Advances in Mathematics of Communications
Volume 5, No. 2, 2011, 161–176

doi:10.3934/amc.2011.5.161

ON q-ANALOGS OF STEINER SYSTEMS AND COVERING DESIGNS

Tuvi Etzion

Computer Science Department
Technion – Israel Institute of Technology
Haifa, 32000, Israel

Alexander Vardy

Department of Electrical and Computer Engineering
Department of Computer Science and Engineering
Department of Mathematics
University of California San Diego
9500 Gilman Drive, La Jolla, CA 92093, USA

(Communicated by Axel Kohnert)

Abstract. The q-analogs of covering designs, Steiner systems, and Turán designs are studied. It is shown that q-covering designs and q-Turán designs are dual notions. A strong necessary condition for the existence of Steiner structures (the q-analogs of Steiner systems) over $\mathbb{F}_2$ is given. No Steiner structures of strength 2 or more are currently known, and our condition shows that their existence would imply the existence of new Steiner systems of strength 3. The exact values of the q-covering numbers $\mathcal{C}_q(n,k,1)$ and $\mathcal{C}_q(n,n-1,r)$ are determined for all q,n,k,r. Furthermore, recursive upper and lower bounds on the size of general q-covering designs and q-Turán designs are presented. Finally, it is proved that $\mathcal{C}_2(5,3,2) = 27$ and $\mathcal{C}_2(7,3,2) \leqslant 399$. Tables of upper and lower bounds on $\mathcal{C}_2(n,k,r)$ are given for all $n \leqslant 8$.

1. Introduction

Let $\mathbb{F}_q$ be the finite field with q elements. Given positive integers n and $k \leqslant n$, let $\mathcal{G}_q(n,k)$ denote the set of all k-dimensional subspaces of the vector space $\mathbb{F}_q^n$. The set $\mathcal{G}_q(n,k)$ is often called the Grassmannian. In recent years, there has been increasing interest in codes over Grassmannians. This interest stems from the groundbreaking work of Koetter and Kschischang [11] who showed that such codes are precisely what is needed for error-correction in networks (in the randomized noncoherent network-coding model). We observe that codes over Grassmannians are the q-analogs of constant-weight codes that have been studied in coding theory for decades.

Here, we focus on design theory, which is a principal area of combinatorics with deep connection to coding theory. Numerous objects studied in design theory have well-known q-analogs. For example, the q-analog of Sperner's theorem is included in the classic textbook of van Lint and Wilson [13, p.293]. The q-analogs of various t-designs and relationships between them have been studied in [2, 10, 14, 16, 17, 18,

2000 *Mathematics Subject Classification:* Primary: 51E10, 05B40; Secondary: 94B25.

Key words and phrases: Covering designs, q-analogs, Steiner structures, Turán designs.

This research was supported in part by the United States – Israel Binational Science Foundation (BSF), Jerusalem, Israel, under Grant Number 2006097.

19, 20] and other papers. Connections between these topics and certain problems of interest in coding theory were established in [1, 16].

In this paper, we consider the q-analogs of covering designs, Steiner systems, and Turán designs. To the best of our knowledge, the q-analogs of covering designs and Turán designs have not been previously investigated. We begin our discussion with the following definitions:

> *A q-covering design $\mathscr{C}_q(n,k,r)$ is a subset $\mathbb{S}$ of $\mathcal{G}_q(n,k)$ such that each element of $\mathcal{G}_q(n,r)$* is contained in at least one *subspace of $\mathbb{S}$. The q-covering number $\mathcal{C}_q(n,k,r)$ is the minimum size of a q-covering design $\mathscr{C}_q(n,k,r)$.*
>
> *A Steiner structure $\mathscr{S}_q(r,k,n)$ is a subset $\mathbb{S}$ of $\mathcal{G}_q(n,k)$ such that each element of $\mathcal{G}_q(n,r)$* is contained in exactly one *subspace of $\mathbb{S}$. A Steiner structure $\mathscr{S}_q(r,k,n)$, when it exists, is the smallest q-covering design $\mathscr{C}_q(n,k,r)$.*
>
> *A q-Turán design $\mathscr{T}_q(n,k,r)$ is a subset $\mathbb{S}$ of $\mathcal{G}_q(n,r)$ such that each element of $\mathcal{G}_q(n,k)$* contains at least one *subspace from $\mathbb{S}$. The q-Turán number $\mathcal{T}_q(n,k,r)$ is the minimum size of a q-Turán design $\mathscr{T}_q(n,k,r)$.*

The rest of the paper is organized as follows. In the next section, we show that a given subset of $\mathcal{G}_q(n,k)$ is a q-covering design if and only if its orthogonal complement in $\mathcal{G}_q(n,n-k)$ is a q-Turán design. Thus q-covering designs and q-Turán designs are dual notions. We also prove a simple but important bound on the size of $\mathscr{C}_q(n,k,r)$, which holds with equality if and only if $\mathscr{C}_q(n,k,r)$ is a Steiner structure. In Section 3, we establish a new necessary condition for the existence of Steiner structures over $\mathbb{F}_2$. This condition implies that constructing Steiner structures with new parameters is likely to be difficult. In Section 4, we determine the exact values of the q-covering numbers $\mathcal{C}_q(n,k,1)$ and $\mathcal{C}_q(n,n-1,r)$ for all q,n,k, and r. In Section 5, we prove several lower bounds on q-covering numbers which improve upon the bound of Section 2. In Section 6, we describe a recursive construction of q-covering designs that implies a strong upper bound on q-covering numbers. In Section 7, we present constructions and bounds for two specific q-covering numbers: we show that $\mathcal{C}_2(5,3,2)=27$ and $\mathcal{C}_2(7,3,2)\leqslant 399$. In Section 8, we compile tables of $\mathcal{C}_2(n,k,r)$ for all $n\leqslant 8$. We conclude with a list of open problems closely related to our work in Section 9.

2. Covering designs, Turán designs, and Steiner structures

In this section, we derive simple, but fundamental, connections between the combinatorial objects studied in this paper: q-covering designs, q-Turán designs, and Steiner structures. Although we will assume throughout that the ambient space is $\mathbb{F}_q^n$, we point out that our results hold for an arbitrary n-dimensional vector space over $\mathbb{F}_q$.

Two vectors $\boldsymbol{u},\boldsymbol{v}$ in $\mathbb{F}_q^n$ are said to be *orthogonal* if $(\boldsymbol{u},\boldsymbol{v})=0$, where $(\cdot,\cdot)$ stands for the usual inner product over $\mathbb{F}_q$. For a subspace V of $\mathbb{F}_q^n$, its dual $V^\perp$ is given by

$$V^\perp \overset{\text{def}}{=} \left\{ \boldsymbol{u}\in\mathbb{F}_q^n \ : \ (\boldsymbol{u},\boldsymbol{v})=0 \text{ for all } \boldsymbol{v}\in V \right\}.$$

It is easy to see that $\dim V^\perp = n-k$ if and only if $\dim V = k$. Given a subset $\mathbb{S}$ of $\mathcal{G}_q(n,k)$, we define its *orthogonal complement* as $\mathbb{S}^\perp = \{V^\perp\in\mathcal{G}_q(n,n-k) \ : \ V\in\mathbb{S}\}$.

Theorem 2.1. *A subset $\mathbb{S}$ of $\mathcal{G}_q(n,k)$ is a q-covering design $\mathscr{C}_q(n,k,r)$ if and only if its orthogonal complement $\mathbb{S}^\perp$ is a q-Turán design $\mathscr{T}_q(n,n-r,n-k)$.*

Proof. Assume, first, that $\mathbb{S}$ is a q-covering design $\mathscr{C}_q(n,k,r)$. Consider an arbitrary subspace U in $\mathcal{G}_q(n,n-r)$. Then $\dim U^\perp = r$ and, hence, there exists at least one

$V \in \mathbb{S}$ such that $U^\perp \subseteq V$. But $U^\perp \subseteq V$ if and only if $V^\perp \subseteq U$. Since $V^\perp \in \mathbb{S}^\perp$ and U was arbitrary, it follows that *every* subspace in $\mathcal{G}_q(n, n-r)$ contains at least one element of $\mathbb{S}^\perp$. Thus $\mathbb{S}^\perp$ is a q-Turán design $\mathscr{T}_q(n, n-r, n-k)$. A similar argument shows that if $\mathbb{S}$ is a q-Turán design $\mathscr{T}_q(n, n-r, n-k)$ then $\mathbb{S}^\perp$ is a q-covering design $\mathscr{C}_q(n,k,r)$. Again, the key point is that $V^\perp \subseteq U$ if and only if $U^\perp \subseteq V$. □

Corollary 2.2.

$$\mathcal{C}_q(n,k,r) \ = \ \mathcal{T}_q(n, n-r, n-k).$$

Theorem 2.1 and Corollary 2.2 imply that q-covering designs and q-Turán designs are dual objects. The next theorem provides a simple, but fundamental, lower bound on $\mathcal{C}_q(n,k,r)$, and establishes the connection between q-covering designs and Steiner structures. Note that the *q-ary Gaussian coefficient* $\begin{bmatrix} n \\ k \end{bmatrix}_q$ is defined as follows:

$$\begin{bmatrix} n \\ k \end{bmatrix}_q \overset{\text{def}}{=} \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)} \quad \text{and} \quad \begin{bmatrix} n \\ 0 \end{bmatrix}_q \overset{\text{def}}{=} 1.$$

Theorem 2.3. *Let $\mathbb{S}$ be a q-covering design $\mathscr{C}_q(n,k,r)$. Then $|\mathbb{S}| \geqslant \begin{bmatrix} n \\ r \end{bmatrix}_q \Big/ \begin{bmatrix} k \\ r \end{bmatrix}_q$ with equality if and only if $\mathbb{S}$ is a Steiner structure.*

Proof. Every element of $\mathbb{S}$ has dimension k, and therefore contains (covers) exactly $\begin{bmatrix} k \\ r \end{bmatrix}_q$ distinct r-dimensional subspaces. The total number of r-dimensional subspaces covered is $\begin{bmatrix} n \\ r \end{bmatrix}_q$, and hence $|\mathbb{S}| \geqslant \begin{bmatrix} n \\ r \end{bmatrix}_q / \begin{bmatrix} k \\ r \end{bmatrix}_q$.

If $|\mathbb{S}|$ achieves this bound with equality, each r-dimensional subspace is contained in exactly one element of $\mathbb{S}$, which means that $\mathbb{S}$ is a Steiner structure $\mathscr{S}_q(r,k,n)$. □

3. On the existence of Steiner structures

It follows from Theorem 2.3 that the most interesting q-covering designs are Steiner structures, which are the natural q-analogs of Steiner systems. For which parameters do Steiner structures exist? Clearly, $\mathscr{S}_q(r,r,n)$ and $\mathscr{S}_q(1,n,n)$ exist for all r and n. These are trivial structures. The only nontrivial Steiner structures known [1, 3, 13, 16] are of the form $\mathscr{S}_q(1,k,n)$. These Steiner structures, also called *spreads*, exist if and only if k divides n. Various constructions of spreads can be found in [3, 7, 9] and other papers. For all other parameters, no Steiner structures are known. Based upon the results reported by Thomas [19, 20] and upon the extensive computer search we have performed, it is tempting to conjecture that no such Steiner structures exist. The present section provides further evidence for this conjecture.

Recall that a *Steiner system* $\mathcal{S}(t,k,n)$ is a collection $\mathbb{S}$ of k-subsets (called blocks) of an n-set such that every t-subset of the n-set is contained in exactly one block of $\mathbb{S}$. The parameter t is said to be the *strength* of the system. The following connections between Steiner structures and Steiner systems were established in [20] and [16].

Theorem 3.1. *Existence of a Steiner structure $\mathscr{S}_q(2,k,n)$ implies the existence of Steiner systems $\mathcal{S}\big(2, q^{k-1}, q^{n-1}\big)$ and $\mathcal{S}\big(2, (q^k-1)/(q-1), (q^n-1)/(q-1)\big)$. Furthermore, existence of $\mathscr{S}_2(3,k,n)$ implies the existence of $\mathcal{S}(3, 2^{k-1}, 2^{n-1})$.*

Theorem 3.1 does *not* indicate that constructing new Steiner structures, especially $\mathscr{S}_q(2,k,n)$, is a formidable task. By Theorem 3.1, such Steiner structures lead to Steiner systems of strength 2, which are not that rare. The case $q = 2$ appears to be the easiest; indeed, numerous $\mathcal{S}(2, 2^{k-1}, 2^{n-1})$ and $\mathcal{S}(2, 2^k-1, 2^n-1)$ Steiner systems are known [6]. Our main result is the following theorem, which shows that constructing $\mathscr{S}_2(2,k,n)$ is likely to be much harder than what Theorem 3.1 suggests.

Theorem 3.2. *Existence of a Steiner structure $\mathscr{S}_2(2,k,n)$ implies the existence of a Steiner system $\mathcal{S}(3,2^k,2^n)$.*

Proof. Let $\mathbb{S}$ be a Steiner structure $\mathscr{S}_2(2,k,n)$. Each subspace of $\mathbb{S}$ partitions $\mathbb{F}_2^n$ into 2^{n-k} additive translates of itself. Consider the set of all such translates, namely:

$$\mathbb{S}' \overset{\text{def}}{=} \Big\{ \{\boldsymbol{u}, \boldsymbol{u}+\boldsymbol{v}_1, \boldsymbol{u}+\boldsymbol{v}_2, \ldots, \boldsymbol{u}+\boldsymbol{v}_{2^k-1}\} \ : \ \{\boldsymbol{0}, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{2^k-1}\} \in \mathbb{S},\ \boldsymbol{u} \in \mathbb{F}_2^n \Big\}.$$

We claim that $\mathbb{S}'$ is a Steiner system $\mathcal{S}(3,2^k,2^n)$. Observe that $\mathbb{S}'$ has the right cardinality. That is

$$|\mathbb{S}'| = 2^{n-k}|\mathbb{S}| = 2^{n-k}\frac{\begin{bmatrix} n \\ 2 \end{bmatrix}_2}{\begin{bmatrix} k \\ 2 \end{bmatrix}_2} = 2^{n-k}\frac{(2^n-1)(2^{n-1}-1)}{(2^k-1)(2^{k-1}-1)} = \frac{\binom{2^n}{3}}{\binom{2^k}{3}} = \big|\mathcal{S}(3,2^k,2^n)\big|.$$

Hence, to complete the proof, it would suffice to show that every 3-subset $\{\boldsymbol{x},\boldsymbol{y},\boldsymbol{z}\}$ of $\mathbb{F}_2^n$ is contained in some block of $\mathbb{S}'$. Since $\mathbb{S}$ is a Steiner structure $\mathscr{S}_2(2,k,n)$, the two-dimensional subspace $\{\boldsymbol{0}, \boldsymbol{x}+\boldsymbol{y}, \boldsymbol{x}+\boldsymbol{z}, \boldsymbol{y}+\boldsymbol{z}\}$ is contained in some k-dimensional subspace of $\mathbb{S}$, call it V. By the definition of $\mathbb{S}'$, we know that $\boldsymbol{x}+V$ is a block of $\mathbb{S}'$. But $\boldsymbol{x} + \{\boldsymbol{0}, \boldsymbol{x}+\boldsymbol{y}, \boldsymbol{x}+\boldsymbol{z}, \boldsymbol{y}+\boldsymbol{z}\} = \{\boldsymbol{x},\boldsymbol{y},\boldsymbol{z},\boldsymbol{x}+\boldsymbol{y}+\boldsymbol{z}\}$ and therefore $\{\boldsymbol{x},\boldsymbol{y},\boldsymbol{z}\} \subset \boldsymbol{x}+V$. □

At present, no $\mathcal{S}(3,2^k,2^n)$ Steiner systems with $2^k \geqslant 8$ are known. Numerous efforts to find such Steiner systems, spanning several decades, have been unsuccessful. In view of this, Theorem 3.2 implies that constructing $\mathscr{S}_2(2,k,n)$, if such structures at all exist, would be extraordinarily difficult.

In fact, the same conclusion can be extended to *any* Steiner structure over $\mathbb{F}_2$ with new parameters. It is shown in [16] and [20] that given a Steiner structure $\mathscr{S}_q(r,k,n)$, one can always construct the derived structure $\mathscr{S}_q(r-1,k-1,n-1)$. Consequently, if $\mathscr{S}_2(r,k,n)$ exists for some $k > r \geqslant 2$, then $\mathscr{S}_2(2,k-r+2,n-r+2)$ also exists, which implies by Theorem 3.2 the existence of a Steiner system $\mathcal{S}(3,2^{k-r+2},2^{n-r+2})$.

Among the $\mathscr{S}_2(2,3,n)$ Steiner structures, those of the form $\mathscr{S}_2(2,3,n)$ have the smallest parameters. Thus resolving their existence is a natural target for investigation. It can be easily shown that if $\mathscr{S}_2(2,3,n)$ exists, we must have $n \equiv 1,3 \pmod 6$. Many other necessary conditions for the existence of $\mathscr{S}_2(2,3,n)$ can be obtained by considering derived designs related to any fixed $(n-1)$-dimensional subspace.

4. Optimal q-covering designs

In this section, we determine the exact values of the q-covering numbers $\mathcal{C}_q(n,k,1)$ and $\mathcal{C}_q(n,n-1,r)$ for all q, n, k, and r. In each case, explicit constructions of the corresponding optimal q-covering designs are given.

Lemma 4.1.

$$\mathcal{C}_q(n,k,1) = \frac{q^n-1}{q^k-1} \qquad \textit{whenever } k \textit{ divides } n.$$

Proof. By Theorem 2.3, a Steiner structure $\mathscr{S}_q(1,k,n)$ is an optimal q-covering design, when it exists. As shown in [3, 16] and other papers, such Steiner structures exist iff k divides n, and it is easy to see that $|\mathscr{S}_q(1,k,n)| = (q^n-1)/(q^k-1)$. □

Lemma 4.2.

$$\mathcal{C}_q(n,k,r) \leqslant \mathcal{C}_q(n-1,k-1,r).$$

Proof. Let us represent $\mathbb{F}_q^n$ as $\mathbb{F}_q^{n-1} \times \mathbb{F}_q$, namely $\mathbb{F}_q^n = \big\{(\boldsymbol{x},\alpha) : \boldsymbol{x} \in \mathbb{F}_q^{n-1},\ \alpha \in \mathbb{F}_q\big\}$. Let $\mathbb{S}$ be a q-covering design $\mathscr{C}_q(n-1,k-1,r)$ in $\mathbb{F}_q^{n-1}$. For each $V \in \mathbb{S}$, we define

$$V' \overset{\text{def}}{=} \big\{\,(\boldsymbol{v},\alpha)\ :\ \boldsymbol{v} \in V,\ \alpha \in \mathbb{F}_q\,\big\}.$$

Then V' is a k-dimensional subspace of $\mathbb{F}_q^n = \mathbb{F}_q^{n-1} \times \mathbb{F}_q$. Let $\mathbb{S}'$ be the set of all such subspaces, that is $\mathbb{S}' = \{V' \in \mathcal{G}_q(n,k)\ :\ V \in \mathbb{S}\}$. It can be easily verified that $\mathbb{S}'$ is a q-covering design $\mathscr{C}_q(n,k,r)$, and the lemma follows. □

Corollary 4.3.

$$\mathcal{C}_q(n+\delta,k+\delta,r) \leqslant \mathcal{C}_q(n,k,r) \qquad \textit{for all nonnegative integers } \delta.$$

Lemma 4.4.

$$\mathcal{C}_q(n,k,1) \;=\; q^{n-k}+1 \qquad \textit{for } k = \left\lceil \tfrac{n}{2} \right\rceil, \left\lceil \tfrac{n}{2} \right\rceil + 1, \ldots, n-1.$$

Proof. We have $\mathcal{C}_q(2(n-k),n-k,1) = (q^{2(n-k)}-1)/(q^{n-k}-1) = q^{n-k}+1$ by Lemma 4.1. Let $\delta = 2k-n$. Then δ is a nonnegative integer for $k \geqslant n/2$, and therefore

$$\mathcal{C}_q(n,k,1) \;=\; \mathcal{C}_q\big(2(n-k)+\delta, n-k+\delta, 1\big) \;\leqslant\; \mathcal{C}_q\big(2(n-k), n-k, 1\big) \;=\; q^{n-k}+1$$

in view of Corollary 4.3. On the other hand, $\mathcal{C}_q(n,k,1) \geqslant (q^n-1)/(q^k-1)$ by Theorem 2.3. But $\big\lceil (q^n-1)/(q^k-1) \big\rceil = q^{n-k}+1$ for all $k = \lceil n/2 \rceil, \lceil n/2 \rceil + 1, \ldots, n-1$, which completes the proof of the lemma. □

The proof of Lemma 4.4 indicates how q-covering designs that achieve the q-covering number $\mathcal{C}_q(n,k,1) = q^{n-k}+1$ can be constructed. Start with a Steiner structure $\mathscr{S}_q\big(2(n-k),n-k,1\big)$. In order to construct $\mathscr{S}_q\big(2(n-k),n-k,1\big)$, any of the several known constructions of spreads can be used [3, 7]. Next, apply the construction described in the proof of Lemma 4.2 iteratively $\delta = 2k-n$ times. This method applies whenever $k \geqslant n/2$. It is interesting that for $k < n/2$, a completely different construction is required. In particular, we will make use of the following lemma.

Lemma 4.5. *Let ρ be the remainder obtained when k is divided into n, and define $m = k+\rho$. Then there exists a set $\mathbb{X}$ consisting of one m-dimensional subspace of $\mathbb{F}_q^n$ and $(q^n-q^m)/(q^k-1)$ k-dimensional subspaces of $\mathbb{F}_q^n$, such that*

$$V \cap V' \;=\; \{\mathbf{0}\} \qquad \textit{for all } V, V' \in \mathbb{X}. \tag{1}$$

An explicit construction of the set $\mathbb{X}$ along with a detailed proof of Lemma 4.5 can be found in [8, Section III]. Let U be a one-dimensional subspace of $\mathbb{F}_q^n$. Then (1) implies that there is *at most one* subspace V of $\mathbb{X}$ that contains U. The total number of one-dimensional subspaces contained in some subspace of $\mathbb{X}$ is given by

$$\frac{q^n-q^m}{q^k-1}\begin{bmatrix} k \\ 1 \end{bmatrix}_q + \begin{bmatrix} m \\ 1 \end{bmatrix}_q \;=\; \frac{q^n-q^m}{q^k-1}\cdot\frac{q^k-1}{q-1} + \frac{q^m-1}{q-1} \;=\; \frac{q^n-1}{q-1} \;=\; \begin{bmatrix} n \\ 1 \end{bmatrix}_q.$$

This implies that *every* one-dimensional subspace of $\mathbb{F}_q^n$ is contained in *exactly one* subspace of $\mathbb{X}$. Thus $\mathbb{X}$ can be regarded as a generalization of the notion of a spread to the case where k does not divide n (if k divides n, the set $\mathbb{X}$ is, in fact, a spread).

Theorem 4.6.

$$\mathcal{C}_q(n,k,1) \;=\; \left\lceil \frac{q^n-1}{q^k-1} \right\rceil \qquad \textit{for } k=1,2,\ldots,n.$$

Proof. As in Lemma 4.5, let ρ be the remainder obtained when k is divided into n, and define $m=k+\rho$. If $\rho=0$, the claim of the theorem follows immediately from Lemma 4.1. Thus it remains to consider the case where k does not divide n, and therefore $k<m<2k$. In this case, we will modify the set $\mathbb{X}$ exhibited in Lemma 4.5 to obtain a q-covering design $\mathscr{C}_q(n,k,1)$, as follows. Let $\mathcal{W}$ denote the single m-dimensional subspace of $\mathbb{X}$, and let $\mathbb{S}$ be a q-covering design consisting of k-dimensional subspaces of $\mathcal{W}$ such that every one-dimensional subspace of $\mathcal{W}$ is contained in at least one element of $\mathbb{S}$. Then clearly $\mathbb{S}\cup\big(\mathbb{X}\setminus\{\mathcal{W}\}\big)$ is a q-covering design $\mathscr{C}_q(n,k,1)$. Since $\dim\mathcal{W}=m$, this implies that

$$(2)\quad \mathcal{C}_q(n,k,1) \;\leqslant\; \frac{q^n-q^m}{q^k-1} + \mathcal{C}_q(m,k,1) \;=\; \frac{q^n-q^m}{q^k-1} + q^{m-k}+1 \;=\; \frac{q^n-q^\rho}{q^k-1}+1$$

where the first equality follows from Lemma 4.4 along with the fact that $k<m<2k$. Note that the right-hand side of (2) is equal to $\left\lceil (q^n-1)/(q^k-1)\right\rceil$ when $\rho\neq 0$. Finally, observe that $\mathcal{C}_q(n,k,1)\geqslant\left\lceil (q^n-1)/(q^k-1)\right\rceil$ by Theorem 2.3. □

Corollary 4.7.

$$\mathcal{T}_q(n,n-1,r) \;=\; \left\lceil \frac{q^n-1}{q^{n-r}-1} \right\rceil \qquad \textit{for } r=1,2,\ldots,n-1.$$

Proof. Follows from Theorem 4.6 and Corollary 2.2. □

Having determined the q-covering numbers $\mathcal{C}_q(n,k,1)$ in Theorem 4.6, let us now deal with $\mathcal{C}_q(n,n-1,r)$. In this case, it will be more convenient to consider the dual problem of determining the q-Turán numbers $\mathcal{T}_q(n,k,1)$. We begin with a simple upper bound on $\mathcal{T}_q(n,k,r)$ that holds for all q,n,k and r.

Lemma 4.8.

$$\mathcal{T}_q(n,k,r) \;\leqslant\; \begin{bmatrix} n-k+r \\ r \end{bmatrix}_q.$$

Proof. Let U be any fixed subspace of $\mathbb{F}_q^n$ with $\dim U = n-k+r$. Let $\mathbb{S}$ be the set of all r-dimensional subspaces of U. Clearly, $|\mathbb{S}| = \left[{n-k+r \atop r}\right]_q$. We claim that $\mathbb{S}$ is a q-Turán design $\mathscr{T}_q(n,k,r)$. To see this, consider an arbitrary k-dimensional subspace V of $\mathbb{F}_q^n$. Then $U\cap V$ is a subspace of U of dimension

$$\dim(U\cap V) \;=\; \dim U + \dim V - \dim(U+V) \;\geqslant\; (n-k+r)+k-n \;=\; r$$

and as such it must contain at least one element of $\mathbb{S}$. Thus $\mathbb{S}$ is, indeed, a q-Turán design $\mathscr{T}_q(n,k,r)$, and the lemma follows. □

Corollary 4.9.

$$\mathcal{C}_q(n,k,r) \;\leqslant\; \begin{bmatrix} n-k+r \\ r \end{bmatrix}_q.$$

Proof. $\mathcal{C}_q(n,k,r) = \mathcal{T}_q(n,n-r,n-k)$ by Corollary 2.2. Now use the upper bound on $\mathcal{T}_q(n,n-r,n-k)$ in Lemma 4.8 and observe that $\left[{n-(n-r)+(n-k) \atop n-k}\right]_q = \left[{n-k+r \atop r}\right]_q$. □

Theorem 4.10.

$$\mathcal{T}_q(n,k,1) \;=\; \frac{q^{n-k+1}-1}{q-1} \qquad \textit{for } k=1,2,\ldots,n.$$

Proof. The fact that $\mathcal{T}_q(n,k,1)\leqslant(q^{n-k+1}-1)/(q-1)$ follows as a special case of Lemma 4.8 with $r=1$. Hence, it remains to prove that $(q^{n-k+1}-1)/(q-1)$ is also an upper bound on $\mathcal{T}_q(n,k,1)$. To this end, consider an arbitrary set $\mathbb{S}$ of one-dimensional subspaces of $\mathbb{F}_q^n$ with $|\mathbb{S}| = (q^{n-k+1}-1)/(q-1)-1$. We claim that there is a k-dimensional subspace of $\mathbb{F}_q^n$ that does not contain any element of $\mathbb{S}$.

Let U be the largest subspace of $\mathbb{F}_q^n$ such that $U \cap V = \{\mathbf{0}\}$ for all $V \in \mathbb{S}$. Define $m = \dim U$. If $m \geqslant k$ we are done, since then every k-dimensional subspace of U does not contain any element of $\mathbb{S}$. Thus let us assume to the contrary that $m < k$. Now fix a $V \in \mathbb{S}$ and consider the vector space $\langle V \cup U \rangle$ spanned by all the vectors in the set $V \cup U$. Since $\dim U = m$, $\dim V = 1$, and $U \cap V = \{\mathbf{0}\}$, we have $\dim \langle V \cup U \rangle = m+1$. Thus $\langle V \cup U \rangle$ contains exactly $q^{m+1} - q^m$ vectors that are not contained in U. Hence

$$\left| \bigcup_{V\in\mathbb{S}} \langle V \cup U \rangle \right| \leqslant |\mathbb{S}|\big(q^{m+1} - q^m\big) + |U| = q^{n-k+m+1} - q^m(q-1). \tag{3}$$

For $m < k$, the right-hand side of (3) is bounded by $q^n - 1$. Consequently, there exists a nonzero vector $\boldsymbol{x} \in \mathbb{F}_q^n$ such that $\boldsymbol{x} \notin \cup_{V\in\mathbb{S}} \langle V \cup U \rangle$. Consider the vector space $\mathcal{W} = \langle \{\boldsymbol{x}\} \cup U \rangle$. We have $\mathcal{W} \cap V = \{\mathbf{0}\}$ for all $V \in \mathbb{S}$ and $\dim \mathcal{W} = m+1$, by the definition of $\boldsymbol{x}$. But this is in contradiction to the maximality of U. It follows that we must have $m \geqslant k$, which establishes the claim of the foregoing paragraph. □

Corollary 4.11.

$$\mathcal{C}_q(n, n-1, r) = \frac{q^{r+1}-1}{q-1} \qquad \textit{for } r = 1, 2, \ldots, n-1.$$

To construct q-covering designs that achieve the q-covering number $\mathcal{C}_q(n, n-1, r)$ in Corollary 4.11, first construct a q-Turán design $\mathscr{T}_q(n, n-r, 1)$ as the set of all one-dimensional subspaces of a fixed vector space $U \subset \mathbb{F}_q^n$ of dimension $r+1$ (cf. Lemma 4.8), then take the orthogonal complement of $\mathscr{T}_q(n, n-r, 1)$ as in Theorem 2.1.

5. Lower bounds on q-covering numbers

We now present two lower bounds on q-covering numbers. In Theorem 5.1 and Corollary 5.2, we establish the q-analog of a well-known bound of Schönheim [15]. In Theorem 5.3, we state the q-analog of a bound by de Caen [5].

Theorem 5.1.

$$\mathcal{C}_q(n,k,r) \geqslant \left\lceil \frac{q^n-1}{q^k-1}\, \mathcal{C}_q\big(n-1, k-1, r-1\big) \right\rceil.$$

Proof. Let $\mathbb{S}$ be a q-covering design $\mathscr{C}_q(n,k,r)$ with $|\mathbb{S}| = \mathcal{C}_q(n,k,r)$. Each element of $\mathbb{S}$ contains $(q^k-1)/(q-1)$ one-dimensional subspaces of $\mathbb{F}_q^n$. Since the total number of such subspaces is $(q^n-1)/(q-1)$, there is a one-dimensional subspace $X \subset \mathbb{F}_q^n$ that is contained in at most $(q^k-1)/(q^n-1)|\mathbb{S}|$ elements of $|\mathbb{S}|$. Let us represent $\mathbb{F}_q^n$ as $X \oplus \mathcal{W}$, where $\mathcal{W}$ is an $(n-1)$-dimensional subspace, and define

$$\mathbb{S}' \overset{\text{def}}{=} \Big\{ V \cap \mathcal{W} \ :\ V \in \mathbb{S} \text{ and } X \subset V \Big\}.$$

By construction, the set $\mathbb{S}'$ consists of at most $(q^k-1)/(q^n-1)|\mathbb{S}|$ subspaces of $\mathcal{W}$, one such subspace for each $V \in \mathbb{S}$ that contains X. We claim that $\mathbb{S}'$ is a q-covering design $\mathscr{C}_q(n-1, k-1, r-1)$, and therefore

$$\mathcal{C}_q(n-1, k-1, r-1) \leqslant \frac{q^k-1}{q^n-1}\,|\mathbb{S}| = \frac{q^k-1}{q^n-1}\,\mathcal{C}_q(n,k,r). \tag{4}$$

It is clear that $\mathbb{S}'$ consists of $(k-1)$-dimensional subspaces of $\mathcal{W}$, a vector space of dimension $n-1$. Hence in order to prove the claim, we need to show that every $(r-1)$-

dimensional subspace of $\mathcal{W}$ is contained in at least one element of $\mathbb{S}'$. Let U be such a subspace. Then $X \oplus U$ is an r-dimensional subspace of $\mathbb{F}_q^n$. Therefore, there exists a $V \in \mathbb{S}$ such that $X \oplus U \subset V$. But then $V' = V \cap \mathcal{W}$ is an element of $\mathbb{S}'$. Moreover $U \subset \mathcal{W}$ and $X \oplus U \subset V$ together imply that $U \subset V'$. This proves our claim that $\mathbb{S}'$ is a q-covering design $\mathscr{C}_q(n-1, k-1, r-1)$ and establishes (4). The theorem then follows as an immediate consequence of (4). □

Corollary 5.2.

$$\mathcal{C}_q(n,k,r) \geqslant \left\lceil \frac{q^n-1}{q^k-1} \left\lceil \frac{q^{n-1}-1}{q^{k-1}-1} \cdots \left\lceil \frac{q^{n-r+1}-1}{q^{k-r+1}-1} \right\rceil \cdots \right\rceil \right\rceil.$$

Proof. Follows by applying Theorem 5.1 iteratively $r-1$ times, then observing that $\mathcal{C}_q(n-r+1, k-r+1, 1) = \lceil (q^{n-r+1}-1)/(q^{k-r+1}-1) \rceil$ by Theorem 4.6. □

Note that if one ignores all the ceilings in Corollary 5.2, one recovers precisely the lower bound $\begin{bmatrix} n \\ r \end{bmatrix}_q / \begin{bmatrix} k \\ r \end{bmatrix}_q$ of Theorem 2.3. Thus Corollary 5.2 is always at least as strong (and usually much stronger) as Theorem 2.3.

Corollary 5.2 is the q-analog of the well-known Schönheim bound [15] on (ordinary) covering numbers $C(n,k,r)$. Recall that $C(n,k,r)$ is defined as the smallest number of k-subsets of an n-set that cover (contain) every r-subset of the n-set. Schönheim's bound [15] asserts that

$$C(n,k,r) \geqslant \left\lceil \frac{n}{k} \left\lceil \frac{n-1}{k-1} \cdots \left\lceil \frac{n-r+1}{k-r+1} \right\rceil \cdots \right\rceil \right\rceil. \tag{5}$$

Another general lower bound on covering numbers is due to de Caen [4]. This bound, which is often better than (5) for large k and r, asserts that

$$C(n,k,r) \geqslant \frac{(r+1)(n-r)}{(k+1)(n-k)} \frac{\binom{n}{r}}{\binom{k}{r}}.$$

Unfortunately, we could not prove the q-analog of this bound for all values of q, n, k and r. However, we do have a proof for the special case where $r = k-1$.

Theorem 5.3.

$$\mathcal{C}_q(n,k,k-1) \geqslant \frac{(q^k-1)(q-1)}{(q^{n-k}-1)^2} \begin{bmatrix} n \\ k+1 \end{bmatrix}_q.$$

The proof of Theorem 5.3 follows closely the argument of de Caen in [5], and proceeds by establishing the equivalent result for q-Turán numbers, namely

$$\mathcal{T}_q(n,r+1,r) \geqslant \frac{(q^{n-r}-1)(q-1)}{(q^r-1)^2} \begin{bmatrix} n \\ r-1 \end{bmatrix}_q. \tag{6}$$

We omit the technical details of our proof of (6), since this proof is essentially q-identical to de Caen's proof of the analogous result for Turán designs in [5].

6. An upper bound on q-covering numbers

So far, the only general upper bound we have for q-covering numbers (resp. q-Turán numbers) is Corollary 4.9 (resp. Lemma 4.8). Although this bound is tight for $r = 1$ (cf. Theorem 4.10 and Corollary 4.11), it is quite weak for $r \geqslant 2$. In this section, we introduce a recursive construction of q-covering designs that leads to a new general upper bound on $\mathcal{C}_q(n,k,r)$, which improves considerably upon Corollary 4.9. In contrast to Theorem 5.1 and Theorem 5.3, the construction described in the following theorem is *not* a q-analog of any known construction of covering designs.

Theorem 6.1.

$$\mathcal{C}_q(n,k,r) \leqslant q^{n-k}\mathcal{C}_q(n-1,k-1,r-1) + \mathcal{C}_q(n-1,k,r).$$

Proof. As in Lemma 4.2, let us represent $\mathbb{F}_q^n$ as $\{(\boldsymbol{x},\alpha) : \boldsymbol{x}\in\mathbb{F}_q^{n-1},\ \alpha\in\mathbb{F}_q\}$. Suppose that $\mathbb{S}_1$ is a q-covering design $\mathscr{C}_q(n-1,k,r)$ in $\mathbb{F}_q^{n-1}$, and $\mathbb{S}_2$ is a q-covering design $\mathscr{C}_q(n-1,k-1,r-1)$ in $\mathbb{F}_q^{n-1}$. Given a subspace V of $\mathbb{F}_q^{n-1}$, we define a corresponding subspace $V\times\{0\}$ of $\mathbb{F}_q^n$ as follows: $V\times\{0\} = \{(\boldsymbol{v},0)\in\mathbb{F}_q^n : \boldsymbol{v}\in V\}$. It is clear that $\dim\big(V\times\{0\}\big) = \dim V$. Also note that if $\dim V = k-1$, there are exactly q^{n-k} distinct subspaces of the form $\big(V\times\{0\}\big)\oplus\langle(\boldsymbol{x},1)\rangle$, each of dimension k (since we can choose $\boldsymbol{x}$ from any one of the q^{n-k} cosets of V in $\mathbb{F}_q^{n-1}$). With this, we now define the sets $\mathbb{S}_1'$ and $\mathbb{S}_2'$ as follows:

$$\mathbb{S}_1' \overset{\text{def}}{=} \Big\{V\times\{0\}\subset\mathbb{F}_q^n \ :\ V\in\mathbb{S}_1\Big\},$$

$$\mathbb{S}_2' \overset{\text{def}}{=} \Big\{\big(V\times\{0\}\big)\oplus\big\langle(\boldsymbol{x},1)\big\rangle\subset\mathbb{F}_q^n \ :\ V\in\mathbb{S}_2,\ \boldsymbol{x}\in\mathbb{F}_q^{n-1}\Big\}.$$

Let $\mathbb{S}' = \mathbb{S}_1'\cup\mathbb{S}_2'$. By construction, the set $\mathbb{S}'$ consists of $|\mathbb{S}_1| + q^{n-k}|\mathbb{S}_2|$ subspaces of $\mathbb{F}_q^n$, each of dimension k. Therefore, to complete the proof, it remains to show that for each r-dimensional subspace U of $\mathbb{F}_q^n$ there is a subspace $V'\in\mathbb{S}'$ such that $U\subset V'$.

First, suppose that $U\subset\mathbb{F}_q^{n-1}\times\{0\}$. Then U is contained in at least one subspace of $\mathbb{S}_1'$, since $\mathbb{S}_1'$ is a $\mathscr{C}_q(n-1,k,r)$ q-covering design in $\mathbb{F}_q^{n-1}\times\{0\}$. If U is not a subset of $\mathbb{F}_q^{n-1}\times\{0\}$, it must contain a vector of the form $(\boldsymbol{x},1)$ for some $\boldsymbol{x}\in\mathbb{F}_q^{n-1}$. This, in turn, implies that U admits a basis of the form $\{(\boldsymbol{u}_1,0),(\boldsymbol{u}_2,0),\ldots,(\boldsymbol{u}_{r-1},0),(\boldsymbol{x},1)\}$ and, hence, can be represented as $\big(U'\times\{0\}\big)\oplus\langle(\boldsymbol{x},1)\rangle$, where $U' = \langle\boldsymbol{u}_1,\boldsymbol{u}_2,\ldots,\boldsymbol{u}_{r-1}\rangle$. Since U' is an $(r-1)$-dimensional subspace of $\mathbb{F}_q^{n-1}$ whereas $\mathbb{S}_2$ is a q-covering design $\mathscr{C}_q(n-1,k-1,r-1)$ in $\mathbb{F}_q^{n-1}$, there exists a subspace $V\in\mathbb{S}_2$ that contains U'. It is easy to see that the corresponding subspace $\big(V\times\{0\}\big)\oplus\langle(\boldsymbol{x},1)\rangle$ of $\mathbb{S}_2'$ contains U. □

The construction of Theorem 6.1 can be iterated to obtain an upper bound on the q-covering number $\mathcal{C}_q(n,k,r)$ for any given set of parameters. For example, we have

$$\mathcal{C}_2(5,3,2) \leqslant 2^2\mathcal{C}_2(4,2,1)+\mathcal{C}_2(4,3,2) = 2^2\cdot 5+7 = 27, \tag{7}$$

$$\mathcal{C}_2(6,3,2) \leqslant 2^3\mathcal{C}_2(5,2,1)+\mathcal{C}_2(5,3,2) \leqslant 2^3\cdot 11+27 = 115, \tag{8}$$

$$\mathcal{C}_2(7,3,2) \leqslant 2^4\mathcal{C}_2(6,2,1)+\mathcal{C}_2(6,3,2) \leqslant 2^4\cdot 21+115 = 451, \tag{9}$$

where we have also made use of Corollary 4.11 (which implies that $\mathcal{C}_2(4,3,2)=7$) and Theorem 4.6 (which implies $\mathcal{C}_2(4,2,1)=5$, $\mathcal{C}_2(5,2,1)=11$, and $\mathcal{C}_2(6,2,1)=21$). Continuing in this manner, we arrive at the following bound:

$$\mathcal{C}_q(n,k,2) \leqslant \frac{q^3-1}{q-1} + \sum_{i=1}^{n-k-1} q^{n-k-i+1}\left\lceil\frac{q^{n-i}-1}{q^{k-1}-1}\right\rceil.$$

Alternatively, consider the recursion $g(n) = 4g(n-1)+2^{n-2}-1$, bootstrapped with $g(4)=\mathcal{C}_2(4,2,1)=5$. Then Theorem 6.1 implies that $\mathcal{C}_2(n,n-2,n-3)\leqslant g(n)$, and solving the recursion, we obtain $\mathcal{C}_2(n,n-2,n-3)\leqslant 9\cdot 2^{2n-8}-2^{n-2}-(2^{2n-8}-1)/3$.

7. Covering numbers for specific parameters

This section contains two specific results: $\mathcal{C}_2(5,3,2) = 27$ and $\mathcal{C}_2(7,3,2) \leqslant 399$. Despite the small parameters involved, the proofs seem to require considerable effort. Such proofs appear to be worth pursuing, however, since in conjunction with Theorem 5.1 and Theorem 6.1, these two specific results imply many new upper and lower bounds on q-covering numbers for $q = 2$ (cf. Section 8). The bound $\mathcal{C}_2(7,3,2) \leqslant 399$ is also important in connection with the question of existence (or nonexistence) of the Steiner structure $\mathscr{S}_q(7,3,2)$, as discussed in Section 9.

We already know from (7) that $\mathcal{C}_2(5,3,2) \leqslant 27$. In what follows, we present a series of lemmas that eventually lead to the conclusion that $\mathcal{C}_2(5,3,2) = 27$.

Let $\mathbb{S}$ be a q-covering design $\mathscr{C}_2(5,3,2)$ in $\mathbb{F}_2^5$, with $|\mathbb{S}| = \mathcal{C}_2(5,3,2)$. For each nonzero vector $\boldsymbol{x} \in \mathbb{F}_2^5$, we define $\mathbb{S}(\boldsymbol{x}) = \{V \in \mathbb{S} \,:\, \boldsymbol{x} \in V\}$.

Lemma 7.1. *For all nonzero $\boldsymbol{x} \in \mathbb{F}_2^5$, we have $|\mathbb{S}(\boldsymbol{x})| \geqslant 5$. Moreover, if $|\mathbb{S}(\boldsymbol{x})| = 5$ for some $\boldsymbol{x}$, then $V_i \cap V_j = \{\boldsymbol{0}, \boldsymbol{x}\}$ for all distinct $V_i, V_j \in \mathbb{S}(\boldsymbol{x})$.*

Proof. There are 30 nonzero vectors $\boldsymbol{y}$ distinct from $\boldsymbol{x}$. Each of the 30 pairs $\{\boldsymbol{x}, \boldsymbol{y}\}$ defines the two-dimensional subspace $\{\boldsymbol{0}, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{x}+\boldsymbol{y}\}$; therefore it must be contained in some subspace V of $\mathbb{S}(\boldsymbol{x})$. On the other hand, each given subspace V of $\mathbb{S}(\boldsymbol{x})$ contains $|V \backslash \{\boldsymbol{0}, \boldsymbol{x}\}| = 6$ such pairs. It follows that $|\mathbb{S}(\boldsymbol{x})| \geqslant 30/6$. Moreover, if this holds with equality, then the 6 pairs covered by the subspaces $V_1, V_2, \ldots, V_5$ in $\mathbb{S}(\boldsymbol{x})$ must be all different, which implies that $V_i \cap V_j = \{\boldsymbol{0}, \boldsymbol{x}\}$. □

Lemma 7.2. *Suppose that $|\mathbb{S}(\boldsymbol{x})| \geqslant 6$ for all nonzero $\boldsymbol{x} \in \mathbb{F}_2^5$. Then $|\mathbb{S}| \geqslant 27$.*

Proof. Consider the sum $\sum_{\boldsymbol{x}} |\mathbb{S}(\boldsymbol{x})| \geqslant 31{\cdot}6$, where the summation is over $\boldsymbol{x} \in \mathbb{F}_2^5 \backslash \{\boldsymbol{0}\}$. Each subspace $V \in \mathbb{S}$ is counted $|V \backslash \{\boldsymbol{0}\}| = 7$ times in this sum, so $|\mathbb{S}| \geqslant \lceil 186/7 \rceil$. □

In view of Lemma 7.2, let us henceforth consider the situation where $|\mathbb{S}(\boldsymbol{z})| = 5$ for some nonzero $\boldsymbol{z} \in \mathbb{F}_2^5$. For notational convenience, let us write:

$$\mathbb{S}(\boldsymbol{z}) \overset{\text{def}}{=} \{U_1, U_2, U_3, U_4, U_5\}$$

and define $\mathcal{U}_i \overset{\text{def}}{=} U_i \backslash \{\boldsymbol{0}, \boldsymbol{z}\}$ for $i = 1, 2, \ldots, 5$. With this, it follows from Lemma 7.1 that $\mathcal{U}_i \cap \mathcal{U}_j = \varnothing$ for all $i \neq j$, and therefore $\mathcal{U}_1 \cup \mathcal{U}_2 \cup \mathcal{U}_3 \cup \mathcal{U}_4 \cup \mathcal{U}_5 = \mathbb{F}_2^5 \backslash \{\boldsymbol{0}, \boldsymbol{z}\}$.

Lemma 7.3. *Consider a subspace V of $\mathbb{S}$ that does not contain $\boldsymbol{z}$. Then $|V \cap \mathcal{U}_i| = 3$ for some $i \in \{1,2,3,4,5\}$ and $|V \cap \mathcal{U}_j| = 1$ for all $j \neq i$ in $\{1,2,3,4,5\}$.*

Proof. Since $\mathcal{U}_1, \mathcal{U}_2, \mathcal{U}_3, \mathcal{U}_4, \mathcal{U}_5$ form a partition of $\mathbb{F}_2^5 \backslash \{\boldsymbol{0}, \boldsymbol{z}\}$ and $V \backslash \{\boldsymbol{0}\}$ is a subset of $\mathbb{F}_2^5 \backslash \{\boldsymbol{0}, \boldsymbol{z}\}$, we have $\sum_{i=1}^5 |V \cap \mathcal{U}_i| = 7$. Furthermore, since

$$\dim\bigl(V \cap U_i\bigr) \;=\; \dim V + \dim U_i - \dim\bigl(V + U_i\bigr) \;\geqslant\; 3 + 3 - 5 \;=\; 1,$$

we must have $|V \cap U_i| = 2$ or $|V \cap U_i| = 4$ for all i. This implies that $|V \cap \mathcal{U}_i| = 1$ or $|V \cap \mathcal{U}_i| = 3$ for all $i \in \{1,2,3,4,5\}$, and the lemma follows. □

Next, let $\mu(\mathcal{U}_i)$ denote the number of subspaces V of $\mathbb{S}$ that intersect $\mathcal{U}_i$ in exactly three points. That is, $\mu(\mathcal{U}_i) = \bigl|\{V \in \mathbb{S} \,:\, |V \cap \mathcal{U}_i| = 3\}\bigr|$. Further, let us assume without loss of generality that $\mu(\mathcal{U}_1) \leqslant \mu(\mathcal{U}_2) \leqslant \mu(\mathcal{U}_3) \leqslant \mu(\mathcal{U}_4) \leqslant \mu(\mathcal{U}_5)$.

Lemma 7.4. *Suppose that $\mu(\mathcal{U}_1) \geqslant 5$. Then $|\mathbb{S}| \geqslant 30$.*

Proof. By Lemma 7.3, each subspace V in $\mathbb{S} \backslash \mathbb{S}(\boldsymbol{z})$ intersects exactly one $\mathcal{U}_i$ in three points. Hence $|\mathbb{S}| = |\mathbb{S}(\boldsymbol{z})| + \sum_{i=1}^5 \mu(\mathcal{U}_i) \geqslant 5 + 5\mu(\mathcal{U}_1) \geqslant 30$. □

Lemma 7.5. *Suppose that $\mu(\mathcal{U}_1) = 0$. Then $|\mathbb{S}| \geqslant 29$.*

Proof. Let us write $\mathcal{U}_1 = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_6\}$. We know from Lemma 7.1 that $|\mathbb{S}(\boldsymbol{x}_i)| \geqslant 5$ for all i. Thus, for each i, there are at least 5 subspaces in $\mathbb{S}$ that contain $\boldsymbol{x}_i$. Of course, one of these subspaces is U_1. We claim that the others are all different — that is, the sets $\mathbb{S}(\boldsymbol{x}_i)\backslash\{U_1\}$ are disjoint. Indeed, assume to the contrary that there exists a subspace V in $\mathbb{S}\backslash\{U_1\}$ that contains both $\boldsymbol{x}_i$ and $\boldsymbol{x}_j$. But then $|V \cap \mathcal{U}_1| \geqslant 2$, in contradiction to Lemma 7.3 and the assumption that $\mu(\mathcal{U}_1) = 0$. This establishes our claim which, in turn, implies that $|\mathbb{S}| \geqslant |\mathbb{S}(\boldsymbol{z})| + \sum_{i=1}^{6} |\mathbb{S}(\boldsymbol{x}_i)\backslash\{U_1\}| \geqslant 5 + 6\cdot 4 = 29$. □

Lemma 7.6. *Suppose that $\mu(\mathcal{U}_1) = 1$. Then $|\mathbb{S}| \geqslant 27$.*

Proof. The proof is similar to that of Lemma 7.5, except that now there is exactly one subspace V in $\mathbb{S}\backslash\{U_1\}$ that contains 3 elements from the set $\mathcal{U}_1 = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_6\}$. This subspace is counted thrice in $\sum_{i=1}^{6} |\mathbb{S}(\boldsymbol{x}_i)\backslash\{U_1\}|$ while all the other subspaces of $\mathbb{S}\backslash\mathbb{S}(\boldsymbol{z})$ are counted at most once. Hence $|\mathbb{S}| \geqslant |\mathbb{S}(\boldsymbol{z})| + \sum_{i=1}^{6} |\mathbb{S}(\boldsymbol{x}_i)\backslash\{U_1\}| - 2 \geqslant 27$. □

In view of Lemma 7.4, Lemma 7.5, and Lemma 7.6, it remains to deal with the case where $\mu(\mathcal{U}_1) \in \{2, 3, 4\}$. This case requires an elaborate analysis, during which we will make use of the next two lemmas.

Lemma 7.7. *Suppose that $\mu(\mathcal{U}_1) \geqslant 1$ and consider a subspace V of $\mathbb{S}\backslash\{U_1\}$ such that $|V \cap \mathcal{U}_1| = 3$. Then $|\mathbb{S}(\boldsymbol{x})| \geqslant 6$ for all $\boldsymbol{x} \in (V \cap \mathcal{U}_1)$.*

Proof. By Lemma 7.1, if $|\mathbb{S}(\boldsymbol{x})| = 5$ then any two subspaces of $\mathbb{S}$ that contain $\boldsymbol{x}$ intersect in exactly two points, namely $\{\mathbf{0}, \boldsymbol{x}\}$. However, in the situation at hand, both V and U_1 contain $\boldsymbol{x}$ and $|V \cap U_1| = 4$. □

Lemma 7.8. *Suppose that $\mu(\mathcal{U}_1) \geqslant 2$ and consider two subspaces V_1, V_2 of $\mathbb{S}\backslash\{U_1\}$ such that $|V_1 \cap \mathcal{U}_1| = |V_2 \cap \mathcal{U}_1| = 3$. Then $|\mathbb{S}(\boldsymbol{x})| \geqslant 7$ for all $\boldsymbol{x} \in (V_1 \cap V_2 \cap \mathcal{U}_1)$.*

Proof. Assume the contrary that $|\mathbb{S}(\boldsymbol{x})| < 7$. Then $|\mathbb{S}(\boldsymbol{x})| = 6$ by Lemma 7.7, and therefore, in addition to V_1, V_2 and U_1, the vector $\boldsymbol{x}$ is contained in three other subspaces of $\mathbb{S}$, say V_3, V_4, V_5. By Lemma 7.3, each of the five subspaces V_1, V_2, V_3, V_4, V_5 intersects exactly one of $\mathcal{U}_1, \mathcal{U}_2, \mathcal{U}_3, \mathcal{U}_4, \mathcal{U}_5$ in three points and all the others in one point. Since $|V_1 \cap \mathcal{U}_1| = |V_2 \cap \mathcal{U}_1| = 3$, this implies that at least one of the sets $\mathcal{U}_2, \mathcal{U}_3, \mathcal{U}_4, \mathcal{U}_5$ intersects each of V_1, V_2, V_3, V_4, V_5 in exactly one point. W.l.o.g., let $\mathcal{U}_5$ be this set. Then $\mathcal{U}_5$ contains a nonzero vector $\boldsymbol{y}$ that does not belong to any of V_1, V_2, V_3, V_4, V_5. Now consider the two-dimensional subspace $\{\mathbf{0}, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{x}+\boldsymbol{y}\}$, which must be contained in some subspace of $\mathbb{S}(\boldsymbol{x})$. But $\mathbb{S}(\boldsymbol{x}) = \{U_1, V_1, V_2, V_3, V_4, V_5\}$ and none of its elements contains $\boldsymbol{y}$, a contradiction. □

Lemma 7.9. *Suppose that $\mu(\mathcal{U}_1) \in \{2, 3, 4\}$. Then $|\mathbb{S}| \geqslant 27$.*

Proof. Henceforth, in order to simplify notation, let us denote $m \overset{\text{def}}{=} \mu(\mathcal{U}_1)$. Consider the following bipartite graph G. The left vertices of G are the elements of the set $\mathcal{U}_1 = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_6\}$, and the right vertices of G are the subspaces V of $\mathbb{S}$ such that $|V \cap \mathcal{U}_1| = 3$. Thus there are 6 left vertices and m right vertices, say $V_1, V_2, \ldots, V_m$. There is an edge $\{\boldsymbol{x}_i, V_j\}$ in G iff $\boldsymbol{x}_i \in V_j$. Thus the total number of edges in G is $3m$. For each $\boldsymbol{x}_i \in \mathcal{U}_1$, let $\deg(\boldsymbol{x}_i)$ denote the degree of $\boldsymbol{x}_i$ in G. Note that if $\deg(\boldsymbol{x}_i) \geqslant 1$, then $|\mathbb{S}(\boldsymbol{x}_i)| \geqslant 6$ by Lemma 7.7 and if $\deg(\boldsymbol{x}_i) \geqslant 2$, then $|\mathbb{S}(\boldsymbol{x}_i)| \geqslant 7$ by Lemma 7.8. Let ν_d denote the number of elements $\boldsymbol{x}_i$ in $\mathcal{U}_1$ with $\deg(\boldsymbol{x}_i) = d$. The equality

$$\nu_1 + 2\nu_2 + \cdots + m\nu_m \;=\; 3m \tag{10}$$

is easily obtained by counting the edges of G (note that the total number of edges is $3m$, and $\deg(\boldsymbol{x}_i) \leqslant m$ for all i, since m is the number of right vertices in G).

We now proceed as in Lemma 7.6 and consider the sum $\sum_{i=1}^{6} |\mathbb{S}(\boldsymbol{x}_i)\backslash\{U_1\}|$. Each of the m subspaces $V_1, V_2, \ldots, V_m$ that intersect $\mathcal{U}_1$ in 3 points is counted three times in this sum, while all other subspaces of $\mathbb{S}\backslash\mathbb{S}(\boldsymbol{z})$ are counted at most once. Hence

$$\begin{aligned}|\mathbb{S}| &\geqslant |\mathbb{S}(\boldsymbol{z})| + \sum_{i=1}^{6} |\mathbb{S}(\boldsymbol{x}_i)\backslash\{U_1\}| - 2m \\ &\geqslant 5 + 6\cdot 4 + \nu_1 + 2(\nu_2+\nu_3+\cdots+\nu_m) - 2m,\end{aligned}$$

where the second inequality follows from Lemma 7.7 and Lemma 7.8. Therefore, to prove that $|\mathbb{S}| \geqslant 27$, it suffices to show that $\nu_1 + 2(\nu_2+\nu_3+\cdots+\nu_m) \geqslant 2m-2$. Consider minimizing the function $\nu_1 + 2(\nu_2+\nu_3+\cdots+\nu_m)$ subject to the constraint in (10). It is easy to see that the solution to this minimization problem is given by $\nu_1 + 2(\nu_2+\nu_3+\cdots+\nu_m) = 6$ for all $m \geqslant 2$ (obtained for $\nu_1 = \nu_2 = \cdots = \nu_{m-1} = 0$ and $\nu_m = 3$). Since $2m-2 \leqslant 6$ for $m \in \{2,3,4\}$, the lemma follows. □

Theorem 7.10. *$\mathcal{C}_2(5,3,2) = 27$.*

Proof. As before, let $\mathbb{S}$ be a q-covering design $\mathscr{C}_2(5,3,2)$ in $\mathbb{F}_2^5$, with $|\mathbb{S}| = \mathcal{C}_2(5,3,2)$. The cases considered in Lemma 7.2, Lemma 7.4, Lemma 7.5, Lemma 7.6, and Lemma 7.9 are exhaustive, and in each case we have proved that $|\mathbb{S}| \geqslant 27$. The fact that $\mathcal{C}_2(5,3,2) \leqslant 27$ follows from the construction in (7). □

Theorem 7.10 stems from an elaborate proof of a lower bound on $\mathcal{C}_2(n,k,r)$ for a specific set of parameters. In contrast, the next result in this section is an explicit construction, which gives an upper bound on $\mathcal{C}_2(n,k,r)$ for a specific set of parameters. Our construction is based upon difference sets. Specifically, let

$$A_1 = \{0,1,4,16\}, \tag{11}$$

$$A_2 = \{0,2,8,32\}, \tag{12}$$

$$A_3 = \{0,5,27,40\}, \tag{13}$$

$$A_4 = \{0,7,44,53\}, \tag{14}$$

$$A_5 = \{0,11,29,49\}. \tag{15}$$

Lemma 7.11. *Define $\mathcal{D}_i \overset{\text{def}}{=} \{a-b \pmod{63} : a,b \in A_i,\ a \neq b\}$ for $i = 1,2,\ldots,5$. Then $|\mathcal{D}_i| = 12$ for all $i = 1,2,\ldots,5$, and $\mathcal{D}_1 \cup \mathcal{D}_2 \cup \mathcal{D}_3 \cup \mathcal{D}_4 \cup \mathcal{D}_5 = \mathbb{Z}_{63}\backslash\{0,21,42\}$.*

Proof. Follows by direct verification. □

Theorem 7.12. *$\mathcal{C}_2(7,3,2) \leqslant 399$.*

Proof. Let α be a root of the primitive polynomial x^6+x+1, and hence a primitive element in $\mathbb{F}_{64}$. We represent $\mathbb{F}_2^7$ as $\mathbb{F}_2^7 = \{(\beta,0) : \beta \in \mathbb{F}_{64}\} \cup \{(\beta,1) : \beta \in \mathbb{F}_{64}\}$. We furthermore introduce the following notation: given a subset X of $\mathbb{F}_2^7$ and an element γ of $\mathbb{F}_{64}$, we define $\gamma X = \{(\gamma\beta,0) : (\beta,0) \in X\} \cup \{(\gamma\beta,1) : (\beta,1) \in X\}$. Notice that if X is a *subspace* of $\mathbb{F}_2^7$, then so is γX for all $\gamma \in \mathbb{F}_{64}$. With reference to (11)–(15), let us now construct the sets $X_{1,0}, X_{2,0}, X_{3,0}, X_{4,0}, X_{5,0}$ as follows:

$$\begin{aligned}
X_{1,0} &= \{\mathbf{0}, (1+\alpha^1,0), (1+\alpha^4,0), (1+\alpha^{16},0), (1,1), (\alpha^1,1), (\alpha^4,1), (\alpha^{16},1)\}, \\
X_{2,0} &= \{\mathbf{0}, (1+\alpha^2,0), (1+\alpha^8,0), (1+\alpha^{32},0), (1,1), (\alpha^2,1), (\alpha^8,1), (\alpha^{32},1)\}, \\
X_{3,0} &= \{\mathbf{0}, (1+\alpha^5,0), (1+\alpha^{27},0), (1+\alpha^{40},0), (1,1), (\alpha^5,1), (\alpha^{27},1), (\alpha^{40},1)\}, \\
X_{4,0} &= \{\mathbf{0}, (1+\alpha^7,0), (1+\alpha^{44},0), (1+\alpha^{53},0), (1,1), (\alpha^7,1), (\alpha^{44},1), (\alpha^{53},1)\}, \\
X_{5,0} &= \{\mathbf{0}, (1+\alpha^{11},0), (1+\alpha^{29},0), (1+\alpha^{49},0), (1,1), (\alpha^{11},1), (\alpha^{29},1), (\alpha^{49},1)\}.
\end{aligned}$$

Given the sets A_1, A_2, A_3, A_4, A_5 in (11)–(15), it is easy to verify that $\alpha + \alpha^4 + \alpha^{16} = \alpha^2 + \alpha^8 + \alpha^{32} = \alpha^5 + \alpha^{27} + \alpha^{40} = \alpha^7 + \alpha^{44} + \alpha^{53} = \alpha^{11} + \alpha^{29} + \alpha^{49} = 1$. This, in turn, implies that each of the sets $X_{1,0}, X_{2,0}, X_{3,0}, X_{4,0}, X_{5,0}$ is a three-dimensional subspace of $\mathbb{F}_2^7$. Let us now construct $62 \cdot 5 = 310$ additional three-dimensional subspaces of $\mathbb{F}_2^7$ as follows:

$$X_{i,j} \overset{\text{def}}{=} \alpha^j X_{i,0} \qquad \text{for } i = 1, 2, \ldots, 5 \text{ and } j = 1, 2, \ldots, 62, \tag{16}$$

and let $\mathcal{X}$ denote the set of all the $5 + 310 = 315$ subspaces $X_{i,j}$. Next, we construct a three-dimensional subspace Y_0 of $\mathbb{F}_2^7$ as follows:

$$Y_0 = \big\{\mathbf{0}, (1,0), (\alpha^{21},0), (\alpha^{42},0), (0,1), (1,1), (\alpha^{21},1), (\alpha^{42},1)\big\},$$

and define $Y_j \overset{\text{def}}{=} \alpha^j Y_0$ for $j = 1, 2, \ldots, 20$. Let $\mathcal{Y}$ be the set of all the 21 subspaces Y_j. Finally, construct a three-dimensional subspace Z_0 of $\mathbb{F}_2^7$ as follows:

$$Z_0 = \big\{\mathbf{0}, (1,0), (\alpha,0), (\alpha^4,0), (\alpha^6,0), (\alpha^{16},0), (\alpha^{24},0), (\alpha^{33},0)\big\},$$

and define $Z_j \overset{\text{def}}{=} \alpha^j Z_0$ for $j = 1, 2, \ldots, 62$. Let $\mathcal{Z}$ be the set of all the 63 subspaces Z_j. The resulting q-covering design $\mathscr{C}_2(7,3,2)$ in $\mathbb{F}_2^7$ is $\mathbb{S} = \mathcal{X} \cup \mathcal{Y} \cup \mathcal{Z}$. It is clear that $|\mathbb{S}| = 315 + 21 + 63 = 399$. The fact that every two-dimensional subspace of $\mathbb{F}_2^7$ is contained in some subspace of $\mathbb{S}$ can be verified using a simple computer program.

This fact can be also proved by hand; we give only a sketch of the proof here. It is easy to see that each of the 63 subspaces of the form $\big\{\mathbf{0}, (0,1), (\alpha^j,1), (\alpha^j,0)\big\}$ is contained in exactly one subspace of $\mathcal{Y}$. Moreover, it follows from Lemma 7.11 that every pair of vectors of the form $\{(\alpha^a,1), (\alpha^b,1)\}$, where a, b are distinct elements of $\mathbb{Z}_{63}$, is contained in exactly one subspace of $\mathcal{X} \cup \mathcal{Y}$. Therefore, each of the $\binom{63}{2} = 1953$ subspaces of the form $\big\{\mathbf{0}, (\alpha^a,1), (\alpha^b,1), (\alpha^a + \alpha^b, 0)\big\}$ is contained in exactly one subspace of $\mathcal{X} \cup \mathcal{Y}$. Note that $\begin{bmatrix}7\\2\end{bmatrix}_2 - 63 - 1953 = \begin{bmatrix}6\\2\end{bmatrix}_2$ and, indeed, it remains to consider the $\begin{bmatrix}6\\2\end{bmatrix}_2 = 651$ two-dimensional subspaces that belong to $\mathbb{F}_2^6 \times \{0\}$. Of these, each of the $4 \cdot 63 + 21 = 273$ subspaces of the form:

$$\begin{aligned}
&\big\{\mathbf{0}, (\alpha^j,0), (\alpha^{j+7},0), (\alpha^{j+26},0)\big\} && \text{for } j = 0, 1, \ldots, 62,\\
&\big\{\mathbf{0}, (\alpha^j,0), (\alpha^{j+9},0), (\alpha^{j+45},0)\big\} && \text{for } j = 0, 1, \ldots, 62,\\
&\big\{\mathbf{0}, (\alpha^j,0), (\alpha^{j+11},0), (\alpha^{j+25},0)\big\} && \text{for } j = 0, 1, \ldots, 62,\\
&\big\{\mathbf{0}, (\alpha^j,0), (\alpha^{j+13},0), (\alpha^{j+35},0)\big\} && \text{for } j = 0, 1, \ldots, 62,\\
&\big\{\mathbf{0}, (\alpha^j,0), (\alpha^{j+21},0), (\alpha^{j+42},0)\big\} && \text{for } j = 0, 1, \ldots, 20
\end{aligned}$$

belongs to at least one subspace of $\mathcal{X} \cup \mathcal{Y}$. The remaining 378 two-dimensional subspaces of $\mathbb{F}_2^6 \times \{0\}$ have the form $\big\{\mathbf{0}, (\alpha^j,0), (\alpha^{2^i+j},0), (\alpha^{3\cdot 2^{i+1}+j},0)\big\}$ for $i = 0, 1, \ldots, 5$ and $j = 0, 1, \ldots, 62$, and each of them is contained in at least one subspace of $\mathcal{Z}$. □

8. Tables of upper and lower bounds on $\mathcal{C}_2(n,k,r)$

In this section, we compile tables of upper and lower bounds on q-covering numbers $\mathcal{C}_q(n,k,r)$, for $q = 2$ and $n \leqslant 8$. The lower bounds follow from Theorem 4.6, Corollary 4.11, Theorem 5.1, Corollary 5.2, Theorem 5.3, and Theorem 7.10. The upper bounds follow from Theorem 4.6, Corollary 4.11, Theorem 6.1, and Theorem 7.12. In the tables below, we also made use of the trivial identity $\mathcal{C}_2(n,k,k) = \begin{bmatrix}n\\k\end{bmatrix}_2$ which determines the entries on the main diagonals. Another trivial identity is $\mathcal{C}_2(n,n,r) = 1$. Finally, the values of $\mathcal{C}_2(n,k,r)$ for $n \leqslant 3$ are also trivial.

Bounds on $\mathcal{C}_2(4,k,r)$

r	k		
	3	2	1
3	15		
2	7	35	
1	3	5	15

Bounds on $\mathcal{C}_2(5,k,r)$

r	k			
	4	3	2	1
4	31			
3	15	155		
2	7	27	155	
1	3	5	11	31

Bounds on $\mathcal{C}_2(6,k,r)$

r	k				
	5	4	3	2	1
5	63				
4	31	651			
3	15	114–123	1395		
2	7	21–27	99–115	651	
1	3	5	9	21	63

Bounds on $\mathcal{C}_2(7,k,r)$

r	k					
	6	5	4	3	2	1
6	127					
5	63	2667				
4	31	468–523	11811			
3	15	87–123	839–1043	11811		
2	7	21–27	77–99	381–399	2667	
1	3	5	9	19	43	127

Bounds on $\mathcal{C}_2(8,k,r)$

r	k						
	7	6	5	4	3	2	1
7	255						
6	127	10795					
5	63	1895–2155	97155				
4	31	353–523	6902–8867	200787			
3	15	85–123	634–915	6477–7427	97155		
2	7	21–27	75–99	323–403	1567–1775	10795	
1	3	5	9	17	37	85	255

We observe that the upper and lower bounds on $\mathcal{C}_2(n,k,r)$ coincide for all $n \leqslant 5$ (this is due in large part to the proof that $\mathcal{C}_2(5,3,2) = 27$ in Theorem 7.10). Thus the smallest unresolved case appears to be $21 \leqslant \mathcal{C}_2(6,4,2) \leqslant 27$. The most interesting unresolved case is $381 \leqslant \mathcal{C}_2(7,3,2) \leqslant 399$, as discussed in the next section.

9. Conclusions and open problems

We have introduced and studied the q-analogs of covering designs and Turán designs. We have also considered the q-analogs of Steiner systems, and derived a strong necessary condition for their existence. We conclude this paper with several open problems that are directly related to our results herein.

- Does a Steiner structure $\mathscr{S}_2(2,3,7)$ exist? Thomas studied this question in detail in [19, 20], but did not arrive at a definitive conclusion regarding the existence of $\mathscr{S}_2(2,3,7)$. Note that if $\mathscr{S}_2(2,3,7)$ exists it must contain 381 subspaces. Thus the q-covering design $\mathscr{C}_2(7,3,2)$ with 399 subspaces (constructed in Theorem 7.12) comes tantalizingly close. The closest result from the other direction — that is, a packing of three-dimensional subspaces of $\mathbb{F}_2^7$ such that no two intersect in the same two-dimensional subspace — is due to Kohnert and Kurz [12], who showed that it is possible to pack at least 304 three-dimensional subspaces of $\mathbb{F}_2^7$ in this manner.

- Do *any* nontrivial Steiner structures $\mathscr{S}_2(r,k,n)$ with $r \geqslant 2$ exist? $\mathscr{S}_2(2,3,7)$, if it exists, would be the smallest possible example of such a structure. However, if it turns out that $\mathscr{S}_2(2,3,7)$ does not exist, this would not preclude the existence of larger nontrivial Steiner structures with $r \geqslant 2$.
- Another set of parameters for which one might expect to determine the q-covering numbers exactly is $\mathcal{C}_2(n,n-2,2)$. From the tables compiled in the previous section, we see that $21 \leqslant \mathcal{C}_2(n,n-2,2) \leqslant 27$ for $n = 5,6,7,8$. This is not a coincidence — in fact, this is true for all $n \geqslant 5$. By Corollary 5.2, we have
$$\mathcal{C}_2(n,n-2,2) \geqslant \left\lceil \frac{2^n-1}{2^{n-2}-1} \left\lceil \frac{2^{n-1}-1}{2^{n-3}-1} \right\rceil \right\rceil = 21$$
for all $n \geqslant 6$. By Lemma 4.2, we have $\mathcal{C}_2(n,n-2,2) \leqslant \mathcal{C}_2(5,3,2)$ and from (7), we know that $\mathcal{C}_2(5,3,2) = 27$. Can the method of proof introduced in Theorem 7.10 be extended to larger values of n, in order to improve upon the lower bound $\mathcal{C}_2(n,n-2,2) \geqslant 21$?
- The construction method introduced in Theorem 7.12 is based on cyclic shifts in $\mathbb{F}_{64}$ (if we map the nonzero elements of a vector space $V \subset \mathbb{F}_{64}$ into the corresponding binary characteristic vector $\boldsymbol{x}_V = (x_0, x_1, \ldots, x_{62})$, then multiplication by an element of $\mathbb{F}_{64}$, as in (16), corresponds to a cyclic shift of $\boldsymbol{x}_V$). In the case of Theorem 7.12, such cyclic shifts produce a very efficient covering. We note that certain codes (packings) based upon cyclic shifts were constructed in [8] and [12]. However, in both cases, the methods used are ad-hoc. Is there a general construction method for such "cyclic" packings and/or coverings? In particular, can useful bounds on the parameters of such a packing or covering be obtained using algebraic techniques?

References

[1] R. Ahlswede, H. K. Aydinian and L. H. Khachatrian, *On perfect codes and related concepts*, Des. Codes Crypt., **22** (2001), 221–237.

[2] M. Braun, A. Kerber and R. Laue, *Systematic construction of q-analogs of t-(v,k,λ)-designs*, Des. Codes Crypt., **34** (2005), 55–70.

[3] T. Bu, *Partitions of a vector space*, Disc. Math., **31** (1980), 79–83.

[4] D. de Caen, *Extension of a theorem of Moon and Moser on complete subgraphs*, Ars Combinatoria, **16** (1983), 5–10.

[5] D. de Caen, *The current status of Turán's problem on hypergraphs*, in "Extremal Problems for Finite Sets" (eds. P. Frankl, Z. Füredi, G. Katona and D. Miklós), János Bolyai Mathematical Society, Budapest, (1991), 187–197.

[6] C. J. Colbourn and R. Mathon, *Steiner systems*, in "Handbook of Combinatorial Designs" (eds. C.J. Colbourn and J.H. Dinitz), CRC Press, Boca Raton, FL, (2007), 102–110.

[7] T. Etzion, *Perfect byte-correcting codes*, IEEE Trans. Inform. Theory, **44** (1998), 3140–3146.

[8] T. Etzion and A. Vardy, *Error-correcting codes in projective space*, IEEE Trans. Inform. Theory, **57** (2011), 1165–1173.

[9] S. J. Hong and A. M. Patel, *A general class of maximal codes for computer applications*, IEEE Trans. Comput., **21** (1972), 1322–1331.

[10] T. Itoh, *A new family of 2-designs over* $\mathrm{GF}(q)$ *admitting* $\mathrm{SL}_m(q^\ell)$, Geom. Dedicata, **69** (1998), 261–286.

[11] R. Koetter and F. R. Kschischang, *Coding for errors and erasures in random network coding*, IEEE Trans. Inform. Theory, **54** (2008), 3579–3591.

[12] A. Kohnert and S. Kurz, *Construction of large constant dimension codes with a prescribed minimum distance*, Lect. Notes Comput. Sci., **5393** (2008), 31–42.

[13] J. H. van Lint and R. M. Wilson, "A Course in Combinatorics," Cambridge University Press, 1992.

[14] M. Miyakawa, A. Munemasa and S. Yoshiara, *On a class of small 2-designs over* $\mathrm{GF}(q)$, J. Combin. Des., **3** (1995), 61–77.

[15] J. Schönheim, *On coverings*, Pacific J. Math., **14** (1964), 1405–1411.

[16] M. Schwartz and T. Etzion, *Codes and anticodes in the Grassman graph*, J. Combin. Theory Ser. A, **97** (2002), 27–42.

[17] H. Suzuki, *2-designs over* $\mathrm{GF}(2^m)$, Graphs Combin., **6** (1990), 293–296.

[18] H. Suzuki, *2-designs over* $\mathrm{GF}(q)$, Graphs Combin., **8** (1992), 381–389.

[19] S. Thomas, *Designs over finite fields*, Geom. Dedicata, **21** (1987), 237–242.

[20] S. Thomas, *Designs and partial geometries over finite fields*, Geom. Ded., **63** (1996), 247–253.

Received March 2010; revised October 2010.

E-mail address: etzion@cs.technion.ac.il
E-mail address: avardy@ucsd.edu