{q^2}$. We conclude that $\mathcal{E}_1\cup\mathcal{E}_2$ implies that $\boldsymbol{\xi}\cdot\boldsymbol{a}^{\mathsf{T}}=0$, for some nonzero $\boldsymbol{a}\in\mathbb{F}_{q^2}^k$ whose leading nonzero coefficient is 1 (say). Thus,

$$\mathsf{Prob}\left\{\mathcal{E}_1\cup\mathcal{E}_2\right\} \leq \frac{q^{2k}-1}{(q^2-1)\cdot q^n} = \frac{q^k-1}{(q-1)\cdot q^n}\cdot\frac{q^k+1}{q+1}, \quad (14)$$

which proves the theorem for $k=2$ (see also Lemma 49 in Appendix A). Hence, we assume hereafter that $k\geq 3$.

[7]When n is odd, linear dependence over $\mathbb{F}_{q^2}$ is the same as linear dependence over $\mathbb{F}_q$.

In the sequel, we will need a lower bound on the following difference:

$$\frac{|\mathcal{Q}_q(k,1)|+|\mathcal{Q}_q(k,2)|}{q^n(q-1)} - \mathsf{Prob}\left\{\mathcal{E}_1\cup\mathcal{E}_2\right\}$$
$$\overset{(\star)}{\geq} \frac{1}{q^n(q-1)}\cdot \left(\begin{bmatrix}k\\1\end{bmatrix}_q\cdot|\mathcal{Q}_q(1)|+\begin{bmatrix}k\\2\end{bmatrix}_q\cdot|\mathcal{Q}_q(2)|-(q^k-1)\cdot\frac{q^k+1}{q+1}\right)$$
$$\overset{(\dagger)}{=} \frac{1}{q^n(q-1)}\cdot \left(q^k-1+\frac{q^2(q^k-1)(q^{k-1}-1)}{q^2-1}-(q^k-1)\cdot\frac{q^k+1}{q+1}\right)$$
$$= \frac{q^k-1}{q^n(q^2-1)}\cdot\frac{q^k-q}{q-1}$$
$$\overset{k\geq 3}{>} \frac{q^k-1}{q^n(q-1)}\,, \tag{15}$$

where $(\star)$ follows from (14) and Lemma 53, and $(\dagger)$ follows from Lemma 53. Continuing now with the right-hand side of (12), we have:

$$\mathsf{Prob}\left\{\cup_{r\in[k]}\mathcal{E}_r\right\} \overset{\text{Lemma 52}}{\leq} \mathsf{Prob}\left\{\mathcal{E}_1\cup\mathcal{E}_2\right\} + \frac{q^{n(k-1)}}{q^{nk}(q-1)}\cdot \left(\sum_{r=3}^{k}|\mathcal{Q}_q(k,r)|+\sum_{i=2}^{\lfloor k/2\rfloor}|\mathcal{Q}_q(k,2i)|\cdot(q^n-1)\cdot q^{-in}\right)$$
$$\overset{(15)}{<} \frac{1}{q^n(q-1)}\cdot\Bigg(\underbrace{\sum_{r\in[k]}|\mathcal{Q}_q(k,r)|}_{q^{k(k+1)/2}-1}-(q^k-1) + (q^n-1)\sum_{i=2}^{\lfloor k/2\rfloor}|\mathcal{Q}_q(k,2i)|\cdot q^{-in}\Bigg)$$
$$= \frac{q^{k(k+1)/2}-q^k}{q^n(q-1)} + \frac{q^n-1}{q^n(q-1)}\underbrace{\sum_{i=2}^{\lfloor k/2\rfloor}|\mathcal{Q}_q(k,2i)|\cdot q^{-in}}_{\triangleq\,\varepsilon(n)}$$
$$< \frac{q^{k(k+1)/2-n}}{q-1}+\frac{1}{q-1}\left(\varepsilon(n)-q^{k-n}\right).$$

Hence, in order to complete the proof, it suffices to show that $\varepsilon(n)\leq q^{k-n}$. Indeed, for $k=3$ we have $\varepsilon(n)=0$; otherwise, for $k\geq 4$,

$$\begin{aligned}
\varepsilon(n) &= \sum_{i=2}^{\lfloor k/2\rfloor}|\mathcal{Q}_q(k,2i)|\cdot q^{-in}\\
&\overset{\text{Lemma 53}}{=} \sum_{i=2}^{\lfloor k/2\rfloor}\begin{bmatrix}k\\2i\end{bmatrix}_q\cdot\underbrace{|\mathcal{Q}_q(2i)|}_{<\,q^{i(2i+1)}}\cdot q^{-in}\\
&\overset{\text{Lemma 54}}{<} 4\cdot\sum_{i=2}^{\lfloor k/2\rfloor}q^{2i(k-2i)+i(2i+1)-in}\\
&= 4\cdot q^{4k-2n-6}\sum_{i=0}^{\lfloor k/2\rfloor-2}q^{i(2k-n)-(2i+7)i}\\
&< 4\cdot q^{4k-2n-6}\underbrace{\sum_{i=0}^{\infty}q^{i(2k-n)}}_{<\,2}\\
&< q^{4k-2n-3}<q^{k-n},
\end{aligned}$$

whenever $k\geq 4$ and $n\geq\binom{k+1}{2}$. □

Remark 55. For $q=2$ and $n=\binom{k+1}{2}$, our analysis does not rule out the possibility that the fraction of max-span Sidon spaces within $\mathcal{G}_q(n,k)$ is exponentially small in n. However, empirical results suggest that, as k increases, this fraction converges—for the tested values of q—to (approximately) $\prod_{i=1}^{\infty}(1-q^{-i})$, similarly to the fraction of invertible matrices among all $k\times k$ matrices over $\mathbb{F}_q$; for $q=2$, this limit is approximately 0.288. Our analysis herein was too crude to capture this behavior, and a proof that the said fraction indeed converges to this limit is yet to be found. □

Ron M. Roth (M'88–SM'97–F'03) received the B.Sc. degree in computer engineering, the M.Sc. in electrical engineering, and the D.Sc. in computer science from Technion—Israel Institute of Technology, Haifa, Israel, in 1980, 1984, and 1988, respectively. Since 1988 he has been with the Computer Science Department at Technion, where he now holds the General Yaakov Dori Chair in Engineering. During the academic years 1989–91 he was a Visiting Scientist at IBM Research Division, Almaden Research Center, San Jose, California, and during 1996–97, 2004–05, and 2011–2012 he was on sabbatical leave at Hewlett–Packard Laboratories, Palo Alto, California. He is the author of the book *Introduction to Coding Theory*, published by Cambridge University Press in 2006. Dr. Roth was an associate editor for coding theory in IEEE TRANSACTIONS ON INFORMATION THEORY from 1998 till 2001, and he is now serving as an associate editor in *SIAM Journal on Discrete Mathematics*. His research interests include coding theory, information theory, and their application to the theory of complexity.

Netanel Raviv (S'15–M'17) received a B.Sc. in mathematics and computer science in 2010, an M.Sc. and Ph.D. in computer science in 2013 and 2016, respectively, all from the Technion, Israel. While this work was done he was a postdoctoral researcher at the Technion and at the Tel-Aviv University. He is now a postdoctoral scholar at the Center for the Mathematics of Information (CMI) at the California Institute of Technology. He is an awardee of the IBM Ph.D. fellowship for the academic year of 2015-2016, the first prize in the Feder family competition for best student work in communication technology, and the Lester-Deutsche Postdoctoral Fellowship. His research interests include applications of coding theory to networks, storage, and machine learning.

Itzhak Tamo (M'10) was born in Israel in 1981. He received a B.A. in Mathematics and a B.Sc. in Electrical Engineering in 2008, and a Ph.D. in Electrical Engineering in 2012, all from Ben-Gurion University, Israel. During 20122014 he was a postdoctoral researcher at the Institute for Systems Research, University of Maryland, College Park. Since 2015 he has been a senior lecturer in the Electrical Engineering Department, Tel Aviv University, Israel. He was a co-recipient (with Zhiying Wang and Jehoshua Bruck) of the IEEE Communication Society Data Storage Technical Committee 2013 Best Paper Award. Together with Alexander Barg, he received the 2015 IEEE Information Theory Society Paper Award. His research interests include storage systems and devices, coding, information theory, and combinatorics.